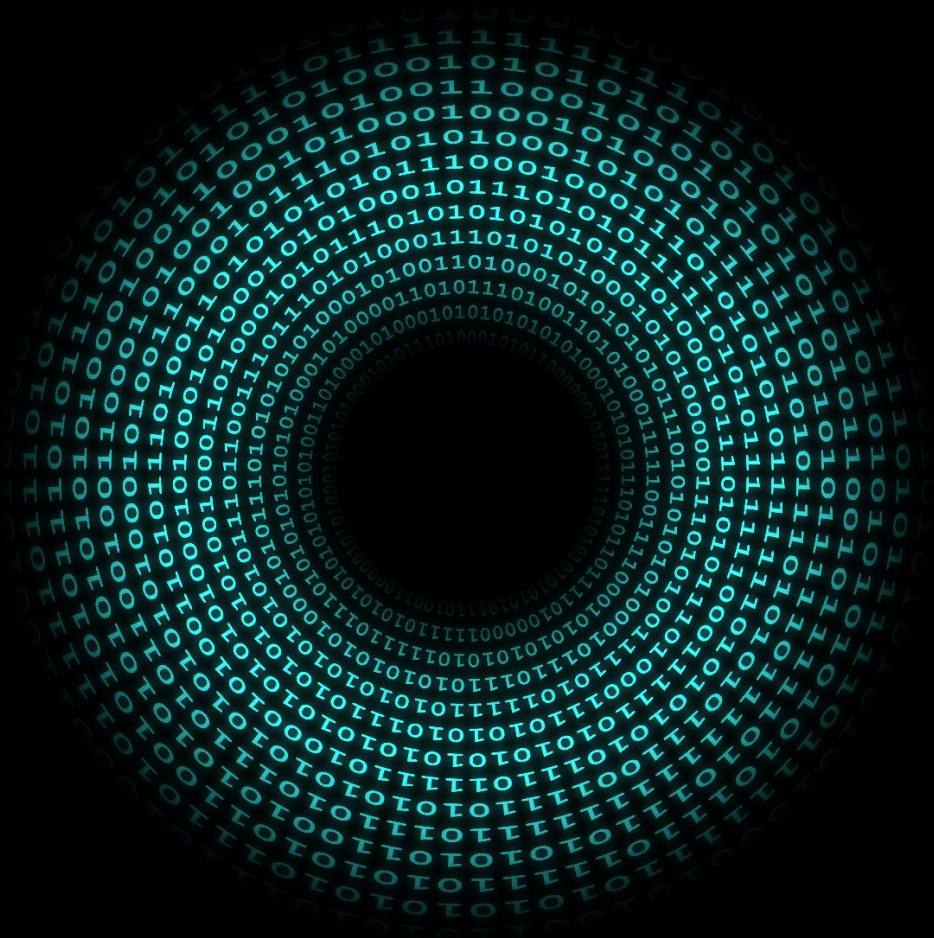
Zero Trust Architecture

Design Principles for a Transformation towards a Perimeter-less Enterprise Architecture

By T.P.J. Steenbrink



TU Delft

Deloitte.

Zero Trust Architecture

Design Principles for a Transformation towards a Perimeter-less Enterprise Architecture

By

T.P.J. Steenbrink

in partial fulfilment of the requirements for the degree of

Master of Science
in Complex Systems Engineering & Management

at the Delft University of Technology,
to be defended publicly on Friday, July 8, 2022, at 15:00 AM.

Supervision

TU Delft
Prof dr.ir. M.F.W.H.A. (Marijn) Janssen
Dr. ir. R.S. (Rolf) van Wegberg

Deloitte
S.F. (Sander) van den Bosch MSc.
M.N. (Marten) Posthumus MSc.

An electronic version of this thesis is available at http://repository.tudelft.nl/.

Cover Image source: Deloitte Brandspace – Circular motif

TU Delft

Deloitte.

Preface

Dear reader,

I am proud to introduce to you my final master thesis. Although I have enjoyed my time as a student at the Delft University of Technology, this journey would not have been possible without numerous people who helped me get through.

Marijn, I am grateful for being one of your students and writing my master thesis under your supervision. I very much enjoyed the bi-weekly connects; these sessions helped me make choices and narrow my scope. Furthermore, the meetings always motivated me to keep learning and be more curious about the "how and why" questions.

Marten, thank you for being my buddy at Deloitte for the past six months. I very much enjoyed the weekly check-ins and coffee breaks; these sessions helped me discover new ways to approach my research. Moreover, I enjoyed them, as there was room to talk about the "non-thesis" matters.

Sander, the bi-weekly meetings with you were a constant platform for ideation, brainstorming, questioning, and reflecting. I admire your drive and passion for Enterprise Architecture and Cloud transformations. Especially, I would like to thank you for providing feedback during your parental leave.

Rolf, I enjoyed the moments I could pass by your office to get some help while enjoying a cup of tea. I was impressed by your passion for combatting cybercrime and money laundering. Furthermore, I want to thank you for teaching me how to construct and analyse interviews to get the most insights out of them.

Then, a few people deserve a shout-out for keeping me company the last few months. The first group are the fellow interns, Derron, Joost, Linde, Martijn and Willemijn, for the discussions and always helping me move forward by sharing new ideas. Next, all the Deloitte Technology Strategy & Transformation team members, I will miss the coffee breaks, and lunch walks to 'Dagelijks lekker'. CosEMatties, Anniek, Anton and Valentijn, it always helped to share our thoughts during the master program and support each other. Last of all, I would like to express my gratitude to all the participants who took the time to participate in this research.

To conclude, I could not have done this without the support from my family and friends. First, I want to thank my roommates, Douwe, Ties, Tijn and Gaius. Throughout the past months, they have been a steady factor in my life, helping me structure my thoughts and always making me laugh when I needed it. Furthermore, I am grateful for my mother and sister's support throughout my studies as they were always there for me. The last thanks go out to my friends for giving me the right distraction when I needed it and for enduring my texts and calls of cancellation due to thesis work that had to be finished.

All in all, it was a memorable journey!

T.P.J. Steenbrink
Amsterdam, June 2022

Executive Summary

Recent advances in the field of 'Zero Trust' security strategies have revealed that there is still much novelty regarding the concept of Zero Trust architecture (ZTA). Zero Trust has recently gained attention as the traditional approach, based on network perimeter security, is being outplayed by sophisticated cyberattacks. This research contributes significantly to the scientific knowledge base, as ZTA is hardly investigated. Moreover, recent developments are causing the perimeter to disappear, such as increasing collaboration between companies, ecosystem connections, and working from home due to Covid-19. As a result, public and private organizations need to rethink how to protect their IT infrastructure, assets and data better.

Several organizations are willing to opt for a Zero Trust approach because of its benefits. These benefits include improved security, reduced complexity, and lower overhead and operational costs. Additionally, innovation in enterprise architecture security is urgently needed as it can reduce data breaches, decrease lateral movement, and avoid ransom payments and a company freeze.

Even though Zero Trust brings many advantages, it has not yet replaced existing perimeter-based security approaches. The complication is that many organizations struggle with the implementation of ZTA due to a lack of knowledge and unclarity on how to implement the Zero Trust security strategy. Additionally, "Zero Trust" is one of the most frequently used buzzwords in cybersecurity, making it hard to distinguish an actual ZTA. Complexity and misunderstandings of Zero Trust lead to failed projects and implementations. Furthermore, ZTA implementations are complex, and a predefined one-size-fits-all approach does not exist.

Moreover, organizations willing to transform their traditional architecture to a more advanced ZTA lack guidance in their transformation. However, Zero Trust solutions are marketed by multiple vendors, including Zscalar, IBM, Microsoft, and Palo Alto. There is no clear guidance for Enterprise Architects to support organizations in the transformation to a ZTA. Thus, research is needed to investigate 1) what Zero Trust architectures are, 2) what the challenges are, and 3) what the design principles for a successful ZTA transformation are.

The main research question is as follows:
How can enterprises transform their current [security] architecture by adopting Zero Trust concepts?

This question was answered using four sub-questions and approached as follows:

First, is analysed what defines a ZTA, which elements of an Enterprise Architecture (EA) are involved and what methods and techniques can be used to achieve such an architecture. The goal was to clarify Zero Trust, identify the frequently used ZTAs, and afterwards model various reference architectures that can be used in practice.

Second, the challenges that arise when realising a Zero Trust enterprise architecture are investigated. The goal was to gather empirical evidence from multiple perspectives to create an overview of challenges, limitations, pitfalls and success criteria to be conscious of.

Third, the design principles for Zero Trust EA transformations are examined. More specifically, the aim is to construct design principles for architects that can be used to transform the EA of an established organization.

Finally, the design principles are evaluated by experts in enterprise and security architecture. The sessions aimed to understand the practical value more thoroughly and get suggestions and recommendations to finetune the knowledge artefact.

The first question was answered with a multivocal literature study concentrating on the ZTA characteristics. Since not much is written about ZTA in formal literature, most data is retrieved from grey literature. In the conventional approach, endpoints and users are automatically trusted within the perimeter, allowing compromised accounts unrestricted access to resources, making the organization vulnerable. In contrast, a ZTA distinguishes itself from the conventional security architecture by not trusting endpoints, such as devices, applications and services, by default, even if the endpoints are part of the corporate network. Additionally, ZTA's are characterised by; 1) extensive identity & device verification, 2) segmentation on all architectural layers, 3) dynamic access policies, 4) active monitoring and 5) auto-remediation.

The second question was answered by interviewees (n=18) consisting of scientists, vendors, advisors, and project leads who shared the following insights about the creation of ZTAs. Most interviewees indicated that the cultural shift or form of cultural acceptance is the biggest challenge when creating a ZTA, as broader transformation efforts are needed. Additionally, formulating access policies is complicated due to the different interests of the stakeholders involved. It is crucial to start the ZTA project small at first with simple systems to ensure the transformation is not truncated prematurely. The legacy systems and operational technology equipment are elements that organizations hold back as they are hesitant to touch the "golden goose", the IT system that is generating the revenue. Although encrypting data-at-rest and data-in-transit is an excellent academic concept, putting it into practice is challenging as not all endpoints are equipped with the required processing power.

The third question was answered with two complementary instruments, interviews and desk research are used to formulate the design principles, resulting in a list of 12 design principles to guide the transformation. The list is structured into four categories to improve traceability: fundamentals, people, process and technology. The existing principles in white papers and webpages primarily focus on; 1) 'verification', 2) 'least privilege', and 3) 'visibility' but are missing a rationale and further implications. Moreover, they only focus on the target state and do not consider the transformation.

The fourth question was answered with the use of a workshop. The draft list of principles was reviewed by architects (n=17) of the Digital Architects NetWork, who provided suggestions and (partially) accepted the principles. This workshop ultimately resulted in 12 revised principles that can guide the architects in adopting Zero Trust concepts. The design principle perceived as the most relevant is 'enforce least privilege' as limiting the access rights is still one of the most effective precautions against the common adversary 'credential theft'.

This research contributes to the knowledgebase by providing; 1) a structured overview of the methods, technologies, capabilities, and reference architectures that can be used when adopting ZTAs, 2) an examination of the challenges, pitfalls, success criteria and limitations, 3) design principles accepted by lead architects that can be used for the transformation to a ZTA of public and private organizations.

Five concrete steps for further research are:

1. Focus on the impact on the end-user. As the implementation of Zero Trust becomes mature, scholars should evaluate the concept's value proposition using case studies. Using this empirical data will clarify the benefits and disadvantages of ZTAs to reduce the uncertainty concerning the novelty of the concept. Moreover, this will help identify the governance, risk, and compliance considerations for Zero Trust.
2. The principles should be put into practice with case studies to understand their practical value.
3. Research the generalizability of Zero Trust to smaller organizations or companies operating in various industries besides healthcare and industrials.
4. It would be interesting to learn more about the impact of culture as enterprises move towards these Zero Trust designs because many cultural issues have not been fully explored.
5. Finally, a ZTA transformation should be quantifiable, e.g., by quantifying the costs of replacing legacy to convince the executives to start the Zero Trust journey.

List of Acronyms

Acronym	Definition
BYOD	Bring Your Own Device
DAAS	Data, applications, assets, services
EA	Enterprise Architecture
MFA	Multi-Factor Authentication
OT	Operational Technology
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PoLP	Principle of Least Privilege
SDN	Software Defined Network
SDP	Software Defined Perimeter
ZT	Zero Trust
ZTA	Zero Trust Architecture

List of Tables

Table 1: EA Characteristics 11
Table 2: Internal interviews, Exploring, Focus on the ZT Value 18
Table 3: External interviews, Focus ZTA Challenges 18
Table 4: Comparison of Architecture Models 24
Table 5: ZTA Frameworks 28
Table 6: Alternatives for the configuration of governance 28
Table 7: Alternatives for the configuration of visibility & analytics 29
Table 8: Alternatives for the configuration of automation & orchestration 29
Table 9: Alternatives for the configuration of identity 30
Table 10: Alternatives for the configuration of endpoints 30
Table 11: Alternatives for the configuration of the network 30
Table 12: Alternatives for the configuration of data 31
Table 13: Alternatives for the configuration of applications 31
Table 14: Alternatives for the configuration of infrastructure 32
Table 15: Reference architectures 32
Table 16: Overview of existing principles 34
Table 17: Rules & Regulations focusing on information security 41
Table 18: Design principle template 46
Table 19: Design principle criteria (Rozanski, 2012) 47
Table 20: Overview of principle drivers 48
Table 21: Reduced list of credos 49
Table 22: Perceived importance of principles 58
Table 23: Overview of Final principles 65
Table 24: EA Definitions 77
Table 25: Overview of adversaries 79
Table 26: SLR protocol 80
Table 27: Formal Literature 82
Table 28: White papers 83
Table 29: ZT types in formal literature 84
Table 30: ZTA in white papers 84
Table 31: Overview of capabilities 85
Table 32: Overview of supporting technologies 86
Table 33: Applied codes 89
Table 34: Components of Architecture Principles according to TOGAF 105
Table 35: Overview of Credos 105

List of Figures

Figure 1: Elements of a socio-technical system (Bostrom, 1977) 2
Figure 2: Classic vs Zero Trust approach (OpenGroup, 2021) 3
Figure 3: Information System Research Framework (Hevner, 2004) 6
Figure 4: Design Science Research Cycles (Hevner, 2007) 7
Figure 5: Thesis Structure 9
Figure 6: BAIT Model, TOGAF 9.1 10
Figure 7: Overview of methods, tools and product 15
Figure 8: Design of Systematic Literature Review, adapted from (Kitchenham, 2007) 16
Figure 9: Overview of Research Method for Extracting Principles inspired by Bharosa (2015) 21
Figure 10: Process for formulating design principles (Greefhorst, 2011) 21
Figure 11: Distribution of publications 23
Figure 12: Simplistic representation of the data plane of the resource portal-based model 25
Figure 13: Simplistic representation of the data plane of the enclave-based model 25
Figure 14: Simplistic representation of the data plane of the device agent/gateway-based model 26
Figure 15: ZTA Foundation 27
Figure 16: Network diagram of codes used in Atlas.ti: 36
Figure 17: Code prevalence in interviews 37
Figure 18: Number of codes applied to an interview 37
Figure 19: Overview of new codes used over the time 38
Figure 20: Meaning saturation 38
Figure 21: Scope of Architects (Woods, 2010) 47
Figure 22: Overview of workshop participants 57
Figure 23: Assessment of design principles 58
Figure 24: Design principle framework 59
Figure 25: Venn diagram 80
Figure 26: Multivocal Literature Review 81
Figure 27: Code use in interviews 93
Figure 28: Zone Driven ZTA 95
Figure 29: Service Mesh driven ZTA 96
Figure 30: SDP Driven ZTA 97
Figure 31: Identity driven ZTA 98
Figure 32: Behaviour driven ZTA 99

Contents

Executive Summary ..... **I**
List of Acronyms ..... **III**
List of Tables ..... **IV**
List of Figures ..... **V**
Chapter 1. Introduction **1**
1.1 Problem introduction 1
1.1.1 Increase of cyber threats and attacks 1
1.1.2 Socio-technical nature 2
1.1.3 Need for a new EA approach 3
1.1.3 Zero Trust: a contribution to EA 3
1.1.4 Problem Statement 3
1.2 Core Concepts 4
1.3 Knowledge gap and Research objective 4
1.4 Research questions and approach 5
1.5 Research Method 6
1.5.1 Information System Research framework 6
1.5.2 Design Science Research Cycles 7
1.5.3 Risks 8
1.6 Research Scope & Focus 8
1.7 Research Flow Diagram 8
Chapter 2. Theoretical Background **10**
2.1 Enterprise Architecture 10
2.1.1 Architecture Security Strategies 11
2.2 Zero Trust Basics 12
2.2.1 The impact of Zero Trust on organizations 13
2.3 Enterprise Adversaries 13
2.4 Conclusion 14
Chapter 3. Research Method **15**
3.1 Method – Qualitative Study 15
3.2 Multivocal Literature Review 16
3.2.1 Systematic Literature Review 16
3.2.2 Grey Literature Review 16
3.3 Semi-structured Interviews 17
3.3.1 Planning 17
3.3.2 Overview of Interviewees 18

3.3.3 Interviews analysis in Atlas.ti ... 19
3.3.4 Assess output ... 20
3.4 Principle-based design ... 20
3.4.1 Approach ... 20
3.4.2 Process cycle of Greefhorst ... 21
3.5 Assessing Reliability and Validity ... 22
3.5.1 Reliability ... 22
3.5.2 Validity ... 22
Chapter 4. Zero Trust Architecture ... 23
4.1 Literature on Zero Trust Architecture Models & Strategies ... 24
4.1.1 Core components ... 24
4.1.2 ZTA models in literature ... 24
4.1.3 ZTA strategies in literature ... 26
4.2 Literature on ZTA Foundation ... 27
4.3 Literature on ZTA Configurations ... 28
4.4 Derived Reference Architectures ... 32
4.5 Literature focussing on Zero Trust Principles ... 34
4.6 Reflection on Literature ... 35
4.7 Conclusions ... 35
Chapter 5. ZTA Realisation Challenges ... 36
5.1 Atlas.ti Analysis ... 36
5.1.1 Overview of Codes ... 36
5.1.2 Code Prevalence ... 37
5.1.3 Code Saturation ... 37
5.1.3 Meaning Saturation ... 38
5.2 Interview Results ... 39
5.2.1 People in ZTA transformations ... 39
5.2.2 Process in ZTA transformations ... 40
5.2.3 Technology in ZTA transformations ... 40
5.2.4 Rules & Regulations applied to ZTA ... 41
5.2.5 Resources needed for realising a ZTA ... 41
5.2.6 Industry specials ... 42
5.2.7 ZTA Features ... 43
5.2.8 ZTA Tactics ... 44
5.3 Conclusion ... 45
Chapter 6. Design Principle Development ... 46

6.1 Proof of Principle-Based Design ... 46
6.1.1 Usefulness of principle-based design ... 46
6.1.2 Principle structure ... 46
6.1.3 Elements making a good design principle ... 47
6.1.3 Design principle criteria ... 47
6.2 Principle Formulation ... 48
6.2.1 Principle grounding ... 48
6.2.2 Principle drivers ... 48
6.2.3 Candidate principles ... 49
6.2.4 Testing of the preliminary list ... 49
6.2.5 Principle specification ... 50
6.2.6 Principle classification ... 55
6.3 Conclusion ... 56
Chapter 7. Practical Value ... 57
7.1 Principle Demonstration ... 57
7.2 Principle Evaluation ... 57
7.2.1 Workshop Goal & structure ... 57
7.2.2 Feedback ... 58
7.2.3 Workshop limitation ... 58
7.3 Principle Communication ... 59
7.4 Conclusion ... 62
Chapter 8. Conclusion & Discussion ... 63
8.1 Conclusion ... 63
8.2 Contribution of this research ... 66
8.3 Discussion, Limitations & Recommendations ... 66
8.3.1 Discussion of the findings ... 66
8.3.2 Limitations of the study ... 67
8.3.3 Recommendation ... 68
8.4 Reflection ... 69
8.4.1 Relevance of the research ... 69
8.4.2 Link with CoSEM ... 69
8.4.3 Reflection on the process ... 70
References ... 71
Appendix ... 77
Appendix A: Understanding of Traditional and ZT EA ... 77
Appendix B: Adversaries ... 79

Appendix C: Multivocal Literature Review 80
C1. Planning the review 80
C2. Conducting the review 81
C3. Reporting the Review 82
Appendix D: Interviews Protocols 87
Appendix E: Interview Analyses 89
Appendix F: Architypes 94
F1: Zone driven (software defined network) 95
F2: Service Mesh Driven 96
F3: SDP Driven 97
F4: Identity Driven 98
F5: Behaviour Driven 99
Appendix G: Existing principles 100
Appendix H: Design principles development 105

Chapter 1. Introduction

In this first chapter, the research will be introduced. First, the problem is described. Second, an overview of the core concepts is discussed. Third, the knowledge gap and research objectives are discussed. Fourth, the research questions and their approach are elaborated. Fifth, the chosen research method is described. Lastly, the research scope and focus are defined using a corresponding research flow diagram.

1.1 Problem introduction

Enterprise Architecture (EA), the conceptual blueprint defining IT, processes and governance, is becoming a vital aspect of public and private organizations (Hoogervorst, 2004; Winter, 2008). To ensure intellectual property and personal data are always secured, organizations and processes must change sincerely in the coming years, and so does the EA. Additionally, the number of data breaches increased by 30% in 2020 compared to the previous year, according to 'Autoriteit Persoonsgegevens' (Autoriteit Persoonsgegeven, 2021). Moreover, the focus of cybercriminals has shifted from individuals to businesses, making a solid EA even more essential (Meijer, 2021). This adjusted focus of attackers is due to the possible high success bonus when breaching large corporates (Trautman, 2018). A company freeze due to a cyberattack, ransomware, brute force attacks, data breach or Denial of Service will cost a significant quantity of money, so the willingness of a company to pay a ransom is high (Simmonds, 2017).

1.1.1 Increase of cyber threats and attacks

Incidents

Due to a series of incidents, cyber security became an important topic discussed by the chief executives of organizations active in both the private and public sectors. Numerous cyber-attacks caused significant damage in recent years, such as:

- In June 2017, the shipping conglomerate Maersk was hit by the powerful 'Not Petya' ransomware, infecting almost all their software and hardware systems except for one server rack, which was fortunately down due to a power failure. The consequence was a 9-day shutdown and a financial loss of $300 million lost revenue (Greenberg, 2017).
- In May 2021, Colonial Pipelines was hit by an attack that forced the organization to cut off the entire fuel supply for the east coast of the US. The organization could not resolve the hack, so it paid over $4 million to the hackers to turn its systems back on (Dudley, 2021).
- In October 2021, VDL Nedcar, an independent car manufacturer currently responsible for the production of BMW cars, was hit by a cyber-attack that caused an enterprise freeze for VDL and cost them €100 million (Van Rooij, 2021).
- In December 2021, multiple governments and banks took their systems offline as a precaution due to a 'code red' situation. The reason for this shutdown was a Denial-of-Service vulnerability discovered in a patch distributed for the Log4j application (Wijnen, 2021).

In 2021, the costs of an average data breach reached an all-time high, $4.24 million, according to the survey of IBM (2021). Experts believe that the number and impact of data breaches will increase even more in the future for various reasons. Some experts argue that the traditional "castle-and-moat" network security model cannot defend itself against increasingly more sophisticated cyber-attacks (Rose, 2020). This vulnerability exists because the conventional approach protection was placed on the perimeter, and once breached, a criminal has access to the

entire network. With a ZTA, the protection is placed on the asset itself, which requires continuous verification but prevents lateral movement.

Another reason the number of data breaches might grow is the increasing sophistication of attacks. At first, some standalone attackers felt the urge to prove that they could hack and break into systems despite antivirus programs. Several years later, so-called cluster attackers would target victims based on geography, political ideology, or solid financial standing. Attackers have recently established cybercrime networks that operate and profit like regular businesses and even recruit staff globally (AP, 2021).

Besides external attacks, preventing employees with wrong intentions from misusing their privileges becomes harder. Until the Covid-19 virus forced employees to work from home, company information and confidential intellectual property were stored within the company perimeters. However, research has shown that this hybrid way of working has become the new normal and is likely to stay in the post-pandemic years. (KPN, 2021). Lastly, the trends of "bring your own device" (BYOD) and "Internet of Things" (IoT) cause exponential growth of the existing network and even more complex network security (Moubayed, 2019), making it challenging to keep information secure (IBM, 2021).

1.1.2 Socio-technical nature

A transformation to a ZTA has a strong influence on the social and technical elements, which can be seen as a complex socio-technical system (Tangy, 2021). This impact is due to the highly complex, interconnected, multi-stakeholder and rapidly developing field. Figure 1 shows a simplistic representation of a socio-technical system (Bostrom, 1977), consisting of five elements that will be discussed below.

- **People**: The transformation will influence the duties, tasks, complexity of work, and competencies of the workforce. Moreover, the transformation will endorse values and personal and collective behaviour. The collaboration between actors is vital in achieving a Zero Trust philosophy as there is no silver bullet, and thus solutions of different vendors must be integrated.
- **Structure**: The transformation will impact the standardization, centralization, decentralization, hierarchy, external relationships and flexibility. Because one of the fundamentals of Zero Trust is architecture segmentation, resulting in those elements of the architecture can be isolated or placed into single containers.
- **Technology**: The right expertise is needed to leverage technology in establishing a ZTA. Organizations cannot create a safer environment without the right technology available. Besides, it is currently unclear how these technologies can be applied in different ecosystems as best practices of a ZTA are unknown, and there is not a single solution existing to achieve a ZTA.
- **Tasks**: The transformation will demand a reengineering of the existing processes and reconsidering process management and control. Because in a ZTA, access rights will be based on dynamic policies that must be formulated in collaboration with multiple teams.
- **Information Systems (MIS)**: Transformation can lead to introducing new information systems and replacing existing ones. Additionally, the integration amongst different Information Systems, the interoperability and IT infrastructure.

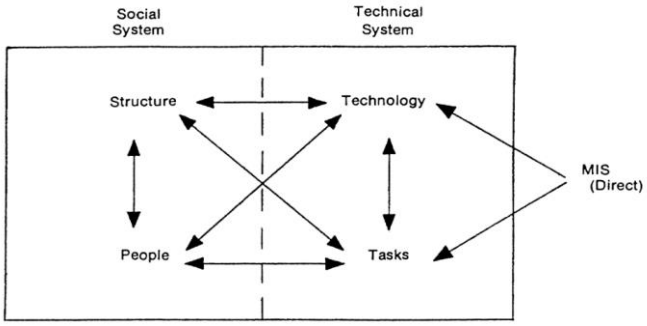


Figure 1: Elements of a socio-technical system (Bostrom, 1977)

1.1.3 Need for a new EA approach

To fix this socio-technical problem caused by the accelerating digital transformation, growing hybrid workforce, change in security operations, and continued migration to the cloud, a reconsideration of the current Enterprise Architecture leveraging network perimeter security is required (Sheridan, 2021; Embrey, 2022). Moreover, creating and maintaining secure network zones is complex. The data gathered from modern networks are not used for authentication. The conventional security strategy assumes that networks can be trusted based on the user's location. There is little to no control over the traffic inside a zone as everything is believed to be safe. Systems are chained together to ensure smooth data transfers. Although this approach sounds accurate, the right policies are needed to prevent lateral movement.

The need for a transformation can be seen as socially relevant since data breaches and external cyber-attacks are hitting private organizations, health care institutions, and universities. Therefore, "implicit trust" should be taken out of the equation as it is the single largest vulnerability in the way architects have designed in the past. (Seepers, 2020).

There is chosen for a 'transformation' instead of a 'change' to a ZTA because a transformation is more loosely defined, overarching, not concrete and defined. This action will be a better fit since the object focussed on is a socio-technical system.

1.1.3 Zero Trust: a contribution to EA

The previously discussed events could have been prevented if the IT infrastructures had undergone a transformation in which trust plays a less critical factor (Rose, 2020). One of these solutions is applying the so-called 'Zero Trust' core principles; 1) do not trust any device by default, 2) enforce least privilege access, and 3) implement comprehensive security monitoring. This strategic initiative ensures public and private companies a more secure IT infrastructure. Figure 2 shows a simplistic representation of the two different approaches. The classic approach is presented on the left side. In this architecture, the same entry point secures all data and assets. On the right side, the Zero Trust approach is presented in which the security is placed on the endpoint.

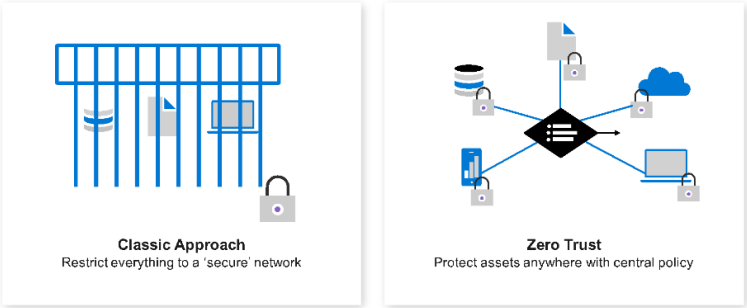


Figure 2: Classic vs Zero Trust approach (OpenGroup, 2021)

1.1.4 Problem Statement

It is unclear for organisations if and how they should incorporate ZT capabilities into their existing architecture. Given its potential, ZTA is a hot topic for many industries, but there is still much to be discovered. All major IT companies have recently published whitepapers on this topic; however, according to the sources, many things are still unclear about how these capabilities should be used in practice. Moreover, there is no clear starting point for a transformation (Campbell, 2020). Since ZTA is an innovative and novel technology, research should be conducted about what ZTA are, what challenges are of establishing a ZTA, and what design principles support the transformations of a traditional EA into a ZTA. The following problem statement has been formulated:

"***Zero Trust Architecture*** *can be significantly more robust against cyber-attacks than traditional EA; However, there is* ***no guidance*** *on how a traditional EA can be transformed into a* ***Zero Trust Architecture****."*

The research will contribute to society by creating design principles and reference architectures for public and private organizations to transform their EA into an environment in which Zero Trust is applied. Moreover, this will prevent the spread of malware, improve user productivity, and decrease the change of cyber-attacks (Rosencrance, 2021).

To summarize, the value of implementing a Zero Trust Architecture (ZTA) is evident, but many organizations do not know where to commence with the transformation. In addition, the technology is still in its infancy, making it challenging to establish a ZTA and improve cybersecurity successfully.

1.2 Core Concepts

To elucidate what "Zero Trust Enterprise Architecture Transformation" entails, a definition is provided for the following three elements; 'Zero Trust', 'Enterprise Architecture' and 'transformation'.

1. **Zero Trust (ZT)** is defined as:
   '*An evolving set of cybersecurity paradigms that move defences from static, network-based perimeters to focus on users, assets, and resources. It provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised (Rose, 2020).*'

Moreover, it is a concept that can be used for the EA of an organization, based on the principle of *never trust, always verify*. This thought helps prevent data breaches by eliminating the concepts of trust from an organization's architecture.

2. **Enterprise Architecture (EA)** is defined as:
   'The blueprint that documents all the information systems within the enterprise, their relationships, and how they interact to fulfil the enterprises mission (Langenberg, 2004).'

Likewise, the target architecture prescribes a set of desired capabilities and characteristics (Armour, 2001).

3. **Transformation** is defined as:
   'a second-order organizational change enabled by digital technologies transforming the way organizations are structured and organized and resulting in a new state, from the point of view of processes, culture, roles, relationships, and possibly all aspects of the organization.' (Levy, 1986)

1.3 Knowledge gap and Research objective

Knowledge gap

In literature, little can be found about what a state-of-the-art ZTA should resemble. Subsequently, there are few cases where a ZTA has been applied. The benefits of a ZTA are well described, but guidance is missing on how to implement the ZT concepts.

To conclude, there is a knowledge gap in the literature exploring the transformation to a Zero Trust EA.

1. There are no architypes or reference architectures available that can be followed when transforming to a Zero Trust EA.
2. There is no set of design principles focussing on ZTA transformations that guides an architect who wants to adopt Zero Trust elements in a traditional Enterprise Architecture.

Research objective

This research aims to define design principles for ZTA transformations and, as a result, increase an organization's cybersecurity. This study will identify the frequently used ZTA's through a Multivocal Literature Review (MLR) focusing on both formal and grey literature. Next, the challenges that arise when realising a ZTA are gathered via semi-structured interviews. Hereafter, design principles are digested from literature and interview transcripts to formulate design principles. Lastly, the guidelines will be evaluated during online workshops in which the design principles are reviewed to assess the practical value and formally accept them.

1.4 Research questions and approach

After identifying the knowledge gap, an adequate research approach was selected. For this research, a **qualitative approach** would be suitable as the objective is to understand better how a transformation to a Zero Trust EA can be performed.

The chosen approach will support the research activities which have to answer the research question (RQ):

*"How can enterprises transform their current [security] architecture by adopting **Zero Trust** concepts?"*

The main research question will be answered using four sub-questions described below.

Exploratory

The first question examines the various Zero Trust architectures described in formal and grey literature. The goal is to identify the frequently used configurations and model the variations that can be used in practice. Therefore, the first sub-question (SQ1) is:

"What defines a Zero Trust architecture?"

Strategic

The second question discovers the challenges of realising a Zero Trust Enterprise Architecture. The goal is to identify all obstacles that should be overcome when implementing a ZTA. Therefore, the second sub-question (SQ2) is:

"What are the challenges for realising a Zero Trust architecture?"

Tactical

The third question constructs the design principles for Zero Trust EA transformations. Design principles are defined by Bharosa (2015) as *"normative, reusable and directive guidelines, formulated towards taking action by the information system architects".* These principles can be interpreted as design rules for architects with room for adjustments without hard constraints or requirements. The goal is to create a framework that can be used to transform the EA of an established organization. Therefore, the third sub-question (SQ3) is:

"What are design principles for Zero Trust architecture transformations?"

Operational

The fourth question tests the practical value and relevance. Workshops with lead architects will be organised to receive feedback. During the session, suggestions and recommendations will be gathered to finetune the knowledge artefact. Therefore, the last sub-question (SQ4) is:

"To what extent are the created design principles usable in practice?"

1.5 Research Method

After defining the main and sub-questions, an acceptable research method can be chosen. The methodology used will be the 'Information System Research' (ISR) framework of Hevner (2004).

1.5.1 Information System Research framework

The ISR framework (Hevner, 2004) will be used to structure the research. The main research question can be subdivided into four elements that will form the research's backbone. The ISR framework is relevant as it considers both the business needs and the relevant knowledge aspects. In figure 3, the ISR framework is presented.

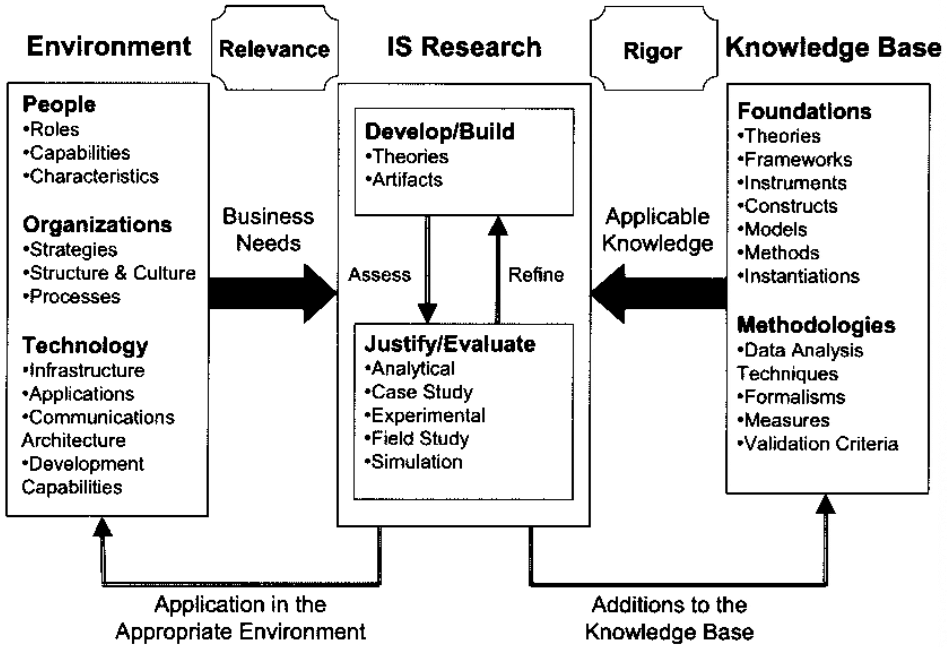


Figure 3: Information System Research Framework (Hevner, 2004)

The ISR framework is applied as follows:

Top right, the knowledge base consists of the Zero Trust architectures, capabilities and technologies derived from formal and grey literature. Additionally, existing Zero Trust principles are gathered. Theory focussing on the formulation of design principles and their structure.

Top left, the environment consists of cyber security, enterprise architecture and Zero Trust experts. The roles of these people are vendors, scientists, advisors, and project leads.

The build phase is positioned in the top middle, focusing on creating three knowledge artefacts: six reference architectures, a list of challenges and success criteria and design principles.

The justify phase is positioned in the bottom middle, where the design principles will be assessed and refined twice. The first assessment will be performed by the Chief Architect Community, a group of architects of large Dutch corporates, and members of the Digital Architects NetWork will perform the second assessment.

1.5.2 Design Science Research Cycles

In figure 4, the three 'design science research' cycles are presented. Each cycle is elaborated on below.

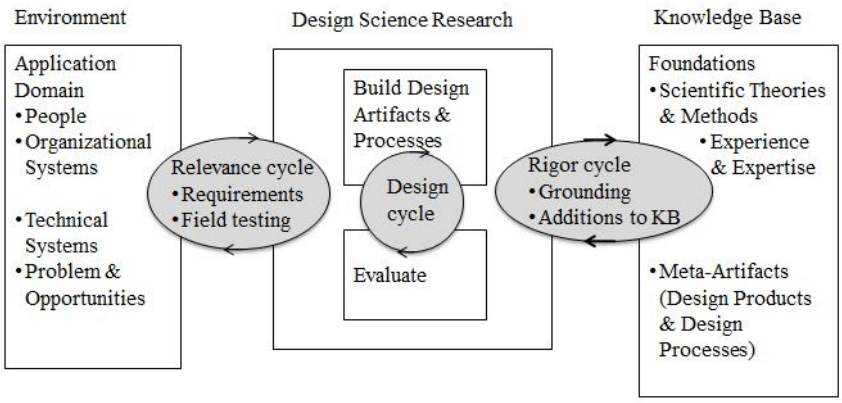


Figure 4: Design Science Research Cycles (Hevner, 2007)

The rigor cycle

The rigor cycle explores the theories, frameworks and white papers that exist. It ensures that the developed artefact is new and contributes to the existing knowledge base. In addition, this source of theories can help define new creative ideas (Hevner, 2007). Therefore, a systematic literature review is performed in the fourth chapter to 1) map the capabilities used to construct a ZTA and 2) visualise reference architectures that can be used during a ZTA transformation—resulting eventually in answer to the first sub-question of this study.

The data used for the research will be retrieved from three different sources: Google Scholar, Science Direct and Scopus. All references are stored in Mendeley. Since this research topic is novel, there is not much formal literature on the transformations to a ZTA. The small amount of existing information/literature is a limitation of the research. Therefore, both grey literature and white papers are included in the research.

The result of this cycle will be used to construct the protocols for the semi-structured interviews performed to retrieve business needs from the environment.

The relevance cycle

The relevance cycle is used to gather the business needs of the environment (Hevner, 2007) and improve the setting by building an artefact (Simon, 1996). Consequently, people with experience in realizing a ZTA are questioned. Empirical evidence will be gathered using semi-structured interviews, which should answer the second sub-question. Moreover, the results serve as input to build a knowledge artefact, a set of design principles in chapter 6.

The data will be retrieved from different sources to broaden the perspective of the challenges faced when realizing a ZTA. Evaluating this research through multiple lenses, such as advisors, scientists, and vendors, is essential.

The limitations of this step would be that time is scarce, and therefore only a limited number of practitioners can be interviewed.

