Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust

Christoph Buck[a], *Christian Olenberger*[b,*], *André Schweizer*[c], *Fabiane Völter*[d], *Torsten Eymann*[e]

[a] *Project Group Business & Information Systems Engineering of the Fraunhofer FIT, University of Bayreuth, Wittelsbacherring 10, 95444 Bayreuth, Germany; Centre for Future Enterprise, QUT Business School, Queensland University of Technology, QUT Gardens Point Campus, 2 George St, Brisbane City QLD 4000, Brisbane, Australia*

[b] *FIM Research Center, University of Augsburg, Project Group Business & Information Systems Engineering of the Fraunhofer FIT, Universitaetsstrasse 12, 86159 Augsburg, Germany*

[c] *Centre for Blockchain Technologies at University College London, qbound, Friedrichshafener Str. 1, 82205 Gilching, Germany*

[d] *FIM Research Center, University of Bayreuth, Project Group Business & Information Systems Engineering of the Fraunhofer FIT, Wittelsbacherring 10, 95444 Bayreuth, Germany*

[e] *Chair of Information Systems Management, University of Bayreuth, Project Group Business & Information Systems Engineering of the Fraunhofer FIT, Universitaetsstrasse 30, 95447 Bayreuth, Germany*

ARTICLE INFO

Article history:
Received 30 January 2021
Revised 5 August 2021
Accepted 6 August 2021
Available online 13 August 2021

Keywords:
Zero-trust
Network security
Access control
Software-defined perimeter
SDP
Multivocal literature review

ABSTRACT

In response to weaknesses of current network security solutions, the zero-trust model follows the idea that no network – whether internal or external – is trustworthy. The concept of zero-trust is enjoying increasing attention in both research and practice due to its promise to fulfil complex new network security requirements. Despite zero-trust's advantages over traditional solutions, it has not yet succeeded in replacing existing approaches. Uncertainty remains regarding the concept's distinct benefits and drawbacks for organisations and individuals, which hinders a holistic understanding of zero-trust and wide-spread adoption. Research can make valuable contributions to the field by systematically providing new insights into zero-trust. To support researchers in this endeavour, we aim to consolidate the current state of the knowledge about zero-trust and to identify gaps in the literature. Thus, we conduct a multivocal literature review, analysing both academic and practice-oriented publications. We develop a research framework for zero-trust to structure the identified literature and to highlight future research avenues. Our results show that the academic literature has focused mainly on the architecture and performance improvements of zero-trust. In contrast, the practice-oriented literature has focused on organisational advantages of zero-trust and on potential migration strategies. However, economic analyses and user-related studies have been neglected by both academia and practice. Future research may rely on our findings to advance the field in meaningful ways.

* Corresponding author.
E-mail addresses: christoph.Buck@fim-rc.de (C. Buck), christian.olenberger@fim-rc.de (C. Olenberger), andre.schweizer@qbound.io (A. Schweizer), fabiane.voelter@fit.fraunhofer.de (F. Völter), torsten.eymann@uni-bayreuth.de (T. Eymann).

https://doi.org/10.1016/j.cose.2021.102436
0167-4048/

1. Introduction

The digitalisation of our world is leading to increasing connectivity. Recent trends such as cloud computing, the Internet of Things (IoT) and bring your own device (BYOD) are causing existing networks to grow larger (Moubayed et al., 2019). Thus, more and more devices and services are exchanging information within a network, but also across its boundaries (Chen et al., 2019). These changes are resulting in complex new network security requirements, which existing solutions are struggling to keep up with (Chen et al., 2019; Compastie et al., 2016) as highlighted by the increasing number of data breaches and hacking attacks (DeCusatis et al., 2016; Moubayed et al., 2019; Shlapentokh-Rothman et al., 2020; Vanickis et al., 2018). Today, most network security concepts are based on a separation between internal and external networks. Firewalls, virtual private networks (VPNs) and network access controls (NACs) are used to isolate internal networks (Campbell, 2020; Chifor et al., 2019). All users, devices and services within this protected internal network are trusted, while outside users, devices and services are classified as untrustworthy (Chen et al., 2019). However, this approach's shortcomings become clear when considering that intruders can exploit security vulnerabilities or unsecured devices so as to gain access to an internal network (Mcginthy & Michaels, 2019; Moubayed et al., 2019), or that malicious insiders also pose a threat (Mehraj & Banday, 2020; Pan & Yang, 2018). Thus, the idea that no network – whether internal or external – is trustworthy is gaining traction in both academia and practice (Mehraj & Banday, 2020; Zaheer et al., 2019).

The zero-trust concept is a novel network security paradigm that is rapidly gaining recognition to address the above-mentioned challenges. The core idea is that there are no trustworthy areas (DeCusatis et al., 2016) and that every request must be evaluated and approved. In short, zero-trust means to "never trust, always verify" (Samaniego & Deters, 2018, p. 89). This more restrictive approach attempts to improve the protection of resources.

However, despite its potential to provide more secure networking as well as the increasing interest in zero-trust solutions, many organisations still rely on perimeter-based architecture (Polacek, 2020). The decision to invest in a new security solution is a complex and multifaceted process (Weishäupl et al., 2018). Since security investments are hard to evaluate quantitatively, because they often do not generate an obvious return on investment (Weishäupl et al., 2018), it is particularly important to consider the benefits for business processes, employees and customers so as to be able to make an informed decision.

Research has mainly focused on technical aspects and has neglected business-oriented questions. Yan and Wang (2020) present a first literature-based overview in their survey on zero-trust network security. They describe the technological framework and exemplary fields of application. However, since Yan and Wang (2020) do not conduct a structured literature review, there is still no multi-perspective examination of zero-trust considering the technical concept, organisations, users and society. Addressing research questions such as design and implementation options following the zero-trust paradigm, benefits and costs related to the concept, and the organisational steps necessary to successfully implement and operate zero-trust-based solutions are essential if one is to holistically understand the concept of zero-trust. Therefore, we seek to organise the current state of the knowledge and to identify gaps in the literature, so as to lay the foundation for a meaningful advancement of research into the zero-trust approach. Thus, our objective is to explore:

What is the current state of the knowledge about zero-trust, and what are avenues for future research?

To answer this question, we conduct a multivocal literature review based on guidelines provided by Garousi et al. (2019). To get a more comprehensive perspective on zero-trust, it is important to consider not only the academic literature (AL), but also practitioners' findings. Building on an previous research (Risius and Spohrer, 2017), we develop a research framework for zero-trust to structure our multivocal review and identify gaps in the literature. We then derive new research areas to inspire researchers to contribute new insights on zero-trust. Our research generates generalisable knowledge and derives important implications for both practice and research.

Our results reveal, that research focuses on the technical (e.g. Campbell (2020), Adikari et al. (2011), Singh et al. (2020b), Tao et al. (2018)) and performance facets (e.g. Chen et al. (2019), DeCusatis et al. (2016)). Despite the detailed technical discussion, the economic perspective has been neglected. Researchers should examine the disadvantages and costs of zero-trust, especially using economic methods. Further, there is no research on zero-trust solutions' users. Users are a key element in the adaptation of the concept. We contribute to the current literature by providing a multi-perspective review of the existing knowledge on zero-trust. We present a research framework to structure the current state of the research field. Further, we highlight knowledge gaps and point out future research avenues. Our work provides a foundation for the meaningful advancement of this research field.

The remainder of the paper is structured as follows. First, we explain the basics of zero-trust. Second, we describe our approach to the multivocal literature review and how we organised the articles in our research framework. Third, we describe the current state of the knowledge and identify new research topics. Fourth, we discuss our work's limitations and then conclude.

2. Conceptual background

2.1. *Vulnerabilities of traditional solutions*

In recent years, organisational operations have shifted. With the increasing popularity of working from home and trends such as BYOD, users and devices need dynamic access to data and applications from outside the internal corporate network (Chen et al., 2019; Moubayed et al., 2019). This trend is being amplified by the Coronavirus pandemic and the growing number of employees who are working from home (Gaudecker et al., 2020). Further, external connections, such as the integration of service providers and partners, or the sharing of resources with external parties, create challenges for or-

ganisational network infrastructure (DeCusatis et al., 2016). To date, most organisations have enabled external access to internal resources by establishing an encrypted connection between the external user or service and the internal network (Moubayed et al., 2019). Users and services within the network are classified as trusted and thus have access to its resources (Chen et al., 2019). However, current solutions have difficulties responding to such dynamic changes, because they often consist of static rule sets, firewalls, VPNs and subnetworks (Chen et al., 2019; DeCusatis et al., 2016; Pan and Yang, 2018). This architecture results in serious vulnerabilities. First, no controls or segmentation exist within the internal network (Chen et al., 2019). Once an external intruder or malicious insider has gained access to an internal network, they have access to large areas of the network and can therefore read, modify and damage many organisational resources (Shlapentokh-Rothman et al., 2020). There are no or very few measures to restrict lateral movement through the network (Kumar et al., 2019). Second, the security level depends on the weakest protected device or application. Intruders can use poorly protected devices or applications as an entry point into an internal network (Chen et al., 2019; Shlapentokh-Rothman et al., 2020). Thus, the internal network is only as secure as the worst-protected device or application. Third, IP addresses of devices and services are known externally. Existing solutions first establish a connection and then verify the access rights. This makes them potential targets that can be exploited to enter or disrupt a network, for instance by distributed denial-of-service (DDoS) attacks (Kumar et al., 2019). Fourth, log files are stored on centralised log servers. By accessing the log files, intruders can disguise their activities and can erase their tracks.

2.2. *Zero-trust as a promising solution*

In order to address the weaknesses of current networking solutions (Kindervag, 2010b), Zero-trust approaches follow the core idea that no network participant is trusted and any access to organisational resources represents a potential threat. Thus, every single access is inspected and verified. Access is granted only after successful verification of a request. Full access to a service can be granted or only to specific functions or data for which the user is authorised. The verification should not be performed only based on a password, but considers multiple factors and information sources: user password, the device used, current location time (Omar and Abdelaziz, 2020) and access privileges (Yan and Wang, 2020). Furthermore, the principle of least privilege applies (Eidle et al., 2017), meaning that access is granted only to those resources required to perform functions. It is therefore important to define access policies and to strictly adhere to them. However, these access policies are not static (Yan and Wang, 2020). Through the continual analysis and logging of network traffic (Eidle et al., 2017), the network participants' behaviour patterns can be identified as well as integrated into the verification process (Pan and Yang, 2018). Overall, zero-trust is not a specific technology, but a holistic approach that incorporates different core principles (Sultana et al., 2020). Thus, different technologies (already existing or newly developed) can be used to implement zero-trust. The core principles of zero-trust can be summarised as follows (Rose et al., 2020):

1. All data sources and computing services are treated as organisational resources, which must be secured.
2. Despite the network location of access request, all communication is secured. No trust is granted automatically and no assets requesting access are trusted by default.
3. Access to resources is granted per session only.
4. Access is determined based on device characteristics, behavioural and environmental attributes.
5. Least privilege applies.
6. Access is not granted statically but continuously re-evaluated.
7. Information about assets, network infrastructure, and communications is collected and used to improve security.

While the term zero-trust was officially coined in 2010 (Kindervag, 2010b), the idea of the concept that no network participant is trusted goes back to the beginning of secure computing. For example, Saltzer and Schroeder (1975) already proposed complete mediation and least privilege in 1975. Some of these were also picked up by development methods such as Model-driven security (Basin et al., 2003; Jensen and Jaatun, 2011) or security-by-design. The former aims to integrate security policies, security requirements, and functional requirements into account during the whole development cycle (Basin et al., 2003; Nguyen et al., 2015). In specific, role-based access control policies define and constraint access (Jensen and Jaatun, 2011). The latter refers to security being an essential requirement from the very beginning of the software engineering cycle for systems and networks to be secure by design (Devanbu and Stubblebine, 2000). The individual principles of zero-trust are not novel itself, but rather the fact that all principles are used to protect organisational resources (Rose et al., 2020). While model-driven security or security-by-design refer to development methods for security engineering which can be applied to a variety of products (Basin et al., 2003; Devanbu and Stubblebine, 2000; Jensen and Jaatun, 2011), zero-trust describes a concept focusing on access security (Kindervag 2010a). Thus, in addition to integrating the highest level of security into assets and products from the point of creation, zero-trust addresses external threats to assets stemming from untrusted endpoints.

While the implementation of zero-trust workflows may vary depending on the organisation's requirements, architectures generally comprise two main components responsible for access control. These are the (1) zero-trust *policy enforcement point* (PEP) and a (2) zero-trust *engine*.

The former enables the communication between a network participant and a resource. For this purpose, the zero-trust PEP forwards incoming requests to the zero-trust engine; in response, it receives the instruction to establish or terminate the communication. Thus, direct communication between the subject and the resource is not possible. Further, the zero-trust PEP monitors and logs traffic (Rose et al., 2020). At the same time, the Zero-trust *engine* makes the decision whether or not a requestor is granted access to an organisational resource. Based on input information from the request (authentication information, required resource), access information from the policy information point (e.g. user data, activity logs), and defined access policies from the policy storage,

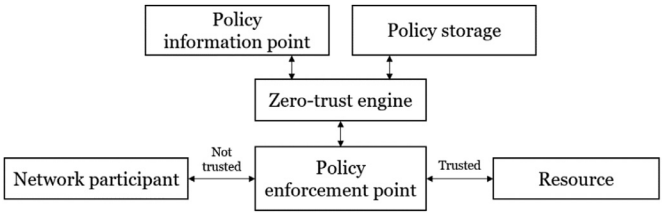

Fig. 1 – An overview over the zero-trust model.

the engine's trust algorithm decides whether a request gets verified (Dimitrakos et al., 2020). In this process, the identity of the user or service is verified, as well as the utilised device's trustworthiness. For this purpose, developers can rely on a variety of technologies including but not limited to identity and access management, multifactor authentication, or device verification (Mehraj and Banday, 2020). If the zero-trust engine accepts the request, it instructs the PEP to establish a connection between the network participant and requested resource. In case it is not accepted, the PEP does not establish a new connection, or terminates the existing connection (Mehraj and Banday, 2020; Rose et al., 2020). Fig. 1 provides an overview over the zero-trust model's set-up.

