UNEC Journal of Computer Science and Digital Technologies
Volume 1, № 1, 2025, pp. 69-82
https://doi.org/10.30546/UNECCSDT.2025.01.069

Section:
Cybersecurity & Privacy

Is Zero Trust the Future of Cyber Defence? An Analysis of Principles, Adoption, and Effectiveness

Guliyeva Asya[1], Guliyeva Goncha[2*]

[1, 2*] *Department of Digital Technologies and Applied Informatics, UNEC, Baku, Azerbaijan*
[1] *0009-0009-4132-0848, quliyeva.asya@unec.edu.az*
[2*] *0009-0006-4061-4113, guliyeva.gonjha.ikram.2022@unec.edu.az*

Abstract

Traditional network security models face increasing challenges due to evolving cyber threats and shifting IT environments. The Zero Trust model, which operates on the principle that no user, device, or system should be implicitly trusted regardless of network location, has gained significant attention in both research and practice. Despite its promise to address modern cybersecurity demands, widespread adoption of Zero Trust remains uneven, and questions persist regarding its practical benefits, implementation challenges, and long-term viability. This article aims to consolidate current knowledge on Zero Trust by examining its fundamental principles, architectural components, and enabling technologies. Additionally, we conducted a survey with IT professionals and academics to gather empirical insights on awareness, adoption levels, and perceived effectiveness of Zero Trust Security. Our analysis reveals that while Zero Trust is increasingly recognized for enhancing security posture and mitigating insider and advanced threats, obstacles such as lack of expertise and organizational resistance impede broader implementation. The findings highlight gaps in both academic research and practical guidance, underscoring the need for further study on deployment strategies, cost-benefit analyses, and user experience. This work provides a foundation for future research and practical efforts to advance Zero Trust as a robust cybersecurity framework.

Keywords: zero trust architecture, cybersecurity, micro-segmentation, network security, advanced persistent threats, continuous monitoring

Received:	*Revised:*	*Accepted:*	*Published:*
28/05/2025	*04/06/2025*	*08/06/2025*	*14/06/2025*

1. Introduction

Traditional cybersecurity models have primarily depended on perimeter-based defenses such as firewalls, virtual private networks (VPNs), and network segmentation [1]. These approaches operate under the assumption that entities inside the network boundary are inherently trustworthy, while threats come from outside. However, this assumption has become increasingly outdated and inadequate in addressing today's complex cyber threat landscape. The growing sophistication of cyberattacks—including advanced persistent threats (APTs), ransomware, and insider threats—has exposed significant vulnerabilities in traditional models [2]. According to IBM's *Cost of a Data Breach Report 2024*, the global average cost of a data breach reached a record high of USD 4.9 million, marking a 10% increase over the previous year, underscoring the urgent need for more resilient cybersecurity frameworks [3].

As technology continues to evolve, and with the widespread adoption of virtual working environments, organizations face unprecedented challenges in protecting their digital assets. The rise of cloud computing and remote access means data no longer resides within a fixed perimeter but is accessed from diverse locations and devices. Moreover, the rise of cloud computing, mobile workforces, and bring-your-own-device (BYOD) policies has blurred traditional network boundaries, rendering perimeter-centric defenses less effective in protecting sensitive resources dispersed across diverse environments [4]. This dynamism renders perimeter-based security frameworks ineffective in meeting modern information security demands. Consequently, there is a pressing need for more proactive, adaptive, and comprehensive security models that can effectively safeguard organizational resources regardless of where or how they are accessed. Zero Trust Security (ZTS), first introduced by analyst John Kindervag in 2010 [5], represents such a paradigm shift. The core principle of Zero Trust is “never trust, always verify” [6], eliminating implicit trust based on network location. Instead, every access request must be authenticated, authorized, and continuously validated, irrespective of whether the user or device is inside or outside the traditional network boundary. This approach emphasizes strict identity verification, least privilege access, and continuous monitoring to minimize attack surfaces and contain potential breaches. According to a 2021 survey by Microsoft Security found that 96 percent of security decision-makers consider Zero Trust cybersecurity pivotal to their organization’s success, citing strengthened overall security posture and improved user experience as key benefits [7].

This article aims to explore the growing prominence of Zero Trust Security and critically evaluate its potential as the future of cybersecurity. By examining the fundamental principles of Zero Trust, its implementation challenges, and the increasing relevance in today’s evolving cyber landscape, this paper seeks to provide insights into whether Zero Trust is poised to replace traditional security models or coexist alongside them as a necessary complement.