The design cycle

The model's core is used in the design cycle to develop the artefact. The artefact's design is vital, but the performance of a scientific evaluation is even more critical. The Principle-Based Design methodology (Bharosa, 2015) uses the design cycle to construct design principles for ZTA transformations. This cycle should answer sub-question three, which focuses on the formulation of design principles. But also, on sub-question four, the last step of the research

is to test the practical value of the design principles. The rigor and relevance cycles are used for the artefact design as the principles are based on business needs and theoretical knowledge.

A limitation of this step can be testing the design principles because this is not possible in practice, as a ZTA transformation can take up to 4 years. Therefore, the justification and evaluation will be performed via two workshops with senior enterprise architects.

1.5.3 Risks

For this qualitative research, some aspects are crucial for making the research a success. The first drawback is that the number of experts who need to be interviewed is insufficient. Therefore, it is vital to start planning early to retrieve enough data; otherwise, the elbow curve will not be visible, and the statements are not supported by empirical evidence.

The second drawback that could happen is that the clients of the consulting firm Deloitte, which supports the research, do not want to participate in the study about Zero Trust EA transformations. If this is the case, new companies must be approached outside the Deloitte network to gain enough interviewees with ZT experience. Nonetheless, a plan B consists of a backup list of businesses that could be approached for the interviews. The last and most unfavourable drawback is insufficient data quality, causing incomplete answers to the research questions.

1.6 Research Scope & Focus

The focus of the research is on the following facets:

- EA transformations to a Zero Trust environment
- Organizations active in all industries
- Organizations that have applied Zero Trust/ are transforming to / have a Zero Trust EA
- Large companies with an international presence

1.7 Research Flow Diagram

The thesis will be subdivided into eight chapters, presented on the next page in figure 5. Below each chapter, the needed in and outputs are presented. If applicable, the sub or main question that will be answered is also highlighted.

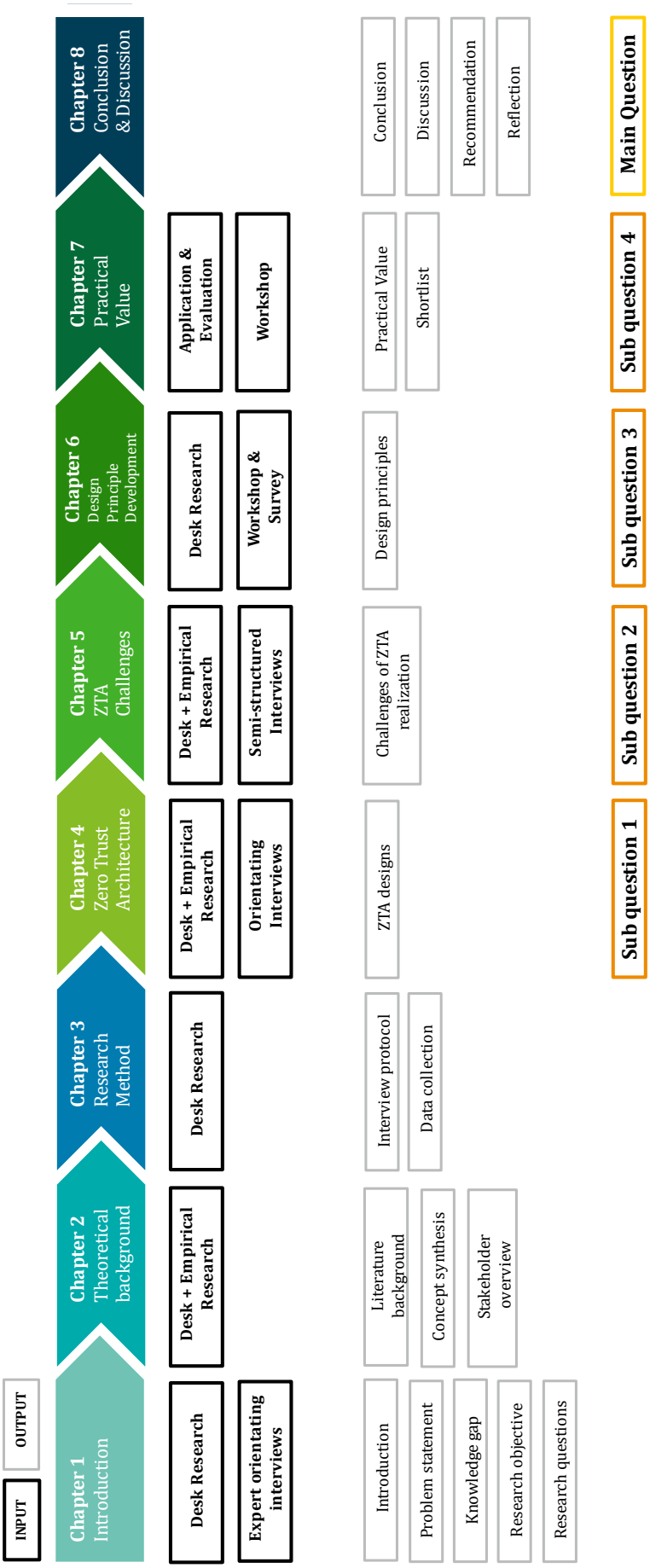


Figure 5: Thesis Structure

Chapter 2. Theoretical Background

In order to compare findings regarding Zero Trust, it is crucial to have a clear understanding of the scope of Enterprise Architecture research, what perspective the researchers take and to state what definitions are used throughout the research.

The purpose of this chapter is to provide relevant concepts and theories to understand the position of this research in the context of Enterprise Architecture transformation. First, in section 2.1, the concept of enterprise architecture is specified. Secondly, in section 2.2, the basics of Zero Trust are explained. Thirdly, in section 2.3, the enterprise adversaries are discussed to show which perils should be combated.

2.1 Enterprise Architecture

Enterprise Architecture (EA) is a broad concept defined in literature as a systematic and structured instrument to provide direction to the development of the ICT landscape and provide a holistic view of the organization (Janssen, 2012). Although there are different approaches in which an EA can support organizational change, the facilitating conditions are essential to ensure value creation within the organization. (Gong & Janssen, 2019). With the help of EA, organizations can become more agile over time as EA transformation can deliver significant value in a wide range of domains (Hoogervorst, 2004). Likewise, EA will make organizations more flexible and resilient (Korhonen & Halen, 2017). Therefore, enterprise architecture should play a pivotal role in governing the continuous improvement process of an enterprise (Proper, 2010).

How an EA is structured can vary, suggesting there is no right or wrong (Banaeianjahromi, 2016). The architect is free to choose which level of segregation will be applied. According to TOGAF 9.1, the EA can be seen as a pyramid separated into four layers, also referred to as the **BAIT** model. In figure 5, a visualisation is presented. At the top of the pyramid, the **B**usiness layer can be identified, which captures all processes and activities that an organization performs. Next is the **A**pplication layer. This layer is the interface for the business to get to their information or data. Below, the **I**nformation layer can be found, embodying data storage, analysis, and usage, including governance, to keep this layer organized. The **T**echnology layer can be found at the bottom, focusing on the needed hardware.

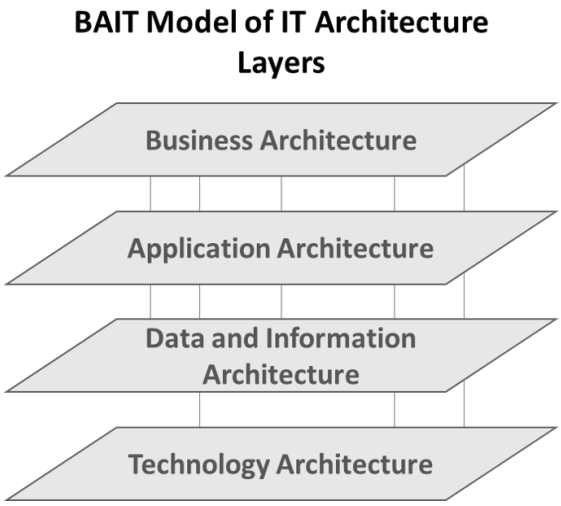


Figure 6: BAIT Model, TOGAF 9.1

2.1.1 Architecture Security Strategies

In this report, a distinction will be made between 'Traditional Architecture' and 'Zero Trust architecture'. Since it is not clear what is meant by these two architectures, an overview of the different interpretations used by the big IT corporates can be found in Appendix A. Moreover, a description of the strategies is presented below.

Traditional, perimeter-based EA
A traditional architecture provides users access to any application, server or other infrastructure using a trusted corporate network. Therefore, a perimeter-based network only trusts users inside a network. Users can be physically connected in an office or remotely via a VPN. The concept of a traditional EA, border security, splits networks into two categories: internal and external. The internal network covers all subjects within a hard border depending on the physical location of the devices, whereas the external network covers everything else. Firewalls, intrusion detection systems, intrusion prevention systems, and other security controls are typically deployed at the organization network's edges to create a secure boundary or "network perimeter" that separates its internal network from the rest of the internet. This concept is the foundation of perimeter-based network security (Teerakanok, 2021). In general, perimeter-based security makes use of implicit trust. Once a subject has been validated and granted access to the internal network, it is considered trustworthy indefinitely. This trust can result in a malicious, compromised subject that can execute more lateral movement and roam freely within the internal network. Moreover, a single point of attack can threaten the entire network.

Zero Trust, perimeter less EA
A ZTA uses the Zero Trust security strategy based on strong verification, granular access control and is designed to prevent data breaches (Rose, 2020). Moreover, the enterprise must assume that all the entities are untrusted, no matter their location. Therefore, enterprise-owned devices are not more trustworthy than private-owned devices (Teerakanok, 2021). However, solid authentication and authorisation can earn trust on a session basis.

To summarize, in table 1, a comparison is presented of traditional EA and a ZTA:

Table 1: EA Characteristics

Characteristic	Traditional EA	Zero Trust EA
Trust	Everything behind the Firewall is safe and trusted	No one is trusted, 'least privilege' access is provided
Infrastructure	On-premises	Cloud / hybrid
Defence placement	On the perimeter	On the application/trust zone
Security approach	Castle-and-moat	No perimeter
User and device verification	One time	Real-time, for every transaction
Segmentation	Macro-level	Micro-level, fine-grained
Activity monitoring	Intermittent	Continuous

In the next section, the concept of Zero Trust will be discussed more extensively.

2.2 Zero Trust Basics

Zero Trust can be seen as a concept focusing on access security (Kindervag, 2010) and as a set of security principles that treat every component, service and user of a system as continuously exposed to and potentially compromised by a malicious adversary (MIT Lincoln Laboratory, 2022). Moreover, Gilman (2017) describes that a Zero Trust architecture should follow a couple of fundamental rules. The first important aspect is that the network should always be assumed to be hostile as threats (internal and external) can always exist on the network. Therefore, network locality is insufficient for deciding a network's trustworthiness. Next, every device, user, and network flow should be authenticated and authorised. Lastly, policies must be dynamic and calculated from as many data sources as possible. Although Rose (2020) agrees with these statements, he adds in the publication of NIST that assets and workflows, moving between enterprise and non-enterprise infrastructure, should always have a consistent security policy and posture.

According to several web pages (ON2IT, 2022; ISACA, 2021) and whitepapers (Forrester, 2016; GSA, 2021), the concept of Zero Trust (ZT) was introduced in 2010 by John Kindervag when he presented a model at Forrester Research incl. (Kindervag, 2010). Although, this is not entirely valid as the term Zero Trust was already coined in the 90s in the doctoral thesis of Stephen Paul Marsh at the University of Stirling (Marsh, 1994). In addition, the 'Jericho forum' now called 'Open Group' already published a visioning white paper in February 2005 on the de-perimeterisation of enterprise architectures (Jericho Forum, 2005). Furthermore, in 2007 the Jericho Forum published the Jericho Commandments, a set of eleven fundamental rules that define the areas and the principles that must be observed when planning for a de-perimeterised future (Jericho Forum, 2007).

Nonetheless, John Kindervag was "the" person who popularised the concept of "Zero Trust" and therefore is seen as the founding father. Sometime later, Google started also using the two words in the marketing of Beyond Corp. This cloud solution was built in 2009 and used ZT elements in network security (Google, 2014). This solution accelerated the tech community's adoption, resulting in Gartner listing ZT as a core component of security in 2019 (Gartner, 2019). Next, the National Institute of Standards and Technologies (NIST), a scientific institution that is under the control of the United States federal government, started working on Zero Trust and published their approach and framework of Zero Trust in SP-800-207 (Rose, 2020). From 2020 onwards, ZT was widely promoted in the IT/security landscape, becoming a buzzword used by multiple vendors pretending they had the ZT solution.

Zero Trust is being misused as a marketing term. Vendors are applying the term 'Zero Trust' to market everything in security, creating significant marketing confusion.
Neil MacDonald – 2019 (Gartner)

A ZTA commonly includes six elements (Gilman, 2017):

1. **Identity verification**: strong multi-factor user and device authentication to assure 'least privilege.'
2. **Access control**: security and authentication of access to resources
3. **Resource protection**: fine-grained control of approved resource utilization based on identity.
4. **Policy and orchestration**: dynamic management of system use
5. **Monitoring and analytics**: analysing system usage and security functions
6. **Continuous operations**: the process of managing risks while supporting usability

Although there are many drivers for moving to a Zero Trust architecture, the value can be clustered into three different categories. The first driver is 'security'. As adversaries are becoming more sophisticated and are outmatching current cyber defences, new measures are needed to mitigate cyber risk. In addition, the shift to the

cloud is demanding a new approach to secure business-critical data (Deloitte, 2021). The second driver is 'flexibility' since the demand for better and easier business collaboration requires a more agile approach to security. Moreover, an increasingly mobile workforce now expects to be able to work from anywhere, from any device. The last driver is 'efficiency', as compliance costs rise due to overlapping and rigid controls and more strenuous requirements. Additionally, the rapid pace of digitalisation is increasing IT complexity and driving up costs.

There are some myths regarding Zero Trust that should be debunked. Starting with that, Zero Trust is an entirely new concept. This concept is not new, as it builds on earlier studies of the Jericho Forum. Next, Zero Trust has an end-state. Although a roadmap can have a finish line, Zero Trust has no final state as the level of granularity can be improved infinitely.

> *"One more time for those in the back: Zero Trust is an information security model, one that can be worked toward but without an ultimate end state."*
> *David Holmes - 2022 (Forrester)*

Third, Zero Trust is a one-size-fits-all solution. Also, this myth must be debunked as it needs to be tailor-made since each organization is different and can prioritise different capabilities.

2.2.1 The impact of Zero Trust on organizations

This section will describe the impact of technical solutions on organizations. Here, both the benefits and the barriers will be discussed.

Benefits: IBM (2021) published a study on the possible benefits of Zero Trust. The outcomes show that organisations that engage in Zero Trust save money as they can reduce the complexity of their IT infrastructure. According to Conningham (2017), eight benefits of Zero Trust can be defined which are: 1) Improvement of network visibility, breach detection, and vulnerability management, 2) Stopping the propagation of malware, 3) Reduction of both capital and operational expenditures on security 4) Reduction of the scope and cost of compliance initiatives 5) Elimination of intersilo finger-pointing 6) Increasing data awareness and insights 7) Stopping the exfiltration of sensitive data into the hands of malicious actors 8) Enabling digital business transformation

Barriers: Conforming with Zero Trust protocols can be challenging, requiring many custom configurations and time-intensive development projects. Moreover, the transformation requires a hodgepodge of tools to obey the three tenets of Zero Trust: segmentation, access control, and visibility. Next, the legacy systems and third-party applications that cannot be modified to conform to the Zero Trust model will have to be rebuilt. The performance will not get interfered by the security measures. Understanding the workforce is needed. Therefore, an adjustment of the mindset of the users is necessary.

2.3 Enterprise Adversaries

As described in section 1.1, Zero Trust can be a solution for cyber-attacks, one of the organizations' adversaries. The prioritisation of the protection can vary amongst industries as the violation concerns differ. According to Samonas (2014), the concerns can be clustered in the CIA Triad; 1) **C**onfidentiality, the unauthorized information release, 2) **I**ntegrity, the unauthorized information modification; and 3) **A**vailability, the unauthorized denial of use (Samonas, 2014). Confidentiality is the biggest fear for corporate networks as their intellectual property needs to be secured. This fear is different for mission systems, such as 'Intelligence Surveillance & Reconnaissance' (ISR) and 'Processing, Exploitation, and Dissemination' (PED) systems. Integrity is vital here as the main aim is command and control. Lastly, availability is significantly more important for critical infrastructures such as air traffic control as they must ensure flight safety. A system can be compromised via various routes. The ATT&CK framework (MITRE, 2022)

identifies cybercriminals' fourteen key tactics. In Appendix B, the adversaries are listed, and the Zero Trust elements are mapped against these adversaries to give an idea of their added value.

2.4 Conclusion

The goal of this chapter was to provide an overview of the relevant concepts and theories to understand the position of this research in the context of Enterprise Architecture transformation.

Enterprise architecture is a method to align the business and IT to streamline organisational processes. There are multiple frameworks that architects can use to create a holistic overview of the business in which the capabilities are mapped. Likewise, the methods needed to secure the architecture can vary. In most traditional architectures, the security was placed on the perimeter, but in Zero Trust architectures, there is no perimeter. Therefore, strong verification will occur before the end-user access to data or applications is provided.

Although the concept of 'Zero Trust' is marketed as something new, research shows that the name was already coined in 1994 by Stephen Paul Marsh during his PhD. Moreover, the idea of de-perimeterisation of the architecture was already discussed within the Jericho form in 2007. This publication could be seen as the starting point for developing a ZTA. Though it took some time before the concept gained attention, from 2020 onwards, ZT was widely promoted within the IT/security landscape.

The possible enterprise adversaries are diverse as cybercriminals try different methods and techniques to penetrate an organization. A transition in security strategies is occurring as the traditional castle and moat strategy no longer keeps up against ransomware attacks. The concept of Zero Trust could be a solution for organizations to bring their enterprise security to the next level by verifying each transaction that is made.

The research method will be presented in the next chapter to conduct the qualitative study.

Summary Chapter 2

This chapter gives the reader an overview of the concepts to place this study in a better perspective. Enterprise Architecture is the process by which organizations standardise and organise the IT infrastructure to align with their business goals. Different EA security strategies exist to protect the organization. Zero Trust is a new approach to harden the cyber security of an organization by applying a new concept. There is a large variety of enterprise adversaries that should be taken care of to protect your business.

Chapter 3. Research Method

This chapter aims to explain the methods used in this research and how the data is collected and analysed to draw conclusions to answer the research questions. Figure 7 shows an overview of the methods and tools used.

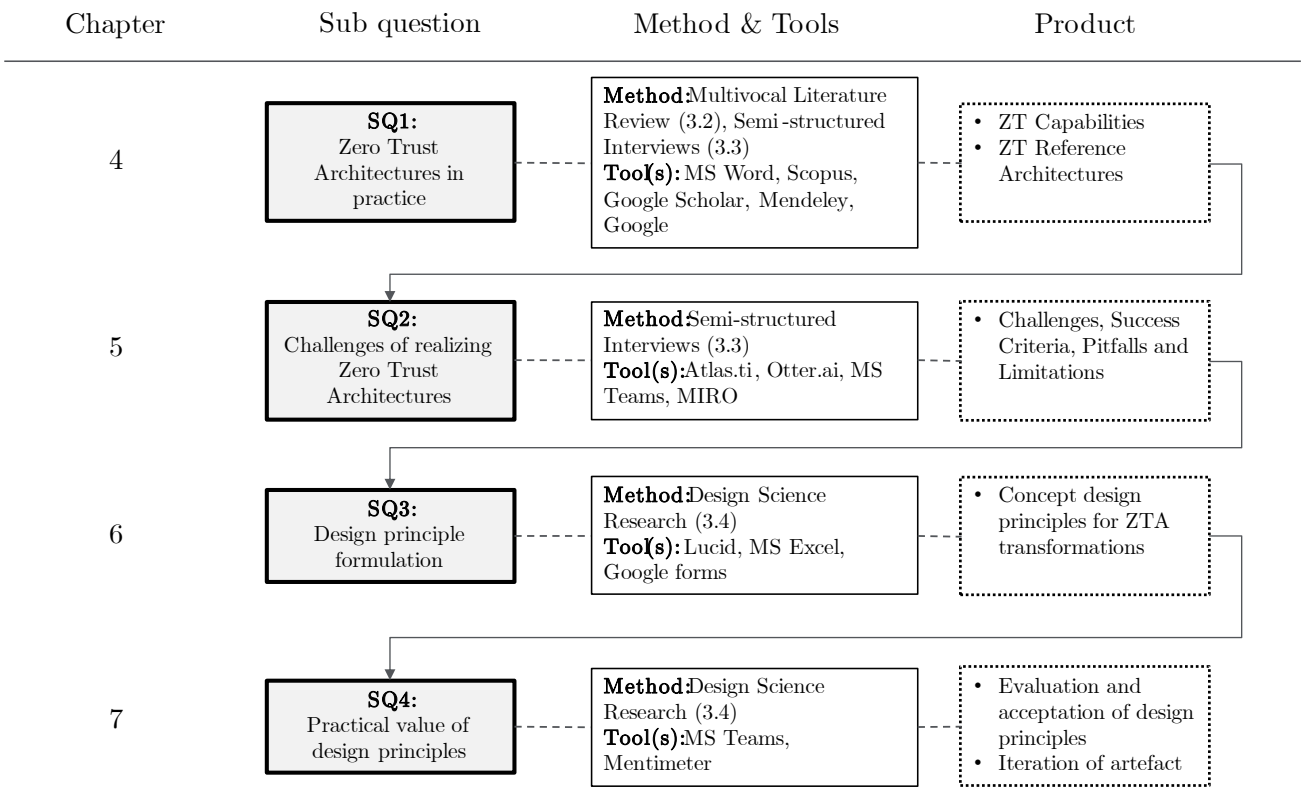


Figure 7: Overview of methods, tools and product

3.1 Method – Qualitative Study

This thesis answers the main research question by using a qualitative approach. This type of study was chosen because of several reasons:

A. Firstly, Zero Trust is still a novel topic. Therefore, it should be investigated with relatively open-ended, exploratory questions to gain as much data as possible. For collecting such open-ended, emerging data and further exploring this scientific field, a qualitative research method is particularly suitable, according to Campbell (2014).
B. Moreover, a qualitative study is suitable because it focuses on defining concepts, categorising typologies, and exploring and mapping new phenomena (Ritchie & Spencer, 2002).
C. In addition, the answers to the research question might be practices that have not been identified before and thus cannot be known a priori. Identifying such unknown practices is possible using qualitative research and in-depth data collection (Borrego, 2009; Patton, 2005).
D. Qualitative research is used to explore the potential antecedents and factors about which little has been known and explored (Strauss, 1994)

3.2 Multivocal Literature Review

The first sub-question, namely "*What makes a Zero Trust architecture?",* is answered by performing a so-called Multivocal Literature Review (MLR), which is a combination of both a grey, non-scientific literature review and a systematic, protocol-based literature review (Garousi, 2019). An MLR is chosen because it forms an appropriate way to summarise all existing information about a phenomenon thoroughly and unbiasedly. Moreover, it is the most suitable type of literature review because this study is performed in a novel research field (Adams, 2017). The reason why grey literature is included in the study is that the scientific literature may not include the most state-of-the-art knowledge. Additionally, this method makes it possible to reveal blind spots on either side of the spectrum (Garousi, 2019).

3.2.1 Systematic Literature Review

An SLR is defined by Kitchenham (2007) as *a study that uses a well-defined methodology to identify, analyse and interpret all available evidence related to a specific research question in an unbiased and repeatable way.* In other words, an SLR has the advantage of consistent findings.

The literature review will be divided into three stages: Planning, conducting the review, and reporting the findings. These three stages consist of eight steps in total. In figure 8, an overview is presented, and a description of each step is provided in Appendix C.

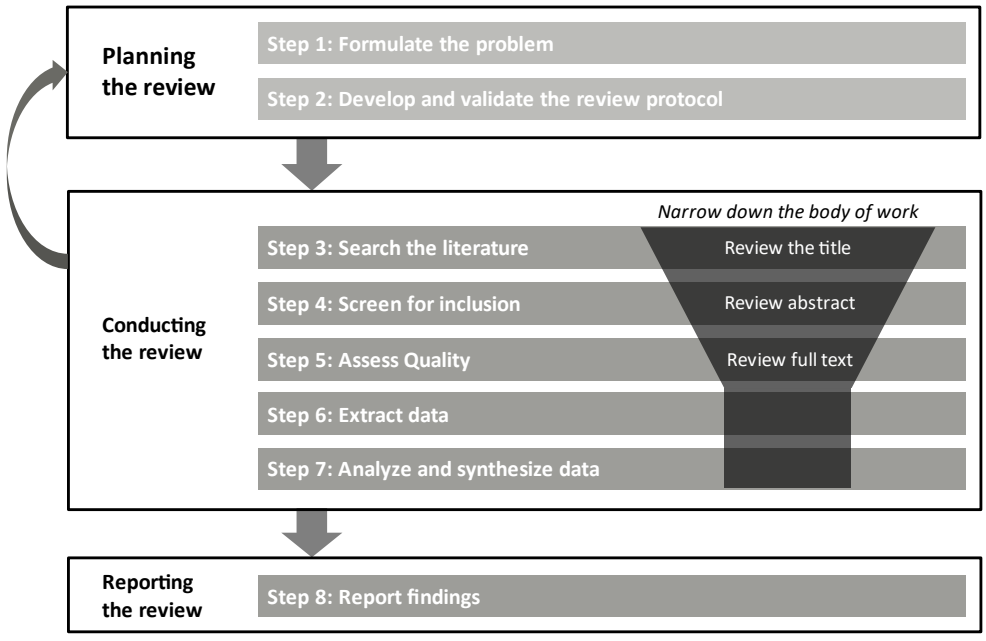


Figure 8: Design of Systematic Literature Review, adapted from (Kitchenham, 2007)

3.2.2 Grey Literature Review

To ensure the quality of the selection of grey literature and enable evaluation and critical appraisal, the AACODS checklist is used (Tyndall, 2010; Garousi, 2019). This checklist covers the factors, Authority, Accuracy, Coverage, Objectivity, Date, and Significance. According to Kitchenham (2007), these criteria should be interpreted liberally.

3.3 Semi-structured Interviews

The interviews aim to gather a broad view of perceptions on 1) the concept of Zero Trust and 2) the challenges that can arise while realising a Zero Trust architecture. In the upcoming paragraphs, an explanation of how the interviews and the analyses will be performed is given.

Semi-structured interviews will be used to gather empirical evidence. The goal is to yield as much information as possible while simultaneously addressing the research's goals and objectives. The questions for this qualitative study will be open-ended, unbiased, sensitive, and intelligible. The interview will start with easy-to-answer questions, and more complex or sensitive issues will be addressed further in the conversation. (Gill, 2008)

3.3.1 Planning

Interviewee requirements

- Five years of working experience in IT
- Active in cyber security/enterprise architecture
- Expertise/experience with Zero Trust transformation or implementation

Defining the protocol

For the semi-structured interviews, a protocol is created, see Appendix D, to strengthen the research's reliability and thereby improve the quality of the obtained data (Castillo-Montoya, 2016). The two vital elements are 1) how you introduce yourself to the interviewee and 2) the questions that will be asked. The first element can be seen as necessary as a safe environment will help elicit truthful answers from the interviewee. The person should feel that everything can be said without judgment (Rabionet, 2011).

Finding the interviewees

A gold/premium membership on LinkedIn is purchased to be able to send in-mails to Zero Trust enthusiasts and practitioners

Grouping the Interviewees

Interviewees can be grouped using personas, making it easier to process the findings. The people who participated in the study are clustered into four groups as they look at ZTA from different perspectives.

1. The first lens, **Advisors,** consists of the interviewees who provide organizations support in enterprise architecture, cyber security and cyber risk. Although their focus is not zero trust, they all have worked on projects in which Zero Trust was an element.

2. The second lens, **Project Leads**, covers engineers involved in realising Zero Trust capabilities in distinct industries. The empirical evidence of these interviewees was gained from the chip manufacturing, petrochemical and medical industry.

3. The third lens, **Scientists**, consists of professors working for the National Institute of Standards and Technology (NIST) and the MIT Lincoln laboratory.

4. The fourth lens, **Vendors**, consists of the IT solution providers: IBM, Microsoft, Fortinet, Kidelsky Security, Palo Alto and Zscalar.

Inviting the interviewees

Via email, a list of timeslots will be shared with the interviewees from which they can choose the most suited. After planning the interview, a pre-read is sent with the list of questions and additional material.

Conducting the interviews

All the interviews will be conducted online via Microsoft Teams or Zoom, making it easier for the researcher and the interviewee to connect. Based on the interviewees' preferences, a program will be selected. Additionally, for the mapping of the capabilities, MIRO is used. This tool will provide a means to map the Zero Trust capabilities into one of the four quadrants.

3.3.2 Overview of Interviewees

In table 2, an overview of the first round of interviews is presented. These exploring conversations aimed to understand the value of Zero Trust better. In table 3, an overview of the second round of interviews is presented, focusing on the challenges of establishing a ZTA.

Table 2: Internal interviews, Exploring, Focus on the ZT Value

ID	INTERVIEWEE ROLE	ORGANISATION	EXPERTISE	WORK EXPERIENCE
A1	Consultant	Deloitte	Cloud Security & Security Assessment	7 years
A2	Senior Specialist	Deloitte	Cyber Security	5 years
A3	Director	Deloitte	Cloud Security & Crypto Engineering	16 years
A4	Security Engineer	Deloitte	Cyber Security	5 years
A5	Capability Leader	Deloitte	Cyber Risk Management	32 years
A6	Researcher	TNO	Cyber Security	11 years
A7	Director	Deloitte	Cyber Risk Services	18 years

The first round of interviews was conducted between 01/03/22 – 07/03/22

Table 3: External interviews, Focus ZTA Challenges

ID	INTERVIEWEE ROLE	ORGANISATION	EXPERTISE	WORK EXPERIENCE
B1	Advisor	Deloitte	Enterprise Architect with a focus on financial services	36 years
B2	Vendor	Fortinet	Enterprise systems engineer focussing on OT and Zero Trust Access	18 years
B3	Scientist	NIST	Computer science	22 years
B4	Advisor	EY	Cyber advisory leader of programs including Zero Trust and Cloud Security	20 years
B5	Vendor	IBM	Business Development Executive Identity & Access Management & Zero Trust	40 years
B6	Advisor	Accenture	Cyber & strategic risk advisor with a focus on Zero Trust architecture	13 years
B7	Advisor	Deloitte	Enterprise Architect with a focus on industrials	15 years
B8	Project Lead	NXP	Enterprise security architecture of OT / semiconductor industry	10 years
B9	Advisor	Freelance	Architect focussing on non-secure by design components	30 years
B10	Vendor	Fortinet	Systems engineers with a focus on Zero Trust	13 years

B11	Vendor	Microsoft	Chief security advisor with a focus on ransomware and data protection	22 years
B12	Vendor	Microsoft	Security, Compliance and Identity director, assisting customers on their Zero Trust journey	25 years
B13	Vendor	Kidelsky security	Design and implementation of Zero Trust solutions to secure digital infrastructure, OT and secure identities	11 years
B14	Scientist	Colorado TU	Information scientist with a focus on Zero Trust, cyber warfare and cyber security	12 years
B15	Project Lead	Mount Sinai South Nassau	Governance and technological aspects of information security within healthcare	22 years
B16	Project Lead	Shell	Zero Trust and security in Industrial OT environments	32 years
B17	Scientist	MIT	Cyber security and information sciences	26 years
B18	Vendor	Palo Alto	Zero Trust and SASE cybersecurity solutions	18 years

The second round of interviews was conducted between 28/03/22 – 28/04/22

3.3.3 Interviews analysis in Atlas.ti

Atlas.ti

Inductive analyses are performed to obtain information from the interview transcripts (Ritchie, 2002). Likewise, to process the interviews, all the transcripts are coded with the use of 'Atlas.ti', a qualitative data analysis tool. This program makes it possible to mark parts of the conversations, enabling the researcher to make analyses based on a stack of transcriptions.

Code Distillation

Before starting the coding process, eight codes are extracted from the literature. The first three codes, 'People', 'Process' and 'Technology', are distilled from the PPT framework derived from Leavitt's Diamond Model (Leavitt, 1960). These codes are selected as these are necessary components for organizational transformation. However, these three concepts do not cover all the key concepts for a ZTA transformation. Therefore, the set of codes is extended with 'Rules & Regulations' and 'Resources', which should be considered in socio-technical environments (Kane, 2015). With these five codes, the analyses cannot yet be started as the transcripts should also be checked for specials. These are comments made by the interviewees on either a specific 'Industry', 'ZTA features' and 'ZTA tactics'. The coding process will start with these codes, but more specific subcodes will be created during the coding process. The following section describes how the coding process is executed.

Interview Coding

The interview coding is subdivided into three stages: open coding, merge categories and selective coding.

In the first stage of analysis, 'open coding' is applied. Any line of data that could be important or relevant was deductively coded with eight codes. Additionally, inductively 37 subcodes were created to make the coding more granular.

Similar subcodes are grouped and merged in the second stage into higher-order categories. This way, the number of subcodes could be reduced from 37 to 24, as shown in table 33, Appendix E.

In the third stage, 'selective coding' is applied. The data and codes are examined for themes, concepts, and relations (Silver, 2014). This additional coding round was performed to identify the 'Challenges', 'Success criteria', 'Pitfalls' and 'Limitations' (CSPL) that should be considered when realizing a ZTA.

3.3.4 Assess output

The output of the coding phase will be assessed with three different factors: 'code prevalence', 'code saturation' 'meaning saturation'. This assessment is performed to show how reliable and valuable the insights of the interviews are.

1. **Code Prevalence**

First, the prevalence of the codes will be assessed, meaning the number of instances a code appears in the interviews to verify which codes have a high and low prevalence.

2. **Code Saturation**

The interview transcripts will be assessed on code saturation to identify if the additional data collection will be redundant or adds value to the study. Code saturation is achieved when no additional codes are needed for the interview coding after some time.

3. **Meaning saturation**

Meaning saturation will occur when the number of interviews increases, but the number of the dimensions of the codes does not increase. This check is performed to validate if the number of interviews performed is sufficient and to determine the value of executing additional interviews.

3.4 Principle-based design

Design principles will be developed in the ISR framework's design cycle (Hevner, 2004). The goal of the design cycle is to develop a knowledge artefact, a set of design principles *"normative, reusable and directive guidelines, formulated towards taking action by the information system architects"* (Bharosa & Janssen, 2015) that can be used by architects in their transformation to a Zero Trust architecture.

The requirements for the knowledge artefact are as follows.

- The list of design principles should be concise and therefore limited to 10-15 principles
- The design principles should give direction, should focus on the essence and represent a key choice
- Each principle should have a name, statement, associated rationale, and implications (OpenGroup, 2006)

The artefact development should result in a list of design principles that should be followed when transforming a traditional architecture into a Zero Trust architecture. This list can be interpreted as design rules for architects with room for adjustments without hard constraints or requirements.

According to OpenGroup (2006), five criteria define a good set of principles, which are understandable, robust, complete, consistent and stable. According to Greefhorst (2011), the quality criteria for individual principles are slightly different. He states that the principles should be specific, measurable, achievable, and relevant. Additionally, the complete set of design principles must be representative, accessible and consistent.

3.4.1 Approach

In the design cycle of Hevner (2004), the principle-based design method of Bharosa (2015) will be applied. In figure 9, an illustration of the approach is presented. The boxes illustrate the different activities that need to be performed, and the arrows are the findings of each phase.

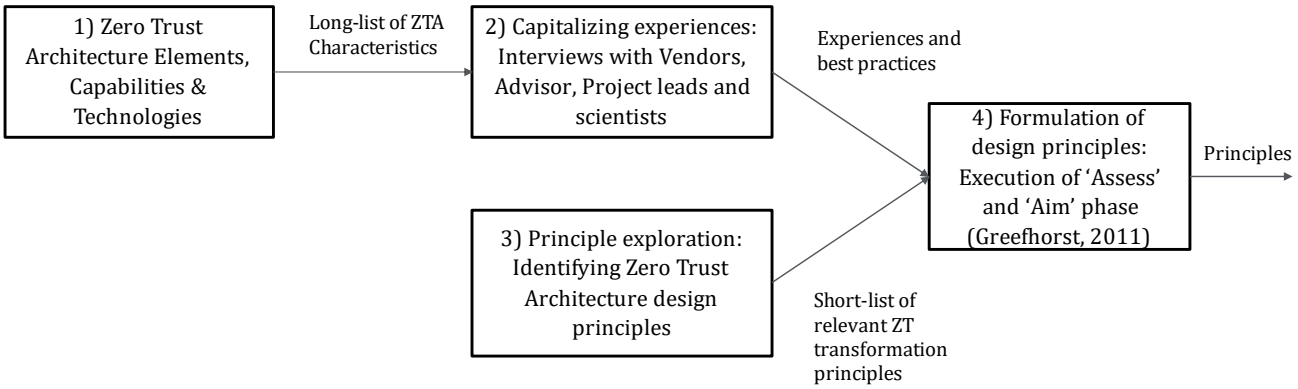


Figure 9: Overview of Research Method for Extracting Principles inspired by Bharosa (2015)

The first activity is accomplished by executing the Multivocal Literature review, discussed in chapter 3.2. The second activity is covered by conducting semi-structured interviews, discussed in chapter 3.3. The third activity is also covered by the Multivocal Literature review, discussed in chapter 3.2. The fourth activity is executed via the process cycle of Greefhorst (2011) and discussed in subsection 3.4.1.

3.4.2 Process cycle of Greefhorst

In figure 10, the suggested process is presented for formulating design principles. Only the first phase, 'Assess', and the second phase, 'Aim', will be executed in this research, so the third phase, 'Act', will remain out of the scope of this research. This third phase is not executed because the principles will not be applied in practice due to limited available use cases.

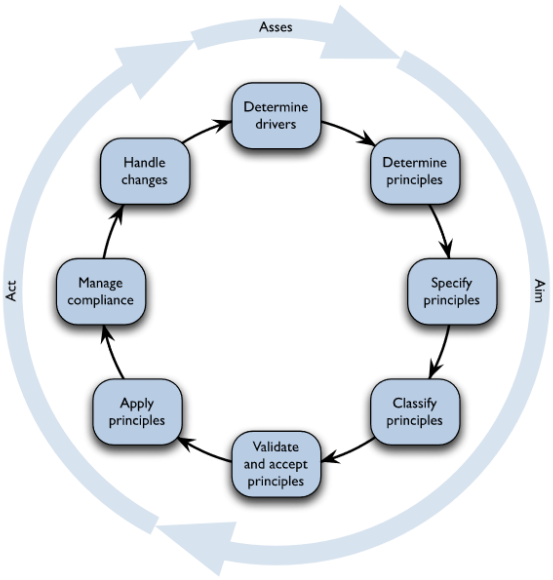


Figure 10: Process for formulating design principles (Greefhorst, 2011)

Phase 1: The first phase, 'Assess', consists of one action, which is to determine the drivers. During this step, the relevant inputs for determining architecture principles are collected, such as the objectives & goals, risks & issues. Additionally, the interviewees' experiences will be capitalized and used as input for the credos.

Phase 2: The second phase, 'Aim', consists of four steps.

1. **Determination**: the principle drivers are translated to a list of candidate architecture principles. At this stage, the architecture principles can be considered credos.

2. **Specification**: the candidate principles are specified in detail, including their rationale and implications. This subprocess translates architecture principles from credos to norms.
3. **Classification:** the principles are classified in several dimensions to increase their accessibility.
4. **Validate & Accept:** the final step of this phase is to validate and accept the architecture principles with relevant stakeholders. Two workshops will be organised to test the practical value of the principles. The first session is organised for the 'Chief Architect Community'. The lead architects of this community will be asked to assess the practical value of the set of principles and come up with suggestions. The second session is organised for the 'Digital Architects NetWork' in which the iterated version of the list of principles is evaluated. This activity will help to test whether the suggested changes are implemented correctly.

3.5 Assessing Reliability and Validity

3.5.1 Reliability

Reliability means that another researcher can repeat the research, and the outcome should give similar results. Therefore, all research activities should be well documented and based on scientific frameworks or other scientific publications. Not only the outcome should be described extensively, but also the methodology used. Therefore, protocols are constructed such that the research activities are performed the same way each time. In the appendix D, the protocols of the literature review, interviews and artefact testing can be found.