While implementations vary, the concept zero-trust imposes controls to lie close to applications and users rather than in the network infrastructure. This ensures that constraints can follow the semantics of the underlying security concept. In contrast, if controls lie within the network infrastructure, network layers are burned with additional complexity (Banyan, 2019).

Various practical approaches exist to follow above-listed principles and implement the logical components PEPs and engines. Among the most common concepts included in zero-trust architectures are software-defined perimeter (SDP), reverse proxies, micro-segmentation, and enhanced identity governance. Regarding SDP, a 'black box' is created that hides the infrastructure and resources from public view (Kumar et al., 2019). Only after successfully passing a verification process, a connection to the required resource can be established (Refaey et al., 2019). This results in a dynamic network segmentation (DeCusatis et al., 2016), which allows an adaptive enforcement of access policies (Compastie et al., 2016). Moreover, reverse-proxies can support in the deployment of zero-trust. In specific, reverse-proxy models require users to authenticate with a proxy responsible for the verification. In addition, micro-segmentation may also be used to implement zero-trust architectures, which refers to PEPs protecting individual resources or groups of resources. While micro-segmentation supports implementing zero-trust, it does not represent a stand-alone measure. Furthermore, enhanced identity governance may support in developing access policies in zero-trust architectures (Rose et al., 2020).

Owing to the design of zero-trust models, it has several advantages in comparison to current working solutions (DeCusatis et al., 2016; Eidle et al., 2017; Rose et al., 2020). First, the use of several factors in authentication better protects resources and data against attacks and breaches (Yan and Wang, 2020). Second, the fine segmentation of access prevents attackers and malware from moving around the network (Mehraj and Banday, 2020). Third, the resources may also be better protected against DDoS attacks – one of the most common forms of attack. Since access is only possible via the zero-trust PEP, external and unauthorised requests can be rejected immediately (Kumar et al., 2019; Omar and Abdelaziz, 2020). Fourth, the improved authentication mechanisms and the explicit definition of access policies allow access to the network to be precisely controlled. This enables more fine-grained access and rights models than existing solutions (Kumar et al., 2019). Fifth, through the continual logging and monitoring of traffic, suspicious behaviours and attacks can be detected and interrupted more quickly. At the same time, zero-trust increases traceability for forensics and thus allows learning from past incidents (Kindervag, 2010a).

Despite these many advantages, zero-trust has not yet succeeded in replacing the existing solutions (Polacek, 2020). The zero-trust approach is very different to traditional solutions, which is why an implementation is associated with high risk, and the decision should therefore be well founded. Specifically, owing to the zero-trust approach's innovativeness, existing solutions need to be replaced or integrated in a complex way (Moubayed et al., 2019), which leads to investment costs – for instance, for new infrastructure, the adaptation of existing processes, and employee training. However, as with many cybersecurity measures, the return on investment is not obvious and is hard to evaluate (Weishäupl et al., 2018). Thus, it is uncertain whether an investment in zero-trust is profitable. Further, there is little knowledge on organisational problems caused by zero-trust (Gigamon, 2020). These unanswered questions challenge a comparison of advantages and disadvantages and thus impede the adoption of zero-trust. We argue that researchers can make valuable contributions by systematically gaining new knowledge about and a holistic understanding of zero-trust.

3. Methodology

We seek to provide a comprehensive overview over the current knowledge on zero-trust and to identify relevant gaps for future research (Saltan and Smolander, 2021; Scheuner and Leitner, 2020). We intend to motivate further research by highlighting relationships to existing work and by identifying avenues for new research streams. Owing to more diligent and thus lengthy publication processes, including only academic research articles may not reflect the most recent state of the knowledge. Examining the divergence of academia and practice can reveal critical blind spots on either side. We ar-

Table 1 – Research framework and research questions (based on Risius and Spohrer, (2017)).

Level of analysis	Activities		
	Design and features	Measurement and value	Management and organisation
Concept and architecture	RQ1: How to design and/or implement a zero-trust architecture?	RQ4: What are the value propositions and the limitations of zero-trust technology compared to established solutions?	RQ7: Which skills, talent or human resources should zero-trust providers and operators develop?
Firms and industries	RQ2: How can firms utilise zero-trust concepts for the security of their operations?	RQ5: How does zero-trust provide added value for organisations?	RQ8: How should organisations organise, govern, fund and develop their zero-trust capabilities?
Users and society	RQ3: How do zero-trust features and design affect the interaction between users and technology adoption?	RQ6: What are the benefits and costs of using zero-trust technology for individual users and society?	RQ9: How does one balance user privacy and legal demands?

gue that it is important to also consider grey literature (GL) when developing a research roadmap. Therefore, we conducted a multivocal literature review based on the guidelines provided by Garousi et al. (2019). We divided the review process into three stages: planning, conducting and reviewing. During the planning stage, we first determined the need for a multivocal literature review, defined its scope and derived the corresponding research questions. Then we conducted a database search to identify AL and a web search for GL. During the reviewing stage, we extracted the data, aggregated the results and wrote down the review's findings and contributions.

3.1. *Research questions*

Our research objective is to structure the existing knowledge on zero-trust and to systematically identify new research streams. Thus, we adopted the approach of Risius and Spohrer (2017), who introduced a research framework on blockchain technology, to derive and structure our research questions. In our view, their approach can be used as a foundation for the development of a research framework in the zero-trust domain, for two reasons. First, early research into blockchain technology and the current literature on zero-trust show various similarities. In parallel to early advances of research into blockchain, research into zero-trust has focused primarily on technological advancements. Second, both blockchain and zero-trust can be considered as emerging technologies or concepts, respectively. Like the hype around blockchain technology in 2017, there has been a surge in attention on zero-trust (Yan and Wang, 2020). Given these similarities, we argue that Risius and Spohrer's research framework (2017) can also be adopted for the context of zero-trust.

The research framework addresses two dimensions: activities and the levels of analysis influenced by them. Activities refer to the actions that a developer or user can perform. They are divided into three groups. First, activities of *design and features* address the understanding of the implementation and design of the concepts and their features, including certain design choices' consequences (Risius and Spohrer, 2017). Second, questions of *measurement and value* evolve around the added value provided, specifically how to create and measure additional value for stakeholders involved. Third, *management and organisation* addresses actions necessary for successful implementation. These include required organisational capabilities, skills and talents, implementation strategies, and the management of sensitive governance-related aspects, for instance the balancing of privacy and legal demands. The level of analysis specifies the research object's scope. Risius and Spohrer (2017) distinguished between four levels: *platforms, intermediaries, firms and industries*, and *users and society*.

While activities apply to the zero-trust concept as is, we adjusted the levels of analysis. In contrast to blockchain technology, zero-trust is not a platform but a multifaceted concept. The architecture may be adjusted depending on the usage case and its requirements. To capture this aspect, we included the level *concept and architecture* instead of *platforms*, referring to the development and implementation, architectural variations, and protocols of zero-trust. Intermediaries and their future functions are a key aspect of blockchain technology. However, because intermediaries are not relevant for zero-trust, we decided to remove the *intermediaries* level. In line with Risius and Spohrer (2017), we included *firms and industries*, because they are key stakeholders for driving the adoption of zero-trust. On this level, the focus is on the implementation and uses of zero-trust in organisations or industries. Further, we adopted the *users and society* level, focusing on the uses and implications for users and society (Risius and Spohrer, 2017). Thus, the modified research framework covers three levels of analysis: *concept and architecture, firms and industries*, and *users and society*. We used the dimensions resulting from the intersection of activities and levels of analysis to derive the research questions guiding our multivocal literature review. For each intersection we developed one specific research question. Table 1 provides an overview over the research framework and the corresponding research questions.

3.2. *Search strategies*

The multivocal literature review process consists of two separate parts. First, we conduct a conventional literature review to select academic peer-reviewed literature (e.g. journal and

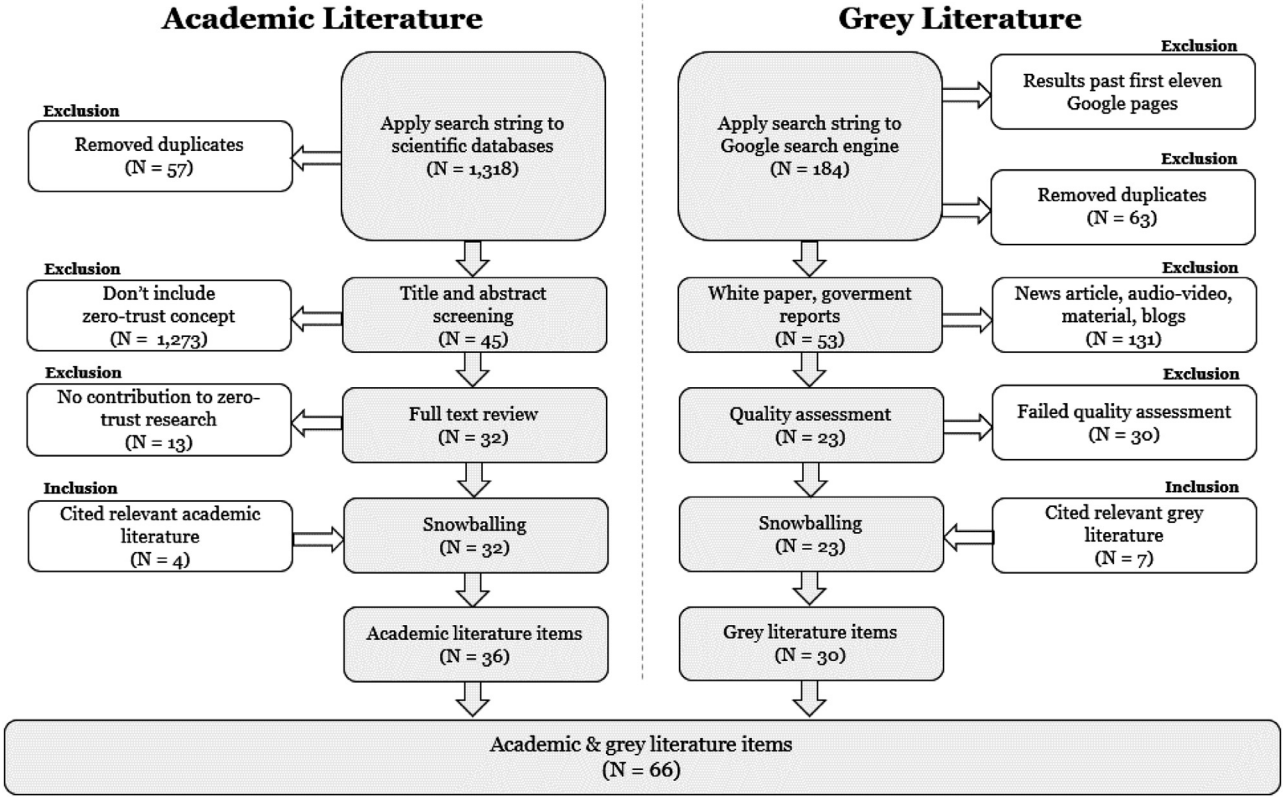

Fig. 2 – An overview over the search strategy and selection process.

conference papers) (Kitchenham and Charters, 2007). Second, we conduct a web search to identify relevant GL. However, we focus on GL with a high degree of credibility and expertise, i.e. white papers, books and government reports. Fig. 2 summarises our approach (Garousi et al., 2019).

3.2.1. *Database search for academic literature*

As suggested by Kitchenham and Charters (2007), we first elaborated a search string. We conducted an initial search on Google Scholar to explore the zero-trust field. We used the term combination *zero-trust*, deliberately not placing any further restrictions so as to obtain a broad overview. Based on the most relevant results, we identified related terms that were used as synonyms for zero-trust concepts. We included SDP and BeyondCorp as frequently mentioned implementations for zero-trust. Further, since it became apparent that *zero-trust* does not exclusively cover security-related topics, we explicitly included security-related terms. Thus, we defined the following search string:

> *(("Zero Trust" OR "Zero-trust") OR ("Software-Defined Perimeter" OR "SDP") OR ("BeyondCorp")) AND ("security" OR "authentication")*

Second, the searching has been applied to nine well-established databases for AL: AIS eLibrary, ACM Digital Library, ScienceDirect, IEEE Xplore, Web of Science, SpringerLink, JSTOR, EBSCO and ProQuest. The title and abstract search performed in May 2021 yielded 1,318 articles without duplicates.

Third, we defined inclusion and exclusion criteria. We included articles (1) with available full texts, (2) that are published in peer-reviewed journals or conferences and (3) that explore the concepts of zero-trust. Furthermore, we excluded articles that (1) don't include the concept of zero-trust or (2) only briefly mention it without contributing to the state of knowledge. (3) Articles that are not written in English have also been removed. Two authors independently screened titles, abstracts and keywords against the defined selection criteria (agreement rate: 98%). Discrepancies could be resolved in discussions between the authors, resulting in 32 relevant AL items.

Fourth, we performed backward snowballing by examining the reference list of relevant AL items to also include papers that were not covered by previous steps (Webster and Watson, 2002). Potentially relevant papers were evaluated using the inclusions and exclusions criteria. We identified four additional AL items. In sum, the structured literature search resulted in 36 AL items.