2. Zero Trust Architecture

Zero Trust Architecture (ZTA) is a modern cybersecurity framework designed to fundamentally rethink how organizations protect their IT environments. Unlike traditional security models that rely on perimeter-based defenses and assume that entities inside the network are trustworthy, ZTA operates on the premise that no user, device, or system should be inherently trusted—regardless of its location or origin [8]. Every resource, data source, and computing service, whether hosted on-premises, in the cloud, or accessed via personal devices, is treated as a protected asset requiring strict verification. This approach acknowledges the increasing complexity of enterprise IT landscapes, where cloud computing, mobile workforces, and interconnected devices expand the attack surface. Consequently, communication between any two entities must be secured and authenticated, regardless of network location, ensuring that confidentiality, integrity, and identity verification are continuously enforced. In this section, we explore the foundational tenets that underpin Zero Trust, the key components that make it operational, and the technologies that enable its practical implementation.

2.1 Core Tenets of Zero Trust

Zero Trust Architecture is grounded on several fundamental tenets that collectively establish a resilient and adaptive cybersecurity posture. As outlined by the National Institute of Standards and Technology (NIST) Special Publication 800-207 [8], these tenets include:

1. All data sources and computing services are treated as protected resources, regardless of whether they reside on traditional enterprise-owned devices, cloud services, or personal devices accessing corporate data.

2. Communication between all resources must be secured irrespective of their network location. Every access request, whether originating from inside or outside the corporate

network, must meet stringent security requirements to ensure confidentiality, integrity, and authentication.

3. Access to resources is granted dynamically on a per-session basis and always follows the principle of least privilege. Trust is never assumed by default, even for repeated requests; instead, continuous evaluation of the requester's identity and context is required before access is approved. Importantly, authorization to one resource does not imply access to others.

4. Access decisions are governed by dynamic policies that incorporate multiple factors, such as the identity and behavior of the user or device, the sensitivity of the resource, and environmental conditions like time and location.

5. Continuous monitoring and assessment of all assets' security posture is essential. No device or user is inherently trusted; instead, enterprises must constantly evaluate the integrity and compliance of endpoints, applying restrictions or denying access as needed based on their security status.

6. Authentication and authorization processes are dynamic and strictly enforced throughout the lifecycle of a session or transaction. This includes the use of strong identity and access management tools, such as multi-factor authentication, and ongoing verification to adapt to emerging threats or anomalous behavior.

7. Enterprises collect and analyze extensive telemetry from assets and network activity to inform and improve their security posture continuously. This data-driven approach enhances policy enforcement and helps detect and respond to threats in real-time.

2.2 Key Logical Components of Zero Trust

Zero Trust Architecture relies on a set of integrated components that govern how access decisions are made, implemented, and enforced across an enterprise's digital ecosystem. At the center of this architecture are three key logical functions: *The Policy Engine (PE), Policy Administrator (PA), and Policy Enforcement Point (PEP)* [9]. These components work together to ensure that every access request is subject to rigorous verification, based on real-time data and context, before being granted. Their coordinated operation forms the decision-making and control infrastructure that distinguishes Zero Trust from traditional security models.

The Policy Engine (PE) serves as the brain of the Zero Trust system [8]. It is responsible for evaluating access requests and making the final authorization decisions. Unlike legacy models that rely on predefined access control lists or simple perimeter rules, the PE applies a combination of dynamic risk-based policies, contextual data, and behavioral analytics to determine whether access should be granted. It processes inputs such as user identity, device health, location, time of request, type of resource requested, and even previously observed behavior patterns. These variables are assessed in accordance with organizational policies and risk tolerance levels. The Policy Engine does not operate on static parameters alone; it continuously analyzes real-time signals to ensure that trust is established and maintained throughout the access lifecycle. As a result, decisions are session-based and can change at any time based on new risk information.

Once the PE has made an access decision, the Policy Administrator (PA) takes over to implement it. The PA is responsible for coordinating between the decision-making logic and the enforcement infrastructure. It configures the environment to allow or deny access by interacting with network controllers, endpoint agents, identity services, or other control mechanisms. For example, if a user is granted access to a cloud-hosted database, the PA ensures that the proper session is created with exactly the level of access permitted—no more, no less. This component is especially critical in dynamic environments, as it can also revoke or adjust access mid-session if conditions change (e.g., a device becomes non-compliant, or anomalous behavior is detected). Importantly, the PA itself does not enforce access at the data plane level; instead, it orchestrates enforcement based on the PE's decisions.

Together, the Policy Engine and Policy Administrator make up what is commonly referred to as the Policy Decision Point (PDP) [10]. The PDP is responsible for both evaluating and executing access control decisions, though it does not enforce them directly. This separation of duties enhances modularity and scalability, and ensures a more flexible security architecture that can adapt in real time to changing conditions.

