7-1-2022

Zero Trust Architecture: Trend and Impacton Information Security

Onome Christopher Edo
Auburn University at Montgomery

Theophilus Tenebe
Texas State University

Egbe-Etu Etu
San Jose State University, egbe-etu.etu@sjsu.edu

Atamgbo Ayuwu
Texas State University

Joshua Emakhu
Wayne State University

See next page for additional authors

Recommended Citation

Onome Christopher Edo, Theophilus Tenebe, Egbe-Etu Etu, Atamgbo Ayuwu, Joshua Emakhu, and Shakiru Adebiyi. "Zero Trust Architecture: Trend and Impacton Information Security" *International Journal of Emerging Technology and Advanced Engineering* (2022): 140-147. https://doi.org/10.46338/ijetae0722_15

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (E-ISSN 2250-2459, Scopus Indexed, ISO 9001:2008 Certified Journal, Volume 12, Issue 07, July 2022)
Manuscript Received: 22 May 2022, Received in Revised form: 27 June 2022, Accepted: 01 July 2022 DOI: 10.46338/ijetae0722_15

Zero Trust Architecture: Trend and Impact on Information Security

Onome Christopher EDO[1], Theophilus Tenebe[2], Egbe-etu Etu[2], Atamgbo Ayuwu[3], Joshua Emakhu[3], Shakiru Adebiyi[3]

[1]*Auburn University at Montgomery, Department of Information Systems Alabama, United States*
.[2]*Texas State University, Ingram School of Engineering, Texas, United States.*
[2]*San Jose State University, Department of Marketing and Business Analytics, California, United States.*
[3]*Texas State University, Ingram School of Engineering, Texas, United States.*
[3]*Wayne State University, Department of industrial and System Engineering, Michigan, United State,*
[3]*Netapp Inc. San Jose, California, United States.*

***Abstract*— Traditional-based security models are a threat to information security; they have been regarded as weak and ineffective to meet the dynamics of information system trust. An emerging framework, Zero Trust Architecture (ZTA) seeks to close the trust gap in information security through enforcing policies based on identity and continuous authentication and verification. This framework is built on several trust nodes and logical components that attempt to close the trust gap that exists in an information system. The adoption of this framework is still in its teething stage which is a result of several misleading deductions and assumptions. We attempt to explore the intricacies in the framework and close the existing knowledge gap. we surveyed the literature on ZTA and provided a foundational discussion on its implementation and effectiveness from prior studies. while we do not critique other models, this paper studied the strength and variables of the zero-trust security architecture and attempt to provide an overview of the model and close the knowledge gap on the effectiveness of adopting a Zero trust philosophy.**

***Keywords*— Cyberthreat, Information security, Risk, Trust, Zero-trust**

I. INTRODUCTION

Cybersecurity threats continue to rise on a magnitude scale and remain a global concern. Organizations world over have been victims of data theft arising from intrusion and malicious attacks on servers and other hardware components, individuals are susceptible to the risk, one will think that the government would be left out of this matrix.

Surprisingly, the government remains the biggest target, the year 2021 recorded over 1862 breaches, which is 68% over the year 2020 [1] On a global outlook, over 11 significant security breaches were recorded in January 2022, with the government of Canada, Australia, and Belarus as top victims, the United States Department of Homeland security suffered the same fate in 2021 [2]

This entropy continues to foster distrust and users are quite pessimistic about the security and privacy of their data. Thus, limiting users' perception of information technology. These threats are of various kinds; however, recent trends and attacks are often in the form of ransomware, data breaches, identity fraud, phishing, cloud vulnerability, insider threats, and the internet of things.

These activities affect businesses and individuals, for example, ransomware attacks have been linked to information system downtime, poor turnaround time, and productivity [3]. The outcome of this is consequential and institutions such as healthcare and other critical infrastructure have been limited to full capacity. In another scenario, victims of this attack are requested to make payments or risk the loss of their data, and this often damages the organization's reputation [4]. Hackers intend to gain access through the weakest link of an organization and exploit the surface to their advantage, these weak surfaces could be insiders within the organization or a porous network surface. Several studies have identified insiders as the weakest attack surface in information security [5]–[12]

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (E-ISSN 2250-2459, Scopus Indexed, ISO 9001:2008 Certified Journal, Volume 12, Issue 07, July 2022)

Although measures are deployed to combat the possibility of an attack, hackers still gain access to classified information, cyber-attacks do not necessarily begin with software, the software does not exist on its own [8], and hardware and insiders are critical factors in an information security system and their vulnerability is a conduit to an intrusion. the advent of remote working on a cloud basis has widened the threat gap and a more nuanced security approach is required to counter these attacks.