3.2.2. *Web search for grey literature*

The web search for GL followed the guidelines of Garousi et al. (2019). We started with the development of a search string. Based on the insights from the database search for AL, we created the following search string:

> *("Zero Trust" OR "Zero-trust") OR ("Software-Defined Perimeter" OR "SDP") OR ("BeyondCorp")*

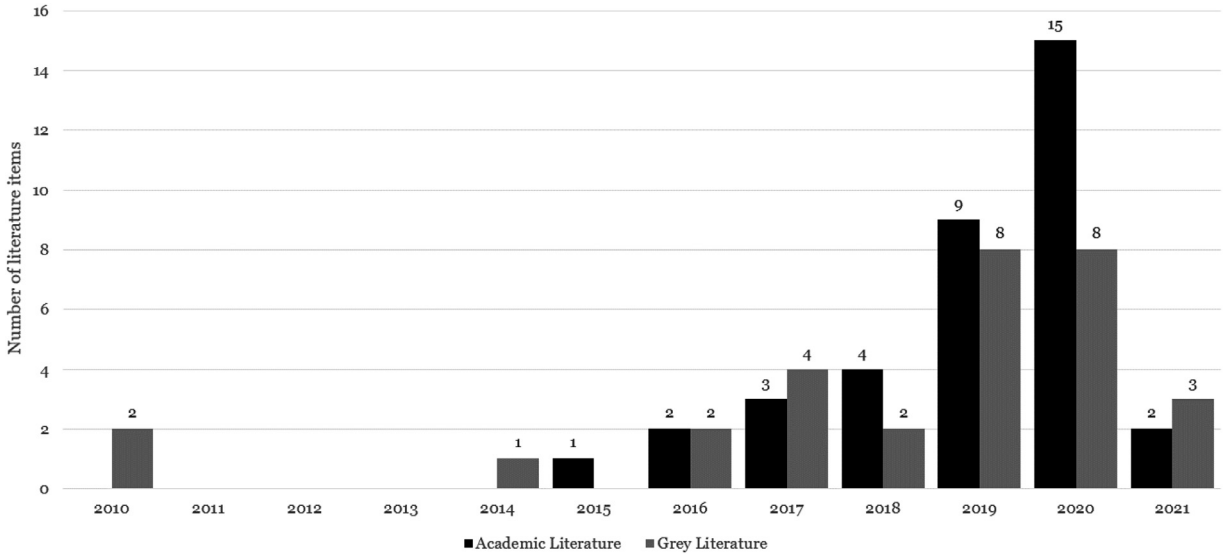

Fig. 3 – Distribution of academic and grey literature over time.

We applied the search string to the Google Search Engine in May 2021. We used a stricter version of the approach presented by Butijn et al. (2020), so that if, for three consecutive pages, less than 25% of the results were relevant, then the search was stopped. Relevance was determined using the following inclusion criteria: (1) The GL item can be assigned to the first tier of GL as defined by Garousi et al. (2019) (i.e. white papers, government reports, magazines, books), (2) the full-text is available, (3) the authors explore the concepts of zero-trust. In addition, GL items with the following criteria were excluded: (1) The GL item doesn't include the concept of zero-trust, (2) the text is written in any other language than English. In total, we identified 53 potentially relevant GL items on the first eleven result pages.

Since GL does not follow a controlled review process, the quality may vary. To understand and improve the quality of the results, Garousi et al. (2019) present a checklist to assess the quality of GL. This checklist consists of eight dimensions (with a total of 20 questions) that assess, for example, the authority of the producer, the methodology, the objectivity, but also the novelty and the impact. We assessed the 53 potentially relevant GL items against these criteria and excluded all items that did not satisfy at least ten of the 20 criteria (Garousi et al., 2019). Appendix A contains an overview of the criteria. A first analysis showed that especially the dimensions methodology and objectivity are rated low. However, this is in line with our expectations, as most white papers come from software providers and consulting companies that aim to communicate the concept of zero-trust to potential customers. In total, we identified 23 relevant GL items that met the requirements.

To also include GL items that were not covered by previous steps, we performed backward snowballing by examining the reference list of relevant items. In addition, we also searched the respective websites where the GL items were published for further relevant articles. For potentially relevant GL items, the inclusion and exclusion criteria were examined and the quality assessed. We identified seven additional GL items. In sum, the web search resulted in 30 relevant GL items. Appendix B provides an overview of all articles used in the literature review.

4. Results

4.1. *Current state of the knowledge*

Considering the publication dates of the body of literature, our results are consistent with previous findings that zero-trust is currently gaining much interest in academia and practice (Yan and Wang, 2020). At the same time, it is clear that zero-trust was developed in practice and subsequently attracted the interest of researchers. Fig. 3 illustrates the distribution of literature items over time.

Our data set contained two GL items that introduced the zero-trust concept in 2010 and one GL item that further explored the topic in 2014, introducing Google's BeyondCorp project. Further, we identified two GL items from 2016, four from 2017 and two from 2018. However, the number of articles increased in recent years to eight GL items from 2019, eight in 2020 and three by the time of the GL search in May 2021. In contrast, our data set included no AL items between 2010 and 2014 on zero-trust. However, we identified one AL item from 2015, two from 2016, three from 2017 and four from 2018. As in practice, interest in zero-trust increased in 2019, resulting in nine AL items published in that year, 15 in 2020 and two by May 2021. Our body of AL consisted of 13 journal publications and 23 conference papers. The GL was mainly published by software providers and consulting companies. Fig. 4 summarises distribution of publication venues and sources.

We found that researchers have focused mainly on conceptual and technical aspects of zero-trust by demonstrat-

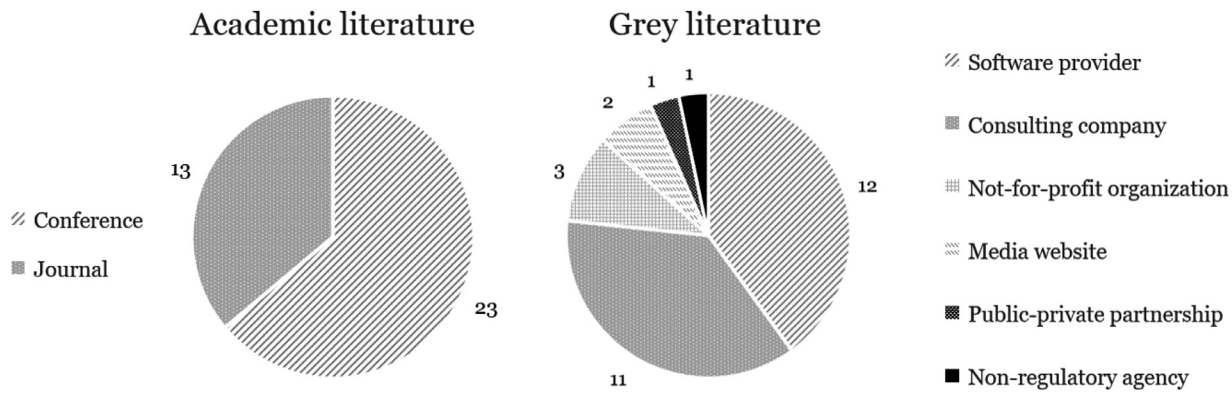

Fig. 4 – Distribution of publication venues and sources.

ing the approach's superiority concerning security and resilience (DeCusatis et al., 2016; Omar and Abdelaziz, 2020; Sallam et al., 2019a). Most authors provided a detailed explanation of zero-trust, highlighting that there is no standard work for reference purposes. Architectural and technical variations of zero-trust were also addressed (e.g. Campbell, 2020; Omar and Abdelaziz, 2020; Singh, Refaey, and Shami, 2020b; Tao et al., 2018). We also found contributions to the application of zero-trust in specific industries (e.g. cloud computing) (Albuali et al., 2020; Mehraj and Banday, 2020) and IoT (Chifor et al., 2019; Samaniego and Deters, 2018). Further, researchers have conducted performance analyses, protocol improvements and comparisons to existing network security solutions (Chen et al., 2019; DeCusatis et al., 2016). While some GL items have addressed implementation strategies, the academic research lacks analyses of organisational aspects in the context of zero-trust. Further, user-related aspects of the concept – including interactions with zero-trust solutions and consequences for the end-users – have not yet been analysed by academic researchers. In contrast, the GL has focused on the advantages of zero-trust and on possible migration strategies (Balaouras et al., 2018; Rose et al., 2020). While there are also contributions concerned with zero-trust solutions' users (Escobedo et al., 2017), these are still rare. Fig. 5 summarises the number of contributions for each research question. Appendix C provides a complete overview of the mapping of the identified literature to the research questions. For each research field, we distinguished between the AL and the GL. Following these distinctions, we will analyse the identified literature for each research question.

4.2. *Activity: design and features*

The activity *design and features* focuses on conceptual considerations in relation to the underlying architecture, industries and users. While architectural aspects of the technology have been examined in detail by researchers, we have lacked considerations of how users interact with zero-trust or its individual features. We will now address all three levels of activity.

4.2.1. *(RQ1) Level of analysis: concept and architecture*

The aim of the intersection between *design and features* and *concept and architecture* is to answer how a zero-trust architecture can be designed and implemented. It addresses differences in features and the structure of zero-trust architectures compared to established security paradigms. Our findings show that most AL items (78 %) in this field address an enhancement of some specific aspect of the concept. Further, while they all address the architecture of zero-trust in detail, there is as yet no standard reference. This stands in parallel to the GL, as practitioners also focus mostly on architectural features of a zero-trust implementation.

Regarding the key features and processes of zero-trust, researchers and practitioners agree that, in zero-trust, trust is not static but dynamic. A central controller is responsible for the authentication (Omar and Abdelaziz, 2020; Puthal et al., 2017; Singh et al., 2020b; Yao et al., 2020) and enforcement of access policies. The controller accepts connection requests initiated by hosts and instructed services or applications to accept requests (Moubayed et al., 2019). The access policies are defined according to the principle of "least privilege" (Campbell, 2020; Chen et al., 2019; Kindervag, 2010b; Omar and Abdelaziz, 2020; Tao et al., 2018) and are applied to all resources throughout the network (American Council for Technology, 2019; Campbell, 2020; Gartner, 2020; Kindervag, 2010b; King et al., 2018; Omar and Abdelaziz, 2020; Rose et al., 2020; Tao et al., 2018; Yan and Wang, 2020), which is segmented into various micro-areas so as to minimise the risk of movement within the network (American Council for Technology, 2019; Kindervag, 2010a; Rose et al., 2020). This approach restricts the discoverability and visibility of resources (Campbell, 2020; Kindervag, 2010b). Further, the logging and inspection of all traffic (Omar and Abdelaziz, 2020; Tao et al., 2018; Yan and Wang, 2020) enables dynamic reactions and the identification of further optimisation potentials (American Council for Technology, 2019; Kindervag, 2010b; Rose et al., 2020).

Five key components are presented to achieve these process flows. First, a single packet authentication (SPA) protocol is used as a passive authentication technique (Omar and Abdelaziz, 2020; Singh, Refaey, and Shami, 2020b). SPA allows the PEP to discard requests from unauthorised sources before establishing a connection (Sallam et al., 2019a). This approach can, for example, significantly reduce the traffic during a DDos attack and thus mitigate the negative effects. Second, all communication between the components is encrypted using Mutual Transport Layer Security (mTLS)

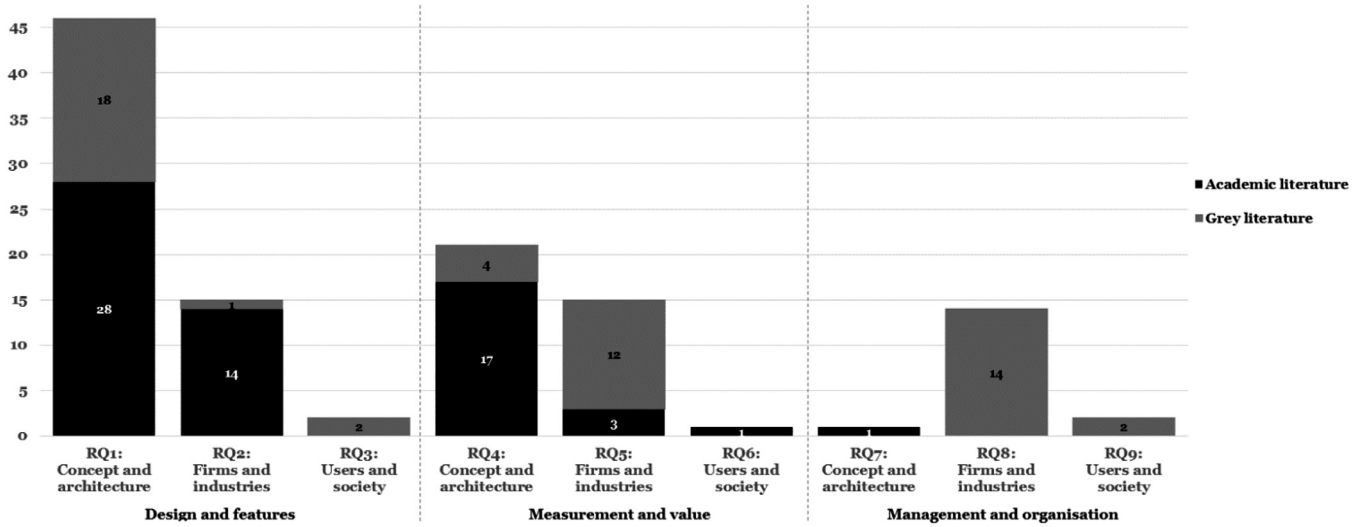

Fig. 5 – Number of contributions for each research question.

(Kumar et al., 2019; Moubayed et al., 2019; Omar and Abdelaziz, 2020; Singh et al., 2020b). Third, dynamic firewalls deny all traffic unless the controller explicitly permits the passing of packets (Kumar et al., 2019; Moubayed et al., 2019; Omar and Abdelaziz, 2020). Fourth, all devices and users are validated (Kumar et al., 2019; Moubayed et al., 2019). Fifth, application traffic is isolated after access has been granted (Kumar et al., 2019; Moubayed et al., 2019; Puthal et al., 2017). DeCusatis et al. (2016) demonstrated the principles using a transport access control system. Further, Ward and Beyer (2014) as well as Osborn et al. (2016) demonstrated how these components and principles can be applied in practice by describing Google's BeyondCorp approach.

While a consensus on the basic components prevails, the articles differ in the specific focus of design-related aspects. Some authors focus on comparing zero-trust to traditional access control concepts (Omar and Abdelaziz, 2020; Puthal et al., 2017) and have tried to demonstrate the superiority of zero-trust. While authors focused on comparisons with traditional concepts, we could not identify literature on extensions of zero-trust with further emerging concepts such as user-managed verifiable credentials for access management. We also found propositions on architectural variations. For instance, Ahmed et al. (2020) address access control to sensitive data, and Garbis and Koilpollai (2019) demonstrate zero-trust architectures for the use cases: internal server structures, Infrastructure-as-a-Service offers, or IoT networks (Xiaojian et al., 2021). Sallam et al. (2019b) as well as Chifor et al. (2019) focus on smart home networks and demonstrate the applicability to smart-home infrastructures. Regarding the design process of zero-trust, Vanickis et al. (2018) state that the most important design trade-off regarding policy enforcement is the operational need for access vs. security risks. Further design principles include compatibility, manageability, distribution and customisation (Chen et al., 2019).