The Policy Enforcement Point (PEP) is the final stage in the Zero Trust decision pipeline. This is the component that physically or logically enforces access by sitting between the subject (such as a user, device, or application) and the resource being requested. It ensures that only traffic approved by the Policy Administrator is allowed to proceed. Depending on the architecture and deployment model, PEPs can take many forms: they may be firewalls configured with dynamic rules, endpoint security agents, software-defined networking components, API gateways, or cloud-native access brokers. The PEP monitors active sessions and can terminate them immediately if the policy state changes—such as when new risks emerge or compliance status is lost. This real-time enforcement capability ensures that Zero Trust is not a one-time check but a continuous verification process.

Together, the Policy Engine, Policy Administrator, and Policy Enforcement Point create a highly adaptable and intelligent security infrastructure. This triad supports continuous access evaluation, dynamic policy enforcement, and fine-grained control over enterprise resources. Unlike perimeter-based models, which typically operate on implicit trust within the network boundary, Zero Trust's architecture demands that trust is earned and continuously validated, not assumed [11]. This results in significantly improved resilience against internal and external threats, even in complex environments that include remote users, cloud services, and personal devices.

Figure 1. illustrates the core logical components of Zero Trust Architecture—Policy Engine, Policy Administrator, and Policy Enforcement Point—and their interactions in the access decision and enforcement process.

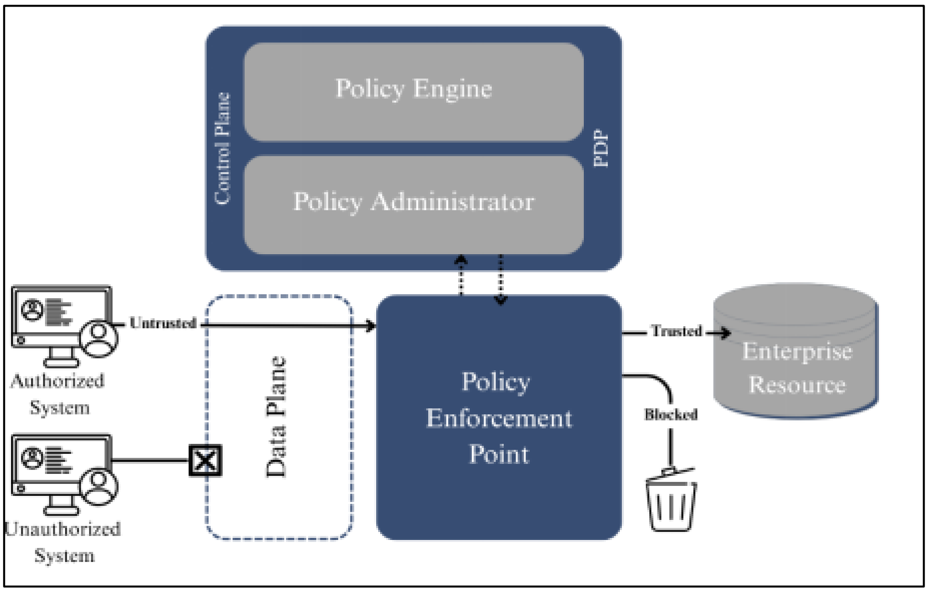

Figure 1. Interactions of logical components of Zero Trust Architecture in the access decision and enforcement process.

2.3 Security Technologies Enabling Zero Trust

While the Policy Engine, Policy Administrator, and Policy Enforcement Point form the foundation for decision-making and enforcement in Zero Trust Architecture, the practical implementation of ZTA is supported by several critical security technologies and functional components. These components ensure that access control, continuous verification, and threat detection are not only policy-driven but also embedded into the organization's daily operations.

Among the most essential technologies that enable Zero Trust are *Least Privilege, Micro-Segmentation, Identity and Access Management (IAM), and Continuous Monitoring* [12, 13].

Least Privilege is a fundamental security principle that limits users, devices, and applications to only the minimum levels of access necessary to perform their legitimate functions. By restricting permissions, organizations reduce the attack surface and mitigate the risk of privilege escalation and insider threats. This principle is implemented through tools such as role-based access control (RBAC) and just-in-time (JIT) access [14], which grant temporary permissions aligned with user roles and task requirements. In a Zero Trust context, access rights are continuously re-evaluated to ensure they remain appropriate, minimizing unnecessary exposure to sensitive resources.

Micro-Segmentation plays a pivotal role in enhancing network security within Zero Trust frameworks [15]. It involves dividing the broader network into smaller, isolated segments or zones, each protected by its own security policies. This containment strategy limits an attacker's ability to move laterally across the network if they compromise one segment. John Kindervag, the originator of the Zero Trust concept, emphasizes the importance of micro-segmentation by stating that "*your Zero Trust security project is incomplete if you don't have micro-segmentation.*" [16]. This technique is particularly vital in today's cloud and hybrid environments, where traditional perimeter defenses are insufficient. Micro-segmentation ensures that even within trusted environments, strict controls govern access between systems and applications.