As technology continues to evolve, and with the advent of virtual working, organizations must take proactive measures to safeguard their assets and resources as a perimeter-based security framework is not effective to meet the demands of the dynamism in information security, especially concerning cloud computing where data could be access remotely. Hence an effective countermeasure and preventive framework are required to meet these demands.

A more robust approach with emphasis on intermittent security checks, user authentication, validation, and verification is required for information security assurance, while there are a ton of security architecture that aims to repeal the effect of an attack, hackers still exploit an organization's vulnerability. Thus, a comprehensive framework is required in this regard, and the Zero-Trust Architecture (ZTA) has continued to receive attention in recent times.

The zero trust model addresses trust-based vulnerabilities and it is premised on the philosophy of "never trust" taking cognizance of factors within and outside the organization's perimeter [9], first coined by Stephen Paul Marsh in his doctoral thesis on computer security [10] and adopted as a security tool by John Kindervag, a Forrester Research Analyst in the year 2010 [11].

Although new in the cybersecurity domain, its potency, however, overcome the information security threats posed by hackers. however, its adoption remains at about 15% in the Information technology domain [12]. A possible reason for this is the knowledge gap, misleading deductions, and difficulty in operationalizing the concept in a standard information system. It thus becomes challenging to adopt this methodology [17],[18]. although much has not been published on ZTA, this study aims to review literature on studies that have proposed or developed a ZTA and attempt to close the knowledge gap by presenting an overview of the concepts in the current information system setting and the impacts of its adoption on business enterprises. This will thus eliminate the scepticism of adopting ZTA and provide a conceptual understanding of ZTA.

To address these objectives, the next section of the paper discusses the methodology, section three is a review of the prior information security framework, and section four concludes the paper.

II. Literature Review

The concept of trust has been defined in a social context and viewed from different perspectives, while our focus is on the trust factor as a weak link to information security vulnerability, it is however pertinent to provide a conceptual definition of the term.[16] defined it as "assured reliance on the character, ability, strength, or truth of someone or something" it is a behavioral construct [17] and as such, could be unpredictable.

Research on ZTA is at its early stage, the shortcomings of current legacy systems have informed a more nuanced approach toward cyberthreats. To close the trust gap [18] adopted the ZTA framework and proposed a trust model in cloud environments, their study offered a fine-grained model to enhancing trust in an organization's information system reference components from the National Institute of standard and technology was adopted in the design, and performance analysis was carried out to test the efficacy of the model, it was evident that intrusion can be controlled with the distribution of trust-based node. Owing to the inefficiencies of current cyber security measures in virtual power plants [19] adopted the ZTA to enhance privacy and data protection in the energy sector, their model was built on the ZTA foundation and performance provided a feasible solution to data theft and breaches. The use cases of zero trust have continued to rise since the emergence of the pandemic and have changed the dynamics of work the place environment. Thus organizations sanctions remote working environment, while remote work attempts to contain the viral spread of the virus, however, it appears to increase the susceptibility of network and system intrusion, hence zero trust model appeals to the network intrusion gap and aims to close these gaps, consequently, organizations continue to adopt the model as a countermeasure to hacking, a significant institution that has adopted the model in the United States government specifically, the department of defense, the department of health and services and the department of homeland security [20], [21]. To further advance the adoption of the model and its deployment, information technology firms have developed a working model in consonance with the framework as enshrined in the NIST policy, prominent among these organizations is Microsoft.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (E-ISSN 2250-2459, Scopus Indexed, ISO 9001:2008 Certified Journal, Volume 12, Issue 07, July 2022)

[22]researched zero trust architecture for transitioning in the healthcare industry, they concluded that medical devices could be secured with a combination of the model and firewalls. Consequently, all unnecessary traffic will be halted and result in network performance, this result aligns with the summation of [23]