3.5.2 Validity

The value of this research will be discussed based on its validity. According to Creswell (2007), validity is the extent to which the data and interpretation are credible. In addition, eight different strategies can be used to ensure the validity of the research. For this study, the following strategies are used:

- **Prolonged engagement**: ensures that the researcher does not draw conclusions based upon an isolated, idiosyncratic experience with a phenomenon.
- **Rich, thick description:** ensures a sufficient level of detail about the phenomenon studied is included such that others might draw the same or similar conclusions.
- **Triangulation:** using multiple data sources to build a complete picture of a phenomenon. In this study, multiple sources are used, including formal and grey literature, interviews, workshops and a survey.
- **Member checking**: allows the researcher to present the findings and conclusions to the participants so they can comment on whether they believe their perspectives are accurately portrayed.

Besides these strategies, the research creates internal validity by involving multiple architects, different workshops, various vendors, and consultants. Moreover, the external validity of this study would be higher if the research had been applied to several use cases. This activity is not performed because there are no use cases available in practice that could be studied. Although the external validity can be improved in future studies, the qualitative study can still be considered valid as all the interviews followed the same protocol uniformly.

Summary Chapter 3

The methodology used for the investigation is a qualitive study which is divided into three different stages. During the first stage a systematic literature review will be performed to identify what Zero Trust architectures can be derived from formal and grey literature. The second stage focusses on semi-structured interviews to discover the challenges during the realization of a ZTA. Lastly, in the third stage a knowledge artefact will be created and tested with use of the principle formulation cycle.

Chapter 4. Zero Trust Architecture

The first goal of this research is to investigate how scholars and non-scientific writers characterise ZTAs. Therefore, in this chapter, the ZTA's, derived from formal and grey literature, are delineated. Therefore, this chapter aims to answer the following sub-question:

"What defines a Zero Trust architecture?"

As illustrated in the methodology, a Multivocal Literature Review (MLR) is chosen to get a complete picture of this still a vague and novel topic (Webster, 2002). According to Whyte (1990), combining both formal and grey literature is highly recommended for fields characterized by an abundance of various documents and a scarcity of systematic investigations. An MLR helps to give a more detailed and balanced picture of the situation. Moreover, it will create an innovative way to understand the phenomenon as there is still much ambiguity regarding Zero Trust architectures (Kitchenham, 2007).

This literature research investigates the Zero Trust architectures that can be applied to public and private organizations. Using this scope together with the keywords of already discovered articles and their corresponding keywords, the following search string was used: Zero AND Trust AND {"Enterprise" OR "Organization"} Architecture AND {"Type" OR "Design" OR "Blueprint"}

Scopus, Science Direct and Google Scholar were queried using these keywords, which resulted in 216 articles. After the identification, the duplicates (n=53) were removed. The remaining records (n=163) were screened for relevance based on the title, abstract and keywords. This process again excluded a set of records (n=111) as the title, abstract, or keywords were not concerning ZTA. The full text of the records (n=52) is assessed on eligibility. Again records (n=46) were excluded as the full text was not discussing capabilities, technologies, or architypes. The included articles focus explicitly on ZTA types or designs, which eventually resulted in the selection of 6 papers. As this is only a limited number of papers, the literature review will be extended with grey literature (n=18). In figure 11, an overview is presented and extensive description of the approaches taken for this systematic literature review is reported in Appendix C.

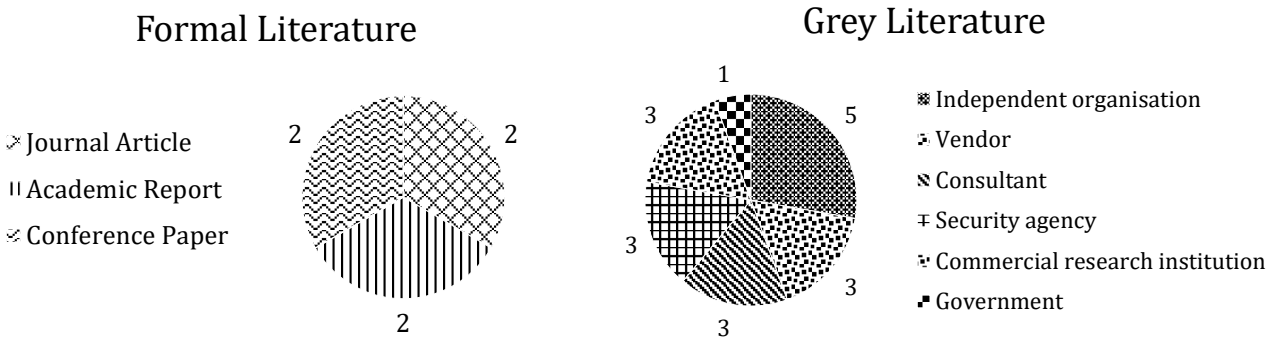


Figure 11: Distribution of publications

The following strategy is used to answer the first sub-question. First, an overview of the ZTA models and strategies available in the literature is given in section 4.1. Second, an overview of the Zero Trust foundational elements that can be derived from the literature is presented in section 4.2. Third, a systematic overview of the capabilities and technologies is created in section 4.3. Finally, the different ZTA's characteristics are described, and a design is created in section 4.4.

4.1 Literature on Zero Trust Architecture Models & Strategies

First, the core components of a ZTA (Rose, 2020) to which scholars frequently refer are described in subsection 4.1.1. Second, different perspectives on the ZTA basis are reported. Also, the used models are presented and discussed in subsection 4.1.2. whereafter, the strategies are presented in subsection 4.1.3.

4.1.1 Core components

Most ZTAs can be split into two sections the control plane and the data plane (Gilman, 2017). The control plane, formed by the Policy engine and the Policy administrator, supports the system with the controls and configurations. The access requests will first go through this layer to authenticate and authorize both the device and the user. The applied policies can be as fine-grained as possible. Likewise, the policy engine can use as many attributes as needed. Once access is allowed by the control plane, the policy enforcement point, which is part of the data plane, will dynamically configure the data plane to allow access to the specific element of the network. This configuration step can be done by creating a temporary encrypted tunnel between the endpoints using keys or one-time-use credentials.

4.1.2 ZTA models in literature

According to Rose (2020), three different approaches and three models can be used in achieving a ZTA, whereas Uttecht (2020) has identified three theoretical architypes and four commercial deployed types. However, Campell (2020) defines six approaches to achieving a ZTA. But, the CSA (2020) only presents two high-level generic presentations of ZTA's. Nevertheless, the CISA (2021) is not providing any architypes. Only some elements that should be focused on when applying the incremental approach are debated.
As there is no consensus among the authors, an overview of the possible methods must be created. In the following paragraphs, three abstract models are presented of a ZTA, which all consist of a decoupled control- and data plane as described in section 4.1.1. In addition, the seven architectures found are linked to the models.

Model comparison
Before the three models are explained in-depth, an overview of their characteristics is given in table 4.

Table 4: Comparison of Architecture Models

		Model		
		Resource portal based	*Enclave based*	*Device Agent/Gateway-based*
Characteristic	*Agent needed on the endpoint*	No	Yes	Yes
	Number of gateways	Single not integrated	Multiple not integrated	Multiple and integrated
	The complexity of the architecture	Low	Medium	High
	The granularity of the access rights	Low	Medium	High

1. Resource portal-based model

The resource portal-based model**,** presented in figure 12, is the least fine-grained as the policy enforcement is not integrated into the endpoint or the application. Though, the control plane and data plane are decoupled (Uttecht, 2020). Moreover, this technical model was one of the first ZTAs created and uses isolation, VLANS, Subnets, Risk driven trust zones and an Access Control List (ACL).

The literature revealed two architectures in which the resource portal-based model was used as a foundation:

- **Next Generation Firewall** (Uttecht, 2020; Kindervag, 2010) - With the use of physical network segmentation, a ZTA can be derived. This method is the simplest and the lowest cost solution. Therefore, also not the strongest in terms of security.
- **Software Defined Network** (Uttecht, 2020) – With the use of both hardware and software, network segmentation is created.

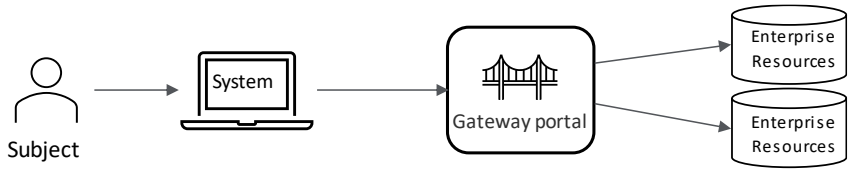


Figure 12: Simplistic representation of the data plane of the resource portal-based model

2. Enclave-based model

The enclave-based model, presented in figure 13, is an approach characterized by a gateway that does not reside in front of the individual resources. Moreover, it makes use of cloud-based micro-services. This form of micro-segmentation is used to place groups of resources on a unique network segment to enhance protection (Rose, 2020). This technique will enable segmentation on workload level and granular isolation to individual hosts and containers.

The literature revealed three ways how the enclave-based model is used:

- **Software Defined Perimeter** (Uttecht, 2020; Campbell, 2020; Rose, 2020) – This method does not require integration with the application or resource, though it does require installation and configuration on both the resource server and the user's device. The architype makes use of enhanced user identity and micro-segmentation.
- **Zero Trust Network Access** (Fortinet, 2021; Appgate, 2022) – Frequently referred to as ZTNA or a client-initiated architecture (Gartner, 2019).
- **Service Mesh** (Gartner, 2019; Seepers, 2020; D'Silva, 2021) – This method is the most profound embedded scenario in the service architecture. It uses the container layout, placing applications in separate containers and micro-service technology. Docker containers and Kubernetes can play a significant role in creating these delicate mazed implied trust zones.

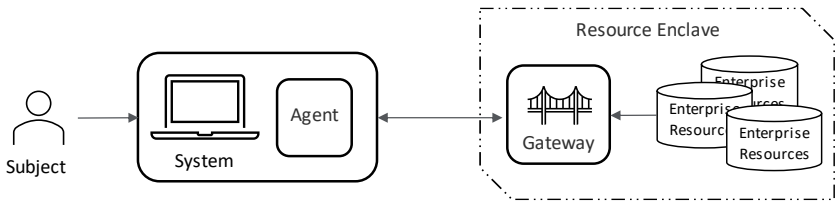


Figure 13: Simplistic representation of the data plane of the enclave-based model

3. Device agent/gateway-based model

The device agent/gateway-based model, presented in figure 14, is the most fine-grained approach compared to the other two models described above. This difference in model is because the gateway is tightly integrated within the resource or application (Uttecht, 2020).

The literature revealed three ways how the Device Agent/Gateway-based model can be used:

- **Proxy-based** (Campbell, 2020) – Google commercially deploys this method in their "Beyond Corp" solution. The proxy acts as the enforcement point to a hosted application delivered on the Google platform. The advantage of the *Beyond Corp* solution is that it is not needed to install any software on an endpoint. Nevertheless, Google cloud should be used, making users dependent on a vendor and creating lock-in. Likewise, this proxy-based method can be defined as a service-initiated architecture (Gartner, 2019)
- **Virtualized Systems** (Uttecht, 2020) – This method is commercially deployed by VMWare in their NSX solution and is specially designed for enterprises utilizing a virtual desktop infrastructure (VDI) and predominantly virtualized systems.
- **Sandboxing** (Rose, 2020) – Processes or applications run on compartmentalized assets, such as virtual machines or containers.

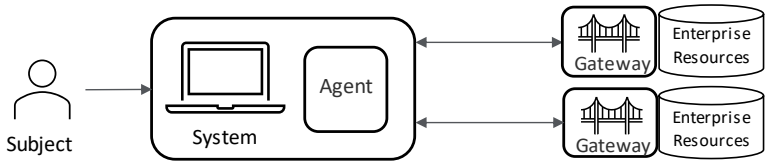


Figure 14: Simplistic representation of the data plane of the device agent/gateway-based model

4.1.3 ZTA strategies in literature

In addition to the three abstract ZTA models, five strategies described in the literature can support the transformation to a ZTA.

A. User focus / Enhanced identity Driven

When using the enhanced identity governance strategy, the actors' identity is the critical component for creating policies (Rose, 2020). Although users can only access enterprise resources with appropriate access privilege, this approach is not fool proof. The downside is that malicious actors can still attempt network reconnaissance and use the network to launch denial of service attacks (Rose, 2020). The CARTA framework (Gartner, 2018) could be used to mitigate this problem. This framework refines the Zero Trust framework by extending identity verification to include device certification, compliance, and context-driven authentication & authorization (Campbell, 2020).

B. Segmentation driven

The segmentation strategy can be executed in multiple ways. The simple approach would be the resource portal-based approach, establishing the network segmentation. However, this solution comes with less advanced gateway devices or firewalls and will, in the long term, create higher administration costs as they cannot adapt to changes quickly (Rose, 2020). A more advanced approach would be micro-segmentation, placing individuals or groups of resources on a unique network segment protected by a gateway security component (Rose, 2020).

C. Trust Algorithm Driven

The trust algorithm-driven strategy can use an undefined number of factors as input. However, a distinction must be made between a 'singular' and 'contextual' algorithm. The precise algorithm does not consider the subject or network agent's recent history for evaluating the access request, whereas the contextual algorithm does so (Rose, 2020). Moreover, the algorithm can be 'criteria' based, implying that a set of attributes must be met before access is granted or 'score' based, meaning a confidence level or threshold value needs to be met before access is granted (Rose, 2020). According to Mitre (2021), the algorithm should take into consideration six factors: 1) User identity

attributes, 2) Access request environment, 3) Device posture, 4) Threat Intelligence, 5) User & Device Behaviour, 6) Data sensitivity assessment

D. Automation driven

With the automation-driven strategy, three elements can contribute to an automated ZTA. The first element is the Security Orchestration, Automation and Response (SOAR) system which supports the transition to an automated approach of security operations (Campbell, 2020). This automatic threat and vulnerability response system is marked as a method for auto-remediation. The second thing would be risk-adaptive decision-making, which contributes considerably to automation as decisions are made based on a trade-off between current risks, acceptable risks and the need for the requested action (Hut, 2019). Lastly, the architecture should integrate automated policy enforcement, threat intelligence and protection across all pillars (Microsoft, 2021).

E. Artificial Intelligence (AI) driven

The AI-driven strategy supports the demand for computational sophistication needed to determine the dynamic access risk as a rule-based system cannot simply provide it. Therefore, the future of Zero Trust rests in AI (Campbell, 2020). Likewise, contemporary AI algorithms can be developed to protect data in untrusted networks (Ramezanpour, 2021).

4.2 Literature on ZTA Foundation

The foundational elements that form the architecture are examined as only a little information is available on the different architypes. The taxonomy of DISA & NSA (2021) consists of five pillars: user, device, network, application, and data. Additionally, GSA (2020) defined two cross-components: visibility & analytics and automation & orchestration and they were included in the five pillars of DISA & NSA (2021). On the other hand, Microsoft (2021) uses nine security pillars. In their paper, infrastructure, policy optimization, policy enforcement and threat protection are added but do not use a visual representation. Next, the ZTX framework of Cunningham (2018) focuses on seven pillars: data, networks, people, workloads, devices, visibility & analytics, and automation & orchestration. According to Cunningham (2018), a model can be named ZTX when it focuses on at least three framework pillars.

Although there are different approaches to Zero Trust, distillation has been made from the nine architectural core components that are assumed to be the most important for a ZTA. In figure 15, visualisation is shown of these components. Inspiration for this model was deducted from (CISA, 2020) (Microsoft, 2021), (Cunningham, 2018) (GSA, 2020). The developed model, the Zero Trust Architecture Foundation, gives a decent overview of the EA elements that must be addressed when applying a Zero Trust strategy.

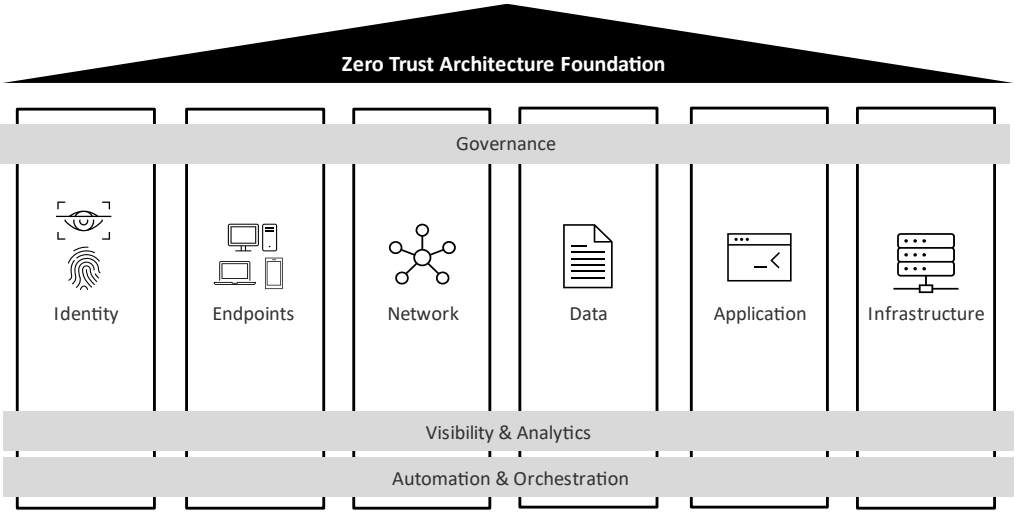


Figure 15: ZTA Foundation

Besides this foundation, there are four frameworks; SP 800 207, CARTA, ZTX ecosystem and Beyond Corp that can be used for a transformation to a ZTA. Although these frameworks are not designs, they can guide architects on how architectures must be designed (Campbell, 2020). An overview of the four identified frameworks is presented in table 5. From these frameworks, it can be concluded that a ZTA should at least have the following three capabilities: strong verification, least privilege, and continuous monitoring.

Table 5: ZTA Frameworks

Developer	Framework	Description
NIST	SP 800 207	A high-level overview of Enterprise Architecture. Separated in a control plane and data plane to which eight different measures are applied
Gartner	CARTA	A model continues circle consisting of four different phases: attack prevention, incident detection, incident response, and threat anticipation
Forrester	ZTX Ecosystem	Abstract model focussing on data and how it interacts with workloads, people, networks, and devices
Google	Beyond Corp	A model discarding traditional VPNs and using policy-based information about a device, its state and related user

4.3 Literature on ZTA Configurations

The methods and technologies used to establish a ZTA are mapped on the "ZTA Foundation" and briefly discussed here. Moreover, a structured overview of the literature mapping can be found in table 27-30, Appendix C.

Configurations for the Governance

Governance oversees the policy creation and abidance to ensure 'least privilege' access. Likewise, it can revoke access in case of deviant or suspicious behaviour. Therefore, governance applies to all the pillars. The literature review results in three alternatives for the organisation of governance. In table 6, an overview is presented.

Table 6: Alternatives for the configuration of governance

Alternatives	Description	Prevalence in literature
Attribute-based access control	Based on the predefined attributes, authorisation will be provided to the requested data or application (Rose, 2020)	15/24
Role-based access control	Based on the user's role, authorisation will be provided to the requested data or application (Uttecht, 2020)	4/24
Policy-based access control	Based on the constructed policy, authorisation will be provided to the requested data or application (Yao, 2020)	18/24

Configurations for the Visibility & Analytics

This component focuses on continuously monitoring the enterprises' activities to detect attacks, malicious traffic, threats, and vulnerabilities and prevent fraud. The literature review revealed five alternatives to set up visibility & analytics. In table 7, an overview is presented.

Table 7: Alternatives for the configuration of visibility & analytics

Alternatives	Description	Prevalence in literature
Threat Intelligence Feed	Threat intelligence gives the policy engine information from internal or external sources to assist it in making access choices.	15/24
Activity Logging	Asset logs of network traffic, resource access activities, and other events are gathered and analysed to offer real-time (or near-real-time) feedback on the security posture of business information systems.	10/24
Security Information & Event Management (SIEM) system	A system that gathers security-related data to fine-tune regulations and warn of potential assaults on corporate assets.	12/24
Entity and user behaviour analytics (EUBA)	Data on users' and entities' normal behaviour is acquired from system logs. Subsequently, data is analysed using complex analytical tools, and a baseline of user activity patterns is established.	3/24
Network analysis and visibility (NAV)	A tool that will identify unmanaged assets by capturing and analysing all traffic traversing the network. (Kindervag, 2010)	4/24

Configurations for the Automation & Orchestration

The Automation & Orchestration mechanisms focus on enterprise adversaries' automated detection and response. The literature results in five alternatives for automation & orchestration. In table 8, an overview is presented.

Table 8: Alternatives for the configuration of automation & orchestration

Alternatives	Description	Prevalence in literature
Risk Assessment	A Method of identifying prospective dangers and determining what could happen if the hazard occurs	11/24
Continuous Diagnostics and Mitigation system (CDM)	A risk-based program aimed at reducing agency threat surfaces, improving the visibility of the security posture, and refining the incident response capabilities	7/24
Single Sign-On (SSO) system	An authentication mechanism that lets a user log in to numerous connected but separate software applications with a single ID	15/24
Security Orchestration, Automation and Response (SOAR) platform	A platform which develops automated incident response actions in response to cybersecurity threats	8/24
Auto-remediation	A tool that is triggered by alerts or events and reacts by executing activities that can avoid or solve the problem	5/24

Configurations for the Identity

One of the critical aspects of Zero Trust is the continuous authentication of trusted users to monitor and validate their trustworthiness continuously and govern their access and privileges. The literature review results in three alternatives to verify identity. In table 9, an overview is presented.

Table 9: Alternatives for the configuration of identity

Attribute	Description	Prevalence in literature
Continuous Multi-Factor Authentication (CMFA)	Authentication is characterized by something one must know and have. Additionally, it confirms the user based on the behavioural metrics	4/24
Biometrics	Measuring and statistically analysing people's distinct physical and behavioural features	6/24
Dynamic authorisation	Using attribute-based rules and policies to authorize and grant access rights dynamically in real-time to an organization's network, applications, data, or other sensitive assets (D'Silva, 2021)	13/24

Configurations for the Endpoints (devices)

Besides knowing that a user can be trusted, the device's trustworthiness is vital. The endpoints should comply with the organizational policies, which means the device is not compromised, up to date (patched), and protected before a connection is established. The literature review revealed two alternatives to connect safely with endpoints. In table 10, an overview is presented.

Table 10: Alternatives for the configuration of endpoints

Alternatives	Description	Prevalence in literature
Compliance Monitoring	A solution that continuously checks the security and compliance posture of the endpoints	13/24
Single Packet Authorisation	A security scheme which makes use of port knocking to set up a secure connection	5/24

Configurations for the network

The network is critical for a ZT architecture as the perimeter of the networks is shifting or even disappearing. In the earlier days, the network could be protected with one thick firewall; however, this was no longer sufficient. The focus is currently on segmentation which is a means to reduce the blast radius of attacks. The literature review revealed six alternatives to structure the network. In table 11, an overview is presented.

Table 11: Alternatives for the configuration of the network

Alternatives	Description	Prevalence in literature
Network segmentation	Segmentation of the network in smaller compartments or trust zones	21/24
Secure Web Gateway	A security service which is placed between the users and the internet	8/24
Secure Access Service Edge	A network architecture which enables users to connect to applications via the use of cloud solutions directly	4/24
Mutual TLS	Authentication between two parties who are both using the TLS protocol	5/24
Software Defined Perimeter	Base the network perimeter on software instead of hardware which makes it more accessible to hide the infrastructure	15/24

Configurations for data

The data pillar focuses on the safeguarding of data when stored or transmitted. The literature review revealed five alternatives to secure data. In table 12, an overview is presented.

Table 12: Alternatives for the configuration of data

Alternatives	**Description**	**Prevalence in literature**
Obfuscation / redaction	This method makes sensitive data useless to attackers by adding an extra layer of data protection.	4/24
Encryption at Rest & in Transit	This technology encrypts the stored data on all the endpoints and encrypts the data during transfer.	8/24
Tokenization	A process in which sensitive data is replaced by surrogate values or tokens	5/24
Classification	Data is tagged according to its type, sensitivity and importance to the organization.	9/24
Data Rights Management	A tool that enables the management of how we use, edit, and share information/content	12/24

Configurations for applications

The application component consists of the programs and services that are executed on-premises, as well as in the cloud. Moreover, the application focuses on virtualisation and containerization to create better insights and improve system utilization. The literature review revealed five alternatives to access applications. In table 13, an overview is presented.

Table 13: Alternatives for the configuration of applications

Alternatives	**Description**	**Prevalence in literature**
API connections	Set of rules that define how applications and endpoints can communicate with each other.	14/24
Micro-segmentation	Segmentation of the infrastructure on the application level	6/24
Microservices & containers	Building an architectural design for distributed applications via the use of containers	9/24
Adaptive access	Policies enable administrators to manage user access to applications, files, and network functions depending on various real-time parameters.	5/24
Just Enough Administration	Set of rules that enable just those rights to be granted that are essential to execute a specific task or duty (DISA & NSA, 2021)	6/24

Configurations for infrastructure

The infrastructure pillar consists of all the on-premises and multi-cloud hardware, software and micro-services, networking infrastructure and facilities required for IT delivery. The literature review revealed two technologies (T) to build the infrastructure. In table 14, an overview is presented.

Table 14: Alternatives for the configuration of infrastructure

Alternatives	Description	Prevalence in literature
Public Key Infrastructure	Governs the issuing of digital certificates to secure end-to-end communication, protect sensitive data, and give unique digital identities to people, devices, and applications.	6/24
Cloud Access Security Broker	A cloud-based or on-premises security policy enforcement point ensures the communication between the consumers and cloud service providers	8/24
Macro-segmentation	Segmenting the network via the use of hardware and VLANs	16/24

4.4 Derived Reference Architectures

There are many approaches and a lack of consensus in the literature on what a ZTA entails. Only abstract examples, approaches and frameworks can be found. Therefore, a taxonomy of the ZTA types (knowledge artefact) will be created. From the synthesis, the following reference architectures are derived and presented in table 15 and discussed below. Furthermore, in Appendix F, a visual representation of the various architectures can be found.

Table 15: Reference architectures

	A. Hardware driven	B. SDN driven	C. SDP driven	D. Service Mesh	E. Identity driven	F. Behaviour Driven
Characteristics	Physical Isolation	Dynamic Subnets	SDP controller	Microservices, containers, API Gateway	Trust Score generator	Artificial Intelligence
ZT Approach	Network segmentation	Network segmentation	Micro-segmentation	Application and data protection	Enhanced User and Identity governance	Automatic behaviour detection and response
Applicable for environment	Industrial / OT	Legacy	Cloud	Development	External users	B2C
Ease of Implementation (D-S)	Simple	Medium	Difficult	Difficult	Medium	Difficult
Strengths	Simplicity	Scalability / Reliability	Granularity	Modularity	Authentication	Automation
Weakness	Flexibility	Latency	Compatibility	Management	Single point of failure	Privacy

A. Hardware driven

This architecture is one of the simplest to implement as it only focuses on network segmentation. The architecture is characterised by an access control list and hardware solutions allowing users access to specific network zones. The different zones' endpoints, servers and databases are physically isolated to prevent lateral movement. This type of architecture can be applied to, e.g., industrial organizations dependent on OT equipment.

B. Software Defined Network (SDN) / Policy-Driven Architecture

This architecture is also focussing on network segmentation. However, the creation of compartments is not achieved with hardware but with software. All decisions are made by a centralised policy decision point that grants entities access based on their identity. Moreover, legacy systems can be included in the network and therefore do not have to be depreciated.

C. Software Defined Perimeter (SDP)

The SDP creates a “black cloud, " ensuring that internal and external users can discover and access services only if they have the proper credentials (Campbell, 2020). The downside of this approach is that an SDP client needs to be installed to access the data and applications Campbell (2020). This approach is frequently implemented on the application network layer, OSI 7 and can be seen as the successor of Software Defined Networks (Rose, 2020).

According to CSA (2020), the SDP is the most advanced implementation of a Zero Trust strategy as 1) the control plane and data plane are separated, 2) the complete infrastructure is hidden, 3) single packet authorization makes ‘least privilege’ implicit.

Even though it will take longer to establish the connection, an SDP-secured network is more resistant to port scanning and distributed denial of service assaults since it does not provide any information and maintains a high average network throughput (Moubayed, 2019).

This architecture combines micro-segmentation and identity-based access because micro-segmentation does not consider identity, GPS location or device posture. With software-defined perimeters, virtual environments can be created for each user. This architecture works optimally if the organization is mainly in the cloud, making it especially suitable for most tech companies. Moreover, this approach provides security and business benefits (CSA, 2020).

D. Service Mesh Driven

The service mesh-driven architecture uses an API gateway and microservices, making it possible to position applications in different containers. Moreover, the micro-segments assure that a subnet cannot talk to any other subnet. This architecture is prevalent in dynamic organizations with a lot of application development as the architecture is modular. Besides, the service mesh creates good visibility as the proxy can measure metrics such as latency, HTTP errors and user agents. Therefore, there is no need to place instruments on the application itself. Additionally, the environment enables the developers to switch easily between different services.

E. Identity Driven

Although identity is one of the fundamental aspects of any ZTA, this reference architecture expands this even further. A trust score generator is used in this architecture, which determines the authorisation of the entities trying to connect to another endpoint. The score can be based on multiple inputs, but in this architecture, the device health, metadata of the user and biometrics are used for the verification process. This architecture is typically preferred for more external-facing applications in which organizations do not have too many network-centric controls attached to the application.

F. Automatic behaviour detection and response

This architecture is the most advanced. Therefore, all the essential elements of Zero Trust, ‘identity & inventory management’ and ‘device inventory’ need to be in place to make this architecture work. This architecture reacts instantly and autonomously to suspicious behaviour by remedying the incident that caused the policy violation. Moreover, this architecture can be applied to organisations in the B2C environment, e.g., financial services, in which it is critical to respond directly to suspicious behaviour.

4.5 Literature focussing on Zero Trust Principles

The last part of the literature study was to examine the existing guidance. The research resulted in twelve different sets of principles focusing on Zero Trust. The complete list of principles can be found in Appendix G, but in table 16, an overview is presented, and the main takeaways are discussed below.

Table 16: Overview of existing principles

Source	Number of principles	Source	Number of principles	Source	Number of principles
NCSC NL	5	NSA	7	NIST	7
NCSC UK	8	Google	3	Palo Alto	4
Forrester	3	Microsoft	3	Zscalar	3
IBM	5	OpenGroup	9	Forbes	5

Frequently mentioned topics
The synthesis of the existing principles results in the following six topics which are:

1) **Identity:** Multiple contextual factors should be used to determine the users' access (Google, 2020; NSA, 2021), such as user behaviour, device health or a combination of both (Microsoft, 2020; NIST, 2020; Palo Alto, 2021; IBM, 2021). All available telemetry should be used for the data collection (OpenGroup, 2021). This information will help establish confidence in the systems (NCSC UK, 2021). Properties of the access request could be account, device, IP address and location (NCSC NL, 2021).
2) **Least privilege:** Access control should be as strict as possible. Furthermore, access should be provided on a need-to-know basis. This level of control can be assured with the principle of least privilege (NCSC NL, 2021; OpenGroup, 2021; Forrester, 2021; NSA, 2021; NIST, 2020; Palo Alto, 2021; IBM, 2021). Additionally, the access should be removed if not needed any longer (OpenGroup, 2021). The limitation of user access can be accomplished with just-in-time and just-enough-access (Microsoft, 2020)
3) **Inventory:** An overview of all the endpoints, such as devices, assets and services in the network, should be created (NCSC NL, 2021; NCSC UK, 2021; NSA, 2021; Palo Alto, 2021; IBM, 2021).
4) **Visibility:** Extensive monitoring should be implemented on the network (NCSC NL, 2021; Forrester, 2021; NSA, 2021; NIST, 2020). Monitoring will benefit from establishing device and user health (NCSC UK, 2021)
5) **Breach:** Assume the environment is hostile and a breach can happen at any given moment (NCSC UK, 2021, Forrester, 2021; NSA, 2021; Microsoft, 2020; IBM, 2021)
6) **Cryptology**: All the connections should be encrypted regardless of their location (NCSC NL, 2021; NCSC UK, 2021; Google, 2020; Palo Alto, 2021)

Main observations & takeaways
There is no standard in the number of principles that should be adopted. As a result, the number of principles and the focus area which should be followed differs per case. For example, the principles of the NCSC NL are different from those of the NCSC of the United Kingdom. A possible explanation for the differences between the principles is that “Zero Trust” is not fully elaborated and is still immature. Likewise, it is still largely unknown how to implement the philosophy substantively.

4.6 Reflection on Literature

There is no consensus on what the requirements of a ZTA are and on what the exact number of different ZTAs are. Furthermore, there is no common framework or vocabulary for ZTA, and each source uses different wording. Likewise, there are no coherent requirements and policies for designing ZTAs, and there is no standard way to view, model and discuss ZTA solutions. In addition, most vendors pretend to have the ZTA solution in place, while in reality, a common standard is missing.

The grey literature concentrates mainly on the direct benefits of ZT, which apply to organizations. However, the indirect benefits for users and society are neglected. Moreover, formal and grey literature primarily focuses on the architectural aspects of a zero-trust implementation. The end-user perspectives are underexposed.

Additionally, the outcome of the literature review was discussed with seven cyber security experts. The respondents validated the findings which were found in the literature. The core capabilities of a Zero Trust EA vary a lot due to the different approaches.

4.7 Conclusions

Although the formal literature on "Zero Trust architecture" is limited, several insights were found to answer the first sub-question: *"What defines a Zero Trust architecture?"*

There is no consensus in the literature about the requirements of a ZTA, and the examination indicates that various methods can be used to establish a ZTA. Nevertheless, the commercially deployed ZTA's can be clustered in three generic models, and all found architectures can be divided into a control and data plane.

Although the scholars and non-scientific authors have different opinions, they all agree that identity management is fundamental to any Zero Trust solution since a ZTA cannot be established without identity verification and access control.

Additionally, five strategies contribute to the establishment of a ZTA. The first two strategies, 'enhanced identity' and 'segmentation', can be applied immediately. However, for the other three strategies, 'trust algorithm', 'automation', and 'artificial intelligence', a fundament consisting of device and user management must be in place.

Besides the strategies, there are various configurations possible to achieve a ZTA. The alternatives can be clustered into six pillars: identity, endpoints, network, data, application and infrastructure. Additionally, three cross pillar themes are found: governance, visibility & analytics, automation & orchestration.

Lastly, the literature review indicates that Zero Trust is not an architype but rather a way of designing an organization's security architecture.

In the next chapter, the challenges that appear when realising a ZTA are investigated, which should support the architects in the future with establishing a ZTA.

Summary Chapter 4

With use of a multivocal literature review an overview of the ZTAs is created. Moreover, the supporting technologies to enable a capability are diverse. In literature only a limited number of ZT designs can be found but there is a wide range of technologies and methods available that can contribute to establishing a ZTA. Additionally, several reference architectures are modelled which should provide guidance for the architects.

Chapter 5. ZTA Realisation Challenges

To ensure a solid ZTA realisation, knowing what parts of the transformation need some additional devotion is valuable. As there is not much documentation available on the hurdles that should be considered when transforming to a ZTA, an examination must be performed. Therefore, one of the research intentions is to examine what the challenges are for the realization of a ZTA by gathering empirical evidence and experiences from a variety of perspectives. Likewise, it aims to answer the sub-question:

"What are the challenges for realising a Zero Trust architecture?"

First, an overview of the executed 'Atlas.ti' analysis is presented in section 5.1. Second, all the insights retrieved from the interviews are presented in section 5.2.

5.1 Atlas.ti Analysis

Atlas.ti is used to distil data from the 18 interviews conducted. All the interview transcripts are coded with 8 codes and 24 subcodes. The coding was performed in three stages: stage 1: open coding, stage 2: merging codes and stage 3: selective coding. Moreover, the coding process started with deductive coding, but inductively additional codes were generated during the coding process, and iterations were made to the codes.

5.1.1 Overview of Codes

From the MLR described in the previous chapter, codes are distilled to analyse the outcome of the interviews. These codes are applied to the transcripts of the semi-structured interviews. In table 33, Appendix E, an overview of the final list of generated codes is presented. Starting deductively with an initial list of eight codes and inductively, twenty-four subcodes were created, merged and iterated following the theory of Silver (2014).

In figure 16, a network diagram shows the relationship between the codes used in the coding process in Atlas.ti.

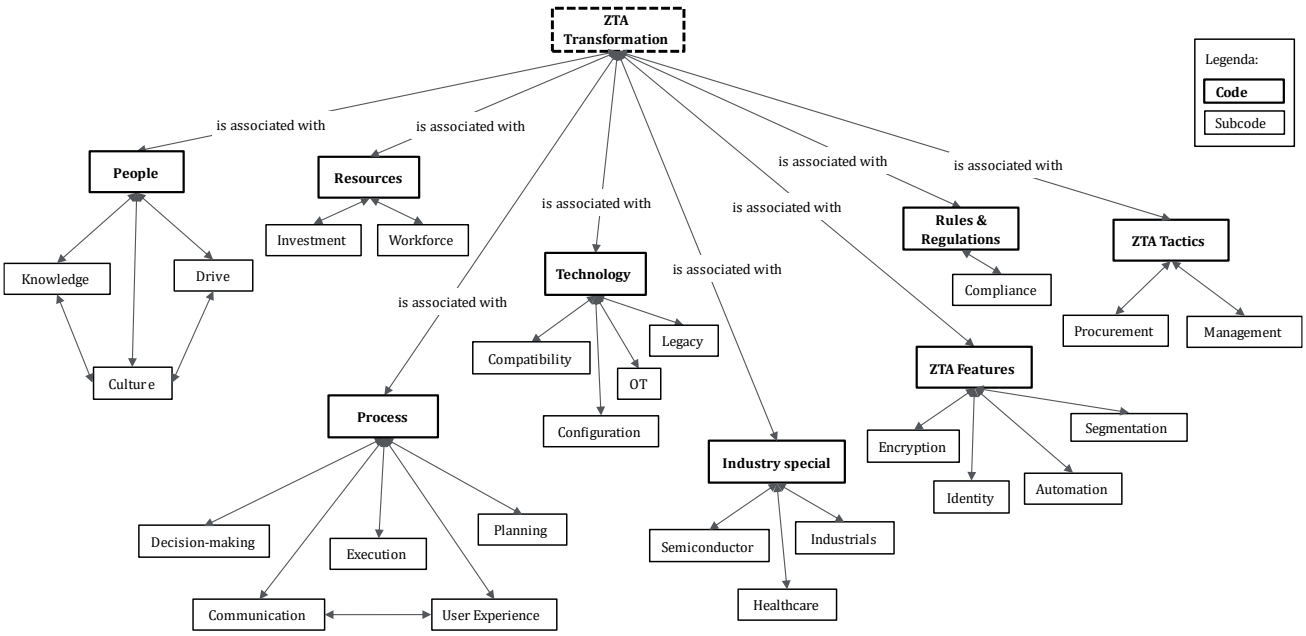


Figure 16: Network diagram of codes used in Atlas.ti:

5.1.2 Code Prevalence

Figure 17 shows which codes are the most prevalent in this study. The bars indicate the number of interviews in which the sub-codes were used. The sub-codes are clustered within their main code and ordered on their prevalence from high to low. Moreover, the first subcode of each cluster is indicated by a darker colour.

Additionally, in appendix E, figure 32, the overall code use is presented. This chart indicates that challenges regarding the realization of a ZTA deal with the execution of the transformation process.