In sum, the academic and practise-oriented literature on *design and features* as well as *concept and architecture* barely differ. The only difference we identified is that the AL addressed improvements in relation to specific aspects of the concept more often than the practice-oriented literature. However, our analysis reveal that both researchers and practitioners agree on key features and components of a zero-trust architecture.

4.2.2. *(RQ2) Level of analysis: firms and industries*

The intersection of *firms and industries* and *design and features* focuses on the practical application of the concept. It addresses zero-trust features' effects on businesses and industries and their processes. We found that the AL mainly addresses conceptual aspects for the context of firms and industries, while practitioners address application areas for which zero-trust is particularly suitable, including organisations collaborating across their boundaries or with open interfaces for customers (Rose et al., 2020). Similar to the AL, there is a focus on securing the use of external services, for instance from cloud providers (Rose et al., 2020).

Regarding conceptual aspects, the academic authors focus on the practical applicability of SDP for corporate networks and highlight that it reduces network reconnaissance scans and network eavesdropping (Chen et al., 2019). Regarding the implementation process of zero-trust, the authors suggest a risk evaluation. This may include the creation of a graph that maps the organisation's mission through the processes to IT assets. For each verification, the graph is used to dynamically calculate a resource's criticality to the whole organisation and to better protect important resources (Lee et al., 2017). Further, Balachandran et al. (2020) discuss the issue that customers of SDP network services have little to no information about the underlying network provided by a vendor. Therefore, they present a blockchain-based framework that provide more auditing capabilities to customers (Balachandran et al., 2020). The academic authors have also put forward conceptual propositions for the cloud environment and for IoT. Regard-

ing the former, the zero-trust concept is considered specifically applicable, since cloud services are offered remotely, making protection mechanisms for resources crucial (Yan and Wang, 2020). This also applies to volunteer cloud computing, where a user makes the power of one's computer available to other users. Regarding conceptual propositions, authors present an approach for a zero-trust-based authentication system (Mehraj and Banday, 2020). Also, a zero-trust identity management model has been presented, which includes behavioural analysis in addition to multifactor authentication to determine a node's trustworthiness (Albuali et al., 2020). Further, zero-trust may be particularly important for the security of IoT applications, as it often involves networks with a growing number of devices requiring flexible security concepts (Yan and Wang, 2020). For example, Sateesh and Zavarsky (2020) present an SDP architecture for Vehicular Adhoc Networks to enable the spontaneous creation of a network between vehicles. Zero-trust is even considered a prerequisite for the "Internet of Everything" (Balfour, 2015). Authors have implemented proofs of concept, which demonstrate zero-trust's applicability for IoT (Chen et al., 2019; Dimitrakos et al., 2020; Puthal et al., 2020; Zaheer et al., 2019). Also, smart home applications are considered to benefit from zero-trust, because different devices on a network are used to communicate with a cloud service. To ensure that access to the service from unauthorised nodes in the network is blocked, a user's smartphone may serve as an SDP controller, mediating the communication between IoT and the cloud (Chifor et al., 2019). To overcome challenges relating to a central verification instance, Samaniego and Deters (2018) present blockchain-based middleware that handles access validation in a decentralised way. Further, zero-trust principles can also be used to transfer sensitive data. Sultana et al. (2020) developed a framework that uses zero-trust and blockchain technology to enable the secure exchange of sensitive medical images, e.g. x-ray data.

In contrast to the AL, which addresses conceptual issues for specific application areas, practitioners focus on use cases that zero-trust is particularly suitable for, including organisations that collaborate across boundaries or that have open interfaces for customers (Rose et al., 2020). There was a special focus on securing the use of cloud services, as organisations are increasingly using external services (Rose et al., 2020).

In sum, the focus of the AL and the GL clearly diverged for the intersection of *firms and industries* and *design and features*. While the former focuses on conceptual aspects in relation to the application of zero-trust in the industrial context, the GL addresses concrete usage cases of zero-trust.

4.2.3. *(RQ3) Level of analysis: users and society*

The intersection of the activities *design and features* and *users and society* addresses the interactions between end-users creating zero-trust concepts and the design of features to appeal to users. These aspects are crucial for the success of new concepts and technologies, because they affect the willingness to use (Venkatesh et al., 2003).

However, we found no AL that addressed these aspects, and practitioners have not yet focused on these topics either. We identified only two articles by Google Research, which published user-related findings from the implementation of BeyondCorp. Cittadini et al. (2016) argue that the handling of security certificates and possible problems can lead to frustration among users. Accordingly, to reduce complexity for the users, settings should be pre-loaded and automatically updated (Escobedo et al., 2017). Further, traceability can be increased by providing brief explanations about reasons for access denials. Finally, to minimise user frustration from the outset, potential conflicts and problems should be anticipated and response measures should be put in place (Escobedo et al., 2017). Despite these first observations, the field largely remains unexplored.

4.3. *Activity: Measurement and value*

The activity *measurement and value* focuses on the benefits of zero-trust. This includes quantifying zero-trust implementations' value for various stakeholders. Our analysis shows that most AL that addresses the underlying activity focuses on the *concept and architecture* level. Specifically, performance tests highlight the concept's superiority compared to traditional security concepts. These tests are predominantly conducted using experimental platforms based on physical networks (Chen et al., 2019; Kumar et al., 2019; Refaey et al., 2019; Sallam et al., 2019a), while DeCusatis et al. (2016) use cloud test beds. In contrast to AL, the GL focuses mainly on zero-trust's benefits to firms and industries. However, the benefits for users and for society are not addressed.

4.3.1. *(RQ4) Level of analysis: concept and architecture*

The intersection of the research field *concept and architecture* with the activity *measurement and value* addresses the value propositions and limitations of the zero-trust concept compared to traditional security concepts independent of the application domain. Our analysis shows that both the AL and the GL mostly evaluated the concept's value in relation to its security and performance. While most researchers highlight zero-trust's superiority, very few point out its shortcomings.

Experiments evaluating the security of zero-trust usually simulate an attack on a specific zero-trust implementation while measuring the proposed system's resilience. Evaluation experiments are mostly done by academic researchers. However, GL provide a list of preventable attacks using zero-trust including access on the basis of false or stolen credentials, breached devices, DDoS or remote surveillance (Koilpillai, 2017; Koilpillai et al., 2019; Koilpillai and Murray, 2020). The authors usually base those claims on the conceptual setup of architectures following the zero-trust paradigm (Koilpillai, 2017; Koilpillai et al., 2019; Koilpillai and Murray, 2020). The majority of AL focuses on highlighting zero-trust's resilience against Denial-of-Service (DoS) attacks, which is demonstrated by measuring network traffic throughout (Chen et al., 2019; DeCusatis et al., 2016; Kumar et al., 2019; Refaey et al., 2019; Sallam et al., 2019a, 2019b; Singh et al., 2020a; Singh et al., 2020b). In addition, Eidle et al. (2017) measure the response time in blocking IP addresses. However, as Sallam et al. (2019a) note, indirect DoS attacks from inside a network can still be performed on architectures based on zero-trust. Further, researchers simulate port scanning attacks and demonstrate that no information about open ports is shown

(Moubayed et al., 2019; Sallam et al., 2019a; Singh et al., 2021; Singh et al., 2020a). Also, zero-trust's resilience against IP spoofing (Sallam et al., 2019b), sniffing attacks (Balfour, 2015), intercept worms, and network scanning attacks (Chen et al., 2019) is demonstrated. Further, reconnaissance scans reveal no relevant information to an attacker (DeCusatis et al., 2016).

In the context of above-mentioned security evaluation experiments, the system's performance under attack is also evaluated. The consensus is that registered performance hits are negligible (DeCusatis et al., 2016; Moubayed et al., 2019; Singh et al. 2020b). According to Sallam et al. (2019a), 75% of network throughput can be maintained during a DoS and a port scanning attack. Also Singh et al. (2021) found that CPU usage under attack is not affected significantly. Furthermore, connection setup time is measured in comparison to traditional network solutions (Kumar et al., 2019; Refaey et al., 2019; Sallam et al., 2019a; Singh et al., 2021; Singh, Refaey and Koilpillai, 2020a). It generally may be concluded that the marginal latency overhead is caused by end-to-end rule processing. Sallam et al. (2019b) conclude that zero-trust has insignificant effects on the network throughput in the context of smart home networks.

While predominantly AL highlights zero-trust's benefits concerning security and performance, the authors rarely address the system's shortcomings. So far, known disadvantages of the systems include only additional flow overhead (Chen et al., 2019; Sateesh and Zavarsky, 2020) the prolonged time for clients to connect to the server than in traditional systems (Moubayed et al., 2019). Further, in Pan and Yang (2018) pointed out that it is "still an open issue for SDN to prevent DoS attack, spoofing attack and malicious injection attack" (p. 2). Only Kumar et al. (2019) specifically list the system's benefits and disadvantages. Accordingly, while zero-trust is highly scalable, the fact that one certificate authority provides and restricts access to services also has drawbacks: The single location of a revocation list causes design complications, raises initial costs, and increases complications when the certificate authority is compromised. Accordingly, there is no consensus on whether zero-trust is the most superior security strategy. While Sallam et al. (2019b) state that zero-trust provides a "complete secure and flexible environment" (p. 1993), Kumar et al. (2019) note that while zero-trust provides protections against a wide range of attacks, it cannot ensure complete protection. GL also barely addresses the disadvantages of zero-trust. Riley et al. (2020) also argue that if there is not enough redundancy, the PEP can become a single point of failure, which can result in latency or downtimes. Although the zero-trust provides several benefits, there are also concerns and potential issues. Thus, it is hard to draw a final conclusion on the concept's benefits.

In sum, mainly the AL items address the intersection of *concept and architecture* and *measurement and value*. While the authors agree on the attacks that can be prevented by zero-trust, only some mention that there may also be drawbacks from using zero-trust. However, these shortcomings have not yet been addressed in detail.

4.3.2. *(RQ5) Level of analysis: firms and industries*

The intersection of *measurement and value* and *firms and industries* addresses the benefits of a zero-trust strategy for firms and industries. Our results show that there are first findings from AL, but GL in particular addresses the benefits for firms and industries. However, both researchers and practitioners do not discuss the possible shortcomings.

Pan and Yang (2018) state that zero-trust is a business enabler of secure IoT, while Sallam et al. (2019a) point out that the concept may reduce organisations' operating and capital expenditures. Based on a case study of a zero-trust implementation, Dhar and Bose (2020) show that zero-trust increases enterprise security against attacks by removing a trusted area and segmenting the network. However, there is a lack of empirical data to measure and verify these effects.

Considering that most authors of GL are interested in advertising their solutions and highlighting the benefits for organisations, the finding that they address mostly the benefits for organisations is unsurprising. The benefits mentioned can be distinguished into operational, security-, management- and cost-related aspects. Regarding the operational benefits, zero-trust is posited to enable agile IT and business operations (Cunningham and Pollard, 2017; Garbis and Koilpollai, 2019; Gigamon, 2020), because it can meet the requirements of modern business and operation models: First, zero-trust networks are modular and thus provide scalability for growing organisations. Second, they enable secure virtualisation and multi-tenant environments, since their segmentation suits the requirements of cloud and Software-as-a-Service (SaaS) strategies (Garbis and Koilpollai, 2019; Kindervag, 2010a). Also, the adoption of IoT and schemes such as BYOD are facilitated (Cunningham and Pollard, 2017). Third, zero-trust provides secure mobile working, because user mobility and remote access are key principles of zero-trust (Osborn et al., 2016). Fourth, owing to its platform agnosticism, any resource type can be used, enabling device interoperability (Kindervag, 2010a). Cunningham and Pollard (2017) even point out that zero-trust is the "enabler of digital business transformation" (p.10).

The security-related benefits mentioned by authors are putting into context the above-mentioned performance evaluations from the field *measurement and value* and *concept and architecture*. Specifically, zero-trust has two primary operational benefits. First, it reduces the attack surface and improves threat suppression (American Council for Technology, 2019). Second, it allows monitoring network traffic for malicious activities (Cunningham and Pollard, 2017; Prisma, 2019), which increases data awareness and limits the chances of a successful attack in the first place. In case of a successful attack, the damage from data breaches is minimised, because exposed resources are limited (Cunningham and Pollard, 2017; Schulze, 2019, 2020). Also, the spread of malware from end-user systems to particularly sensitive systems and data centre resources is reduced (Cunningham and Pollard, 2017; Gigamon, 2020).

Zero-trust's management-related benefits include lower operational costs (American Council for Technology, 2019; Cunningham and Pollard, 2017; Garbis and Koilpollai, 2019; Kindervag, 2010a). First, network management costs can be kept to a minimum, since changes such as access modifications are easy to do (Cunningham and Pollard, 2017). Second, higher network security leads to lower costs of data breaches – including lost productivity, remediation costs, credit monitoring costs, and costs related to reputational damage and law-

suits (American Council for Technology, 2019). Third, owing to network segmentation, only distinct parts of the network underlie compliance assessments, which reduces the compliance scope and costs (American Council for Technology, 2019; Cunningham and Pollard, 2017; Garbis and Koilpollai, 2019; Kindervag, 2010a). Similarly, the management of vulnerabilities is reduced (Cunningham and Pollard, 2017).

In sum, organisation-related benefits are primarily addressed by GL. The authors agree that implementing zero-trust has advantages for an organisation's operations, security and management, which result in lower costs. In parallel to the dimensions *measurement and value* as well as *concept and architecture*, shortcomings for organisations have not been addressed by either the AL or GL.

4.3.3. *(RQ6) Level of analysis: users and society*

The intersection of *measurement and value* and *users and society* addresses the benefits and downsides of the zero-trust system specifically from an end-user perspective. However, only one AL item slightly touches on user-related aspects by pointing out that the structure of a central certification authority can have negative effects on usability, since processes may become more complicated for users (Singh, Refaey, and Shami, 2020b). The end-user perspective is not considered by GL.