Another practical study [24] explored the implications of adopting a Zero trust model in the banking sector, the study revealed that the model is efficient and effective in countering the prevalent of intrusion in the banking sector and it serves as a strong forcess against security breaches in the banking sector, technically, this helps solves the prevalence of hacking various customer accounts and enhances the reputation of the banking industry. Similarly [25] proposed a ZTA network for managing microservices, the model was based on access control principles and, policy enforcement which is used to secure access and monitor packets across the network, the endpoint of the model showed an effective countermeasure against vulnerability and intrusion.[26] investigated the impact of ZTA in a university environment, after taking cognizance of the components and policies they concluded that ethe xisting security framework lacks the capabilities to halt intrusion and cyber threats and support the deployment of ZTA. Due to the weakness of the perimeter-based security framework [27] proposed a trust scores framework in the university environment for securing research work, the model was designed to calculate the trust score based on identity and access based control mechanisms, with the validated core, the system is automated to release access to users based on the level of trust identified by the system, they concluded that the framework fosters security and appears to be more viable compared to a permitter based model [28] proposed a policy enforcement language for operationalizing access and identity control in a ZTA, their model was based on a policy language and firewalls rules, the policy enforcement was developed on a rule-based principle and integrated with the system firewall which is triggered when an intrusion is detected, the architecture was tested for efficiency and its effectiveness, and the system proved to be anti-threat architecture.[29] proposes a zero-trust cloud network with transport control and authentication, The study proposed a novel idea by incorporating two security mechanisms, a transport control mechanism and a packet authentication, access to the system network or resources is first authenticated for trust with the transport control mechanism, and a second check is authenticated using tokens to validate identity and access. The combination of these mechanisms was built on a trust foundation that helps mitigate unauthorized access and identity theft. in another study[30] researched current security architecture, they submitted that the current framework cannot curtail recent security trends and challenges, hence they proposed a combination of blockchain-based security architecture and a ZTA as a framework for the internet of things which promotes authentication and secure access to devices and resources.

On a general note, the operational impact of the model outweighs the cost [31], [32] and has been categorized as effective over other security models in the business context, telecommunication organizations such as At&T have confirmed that its reduces organizational risk and closes lapses in cloud control mechanisms, more so, it reduces the risk of a data breach, thus saving organizations the cost of litigations and unauthorized use of customer data for espionage, and more importantly, it reduces the risk of security breach both on-premise and virtually.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (E-ISSN 2250-2459, Scopus Indexed, ISO 9001:2008 Certified Journal, Volume 12, Issue 07, July 2022)

Table 1
Summary of literature

Author	Year	Title	Scope	Performance
Ferretti, Magnanini, Andreolini, and Colajanni	2021	Survivable zero trust for cloud computing environments	ZTA and cloud computing	The architecture is deemed feasible and effective as a countermeasure to intrusion
Alagappan,Venkatachary,and Andrews	2022	Augmenting Zero Trust Network Architecture to enhance security in virtual power plants	ZTA	The performance testing closes the trust-based vulnerability compared to the traditional security model
Tyler and Viana	2021	Trust no one? A framework for assisting healthcare organizations in transitioning to a zero-trust network architecture	ZTA	Closes data threat theft gap and initiates policies at different enforcement points
Saini, Saini, and Singh	2019	Security and Trust Model Analysis for Banking System	ZTA	Enhances user application interface and promotes access control mechanism
Dean, Fonyi, Morrell, Lanham, and Teague	2021	Toward a Zero Trust Architecture Implementation in a University Environment	ZTA	Secure university resources and research from hackers
Zaheer, Chang, Mukherjee, and Van Der Merwe	2019	EZTrust:Network-Independent Zero-Trust Perimeterization for Microservices	ZTA, microservices and segmentation	Enforces policy and promotes security
Lukaseder, Halter, and Kargi	2020	Context-based Access Control and Trust Scores in Zero Trust Campus Networks	ZTA and access control	Provides access control and authentication tools for accessing campus resources
Vanickis,Jacob,Dehghanzadeh, and Lee	2019	Access Control Policy Enforcement for Zero-Trust-Networking	ZTA and access control	Enforces policy and promotes security
Decusatis,Liengtiraphan,Sager, and Pinelli	2016	Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication	ZTA and access control	Closes data theft, and secures network packets
Li, Iqbal, and Saxena,	2022	"Future Industry Internet of Things with Zero-trust Security	ZTA and blockchain	Secures devices and includes authentication and identification mechanism

A. Definition of Zero trust

Various definitions have been coined around the Zero Trust Model, a common phrase in the definition is trust and this extends to the users, devices, networks, and other variables that interface within and outside the perimeters of an organization's network. [33]

[34] defined it as a model that considers the internal and external threats, preventing malicious insiders from accessing information they are unauthorized to access, to prevent threats throughout the network and ensure the reduction of vulnerable systems' exposure

[35] sees it as a model that takes cognizance of an attacker's presence within the environment, and that the enterprise-owned environment does not differ from the non-enterprise-owned environment as well as trust and security are concerned.