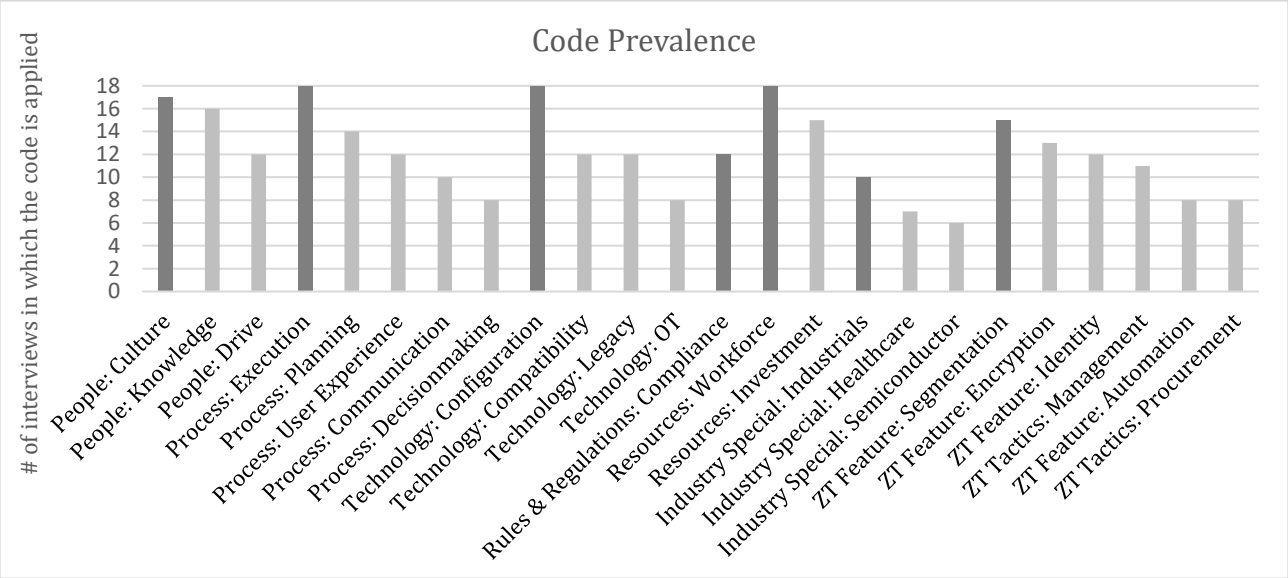


Figure 17: Code prevalence in interviews

5.1.3 Code Saturation

In figure 18, the number of codes applied to the interview transcripts is presented in chronological order. This figure shows that the average number of unique codes applied is 13.4, indicated by the red horizontal line. Additionally, there are some interviews in which the number of codes is relatively low. This undershoot indicates that the number of arguments provided is limited or that the answers provided are irrelevant and therefore cannot be coded.

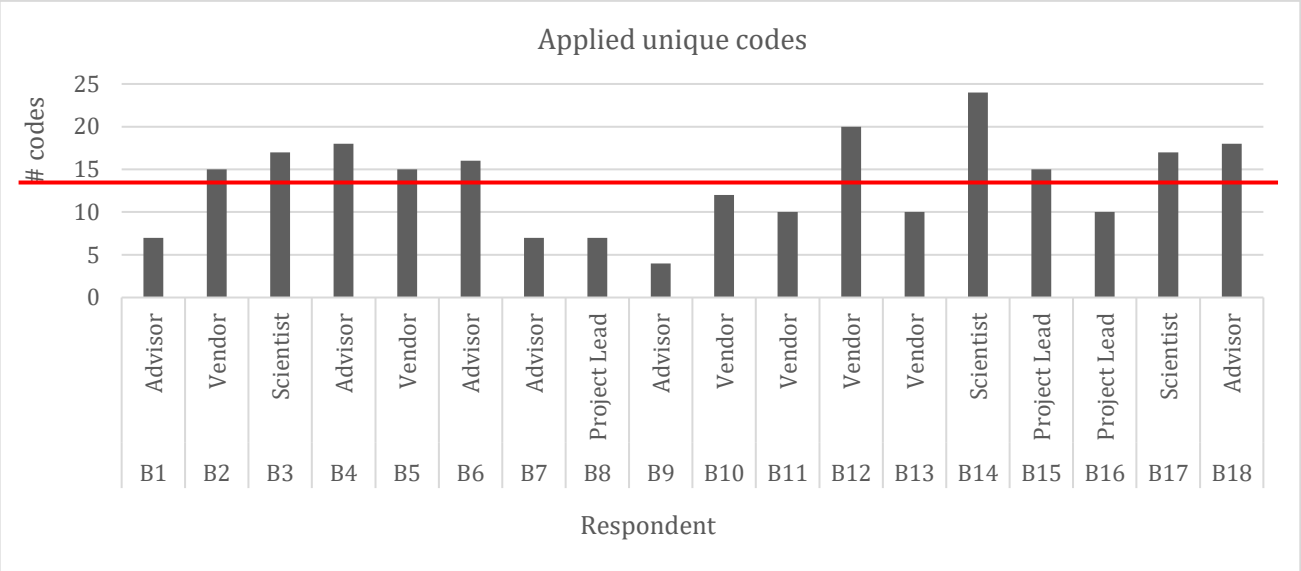


Figure 18: Number of codes applied to an interview

In figure 19, the number of new codes used is cumulatively plotted. Showing there is saturation in the conducted interviews. After interview B14, the 14th interview, no new codes were used in the Atlas.ti analyses.

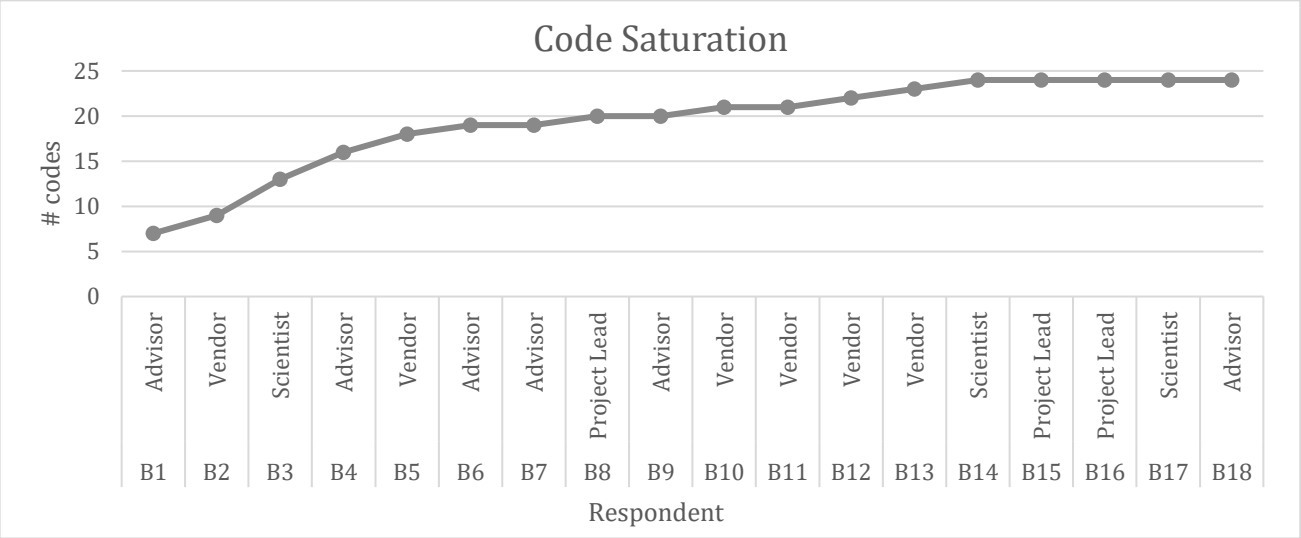


Figure 19: Overview of new codes used over the time

5.1.3 Meaning Saturation

In figure 20, an overview is presented of the meaning saturation. This graph indicates when the codes are used for the first time and when their meaning is saturated. Likewise, indicating that in additional interviews, no new meanings are found when the code is applied.

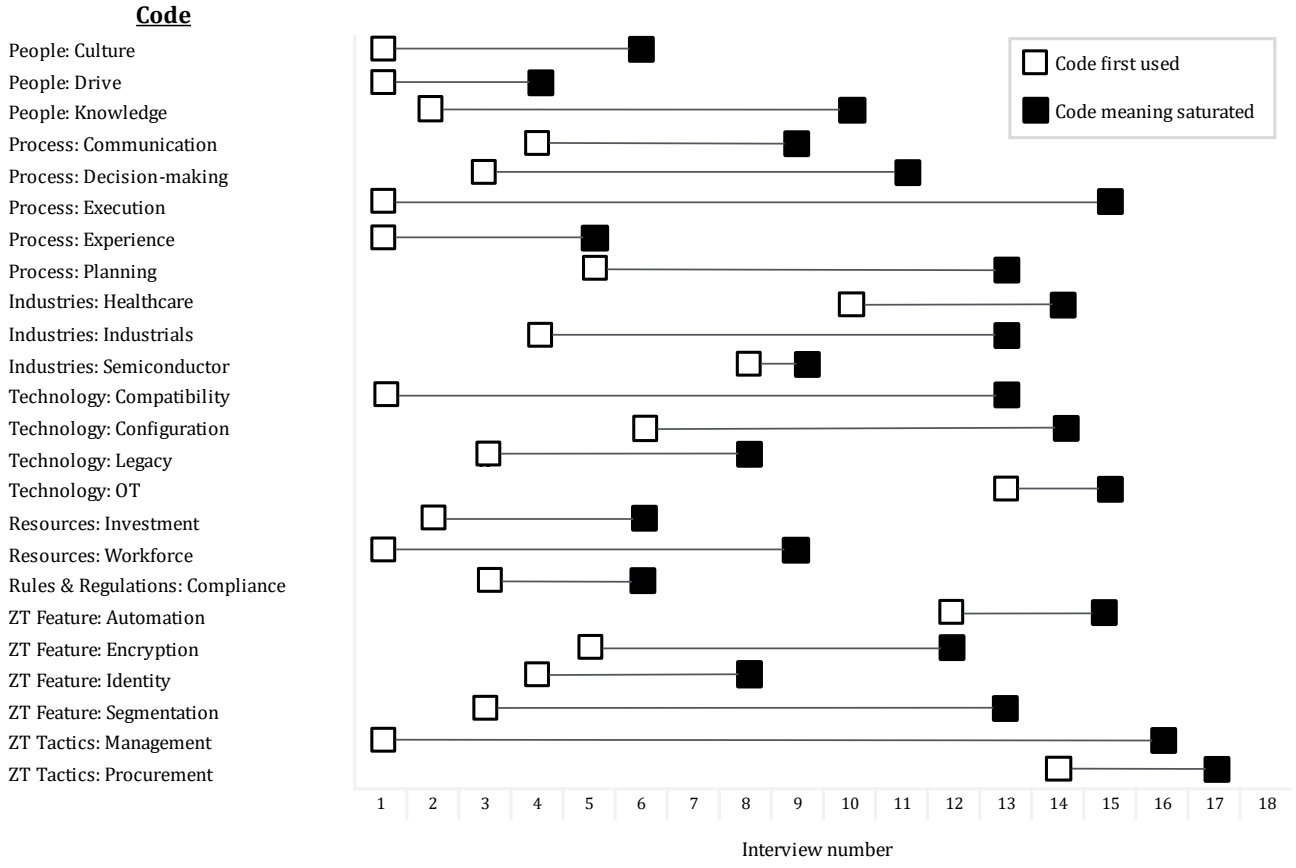


Figure 20: Meaning saturation

5.2 Interview Results

The outcomes of the Atlas.ti analysis are elaborated on below. The insights were gathered based on the distillation of the interviews. The interview findings are subdivided into eight sections which correspond with the previous defined main codes in Atlas.ti. The concepts will be discussed in the following order: People, Process, Technology, Rules & Regulations, Resources, Industry specials, ZTA features and ZT tactics.

5.2.1 People in ZTA transformations

As the transformation to a ZTA has a strong socio-technical nature, people have taken on a crucial role in the transformation. Three challenges were identified. According to the majority of scientists, employees are afraid to oversee the transformation as they do not want to be held responsible for technical implications. Moreover, it was found by one scientist that employees feel they are being viewed as an insider threat as the company wants to implement Zero Trust capabilities. Subsequently, most interviewees agree that a cultural shift or a form of cultural acceptance is the most challenging part for a company. Therefore, Zero Trust adoption requires a mindset shift typically driven by broader transformation efforts. Organizations' leadership must understand the value, endorse it, and provide necessary (non-)financial resources. The end-users will need to understand that a ZTA may work differently. Two tasks' users may have to do more in a ZTA are the following: the workforce will need to interact with the systems to validate their identity on a more regular basis, and they will need to deal with encryption more regularly and overtly.

Five success criteria should be followed. According to the majority of advisors and vendors, the proper understanding of Zero Trust is crucial as this can speed up the transformation process. Moreover, the whole company should be committed to the Zero Trust approach, and not only the architecture team must see the added value. Half of the interviewees suggested that it is important to regularly communicate to the organization about 'what' is done and 'how' this will be done to ensure dedication. Also, having buy-in from C-level is essential during transformation as there can be resistance from various organisational layers. Therefore, leadership alignment is crucial for driving Zero Trust agendas. Another suggestion was to put goals into a common language.

"*For example, a doctor may not care about a DDoS attack, but they do care about the concept of availability because if a clinical system goes down, they cannot treat the patients and the risk of harm to the patient increases." (B14, 2022)*

This statement implies that there is a common goal. Therefore, one of the CISO's vital capabilities is to learn how to get his or her story across the room, to make, e.g., doctors understand the situation. One of the scientists stated that: the organizations which had success educated and prepared their people about their plans and the importance of ZTA. Likewise, the most successful organizations had leadership who considered security a top priority and provided financial and policy support.

Besides the success criteria, architects must be aware of six pitfalls. Most advisors warn that the wrong implementation of a ZTA could lead to security fatigue. According to NIST (2016), this enactment can be seen as a weariness or reluctance to deal with computer security. Moreover, for most of the interviewees, the resistance could be caused by a wrong understanding of Zero Trust as there is still a lack of knowledge within the organizations regarding this topic. In addition, most vendors pointed out that this limited skillset also results in misconfigurations, causing an even more hazardous environment as Zero Trust will make the perimeter disappear. Additionally, organisations often already have the capabilities in-house but do not know how to enable them correctly.

"*For example, they have five licenses with a boatload or wealth of capabilities. Nevertheless, more often than not, organizations do not have the slightest clue of how to use them or leverage those capabilities and implement them." (B12, 2022)*

Another point of concern, according to the scientists, is that the security teams are making decisions behind locked meeting rooms without involving the other teams. The vendors confronted with these complications state that this could eventually cause a postponement of the Zero Trust project due to organizational resistance and a

lack of urgency. Or even worse, the project leads mentioned they had to deal with employees seeking loopholes to bypass security measures. This behaviour results in a growth of shadow IT and devices outside the company's control which would ruin everything that has been done. The scientists argued that employees should not be blamed for doing this as business demands to share the data, and time pressure plays a significant role.

5.2.2 Process in ZTA transformations

Four challenges are derived from the interviews focussing on the process. According to the majority of interviewees, formulating robust policies is one of the most challenging parts of the process. The policy formulation is a demanding process due to the implications Zero Trust can bring and the different interests of the stakeholders, making it difficult to reach a consensus. As reported by the advisors, the governance of access rights for human and technical identities can be challenging and time-consuming due to the dynamic environments. Most interviewees agree that prioritising the different ZT building blocks can cause discussion as the starting point of a transformation is different in each situation, making planning for Zero Trust difficult. Furthermore, implementing Zero Trust can take years to accomplish, as the journey can seem intimidating as there is no true "end state." Although this can sound contradictory, organisations that have invested little in cybersecurity in the past are embracing Zero Trust much quicker than organisations such as banks, which already have an entrenched cyber model.

To make the process successful, most of the interviewees advised to start small and scale the project in a later stage. The following example is provided:

'Do not start with your core banking application or one of your key applications. Start with something simple and learn from that and also build on those successes. So, if you have successfully implemented an element of Zero Trust, celebrate that success, share that success throughout the business, so you can leverage that success in executing the rest of your plan.' (B5, 2022)

Additionally, both the advisors and vendors state that it is vital to show ZT benefits in an early stage by generating measurable results. This exposure will ensure that the project will not be truncated prematurely.

How the process should be approached differs between all the interviewees. Some interviewees suggest it should be a risk-driven transition, while others propose the contrary and urge for an incremental change. In section 5.4, the challenges regarding the different approaches are summed.

The majority of the interviewees agree that the preparation of organizations is frequently not sufficient and that Zero Trust is not implemented over a night of sleep. All the interviewees, excluding the project leads, are convinced that projects start too often by implementing Zero Trust elements without having a clear roadmap. The majority of scientists classify this as "chasing a rabbit" and think organizations are frequently wrapped up in a vendor selection. Moreover, organizations frequently make mistakes by starting with shiny boxes and point solutions before having their policies formulated. Additionally, vendors often experience that organizations tend to make it a theoretical exercise. According to most of the advisors, the process cannot be started without having a solid foundation in place. The device and identity management must be appropriately organised before starting the transformation process.

5.2.3 Technology in ZTA transformations

According to the majority of vendors, the realization of implementing the technology can be seen as rather complex. The automation and orchestration of policies for ZTA are challenging as it requires effort to develop, deploy, and maintain properly. According to all the vendors, it is not easy to implement any security solution in OT environments as it must always operate.

The minority of advisors' state that the definitions for configurations in Azure, AWS and Google are misleading as they all sound similar, but in practice, they are different. One of the scientists pointed out that the poorly maintained legacy systems can be a pain point in a transformation process as people are hesitant to touch the "Golden Goose". The scientists point out that the technology hurdles are mostly around integration and API.

According to most advisors, the Zero Trust philosophy should be imposed on all the existing projects to make technology work. Moreover, the solutions provided by different vendors should be able to integrate properly into the existing system. Next, the technology must guarantee a seamless and consistent user experience. Lastly, the automation of security is critical as it is not an option to look at the incident a night after the attack or breach, as this is far too late. So, the system should not only detect but also must undertake direct actions and afterwards properly communicate what has happened and how the problem can be fixed accordingly.

The minority of interviews discovered that "vendor lock-in" or "vendor overlap" can be a drawback when acquiring new technology. The downside of lock-in is that the acquired solution is not compatible with the technologies of other vendors, making an organisation dependent on the vendor. The downside of overlap is that it is possible to buy equipment that is not needed as the capabilities are already in place.

According to most advisors, organizations have the idea that they can buy a box of Zero Trust, which is not the case. Besides, the introduction of the cloud has caused a sprawl of applications and environments. Advisors state that the vendors tend to overpromise organizations about the capabilities of their solutions.

According to most vendors, the biggest obstacle is OT devices' availability because some machines cannot be migrated as they are part of vital business processes. Moreover, the advisors argue that the possible configuration of security policies with native cloud controls is limited. Additionally, VPNs cannot entirely be removed as suppliers still require them for remote diagnostics.

5.2.4 Rules & Regulations applied to ZTA

The interviews resulted in a minimal number of insights regarding rules and regulations. For most interviewees, regulations were not a hot topic, whereas, for most scientists, it was an important subject. During their studies, it was found that ZTA's could cause auditing complications or, even worse, the loss of accreditation. The underlying motive is that the encryption was causing blind spots in the network visibility. Additionally, the scholars pointed out that the architect should be aware of the regulations presented in table 17, although this could sound evident.

Table 17: Rules & Regulations focusing on information security

Regulation	**Description**
General Data Protection Regulation (GDPR)	The GDPR is a set of rules for the processing of personal data. This EU regulation forces the handling of personal data of clients, employees, or others with care and responsibility.
Baseline Informatiebeveiliging Overheid (BIO)	A basic framework of standards for information security within all levels of government (central government, municipalities, and provinces)
Health Insurance Portability and Accountability Act	A federal law that mandated the development of national guidelines to prevent the disclosure of sensitive patient health information without the patient's knowledge or permission
NIS - Directive (EU) 2016/1148	A procedure to ensure a high degree of security is maintained across all Union networks and information systems
Payment Card Industry Data Security Standard	An information security standard that tightens security measures surrounding cardholder data to minimise payment card fraud
Confidentiality Integrity Availability (CIA) Triad	A model created to direct information security policy inside a company

5.2.5 Resources needed for realising a ZTA

The interviews resulted in generic challenges as most remarks apply to other IT transformations. The resource challenges are limited time, limited budget and a scarce workforce. Likewise, prioritising security investments is

difficult as it does not generate a direct return on investment. Second, the vendors believe the recruitment and development of cybersecurity talents are holding organizations back to change. Third, to make the ZTA transformation successful, proper training should be made available to the entire company. Fourth, the support of external parties such as consultancy firms could be helpful. Lastly, the scientists mention that the number of helpdesk tickets received can indicate whether the new architecture is a success.

5.2.6 Industry specials

In this section, industry-specific challenges regarding Zero Trust will be discussed. In the following order: 'Industrials', 'Healthcare', 'Financial Services'.

Industrials

According to the advisors, the biggest challenge in the 'Oil & Gas' and 'Manufacturing' sector is how security can be guaranteed across the whole value chain. Furthermore, preventing system downtime as operational continuity is one of the KPIs. Additionally, a significant challenge they encounter is the integration of IT & OT. File upload and remote maintenance must be possible within Zero Trust. In OT environments, it is not easy to implement any security solution because it must always operate. The following message is often being told to advisors;

"Yeah, we cannot update this machine. If this machine stops, it will take two hours before we can take it down. An upgrade of this machine will take 12 hours, and then we need to bring it up again. We need to validate if everything is still working. So, we will be out for 24 hours. Moreover, that will cost us millions." (B10, 2022)

Thus, introducing Zero Trust in an operational environment without disruption is one of the biggest complications. Although solutions can be tested in a sandbox, success is not guaranteed. Another challenge mentioned by the project leads is that they must deal with 20-year-old SCADA devices (OT). This issue makes it hard to implement Zero Trust principles on these machines. Vendors add that it is about finding the right balance of how much risk an organization is willing to take versus hardening the machines by adding additional controls around the OT devices to the point that the risk is becoming so big that it must be replaced.

Moreover, vendors mention that industrial businesses must consider firewalling or Deep Packet Inspection solutions. This alternative is needed because agents do not run on the OT device. After all, if something is installed on the OT device, it will break the warranty or support from the vendor. Lastly, one project lead mentioned that data exfiltration is the biggest threat to the semiconductor industry, so protecting their intellectual property is crucial. As they are concerned about field espionage.

Healthcare

For the healthcare industry, system availability is an essential factor. The second thing is the privacy of data rights. One of the most prominent digital initiatives is analytics to drive better healthcare outcomes. So, when it comes to healthcare information analytics and large databases, managing data rights and ensuring privacy is essential.

According to the vendors, the hospitals are slacking in their cybersecurity as they cannot find the right people and do not have the budget for SOC services to perform monitoring activities. Besides this financial constraint, there is a lack of awareness and wrong understanding of the positive consequences of available Zero Trust solutions. The project leads confirm the findings of the vendors and state that the hospitals are too slow in adopting new technologies. Another observation of the vendors is that the management systems of MRI or CT scans are still running on outdated operating systems, Windows 98 and Windows XP. Moreover, installing software on those machines is prohibited as the warranty expires. This limitation creates an obstacle in the transformation to a ZTA as the systems should be accessible to the supplier via a VPN connection to provide remote diagnostics.

Financial Services

The biggest threat of financial services is a fraud, ransomware, and sabotage. Moreover, this sector is regulatory-driven. It has much more obligations that need to be fulfilled. Therefore, organizations must ensure that the Zero Trust capabilities align with the rules and regulations. One of the vendors' major challenges is the consumers'

security, protecting their personally identifiable information. These kinds of organizations must be as transparent as possible and locate everything. This form of transparency means that the policy engines need to be traceable and auditable in the future. It should be understandable how the access decisions have been derived and how the trust level has been determined. The scientists emphasize that finance is all about infrastructure and ensuring that banking data and financial information are never touched. Additionally, financial services focus more on identity because they have a legal framework and are concerned with identity proofing.

5.2.7 ZTA Features

The interviews resulted in a variety of insights regarding **ZTA Features.** Five remarks regarding encryption are gathered. According to advisors, encryption is a crucial aspect of Zero Trust. Although the prerequisites, 'knowing what to encrypt' and 'know where the data is', sound basic, it is hard for many organisations to implement them correctly. Encryption is an excellent academic concept but difficult to implement in practice. For example, the key management can cause issues;

'In Germany, it is obligated to handle and store the keys completely self on-premises, meaning it cannot be done by the cloud provider like Microsoft, Amazon or Google.' (B5, 2022)

One of the scientists stated that applying encryption on the file level is cumbersome because each time a file is accessed, the user must decrypt it and allow access. Therefore, most organizations only focus on encrypting the sensitive files and do not encrypt the bulk. Besides, IKE exchange brings a massive vulnerability as it can become the single point of failure within the key exchange process. The advisors and scientists agree that encryption will put a lag on the system and will drain the performance, especially doing it when files are in transit. This issue is the largest for OT devices as they cannot utilize encryption tools. On the other hand, making encryption work on mobile devices is tricky as third-party applications and workarounds are needed. The user experience is therefore not frictionless, and a decent solution is missing on which mobile users can leverage.

Four remarks about an API gateway are gathered. According to the vendors, the extension of identity and access management of technical and shared accounts needed for APIs can be complicated. The advisors and vendors see the management and monitoring of the microservices as one of the biggest challenges that can form a threat. According to one of the scientists, the real issue that people are going to run into is that there is not enough processing power to make those microservices work at scale, and it is challenging to keep rogue microservices out of the network. Also, the reliance on the APIs of vendors is enormous, and maximum compatibility and interoperability are needed. As a result, the binary rules can form an issue. The basic allow or deny approach does not use dynamic, intelligent, and granular rules. Likewise, it does not consider device posture, location, or identity.

Five remarks about an identity driven ZTA are gathered. In a perfect world, the identity is verified per entity per transaction. However, this is not realistic based on how much is accessed by users all the time. So, organizations need to draw a line here. According to the scientists, this can differ per organization. According to the vendors, the 'identity focus' is a good approach but requires much management. This workload is contrary to what organizations desire, as they are looking for solutions that will lift the security level and lower the management of the IT. The scientists add that the trust score generator looks good on paper, but there is not always a single solution that can handle both the endpoints and user identities. Moreover, there is a fair chance that helpdesks are flooded with calls from people who cannot reach their resources.

Six remarks about a behaviour driven ZTA are gathered. An entire behaviour-driven architecture is hard to implement within the Netherlands due to restrictions of rules & regulations. On the other hand, one of the outlines would be that countries allow unsolicited solutions that can enable someone's webcam. Scientists mention that it can be challenging as cultural acceptance is needed, and human factors prevent this from being deployed. One of the scientists gave an accurate example;

'Humans are ultimately responsible. Though, a human does not want to get reprimanded or fired because the AI denied access to the CEO.' (B3, 2022)

According to the vendors, correctly understanding what is and is not suspicious behaviour is hard to determine for a bot. As there will always be grey areas, administrators are needed to define what is malicious, suspicious or allowed. Moreover, it should not be a black or white outcome, and an additional verification step should also be an option. Likewise, there can be legitimate reasons someone wants to access data outside office hours, such as working in a different time zone. One of the vendors points out that the tools themselves are compliant. Thus, it is more or less how organizations will implement the service, and the monitoring will be critical to comply.

Two remarks regarding software-defined perimeters are gathered. According to a minority of scientists, the challenge of an SDP architecture is that organizations are still wrapped around legacy technology. To get rid of these multimillion-dollar investments, they first must get aged. Another concern is that the vendor operates the SDP controller, resulting in less control over their DNS traffic. Because of this, organizations are holding back on the transformation to an SDP architecture.

5.2.8 ZTA Tactics

The Zero Trust security plan should be based on the existing security strategy. The following example was provided by one of the advisors;

'Ask any plant operator about what is most important. They will say safety, environmental safety, maintaining production goals, and protecting intellectual property is a no-brainer, so if you can base your Zero Trust architecture and your security program on that and can describe how it supports that, so very easy discussion that you are going to have.' (B16, 2022)

The **top-down** tactic focuses first on the cloud environment and afterwards on the physical on-premises devices. Vendors say the easiest way to start the journey is in the cloud. This clean sheet makes it possible to create a strong Zero Trust foundation consisting of a central identity management system and enforcement points. However, they understand that most organizations will stay as hybrids for the next five years.

There are exceptions and caveats; in 20% of the transformations, much cash can still be burned as it is seemingly impossible to integrate Zero Trust. Therefore, the most straightforward scenarios should be approached first, rather than worrying about the legacy infrastructure.

The **bottom-up** tactic is when the transformation starts on-premises and then moves to the cloud. According to the vendors, this will result in complex discussions about segmentation boxes, interoperability between systems and network access. Therefore, they suggest first having a foundation and then selecting the building blocks needed in the architecture. Invest in one building block, prove the success, and then get to the following building blocks.

When picking the **'best of bread'** tactic, it is essential to understand what that product covers and does not cover. Furthermore, where the overlaps are, ensuring that those overlaps do not jeopardize the organization. Additionally, there must be no gaps created without informing the organization.

The scientists are also sceptical about using the best of bread tactic as these solutions have capabilities that organizations either do not use, pay for, or do not work well with others. One example mentioned is that the solutions of Palo Alto and Cisco do not go well together. Another interviewee highlighted that it would be good to start with a vendor that can fulfil as much of the needs and then start looking at solutions around it. According to vendors, Zero Trust is all about the integration of solutions.

All interviewees agree that there is no specific order because each organization covers many different pieces of the puzzle. Even when comparing two banks, the risk model will be different. As a result, each Zero Trust journey is different. According to the project leads, the best way to start a ZT transformation is by first creating the asset inventory before adding the identity-based policies. However, the advisors disagree with this approach as compromised credentials cause most cyberattacks. They suggest starting implanting things like multi-factor authentication and conditional access and building the roadmap from there. The scientists add that the first thing that should be solved is identity and access management regarding the vertical of the organization. These steps are

critical because the easiest things a hacker can leverage are the usernames, passwords and tokens. Beyond that, different approaches can be considered. However, a popular approach is to develop a set of prioritized use cases and focus on implementing the parts of a ZTA that affect each use case. Additionally, advisors mentioned that the NIST framework should not be used as a biblical reference, but it should be used as a backing to start plotting the Zero Trust journey.

5.3 Conclusion

As the concept of Zero Trust is still a novel phenomenon, there are many technical, management, and ethical choices challenging the realisation of a ZTA, several insights were found to answer the second sub-question: *"What are the challenges for realising a Zero Trust architecture?"*

The respondents primarily named challenges from the transformation factors focussing on people, process, and technology. It is assumed that the rules and regulations are a less hot topic for the interviewees as they all have a technological background and a strong focus on IT. The challenges regarding resources, time, budget and workforce apply to a Zero Trust transformation and other transformations.

Although there are many challenges which the industries share, there are still differences. For the industrials, the two biggest challenges are 1) the trade-off between the system availability and system security as the cost of downtime can be much higher than the change of a possible attack and 2) the aged SCADA, OT systems that are not able to run security software. The healthcare industry's main issue is that privacy-sensitive information is not going into an extensive analytics database. The semiconductor industry is also cautious about protecting their data as their primary concern is data exfiltration.

The biggest challenge regarding the ZT capabilities is keeping the user experience frictionless while ensuring end-to-end encryption. At the same time, ensuring maximum compatibility and interoperability of the APIs.

Although the arguments are widespread, the opinions of the interviewees are rarely conflicting. There was only discussion if a ZT journey must be a risk-driven transition or not. Some interviewees are convinced that ZT should be risk-driven because less impact will be made if organizations will start with the easy parts or the elements with less user impact. Others are convinced that it is best to start with the simple systems first and develop a success record, which should help make the organisation more agreeable and allow organizations to try more and more complex transformations in the future.

In the next chapter, the first version of the design principles will be created, which should give the architects direction in adopting Zero Trust concepts.

Summary Chapter 5

An organization can be confronted with multiple challenges, success criteria, pitfalls and limitations when adopting concepts of a ZTA. The cultural shift or form of cultural acceptance is the biggest challenge for most interviewees, as broader transformation efforts are needed. Additionally, formulating policies is complicated due to the different interests of the stakeholders involved. It is crucial to start the project small at first with simple systems to ensure the transformation is not truncated prematurely. The legacy systems and operational technology (OT) equipment are elements that organizations hold back as they are hesitant to touch the "golden goose". Although encrypting data-at-rest and data-in-transit is an excellent academic concept, putting it into practice is challenging as not all endpoints are equipped with the required processing power.

Chapter 6. Design Principle Development

Design principles are needed to enable the transformation to a ZTA and guide the architect through the transformation process. Therefore, one of the research intentions is to find out what design principles can support the transformation. Likewise, this chapter aims to answer the sub-question:

"What are design principles for Zero Trust architecture transformations?"

First, the reasoning is given for principle-based design and why it is beneficial for a ZTA transformation. Subsequently, the draft list of principles is developed using the principle cycle of Greefhorst (2011).

6.1 Proof of Principle-Based Design

6.1.1 Usefulness of principle-based design

Principle-based design is suitable for the transformation to a ZTA as the environment involves actors with different goals but are interdependent. There is a wide range of solutions and alternatives to choose from when adopting Zero Trust concepts, as presented in section 4.3. Due to the various possibilities, design rules are too restrictive, and therefore design principles are seen as more valuable. According to Bharosa & Janssen (2015), design principles are "normative, reusable and directive guidelines, formulated towards taking action by the information system architects".

6.1.2 Principle structure

The template presented in table 18 is inspired by the OpenGroup, an international organization that develops and maintains IT standards. The approach of the OpenGroup will be extended with three additional elements to link to the ZTA Foundation, existing principles (chapter 4), and the challenges (chapter 5).

Table 18: Design principle template

Principle	**[short title to identify the principle]**
Kind/type	[Transformation / Target State]
Statement	Communication of the fundamental rule
Rationale	Justification, reasons for the principle (Why)
Implications	• [Action that should be taken to comply with the principle] • [Action "..."]
Foundational component	[Governance/ Visibility& Analytics / Automation & Orchestration / Identity / Endpoints / Network / Data / Application / Infrastructure]
Inspired by	P1 (……), P4 (……)
Remark	[PE../PR../TE../RR../RE..]

6.1.3 Elements making a good design principle

Although all the design principles should give the architect direction, five different types can be distinguished (Woods, 2010). Design principles can 1) define a goal or 2) indicate a preference or 3) avoid a specific technical problem or 4) encourage a way of working, or 5) remind people of useful, proven observations.

It is vital that the EA principles can be traced back to the organizational goal, and that goal is also communicated. The traceability should be provided by the principle's rationale (Woods, 2010).

According to Woods (2010), one of the common problems is that enterprise architects define strategic policies and standards that application architects find restrictive. They are resulting in ignorance and situations in which the policies and standards are largely ignored by development teams, as they are under pressure to get their system released or delivered on time. The cause of this problem is the actors' differing focus and priorities, as shown in figure 21.

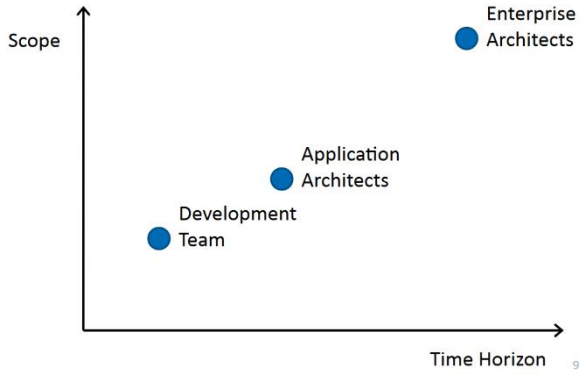


Figure 21: Scope of Architects (Woods, 2010)

6.1.3 Design principle criteria

In table 19, the criteria of Rozanski (2012) that should be considered when defining the design principles are presented.

Table 19: Design principle criteria (Rozanski, 2012)

Criteria	**Description**
Constructive	A principle must be stated for a definite purpose and should act as a helpful guide for decision making
Reasoned	A principle must be rational, logical, and consistent
Prescriptive	A principle must be specific, providing definite guidance
Well-articulated	A principle must be comprehensible by all the necessary stakeholders
Testable	A principle must be possible to be checked if it is followed
Significant	A principle must not be a truism. Would the opposite ever be the case?

6.2 Principle Formulation

As described in the methodology, the process of Greefhorst (2021) will be used for constructing the design principles. First, the drivers are described in section 6.3.1. Second, the drivers will be translated into credos in section 6.3.2

6.2.1 Principle grounding

Two complementary data collection instruments are used to underpin the formulation of the principles. The first instrument is a literature study performed in chapter 2, focussing on the basics of Zero Trust. Additionally, in chapter 4, the different elements that are used for constructing a ZTA are discussed. The second instrument applied is the semi-structured interviews described in chapter 5 to capture empirical evidence on the challenges arising during the realization of a ZTA.

6.2.2 Principle drivers

The drivers for the design principles will be determined first, consisting of the goals and objectives, issues, risks, values, potential rewards and constraints. This action is crucial because it should be traceable to the underlying goal of understanding a design principle. In table 20, an overview is provided of the drivers clustered on their type.

Table 20: Overview of principle drivers

Type	**Drivers**
Goal and objectives	- To enhance the cybersecurity of the enterprise - To reduce the organizations' attack surface (IBM, 2021) - To mitigate adversaries - To ensure that users only have access to the minimal amount of resources - To prevent malicious activity
Issues	- Immaturity and the novelty of Zero Trust - The transformation is complex and not a one-time effort
Risks	- Adversaries; cyber-attacks, and ransomware are becoming more sophisticated (Deloitte, 2021) - The network perimeter is no longer sufficient (Deloitte, 2021) - Lateral movement (IBM, 2021) - External and internal threats are always on the network
Values	- Commitment - Agility - Efficiency - Confidence in security system
Potential rewards	- Fast and secure access to data (Deloitte, 2021) - Improved data protection (Embrey, 2020)
Constraints	- Use a secure transport protocol - Lack of Zero Trust knowledge - Complete asset inventory - Not all devices are compatible - The workforce should be able to work from anywhere on any device (Deloitte, 2021)

6.2.3 Candidate principles

The drivers are translated to a list of candidate architecture principles. At this stage, the architecture principles can be considered credos. The complete list of 32 credos can be found in appendix H. Only the credos that are specific enough and focus on ZT are presented in table 21.

Table 21: Reduced list of credos

Type	Driver	Credo
Constraint	Lack of ZT knowledge	Educate the workforce
Constraint	Asset inventory	Know your architecture
Issue	Complexity	Start the Zero Trust journey simple
Issue	Implicit trust	Verify trust explicitly
Risk	Deviating legislation	Comply with regulations
Risk	Lateral movement	Construct segments
Risk	Lateral movement	Enforce least privilege
Risk	Sophisticated adversaries	Design inside out
Risk	Sophisticated adversaries	Monitor continuously
Value	Agility	Change incremental
Value	Commitment	Leave the ivory tower
Value	Efficiency	Integrate existing instruments

6.2.4 Testing of the preliminary list

In the early stage of the principle development, feedback was gathered from the Chief Architect Community. This community is a group consisting of 48 architects who are clients of Deloitte, from which 11 were willing to participate. The architects are employed at both multinationals and public organizations. During a focus group session, the experts are asked to share their insights on a preliminary version of the principles. As only a limited number (n=4) could participate in the session, a survey was shared with the absentees to gather additional feedback, which resulted in 7 responses.

Insights Workshop (n=4)

An online workshop was organised for the Chief Architect Community. This session was used to gather insights into their vision on what would be a strong principle and to gather their thoughts. For this session, a preliminary principle list was shared to gather already at early-stage feedback on the created work. The first takeaway of this session was that categories should be used to structure the principles. Additionally, more specifics should be added to the principles to understand what concept the principal is supporting. Also, the principles are perceived as too generic, and further specifications must be made.

Insights Survey (n=7)

Not all the architects were able to participate in the session. Therefore, a survey was shared to capture some additional feedback. The respondents are asked to review the principles on the following criteria: Clarity, Usability, Feasibility, and Importance. Subsequently, to review the complete list on the completeness and consistency. These insights are next to the workshop used to sharpen the principles.

6.2.5 Principle specification

The candidate principles are further specified in this phase, including their rationale and implications. This subprocess translates architecture principles from credos to norms. The list consists of the following 12 principles that will be discussed. Below the importance of the principles will be substantiated.