4.4. *Activity: management and organisation*

The *management and organisation* activity addresses management-related issues and organisational aspects of zero-trust. We found that the academic research neither addresses skills and human resources that are vital for the zero-trust paradigm, nor answers the question how zero-trust can be achieved in organisations and which organisational issues they must deal with. In contrast, the GL examines the latter question and also focuses on organisational transition strategies. Regarding user-related aspects, practitioners acknowledge that zero-trust leads to new challenges concerning data security and regulation, since all traffic is examined. However, detailed considerations are missing.

4.4.1. *(RQ7) Level of analysis: concept and architecture*

Similar to other new system implementations, the introduction of zero-trust in organisations will challenge leaders and employees. Both the implementation and the maintenance of the system requires skilled talent, including system architects or administrators managing policy rules (Dhar and Bose, 2020). Further, project managers may be necessary to support the transition process to the new security architecture, while legal assistance should clarify relevant legal issues. Although Dhar and Bose (2020) discuss the topic briefly, we have not found any AL or GL to gain knowledge into this area.

4.4.2. *(RQ8) Level of analysis: firms and industries*

The intersection of the activities *management and organisation* and *firms and industries* addresses the measures that organisations must consider in order to be able to successfully implement zero-trust. This includes inter-organisational structures, the transition process to a zero-trust implementation, and how emerging data protection concerns can be addressed. We found no AL on these aspects.

In contrast, practitioners provide conceptual approaches to the factors influencing a successful transition process from current solutions to zero-trust implementations. Since the adaptation of zero-trust is a complex process (Deloitte, 2021; Tufin, 2021), most suggest a gradual transition. Many of these contributions are published by consulting firms. The findings can be grouped into five categories. First, the support of all organisational units, including top management, is crucial (Gartner, 2020; Peck et al., 2017). Second, the current IT landscape, its dependencies and the traffic must be analysed (Balaouras et al., 2018; Gartner, 2020; Küderli et al., 2020; Osborn et al., 2016; Peck et al., 2017; Rose et al., 2020; Turner et al., 2021). Third, these insights can be used to develop a suitable zero-trust architecture (Balaouras et al., 2018; Küderli et al., 2020; Rose et al., 2020). Its access policies should be driven by the principle of least privilege (Balaouras et al., 2018; Küderli et al., 2020; Rose et al., 2020; Turner et al., 2021). Fourth, regarding the implementation of zero-trust, practitioners suggest starting with few low-risk resources (Rose et al., 2020) as a test environment to prevent the disruption of operations (Gartner, 2020; Osborn et al., 2016). Fifth, continual monitoring and automation (Balaouras et al., 2018; Küderli et al., 2020) is considered crucial to detect suspicious behaviours (Küderli et al., 2020) and to gradually improve the architecture (Balaouras et al., 2018). King et al. (2018) also note that the maintenance measures of a zero-trust network should be defined explicitly.

Besides making conceptual suggestions, Google Research describe concrete experiences (Peck et al., 2017; Ward and Beyer, 2014) and learnings (Osborn et al., 2016) from the implementation of BeyondCorp. First, data quality is key. Small inconsistencies such as spelling mistakes or missing information owing to maintenance and the replacement of devices can result in loss of connection (Osborn et al., 2016). Second, communication with employees is crucial so as to manage expectations (Osborn et al., 2016) and for sensitisation (Balaouras et al., 2018). Third, support options such as self-service desks (Peck et al., 2017) should be provided just as an emergency plan in the case of failure (Osborn et al., 2016).

In sum, there are large divergences between the AL and the GL. While no AL addresses this field, the GL provides both conceptual approaches for successfully implementing zero-trust and learnings from this.

4.4.3. *(RQ9) Level of analysis: users and society*

This field describes organisational activities that must be considered in the context of end-users and society. Although research has not yet addressed this topic, the GL presents first critical observations.

The importance of these activities is highlighted by a Gigamon survey. Accordingly, one of the challenges for the adoption of zero-trust is that employees may feel inspected and controlled (Gigamon, 2020). This concern is caused by the continual monitoring and checking of traffic, which gives rise to new data privacy concerns and challenges (American Council for Technology, 2019). These concerns may affect employees' willingness to adopt zero-trust, but also are directly related to

legal regulations that may have organisational consequences. However, this field remains unexplored.

5. Discussion and avenues for future research

Zero-trust is a novel concept that is rapidly gaining relevance. In order to support the maturity of this research field, we systematically summarise the current state of knowledge from research and practice. We develop a research framework to structure the results and to identify unexplored areas. From these findings, we may derive avenues for future research. In this section we highlight gaps in the literature and open research areas for each intersection of an activity and a level of analysis.

First, regarding *design and features* as well as *concept and architecture,* we found various propositions of architectural variations on how to design and implement zero-trust. However, researchers mostly address small networks, such as organisational or private home networks. In contrast, architectures for large-scale networks – for instance smart cities – are missing (Yan and Wang, 2020). While researchers suggest that following zero-trust principles results in a highly scalable infrastructure, an architecture for such large-scale networks has not yet been proposed, demonstrated or tested. In addition, to decrease uncertainty with respect to the novelty of the concept insights on the actual experience with zero-trust networks should be published. Also, concerning *design and features* as well as *firms and industries*, we found several approaches how firms can utilise zero-trust concepts. The current literature predominantly focuses on specific industries. However, other industries also need to be investigated. For instance, we found no research into sectors such as the healthcare or energy, where security is particularly important. Although Sultana et al. (2020) present a framework for data exchange, there is a lack of approaches for the protection of critical infrastructure. This may be caused by the criticality of these infrastructures and concerns about adapting a new and not yet fully explored technology. However, as experience increases and the concept's suitability is further demonstrated in practice, both researchers and practitioners should also address securing critical infrastructures, because the societal impacts from security issues in these sectors can have large-scale effects. Regarding *design and features* as well as *users and society*, the question how zero-trust features affect interaction and adoption remains unanswered. It must be clarified how these interactions should be designed. To do so, researchers may rely on findings from the human-computer interaction domain. Design science research may represent an appropriate method for addressing these aspects (Adikari et al., 2011). Ideally, researchers provide empirical results on the design of interactions with networks based on zero-trust, which may serve as a basis for practitioners in the creation of zero-trust solutions.

Second, the predominant AL body on the fields *measurement and value* and *concept and architecture* provides a fairly one-dimensional view on the value propositions and limitations of zero-trust, highlighting zero-trust's benefits but neglecting its downsides. For instance, the literature provides a substantial basis on zero-trust's resilience against several attacks from outside a network, while the potential for attacks from inside a zero-trust network remains unclear (Sallam et al., 2019a; Singh, Refaey, and Shami, 2020b). Thus, potential disadvantages of architectures following the zero-trust paradigm compared to traditional perimeter-based networks have not been addressed so far. Regarding *measurement and value* in the context of *firms and industries* and the added value for organisations, mainly the GL addresses zero-trust's benefits and usage cases. While providers of zero-trust have a strong incentive to highlight benefits, independent research has not yet addressed the concept's organisational value. As this aspect highlights the relative immaturity of research on zero-trust, researchers should empirically evaluate the concept's value propositions (using experimental data) as implementations mature. Thus, zero-trust's disadvantages should also be quantifiable. For example, the costs of replacing existing legacy systems should also be examined. However, this also includes the identification of existing and new threats to zero-trust as well as the defence thereof. While researchers argue for the superiority of zero-trust with respect to various known attacks, new attack scenarios should be investigated. Further, value propositions for *users and society* lack substantiated insights. While one AL item briefly addresses potential complications for users (Singh et al., 2020b), we still lack a structured and well-grounded overview over zero-trust's benefits and disadvantages for end-users. The observation that users are not addressed by practitioners may be caused by providers' predominant focus on organisations as their primary customers. This further highlights the importance of independent researchers considering user-related aspects. It is very important to address zero-trust architectures' (potential) downsides, which may include data protection concerns and various measures, before widespread adoption takes place.

Third, the activity *management and organisation* is addressed the least. Regarding research into *concept and architecture*, we found no AL or GL that addresses the skills and human resources required to develop, provide and operate zero-trust solutions. Also, in the context of *firms and industries* it remains mostly unclear how organisations should organise, govern, fund and develop their zero-trust capabilities. Organisational research questions include necessary adaptations of the corporate culture. Further, we still lack concrete examples that demonstrate the implementation of zero-trust. While Google Research provide first information on its implementation of BeyondCorp, a more diversified picture will be necessary for the maturity and advancement of zero-trust. Assessments related to the implementation of the zero-trust paradigm also include action and process models as well as information on the maintenance of zero-trust networks. Similarly, to the activities *design and feature* as well as *measurement and value*, the *users and society* field remains untouched. While the GL provides first insights into employees' privacy concerns, neither researchers nor practitioners address how to balance user privacy and legal demands. Widespread adoption of the zero-trust paradigm can only be ensured if researchers and practitioners holistically observe user-related challenges. Accordingly, we highlight the need to investigate possibilities for traffic analyses and monitoring without interfering with users' privacy. Further, this aspect also relates to legal is-

Table 2 – Exemplary future research areas based on the classification of the current literature.

Level of analysis	Activities Design and features	Measurement and value	Management and organisation
Concept and architecture	Applicability of zero-trust concepts to large-scale networks (e.g. smart cities)	Shortcomings of the zero-trust concept compared to traditional solutions	Examining the skills that are necessary for the conceptual and architectural development of zero-trust concepts
	Studies on actual experience with zero-trust networks	Identification and defence against new and existing threats to the zero-trust concept	
Firms and industries	Examining zero-trust concepts to protect critical energy infrastructure	Quantifying the benefits and disadvantages (e.g. monetary) of zero-trust	Development of strategies for successful deployment of and migration to a zero-trust environment
	Design of zero-trust concepts especially for the health-care sector	Measuring the long-term return on investment of zero-trust	Studies on the corporate culture needed for the introduction of zero-trust
Users and society	Studies on user acceptance of zero-trust concepts	Exploring the benefits of zero-trust concepts for users and for society	Methods to analyse and monitor network traffic while preserving user privacy
	Investigation of certain zero-trust features and their positive or negative impacts on user perceptions	Exploring the disadvantages of zero-trust concepts for users and for society	Analysing legal requirements that must be considered when introducing and operating zero-trust

sues. Interdisciplinary research should identify legal boundaries. Table 2 provides an overview over exemplary research questions and can serve as an initial starting point for future research.

Overall, our findings reveal that both academia and practice intensely address conceptual issues of zero-trust. However, divergences prevail regarding practice-oriented research questions, which are predominantly addressed by the GL. Further, both the current academic and the practice-oriented literature focus on benefits and thus provide a rather one-sided view on zero-trust. Also, user-related aspects are not addressed intensively by research or practice.

6. Conclusions

Zero-trust is posited as a concept providing more secure networking compared to traditional approaches (DeCusatis et al., 2016; Koilpillai, 2017; Koilpillai and Murray, 2020). Despite its potential, there are still some unanswered questions that hinder its widespread acceptance and adoption. However, researchers can make valuable contributions by systematically gaining new knowledge about zero-trust. To support research in this endeavour, we have summarised the existing knowledge on zero-trust and have identified avenues for future research, conducting a multivocal literature review that analysed both academic and practice-oriented publications. We have developed a research framework for the zero-trust concept in order to investigate the research area in a structured way from multiple perspectives. Based on this research framework, we derived nine research questions to guide our multivocal literature review, to organise the literature and to outline avenues for future research.

We have contributed to the literature by summarizing and structuring the current literature on zero-trust. Further, we present a research framework to organise the research area. We thus provide a multi-perspective overview of the current state of knowledge on zero-trust. Pointing out the most recent insights also provides a basis for future researchers engaging in the topic. Our approach has allowed us to highlight avenues for future research that can enhance this research field's maturity. Further, we have contributed by analysing the convergences and divergences of the academic and the practice-oriented research on zero-trust, and have highlighted aspects that the academic research has so far neglected. These insights also have important implications for practice. First, we have provided a basis for practical applications by providing a conceptual summary and consolidation and pointing out relevant literature for implementation and practice. Second, we have enabled the application of insights stemming from AL in practice.

Despite following a rigorous research methodology, our findings are subject to limitations and threats to validity. First, the generalisability of our results may be limited because we might have missed some relevant papers. Zero-trust represents a novel concept and the terminology is still evolving. Therefore, our search string may not cover all relevant or related concepts. Also, papers may still be in the publication process, which is why they could not be included in the selection. To address these issues, we used different search terms to cover different applications and implementations of the zero-trust paradigm. Given the broad scope of our search, the inclu-

sion of different sources (academic and grey literature) and an established search strategy, we are confident that our results reflect the current state of the knowledge on zero-trust. Second, the process of manual information assessment and extraction could lead to inaccuracies and subjectivity. To address this concern, we followed the well-established guidelines for multivocal literature reviews by Garousi et al. (2019). At the same time, the assessments of relevance and quality were performed by two authors independently. Third, our research framework is a simplification of the real world. Although the framework has already been applied in other domains, i.e. blockchain and social media, there may be other areas and perspectives that could be interesting to consider. An evaluation of the framework may highlight further potentials for improvement.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Christoph Buck: Conceptualization, Supervision, Writing – review & editing. **Christian Olenberger:** Conceptualization, Data curation, Formal analysis, Writing – original draft. **André Schweizer:** Conceptualization, Supervision, Writing – review & editing. **Fabiane Völter:** Conceptualization, Data curation, Formal analysis, Writing – original draft. **Torsten Eymann:** Supervision, Writing – review & editing.

Acknowledgements

This project has received funding from the Bavarian Ministry of Economic Affairs, Regional Development and Energy under the grant agreement 'SiZero, No: DIK-2003-0032'. The funding source was not involved in the collection, analysis and interpretation of data, in the writing of the report, and in the decision to submit the article for publication.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.cose.2021.102436.