Similarly, [36] explained that the model goes hand in hand with its architecture. Zero Trust Architecture has to do with technical controls put in place to prevent unauthorized access as well as policies that boost a more mobile and secure workforce.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (E-ISSN 2250-2459, Scopus Indexed, ISO 9001:2008 Certified Journal, Volume 12, Issue 07, July 2022)

Despite several definitions, a common phenomenon is the issue of trust, which attempts to explain that interacting variables within a system should not be trusted, this is not meant to hunt any variable, but to constantly audit, validate and authorize verified identity. However, it is pertinent to mention that the model itself is not a tool, but a philosophy and this influences beliefs, thoughts, and decisions based on the credibility of perceived information within the authorizing engine.

B. Logical components of the model

The architectural design is an ideal framework and the interactions with the framework, this architecture was adapted from the United States National Institute of Standards and technology, the core component is the policy engine, this has a relationship with the policy administrator and the policy enrollment point[21]. The relative components are described below

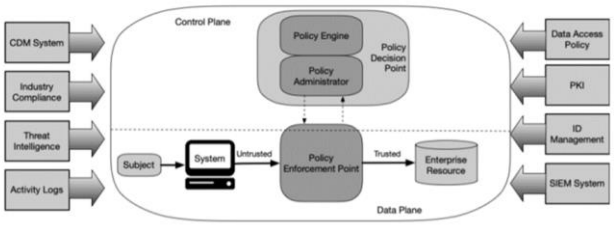

FIGURE I LOGICAL COMPONENTS OF THE MODE, ADAPTED FROM NIIST

1) Policy engine

Policy engine (PE): The policy engine is an important factor in the model, the long-term and final decision to yield access to a device or network is driven by the policy engine. the design of the PE is programmed based on the internal and external working policy adopted by the organization and considers other external factors such as CDM systems, threat intelligence, and activity logs as trust algorithms to grant, deny, or revoke access to the resource. The PE is paired with the policy administrator component. The policy engine makes and logs the decision (as approved, or denied), and the policy administrator executes the decision [21]

2) Policy administrator

The policy administrator is an executor in primary terms, it acts on the flow from the policy engine and is responsible for granting access or shutting down communication path based on the information from the policy engine, in practical terms, the PA authenticates users' identity through token or credential used by a client to access an enterprise resource[21].

3) Policy enrollment point

This component enforces the decisions made by the policy engine, specifically enables, monitors, and terminates traffic between an agent and a client, it is the conduit between the users and the system resources [21].

III. PILLARS OF ZERO TRUST

The model is built on six core factors (users, devices, network, applications, automation, and analytics) that drive the effectiveness and efficiency of the model, the core factors cannot be implemented as a standalone, though independent, there must be a significant interface between the variables for effectiveness. Users are the first and significant factor in the implementation prices because they can be susceptible to compromise within and outside the network perimeters and as such, they require continuous verification and identification, they interface with the devices which, these devices are also validated and authenticated for effective security, the model requires fail-safe applications and automation that interfaces with other factors and an analytical tool that reports on the activities of the operations of the model, below are a graphical architecture of the trust variables.

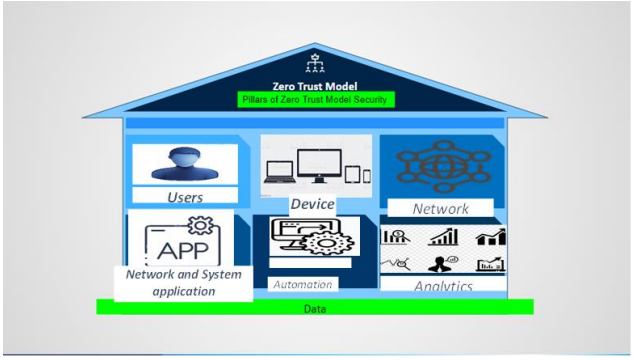

FIGURE II INTERACTING VARIABLE OF ZERO TRUST

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (E-ISSN 2250-2459, Scopus Indexed, ISO 9001:2008 Certified Journal, Volume 12, Issue 07, July 2022)

A. Elements of zero-trust security architecture

Like every other security framework, the zero-trust model is not a stand-alone framework, it comprises variables that drive the adoption and effective deployment of the model. While there are several variables in the deployment of the model, Ngo-Lam (2020) identified three significant elements of the architecture, having considered prior literature, we find these elements noteworthy in the evaluation of the model, they are discussed hereunder.