Name	**Principle 1: Verify trust explicitly**
Statement	Use all available information and telemetry to validate trust and assure security
Rationale	Every request could be a possible breach
Implications	• Treat every user, device, application/workload, and data flow as untrusted. • Authenticate and authorise each request with dynamics policies before providing access. • Use multiple contextual factors such as account, device, IP address and location. • Build a single Identity Access Management system • Ensure an encrypted connection, regardless of the endpoint location or health
Foundational components	Identity / Endpoints / Application
Inspired by	P4 (NCSC NL, 2021); P5, P7 (NCSC UK, 2021); P1, (OpenGroup, 2021); P1 (Forrester, 2021) P1, P2, P3 (Google, 2014); P1, P2, P3 (NSA, 2021); P1 (Microsoft, 2020); P2 (NIST, 2020); P1 (Palo Alto, 2021)
Remarks	n/a

Principle 1 ensures that no connection or communication occurs without validating the identity of an endpoint. This proof is essential because every request could be a possible breach. Therefore, this principle tackles the issue that access can be provided based on implicit trust.

Name	**Principle 2: Enforce 'least privilege'**
Statement	Maintain strict access controls on a need-to-know basis regardless of the endpoint health
Rationale	Enterprises need to ensure users only have access to the minimal amount of resources
Implications	• Deny access to Data, Applications, Assets and Services (DAAS) by default • Scrutinize all users, devices, data flows, and requests for access • Grant access to individual enterprise resources on a per-session basis (JIT/JEA) • Authorise each data or service request based on a dynamic or static policy • Align the security controls on the expected risk and business value
Foundational components	Governance/ Data / Application / Infrastructure
Inspired by	P2, P3 (NCSC NL, 2021); P4 (NCSC UK, 2021); P4, P7 (OpenGroup, 2021); P2 (Forrester, 2021) P6 (NSA, 2021); P2 (Microsoft, 2020); P3, P4, P6 (NIST, 2020); P3 (Palo Alto, 2021); P1 (Zscalar, 2021); P1 (IBM, 2021)
Remarks	n/a

Principle 2 ensures that users only have access to the minimal number of resources by denying access to Data, Applications, Assets and Services (DAAS) by default. Scrutinizing all users, devices, data flows, and access requests. Granting access to individual enterprise resources on a per-session basis. This principle will reduce lateral movement as a compromised account has little room for moving around.

Name	**Principle 3: Monitor continuously**
Statement	All traffic taking place between the endpoints should be monitored, inspected and logged continuously
Rationale	To verify that the communication is legitimate, safe, and secure. Zero Trust assumes that an adversary is already present within the environment
Implications	• Monitor user behaviour, device health, services, configuration changes, resource accesses and network traffic for suspicious activity (anomalies) • Examine all transactions to prevent data loss and attacks through malicious activities • Comply with privacy rules • Inform users that traffic is being logged
Foundational components	Visibility& Analytics / Endpoints / Network
Inspired by	P5 (NCSC NL, 2021); P3, P6 (NCSC UK, 2021); P3 (Forrester, 2021); P7 (NSA, 2021); P5, P7 (NIST, 2020); P2 (Palo Alto, 2021); P5 (IBM, 2021)
Remarks	n/a

Principle 3 ensures that all the network traffic is being monitored. Mitigating the problem of adversaries getting more sophisticated as it is assumed the network is hostile and a breach can always happen.

Name	**Principle 4: Construct segments**
Statement	Segment the infrastructure into small compartments and prevent interconnection.
Rationale	To minimise the lateral movement during a breach, the attacker should not be able to move through the infrastructure
Implications	• Make security controls asset-centric to provide authorisation on the lowest possible level • Build direct user-to-app and app-to-app connections • Ensure that the trust zones are granular
Foundational components	Network / Data / Application / Infrastructure
Inspired by	P5 (OpenGroup, 2021); P3 (Microsoft, 2020); P3 (Zscalar, 2021); P2 (IBM, 2021)
Remarks	PR10, TE02

Principle 4 ensures that the network is divided into small compartments. This segmentation is crucial as it minimises the risk of lateral movement during a breach. Additionally, making it possible to block the compromised sections.

Name	**Principle 5: Leave the ivory tower**
Statement	Do not create the ZTA design & policies isolated but make it a group exercise
Rationale	Multiple teams, including business process owners, system owners, infrastructure and application engineering, should be involved in the decision-making to create consensus, get their support and make them feel accountable.
Implications	• Define policies together • Involve actors from multiple teams to make sure all perspectives are captured • Gain consensus from stakeholders before embarking on the journey • Communicate regularly about what will be done and why this is done
Foundational components	Governance / Automation & Orchestration
Inspired by	P3 (OpenGroup, 2021)
Remarks	PE10, PE21, PR02

Principle 5 ensures that the architect involves other parties during the design process, which will create commitment of different disciplines. Although it can sound like a truism that an architect should not create an architecture design on his or her own, in practice, the involvement of other parties in the process seems to be limited. Therefore, it is crucial to involve people with different perspectives in the decision-making to get their support and make them feel accountable. Moreover, this will help formulate policies widely supported throughout the organization, mitigating the commitment issues.

Name	**Principle 6: Know your architecture**
Statement	Inventorize your business-critical data, applications, assets and services (DAAS)
Rationale	Before starting the Zero Trust journey, organizations should clearly understand what they need to protect.
Implications	• Know where the assets reside • Relevance elements should be tagged • Understand who should have access and under what conditions • Create an overview of the required access for all entities/endpoints connected to the network • Having end-to-end visibility on the assets, resources and the traffic between the assets and resources
Foundational component	Endpoints / Network / Data / Application / Infrastructure
Inspired by	P1, (NCSC NL, 2021); P1, (NCSC UK, 2021); P4 (NSA, 2021); P1 (NIST, 2020)
Remarks	TE11

Principle 6 ensures that all the endpoints and applications part of the organisation's heart are identified. Moreover, this principle should give the architect direction on where the priority of the transformation should be. Depending on what the crown jewels are, an approach can be selected. The goal of this principle is that first, a clear understanding of what needs to be protected is made before starting a Zero Trust journey. Moreover, this will help the prioritization of investments.

Name	Principle 7: Educate the workforce
Statement	Support your IT staff and end-users with the development of the needed skill set, mindset, and Zero Trust knowledge
Rationale	Implementing Zero Trust is a complex activity in which mistakes can be made quickly. The proper knowledge and mindset will mitigate these pitfalls.
Implications	• Create budget • Evangelise the concept of Zero Trust • Integrate the security discipline into the organization's culture, norms and processes
Foundational component	N/a
Inspired by	P3 (OpenGroup, 2021)
Remarks	PE05, PE013, PE15, PE19

Principle 7 ensures that the prior knowledge needed for a successful ZTA transformation is there to prevent pitfalls. This goal can be realised by collaborating with parties such as Nationaal Cyber Security Center (NCSC), Centrum Informatiebeveiliging en Privacybescherming (CIP), Digital Trust Center (DTC). Additionally, the involvement of consultancy firms could support and provide training to the organization.

Name	Principle 8: Start simple
Statement	Start Zero Trust project with simple capabilities (i.e., identity management, network segmentation) and scale big (e.g., auto-remediation) when accomplishments are being made
Rationale	To make sure Zero Trust projects/transformations are not cut due to high costs
Implications	• Do not try to do everything at once. • Zero Trust is not a one-time project • The Zero Trust programme must be agile as Zero Trust is evolving rapidly, and new capabilities arise frequently. • Measurable results should be generated. Buy-in from C-level is needed as the transformations can have implications on parts of the organization
Foundational component	Governance/ Visibility& Analytics / Automation & Orchestration / Identity / Endpoints / Network / Data / Application / Infrastructure
Inspired by	P6 (OpenGroup, 2021)
Remarks	PE22, PR09, PR20, PR21, PR22, TE02

Principle 8 ensures that the transformation process focuses on the less business-critical elements so mistakes can be made. Additionally, the principle should withhold the architect from doing everything at once as every protected surface is a win. This focus is vital to keep stakeholders on board during the transformation as the transformation will impact the way of working. Moreover, ensure success is shared within the organization to ensure projects are not cut due to high costs.

Name	Principle 9: Change incrementally
Statement	Do not try to flip the architecture into Zero Trust in one exercise.
Rationale	To prevent service degradation during the Zero Trust project, improvements to security should be made incrementally
Implications	• Ensure that the implementation of Zero Trust does not create loopholes • Ensure that the implementation of Zero Trust does not overly burden enterprise business processes • Do not focus only on the technical aspects • The organization should embrace changes
Foundational component	Automation & Orchestration / Network / Application / Infrastructure
Inspired by	P8 (OpenGroup, 2021)
Remarks	PR10

Principle 9 ensures that the transformation is not performed at once, and the Zero Trust philosophy is applied to planned transformations. Moreover, multiple iterations will create a more sophisticated design to mitigate the change of a failed project.

Name	Principle 10: Design inside out
Statement	Focus on the protect surface without discounting threat intelligence
Rationale	It is essential to start on the information side to ensure that the access to data, applications, assets and services (DAAS) is authenticated and monitored.
Implications	• Determine who has access to the data, not only the people but also the systems or external services • Start with protecting critical DAAS. Next, secure all paths to access them.
Foundational component	Data / Application / Infrastructure
Inspired by	P5 (NSA, 2021)
Remarks	PR16

Principle 10 ensures that a ZTA transformation focuses on the information side, not the attack vector. Because it is an old-fashioned way of thinking to keep the enemies out of the network, starting on the information side is essential to ensure that the access to DAAS is authenticated and monitored. This principle addresses the issue of adversaries becoming more sophisticated.

Name	Principle 11: Integrate instruments
Statement	Investigate current instruments (i.e., hardware & software or Cloud solutions) for Zero Trust capabilities before buying new services, licences and products to prevent vendor overlap.
Rationale	Organizations own more Zero Trust capabilities than they are aware of. Additionally, these technologies frequently fit seamlessly into a Zero Trust security architecture.
Implications	• Assessment of the current state • Investigation of licenses and services
Foundational component	Governance/ Visibility& Analytics / Automation & Orchestration
Inspired by	n/a
Remarks	TE20, TE21

Principle 11 ensures that no products are acquired which are already in possession. Although this principle can be perceived as a truism, this point was frequently mentioned during the interviews. Therefore, this principle is still part of the list.

Name	**Principle 12: Comply with regulations**
Statement	Cross-check the configurations of Zero Trust solutions to ensure local rules & regulations are not violated
Rationale	The offered Zero Trust solutions are not country specific. Therefore, some capabilities can conflict with local laws and regulations
Implications	• Configurations of Zero Trust solutions must be reviewed before execution • Understand whether there is a legitimate interest in processing the privacy-sensitive data through the Zero Trust solution • Appoint a third party for the assessment
Foundational component	Visibility & Analytics
Inspired by	n/a
Remarks	PE16, RR01, RR03, TE05

Principle 12 ensures that the designed architecture is not conflicting with the local rules and regulations. This precaution is vital as some default configurations of Zero Trust solutions, such as continuous monitoring, are not generally applicable.

6.2.6 Principle classification

To give the principles a better structure, they are clustered in categories to increase their accessibility.
According to Greefhorst (2011), *sets of principles can be grouped into themes, especially if they contain a large number of architecture principles. These themes may also be based on the dimensions* described earlier, although domain-specific clustering may also be very relevant.

The principles are subdivided into the following four categories:

- **Fundaments**: these are principles focussing on the core of the Zero Trust design [P1-P5]
- **People:** these are principles focussing on the human aspects of the transformation [P6, P7]
- **Process:** these are principles addressing the process of the transformation [P8-P10]
- **Technology:** these principles concentrate on the chosen solution for the transformation [P11, P12]

6.3 Conclusion

Currently, there is a lack of guidance in transforming to a ZTA. This issue is caused by the immaturity and novelty of this concept. The objective of this chapter was to develop design principles which provide direction in the transformation to a ZTA.

To answer the third sub-question, "*What are design principles for Zero Trust architecture transformations?*" the theory of Greefhorst (2011) was used.

The existing principles, the Chief Architect Community's input and the insights from the interviews were used to formulate the draft list of twelve design principles that should guide the transformation to a ZTA by using the Zero Trust philosophy. The area's publishers focus on the most are, verifying the identity with as many data points as possible and providing access on a need-to-know basis.

This artefact should accomplish that more organizations will take a Zero Trust approach and start implementing Zero Trust methods/technologies. The list of principles is limited to 12 design principles as the statements should only concentrate on the essence.

In the next chapter, the design principles are evaluated with architects to assess their practical value and formally accept them.

Summary Chapter 6

In this chapter twelve design principles are formulated that should be followed when transforming to a ZTA. In combination with the existing principles and the Chief Architect Community's input, the insights from the interviews were used to formulate design principles. The area's most publishers focus on the most are, verifying the identity with as many data points, and providing access on a need-to-know basis. Based on the theory of Bharossa (2015), Greefhorst (2011) and use of the TOGAF template (OpenGroup, 2018) design principles are formulated, resulting in a list of 12 design principles to guide the transformation. The list is structured into four categories to create better traceability, namely fundamentals, people, process and technology.

Chapter 7. Practical Value

This chapter concentrates on the last activities of the DSRM model, the design principle demonstration, evaluation and communication. Likewise, evaluate the principle value and receive suggestions to sharpen them further where needed.

7.1 Principle Demonstration

The draft principles are demonstrated via an online workshop with the Digital Architects NetWork (DANW), the knowledge and network organization for digital architects in the Netherlands. From this community, 17 people participated in the research. Figure 22 shows the background of each participant. Due to the variety of roles and expertise, a wide range of perspectives is captured.

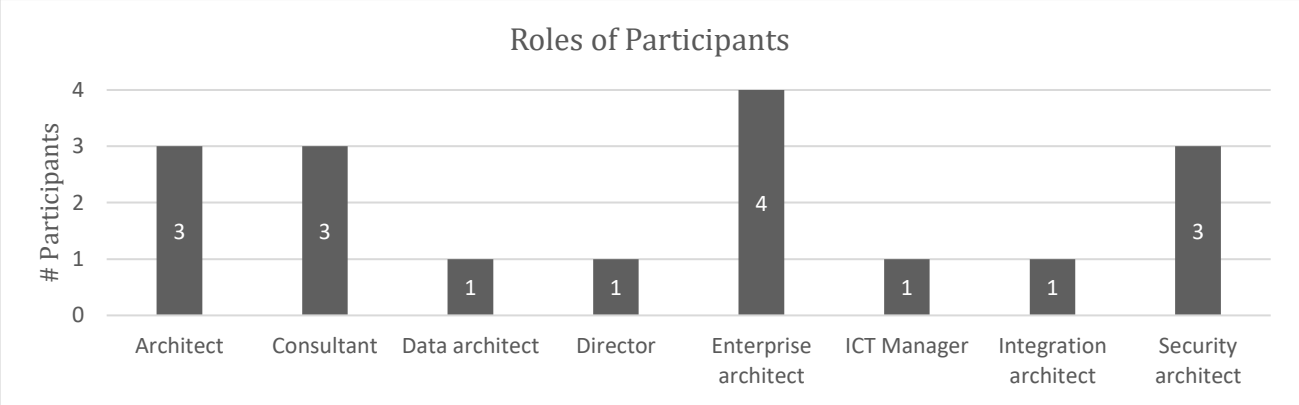


Figure 22: Overview of workshop participants

7.2 Principle Evaluation

7.2.1 Workshop Goal & structure

The workshop's goal was to assess the practical value of the individual principles. Likewise, to collect suggestions for improvement and sharpen the formulation of the name, statement, rationale and implications. Lastly, to discuss the complete set of principles on their completeness.

The workshop was structured as follows. First, the concept of Zero Trust was explained to provide all attendees with minimal needed knowledge. Second, the research goal and the objectives of the workshop were presented. Third, the criteria which should be used during the evaluation were discussed. Fourth, the principles were reviewed with the use of 'Mentimeter' (appendix H). This tool made it possible to create an interactive session in which the practical value could be discussed, and suggestions for improvement could be made.

The attendees were asked to assess the individual principles on their clarity, usability, relevancy and feasibility and the complete set on the representativity, accessibility and consistency

7.2.2 Feedback

Overall, the principles were understood and accepted by the participants. Therefore, in most cases, an additional explanation was not needed. Although the participants agreed that the principles are usable, they were not applied to actual use cases. Thus, this conclusion cannot yet be drawn. The majority of the principles are rated feasible. However, some of the principles sound simple on paper, but the implementation could still be challenging.

The list of principles was seen as complete. However, remarks were made that the general principles for a transformation should also be considered besides the Zero Trust principles. The following two principles were mentioned: 1) Communicate why change is happening and what is in there for the end-user, and 2) Recognize and celebrate milestones to keep momentum.

The participants were asked to assess and comment on the list of existing principles and to come up with different principles. Only one suggestion was made, but this principle was not added to the list as it was not concentrated on ZTA specifically. The suggestions to sharpen the name, statement, rationale and implications and make the principles more specific can be found in appendix H. Of the 12 principles, nine were accepted and did not need much change. However, three principles, P4, P6 and P11, were adjusted based on the received suggestions.

The participants were asked to measure the principle's perceived importance by ordering the 12 principles from most to least important. In table 22, the principles are ordered according to the perceived importance of architects.

Table 22: Perceived importance of principles

#	**Principle**	#	**Principle**
1	P2: Enforce least privilege	7	P10: Change incremental
2	P1: Validate trust Explicitly	8	P12: Integrate instruments
3	P4: Construct segments	9	P9: Start simple
4	P8: Design inside out	10	P7: Educate workforce
5	P3: Monitor continuously	11	P6: Leave the ivory tower
6	P5: Know your architecture	12	P11: Comply with regulations

The workshop participants were asked to assess the complete set of principles on three metrics: representativity, accessibility and consistency. Figure 23 shows the opinion on the complete list of principles.

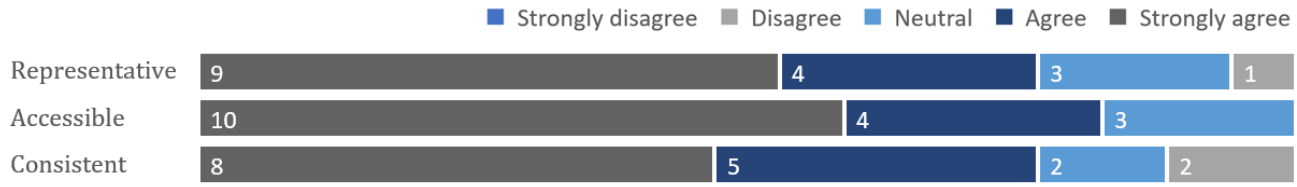


Figure 23: Assessment of design principles

7.2.3 Workshop limitation

As the workshop was organised online via MS Teams, it was sometimes difficult for the participants to interact as one person at a time could speak online. Additionally, as not all the participants had turned on their cameras, not all nonverbal contact could not be detected. The workshop was organised outside office hours between 07:00 pm-09:00 pm. The advantage of this timeslot was that more experts could participate in the workshop. This time of day could have a downside as the participants' energy level could be lower, influencing their sharpness.

7.3 Principle Communication

After evaluating the design principles and processing the feedback to improve the draft design principles, the final design principle framework is presented in figure 24.

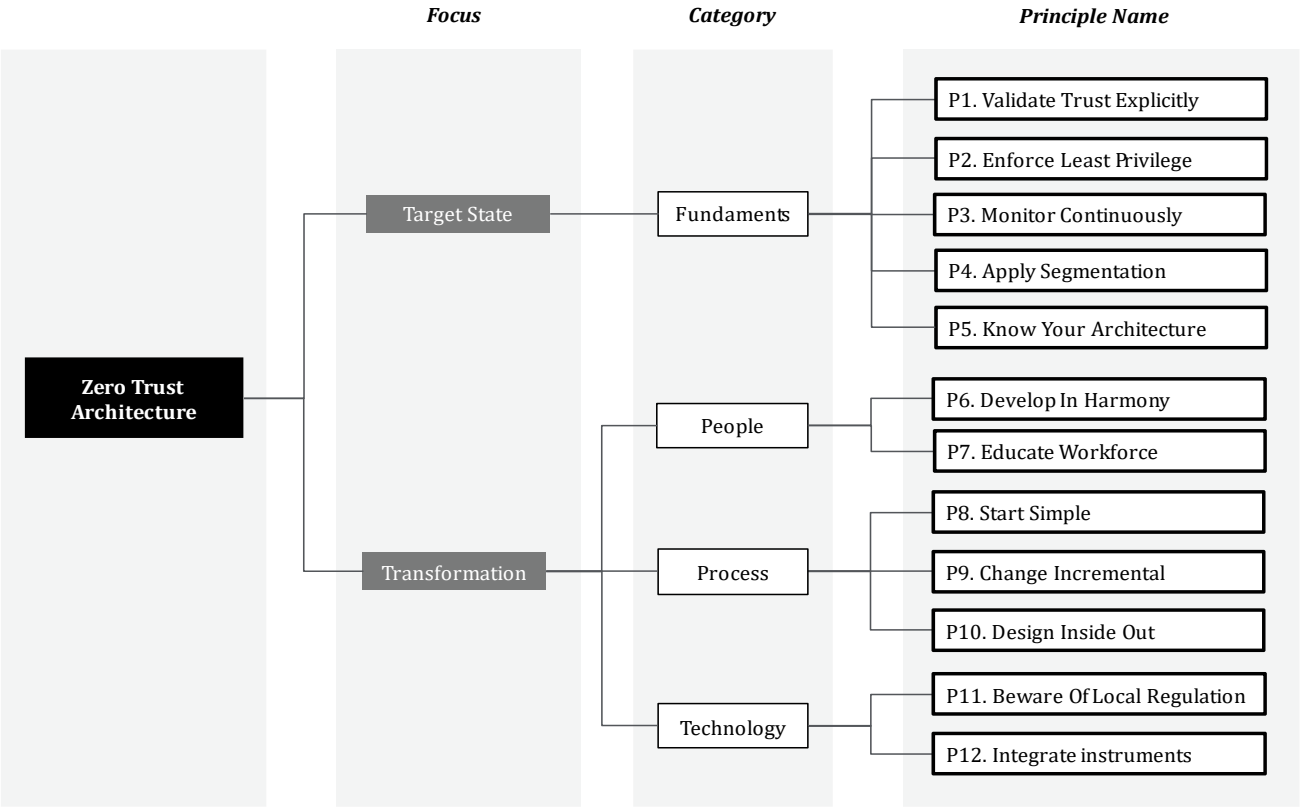


Figure 24: Design principle framework

The following five principles concentrate on the fundaments of a ZTA:

Name	**Principle 1: Validate trust explicitly**
Statement	Treat every user, device, application/workload, and data flow as untrusted
Rationale	To assure every request is inspected for a possible breach
Implications	• Authenticate and authorise each request before providing access • Use the strongest possible authentication to establish identity, like a trust algorithm • The level of assurance should depend on the risks • Make use of tokens for authorisation • Build a single Identity Access Management system

Name	**Principle 2: Enforce 'least privilege'**
Statement	Maintain strict access controls on a need-to-know basis regardless of the endpoint health and location to ensure users only have access to the minimal number of resources
Rationale	To what you do not have access cannot be leaked
Implications	• Deny access to Data, Applications, Assets and Services (DAAS) by default • Scrutinize all users, devices, data flows, and requests for access • Grant access to individual enterprise resources on a per-session basis • Evaluate the validity period of a session

Name	**Principle 3: Monitor continuously**
Statement	Monitor, inspect and log all traffic taking place in the network
Rationale	To verify that the communication is legitimate, safe, and secure, a Zero Trust philosophy assumes that an adversary is already present within the environment
Implications	• Monitor users, devices, services, configuration changes, resource accesses and network traffic for suspicious activity, anomalies and follow up immediately • Examine all transactions to prevent data loss and attacks through malicious activities • Use gathered data for making access decisions • In the case of BYOD, do not capture private network traffic • Automatic monitoring can ensure compliance with privacy rules • Inform users that traffic is being logged

Name	**Principle 4: Apply segmentation on all architectural levels**
Statement	Ensure that the infrastructure and applications are segmented in small compartments and not interconnected.
Rationale	To minimise the lateral movement and mitigate the possible compromise, the attacker should not be able to move through the infrastructure during a breach
Implications	• Make use of microservices, software-defined perimeters and physical equipment. • Execute monitoring • Provide authorisation on the lowest possible level • Ensure that the trust zones are granular

Name	**Principle 5: Know your architecture**
Statement	Identify your business-critical data, applications, assets, and services (DAAS)
Rationale	To understand what needs to be protected prior to starting on a Zero Trust journey
Implications	• Know where the assets reside within the organization • Relevance elements should be tagged • Understand who should have access and under what conditions • Create an overview of the required access for all entities and endpoints connected to the network • Having end-to-end visibility on the assets, resources and the traffic between those assets and resources

The following two principles concentrate on the people in the transformation to a ZTA:

Name	**Principle 6: Develop in harmony**
Statement	Do not create the ZTA design and policies isolated but make it a team exercise
Rationale	To create consensus, get support and create accountability within, multiple teams, including business process owners, system owners, infrastructure and application engineering, should be involved in the decision-making of policies
Implications	• Define policies together • Involve actors from multiple teams to make sure all perspectives are captured • Gain consensus from stakeholders before embarking on the journey

Name	**Principle 7: Educate the workforce**
Statement	Support your IT staff and end-users with the development of the needed skillset and Zero Trust knowledge
Rationale	To mitigate the pitfalls, proper knowledge is needed as implementing Zero Trust is a complex activity in which mistakes can be made quickly.
Implications	• Ensure the budget is available • Zero Trust by design requires knowledgeable staff • Evangelise the concept of Zero Trust

The following three principles concentrate on the transformation process to a ZTA:

Name	**Principle 8: Start simple**
Statement	Start Zero Trust project with simple capabilities (i.e., identity management, network segmentation) to get all involved acquainted and scale big (e.g., auto-remediation) when accomplishments are being made
Rationale	To ensure transformations are not cut due to a lack of motivation and high costs. Moreover, preventing the new security measure creates additional risk.
Implications	• Do not try to do everything at once • Start with the less critical environment first • Scalability last but complete security first • Zero Trust is not a one-time project • The Zero Trust programme must be agile as Zero Trust is evolving rapidly, and new capabilities arrive frequently • Measurable results should be generated. Buy-in from C-level is needed as the transformations can have implications on parts of the organization

Name	**Principle 9: Change incrementally**
Statement	Take advantage of the planned transformations by imposing the Zero Trust philosophy on all the existing projects
Rationale	To minimize the risk and prevent service degradation during the Zero Trust project, improvements to security should be made incrementally
Implications	• Ensure that the implementation of Zero Trust does not overly burden enterprise business processes • Do not focus only on the technical aspects • Deliver quickly and regularly • Communicate regularly about what will be done and why this is done • The organization should embrace changes

Name	**Principle 10: Design inside out**
Statement	Focus on business valuable DAAS (data, applications, assets, and services) without discounting threat intelligence
Rationale	To ensure that the access provided to DAAS is authorized and monitored, the Zero Trust journey should start on the 'protect surface' instead of the 'attack surface.'
Implications	• Determine who has access to the data, not only the people but also the systems or external services • First, focus on protecting critical DAAS. Second, secure all paths to access them.

The following two principles concentrate on technology in the transformation to a ZTA:

Name	**Principle 11: Integrate existing instruments**
Statement	Combine the existing instruments (i.e., hardware & software or Cloud solutions) for Zero Trust capabilities before buying new services, licences and products
Rationale	To prevent vendor overlap, raise awareness of the Zero Trust capabilities organizations already own, as these technologies can fit sometimes seamlessly into a Zero Trust security architecture.
Implications	• Assessment of the current state • Investigation of licenses and services

Name	**Principle 12: Beware of local regulation**
Statement	Cross-check the configurations of Zero Trust solutions on restricted capabilities
Rationale	To ensure local rules & regulations are not violated. Because some capabilities can conflict with local law and regulations since some of the offered Zero Trust solutions are not country specific.
Implications	• Make the Zero Trust solution adaptable to local regulations • Configurations of Zero Trust solutions must be reviewed before execution • Understand whether there is a legitimate interest in processing the privacy-sensitive data through the Zero Trust solution • Appoint a third party for the assessment

7.4 Conclusion

After the demonstration and evaluation, an answer can be provided to the last sub-question; *"To what extent are the created design principles usable in practice?"*

The demonstration and evaluation of the principles were performed with the use of an online workshop. The goal was to assess the practical value based on the feasibility, usability, and perceived importance to the business. Moreover, the participants assessed the quality of the principle, statement, rationale, and implications. Several suggestions were made on how the statement rationale and implications can be sharpened to make the principles more specific.

The architects confirm that 9/12 principles are useful, relevant and have a clear, practical value. Additionally, they confirm that 3/12 principles are less useful, but they can be equally valuable with some refinement. Besides, there were no suggestions for adding any new principles to the complete list of principles. None of the principles was rejected or seen as irrelevant.

The majority of the group was positive about the design principles list despite some discussions as not all participants had the same prior knowledge regarding Zero Trust. To conclude, although the design principles are not yet put into practice, the outcomes of this design cycle can still be seen as valuable.

Summary Chapter 7

In this last chapter the practical value of the principles was tested to measure to what extent the created design principles are usable in practice. The evaluation of the principles with the architects made it possible to formally accept the principles. The participants of the workshop agreed that the design principles were usable, although some of the principles had to be sharpened. Moreover, there were no suggestions for adding different principles.

Chapter 8. Conclusion & Discussion

This chapter will conclude the research by summarizing the main findings in relation to the research objectives and questions (section 8.1). Subsequently, a discussion about the value and contribution will follow (section 8.2), the limitations will be discussed, and recommendations will be made for further research (section 8.3).

8.1 Conclusion

This research was set out to understand how organizations can establish a Zero Trust architecture. Furthermore, the aim was to define design principles for ZTA transformations to increase an organisation's overall cybersecurity. This question arose from the problem that reference architectures or guidelines that support the transformation to a Zero Trust EA seem to be lacking. Therefore, this study focuses on developing knowledge artefacts to give the architects direction during the transformation to a ZTA.

An answer to the research questions can be formulated as the goals of this study are fulfilled.

The main research question was:

"How can organizations transform their current [security] architecture by adopting Zero Trust concepts?".

Based on the reference architectures, an overview of challenges and design principles, the following conclusions can be drawn from this study. An organization can transform to a ZTA by achieving the following:

Before starting the ZTA transformation, it is suggested to facilitate extensive training for the entire organization to ensure the required ZT knowledge is available. Moreover, research suggests creating a shared vision within the board, and the business process owners as the transformations will impact the entire organisation. The training aims to ensure that everyone understands the mission and why a transformation must be achieved.

Moreover, the majority of interviewees suggest to create visibility of the organizations' assets, inventory devices and user accounts. This job can be achieved by having the 'Identity and Access Management' and 'Asset Management' capabilities.

Additionally, a focus area must be defined to prioritize Zero Trust building blocks. The idea is to start with simple non-business critical elements and subsequently expand the transformation scope. Thereafter, impose the ZT philosophy on all existing projects while keeping it cost-efficient.

Lastly, validation of the ZTA is critical before it is rolled out at scale. Failing to validate the architecture properly can result in malfunctioning user accounts and applications. Additionally, it is suggested to demonstrate and communicate business outcomes to the organization to prevent the initiative from fading away.

A wide range of models and a mix of approaches can be used to establish a ZTA, each having its benefits and disadvantages. It is essential to choose a model and an architectural approach that fits the organisation best. The models which can be used are resource portal, enclave or a device agent/gateway-based model. The approaches that can be used are a combination of enhanced identity and/or segmentation and/or dynamic access policies and/or trust algorithm and/or automation and/or Artificial Intelligence-driven.

It is a common misconception that a ZTA can already be achieved by only segmenting the infrastructure and removing the perimeter. Instead, all the social and technical system elements must transform. To conclude, establishing a ZTA is a true transformation of the socio-technical system, and the set of design principles could help with this by providing direction.

The first sub-question was:

"What defines a Zero Trust architecture?"

In chapter 4, an exploratory study was conducted to create an overview of different models, strategies and technologies used to establish a ZTA. The following conclusions were drawn based on this study:

There is no consensus in the literature about the requirements of a ZTA, and the examination indicates that various methods can be used to establish a ZTA. Nevertheless, the commercially deployed ZTA's can be clustered in three generic models, and all found architectures can be divided into a control and data plane.

Although the scholars and non-scientific authors have different opinions, they all agree that identity management is fundamental to any Zero Trust solution since a ZTA cannot be established without identity verification and access control.

Additionally, five strategies contribute to the establishment of a ZTA. The first two strategies, 'enhanced identity' and 'segmentation', can be applied immediately. However, for the other three strategies, 'trust algorithm', 'automation', and 'artificial intelligence', a fundament consisting of device and user management must be in place.

Besides the strategies, there are various configurations possible to achieve a ZTA. The alternatives can be clustered into six pillars: identity, endpoints, network, data, application and infrastructure. Additionally, three cross pillar themes are found: governance, visibility & analytics, automation & orchestration.

Lastly, the literature review indicates that Zero Trust is not an architype but rather a way of designing an organization's security architecture.

The second sub-question was:

"What are the challenges for realising a Zero Trust architecture?"

In chapter 5, the challenges were captured that arise when realizing a ZTA through semi-structured interviews. Furthermore, by using the list of remarks, pitfalls can be mitigated. Likewise, the interviews indicate dependencies for successfully creating a ZTA, and aspects of people, process, technology, rules & regulations, and resources the organizations need to be considered. The following conclusions can be drawn:

As the concept of Zero Trust is still a novel phenomenon, there are many technical, management, and ethical choices challenging the realisation of a ZTA.

A culture shift must be established from inside out to enable ZTA within an organization.
Integrating different technologies and applications can be challenging as there is no 'silver bullet' for achieving a ZTA.

Moreover, the challenges identified vary between the different personas. The scientists point out that organizations are postponing the Zero Trust journey because employees fear the technical implications. Next, the vendors address that the limited skillset is the most challenging because misconfigurations can lead to an even more hazardous environment. Likewise, the advisors are confronted with situations at which point solutions are being used in a sub-optimal way. Lastly, the project leaders find the deployment in an operational environment challenging, as the implementation cannot disrupt the processes. Most interviews suggest making the security frictionless; otherwise, the workforce will use loopholes to bypass the security measures and trust zones.

The third sub-question was:

"What are design principles for Zero Trust architecture transformations?"

In chapter 6, the existing principles, the Chief Architect Community's input and the insights from the interviews were used to formulate the draft list of twelve design principles that should guide the transformation to a ZTA by using the Zero Trust philosophy. The following conclusions can be drawn:

The area's publishers focus on the most are, verifying the identity with as many data points as possible and providing access on a need-to-know basis.

This artefact should accomplish that more organizations will take a Zero Trust approach and start implementing Zero Trust methods/technologies. The list of principles is limited to 12 design principles as the statements should only concentrate on the essence of a ZTA transformation.

In table 23, the final list of principles is presented.

Table 23: Overview of Final principles

Group	#	Principle	Statement
Fundaments	1	Validate trust explicitly	Treat every user, device, application/workload, and data flow as untrusted.
	2	Enforce 'least privilege'	Maintain strict access controls on a need-to-know basis regardless of the endpoint health and location to ensure users only have access to the minimal number of resources
	3	Monitor continuously	Monitor, inspect and log all traffic taking place in the network
	4	Apply segmentation	Ensure that the infrastructure and applications are segmented in small compartments on all architectural levels and not interconnected.
	5	Know your architecture	Identify the business-critical data, applications, assets and services (DAAS)
People	6	Develop in harmony	Do not create the ZTA design and policies isolated but make it a team effort
	7	Educate workforce	Support your IT staff and end-users with the development of the needed skillset and Zero Trust knowledge
Process	8	Start simple	Start Zero Trust project small with simple capabilities (i.e., identity management, network segmentation) to get all involved acquainted, and scale big (e.g., auto-remediation) when accomplishments are being made
	9	Change incremental	Take advantage of the planned changes by imposing the Zero Trust philosophy on all your existing projects
	10	Design inside out	Focus on business valuable DAAS (data, applications, assets, and services) without discounting threat intelligence
Technology	11	Integrate instruments	Combine the existing instruments, including hardware, software or cloud solutions, for Zero Trust capabilities before buying new services, licenses and products to prevent vendor overlap.
	12	Beware of local regulation	Cross-check the configurations of Zero Trust solutions to ensure local rules & regulations are not violated

The fourth sub-question was:

"To what extent are the created design principles usable in practice?"

In chapter 7, the usability of the design principles was tested to measure to what extent the created design principles are valuable for the architects. The evaluation of the principles made it possible to formally accept the principles. The following conclusions can be drawn:

The architects confirm that 9/12 principles are useful, relevant and have a clear, practical value. Moreover, they confirm that 3/12 principles are less useful, but they can be equally valuable with some refinement. Besides, there were no suggestions for adding any new principles to the complete list of principles. None of the principles was rejected or seen as irrelevant.

8.2 Contribution of this research

Scientifically, this research contributes to the academic field by combining all the available information and creating clarity in this novel field. The knowledge artefacts try to close the gap by creating an overview of the characteristics of ZTAs, describing the crucial factors of realising a ZTA. Furthermore, practical value is ensured by providing design principles for architects who want to transform their architecture and create a guarded environment. Last but even more important, the research contributes to society indirect by the improvement of the protection of Intellectual Property and personal data as verification becomes key. Another benefit is that establishing a ZTA will support the possibility of hybrid working, as remote working has increasingly been adopted after the covid-19 pandemic.

In conclusion, this research helps to better understand "Zero Trust" architecture for an environment in which the perimeters are faded. Further, it will help organizations apply the concepts to harness and secure their organization against future attacks. Besides, it provides a theoretical basis for a novel field that is relatively unexplored. The main contribution is a list of evaluated design principles that can guide a transformation to a ZTA. Moreover, an overview of challenges, success criteria, limitations and pitfalls are provided. Lastly, high-level reference architectures are made, which can help in the storytelling and engagement of stakeholders.

8.3 Discussion, Limitations & Recommendations

In section 8.2.1, the research results, the methods & theories used to come to these conclusions are debated. Next, in section 8.2.2, the limitations of this study are elaborated. Lastly, in section 8.2.3, directions for further research are identified.

8.3.1 Discussion of the findings

A qualitative study is performed based on the Information System Research Framework (Hevner, 2004). This method allowed to combine the available literature from the knowledge base with the business needs to develop knowledge artefacts that should help the architect. The study's findings will be discussed following the cycles of the ISR framework.

The benefit of doing a multivocal literature review (MLR) in the rigor cycle is that it provides a very rich amount of data as this methodology combines both formal and grey literature. Likewise, it combines state-of-the-art and state of practice in each area and closes the gap between academic research and professional practice. MLR is suitable for this study as this field of research is not fully explored, and the amount of available literature is limited. The downside of using grey literature is that the probability of misleading information is increased as it is easier to

publish a white paper than a journal. Moreover, grey literature generally provides a one-sided view of Zero Trust as the focus is mainly on the benefits. Most of the publications identified had a commercial agenda.

Using semi-structured interviews in the relevance cycle provides the opportunity to retrieve empirical evidence on this topic. A possible downside could be that the validity cannot be guaranteed with only a limited number of interviewees (N=18). However, a saturation check is performed, and the elbow curve shows that no substantial insights would be generated by increasing the number of interviews. In addition, the vendors are overrepresented, and the scientists and project leads are underrepresented. This uneven distribution of interviewees over the personas is not seen as a problem as it does not influence the research outcome.

The development of codes can vary between researchers, meaning that codes can be more specific or generic, leading to different outcomes.

The advantage of building the knowledge artefact in the design cycle is that the input of the knowledge base and the environment can be combined. Moreover, it is possible to test the artefact multiple times and refine it if needed. For this study, two evaluations were executed with two different groups of architects, after which the principles were refined.

8.3.2 Limitations of the study

Initially, the goal of the research was to define architypes. Unfortunately, at the start of the research, this was not possible. Because it was assumed that there would be different architypes to describe, research proved that different architypes could not be demarcated, and ZTA is more like a security strategy and a philosophy than an architype. Therefore, the initial question SQ1, "*What types of Zero Trust architectures exist?*" is changed into "*What are characteristics of Zero Trust architectures?*". However, an attempt is being made to create five reference architectures that should give an overview of what a ZTA could resemble. Although these architectures are not validated, the described architectures can be helpful for further research.

The amount of empirical evidence for the research is limited since case studies were not involved. Because of the immaturity of ZTA architectures in practice, it was impossible to validate the research with a case study.

Additionally, the knowledge artefacts are not validated in practice but are evaluated with the use of workshops. It was impossible to do a proper evaluation since a complete ZTA transformation can take up to 5 years, while the research was done in only five months.