Appendix A. Overview of the criteria to assess grey literature quality (by Garousi et al. (2019))

Criteria	Questions
Authority of the producer	Is the publishing organization reputable? Is an individual author associated with a reputable organization? Has the author published other work in the field? Does the author have expertise in the area? (e.g. job title principal software engineer)
Methodology	Does the source have a clearly stated aim? Does the source have a stated methodology? Is the source supported by authoritative, contemporary references? Are any limits clearly stated? Does the work cover a specific question? Does the work refer to a particular population or case?
Objectivity	Does the work seem to be balanced in presentation? Is the statement in the sources as objective as possible? Or, is the statement a subjective opinion? Is there vested interest? E.g., a tool comparison by authors that are working for particular tool vendor Are the conclusions supported by the data?
Date	Does the item have a clearly stated date?
Position	Have key related GL or formal sources been linked to / discussed?
Novelty	Does it enrich or add something unique to the research? Does it strengthen or refute a current position?
Impact	Number of citations, Number of backlinks, Number of social media shares. For us, the criterion is fulfilled if there is at least one reference: Tool for backlinks: https://www.seoreviewtools.com/valuable-backlinks-checker/ Tool for social media shares: https://www.sharedcount.com/
Outlet type	Fulfilled for 1st tier GL (measure=1): High outlet control/ High credibility: Books, magazines, theses, government reports, white papers

Appendix B.1. Overview of the academic literature

Author(s)	Year	Title	Published in	Publication Type	H-Index	Ranking*	Classification into Framework
Balfour, R. E.	2015	Building the "Internet of Everything" (IoE) for first responders	2015 Long Island Systems, Applications and Technology Conference	Conference Paper	-	Unranked	Design and Features (Concept and Architecture)
Bertino, E.; Choo, K. R.; Georgakopolous, D.; Nepal, S.	2016	Internet of Things (IoT): Smart and Secure Service Delivery	ACM Transactions on Internet Technology	Journal Editorial	56	Q1 (Computer Networks and Communications)	Design and Features (Concept and Architecture)
DeCusatis, C.; Liengtiraphan, P.; Sager, A.; Pinelli, M.	2016	Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication	2016 IEEE International Conference on Smart Cloud	Conference Paper	-	Unranked	Design and Features (Concept and Architecture), Measurement and Value (Concept and Architecture)
Eidle, D.; Ni, S. Y.; DeCusatis, C.; Sager, A.	2017	Autonomic security for zero trust networks	IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference	Conference Paper	-	Unranked	Design and Features (Concept and Architecture), Measurement and Value (Concept and Architecture)
Lee, B.; Vanickis, R.; Rogelio, F.; Jacob, P.	2017	Situational Awareness based Risk-Adapatable Access Control in Enterprise Networks	Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security	Conference Paper	-	C	Design and Features (Firms and industries)
Puthal, D.; Mohanty, S.P.; Nanda, P; Choppali, U.	2017	Building Security Perimeters to Protect Network Systems Against Cyberthreats [Future Directions]	IEEE Consumer Electronics Magazine	Journal Paper	31	Q1 (Electrical and Electronic Engineering)	Design and Features (Concept and Architecture)
Pan, J.; Yang, Z.	2018	Cybersecurity Challenges and Opportunities in the New "EdgeComputing + IoT" World	Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization	Conference Paper	-	Unranked	Design and Features (Concept and Architecture), Measurement and Value (Firms and industries)
Samaniego, M.; Deters, R.	2018	Zero-Trust Hierarchical Management in IoT	2018 IEEE International Congress on Internet of Things	Conference Paper	-	Unranked	Design and Features (Concept and Architecture)
Tao, Y.; Lei, Z.; Ruxiang, P.	2018	Fine-Grained Big Data Security Method Based on Zero Trust Model	IEEE 24th International Conference on Parallel and Distributed Systems	Conference Paper	-	B	Design and Features (Concept and Architecture)
Vanickis, R.; Jacob, P.; Dehghanzadeh, S.; Lee, B.	2018	Access Control Policy Enforcement for Zero-Trust-Networking	29th Irish Signals and Systems Conference	Conference Paper	-	Unranked	Design and Features (Concept and Architecture)
Assunção, P.	2019	A Zero Trust Approach to Network Security	Proceedings of the Digital Privacy and Security Conference 2019	Conference Paper	-	B	Design and Features (Concept and Architecture)

(*continued on next page*)

Author(s)	Year	Title	Published in	Publication Type	H-Index	Ranking*	Classification into Framework
Chen, Y.; Hu, H.; Cheng, G.	2019	Design and implementation of a novel enterprise network defense system bymaneuveringmulti-dimensional network properties	Frontiers of Information Technology and Electronic Engineering	Journal Paper	32	Q2 (Computer Networks and Communications)	Design and Features (Concept and Architecture, Firms and industries), Measurement and Value (Concept and Architecture)
Chifor, B.; Arseni, S.; Matei, I.; Bica, I.	2019	Security-Oriented Framework for Internet of Things Smart-Home Applications	22nd International Conference on Control Systems and Computer Science	Conference Paper	-	Unranked	Design and Features (Concept and Architecture, Firms and industries)
Kumar, P.; Moubayed, A.; Refaey, A.; Shami, A.; Koilpillai, J.	2019	Performance Analysis of SDP For Secure Internal Enterprises	2019 IEEE Wireless Communications and Networking Conference	Conference Paper	-	B	Design and Features (Concept and Architecture), Measurement and Value (Concept and Architecture)
Moubayed, A.; Refaey, A.; Shami, A.	2019	Software-Defined Perimeter (SDP): State of the Art Secure Solution for Modern Networks	IEEE Network	Journal Paper	129	Q1 (Computer Networks and Communications)	Design and Features (Concept and Architecture), Measurement and Value (Concept and Architecture)
Refaey, A.; Sallam, A.; Shami, A.	2019	On IoT applications: a proposed SDP framework for MQTT	Electronics Letters	Journal Paper	146	Q2 (Electrical and Electronic Engineering)	Design and Features (Concept and Architecture, Firms and industries), Measurement and Value (Concept and Architecture)
Sallam, A.; Refaey, A.; Shami, A.	2019	On the Security of SDN: A Completed Secure and Scalable Framework Using the Software-Defined Perimeter	IEEE Access	Journal Paper	127	Q1 (Computer Science (miscellaneous))	Design and Features (Concept and Architecture), Measurement and Value (Concept and Architecture, Firms and industries)
Sallam, A.; Refaey, A.; Shami, A.;	2019	Securing Smart Home Networks with Software-Defined Perimeter	15th International Wireless Communications and Mobile Computing Conference	Conference Paper	-	Unranked	Design and Features (Concept and Architecture), Measurement and Value (Concept and Architecture)
Zaheer, Z.; Chang, H.; Mukherjee, S.; Van der Merwe, J.	2019	eZTrust: Network-Independent Zero-Trust Perimeterization for Microservices	Proceedings of the 2019 ACM Symposium on SDN Research	Conference Paper	-	Unranked	Design and Features (Concept and Architecture), Measurement and Value (Concept and Architecture)
Ahmed, I.; Nahar, T.; Urmi, S. S.; Taher, K. A.	2020	Protection of Sensitive Data in Zero Trust Model	2020 Proceedings of the International Conference on Computing Advancements	Conference Paper	-	Unranked	Design and Features (Concept and Architecture)

(*continued on next page*)

Author(s)	Year	Title	Published in	Publication Type	H-Index	Ranking*	Classification into Framework
Albuali, A.; Mengistu, T. M.; Che, D.	2020	ZTIMM: A Zero-Trust-Based Identity Management Model for Volunteer Cloud Computing	2020 International Conference on Cloud Computing	Conference Paper	-	B	Design and Features (Firms and industries)
Balachandran, C.; C., P.; Ramachandran, G.; Krishnamachari, B.	2020	EDISON: A Blockchain-based Secure and Auditable Orchestration Framework for Multi-domain Software Defined Networks	2020 IEEE International Conference on Blockchain	Conference Paper	-	Unranked	Design and Features (Firms and industries)
Campbell, M.	2020	Beyond Zero Trust: Trust Is a Vulnerability	Computer	Journal Editorial	169	Q1 (Computer Science (miscellaneous))	Design and Features (Concept and Architecture)
Dhar, S.; Bose, I.	2020	Securing IoT Devices Using Zero Trust and Blockchain	Journal of Organizational Computing and Electronic Commerce	Journal Paper	41	Q2 (Computational Theory and Mathematics)	Design and Features (Concept and Architecture), Measurement and Value (Firms and industries), Management and organisation (Concept and Architecture)
Dimitrakos, T.; Dilshener, T.; Kravtsov, A.; La Marra, A.; Martinelli, F.; Rizos, A.; Rosetti, A.; Saracino, A.	2020	Trust Aware Continuous Authorization for Zero Trust in Consumer Internet of Things	IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications	Conference Paper	-	B	Design and Features (Firms and industries), Measurement and Value (Concept and Architecture)
Mehraj, S.; Banday, M. T.	2020	Establishing a Zero Trust Strategy in Cloud Computing Environment	2020 International Conference on Computer Communication and Informatics	Conference Paper	-	Unranked	Design and Features (Firms and industries)
Omar, R. R.; Abdelaziz, T. M.	2020	A Comparative Study of Network Access Control and Software-Defined Perimeter	Proceedings of the 6th International Conference on Engineering and MIS 2020	Conference Paper	-	Unranked	Design and Features (Concept and Architecture), Measurement and Value (Concept and Architecture)
Puthal, D.; Yang, L. T.; Dustdar, S.; Wen, Z.; Jun, S.; van Moorsel, A.; Ranjan, R.	2020	A User-centric Security Solution for Internet of Things and Edge Convergence	ACM Transactions on Cyber-Physical Systems	Journal Paper	14	Q2 (Artificial Intelligence Computer Networks and Communications)	Design and Features (Firms and industries), Measurement and Value (Concept and Architecture)

(*continued on next page*)

Author(s)	Year	Title	Published in	Publication Type	H-Index	Ranking*	Classification into Framework
Sateesh, H.; Zavarsky, P.	2020	State-of-the-Art VANET Trust Models: Challenges and Recommendations	11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference	Conference Paper	-	Unranked	Design and Features (Firms and industries), Measurement and Value (Concept and Architecture)
Singh, J.; Refaey, A.; Koilpillai, J.	2020	Adoption of the Software-Defined Perimeter (SDP) Architecture for Infrastructure as a Service	Canadian Journal of Electrical and Computer Engineering	Journal Paper	26	Q2 (Electrical and Electronic Engineering)	Design and Features (Concept and Architecture), Measurement and Value (Concept and Architecture)
Singh, J.; Refaey, A.; Shami, A.	2020	Multilevel Security Framework for NFV Based on Software Defined Perimeter	IEEE Network	Journal Paper	129	Q1 (Computer Networks and Communications)	Design and Features (Concept and Architecture), Measurement and Value (Concept and Architecture, Users and society)
Sultana, M.; Hossain, A.; Laila, F.; Taher, K. A.; Islam, M. N.	2020	Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology	BMC Medical Informatics and Decision Making	Journal Paper	73	Q2 (Health Informatics)	Design and Features (Firms and industries)
Yan, X.; Wang, H.	2020	Survey on Zero-Trust Network Security	2020 International Conference on Artificial Intelligence and Security	Conference Paper	-	Unranked	Design and Features (Concept and Architecture, Firms and industries), Measurement and Value (Firms and industries)
Yao, Q.; Wang, Q.; Zhang, X.; Fei, J.;	2020	Dynamic Access Control and Authorization System based on Zero-trust architecture	2020 International Conference on Control, Robotics and Intelligent System	Conference Paper	-	Unranked	Design and Features (Concept and Architecture)
Singh, J.; Bello, Y.; Hussein A. R.; Erbad, A.; Mohamed, A.	2021	Hierarchical Security Paradigm for IoT Multiaccess Edge Computing	IEEE Internet of Things Journal	Journal Paper	97	Q1 (Computer Networks and Communications)	Design and Features (Concept and Architecture), Measurement and Value (Concept and Architecture)
Xiaojian, Z.; Liandong, C.; Jie, F.; Xiangqun, W.;	2021	Power IoT security protection architecture based on zero trust framework	2021 IEEE 5th International Conference on Cryptography, Security and Privacy	Conference Paper	-	Unranked	Design and Features (Concept and Architecture)

***Notes:** Journal ranks are based on the Scimago Journal and Country Rank (https://www.scimagojr.com/); conference rankings are based on the Computing Research and Education ranking (http://portal.core.edu.au/conf-ranks/).