1) No False sense of security

The idea that employees of an organization have passed initial security checks is not enough criteria to validate trust or breaches, while people should be held accountable for their integrity and the belief that people will always remain in consonance with security policies, thus validating trust. However, the Zero Trust model demystify this principle, the architecture protects against insider threat that may be unassumed [37]. As people get familiar with an organization or network, they tend to identify the weaknesses in the network perimeters and insiders can be more threatening in a security breach as they are fundamentally aware of the loopholes in the system architecture. Hence, the model is built on a zero-trust philosophy, hence requiring constant validation of credentials irrespective of the personnel [33].

2) Multi-Factor Authentication

As the name implies, multi-factor authentication is a combination of more than one security application that attempts to validate the identity of a user with two or more factors, the idea is to reassure the system of the user credentials and identity. In conceptual terms, [38] defines a layered approach to application and system security requiring a user to present a combination of two or more credentials to verify a user's identity for login. The failure of one thus denies the authorization to the targeted physical space, computing device, network, or database. In specific terms, it consists of something you know such as a password, pins, something you have such as smart cards, tokens, and something you do like fingerprinting, gestures, signatures, etc.

3) Micro-segmentationion

The concept of micro-segmentation attempts to give the least privilege to users and restrict access to the entire organizations' network. It is based on the theory that users should only have privileges to a segment of the organizations' network that pertains to their job and ensure proper authorization.

It guards against lateral weaknesses and prevents unauthorized access to on-premise assets [37], [39].

4) Model requirements

The design and procedural implementation of zero trust architecture follow a unique set of rules as set out in the policy mandate by the NIST (2020), while several organizations have a user-based procedure, we adopt the methodology enshrined in the policy of the NIST 2020. This includes seven procedural tenets are they are discussed in three different domains namely granting access, controlling access, and monitoring and securing access [40]

5) Granting Access domain

Authentication and authorization: This domain expresses concern on identity management and follows the least privilege access to systems and infrastructure. The model explains that identity should be thoroughly scrutinized, and access is strongly authenticated before allowing entry into a network [21], [40], [41].

Integrity: A critical requirement for implementing the ZTA is to continuously examine the integrity of the security architecture and devices on the network, and the model. All-access request within the network should be validated and continuously examined for intrusion. Thus, trust should not be assumed and access must not be granted based on identity but validated access and identity [21], [40].

Observable state: When an identity attempts to access a resource, verify that identity with strong authentication, and ensure access is compliant and typical for that identity. Follow least privilege access principles

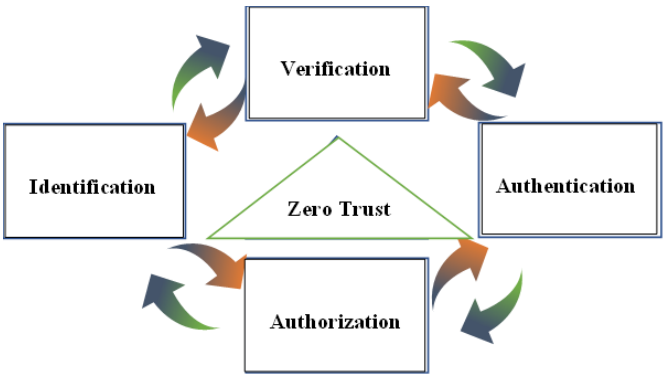

Figure III Zero trust drivers

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (E-ISSN 2250-2459, Scopus Indexed, ISO 9001:2008 Certified Journal, Volume 12, Issue 07, July 2022)

IV. CONCLUSION

Traditional security framework is deployed on a perimeter-based basis, and has resulted in data theft, intrusion, malware, and ransomware attacks, with the advancement in technology and cyber-attacks, the Zero trust security model attempts to mirror these activities and take strong measures to validate the intention and identity of users, devices, and the interacting variables withing the system atmosphere, these policies overrun the latency in the traditional security model and as such adjudged as efficient and effective. The ZTA thus fulfills this ideal, however, little is known about this architecture and as such creates a limitation for its adoption. We present a conceptual overview of the ZTA architecture and an appraisal of efficiency and effectiveness from the literature. We thus find that ZTA closes the trust vulnerability that exists in an organization's information system and the model could be deployed and combined with another security framework. From a policy point of view, the architecture is built on a principle of "never trust" and attempts to identify and authenticate users, and devices before granting access to infrastructure and resources.