Figure 2. illustrates the difference in network security posture between traditional networks without micro-segmentation and networks employing micro-segmentation, highlighting how segmentation limits lateral movement and strengthens overall security.

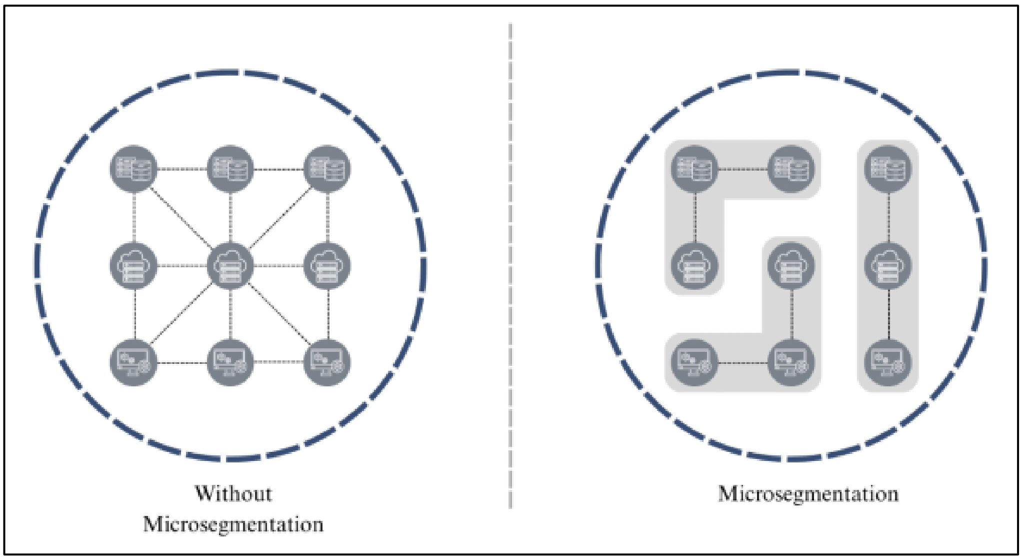

Figure 2. Comparison Between Network Security Without Micro segmentation and With Micro segmentation

Identity and Access Management (IAM) serves as the cornerstone of Zero Trust by managing and verifying the identities of users, devices, and applications. IAM systems implement robust authentication mechanisms such as multi-factor authentication (MFA) and single sign-on (SSO), ensuring that access requests are thoroughly verified before being approved [17]. IAM also supports adaptive authentication, which adjusts security requirements based on contextual factors like device health, location, and behavior patterns. By centralizing and automating identity management, IAM enables organizations to enforce consistent, fine-grained access controls aligned with Zero Trust principles.

Finally, Continuous Monitoring is essential for maintaining the security posture of a Zero Trust environment. It involves real-time tracking and analysis of network traffic, user behavior, device compliance, and environmental conditions to detect anomalies and potential threats as they arise. Security Information and Event Management (SIEM) systems, coupled with User and Entity Behavior Analytics (UEBA), provide the visibility and insights needed to respond quickly to suspicious activities [18]. Continuous monitoring ensures that access decisions remain dynamic and adaptive, allowing organizations to proactively mitigate risks before they lead to breaches.

Together, these security technologies form a comprehensive and practical foundation for implementing Zero Trust Architecture. They operationalize the core tenets of Zero Trust by ensuring that trust is never implicit, access is always verified, and the security posture adapts continuously to evolving threats.

2.4 Steps to Implement Zero Trust

Implementing Zero Trust Architecture requires a structured approach that aligns security efforts with an organization's critical assets and operational realities. The following five steps provide a practical roadmap for adopting Zero Trust principles effectively [19, 20]:

*1. Define the Protect Surface.*The first step is to identify the most critical data, assets, applications, and services—collectively called the protect surface—that require stringent protection. This focused approach helps organizations prioritize resources and apply security controls specifically tailored to safeguard their most valuable and sensitive components.

*2. Map the Transaction Flows.*Once the protect surface is established, organizations must understand how data flows across their environment. This involves mapping how users, devices, and applications interact with protected assets and each other. Comprehensive transaction flow mapping uncovers potential vulnerabilities and informs the design of policies that control and monitor access precisely, limiting unnecessary or risky interactions.

*3. Architect a Zero Trust Network.*With a clear understanding of transaction flows, organizations design a segmented and secure network architecture. This step typically involves implementing micro-segmentation to create isolated zones around protected assets. By controlling and restricting communication between segments, the network becomes resilient to lateral movement by attackers, effectively containing breaches and minimizing impact.