Another limitation could be that articles in the multivocal literature review could be missed due to the limited time. Also, as ZTA is still a novel topic, new articles may still be in the publication phase. Resulting in that this literature is not included in the theoretical research selection. As the terminology is still evolving, it could be possible that the search string of the literature review is not covering all relevant concepts. Moreover, the process of manual information assessment and extraction could lead to inaccuracies and subjectivity, although the guideline of Kitchenham (2017) and Garousi (2019) are followed. Some literature is not publicly available. It is behind the paywall of Forrester or Gartner; single reports can cost up to 1500 dollars. Unfortunately, the budget to access these articles was not available for this research.

Even though the conducted interviews give valuable insights into the challenges that arise when transforming to a ZTA, more interviews could be held to ensure no additional codes or subcodes are missed in the current research. The extent to which the research outcome can be generalized for different industries is not tested. Moreover, the interviewees lived and worked in Europe and North America. Other continents are not covered in this study. For a follow-up study, it could also be interesting to explore if there is a difference in ZTA maturity between different countries or continents.

The use of Atlas.ti web versus desktop limited the analyses of the interview coding. This problem is because the web application has fewer features than the desktop application. In the web application, creating a co-occurrence coefficient table showing the relationships in the data is impossible. Therefore, it is advised to use the desktop application in further studies.

The number of participants involved in the ZTA design principle examination was sufficient to obtain different insights and feedback to create a final version of the knowledge artefact. However, since all interviews and workshops were organized online, more insights could be gained if the session was organised physically. It is assumed that the session could take longer, and eye contact can be made with the participants to ensure they understand the material. Additionally, making sure the participants are paying attention. On the other hand, a positive influence could be that it was easier to provide feedback since participants could type their suggestions in the Mentimeter. Therefore, online interviews and feedback sessions both have positive and negative influences on the research outcome. The study's validity can be increased by repeating the group session with more participants from a broader range of public and private organizations.

With only the use of the set of design principles, a ZTA will not be achieved. The transformation effort will entail much more, as described in chapter 5. Due to the socio-technical nature of the problem, a cultural change is needed within the organisation.

8.3.3 Recommendation

As a result of the discussion and the study's limitations, the following directions can be identified for further research.

First, additional empirical evidence on the end-user experience should be gathered as there are still a lot of cultural issues that have not been addressed. It would be interesting to learn more about these issues as enterprises move towards a ZTA. Conducting case studies would be a viable solution for gathering additional empirical evidence regarding the transformation to a ZTA.

Second, it would be recommended to conduct further studies on the possible disadvantages of ZTAs. The benefits are discussed extensively in the literature and do not concentrate on the possible downsides. Because of all described benefits, the uncertainty with respect to the novelty of the concept decreases. Moreover, further literature research is needed to discover the possible chokepoints of ZTA deployment models, e.g., an unreachable PEP or PDP.

Thirdly, to generalize the outcome of the research and apply it to industries other than healthcare and industrials, the application of Zero Trust should be studied in a wider variety of industries. Additionally, it would be relevant to create reference architectures for different industries.

Next, a cost-benefit analysis should be performed to make the costs for ZTA quantifiable since legacy systems need to be replaced in Zero Trust transformations.

What has remained underexposed in this study are governance, risk, and compliance considerations for Zero Trust. Therefore, it is suggested to investigate these considerations in future studies.

As the practical value of the principles is currently only tested by the CAC and the DANW, two other communities could be involved in the testing of the artefacts, which are the ‘NIST ZTA Forum’ and the ‘OpenGroup ZTA Workgroup’.

Zero Trust benefits by improving the data security of possible citizens' information. However, the needed monitoring, which is part of the fundamental constructs, can be conflicting and cause ethical issues. Implementing “Zero Trust” architecture could harm feelings of trust in the workforce. Therefore, how companies shape their messages and inform their employees is essential. An idea could be to include the end-user in further research, the ones working in an organisation in which a ZTA is applied. Research can show how end-users experience Zero Trust to get an idea if they feel they cannot be trusted.

A suggestion for questions that could be investigated in further research would be: 1) What is the impact of the implementation of Zero Trust concepts on the workforce? 2) What is the perfect balance between security and convenience?

8.4 Reflection

8.4.1 Relevance of the research

The research can be seen as relevant for the enterprise architects and contributes to 'science', 'society' and 'business'. The upcoming paragraphs will discuss why this study can be seen as relevant.

The research is relevant for science as it contributes to resolving the knowledge gap around Zero Trust Architecture Transformations. This resolution is achieved by performing a literature study to present the current knowledge, gathering empirical evidence from the field and developing design principles to transform a traditional EA into a ZTA.

The research can be seen as relevant for society as it makes it manageable to implement ZT elements resulting in improved protection of intellectual property and personal data as verification becomes key.

The research can contribute to a robust cybersecurity strategy for organizations as one of the benefits of Zero Trust is minimizing the blast radius when an external or insider breach occurs. This protection is essential since cybersecurity has become a fixed topic on the agenda of board meetings as the number of data breaches in the Netherlands has increased in 2020 by 30%* according to AP (Autoriteit Persoonsgegeven, 2021).

Moreover, the study is relevant for business as it creates reference architectures that can be used for guidance during a ZTA transformation. The architecture can be extended and changed according to the organization's wishes and needs since each organization is different and faces dissimilar challenges.

8.4.2 Link with CoSEM

The analyses and architecture design of large-scale information structures will ensure a solid link is made with the Complex Systems Engineering and Management (CoSEM) MSc programme. The acquired knowledge of the information and communication track is put into practice. In addition, the research is relevant for science since multiple designs are made of reference architectures to show the current and future state of an EA. These designs present the technology components that need to be in place in enterprise architectures. Moreover, the technical issues which arise when transforming the IT infrastructure will be addressed. Elaboration is done both on process management strategies and system engineering approaches.

Another reason this research has a solid link to CoSEM is the strong socio-technical nature of the transformation to a ZTA. Additionally, while designing or transforming an enterprise architecture, it is necessary to consider the interests, cultures, and human behaviour as well as any current laws, subsidies, distribution channels, and infrastructures. These factors need to be considered and utilised in a Zero Trust architecture transformation as ZT is more than a solid architecture.

The setting of the study is a multi-actor environment. Numerous parties are involved in the design and transformation of architecture. Although an enterprise frequently hires architects, other actors apart from the client are involved in the decision-making. The policy creators are a good example. The laws and regulations created by the Dutch government and the European Union (EU) must be followed carefully.

Moreover, these governmental institutions scrutinize various organizations for public purposes to ensure data is stored and processed correctly. Besides these institutions, third-party service providers supporting the operation with applications or hardware should also be considered as longstanding agreements cannot simply be broken. So, during the investigation, technical challenges will be encountered, and management and ethical choices will be made.

8.4.3 Reflection on the process

Overall, reflecting on the choices made, the research outcome is in line with the objective.

However, finding the proper scientific methodologies was not always easy. At the start, the idea was to execute a case study to gather more empirical evidence since the phenomenon is still novel. Eventually, a case study was not chosen because the available cases were limited, and the chance of succeeding in the research would have been minimal.

It is believed that the multivocal literature review and the semi-structured interviews were the most appropriate methods to discover this field. Although, defining a more precise scope, in the beginning could have been helpful to stay on track instead of going up in details.

During the first month, many articles and whitepapers were read without generating much output. Due to the different wording used to describe ZTA's, it took some time to get to know the topic. However, the conversations with the cyber security experts helped to get a better understanding of this topic.

Reaching out to the interviewees via LinkedIn was something pleasant to do. Although half of the people did not respond to the invites, there were still 18 people who replied with enthusiasm and wanted to contribute to the research. The processing of the interviews took more time than expected as most of the interviews were 60 min instead of 45 min. Furthermore, finding the right approach to code, the interviews was challenging. The handbook of Saldaña (2014) and the article by Weston (2011) helped with coding the interviews.

The development of design principles took more time than expected. Multiple iterations with different experts were needed to come to a solid deck. In the end, this iterative process led to reliable research.

Although the invites were shared on time, the number of experts participating in the study was lower than expected. It was hard to convince the architects to take part in the workshop. Most of them had senior roles, and their mail and agendas were managed by executive assistants, making it harder to connect. In total, 53 people contributed to the research (25 interviews, 2 workshops and 1 survey) consisting of:

- 7 cyber security experts
- 3 project leads
- 3 scientists
- 5 advisors
- 7 vendors
- 11 architects 'Chief Architect Community'
- 17 architects 'Digital Architects NetWork'

In the end, the research activities that were enjoyed the most were conducting the interviews, speaking to different stakeholders with various perspectives and elucidating this novel topic. It was great that both theoretical and practical organisations were involved in this study, resulting in valuable insights on establishing a ZTA. Hopefully, in the future, more research will be done, and the outcome of this research will be used by companies worldwide and contribute to the development of a ZTA in the near future.

References

Scientific Resources

Adams, R. J., Smart, P., & Huff, A. S. (2017). Shades of grey: guidelines for working with the grey literature in systematic reviews for management and organizational studies. International Journal of Management Reviews, 19(4), 432-454.

Ali, R. (2021). Looking to the future of the cyber security landscape. *Network Security*, 2021(3). https://doi.org/10.1016/S1353-4858(21)00029-5

Armour, F. J., & Kaisler, S. H. (2001). Enterprise architecture: Agile transition and implementation. IT Professional Magazine, 3(6), 30.

Banaeianjahromi, N, Smolander, K. What do we know about the role of enterprise architecture in enterprise integration? A systematic mapping study. *J Enter Inf Manage* 2016; 29: 140–164.

Bertino, E. (2021). Zero Trust Architecture: Does It Help?. IEEE Security & Privacy, 19(05), 95-96.

Bharosa, N., & Janssen, M. (2015). Principle-based design: a methodology and principles for capitalizing design experiences for information quality assurance. *Journal of Homeland Security and Emergency Management*, 12(3), 469-496.

Borrego, M., Douglas, E. P., & Amelink, C. T. (2009). Quantitative, qualitative, and mixed research methods in engineering education. *Journal of Engineering education*, *98*(1), 53-66.

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. Part I: The causes. *MIS quarterly*, 17-32.

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *Journal of systems and software, 80*(4), 571-583.

Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers and Security, 110.* https://doi.org/10.1016/j.cose.2021.102436 .

Campbell, M. (2020). Beyond Zero Trust: trust is a vulnerability. *Computer, 53(10)*, 110-113.

Campbell, S. (2014). What is qualitative research?. *Clinical Laboratory Science, 27(1), 3*.

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. The qualitative report, 21(5), 811-831.

Creswell, J. W., & Tashakkori, A. (2007). Differing perspectives on mixed methods research. *Journal of mixed methods research, 1(4)*, 303-308.

Cunningham C, Pollard J. (2017). The Eight Business and Security Benefits of Zero Trust. Forrester Research; 2017. Available: https://www.forrester.com/report/The+Eight+Business+And+Security+Benefits+Of+Zero+Trust/-/E-RES134863 [Accessed 03 04 2022]

Cunningham C., "The Zero Trust eXtended (ZTX) Ecosystem," Forrester, 2018.

DISA, “Zero Trust Reference Architecture” (2021) [Online], Available: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf . [Accessed 2022]

D'Silva D. and Ambawade D. D., "Building A Zero Trust Architecture Using Kubernetes," 2021 6th International Conference for Convergence in Technology (I2CT), 2021, pp. 1-8, doi: 10.1109/I2CT51068.2021.9418203.

Embrey, B. (2020). The top three factors driving Zero Trust adoption. Computer Fraud & Security, 2020(9), 13-15.

Flores, D. A., Qazi, F., & Jhumka, A. (2016, August). Bring your own disclosure: analysing BYOD threats to corporate information. In 2016 IEEE Trustcom/BigDataSE/ISPA (pp. 1008-1015). IEEE.

Garousi, V., Felderer, M., & Mäntylä, M. V. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. Information and Software Technology, 106, 101-121.

Gates, S. 2002. "Review of Methodology of Quantitative Reviews Using Meta-analysis in Ecology." Journal of Animal Ecology 71 (4): 547–57.

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups. British dental journal, 204(6), 291-295.

Gong, Y., & Janssen, M. (2019). The value of and myths about enterprise architecture. International Journal of Information Management, 46. https://doi.org/10.1016/j.ijinfomgt.2018.11.006

Greefhorst, D., & Proper, E. (2011). Architecture principles: the cornerstones of enterprise architecture.

Haddon, D., & Bennett, P. (2021). The Emergence of Post Covid-19 Zero Trust Security Architectures. In Advanced Sciences and Technologies for Security Applications. https://doi.org/10.1007/978-3-030-72120-6_13

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS quarterly, 75-105.

Hevner, A. R. (2007). A three cycle view of design science research. Scandinavian journal of information systems, 19(2), 4.

Hoogervorst, J. (2004). Enterprise architecture: Enabling integration, agility and change. International Journal of Cooperative Information Systems, 13(3). https://doi.org/10.1142/S021884300400095X

Janssen, M, Klievink, B, Chun, SA. Can enterprise architectures reduce failure in development projects? Transforming Government: People, Process and Policy 2012; 6(1): 27–40.

Jericho Forum, (2005) "Visioning White Paper" Available: https://collaboration.opengroup.org/jericho/vision_wp.pdf [Accessed 04 03 2021]

Jericho Forum, (2007) "Commandments" Available: https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf [Accessed 04 03 2021]

Johannesson, P., & Perjons, E. (2014). An introduction to design science (Vol. 10, pp. 978-3). Cham: Springer.

Kane, G. C., Palmer, D., Phillips, A. N., Kiron, D., & Buckley, N. (2015). Strategy, not technology, drives digital transformation. MIT Sloan Management Review and Deloitte University Press, 14(1-25).

Kern, A., & Anderl, R. (2018). Using RBAC to enforce the principle of least privilege in industrial remote maintenance sessions. 2018 5th International Conference on Internet of Things: Systems, Management and Security, IoTSMS 2018. https://doi.org/10.1109/IoTSMS.2018.8554805

Korhonen, J. J., & Halen, M. (2017). Enterprise architecture for digital transformation. Proceedings - 2017 IEEE 19th Conference on Business Informatics, CBI 2017, 1. https://doi.org/10.1109/CBI.2017.45

Kindervag J. (2010), "Build Security Into Your Network's DNA: The Zero Trust Network Architecture," Forrester Research.

Kindervag J. (2010), "No More Chewy Centers: Introducing the Zero Trust Model of Information Security," Forrester Research.

Kitchenham, B. (2004). Procedures for performing systematic reviews. Keele, UK, Keele University, 33(2004), 1-26.

Langenberg, K., & Wegmann, A. (2004). Enterprise architecture: What aspects is current research targeting.

Levy, A. (1986). Second-order planned change: Definition and conceptualization. Organizational dynamics, 15(1), 5-23.

Marsh, S. P. (1994). Formalising trust as a computational concept (Doctoral dissertation, University of Stirling).

Moubayed, A., Refaey, A., & Shami, A. (2019). Software-defined perimeter (sdp): State of the art secure solution for modern networks. IEEE network, 33(5), 226-233.

Niemi, E., & Pekkola, S. (2020). The Benefits of Enterprise Architecture in Organizational Transformation. *Business and Information Systems Engineering*, *62*(6). https://doi.org/10.1007/s12599-019-00605-3

Patton, M. Q. (2005). Qualitative research. Encyclopedia of statistics in behavioral science.

Proper, E., & Greefhorst, D. (2010, November). The roles of principles in enterprise architecture. In International Workshop on Trends in Enterprise Architecture Research (pp. 57-70). Springer, Berlin, Heidelberg.

Rabionet, S. E. (2011). How I learned to design and conduct semi-structured interviews: an ongoing and continuous journey. Qualitative Report, 16(2), 563-566.

Ramezanpour, K., & Jagannath, J. (2021). Intelligent Zero Trust architecture for 5g/6g tactical networks: Principles, challenges, and the role of machine learning. arXiv preprint arXiv:2105.01478.

Rose S., O. Borchert, Mitchell S. and Connelly S. (2020), NIST Special Publication 800-207: Zero Trust Architecture, Washington, DC: NIST.

Rozanski, N., & Woods, E. (2012). Software systems architecture: working with stakeholders using viewpoints and perspectives. Addison-Wesley.

Ritchie, J., & Spencer, L. (2002). Qualitative data analysis for applied policy research. The qualitative researcher's companion, 573(2002), 305-29.

Saldaña, J. (2014). Coding and analysis strategies. *The Oxford handbook of qualitative research*, 581-605.

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. Journal of Information System Security, 10(3).

Seepers, R. M., Smulders, A. C. M., & Meeuwissen, H. B. (2020). Zero Trust-architectuur op basis van implied trust-zones. *Informatiebeveiliging*, (1), 20.]

Sheridan, O. (2021). The state of Zero Trust in the age of fluid working. Network Security, 2021(2), 15-17.

Shore, M., Zeadally, S., & Keshariya, A. (2021). Zero Trust: The What, How, Why, and When. Computer, 54(11), 26-35.

Strauss, A., & Corbin, J. (1994). Grounded theory methodology: An overview. In N. K. Denzin & Y. S. Lincoln (Eds.), Handbook of qualitative research (pp. 273–285). Sage Publications, Inc.

Silver, C., & Lewins, A. (2014). Using software in qualitative research: A step-by-step guide. Sage.

Simmonds, M. (2017). How businesses can navigate the growing tide of ransomware attacks. Computer Fraud & Security, 2017(3), 9-12.

Simon, H., The Sciences of Artificial, 3rd Edition, MIT Press, Cambridge, MA, 1996.

Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to Zero Trust architecture: reviews and challenges. Security and Communication Networks, 2021.

Trautman, L. J., & Ormerod, P. C. (2018). Wannacry, ransomware, and the emerging threat to corporations. Tenn. L. Rev., 86, 503.

Tyler, D., & Viana, T. (2021). Trust no one? A framework for assisting healthcare organizations in transitioning to a zero-trust network architecture. Applied Sciences (Switzerland), 11(16). https://doi.org/10.3390/app11167499

Uttecht, K. D. (2020). *Zero Trust (ZT) concepts for federal government architectures*. MASSACHUSETTS INST OF TECH LEXINGTON.

Van Der Raadt, B., Schouten, S., & Van Vliet, H. (2008). Stakeholder perception of enterprise architecture. Software architecture, 19-34.

Ward R. and Beyer B. (2014), "BeyondCorp: A New Approach to Enterprise Security," ;login:, vol. 39, no. 6, pp. 6-11.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. MIS quarterly, xiii-xxiii.

Weston, C., Gandell, T., Beauchamp, J., McAlpine, L., Wiseman, C., & Beauchamp, C. (2001). Analyzing interview data: The development and evolution of a coding system. Qualitative sociology, 24(3), 381-400.

Whyte W. F. (1990), Participatory Action Research SAGE Publications

Wieringa, R. J. (2014). Design science methodology for information systems and software engineering. Springer.

Winter, R., & Schelp, J. (2008). Enterprise architecture governance: the need for a business-to-IT approach. In Proceedings of the 2008 ACM symposium on Applied computing (pp. 548-552).

Wu, H., Yu, Z., Huang, D., Zhang, H., & Han, W. (2020). Automated enforcement of the principle of least privilege over data source access. *Proceedings - 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020*. https://doi.org/10.1109/TrustCom50675.2020.00075

Yao, Q., Wang, Q., Zhang, X., & Fei, J. (2020). Dynamic access control and authorization system based on zero-trust architecture. In 2020 International Conference on Control, Robotics and Intelligent System (pp. 123-127).

Zimmermann, A., Schmidt, R., Sandkuhl, K., Jugel, D., Bogner, J., & Möhring, M. (2018). Evolution of Enterprise Architecture for Digital Transformation. *Proceedings - IEEE International Enterprise Distributed Object Computing Workshop, EDOCW*, *2018-October*. https://doi.org/10.1109/EDOCW.2018.00023

Zimmermann, A., Schmidt, R., Sandkuhl, K., Wißotzki, M., Jugel, D., & Möhring, M. (2015). Digital enterprise architecture-transformation for the internet of things. *Proceedings of the 2015 IEEE 19th International Enterprise Distributed Object Computing Conference Workshops and Demonstrations, EDOCW 2015*. https://doi.org/10.1109/EDOCW.2015.16

Non - Scientific Resources

Autoriteit Persoonsgegevens. (2021). Rapportages klachten en datalekken. Available: https://www.autoriteitpersoonsgegevens.nl/nl/publicaties/rapportages-klachten-en-datalekken [Accessed 03 02 2022].

CISA (2020). Zero Trust Maturity Model. Available: https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf [Accessed 05 03 2022].

Cser, A. (2018). What is a Zero Trust Architecture. Palo Alto Networks. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture [Accessed 19 02 2022].

CSA (2020). Software Defined Perimeter (SDP) and Zero Trust. Available: https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-and-zero-trust/ [Accessed 05 03 2022].

Deloitte (2021). Zero Trust: A revolutionary approach to Cyber or just another buzz word? Available: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/deloitte-cyber-zero-trust.pdf [Accessed 27 11 2021].

DIB (2019). The Road to Zero Trust (Security). Available: https://media.defense.gov/2019/Jul/09/2002155219/-1/-1/0/DIB_THE_ROAD_TO_ZERO_TRUST_(SECURITY)_07.08.2019.PDF [Accessed 05 03 2022].

DISA & NSA (2021) Department of Defense (DOD) Zero Trust Reference Architecture. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf [Accessed 05 03 2022].

Dudley, R., & Golden, D. (2021). The colonial pipeline ransomware hackers had a secret weapon: self-promoting cybersecurity firms. Available: https://energyrights.info/sites/default/files/artifacts/media/pdf/the_colonial_pipeline_ransomware_hackers_had_a_secret_weapon_self-promoting_cybersecurity_firms_-_propublica.pdf

Ellis A., "Dark Reading," (2019). [Online]. Available: https://www.darkreading.com/threat-intelligence/9-years-after-from-operation-aurora-to-zerotrust/a/d-id/1333901. [Accessed 03 04 2022].

Forrester (2010) Build Security Into Your Network's DNA: The Zero Trust Network Architecture. Available: https://www.forrester.com/report/build-security-into-your-networks-dna-the-zero-trust-network-architecture/RES57047 [Accessed 05 03 2022].

Forrester (2016) No More Chewy Centers: The Zero Trust Model Of Information Security. Available: https://www.forrester.com/report/No-More-Chewy-Centers-The-Zero-Trust-Model-Of-Information-Security/RES56682 [Accessed 05 03 2022].

Garbis J., Koilpollai (2019) J. Software Defined Perimeter Architecture Guide, Cloud Security Alliance https://cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2/ [Accessed 22 03 2022]

Gartner, (2019) “Gartner Top 10 Strategic Technology Trends for 2020” available https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2020 [Accessed 26 03 2022]

Gigamon, (2020) “The IT and Security Landscape for 2020 and Beyond and the Role of Zero Trust” available: https://www.gigamon.com/resources/resource-library/analyst-industry-reports/ar-zerotrust-surveyreport.html [Accessed 26 03 2022]

Google (2014), "BeyondCorp: A new approach to cloud-native security". [Online]. Available: https://storage.googleapis.com/pub-tools-public-publication-data/pdf/43231.pdf. [Accessed 05 03 2022].

Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history. Wired, August, 22. Available: https://qualityplusconsulting.com/BBytes/2018-8-22_NotPetya-TheMost%20DevastatingCyberattackInHistory.pdf

GSA (2021) Zero Trust Architecture Buyer’s guide. Available: https://www.gsa.gov/cdnstatic/Zero%20Trust%20Architecture%20Buyers%20Guide%20v11%20202106 10%20(2).pdf [Accessed 05 03 2022].

IB Magazine (2020) Zero Trust-architectuur op basis van implied trust-zones. Available: https://www.pvib.nl/actueel/ib-magazines/ib-magazine-2020-1/downloaden [Accessed 05 03 2022].

IBM, (2021) “Cost of a Data Breach Report 2021” available: https://www.ibm.com/security/data-breach [Accessed 10 02 2022]

IBM, (2022) “Remote Work Makes it More Important Than Ever to Trust Zero Trust” available: https://securityintelligence.com/articles/remote-work-zero-trust/ [accessed 16 05 2022]

ISACA. (2021, October 13). Zero Trust by the founder John Kindervag, Zero Trust How it is meant to be. ISACA Netherlands Chapter. Retrieved 12 May 2022, from https://isaca.nl/events/zero-trust-by-the-founder-john-kindervag-zero-trust-how-it-is-meant-to-be/

Jericho Forum (2005) Visioning White Paper What is Jericho Forum? available: https://collaboration.opengroup.org/jericho/vision_wp.pdf [Accessed 05 03 2022].

KPN. (2021, 19 Januari). Werken in 2021: hoe gaat dat eruit zien? KPN.com. Geraadpleegd op 15 november 2021, van https://www.kpn.com/zakelijk/blog/werken-in-2021-hoe-gaat-dat-eruit-zien.html

Küderli U., Neher L., Faistauer F. (2020) “Zero Trust architecture: a paradigm shift in cybersecurity and privacy” Pricewaterhouse Coopers Available: https://www.pwc.ch/en/publications/2020/ch-zero-trust-whitepaper-final.pdf

Lohrmann, D. (2021, 10 October). Data Breach Numbers, Costs and Impacts All Rise in 2021. GovTech. Geraadpleegd op 21 november 2021, van https://www.govtech.com/blogs/lohrmann-on-cybersecurity/data-breach-numbers-costs-and-impacts-all-rise-in-2021

Meijer, E. (2021, 31 december). Security in 2022: cybercriminaliteit professionaliseert verder. AG Connect. Geraadpleegd op 30 mei 2022, van https://www.agconnect.nl/artikel/security-2022-cybercriminaliteit-professionaliseert-verder

Microsoft. (2021). Microsoft Zero Trust Guidance Center. Microsoft Docs. Available: https://docs.microsoft.com/en-us/security/zero-trust/ [accessed 16 03 2022]

Mitre (2022). MITRE ATT&CK®. Retrieved 22 May 2022, Available https://attack.mitre.org/

NSA (2021). Embracing a Zero Trust Security Model. Available: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF [accessed 07 03 2022]

OMB (2022). Moving the US Government toward Zero Trust cybersecurity principles. Available: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

ON2IT Inc. (2022, June 3). Zero Trust. ON2IT. Retrieved 1 July 2022, from https://on2it.net/zero-trust/

OpenGroup (2018, 18 April), TOGAF® Standard, Version 9.2, a standard of The Open Group, Available: https://pubs.opengroup.org/architecture/togaf9-doc/arch/index.html [Accessed 28 - 04 2022]

Oracle (2021). Approaching Zero Trust Security with Oracle Cloud Infrastructure. Available: https://www.oracle.com/a/ocom/docs/whitepaper-zero-trust-security-oci.pdf [accessed 07 03 2022]

PricewaterhouseCoopers (2020) Zero Trust Architecture: a paradigm shift in cybersecurity and privacy https://www.pwc.com/sg/en/publications/assets/page/zero-trust-architecture.pdf [accessed 07 03 2022]

Rosencrance, L. (2021, 20 April). principle of least privilege (POLP). SearchSecurity. Geraadpleegd op 28 november 2021, van https://searchsecurity.techtarget.com/definition/principle-of-least-privilege-POLP

Van Rooij, B. J., & Scholtes, P. (2021, 14 oktober). Hoe groot is de financiële schade? En zeven andere vragen over de cyberaanval bij VDL. AD.nl. Geraadpleegd op 25 november 2021, van https://www.ad.nl/economie/hoe-groot-is-de-financiele-schade-en-zeven-andere-vragen-over-de-cyberaanval-bij-vdl~a4e8ec99/

van Wijnen, J. F. (2021, December 13). Banken en overheden schakelen software uit voorzorg uit. Financieel Dagblad. Retrieved 22 March 2022, from https://fd.nl/tech-en-innovatie/1423222/banken-en-overheden-zetten-software-af-uit-angst-voor-hacks

Appendix

Appendix A: Understanding of Traditional and ZT EA

Table 24: EA Definitions

Organization	Traditional EA	Zero Trust EA	Source
IBM	On-premises infrastructure	1) Logs and inspects all corporate network traffic 2) Limits and controls access to the network 3) Verifies and secures network resources.	Taken from IBM (2021) [retrieved on: 22/04/2022] Zero Trust available: https://www.ibm.com/topics/zero-trust
Microsoft	Assuming everything behind the corporate firewall is safe	The Zero Trust model assumes breach and verifies each request as though it originates from an open network. Regardless of where the request originates or what resource it accesses, Zero Trust teaches us to "never trust, always verify." https://www.microsoft.com/en/security/business/zero-trust	Taken from Microsoft (2021) [retrieved on: 22/04/2022] Zero Trust Model - Modern Security Architecture available: https://www.microsoft.com/en-us/security/business/zero-trust
Oracle	The traditional castle-and-moat security model - where anything and everything inside the firewall was automatically trusted	Lowering trust levels of the network and considering how to design security principles and deploy appropriate security controls, based on the assumption that the network is compromised and cannot be trusted.	Taken from Oracle (2022) [retrieved on: 22/04/2022] Approaching zero trust available: https://blogs.oracle.com/cloudsecurity/post/approaching-zero-trust-security-with-oci
Deloitte	-	A Zero Trust strategy for cybersecurity provides the opportunity to create a more robust and resilient security, simplify security management, improve end-user experience, and enable modern IT practices.	Taken from Deloitte (2021) [retrieved on: 22/04/2022] Zero Trust strategy insights available: https://www2.deloitte.com/us/en/pages/advisory/articles/zero-trust-strategy-insights.html
Accenture	If you are on a trusted corporate network (physically connected in an office or remotely via VPN), you should be trusted to access any application, server or other infrastructure.	It enables access decisions based on the context of the transaction, including factors such as the identity of the user, classification of data being accessed, the security profile of the device, the network, the application, and the authenticators used.	Taken from Accenture (2021) [retrieved on: 22/04/2022] Zero Trust Security Architecture available: https://www.accenture.com/us-en/blogs/security/zero-trust-security

Forrester	-	Zero Trust is an information security model that denies access to applications and data by default. Threat prevention is achieved by only granting access to networks and workloads utilizing policy informed by continuous, contextual, risk-based verification across users and their associated devices. Zero Trust advocates these three core principles: all entities are untrusted by default, least privilege access is enforced, and comprehensive security monitoring is implemented.	Taken from Forrester (2021) [retrieved on: 22/04/2022] the definition of modern zero trust available: https://www.forrester.com/blogs/the-definition-of-modern-zero-trust/

Appendix B: Adversaries

Table 25: Overview of adversaries

TACTIC	POSSIBLE TECHNIQUE	DESCRIPTION	ZT ELEMENT
RECONNAISSANCE	Active Scanning	Information gathering is used for planning future operations.	Encryption, segmented infrastructure
RESOURCE DEVELOPMENT	Compromise accounts/system	Establishing resources that can be used to support operations.	Just Enough Access (JEA)
INITIAL ACCESS	Phishing	Getting into your network.	Policy Enforcement Point / Trust Zones
EXECUTION	OS Shell	Running malicious code.	CDM System
PERSISTENCE	Account Manipulation	Maintaining their foothold.	Enhanced Identity
PRIVILEGE ESCALATION	Elevation control	Gaining higher-level permissions.	Deny-all gateway (SDP)
DEFENSE EVASION	Hiding artefacts	Avoid being detected.	Activity logging or continuous monitoring
CREDENTIAL ACCESS	AiTM, Brute Force	Stealing account names and passwords.	Biometrics / MFA
DISCOVERY	Listing	Figuring out your environment.	Deny-all gateway (SDP)
LATERAL MOVEMENT	Exploitation of remote services	Moving through your environment.	Just Enough Access (JEA)
COLLECTION	Adversary in the middle	Gathering data of interest to their goal.	Tokenization, disk encryption
COMMAND AND CONTROL	Data obfuscation	Communicating with compromised systems to control them.	Digital certificates
EXFILTRATION	Automated exfiltration	Stealing data.	Auto remediation
IMPACT	Ransomware	Manipulating, interrupting, or destroying systems and data.	Just Enough Access (JEA)

Appendix C: Multivocal Literature Review

In this section a description will be provided how the Multivocal Literature Review (MLR), presented in figure 26 is performed.

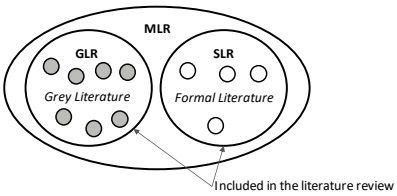


Figure 25: Venn diagram

C1. Planning the review

STEP 1 | Formulate the problem

The research question that should be answered with the MLR is *"What types of Zero Trust architectures exist?"* with the goal to identify blueprints or reference architectures in which Zero Trust is applied.

STEP 2 | Develop and Validate Protocol

During this step a pre-set plan is created that specifies the methods that are used in conducting the review. (Gates, 2002). In table 24, the protocol is presented what is used for the systematic literature review.

Table 26: SLR protocol

SLR Protocol	
Research question	*What types of Zero Trust architectures exist?*
Summary of study	The idea of the study is to find designs, components and capabilities of Zero Trust which can be used to construct reference architectures (architypes)
Search Strings / Syntax	Zero AND Trust AND {"Enterprise" OR "Organization"} Architecture AND {"Type" OR "Design" OR "Blueprint"} Zero AND Trust AND Architecture
Inclusion criteria	- Studies published between January 2002 and January 2022 - Studies published in Formal literature - Studies published in Grey literature
Exclusion criteria	- Exclude studies that do not offer models or architectural designs - Zero Trust Architecture is not in the title of the article - Eliminate studies based on quality evaluations
Study quality assessment	The quality is accessed by looking at the journal in which the article is published. Additionally, the publisher of the white paper is checked.
Data extraction procedure	With the use of a matrix, the elements that define a Zero Trust architecture will be mapped.
Data synthesis procedure	Frameworks and capabilities will be gathered from the studies to create an overview of the components that are used most frequently
Record keeping	The records found will be separately stored. One table will consist of all the formal literature, and the other table will consist of the white papers
Project timetable	Literature will be gathered between the 2nd and 8th of march 2022

The protocol is validated by two individuals who are professionals in the field of Enterprise Architecture to increase the rigor of the study.

C2. Conducting the review

This stage consists of five steps in which the SLR is actually performed
Step 3 | Search the literature: During this step, the literature will be collected. As the quality of the review is dependent on the collected works, a critical eye is needed.
Step 4 | Screen for Inclusion: The list of references found will be screened. This will be done by checking the title and the abstract of the articles and the white papers.
Step 5 | Assess Quality: The text of the articles will be analysed, and based on reasonable and defendable criteria, articles can be excluded from the study. For the grey literature the AACODS criteria will be used.
Step 6 | Extracting data: There are multiple methods that can be used for the extraction of data, such as meta-ethnography, thematic synthesis and deductive or inductive coding. During the research, inductive coding will be used to extract data from the articles.
Step 7 | Analysing and Synthesizing Data: After the data is extracted, it should be organised in a structured way. This can be done with charts, tables or textural descriptions. For this study, matrixes will be constructed to create an overview of the Zero Trust capabilities that can be found in the literature.

Summary of 3 – 7
In figure 26, the flow diagram is presented visualising the steps taken in the literature search and evaluation.

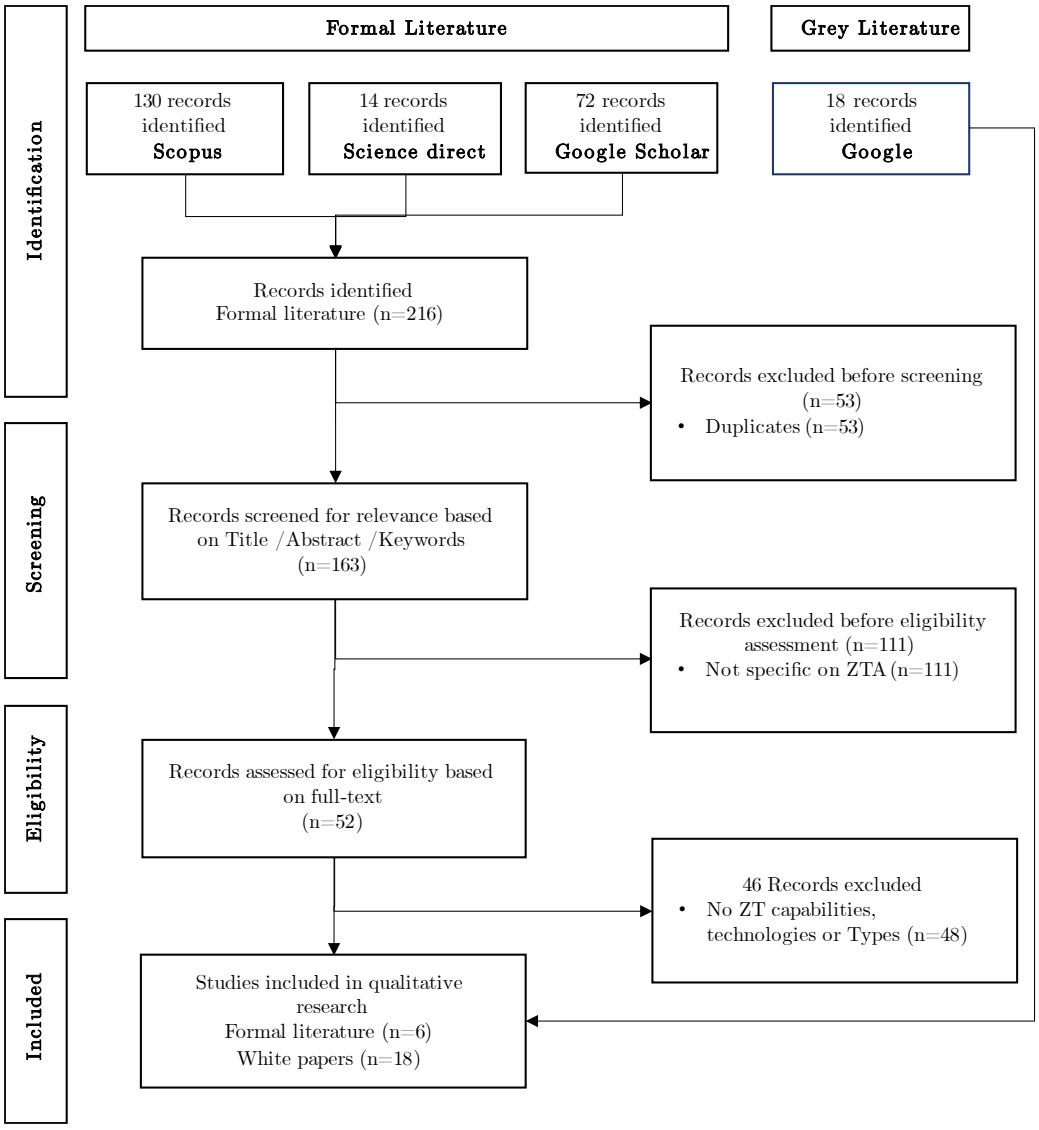


Figure 26: Multivocal Literature Review

C3. Reporting the Review

Formal Literature (FL)

This stage consists of one final, and most important step as the MLR should be reliable and independently repeatable by the reader. Moreover, the matrixes will be used for the presentation of the elements that are found in the literature. A presentation of the formal literature can be found in table 27.

Table 27: Formal Literature

ID	REFERENCE	TITLE	MOTIVATION
FL1	(Campbell, 2020)	Beyond Zero Trust: Trust is a Vulnerability	Enter, Doing and Beyond Zero Trust
FL2	(D'Silva, 2021)	Building A Zero Trust Architecture Using Kubernetes	Zero Trust, Kubernetes, Access Control, Keycloak, Proxy.
FL3	(Rose, 2020)	SP 800 207 – Zero Trust Architecture	Architecture, Cybersecurity, Enterprise, Zero Trust
FL4	(Teerakanok, 2021)	Migrating to Zero Trust Architecture: Reviews and Challenges	Migration from a legacy architecture
FL5	(Uttecht, 2020)	Zero Trust (ZT) Concepts for federal government architectures	Dimensions and capabilities that makeup a ZT architecture
FL6	(Yao, 2020)	Dynamic Access Control and Authorization System based on Zero-trust architecture	Security and privacy; Security services; Access control

Note; the references used can give a wrong impression as the articles used are only recent publications. There are some papers published between 2010 – and 2020, but they are seen as less relevant as they are not mentioning models or architectural designs and ZT capabilities.