REFERENCES

[1] Identity Theft Resource Center, "Annual Data Breach Report Sets New Record for Number of Compromises," 2022. [Online]. Available: https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/.

[2] Center for Strategic and International Studies, "Significant Cyber Incidents," 2022. [Online]. Available: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[3] N. Jones, "5 Ways Ransomware Can Negatively Impact Your Business," ignite Blog, 2022. https://www.egnyte.com/blog/post/5-ways-ransomware-can-negatively-impact-your-business#:~:text=In fact%2C Forbes Insights found,breaches or IT system failures.

[4] M. Ahmed, W. Ahmed, and S. Khan, "Ransomware: Attack, Human Impact and Mitigation," Int. J. Comput. Sci. Inf. Secur., vol. 18, 2020, doi: 10.5281/ZENODO.4425480.

[5] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'weakest link' - A human/computer interaction approach to usable and effective security," BT Technol. J., vol. 19, no. 3, 2001, doi: 10.1023/A:1011902718709.

[6] R. T. West, C. B. Mayhorn, J. B. Hardee, and J. Mendel, "The weakest link: A psychological perspective on why users make poor security decisions," in Social and Human Elements of Information Security: Emerging Trends and Countermeasures, 2008.

[7] S. Thomason, "People – The Weak Link in Security," Glob. J. Comput. Sci. Technol. Network, Web Secur., vol. 13, no. 11, 2013.

[8] L. Edlyn and P. Algirde, "Hardware is a cybersecurity risk. Here's what we need to know," World Economic Forus, 2019. https://www.weforum.org/agenda/2019/12/our-hardware-is-under-cyberattack-heres-how-to-make-it-safe/.

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

[10] S. P. Marsh, "Formalising Trust as a Computational Concept," Computing, vol. Doctor of, no. April, 1994.

[11] GSA, "Zero Trust Architecture (ZTA): Buyer guide," 2021. [Online]. Available: file:///C:/Users/OC Edo/Downloads/Zero Trust Architecture Buyers Guide v11 20210810 (4).pdf.

[12] Cyberecurity Insiders, "Zero Trust Adoption Rate," 2019. https://www.cybersecurity-insiders.com/portfolio/2019-zero-trust-adoption-report/#:~:text=Key Takeaways%3A,have zero trust in place.

[13] C. Buck, C. Olenberger, A. Schweizer, F. Völter, and T. Eymann, "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust," Comput. Secur., vol. 110, 2021, doi: 10.1016/j.cose.2021.102436.

[14] K. D. Uttecht, "Zero Trust (ZT) Concepts for Federal Government Architecture," 2020. [Online]. Available: https://apps.dtic.mil/sti/citations/AD1106904.

[15] D. Padula, "Journal Indexing: Core standards and why they matter," LSE, 2019. https://blogs.lse.ac.uk/impactofsocialsciences/2019/08/22/journal-indexing-core-standards-and-why-they-matter/.

[16] Merriam Webster, "Merriam-Webster Dictionary," Merriam-Webster Dictionary. 1828.

[17] F. Li and S. C. Betts, "Trust: What It Is And What It Is Not," Int. Bus. Econ. Res. J., vol. 2, no. 7, 2011, doi: 10.19030/iber.v2i7.3825.

[18] L. Ferretti, F. Magnanini, M. Andreolini, and M. Colajanni, "Survivable zero trust for cloud computing environments," Comput. Secur., vol. 110, 2021, doi: 10.1016/j.cose.2021.102419.

[19] A. Alagappan, S. K. Venkatachary, and L. J. B. Andrews, "Augmenting Zero Trust Network Architecture to enhance security in virtual power plants," Energy Reports, vol. 8, 2022, doi: 10.1016/j.egyr.2021.11.272.

[20] K. Macri, "What is Zero Trust? Federal Agencies Embrace Cybersecurity Innovation," Govcio Media and Research, 2021. https://governmentciomedia.com/what-zero-trust-federal-agencies-embrace-cybersecurity-innovation.