*4. Deploy Policy Enforcement Mechanisms.*Next, organizations implement technical controls that enforce Zero Trust policies. Policy Enforcement Points (PEPs) such as firewalls, gateways, and endpoint agents are configured to verify every access request dynamically. These mechanisms ensure that only authenticated and authorized users or devices gain access to resources, and they continuously monitor sessions to detect and respond to policy violations or anomalous behavior.

*5. Continuous Monitoring and Response.*Zero Trust is not a set-and-forget strategy. Continuous monitoring is critical to maintain security posture by tracking user behavior, device health, network activity, and environmental conditions in real time. Using tools such as Security Information and Event Management (SIEM) and User and Entity Behavior Analytics (UEBA), organizations can detect suspicious activity quickly and automate responses to contain threats before they escalate.

3. Comparison of Traditional Security and Zero Trust Architecture

While the foundational differences between traditional security models and Zero Trust Architecture have been introduced earlier, it is essential to examine how these approaches diverge in practical implementation and technical capabilities. Traditional security models primarily rely on perimeter defenses, such as firewalls and VPNs, which implicitly trust users and devices once they are inside the network boundary. This implicit trust model creates significant vulnerabilities, as attackers who breach the perimeter can move laterally within the network with minimal resistance. In contrast, Zero Trust Architecture eliminates the assumption of trust based solely on network location, enforcing strict verification for every access request regardless of origin [21]. This approach incorporates continuous authentication, dynamic policy enforcement, micro-segmentation, and comprehensive monitoring, resulting in a more resilient security posture capable of adapting to modern, distributed IT environments. Zero Trust rigorously applies the principle of least privilege, ensuring users and devices have access only to the resources necessary for their tasks. Additionally, it leverages technologies such as micro-segmentation to restrict lateral movement, thereby reducing the impact of potential breaches. Another key distinction lies in visibility and control. Traditional models often lack granular insight into user behavior and device posture once inside the network perimeter. By design, Zero Trust integrates continuous monitoring and advanced analytics, enabling rapid detection of anomalies and adaptive responses to emerging threats.

To provide a clearer distinction between traditional security models and Zero Trust Architecture, the following *Table 1* compares these approaches across several key dimensions.

Aspect	Traditional Security Model	Zero Trust Model
Trust Model	Implicit trust inside network perimeter	Never trust, always verify for every access request
Network Segmentation	Broad network segmentation (typically relying on a single trusted network)	Fine-grained micro-segmentation to isolate network segments
Access Control	Static, perimeter-based access policies	Dynamic, context-aware, least privilege access policies
Authentication	One-time authentication when inside perimeter	Continuous authentication and reauthorization
Visibility & Monitoring	Limited internal visibility and control	Continuous monitoring, real-time threat detection, and analytics
Response to Breach	Reactive, based on perimeter alarms	Proactive, adaptive response to internal and external threats
Support for Remote Work	Limited, relies on VPNs	Built-in support for secure remote access via cloud and hybrid environments
Scalability	Difficult to scale securely with cloud, hybrid, or mobile environments	Scalable across diverse environments with secure access to all resources
Adaptability	Limited adaptability to new threats, technology, and network changes	Highly adaptable to emerging threats, dynamic conditions, and evolving technologies

Table 1. Comparison of Traditional Security and Zero Trust Models (Based on data from Azath Hussain, 2022)

This comparison highlights how Zero Trust's dynamic, data-centric security model addresses the shortcomings of traditional perimeter-based defenses, particularly in today's complex and distributed IT environments [22].

4. Effectiveness and Adoption of Zero Trust Security

This section explores the key benefits of the Zero Trust security model and presents empirical data from a recent survey to provide insights into its current adoption, perceived effectiveness, and implementation challenges.

4.1 Benefits of Zero Trust

Because Zero Trust Framework is a holistic approach [4], it offers several significant advantages that strengthen an organization's overall cybersecurity posture while addressing the challenges of modern digital environments.

Enhanced Cybersecurity. Zero Trust fundamentally reduces risk by eliminating implicit trust and enforcing strict access controls based on continuous verification. By authenticating and authorizing every access request dynamically, organizations can minimize unauthorized access and significantly lower the likelihood of data breaches. The framework's focus on protecting critical assets and applying the principle of least privilege reduces the attack surface and limits potential damage from any single compromised account or device.

Mitigating Insider Threats. Insider threats—whether malicious or accidental—pose substantial risks to organizational security [23]. Zero Trust mitigates these risks by continuously monitoring user behavior and enforcing granular access policies that restrict users to only the resources necessary for their role. This prevents unnecessary access and lateral movement within networks, reducing the opportunity for insiders to exploit privileged access.