Appendix B.2. Overview of the grey literature

Author(s)	Year	Title	Publisher	Classification into Framework
Kindervag, J.	2010	Build Security Into Your Network's DNA: The Zero Trust Network Architecture	Forrester Research	Design and Features (Concept and Architecture), Management and Organisation (Firms and industries)
Kindervag, J.	2010	No More Chewy Centers Introducing The Zero Trust	Forrester Research	Design and Features (Concept and Architecture)
Ward, R.; Beyer, B.	2014	BeyondCorp: A New Approach to Enterprise Security	Google Research	Design and Features (Concept and Architecture), Management and Organisation (Firms and industries)
Cittadini, L.; Spear, B.; Beyer, B.; Saltonstall, M.;	2016	BeyondCorp Part III: The Access Proxy	Google Research	Design and Features (Concept and Architecture), Design and Features (Users and society), Management and Organisation (Firms and industries)
Osborn, B.; McWilliams, J.; Beyer, B.; Saltonstall, M.	2016	BeyondCorp: Design to Deployment at Google	Google Research	Design and Features (Concept and Architecture), Management and Organisation (Firms and industries)
Cunningham, C.; Pollard, J.	2017	The Eight Business And Security Benefits Of Zero Trust	Forrester Research	Measurement and Value (Firms and industries)
Escobedo, V. M.; Beyer, A. E.; Saltonstall, M.; Zyzniewski, F.	2017	BeyondCorp: The User Experience	Google Research	Design and Features (Users and society)
Koilpillai, J.	2017	Software Defined Perimeter (SDP): A Primer for CIOs	Waverley Labs LLC	Design and Features (Concept and Architecture), Measurement and Value (Concept and Architecture)
Peck, J.; Beyer, A. E.; Beske, C. M.; Saltonstall, M.	2017	Migrating to BeyondCorp: Maintaining Productivity While Improving Security	Google Research	Management and Organisation (Firms and industries)
Balaouras, S.; Cunningham, C.; Cerrato, P.	2018	Five Steps To A Zero Trust Network - Road Map: The Security Architecture And Operations Playbook	Forrester Research	Management and Organisation (Firms and industries)
King, H.; Janosko, M.; Beyer, A. E.; Saltonstall, M.	2018	BeyondCorp: Building a Healthy Fleet	Google Research	Design and Features (Concept and Architecture), Management and Organisation (Firms and industries)
American Council for Technology	2019	Zero Trust Cybersecurity: Current Trends	American Council for Technology	Design and Features (Concept and Architecture), Measurement and Value (Firms and industries), Management and Organisation (Users and society)
Banyan	2019	BeyondCorp for the Enterprise	Banyan	Design and Features (Concept and Architecture), Management and Organisation (Firms and industries)
Bjork, P.; Gordon, G.; Lanusse, A.; Navare, S.; Lantinga, H.; Arakelian, C.	2019	Zero Trust Secure Access to Traditional Applications with VMware	VMware	Design and Features (Concept and Architecture)
Garbis, J.; Koilpollai, J.	2019	Software-Defined Perimeter: Architecture Guide	Cloud Security Alliance	Design and Features (Concept and Architecture), Measurement and Value (Firms and industries), Management and Organisation (Firms and industries)

(*continued on next page*)

Author(s)	Year	Title	Publisher	Classification into Framework
Gigamon	2019	The IT and Security Landscape for 2020 and Beyond and the Role of Zero Trust	Gigamon	Measurement and Value (Firms and industries), Management and Organisation (Users and society)
Koilpillai, J.; Garbis, J.; Roza, M.; Murray, N.	2019	Anti-DDoS: Software-Defined Perimeter as a DDoS Prevention Mechanism	Cloud Security Alliance	Measurement and Value (Concept and Architecture)
Prisma	2019	BeyondCorp: A Step towards Zero Trust for the Cloud	Prisma	Measurement and Value (Firms and industries)
Schulze, H.	2019	Zero Trust Adoption Report	Cybersecurity Insiders	Measurement and Value (Firms and industries)
Crawford, S.; Bekker, G.; Montenegro, F.; Sherrill A.; Hanselman, E.	2020	SASE, ZTNA and XDR: Three security trends catalyzed by the impact of 2020	451 Research	Design and Features (Concept and Architecture)
Cunningham, C.	2020	The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q3 2020	Forrester Research	Design and Features (Concept and Architecture)
Gartner	2020	Zero Trust Architecture and Solutions	Gartner	Design and Features (Concept and Architecture), Management and Organisation (Firms and industries)
Koilpillai, J.; Murray, N. A.	2020	Software Defined Perimeter (SDP) and Zero Trust	Cloud Security Alliance	Design and Features (Concept and Architecture), Measurement and Value (Concept and Architecture, Firms and industries)
Orans, L.; Riley S.	2020	Market Guide for Zero Trust Network Access	Gartner	Design and Features (Concept and Architecture), Measurement and Value (Concept and Architecture, Firms and industries)
Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S.	2020	Zero Trust Architecture	National Institute of Standards and Technology	Design and Features (Concept and Architecture, Firms and industries), Management and Organisation (Firms and industries)
Schulze, H.	2020	Zero Trust Report	Cybersecurity Insiders	Measurement and Value (Firms and industries)
Küderli, U.; Neher, L.; Faistauer, F.	2020	Zero Trust architecture: a pardigm shift in cybersecurity and privacy	PricewaterhouseCoopers	Management and Organisation (Firms and industries)
Deloitte	2021	Zero Trust: A revolutionary approach to Cyber or just another buzz word?	Deloitte	Design and Features (Concept and Architecture), Measurement and Value (Firms and industries), Management and Organisation (Firms and industries)
Tufin	2021	Achieving a Zero Trust Network Security Model with Tufin	Tufin	Management and Organisation (Firms and industries)
Turner, S.; Holmes, D.; Cunningham, C.; Budge, J.; McKay, P.; Cser, A.; Shey, H.; Maxim, M.	2021	A Practical Guide to A Zero Trust Implementation	Forrester Research	Management and Organisation (Firms and industries)

Appendix C. Mapping of the identified literature to our research framework

Level of analysis	Activities					
		Design and features		Measurement and value		Management and organisation
Concept and architecture	Academic literature	Bertino et al. (2016) DeCusatis et al. (2016) Eidle et al. (2017) Puthal et al. (2017) Pan and Yang (2018) Samaniego and Deters (2018) Tao et al. (2018) Vanickis et al. (2018) Assunção (2019) Chen et al. (2019) Chifor et al. (2019) Kumar et al. (2019) Moubayed et al. (2019) Refaey et al. (2019)	Sallam et al. (2019a) Sallam et al. (2019b) Zaheer et al. (2019) Ahmed et al. (2020) Campbell (2020) Dhar and Bose (2020) Omar and Abdelaziz (2020) Shlapentokh-Rothman et al. (2020) Singh, Refaey, and Koilpillai (2020a) Singh, Refaey, and Shami (2020b) Yan and Wang (2020) Yao et al. (2020) Singh et al. (2021) Xiaojian et al. (2021)	Balfour (2015) DeCusatis et al. (2016) Eidle et al. (2017) Chen et al. (2019) Kumar et al. (2019) Moubayed et al. (2019) Refaey et al. (2019) Sallam et al. (2019a) Sallam et al. (2019b)	Zaheer et al. (2019) Dimitrakos et al. (2020) Omar and Abdelaziz (2020) Puthal et al. (2020) Sateesh and Zavarsky (2020) Singh, Refaey, and Koilpillai (2020a) Singh, Refaey, and Shami (2020b) Singh et al. (2021)	Dhar and Bose (2020)
	Grey literature	Kindervag (2010a) Kindervag (2010b) Ward and Beyer (2014) Cittadini et al. (2016) Osborn et al. (2016) Koilpillai (2017) King et al. (2018) American Council for Technology (2019) Banyan (2019)	Bjork et al. (2019) Garbis and Koilpollai (2019) Crawford et al. (2020) Cunningham (2020) Gartner (2020) Koilpillai and Murray (2020) Riley et al. (2020) Rose et al. (2020) Deloitte (2021)	Koilpillai (2017) Koilpillai et al. (2019) Koilpillai and Murray (2020) Riley et al. (2020)		-

(*continued on next page*)

Level of analysis	Activities	Design and features		Measurement and value		Management and organisation
Firms and industries	Academic literature	Balfour (2015) Lee et al. (2017) Samaniego and Deters (2018) Chen et al. (2019) Chifor et al. (2019) Zaheer et al. (2019) Albuali et al. (2020)	Balachandran et al. (2020) Dimitrakos et al. (2020) Mehraj and Banday (2020) Puthal et al. (2020) Sateesh and Zavarsky (2020) Sultana et al. (2020) Yan and Wang (2020)	Pan and Yang (2018) Sallam et al. (2019a) Dhar and Bose (2020)		-
	Grey literature	Rose et al. (2020)	Kindervag (2010a) Cunningham and Pollard (2017) Koilpillai (2017) American Council for Technology (2019) Garbis and Koilpollai (2019) Prisma (2019)	Schulze (2019) Gigamon (2020) Koilpillai and Murray (2020) Riley et al. (2020) Schulze (2020) Deloitte (2021)	Ward and Beyer (2014) Cittadini et al. (2016) Osborn et al. (2016) Peck et al. (2017) Balaouras et al. (2018) King et al. (2018) Banyan (2019)	Garbis and Koilpollai (2019) Gartner (2020) Küderli et al. (2020) Rose et al. (2020) Deloitte (2021) Tufin (2021) Turner et al. (2021)
Users and society	Academic literature	-	Singh, Refaey, and Shami (2020b)		-	
	Grey literature	Cittadini et al. (2016) Escobedo et al. (2017)	-		American Council for Technology (2019) Gigamon (2020)	

REFERENCES

Adikari S, McDonald C, Campbell J. A design science framework for designing and assessing user experience. In: Jacko JA, editor. In: Lecture Notes in Computer Science: Vol. 6761, Human-Computer Interaction: Design and Development Approaches. Springer; 2011. p. 25–34. doi:10.1007/978-3-642-21602-2_3.

Ahmed I, Nahar T, Urmi SS, Taher KA. Protection of sensitive data in zero trust model. In: Proceedings of the International Conference on Computing Advancements. ACM; 2020. p. 1–5. doi:10.1145/3377049.3377114.

Albuali A, Mengistu T, Che D. ZTIMM: a zero-trust-based identity management model for volunteer cloud computing. In: Zhang Q, Wang Y, Zhang L-J, editors. In: Lecture Notes in Computer Science: Vol. 12403. Cloud Computing – CLOUD 2020. Springer; 2020. p. 287–94. doi:10.1007/978-3-030-59635-4_22.

American Council for Technology. Zero Trust Cybersecurity: Current Trends. American Council for Technology; 2019. https://www.actiac.org/zero-trust-cybersecurity-current-trends (accessed 24.06.2021).

Assunção P. In: Proceedings of the Digital Privacy and Security Conference. A zero trust approach to network security. Protugal: Porto; 2019.

Balachandran C, C A, P Ramachandran, G, Krishnamachari B. EDISON: a blockchain-based secure and auditable orchestration framework for multi-domain software defined networks. In: 2020 IEEE International Conference on Blockchain (Blockchain). IEEE; 2020. p. 144–53. doi:10.1109/Blockchain50366.2020.00025.

Balaouras S, Cunningham C, Cerrato P. Five Steps to a Zero Trust Network: Road Map: The Security Architecture and Operations Playbook. Forrester Research; 2018. https://www.forrester.com/report/Five+Steps+To+A+Zero+Trust+Network/-/E-RES120510 (accessed 24.06.2021).

Balfour RE. Building the "internet of everything" (IoE) for first responders. In: 2015 Long Island Systems, Applications and Technology. IEEE; 2015. p. 1–6. doi:10.1109/LISAT.2015.7160172.

Banyan. BeyondCorp for the Enterprise. Banyan; 2019. https://info.banyansecurity.io/beyondcorp-for-the-enterprise (accessed 01.06.2021).

Basin D, Doser J, Lodderstedt T. Model driven security for process-oriented systems. In: Ferrari E, Ferraiolo D, editors. In: Proceedings of the eighth ACM symposium on Access control models and technologies. ACM; 2003. p. 100. doi:10.1145/775412.775425.

Bertino E, Choo K-K R, Georgakopolous D, Nepal S. (2016). Internet of Things (IoT): Smart and Secure Service Delivery. ACM Transactions on Internet Technology, 16(4), 1–7. doi:10.1145/3013520.

Bjork P, Gordon G, Lanusse A, Navare S, Lantinga H, Arakelian C. (2019). Zero Trust Secure Access to Traditional Applications with VMware. VMWare. https://techzone.vmware.com/resource/zero-trust-secure-access-traditional-applications-vmware (accessed 01.06.2021).

Butijn B–J, Tamburri DA, van Heuvel W–J. Blockchains. ACM Comput. Surv. 2020;53(3):1–37. doi:10.1145/3369052.

Campbell M. Beyond zero trust: trust is a vulnerability. Computer 2020;53(10):110–13. doi:10.1109/MC.2020.3011081.

Chen Y, Hu H [Hong-chao], Cheng G. Design and implementation of a novel enterprise network defense system by maneuvering multi-dimensional network properties. Front. Inf. Technol. Electr. Eng. 2019;20(2):238–52. doi:10.1631/FITEE.1800516.

Chifor B–C, Arseni S–C, Matei I, Bica I. Security-oriented framework for internet of things smart-home applications. In: 2019 22nd International Conference on Control Systems and Computer Science. IEEE; 2019. p. 146–53. doi:10.1109/CSCS.2019.00033.

Cittadini L, Spear B, Beyer B, Saltonstall M. BeyondCorp Part III: The Access Proxy. Google; 2016. https://research.google/pubs/pub45728/(accessed 01.06.2021).

Compastie M, Badonnel R, Festor O, He R, Kassi-Lahlou M. A software-defined security strategy for supporting autonomic security enforcement in distributed cloud. In: 2016 IEEE International Conference on Cloud Computing Technology and Science. IEEE; 2016. p. 464–7. doi:10.1109/CloudCom.2016.0079.

Crawford S, Bekker G, Montenegro F, Sherrill Aaron, Hanselman E. (2020). SASE, ZTNA and XDR: Three security trends catalyzed by the impact of 2020. 451 Research. https://www.spglobal.com/marketintelligence/en/news-insights/research/sase-ztna-and-xdr-three-security-trends-catalyzed-by-the-impact-of-2020 (accessed 02.06.2021).

Cunningham C. (2020). The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q3 2020: Tools And Technology: The Zero Trust Security Playbook. Forrester Research. https://www.forrester.com/report/The+Forrester+Wave+Zero+Trust+eXtended+Ecosystem+Platform+Providers+Q3+2020/-/E-RES157494 (accessed 02.06.2021).

Cunningham C, Pollard J. The Eight Business and Security Benefits of Zero Trust. Forrester Research; 2017. https://www.forrester.com/report/The+Eight+Business+And+Security+Benefits+Of+Zero+Trust/-/E-RES134863 (accessed 24.06.2021).

DeCusatis C, Liengtiraphan P, Sager A, Pinelli M. Implementing zero trust cloud networks with transport access control and first packet authentication. In: 2016 IEEE International Conference on Smart Cloud. IEEE; 2016. p. 5–10. doi:10.1109/SmartCloud.2016.22.

Deloitte. Zero Trust: A revolutionary approach to Cyber or just another buzz word?. Deloitte; 2021. https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/deloitte-cyber-zero-trust.pdf (accessed 02.06.2021).

Devanbu PT, Stubblebine S. Software engineering for security: a roadmap. In: Finkelstein A, editor. In: Proceedings of the Conference on The Future of Software Engineering. ACM; 2000. p. 227–39. doi:10.1145/336512.336559.

Dhar S, Bose I. Securing IoT devices using zero trust and blockchain. J. Org. Comput. Electron. Commerce 2020;31(1):18–34. doi:10.1080/10919392.2020.1831870.