[21] NIST, "Zero Trust Architecture, SP 800-207," Natl. Inst. Stand. Technol. Spec. Publ., vol. SP 800-207, 2020.

[22] D. Tyler and T. Viana, "Trust no one? A framework for assisting healthcare organisations in transitioning to a zero-trust network architecture," Appl. Sci., vol. 11, no. 16, 2021, doi: 10.3390/app11167499.

[23] N. Cavalancia, "Zero Trust Architecture explained," At&T Cybersecurity, 2020. https://cybersecurity.att.com/blogs/security-essentials/what-is-a-zero-trust-architecture.

[24] D. K. Saini, H. Saini, and S. Singh, "Security and Trust Model Analysis for Banking System," Int. J. Sensors, Wirel. Commun. Control, vol. 11, no. 1, 2019, doi: 10.2174/2210327910666191218130129.

[25] Z. Zaheer, H. Chang, S. Mukherjee, and J. Van Der Merwe, "EZTrust: Network-Independent Zero-Trust Perimeterization for Microservices," 2019, doi: 10.1145/3314148.3314349.

[26] E. Dean, S. Fonyi, C. Morrell, M. Lanham, and E. Teague, "Toward a Zero Trust Architecture Implementation in a University Environment," Cyber Def. Rev., pp. 37–45, 2021.

[27] T. Lukaseder, M. Halter, and F. Kargi, "Context-based Access Control and Trust Scores in Zero Trust Campus Networks," Lect. Notes Informatics, vol. 53, pp. 53–65, 2020.

[28] R. Vanickis, P. Jacob, S. Dehghanzadeh, and B. Lee, "Access Control Policy Enforcement for Zero-Trust-Networking," 2018, doi: 10.1109/ISSC.2018.8585365.

[29] C. Decusatis, P. Liengtiraphan, A. Sager, and M. Pinelli, "Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication," 2016, doi: 10.1109/SmartCloud.2016.22.

[30] S. Li, M. Iqbal, and N. Saxena, "Future Industry Internet of Things with Zero-trust Security," Inf. Syst. Front., 2022, doi: 10.1007/s10796-021-10199-5.

[31] O. C. Edo, A. Okafor, and Akhigbodemhe Emmanuel Justice, "Corporate Taxes and Foreign Direct Investments: An Impact Analysis," Public Policy Adm. Res., 2020, doi: 10.7176/ppar/10-9-07.

[32] O. C. Edo, A. Okafor, and A. E. Justice, "Tax Policy and Foreign Direct Investment: A Regime Change Analysis.," GATR J. Financ. Bank. Rev., vol. 5, no. 3, 2020, doi: 10.35609/jfbr.2020.5.3(3).

[33] J. Petters, "What is Zero Trust? A Security Model," Inside Out Security Blog, 2021. https://www.varonis.com/blog/what-is-zero-trust.

[34] L. Odell, B. Farrar-Folley, C. Fauntleroy, and R. Wagner, "In-Use and Emerging Disruptive Technology Trend," Inst. Def. Anal., 2015.

[35] F. K. Hansen, "6 Redistribution of Income in Denmark," Int. J. Sociol., vol. 16, no. 3–4, 1986, doi: 10.1080/15579336.1986.11769914.

[36] R. Bernard, G. Bowsher, and R. Sullivan, "Cyber security and the unexplored threat to global health: a call for global norms," Glob. Secur. Heal. Sci. Policy, vol. 5, no. 1, 2020, doi: 10.1080/23779497.2020.1865182.

[37] V. Ngo-Lam, "Zero Trust Architecture: Best Practices for Safer Networks," Exabeamm, 2020. https://www.exabeam.com/information-security/zero-trust-architecture/#:~:text=For example%2C an attacker who,prioritizes protection against insider threats.

[38] C. and infrastructure security Agency, "Multi-factor authentication," Defend Today Secure Tommorrow, 2021. https://www.cisa.gov/sites/default/files/publications/CISA MultiFactor Auth HDO_040721_508.pdf.

[39] AlgoSec, "Micro-segmentation from strategy to execution." [Online]. Available: https://www.algosec.com/wp-content/uploads/2020/06/Micro-segmentation-eBook_FINAL.pdf.

[40] S. Tyagi, "7 Key Tenets of Zero Trust Architecture," Colortokens, 2021. https://colortokens.com/blog/key-tenets-zero-trust-architecture/.

[41] NIST, "[NIST SP 800-207] Zero Trust Architecture," 2020.