Grey Literature (GL)

As the amount of the formal literature is limited, grey literature (white papers / publications of IT businesses & consultancies) has been consulted. A presentation of these articles can be found in table 28.

Table 28: White papers

ID	REFERENCE	TITLE	MOTIVATION
GL1	(CISA, 2020)	Zero Trust Maturity Model	Path to Zero Trust transition
GL2	(CSA, 2020)	Software Defined Perimeter (SDP) and Zero Trust	Examples of SDP implementations
GL3	(Deloitte, 2021)	Zero Trust, A revolutionary approach to Cyber or just another buzz word?	Breakdown of Zero Trust
GL4	(DIB, 2019)	The Road to Zero Trust Security	Independent advice to secretary of defence
GL5	(DISA & NSA, 2021)	Department of Defence Zero Trust Reference Architecture	ZT purpose, principles, positions and patterns
GL6	(Forrester, 2010)	Build security into your network's DNA: The Zero Trust network architecture	Potentials of the Zero Trust model
GL7	(Forrester, 2016)	No more chewy centres: Introducing the Zero Trust model of information security	Vision and key concepts of Zero Trust
GL8	(Gartner, 2019)	Zero Trust Architecture and Solutions	View on Zero Trust
GL9	(Google, 2014)	BeyondCorp, A new approach to Enterprise Security	Zero Trust build into real product
GL10	(GSA, 2021)	Zero Trust Architecture Buyer's guide	Solutions for a Zero Trust journey
GL11	(IB Magazine, 2020)	Zero Trust-architectuur op basis van implied trust-zones	Discussion of one of the crucial ZT capabilities
GL12	(Jericho Forum, 2005)	What is Jericho Forum?	Starting point of perimeter-less EA
GL13	(OMB, 2022)	Moving the US Government toward Zero Trust cybersecurity principles	Concrete actions to transform to a ZTA
GL14	(Microsoft, 2021)	Evolving Zero Trust, How real-world deployments and attacks are shaping the future of Zero Trust strategies	Viewpoint of Zero Trust and learnings clients
GL15	(MITRE, 2021)	Zero Trust Architectures, Are we there yet?	Benefits to organizations
GL16	(NSA, 2021)	Embracing a Zero Trust security model	Explanation and advice on the use of a ZT model
GL17	(Oracle, 2021)	Approaching Zero Trust Security with Oracle Cloud Infrastructure	ZT application on Cloud infrastructure
GL18	(PWC, 2020)	Zero Trust Architecture: a paradigm shift in cybersecurity and privacy	Integration of security architecture into EA

Formal literature

These basics are presented in table 29 and table 30.

Table 29: ZT types in formal literature

Reference	Elements defining Zero Trust Architectures		
	System Components	*Core Capabilities*	*EA Designs*
(Campbell, 2020)	x		
(D'Silva, 2021)	x	x	
(Rose, 2020)	x	x	
(Teerakanok & Inomata, 2021)	x		
(Uttecht, 2020)	x	x	x
(Yao, 2020)	x	x	

White Papers (WP)

Table 30: ZTA in white papers

Reference	Elements defining Zero Trust Architectures		
	System Components	*Core Capabilities*	*EA Designs*
(CISA, 2020)	X	X	
(CSA, 2020)	X	X	X
(Deloitte, 2021)	X	X	X
(DIB, 2019)		X	
(DISA & NSA, 2021)	X	X	X
(Gartner, 2019)	X	X	X
(Google, 2014)		X	X
(GSA, 2021)	X	X	
(IB Magazine, 2020)			X
(Jericho Forum, 2005)		X	
(Forrester, 2010)	X		X
(Forrester, 2016)			
(OMB, 2022)	X	X	
(Microsoft, 2021)	X	X	X
(MITRE, 2021)		X	X
(NSA, 2021)	x		
(Oracle, 2021)	X	X	
(PWC, 2020)	X		

This overview, table 31 gives an idea of the key capabilities when creating a Zero Trust EA.

Table 31: Overview of capabilities

Source	Formal Literature (FL)						Grey Literature (GL)															
Capabilities	(Campbell, 2020)	(D' Silva, 2021)	(Rose, 2020)	(Teerakanok, 2021)	(Uttecht, 2020)	(Yao, 2020)	(CISA, 2020)	(CSA, 2020)	(Deloitte, 2021)	(DIB, 2019)	(DISA & NSA, 2021)	(Forrester, 2010)	(Forrester, 2016)	(Gartner, 2019)	(Google, 2014)	(GSA, 2021)	(IB Magazine, 2020)	(Jericho Forum, 2005)	(OMB, 2022)	(Microsoft, 2021)	(MITRE, 2021)	(NSA, 2021)	(Oracle, 2021)	(PWC, 2020)
Authentication		x	x	x	x		x	x	x	x	x		x	x	x	x		x	x	x		x	x	x
Authorisation		x	x	x	x	X	x	x		x	x		x	x	x	x			x	x		x	x	
Auto Remediation																								
Activity logging		x	x	x			x	x			x		x	x					x				x	
Attribute Based access control			x		x		x	x		x	x	x	x	x		x	x	x	x	x		x	x	
Compliance monitoring			x	x	x	X	x	x	x	x	x	x	x	x		x	x		x	x			X	x
Context based signal filtering			x				x				x									X				
Data Classification																								
Encryption		x			x		x	x	x	x	x	x		x	x	x		x	x	x		x	x	x
Identification		x	x					x		x	x			x	x	x		x	x					x
Inventory management			x	x	x		x				x				x	x		x	x	x				x
Least privilege access	x		x	x	x	X	x	x		x	x	x	x	x		x		x	x	x		x	x	x
Micro segmentation	x		x		x		x	x	x	x	x	x	x	x		x			x	x		x	x	x
Multi Factor Authentication		x	x	x	x		x	x	x	x	x			x	x			x	x	x		x	x	x
Policy Based access control			x	x	x	X	x	x	x		x	x		x		x		x				x	x	x
Risk Assessment	x			x	x		x		x		x	x		x			x	x	x	x		x	x	x
Single Packet Authorisation (SPA)			x	x	x			x		x	x	x		x					x					
Threat intelligence	x		x	x	x			x	x	x	x	x	x			x	x			x			x	x

This overview, table 32 gives an idea of the key technologies when creating a Zero Trust EA.

Table 32: Overview of supporting technologies

Source	Formal Literature (FL)						Grey Literature (GL)																
Technologies	(Campbell, 2020)	(D' Silva, 2021)	(Rose, 2020)	(Teerakanok, 2021)	(Uttecht, 2020)	(Yao, 2020)	(CISA, 2020)	(CSA, 2020)	(Deloitte, 2021)	(DIB, 2019)	(DISA & NSA, 2021)	(Forrester, 2010)	(Forrester, 2016)	(Gartner, 2019)	(Google, 2014)	(GSA, 2021)	(IB Magazine, 2020)	(Jericho Forum, 2005)	(OMB, 2022)	(Microsoft, 2021)	(MITRE, 2021)	(NSA, 2021)	(Oracle, 2021)	(PWC, 2020)
Access Control Engine	x		x	x	x	X		x	x	x	x	x	x	x	x	x	x	x		x		x	x	x
Certificate Authority (CA)			x							x	X				x			x							
Cloud Access Security Broker (CASB)											x		x	x		x								X
CDM system			x		x	X	x	x								x			X					
Mutual TLS								x		x	x			x					x				x	
Policy Engine	x		x	x	x			x	x		x	x		x		x		x		x		x	x	x
Public Key Infrastructure			x					x		x	x		x	x				x						
Secure Access Service Egde (SASE)			x	x			x			x	x			x		x		x						
Secure Web Gateway (SWG)				x		X		x		x	x	x		x			x		x	x		x		
SDP Controller			x		x			x						x										
SIEM System			x	x	x			x			x			x		x	x			x		x	x	x
Single Sign-On (SSO) system				x		X							x	x	x					x			x	
Software Defined Perimeter (SDP)	x		x		x			x						x										x
SOAR	x							x			x								x					x
SSL						X		x		x	x							x					x	

Appendix D: Interviews Protocols

Semi-Structured Interview Protocol – **Consultant / ZT Expert**
Introduction [3 min]
General Information - Thanks for making time - Agenda for today - Goal of the research - Goal of the interview "product/process/results" Permission & Expectation management - Verify time expectations; "Is it correct that we will have 45 minutes to have this interview" - The interview is completely anonymous so no information can be traced down to the respondent
Main questions [±35 min]
Architypes [5 min] - Do you agree with the defined ZT architypes shared via email? o Are there types missing? If so, do you have blueprints you can share? - Which of the types/approaches are frequently used? **Challenges/success criteria [10 min]** - What are the biggest challenges when implementing a Zero Trust architecture? o Can you give examples of brownfield & greenfield projects? - Are the challenges industry-specific? o Can you give examples? - What are the critical success factors for transformation? o Can you give examples? - What are the commonly made mistakes during a transformation? o Can you give examples? o How can these pitfalls be prevented? - Are the key ZT capabilities different between the industries? o Can you give examples? **Constraints / Boundary conditions [5 min]** - What are the boundary conditions that frequently pop up during ZT implementations? o Can you give examples? **Socio-Technical System (STS) Elements [10 min]** - What are the common obstacles regarding the Social-technical system elements? o Structure (organization) o People (cognitive & social) o Physical system (hardware, software and facilities) o Task (work) **Roadmap [10 min] → MIRO** - What are the steps that should be taken during a ZT transformation? - Is there a specific order in which these actions need to be performed?
Ending [2 min]
Summarize the main conclusion of the interview outtakes Call for action; You could help me out with providing - Connecting to Colleagues / Experts Mention that the interviewee will hear from you when he/she is interested in receiving the final version of the report. Thank the person for his/her time

Semi-Structured Interview Protocol - **Architect**

Introduction [3 min]

General Information

- Thanks for making time
- Agenda for today
- Goal of the research
- Goal of the interview "product/process/results"

Permission & Expectation management

- Verify time expectations; "Is it correct that we will have 45 minutes to have this interview"
- The interview is completely anonymous so no information can be traced down to the respondent

Main questions [±35 min]

Architecture Capabilities [5 min]

- Are you familiar with the core capabilities of a Zero Trust Architecture?
    - Which of the listed capabilities are the most challenging to implement?

Challenges Architypes [20 min]

- What are the biggest challenges when creating Implied Trust Zones driven architecture?
    - Can you give examples of brownfield & greenfield projects?
    - Are the challenges industry-specific?
    - What are the critical success factors?
- What are the biggest challenges when creating an API driven / Microservices architecture?
    - Can you give examples of brownfield & greenfield projects?
    - Are the challenges industry-specific?
    - What are the critical success factors?
- What are the biggest challenges when creating a Software-Defined Perimeter (SDP) architecture?
    - Can you give examples of brownfield & greenfield projects?
    - Are the challenges industry-specific?
    - What are the critical success factors?
- What are the biggest challenges when creating a Trust Score driven architecture?
    - Can you give examples of brownfield & greenfield projects?
    - Are the challenges industry-specific?
    - What are the critical success factors?
- What are the biggest challenges when creating an Encryption driven architecture?
    - Can you give examples of brownfield & greenfield projects?
    - Are the challenges industry-specific?
    - What are the critical success factors?
- What are the biggest challenges when creating an AI/Behaviour driven architecture?
    - Can you give examples of brownfield & greenfield projects?
    - Are the challenges industry-specific?
    - What are the critical success factors?

EA Transformation [5 min]

- What are the commonly made mistakes during an EA transformation?
    - How can these pitfalls be prevented?

Socio-Technical System (STS) Elements [10 min]

- What are the obstacles regarding the Social-technical system elements during EA transformations?
    - Structure (organization)
    - People (cognitive & social)
    - Physical system (hardware, software and facilities)
    - Task (work)

Ending [2 min]

1.Summarize the main conclusion of the interview outtakes
2.Call for action; You could help me out with providing
- Connecting to Colleagues / Experts

3. Mention that the interviewee will hear from you when he/she is interested in receiving the final version of the report.
4. Thank the person for his/her time

Appendix E: Interview Analyses

Table 33: Applied codes

Code	Subcode	Code	Subcode	Code	Subcode
People	Culture	Technology	Legacy	Industry	Industrials
People	Drive	Technology	Configuration	Industry	Semiconductor
People	Knowledge	Technology	Compatibility	ZT Features	Encryption
Process	Decision-making	Technology	OT	ZT Features	Segmentation
Process	User experience	Rules & Regulations	Compliance	ZT Features	Identity
Process	Execution	Resources	Workforce	ZT Features	Automation
Process	Planning	Resources	Investment	ZT Tactics	Management
Process	Communication	Industry	Healthcare	ZT Tactics	Procurement

A= Advisors / P= Project lead / S= Scientist / V= Vendor

Tag	Category	Code	Type	Remark	A	P	S	V
PE01	People	Drive	Challenge	Employees don't want to take responsibility for technology implications			x	
PE02	People	Experience	Challenge	Employees feel they are being viewed as the insider threat			x	
PE03	People	Knowledge	Challenge	The recognition and the development of cybersecurity talents				x
PE04	People	Experience	Challenge	Cultural shift and Cultural acceptance	x			x
PE05	People	Knowledge	Limitation	Lack of awareness due to wrong ZT understanding				x
PE06	People	Skill	Limitation	People are not zero trust, okay. If you work together in organization, it naturally implies that you trust each other	x			
PE07	People	Decisionmaking	Limitation	To many stakeholders having political interest, people do not want to change				
PE08	People	Knowledge	Pitfall	Wrong understanding of Zero Trust	x		x	x
PE09	People	Experience	Pitfall	Security fatigue		x		
PE10	People	Decisionmaking	Pitfall	Security team making decisions in a locked room			x	
PE11	People	Decisionmaking	Pitfall	Postponing project due to organizational resistance				x
PE12	People	Experience	Pitfall	Employees seeking for loopholes to bypass measures		x		
PE13	People	Knowledge	Pitfall	Misconfigurations due to lack of skills				x
PE14	People	Knowledge	Pitfall	A missing sense of urgency				x
PE15	People	Knowledge	Pitfall	Lack of ZT expertise within the organisation		x		
PE16	People	Knowledge	Pitfall	People can make fack-ups when they are using default settings.		x		

PE17	People	Decisionmaking	Pitfall	Architect working from an ivory tower, to come up with a perfect new world, but didn't involve the stakeholders.	x			
PE18	People	Experience	Pitfall	Security is never top of mind and people always find ways around security measures	x			
PE19	People	Knowledge	Success Criteria	Understanding of Zero Trust	x			x
PE20	People	Drive	Success Criteria	Company commitment	x			
PE21	Process	Experience	Success Criteria	Regular communication about what & why you do it	x			
PE22	People	Drive	Success Criteria	Get buy in from C-level and IT-teams	x	x	x	x
PE23	People	Knowledge	Success Criteria	Evangelize the concept of zero trust to the users	x			
PE24	People	Decisionmaking	Success Criteria	Management power is needed to support the transformation		x		
PE25	People	Experience	Success Criteria	Security must be friction less so that employees do not work around it		x		
PR01	Process	Execution	Challenge	Defining and managing the roles				x
PR02	Process	Execution	Challenge	Formulation of robust policies	x	x	x	x
PR03	Process	Planning	Challenge	Prioritization of the different ZT building blocks	x			x
PR04	Process	Planning	Challenge	Finding the transformation starting point			x	x
PR05	Process	Execution	Challenge	Governance of access rights of human and technical identities				x
PR06	Process	Execution	Challenge	you need to move while the business is running	x			
PR07	Process	Execution	Challenge	In the way security is organized, setting it up is easy. But, maintaining it is so incredibly hard.	x			
PR08	Process	Execution	Challenge	Once you implement zero trust, it does take a little more coordination, because you probably have to adjust policies or add new policies to account for the new system that you're bringing on board.		x		
PR09	Process	Planning	Limitation	Have a solid foundation in place	x		x	
PR10	Process	Execution	Limitation	Change should happen incrementally	x			
PR11	Process	Execution	Pitfall	Bad preparations, ZT is not implemented over a night of sleep	x			x
PR12	Process	Execution	Pitfall	Account removal of company leavers			x	x
PR13	Process	Execution	Pitfall	Make it a theoretical exercise				x
PR14	Process	Execution	Pitfall	Slow admin alert response	x	x		
PR15	Process	Planning	Pitfall	Start implementing without roadmap	x		x	x
PR16	Process	Execution	Pitfall	Start chasing a rabbit			x	

PR17	Process	Execution	Pitfall	Getting wrapped up in vendor selection			x	
PR18	Process	Organization	Pitfall	Start with the shiny boxes	x		x	
PR19	Process	Execution	Pitfall	People fail because they bid off too big a piece at one time, and then they break stuff		x		
PR20	Process	Planning	Success Criteria	Start small & scale big	x	x	x	x
PR21	Process	Communication	Success Criteria	Show ZT benefits in early stage	x			x
PR22	Process	Communication	Success Criteria	Generate measurable results	x	x		
PR23	Process	Execution	Success Criteria	Make it a risk driven transition	x			x
PR24	Process	Execution	Success Criteria	Start simple, if you start to develop a success record, organization becomes more agreeable to allowing you to try more and more complex stuff		x		
PR25	Process	Execution	Success Criteria	the more complete you do the traffic study, the less problems you're gonna have. And the less you'll have to go back and tweak things		x		
RE01	Resources	Workforce	Challenge	Limited Time			x	x
RE02	Resources	Investment	Challenge	Limited Budget / Money			x	x
RE03	Resources	Workforce	Challenge	Limited Workforce	x	x		x
RE04	Resources	Investment	Challenge	Prioritization of investments	x			x
RE05	Resources	Workforce	Limitation	Availability of project teams	x			
RE06	Resources	Workforce	Limitation	Shortage of security staff				x
RE07	Resources	Investment	Limitation	MS Azure is a expensive solution, not all companies are capable of paying the licenses		x		
RE08	Resources	Procurement	Pitfall	Vendor selection, according to the sales team everything is possible	x			
RE09	Resources	Workforce	Success Criteria	Having the right trainings available	x			xx
RE10	Resources	Workforce	Success Criteria	Support of external party/consultant				x
RR01	Rules & Regulations	Compliance	Challenge	Accreditation & Auditing of ZT architectures			x	
RR02	Rules & Regulations	Compliance	Pitfall	Chasing for compliance with a framework			x	
RR03	Rules & Regulations	Compliance	Challenge	Privacy rules in NL are more strict than in the US				x
TE01	Technology	Design	Challenge	Architecture looks simple on paper, realization is complex	x			x
TE02	People	Knowledge	Challenge	Zero trust is not a box it's a journey				xx
TE03	Technology	Legacy	Challenge	Poorly maintained legacy systems				x
TE04	Technology	Legacy	Challenge	Hesitant to touch the Golden Goose			x	
TE05	Technology	Configuration	Challenge	Definitions for configurations in Azure, AWS and Google all sounds similar, but in practice they are different				x

TE06	Process	Execution	Challenge	Introducing zero trust in an operational environment without disruption (not everything can be tested in the lab		x		
TE07	Technology	Configuration	Limitation	Implementing security policy with native cloud controls				x
TE08	Technology	OT	Limitation	Availability of OT devices				xx
TE09	Technology	OT	Limitation	VPN for remote diagnostics for suppliers				x
TE10	Technology	Configuration	Limitation	Native cloud controls				x
TE11	Technology	Legacy	Limitation	Vital business processes that cannot be migrated			x	
TE12	Technology	capabilities	Limitation	Vendors that overpromise about the capabilities of there solutions	x			
TE13	Technology	Compatibility	Limitation	Having visibility on encrypted network to stay compliant				
TE14	Technology	Capabilities	Limitation	3000 tailor made solutions without granular access rights		x		
TE15	Technology	OT	Limitation	In OT environments, it's difficult to implement any kind of security solution, because it needs to operate at all times.				x
TE16	Technology	Capabilities	Limitation	Connectivity and the limited bandwidth availability, of course, a lot of latencies as well on ships				x
TE17	Technology	OT	Limitation	In industrial sector you have to deal with scada devices which are 20 years old, this makes it hard to implement zero trust principles on these OT devices		x		
TE18	Technology	Configuration	Pitfall	Vendor lock-in			x	
TE19	People	Knowledge	Pitfall	The idea you can buy ZT				x
TE20	Technology	Configuration	Pitfall	Vendor overlap				x
TE21	People	Knowledge	Pitfall	Vague picture of available capabilities	x			
TE22	Technology	Configuration	Pitfall	Compatibilityof a solution	x			
TE23	Technology	Configuration	Pitfall	Sprawl of applications / environments			x	
TE24	Technology	Configuration	Pitfall	Ensure that those technology overlaps do not jeopardize your organization				x
TE25	Technology	Configuration	Pitfall	the main issue I'm seeing is that you know, we all have a lot of point solutions.				x
TE26	Process	Execution	Success Criteria	Start small & scale big	x	x	x	x
TE27	Technology	Configuration	Success Criteria	Imposing ZT philosophy on all your existing projects	x			x
TE28	Technology	Compatibility	Success Criteria	Vendor integration				x
TE29	Technology	Compatibility	Success Criteria	Seamless and consistent user experience	x			
TE30	Process	Execution	Success Criteria	Start with a vendor that can fulfill as much of your needs as if you see and then start looking at the things around it				x

In figure 32, the overall use of codes is presented.

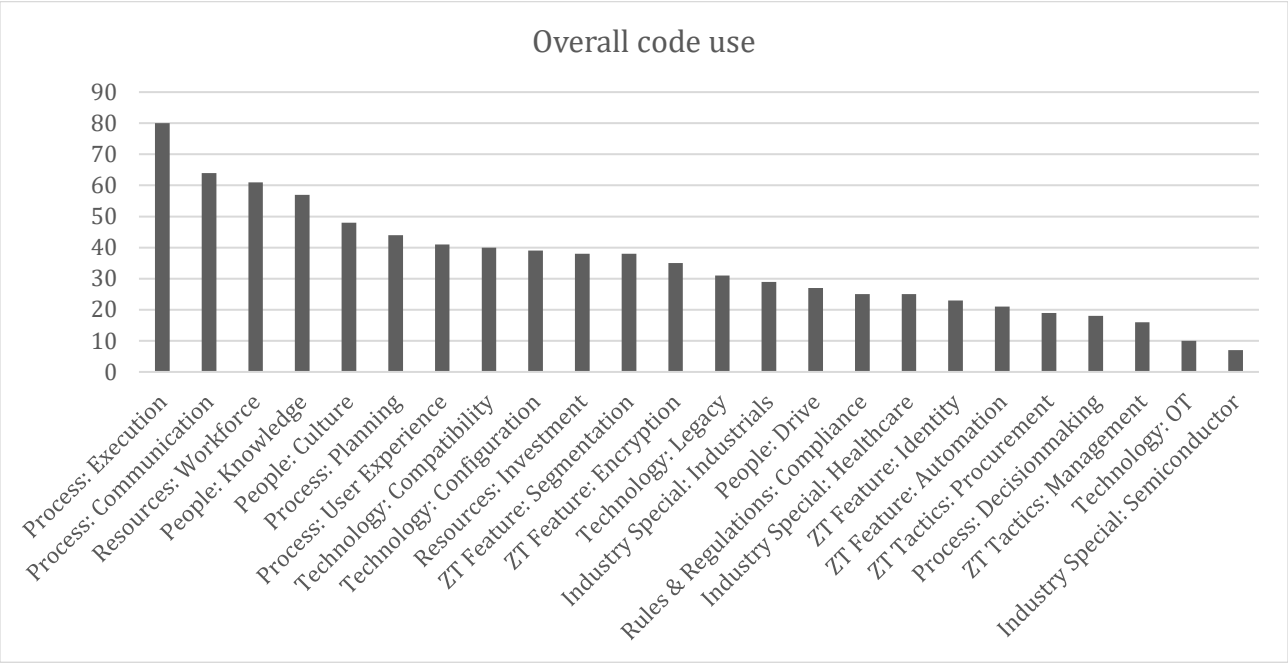


Figure 27: Code use in interviews

Appendix F: Architypes

	F1. SDN driven	F2. API driven	F3. SDP driven	F3. Identity driven	F4. Behaviour Driven
Identity: Identification	Credentials	Credentials	Credentials	Credentials, Biometrics	Credentials
Identity: Authentication	MFA, Policy Decision Point (PDP)	MFA, OCSP Responder	MFA, SDP Controller	MFA, Meta-data, non-repudiation	MFA, Risk-based
Identity: Authorization	Policy Enforcement Point (PEP)	API Gateway	Deny-all Gateway	Trust Scores, Just Enough Access (JEA)	Dynamic
Endpoints	Activity Logging, Device Hygiene	Activity logging	Activity Logging, SDP Client	Activity logging, Device Hygiene	Configuration management
Network	Trust zones, NGFW	Micro API firewalls	Mutual TLS	Identity-Aware Proxy (IAP)	SD-WAN, SWG, DNS protection
Infrastructure	Segmented on server/folder/file level	Containerized	Software-defined	-	
Application	-	Modular, Microservices	-	Conditional Access	
Data	Decentralised, Unencrypted	Decentralised, Unencrypted	Decentralised, Unencrypted	Granular access	DLP, Data obfuscation
Visibility & Analytics	-	-	-	-	SIEM, EUBA and NAV
Automation & Orchestrion	Policy Engine,	-	-	-	Auto remediation
Governance	Policy-Based Access Control (PBAC)	Attribute-Based Access Control (ABAC)	SDP Controller	Policy-Based Access Control (PBAC)	

F1: Zone driven (software defined network)

A zone driven architecture presented in figure 28 makes use of implicit trust zones to assure the least privilege. This type aligns with the ZT core capabilities as the architecture has;

1) Strong verification: users' identity is checked with the use of a password and an authentication app (MFA), and a Policy-Based Access Control (PBAC)
2) Least privilege: The access control mechanism used in this type is a Policy Decision Point (PDP) which evaluates access requests and consists of two components; the 'policy engine' and the 'policy administrator'.
3) Continues monitoring: All activity is being logged as input por the PDP

Strength

- Blast radius easily reduced due to the decentralised data storages
- Relatively easy to implement, due to the transition to the cloud

Weaknesses

- As PDP is compromised no access can be granted
- Trust zones are not by default encrypted, data breaches are still possible

Usability

- This architype can be used for the transformation of traditional architectures as the creation of zones can be done incrementally
- Classification and categorization of data & application is needed to make it a success. This can be a time-consuming job.

Tackled Adversaries

- Lateral Movement
- Discovery/Sniffing

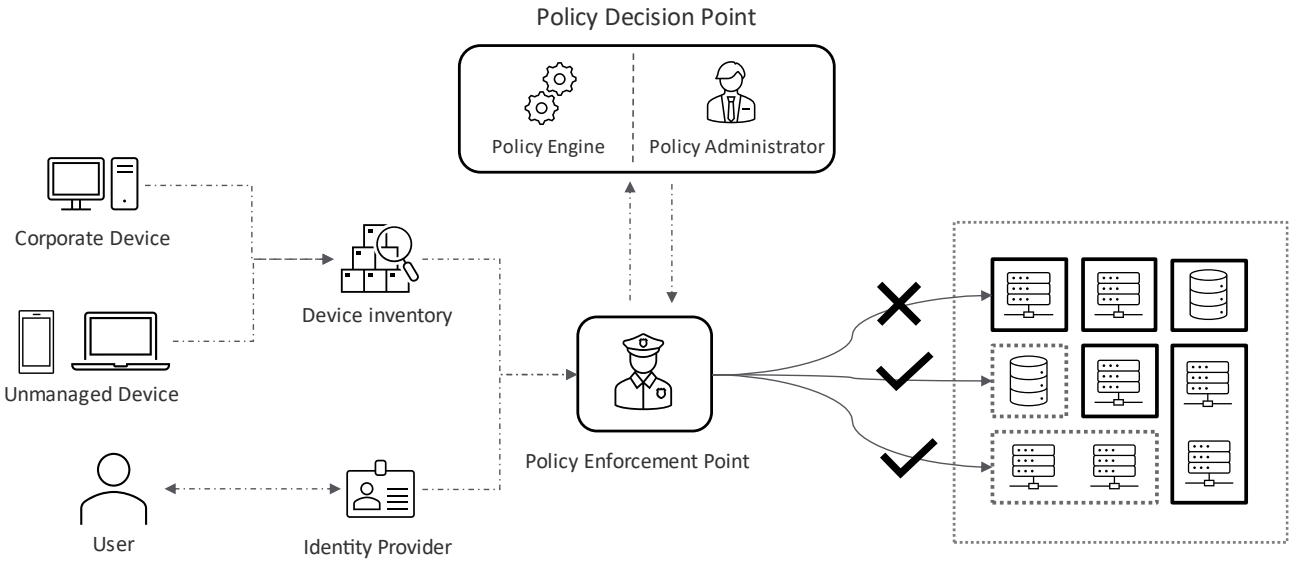


Figure 28: Zone Driven ZTA

F2: Service Mesh Driven

A Service Mesh driven architecture, presented in figure 29 makes use of microservices to assure least privilege. This type aligns with the ZT core capabilities as the architecture has;

1) Strong verification: the API gateway only provides access to a microservice it the right token is presented which is not expired.
2) Least privilege: With use of microservice and a containerized infrastructure least privilege can be guaranteed. The applications are broken into modular, loosely coupled components which are connected with an API to one simple user interface.
3) Continues monitoring: With use of the API Gateway all the data transfers can be logged and analysed to detect deviant behaviour. When a suspicious activity is detected the token provider can be informed to destroy the active/created tokens.

Strength

- Resilience if one application goes down not all services go down.
- Scalability, agility and efficiency and long-term development costs

Weaknesses

- For systems admins it is harder to manage, due to the proliferations of microservices
- Higher chance of failure as there is more communication needed between the services
- Denial of service is a becoming a more complex problem

Usability

- Hard to implement this architecture at large corporates as it is already challenging to keep track of all the different applications used.
- Solid trustworthy automation is required for the orchestration.

Tackled Adversaries

- Brute force attackers
- Exploitation of leaked tokens
- Spearfishing

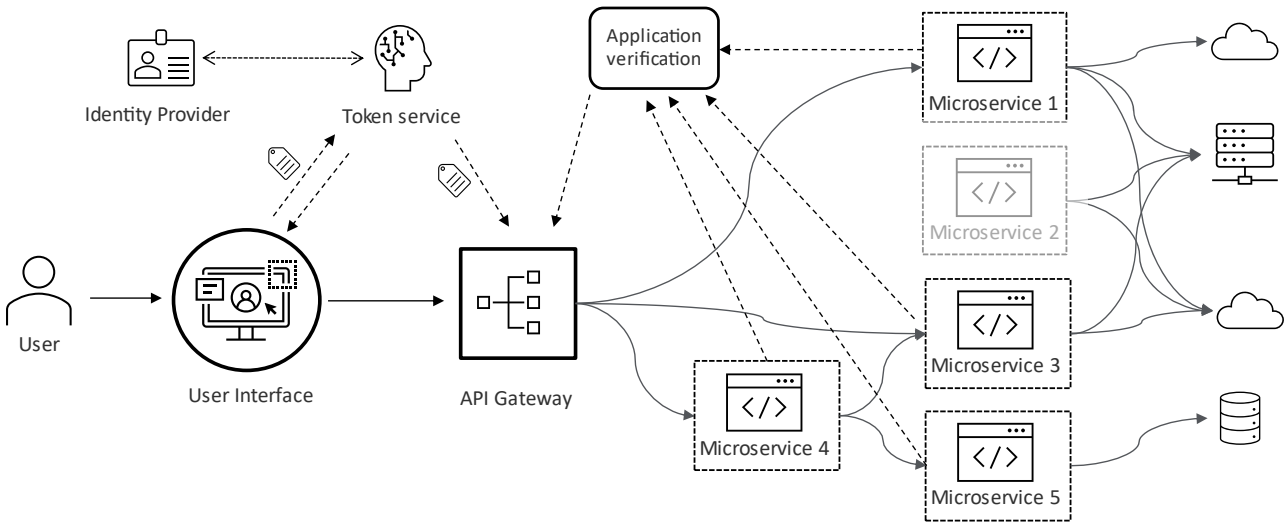


Figure 29: Service Mesh driven ZTA

F3: SDP Driven

A Software Defined Perimeter driven architecture, presented in figure 30 makes use of smaller perimeters to reduce the blast radius. This type aligns with the ZT core capabilities as the architecture has;

1) Strong verification: an IDP can check the user's identity and shares a live entitlement token once a user is verified.
2) Least privilege: with the use of single packet authorisation (SPA) resources are invisible to the prying eyes if access is not permitted. Moreover, only the needed access is provided once the identity of the user is verified.
3) Continues monitoring: All activities performed by the SDP controller and Gateway will be logged and monitored.

Strength

- Ports are not exposed; this ensures that nothing can be attacked. Following the principle; what cannot be seen, cannot be attacked.
- SDP controller can adjust or revoke access in real-time when a role of a user is changed
- Isolation of mission critical applications

Weaknesses

- Controllers have a vital role if they are offline, it is impossible to connect to resources.
- Implementing SDP in a large organization will cause disruption as devices and applications need to be reconfigured.
- Technical limitations, not all devices can run SDP software.

Tackled Adversaries

- Minimized attack surface
- Port & vulnerability scanning
- Spearfishing
- DDOS attacks

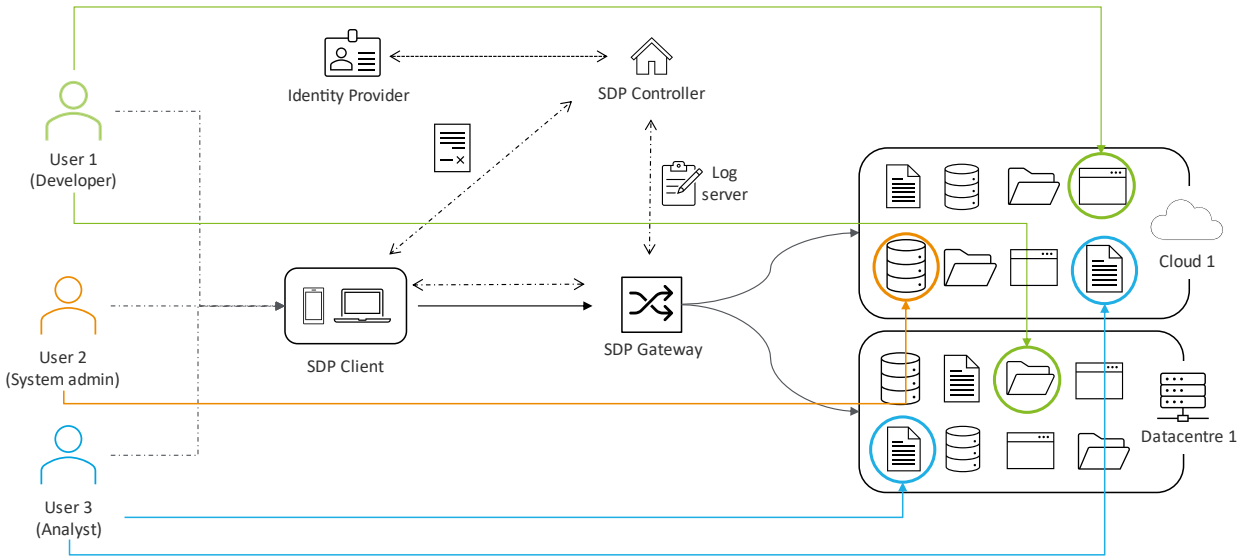


Figure 30: SDP Driven ZTA

F4: Identity Driven

A Software Defined Perimeter driven architecture, presented in figure 31 makes use of smaller perimeters to reduce the blast radius. This type aligns with the ZT core capabilities as the architecture has;

1) Strong verification: both the device and user are heavily screened with the goal to generating a trust score which can be used by the gatekeeper.
2) Least privilege: based on the trust score and the policy decision point, authorization is provided to the user by the gatekeeper.
3) Continues monitoring: the users/device activity is constantly monitored and logged. This storage of meta-data is later used for the generation of the trust scores.

Strength

- Strong focus on the identification of the devices and users

Weaknesses

- All activities are being monitored and stored this is something that can be conflicting with the GDPR

Tackled Adversaries

- Account manipulation

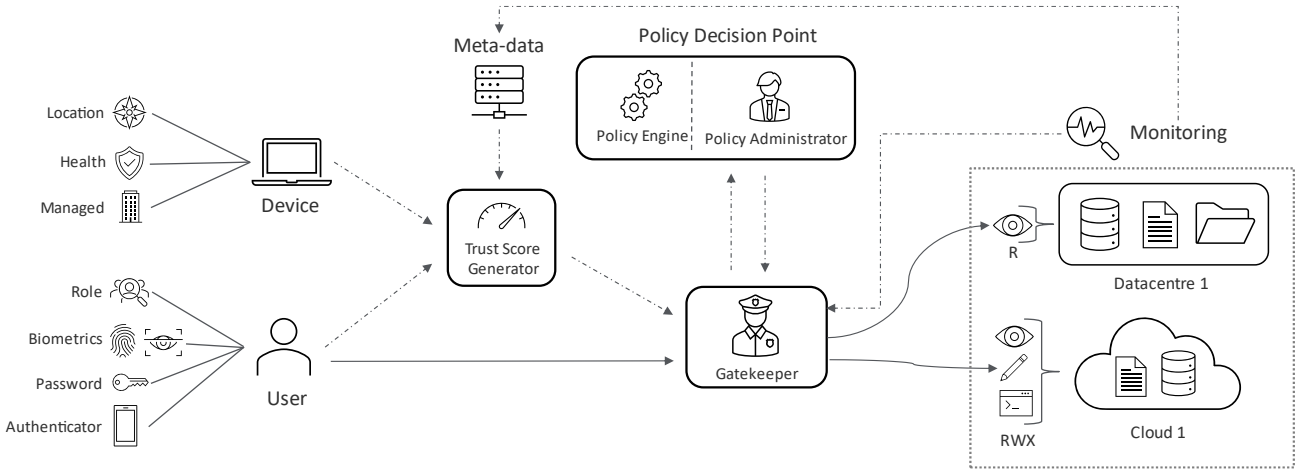


Figure 31: Identity driven ZTA

F5: Behaviour Driven

A behaviour driven architecture, figure 32 is an AI based solution providing security and access by activity monitoring and auto remediation. This type aligns with the ZT core capabilities as the architecture has;

1) Strong verification: -
2) Least privilege: -
3) Continues monitoring: A bot is 24/7 checking if the behaviour of the users is in line with the historic data and the dataset which is fed into the bot.