Defending Against Advanced Persistent Threats (APTs) and Cyberattacks Advanced threats such as APTs and ransomware increasingly target enterprises through sophisticated, multi-stage attacks designed to evade traditional defenses. Zero Trust's micro-segmentation and dynamic policy enforcement disrupt these attack paths by limiting lateral movement and requiring continuous reauthentication [24]. These measures make it harder for attackers to establish persistent footholds and escalate privileges, enhancing resilience against complex cyberattacks.

*Improved End-User Experience.*While security is paramount, user experience must not be compromised. Zero Trust enables secure access from anywhere, supporting cloud services and remote work environments seamlessly [25]. Through technologies like single sign-on (SSO) and adaptive authentication, users benefit from streamlined access processes without excessive friction, balancing security with productivity.

*Improved Monitoring and Alerting.*Monitoring a Zero Trust environment can be complex, but the right tools make it manageable and highly effective. Security Information and Event Management (SIEM) systems, Security Orchestration, Automation, and Response (SOAR) platforms, and Network Detection and Response (NDR) tools leverage log and event analysis combined with artificial intelligence to identify security incidents rapidly. These capabilities provide Security Operations Center (SOC) administrators with actionable insights and enable automated or accelerated responses, reducing dwell time and mitigating threats before they escalate [26].

4.2 Adoption and Implementation: Survey Results

To gain empirical insights into the current state of Zero Trust adoption and perceptions, a survey was conducted by the authors of this article with 100 participants in Azerbaijan, including IT and cybersecurity professionals, academic researchers, and students specializing in IT and cybersecurity. The results revealed that a majority—85%—are familiar with Zero Trust Security concepts, with 40% being very familiar and 45% somewhat familiar.

Regarding organizational adoption, 31% reported that their organizations have fully implemented Zero Trust, while 35% are currently in the process of implementation. Respondents identified multiple primary reasons for adopting or considering Zero Trust. Protecting sensitive data was the leading motivation, cited by 50% of participants. Defending against ransomware and advanced persistent threats (APTs) followed closely at 46%, with 42% emphasizing mitigation of insider threats. Meeting regulatory compliance requirements was also significant, reported by 35% of respondents.

Multi-factor authentication (MFA) emerged as the most widely implemented technology supporting Zero Trust, followed by Identity and Access Management (IAM) systems and endpoint security solutions. Cloud security tools and micro-segmentation were also utilized, often in combination, illustrating a layered and integrated approach to Zero Trust implementation (see *Figure 3* for the survey results).

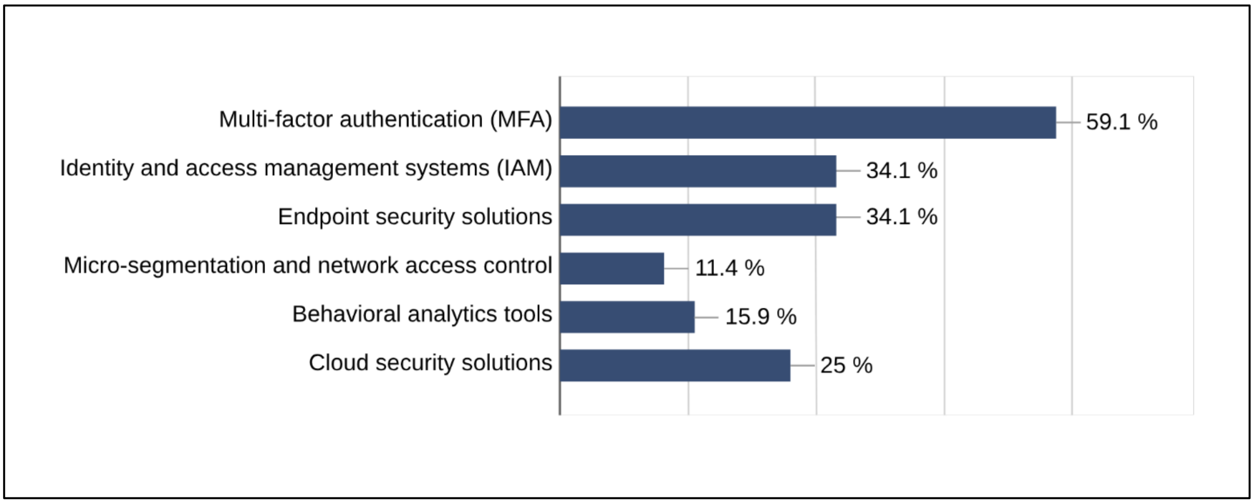

Figure 3. Results of the survey question: 'What technologies or tools have you implemented to support Zero Trust Security?