Dimitrakos T, Dilshener T, Kravtsov A, La Marra A, Martinelli F, Rizos A, Rosetti A, Saracino A. Trust Aware Continuous Authorization for Zero Trust in Consumer Internet of Things. In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE; 2020. p. 1801–12. doi:10.1109/TrustCom50675.2020.00247.

Eidle D, Ni SY, DeCusatis C, Sager A. Autonomic security for zero trust networks. In: 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference. IEEE; 2017. p. 288–93. doi:10.1109/UEMCON.2017.8249053.

Escobedo VM, Zyzniewski F, Beyer AE, Saltonstall M. BeyondCorp: The User Experience. Google; 2017. https://research.google/pubs/pub46366/(accessed 24.06.2021).

Garbis J, Koilpollai J. Software Defined Perimeter Architecture Guide. Cloud Security Alliance; 2019. https://cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2/(accessed 24.06.2021).

Garousi V, Felderer M, Mäntylä M. Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. Inf. Software Technol. 2019;106:101–21. doi:10.1016/j.infsof.2018.09.006.

Gartner. Zero Trust Architecture and Solutions. Gartner; 2020. https://www.gartner.com/teamsiteanalytics/servePDF?g=/imagesrv/media-products/pdf/Qi-An-Xin/Qi-An-Xin-1-1OKONUN2.pdf (accessed 24.06.2021).

Gaudecker H–M, von, Holler R, Janys L, Siflinger B, Zimpelmann C. Labour supply in the early stages of the COVID-19 pandemic: empirical evidence on hours, home office, and expectations. IZA Discussion Paper No. 13158 2020 https://ssrn.com/abstract=3579251 (accessed 24.06.2021).

Gigamon. The IT and Security Landscape for 2020 and Beyond and the Role of Zero Trust. Gigamon; 2020. https://www.gigamon.com/resources/resource-library/analyst-industry-reports/ar-zerotrust-surveyreport.html (accessed 24.06.2021).

Jensen J, Jaatun MG. Security in model driven development: a survey. In: 2011 Sixth International Conference on Availability, Reliability and Security (ARES 2011): Vienna, Austria, 22 - 26 August 2011; [including workshop papers. IEEE; 2011. p. 704–9. doi:10.1109/ARES.2011.110.

Kindervag J. Build Security into Your Network's DNA: The Zero Trust Network Architecture. Forrester Research; 2010a. https://www.forrester.com/report/Build+Security+Into+Your+Networks+DNA+The+Zero+Trust+Network+Architecture/-/E-RES57047 (accessed 24.06.2021).

Kindervag J. No More Chewy Centers: Introducing the Zero Trust Model of Information Security. Forrester Research; 2010b. https://www.forrester.com/report/No+More+Chewy+Centers+The+Zero+Trust+Model+Of+Information+Security/-/E-RES56682 (accessed 24.06.2021).

King H, Janosko M, Beyer AE, Saltonstall M. BeyondCorp 6: Building a Healthy Fleet. Google; 2018. https://research.google/pubs/pub47356/(accessed 24.06.2021).

Kitchenham B, Charters S. Guidelines for performing Systematic Literature Reviews in Software Engineering; 2007. EBSE Technical Report EBSE-2007-01.

Koilpillai J. Software Defined Perimeter (SDP): A Primer for CIOs. Waverley Labs LLC; 2017. https://www.waverleylabs.com/wp-content/uploads/2017/10/waverleylabs-sdp-white-paper.pdf (accessed 24.06.2021).

Koilpillai J, Garbis J, Roza M, Murray N. Anti-DDoS: Software-Defined Perimeter as a DDoS Prevention Mechanism. Cloud Security Alliance; 2019. https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-as-a-ddos-prevention-mechanism/ (accessed 01.06.2021).

Koilpillai J, Murray N. Software defined perimeter (SDP) and zero trust. Cloud Secur. Alliance 2020 https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-and-zero-trust/(accessed 02.06.2021).

Küderli U, Neher L, Faistauer F. Zero trust architecture: a paradigm shift in cybersecurity and privacy. Pricewaterhouse Coopers 2020 https://www.pwc.ch/en/publications/2020/ch-zero-trust-whitepaper-final.pdf (accessed 24.06.2021).

Kumar P, Moubayed A, Refaey A, Shami A, Koilpillai J. Performance analysis of SDP for secure internal enterprises. In: 2019 IEEE Wireless Communications and Networking Conference. IEEE; 2019. p. 1–6. doi:10.1109/WCNC.2019.8885784.

Lee B, Vanickis R, Rogelio F, Jacob P. Situational awareness based risk-adaptable access control in enterprise networks. In: Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security. SCITEPRESS - Science and Technology Publications; 2017. p. 400–5. doi:10.5220/0006363404000405.

Mcginthy JM, Michaels AJ. Secure industrial internet of things critical infrastructure node design. IEEE Int. Things J. 2019;6(5):8021–37. doi:10.1109/JIOT.2019.2903242.

Mehraj S, Banday MT. Establishing a zero trust strategy in cloud computing environment. In: 2020 International Conference on Computer Communication and Informatics. IEEE; 2020. p. 1–6. doi:10.1109/ICCCI48352.2020.9104214.

Moubayed A, Refaey A, Shami A. Software-defined perimeter (SDP): state of the art secure solution for modern networks. IEEE Network 2019;33(5):226–33. doi:10.1109/MNET.2019.1800324.

Nguyen PH, Kramer M, Klein J, Le Traon Y. An extensive systematic review on the model-driven development of secure systems. Inf. Software Technol. 2015;68:62–81. doi:10.1016/j.infsof.2015.08.006.

Omar RR, Abdelaziz TM. A comparative study of network access control and software-defined perimeter. In: Uskenbayeva R, Daineko Y, Aljawarneh SA, editors. In: Proceedings of the 6th International Conference on Engineering and MIS 2020. ACM; 2020. p. 1–5. doi:10.1145/3410352.3410754.

Osborn B, McWilliams J, Beyer B, Saltonstall M. BeyondCorp: Design to Deployment at Google. Google; 2016. https://research.google/pubs/pub44860/ (accessed 24.06.2021).

Pan J, Yang Z. Cybersecurity challenges and opportunities in the new "edge computing + IoT" world. In: Ahn G-J, Gu G, Hu H, Shin S, editors. In: Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization. ACM Press; 2018. p. 29–32. doi:10.1145/3180465.3180470.

Peck J, Beyer AE, Beske CM, Saltonstall M. Migrating to BeyondCorp: Maintaining Productivity While Improving Security. Google; 2017. https://research.google.com/pubs/pub46134.html?hl=tr (accessed 24.06.2021).

Polacek, M. (2020). *Leaders are now committed to zero trust: zero trust is a digital business enabler for all size firms*. https://www.cloudflare.com/en-gb/lp/forrester-opportunity-snapshot-zero-trust/ (accessed 24.06.2021).

Prisma. BeyondCorp: A Step towards Zero Trust for the Cloud. Prisma; 2019. https://www.paloaltonetworks.com/resources/ebooks/beyondcorp-step-toward-zero-trust (accessed 29.05.2021).

Puthal D, Mohanty SP, Nanda P, Choppali U. Building security perimeters to protect network systems against cyber threats [future directions]. IEEE Consum. Electron. Mag. 2017;6(4):24–7. doi:10.1109/MCE.2017.2714744.

Puthal D, Yang LT, Dustdar S, Wen Z, Jun S, van Moorsel A, Ranjan R. A user-centric security solution for internet of things and edge convergence. ACM Trans. Cyber-Phys. Syst. 2020;4(3):1–19. doi:10.1145/3351882.

Refaey A, Sallam A, Shami A. On IoT applications: a proposed SDP framework for MQTT. Electron. Lett. 2019;55(22):1201–3. doi:10.1049/el.2019.2334.

Riley S, MacDonald N, Orans L. Market Guide for Zero Trust Network Access. Gartner; 2020. https://www.gartner.com/en/documents/3986053/market-guide-for-zero-trust-network-access (accessed 02.06.2021).

Risius M, Spohrer K. A blockchain research framework. Bus. Inf. Syst. Eng. 2017;59(6):385–409. doi:10.1007/s12599-017-0506-0.

Rose S, Borchert O, Mitchell S, Connelly S. Zero Trust Architecture. National Institute of Standards and Technology; 2020. https://csrc.nist.gov/publications/detail/sp/800-207/final (accessed 24.06.2021).

Sallam A, Refaey A, Shami A. On the security of SDN: a completed secure and scalable framework using the software-defined perimeter. IEEE Access 2019a(7):146577–87. doi:10.1109/ACCESS.2019.2939780.

Sallam A, Refaey A, Shami A. Securing smart home networks with software-defined perimeter. In: 2019 15th International Wireless Communications and Mobile Computing Conference. IEEE; 2019b. p. 1989–93. doi:10.1109/IWCMC.2019.8766686.

Saltan A, Smolander K. Bridging the state-of-the-art and the state-of-the-practice of SaaS pricing: a multivocal literature review. Inf. Software Technol. 2021;133. doi:10.1016/j.infsof.2021.106510.

Saltzer JH, Schroeder MD. The protection of information in computer systems. Proc. IEEE 1975;63(9):1278–308. doi:10.1109/PROC.1975.9939.

Samaniego M, Deters R. Zero-trust hierarchical management in IoT. In: 2018 IEEE International Congress on Internet of Things. IEEE; 2018. p. 88–95. doi:10.1109/ICIOT.2018.00019.

Sateesh H, Zavarsky P. State-of-the-Art VANET trust models: challenges and recommendations. In: 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE; 2020. p. 757–64. doi:10.1109/IEMCON51383.2020.9284953.

Scheuner J, Leitner P. Function-as-a-service performance evaluation: a multivocal literature review. J. Syst. Software 2020;170. doi:10.1016/j.jss.2020.110708.

Schulze H. In: Cybersecurity Insiders. Zero Trust Adoption report; 2019. https://www.cybersecurity-insiders.com/portfolio/2019-zero-trust-adoption-report/ (accessed 01.06.2021).

Schulze H. Zero Trust Report. Cybersecurity Insiders; 2020. https://www.cybersecurity-insiders.com/portfolio/2020-zero-trust-report-netskope/(accessed 01.06.2021).

Shlapentokh-Rothman M, Hemberg E, O'Reilly U–M. Securing the software defined perimeter with evolutionary co-optimization. In: Coello Coello CA, editor. In: Proceedings of the 2020 Genetic and Evolutionary Computation Conference Companion. ACM; 2020. p. 1528–36. doi:10.1145/3377929.3398085.

Singh J, Bello Y, Hussein AR, Erbad A, Mohamed A. Hierarchical security paradigm for iot multiaccess edge computing. IEEE Int. Things J. 2021;8(7):5794–805. doi:10.1109/JIOT.2020.3033265.

Singh J, Refaey A, Koilpillai J. Adoption of the software-defined perimeter (SDP) architecture for infrastructure as a service. Can. J. Electr. Comput. Eng. 2020a;43(4):357–63. doi:10.1109/CJECE.2020.3005316.

Singh J, Refaey A, Shami A. Multilevel security framework for NFV based on software defined perimeter. IEEE Network 2020b;34(5):114–19. doi:10.1109/MNET.011.1900563.

Sultana M, Hossain A, Laila F, Taher KA, Islam MN. Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. BMC Med. Inf. Decis. Making 2020;20(1):256. doi:10.1186/s12911-020-01275-y.

Tao Y, Lei Z, Ruxiang P. Fine-grained big data security method based on zero trust model. In: 2018 IEEE 24th International Conference on Parallel and Distributed Systems. IEEE; 2018. p. 1040–5. doi:10.1109/PADSW.2018.8644614.

Tufin. Achieving a Zero Trust Network Security Model with Tufin. Tufin; 2021. https://lp.tufin.com/zero-trust-network-security-wp.html (accessed 02.06.2021).

Turner S, Holmes D, Cunningham C, Budge J, McKay P, Cser A, Shey H, Maxim M. A Practical Guide To A Zero Trust Implementation: Roadmap: The Zero Trust Security Playbook. Forrester Research; 2021. https://www.forrester.com/report/A+Practical+Guide+To+A+Zero+Trust+Implementation/-/E-RES157736 (accessed 02.06.2021).

Vanickis R, Jacob P, Dehghanzadeh S, Lee B. Access control policy enforcement for zero-trust-networking. In: 2018 29th Irish Signals and Systems Conference. IEEE; 2018. p. 1–6. doi:10.1109/ISSC.2018.8585365.

Venkatesh Morris, Davis. User acceptance of information technology: toward a unified view. MIS Quarterly 2003;27(3):425. doi:10.2307/30036540.

Ward R, Beyer B. BeyondCorp: A New Approach to Enterprise Security. Google; 2014. https://research.google/pubs/pub43231/(accessed 24.06.2021).

Webster J, Watson RT. Analyzing the past to prepare for the future: writing a literature review. MIS Quarterly 2002;26(2):13–23 http://www.jstor.org/stable/4132319.

Weishäupl E, Yasasin E, Schryen G. Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. Comput. Security 2018;77:807–23. doi:10.1016/j.cose.2018.02.001.

Xiaojian Z, Liandong C, Jie F, Xiangqun W, Qi W. Power IoT security protection architecture based on zero trust framework. In: 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP). IEEE; 2021. p. 166–70. doi:10.1109/CSP51677.2021.9357607.

Yan X, Wang H. Survey on zero-trust network security. In: Sun X, Wang J, Bertino E, editors. In: *Communications in Computer and Information Science. Artificial Intelligence and Security* (Vol. 1252. Singapore: Springer; 2020. p. 50–60. doi:10.1007/978-981-15-8083-3_5.

Yao Q, Wang Q, Zhang X, Fei J. Dynamic access control and authorization system based on zero-trust architecture. In: 2020 International Conference on Control, Robotics and Intelligent System. ACM; 2020. p. 123–7. doi:10.1145/3437802.3437824.

Zaheer Z, Chang H, Mukherjee S, van der Merwe J. eZTrust: network-independent zero-trust perimeterization for microservices. In: Proceedings of the 2019 ACM Symposium on SDN Research. ACM; 2019. p. 49–61. doi:10.1145/3314148.3314349.