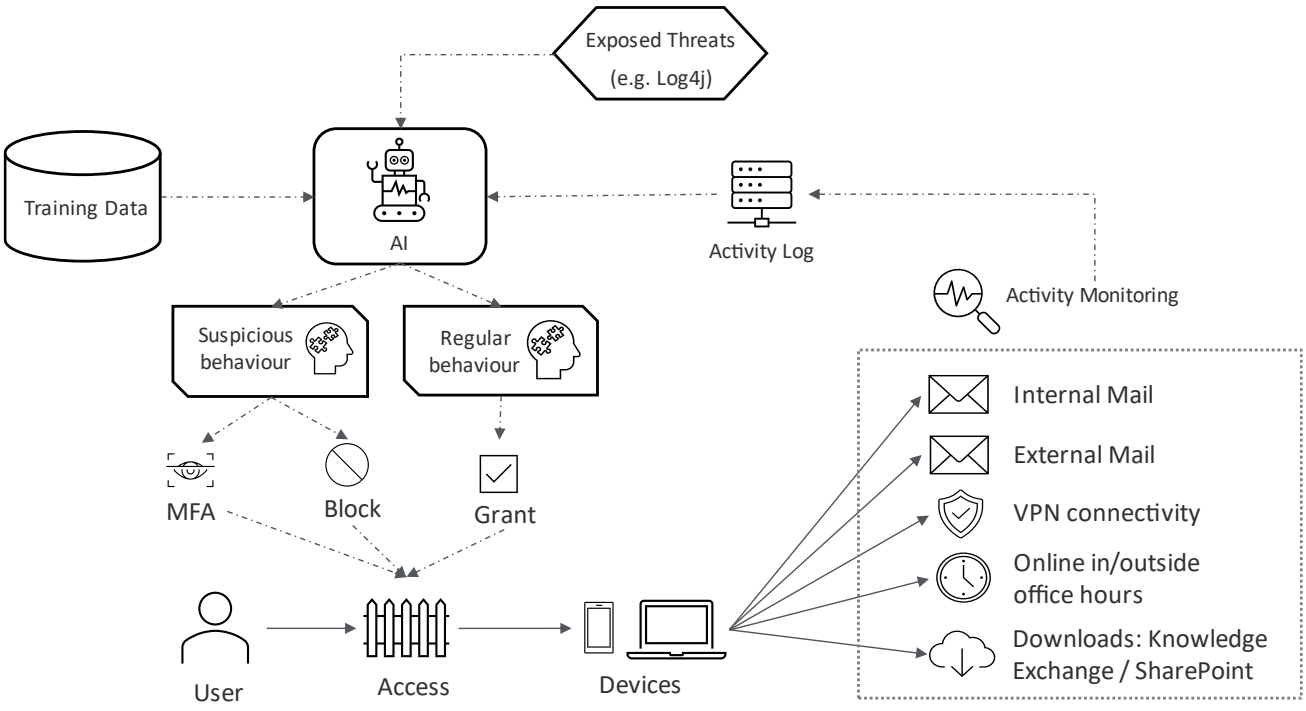


Figure 32: Behaviour driven ZTA

Appendix G: Existing principles

Eight Zero Trust Architecture design principles of NCSC UK

Taken from NCSC UK (2021) [retrieved on: 22/04/2022] Zero Trust architecture design principles. Available: https://www.ncsc.gov.uk/collection/zero-trust-architecture

P1. Know your architecture, including users, devices, services and data - In order to get the benefits from Zero Trust, you need to know about each component of your architecture
P2. Know your User, Service and Device identities - An identity can represent a user (a human), service (software process) or device. Each should be uniquely identifiable in a Zero Trust architecture.
P3. Assess your user behaviour, device and service health - To establish confidence in the security of your systems, user behaviour and service or device health are important signals for policy engines.
P4. Use policies to authorise requests - Each request for data or services should be authorised against a policy.
P5. Authenticate & Authorise everywhere - It is assumed that the network is hostile. Therefore, ensure all connections that access your data or services are authenticated and authorised.
P6. Focus your monitoring on users, devices and services - Monitoring of devices, services and users behaviours will help you establish their health.
P7. Don't trust any network, including your own - Communications over a network, to access data or services, should use a secure transport protocol to gain assurance that your traffic is protected in transit and less susceptible to threats.
P8. Choose services designed for Zero Trust - Using products that utilise standards-based technologies allows for easier integration and interoperability between services and identity providers

Seven guiding principles of NSA

Taken from NSA (2021). [retrieved on: 22/04/2022] Embracing a Zero Trust Security Model. Available: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

P1. Never trust, always verify – Treat every user, device, application/workload, and data flow as untrusted. Authenticate and explicitly authorize each to the least privilege required using dynamic security policies.
P2. Assume breach – Consciously operate and defend resources with the assumption that an adversary already has presence within the environment. Deny by default and heavily scrutinize all users, devices, data flows, and requests for access. Log, inspect, and continuously monitor all configuration changes, resource accesses, and network traffic for suspicious activity.
P3. Verify explicitly – Access to all resources should be conducted in a consistent and secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access decisions to resources.
P4. Define mission outcomes – Derive the Zero Trust architecture from organization-specific mission requirements that identify the critical Data/Assets/Applications/Services (DAAS).
P5. Architect from the inside out – First, focus on protecting critical DAAS. Second, secure all paths to access them.
P6. Determine who/what needs access to the DAAS to create access control policies – Create security policies and apply them consistently across all environments (LAN, WAN, endpoint, perimeter, mobile, etc.).
P7. Inspect and log all traffic before acting – Establish full visibility of all activity across all layers from endpoints and the network to enable analytics that can detect suspicious activity.

Nine Zero Trust Commandments OpenGroup

Taken from Open Group (2021). [retrieved on: 22/04/2022] Zero Trust Commandments. Available: https://pubs.opengroup.org/security/zero-trust-commandments/

P1. Validate Trust Explicitly - Security assurance shall rely on explicitly validating trust decisions using all relevant available information and telemetry.
P2. Enable Modern Work - Security discipline shall enable productivity and manage risk as the organizational capabilities, goals, environment, and infrastructure continuously evolve.
P3. Enable Pervasive Security - Security discipline shall be integrated into the culture, norms, and processes throughout the organization.
P4. Secure Assets by Value - Security controls shall be designed to protect business assets appropriate to their business value and expected risk.
P5. Implement Asset-Centric Controls - Asset-specific security controls (versus broad infrastructure controls) shall be implemented whenever available to minimize disruption of productivity and increase precision of security/business visibility.
P6. Enable Simple and Sustainable Security - Security controls shall be as simple as possible while remaining practicable, scalable, and sustainable for the full lifecycle of the business asset.
P7. Utilize Least Privilege - Access to systems and data shall be provided only as required, and access shall be removed when no longer required.
P8. Improve Continuously - Security teams shall continuously evolve and improve to remain successful in an environment that constantly changes.
P9. Make Informed Decisions - Security teams shall make informed decisions based on the best information that can be made available.

Three core principles of Forrester:

Taken from Forrester (2021) [retrieved on: 22/04/2022] The definition of modern Zero Trust available: https://www.forrester.com/blogs/the-definition-of-modern-zero-trust/

P1. All entities are untrusted by default
P2. Least privilege access is enforced
P3. Comprehensive security monitoring is implemented.

Three Principles of Google

Taken from Google (2014) [retrieved on: 22/04/2022] BeyondCorp Zero Trust Enterprise Security available: https://cloud.google.com/beyondcorp

P1. Access to services must not be determined by the network from which you connect
P2. Access to services is granted based on contextual factors from the user and their device
P3. Access to services must be authenticated, authorized, and encrypted

Three Principles of Microsoft

Taken from Microsoft (2021) [retrieved on: 22/04/2022] Zero Trust Model - Modern Security Architecture available: https://www.microsoft.com/en-us/security/business/zero-trust

P1. Verify explicitly - Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.
P2. Use least privileged access - Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity.
P3. Assume breach - Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

Seven principles of NIST 2020

Taken from NIST (2020) [retrieved on: 22/04/2022] NIST Special Publication 800-207 available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

P1. All data sources and computing services are considered resources.
P2. All communication is secured regardless of network location
P3. Access to individual enterprise resources is granted on a per-session basis.
P4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
P5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
P6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
P7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

Four principles of Palo Alto

Taken from Palo Alto (2021) [retrieved on: 22/04/2022] available: https://docs.paloaltonetworks.com/best-practices/9-1/zero-trust-best-practices/zero-trust-best-practices

P1. Establish identity using the strongest possible authentication. The request is authenticated and authorized to verify identity before granting access. This identity is continuously monitored and validated throughout the transaction.

P2. Verify the device/workload. Identifying the enterprise laptop, a server, a personal smartphone, or a mission-critical IoT device requesting access, determining the device's identity, and verifying its integrity is integral to Zero Trust. The integrity of the device or host requesting access must be verified. This integrity is continuously monitored and validated for the lifetime of the transaction. Or, in the case of applications and cloud infrastructure, identifying the requested device or microservices, storage or compute resources, partner and third-party apps before granting access.

P3. Secure the access. Enterprises need to ensure users only have access to the minimal amount of resources they need to conduct an activity, restricting access to, for example, data and applications. Even after authentication and checking for a clean device, you still need to ensure least privilege.

P4. Secure all transactions. To prevent malicious activity, all content exchanged must be continuously inspected to verify that it is legitimate, safe, and secure. Data transactions must be fully examined to prevent enterprise data loss and attacks on the organization through malicious activity

Three principles of Zscalar 2021

Taken from NCSC UK (2021) [retrieved on: 22/04/2022] Wat is Zero Trust available: https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust

P1. Terminate every connection - Technologies like firewalls use a "passthrough" approach, inspecting files as they are delivered. If a malicious file is detected, alerts are often too late. An effective Zero Trust solution terminates every connection to allow an inline proxy architecture to inspect all traffic, including encrypted traffic, in real time—before it reaches its destination—to prevent ransomware, malware, and more.

P2. Protect data using granular context-based policies - Zero Trust policies verify access requests and rights based on context, including user identity, device, location, type of content, and the application being requested. Policies are adaptive, so user access privileges are continually reassessed as context changes.

P3. Reduce risk by eliminating the attack surface - With a Zero Trust approach, users connect directly to the apps and resources they need, never to networks (see ZTNA). Direct user-to-app and app-to-app connections eliminate the risk of lateral movement and prevent compromised devices from infecting other resources. Plus, users and apps are invisible to the internet, so they can't be discovered or attacked.

Four principles of IBM

Taken from IBM (2020) [retrieved on: 22/04/2022] IBM Security Zero Trust Blueprints available: https://info.techdata.com/rs/946-OMQ-360/images/ZT%20-%20Secure%20the%20Journey%20to%20Cloud%20-%20Webinar%20Series.pdf

P1. Least privilege access - Giving users only as much access as they need, like an army general giving soldiers information on a need-to-know basis. This minimizes each user's exposure to sensitive parts of the network.

P2. Micro segmentation - The practice of breaking up security perimeters into small zones to maintain separate access for separate parts of the network.

• For example, a network with files living in a single data center that utilizes micro segmentation may contain dozens of separate, secure zones.

• A person or program with access to one of those zones will not be able to access any of the other zones without separate authorization.

P3. Multi-factor authentication - MFA simply means requiring more than one piece of evidence to authenticate a user Just entering the right password is not enough to gain access. A commonly seen application of MFA is the two-factor authentication (2FA) used on popular online platforms. In addition to entering a password, users who enable 2FA for these services must also enter a code sent to another device, such as a mobile phone, thus providing two pieces of evidence that they are who they claim to be. Not only does my user know their password, they must also have their mobile phone/email account. Something you know and something you have.

P4. Device knowledge and control - Ensure that every device is authorized. Just being on the network is not authorization. This further minimizes the attack surface of the network.

P5. Detection - Assume the perimeter is breached, detect malicious activity and Utilize notification or orchestration/automation to address detected issues/events

Five principles of Forbes

Taken from Forbes (2022) [retrieved on: 22/04/2022] 5 Core Principles Of The Zero Trust Model Of Cybersecurity available: https://www.forbes.com/sites/splunk/2022/05/01/5-core-principles-of-the-zero-trust-model-of-cybersecurity/?sh=64ee3f315934

P1. Assume the network is always hostile: Basic practice before Zero Trust had been to assume that if you were accessing a known network, you could be relatively certain it was secure. With Zero Trust, you assume it is not secure.

P2. Accept that external and internal threats are always on the network: Traditional security methods assumed networks were secure until a threat was detected. Zero Trust turns this model on its head.

P3. Know that the location of a corporate network or cloud provider locality is not enough to decide to trust in a network: Traditional security rules based on IP address are no longer reliable.

P4. Authenticate and authorize every device, user and network flow: A Zero Trust model authorizes and authenticates user access by least-privilege access on a per-session basis.

P5. Implement policies that are dynamic and calculated from as many data sources as possible: End-to-end data analytics should be established, providing monitoring and threat detection across the entire architecture, including cloud environments, which support both IT and security operations requirements.

Appendix H: Design principles development

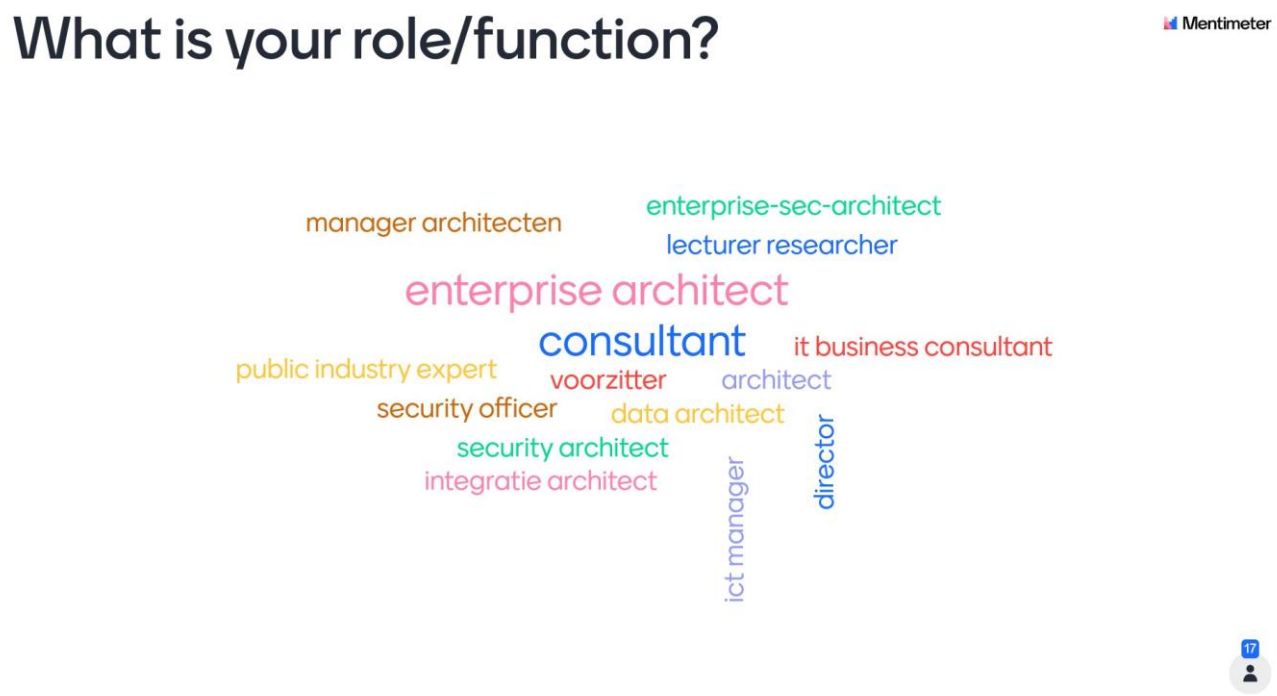
Table 34: Components of Architecture Principles according to TOGAF

Principle Name	Short title to identify the principle and which is easy to remember. No ambiguous words should be used to prevent it from making it fluffy
Statement	Communication of the fundamental rule
Rationale	Justification; the reasoning why a principle should be implemented and should highlight the business benefits when adhered
Implications	Actions/requirements that should be taken to comply with the principle

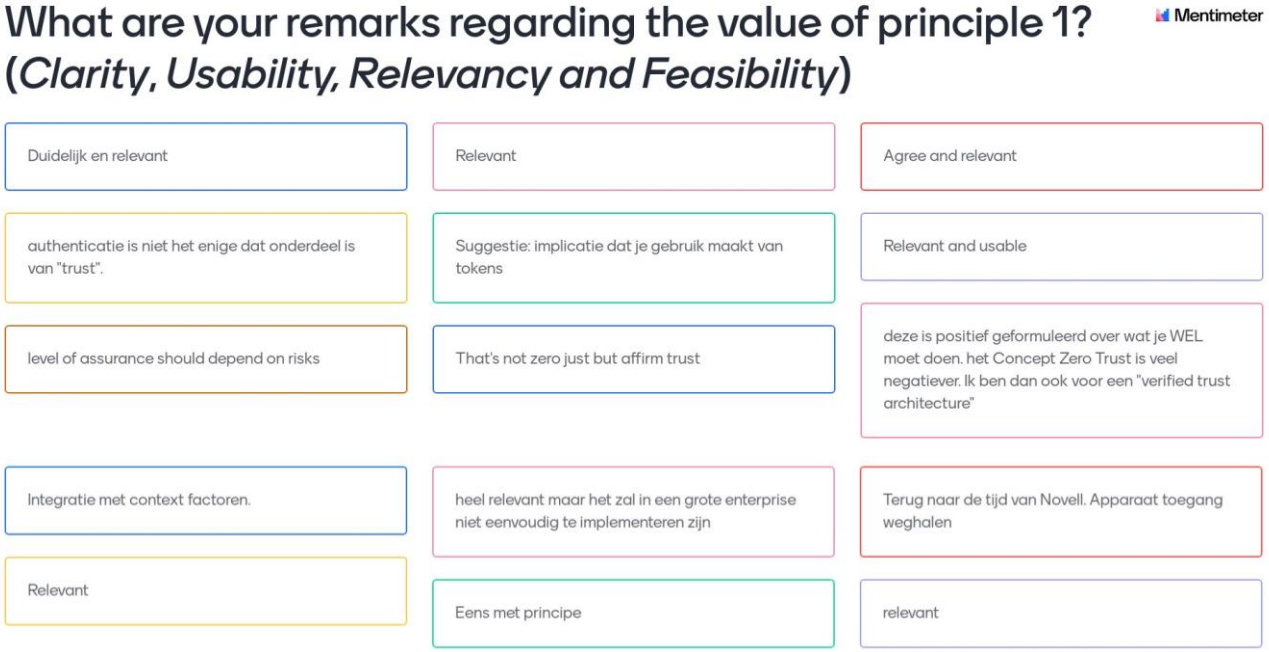
Table 35: Overview of Credos

Type	**Driver**	**Credo**	**Architecture principle?**
Value	Agility	Change incremental	no, not specific
Value	Agility	Evaluate periodically	no, not specific
Value	Agility	Segment in steps	yes, subprinciple
Value	Commitment	Culture is key	no, business principle
Value	Commitment	Get C-level buy-in	no, business principle
Value	Commitment	Leave the ivory tower	yes
Value	Confidence	Know device and service health	Yes
Constraint	Complete asset inventory	Inventorize DAAS Continuously	yes, subprinciple
Constraint	Complete asset inventory	Know your crown jewels	yes, subprinciple
Issue	Complexity	Start segmentation on macro level	yes, subprinciple
Issue	Complexity	Start the Zero Trust journey simple	yes
Risk	Deviating legislation	Comply with regulations	Yes
Risk	Deviating legislation	Review configurations	no, it is an action
Value	Efficiency	Integrate existing instruments	Yes
Value	Efficiency	Use existing instruments	no, it is an action
Issue	Implicit trust	Validate trust explicitly	yes
Constraint	Lack of ZT knowledge	Avoid shiny boxes	yes
Constraint	Lack of ZT knowledge	Educate the end-user	no, it is an action
Constraint	Lack of ZT knowledge	Educate the workforce	yes
Constraint	Lack of ZT knowledge	Leverage on existing practices	Yes
Constraint	Lack of ZT knowledge	Train IT staff	yes, subprinciple
Risk	Lateral movement	Construct segments	Yes
Risk	Lateral movement	Enforce least privilege	Yes
Constraint	Not all devices are compatible	Monitor the incompatible	No, it is a special
Issue	Novelty of Zero Trust	Be flexible	Yes
Issue	Novelty of Zero Trust	Build a flexible roadmap	No, not specific
Risk	Sophisticated adversaries	Design inside out	Yes
Risk	Sophisticated adversaries	Monitor all traffic	Yes
Risk	Sophisticated adversaries	Monitor continously	yes

Feedback DANW

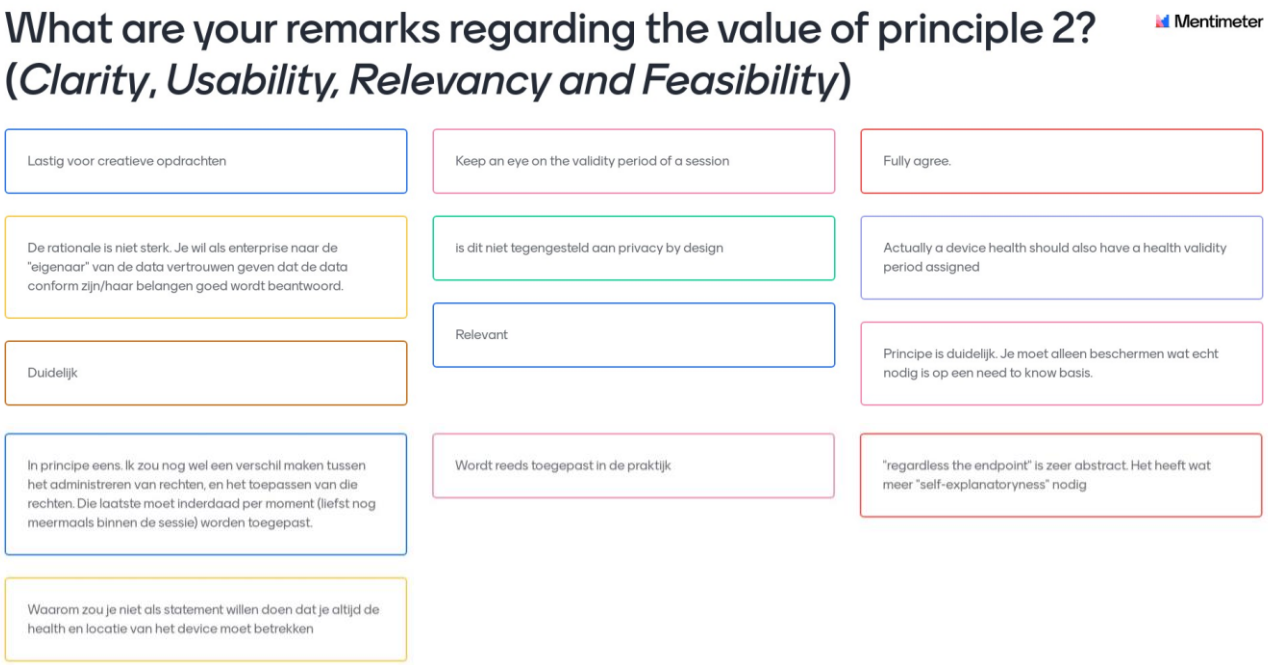


Principle 1 – Validate trust explicitly → Accepted



This principle is clear, useful and relevant according to the participants. However, it can be challenging to apply this principle in a big organization.
Suggestions: add make use of tokens part of the implications and that the level of assurance should depend on the possible risks.

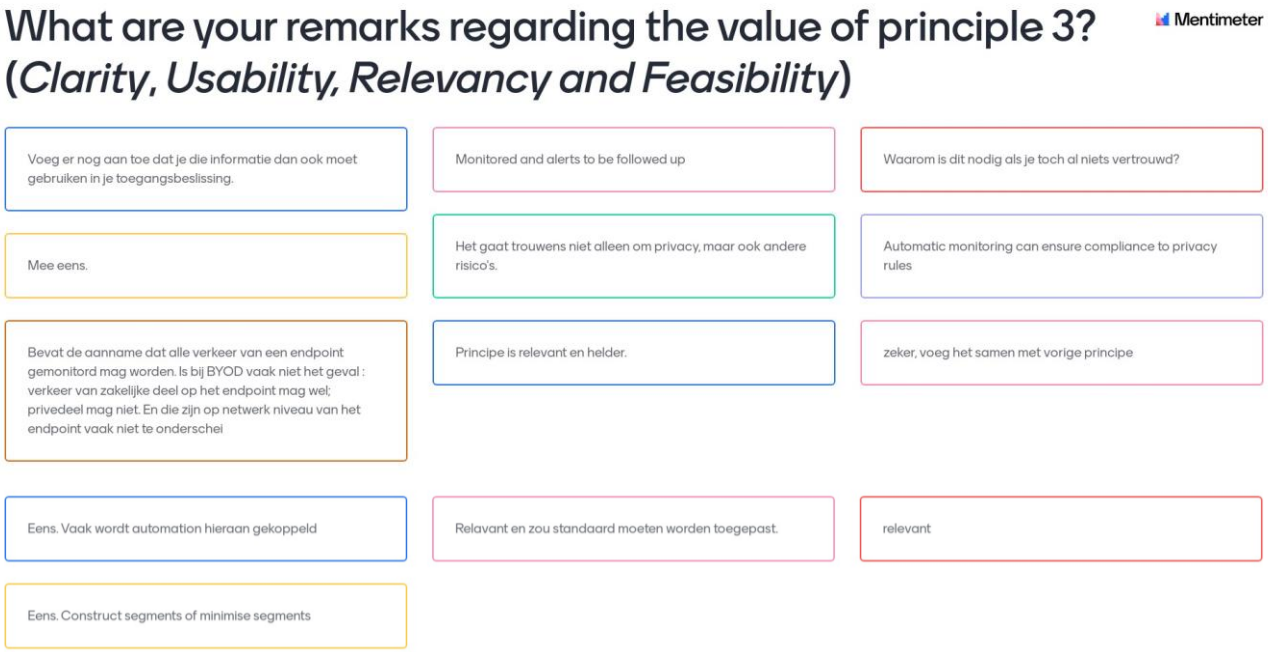
Principle 2: Enforce least privilege → Accepted



This principle is clear, useful and relevant according to the participants. Although it can be hard to apply this principle for creative assignments

Suggestions: add as implication “keep an eye on the validity period of a session”

Principle 3: Monitor Continuously → This principle is accepted when some changes are made.



Feedback

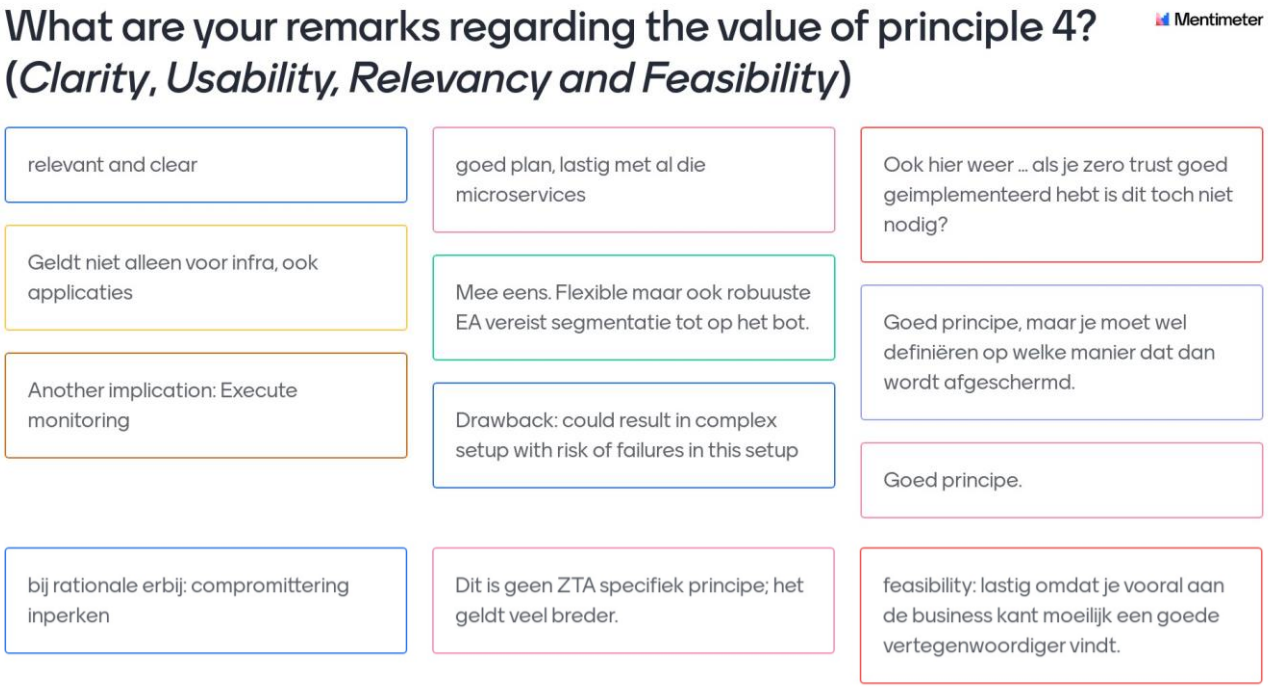
- The principle assumes that all traffic from an endpoint may be monitored. This is often not the case with BYOD: traffic from the business part on the endpoint is allowed; private part is not allowed. And these are often indistinguishable at the network level of the endpoint

- Frequently the automation aspect (auto remediation) is linked to this principle

Suggested changes:

- Include that besides the monitoring, alerts should also be followed up.
- Add as implication “use gathered data for making access decisions”
- Change “comply with privacy rules” to “Automatic monitoring can ensure compliance to privacy rules”

Principle 4: Construct segments → Accepted with some changes



Feedback

- Good idea, only the management of microservices can be hard
- Must be made more specific
- Possible drawback could result in complex setup with risk of failures in this setup
- Feasibility of this principle is difficult as it is hard specially to find a good representative on the business side.

Suggested changes:

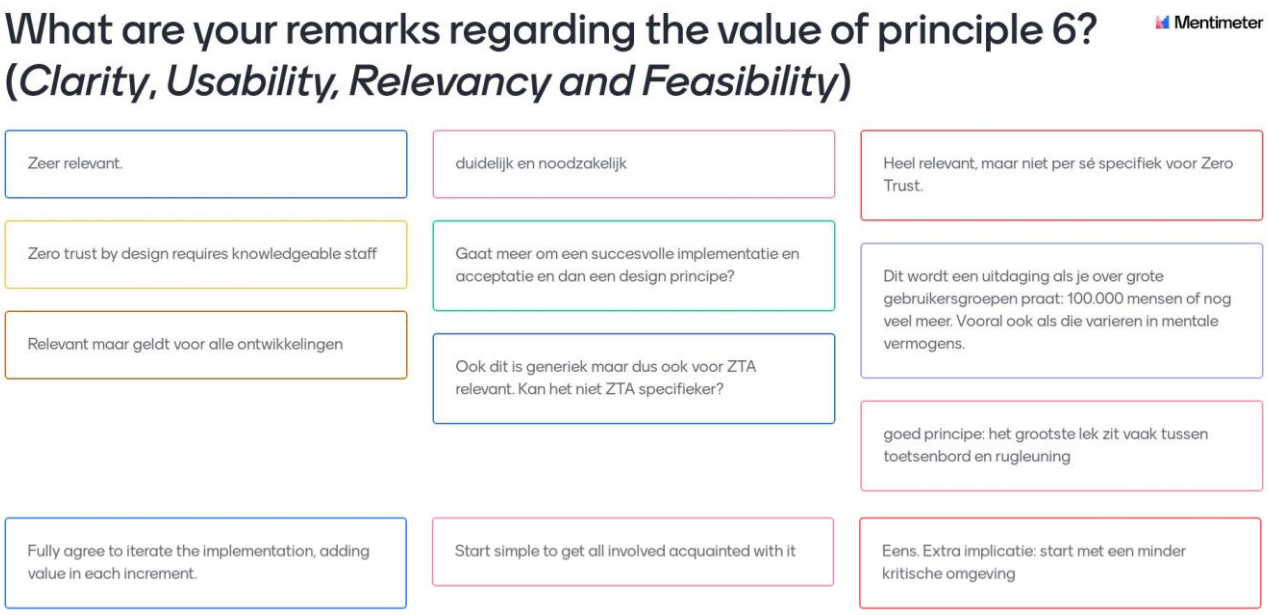
- Specification on how the segments should be created
- Add implication “execute monitoring”
- Not only the infrastructure but also the applications should be segmented
- Add “mitigate compromise” in the rationale

Principle 5: Leave the ivory tower → Rejected in current format, not ZT specific

Feedback

- It is a generic architecture and design starting point
- Seems generic to me and not ZTA specific. So, disagree.
- Is relevant but not specific only to Zero Trust
- Shared responsibility does not exist. There is one person / institute responsible
- This is not a ZTA specific principle; it applies much more broadly.

Principle 6: Educate workforce → Accepted, but need some sharpening not ZT specific



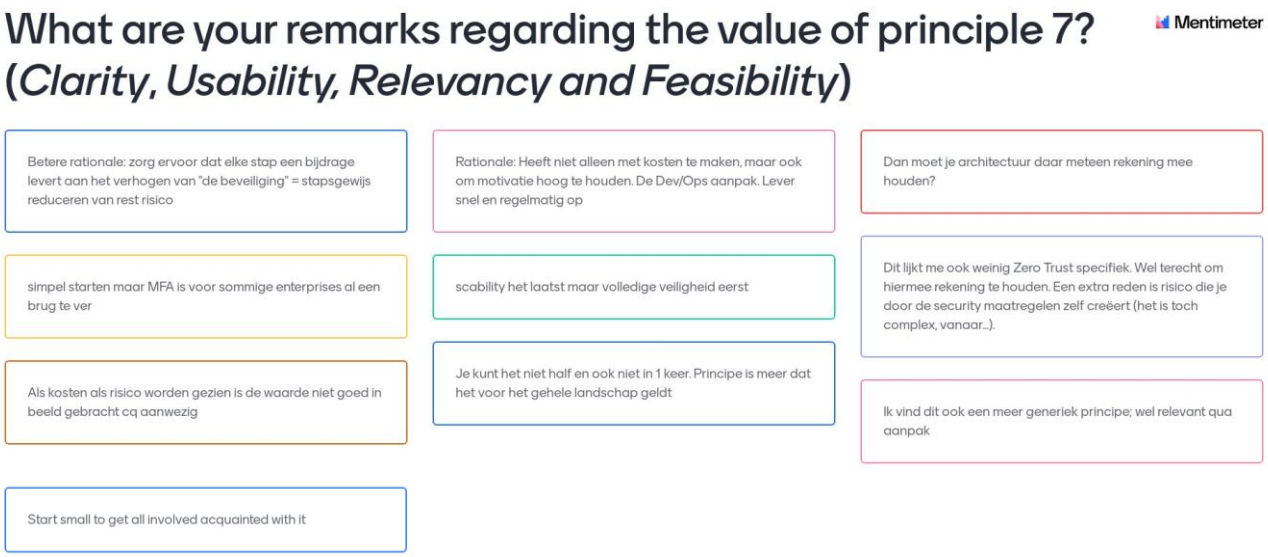
Feedback

- good principle: the biggest leak is often between the keyboard and the backrest
- This becomes a challenge when you talk about large user groups: 100,000 people or many more. Especially if they vary in mental abilities.

Suggested changes:

- make more Zero Trust specific
- add “Zero Trust by design requires knowledgeable staff”

Principle 7: Start simple → Accepted



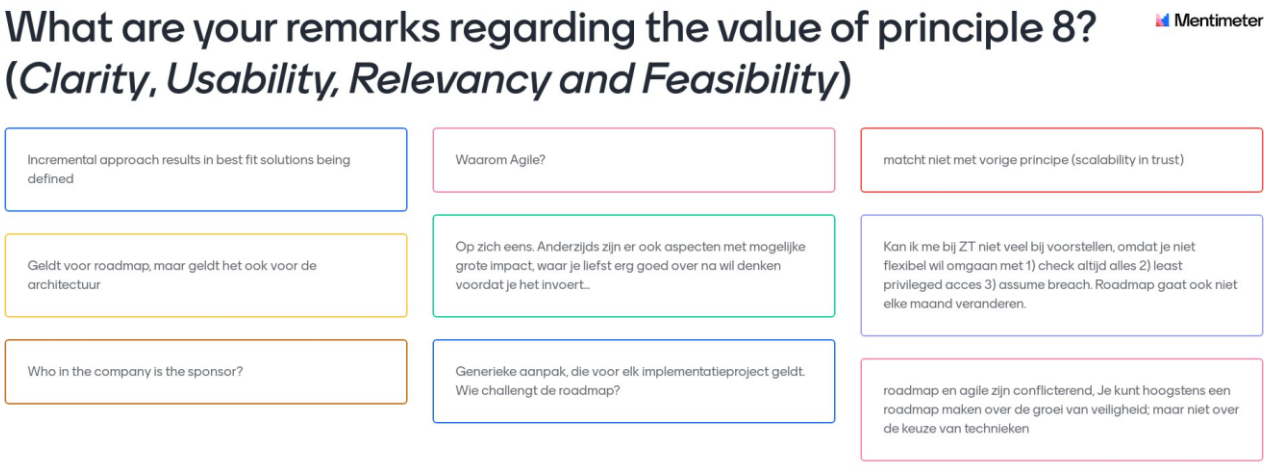
Feedback

- good principle only rationale should be changed
- Rationale: Has not only to do with costs, but also to keep motivation high. The Dev/Ops approach. Deliver quickly and regularly
- This also doesn't seem very Zero Trust specific to me.
- If costs are seen as a risk, the value is not properly visualized or is present
- Fully agree to iterate the implementation, adding value in each increment.

Suggested changes:

- Suggestion to change principle to; Start small to get all involved acquainted with it
- Add implication “scalability last but complete security first”
- Add implication “start with the less critical environment first”
- Better rationale: ensure that every step contributes to increasing "security" = step-by-step reduction of residual risk
- Rationale “An additional reason is the risk that you create through the security measures yourself (it is complex, after all...).”

Principle 8: Be flexible → Rejected



Feedback

- I can't imagine much at ZT, because you don't want to be flexible with 1) always check everything 2) least privileged access 3) assume breach. Roadmap is also not going to change every month.
- roadmap and agile are conflicting. At most you can make a roadmap about the growth of security, but not about the choice of techniques

Suggested changes:

- n/a

Principle 9: Change incremental → Accepted

Feedback

- Incremental approach results in best fit solutions being defined
- Increments keep you creating the most valued solutions from then on
- “Performance degradation is not THE (or only) reason to do it.

Suggested changes:

- Lis of implications can be reduced: with an agile approach (management to minimize risk), everything that is already stated here in terms of implications has already been covered.
- Remove the implication about possible loopholes

Principle 10: Design inside out → Accepted after small changes

Feedback

- I don't understand the relationship between the statement and the name.
- A nice starting point, but a balance is almost always better than either one....
- "Here too, bring your own sources of information, but be open to external possibilities.
- But the essence is that you can integrate flexibly with any relevant signal source."

Suggested changes:

- Rationale: authenticated => use authorized in the rationale

Principle 11: Integrate instruments → Rejected in the current form

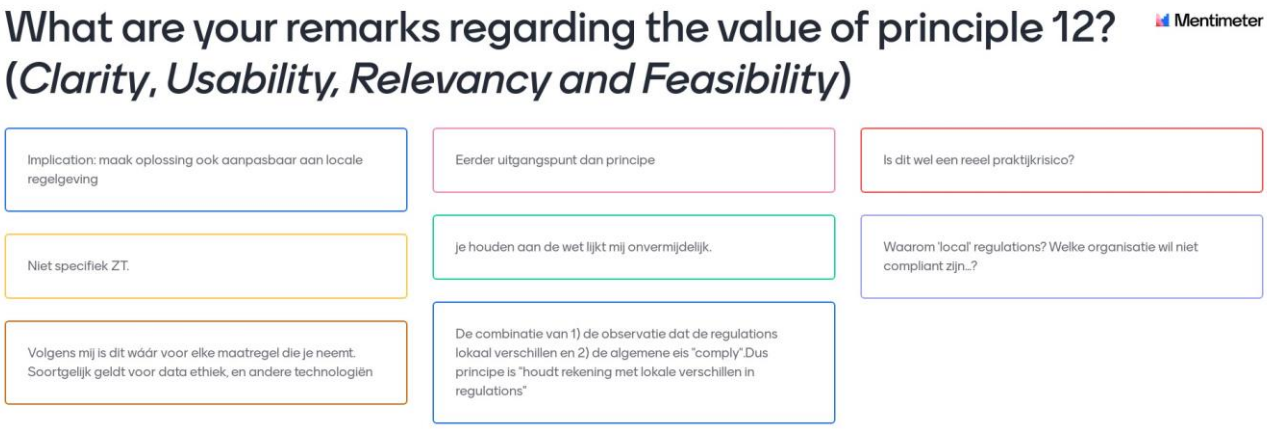
Feedback

- Actually: re-use before buy before build as a statement
- This is basically "reuse before buy before build"
- Put more emphasis on combining the existing
- Name does not make it clear that you prefer to continue working with what you already have at home
- Is a general premise (re-use before buy before build) and not ZT specific? The "frequent" fit seems exaggerated to me, by the way.

Suggested changes:

- n/a

Principle 12: Comply with regulations → Accepted after small changes



Feedback

- your keeping to the law seems inevitable to me.
- Why 'local' regulations? Which organization does not want to be compliant...?
- I think this is true for any measure you take. The same goes for data ethics, and other technologies
- "The combination of 1) the observation that the regulations differ locally and 2) the general requirement "comply".

Suggested changes:

- Implication: make solution also adaptable to local regulations
- Change principle to consider local differences in regulations