In terms of effectiveness, 44% of participants rated Zero Trust as *very effective* and 45% as *somewhat effective* in protecting against insider threats, with only 1% perceiving it as ineffective. Despite growing adoption, significant challenges remain; notably, 50% of respondents cited lack of expertise or knowledge as the biggest barrier, followed by organizational resistance to change (35%) and complexity of implementation, additional concerns were high costs and difficulties integrating Zero Trust with existing systems.

When asked about the future dominance of Zero Trust, responses were almost evenly split: 39% believe Zero Trust will be widely adopted but will not fully replace traditional models, while another 39% expect it to replace traditional security entirely within the next five years. Others were uncertain or believed traditional models will continue to dominate.

These results indicate a positive trend towards embracing Zero Trust principles, yet highlight persistent obstacles that organizations must overcome to fully realize its benefits. The survey underscores the need for continued education, resource allocation, and strategic planning to advance Zero Trust initiatives effectively.

The survey results summarized in this article are available upon request from the author.

The Future of Zero Trust

Zero Trust Security has rapidly emerged as a foundational framework for modern cybersecurity, but its future evolution will be shaped by ongoing technological advancements, organizational adoption, and evolving threat landscapes. As enterprises increasingly embrace cloud computing, hybrid environments, and the Internet of Things (IoT) [27], the principles of Zero Trust are poised to become even more critical for securing diverse and dynamic ecosystems.

One major trend shaping the future of Zero Trust is the growing integration of artificial intelligence (AI) and machine learning (ML) [28]. These technologies enhance continuous monitoring and threat detection by enabling more accurate anomaly identification and faster response times. AI-driven automation can also reduce the operational complexity associated with Zero Trust implementations, helping organizations overcome challenges related to scale and resource constraints. Additionally, the expansion of decentralized identity frameworks and blockchain-based authentication mechanisms promises to strengthen identity verification processes, a core tenet of Zero Trust [29]. These innovations can provide users with greater control over their credentials while improving security and privacy.

However, widespread adoption still faces hurdles. Challenges such as legacy system integration, organizational resistance, and the need for specialized expertise remain significant barriers [30]. Addressing these will require ongoing investment in education, workforce development, and the evolution of more user-friendly and interoperable Zero Trust tools.

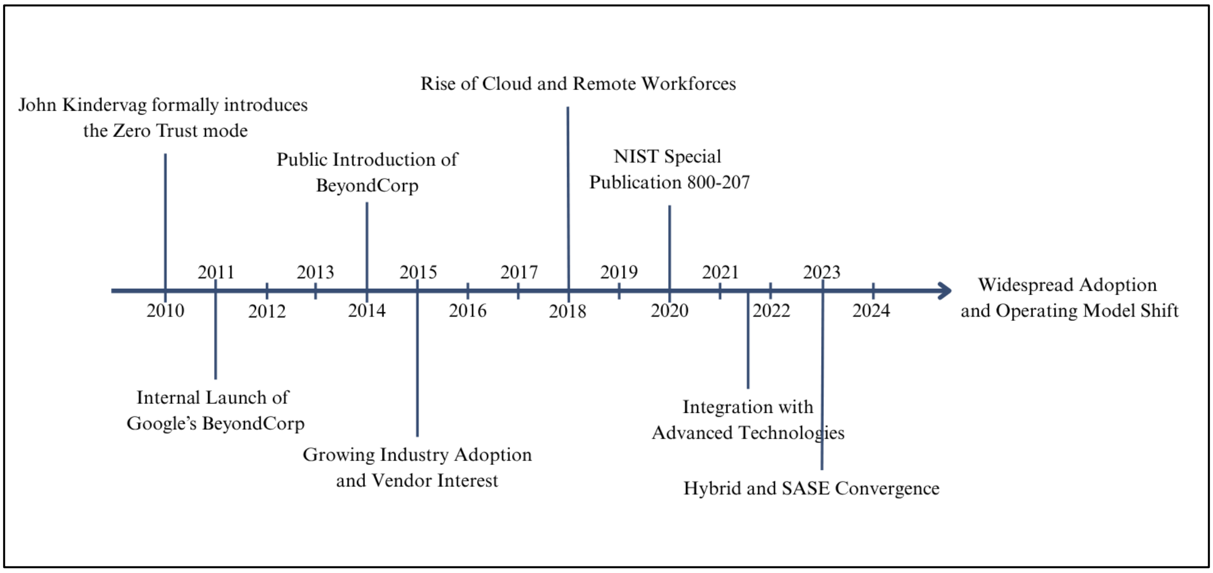
John Kindervag formally introduces the Zero Trust mode
Rise of Cloud and Remote Workforces
Public Introduction of BeyondCorp
NIST Special Publication 800-207
2011
2013
2015
2017
2019
2021
2023
2010
2012
2014
2016
2018
2020
2022
2024
Widespread Adoption and Operating Model Shift
Internal Launch of Google's BeyondCorp
Growing Industry Adoption and Vendor Interest
Integration with Advanced Technologies
Hybrid and SASE Convergence

Figure 4. Evolution of Zero Trust Security from 2010 to Present and Beyond.

Looking ahead, Zero Trust is likely to evolve from a security model to a pervasive security operating model—one that is embedded into every layer of an organization's IT infrastructure and culture. Hybrid approaches that combine Zero Trust with complementary frameworks, such as Secure Access Service Edge (SASE) [31], will also gain traction to provide holistic, context-aware security across networks and cloud environments.

Figure illustrates the key milestones in the evolution of Zero Trust Security, highlighting foundational concepts, major industry initiatives, and emerging trends shaping its future.

2010 – Concept Introduction by John Kindervag [32]

John Kindervag, an analyst at Forrester Research, introduced the term "Zero Trust" in 2010. He emphasized the principle of "never trust, always verify," advocating for the elimination of implicit trust within network perimeters.

2011 – Google's BeyondCorp Initiative [5]

Google begins developing the BeyondCorp initiative in response to the Operation Aurora attacks. This marks one of the first enterprise-scale efforts to implement Zero Trust principles internally, focusing on user and device-based access controls rather than network location.

2014 – Public Introduction of BeyondCorp [5]

Google publishes the first academic paper on BeyondCorp, detailing its internal Zero Trust implementation. This public release helps shape the industry's understanding of Zero Trust in large-scale, real-world environments.

2015 – Early Adoption and Framework Development [33]

By 2015, industry interest in Zero Trust grew, with organizations exploring concepts like micro-segmentation and least privilege access. Vendors began offering solutions aligning with Zero Trust principles, marking the early stages of framework development.

2018 – Rise of Cloud and Remote Workforces [17]

The accelerated adoption of cloud services and the expansion of mobile workforces in 2018 drove the integration of Identity and Access Management (IAM) and Multi-Factor Authentication (MFA) into Zero Trust frameworks as standard components.

2020 – NIST Special Publication 800-207 [21]

In August 2020, the National Institute of Standards and Technology (NIST) published Special Publication 800-207, providing formal guidelines and definitions for Zero Trust Architecture. This publication bolstered the credibility and adoption of Zero Trust principles in both government and enterprise sectors.

2021–2022 – Integration with Advanced Technologies [28]

During this period, Artificial Intelligence (AI) and Machine Learning (ML) technologies enhanced continuous monitoring and threat detection within Zero Trust frameworks. Vendors integrated Zero Trust with Security Orchestration, Automation, and Response (SOAR) and Network Detection and Response (NDR) solutions to bolster security postures.

2023 – Hybrid and SASE Convergence [31]

In 2023, Zero Trust principles increasingly converged with Secure Access Service Edge (SASE) architectures. This convergence focused on securing hybrid cloud and edge environments, enabling organizations to provide secure access regardless of user location or device.

2024 and Beyond – Widespread Adoption and Operating Model Shift
Gartner forecasts that by 2027, 40% of large organizations with remote zero-trust network access (ZTNA) will extend to location-agnostic enforcement. This shift will replace legacy technologies, simplifying access policies and further reducing attack surfaces—an increase from less than 10% of organizations employing such measures in 2024 [34].

Final Assessment Considering the increasing adoption rates, technological advancements, and industry emphasis, Zero Trust is well-positioned to become the dominant cybersecurity model within the next 5 to 10 years. While some organizations may continue to rely on traditional perimeter-based models, the complexity of modern threats and infrastructure makes Zero Trust's adaptive, identity-centric approach indispensable. Therefore, Zero Trust is not only a promising framework for today but is likely to define the future standard in cybersecurity.

5. Conclusion

This article has explored the core principles, architecture, and enabling technologies of Zero Trust Security as a response to the limitations of traditional perimeter-based cybersecurity models. By emphasizing continuous verification, least privilege access, and dynamic policy enforcement, Zero Trust offers a robust framework to secure increasingly complex and distributed IT environments. The comparison between traditional security and Zero Trust highlights the enhanced adaptability, granular control, and improved threat detection capabilities that make Zero Trust well-suited for today's evolving threat landscape.

Empirical survey results underscore a growing awareness and adoption of Zero Trust across industries, driven primarily by the need to protect sensitive data and defend against advanced cyber threats such as ransomware and insider attacks. However, significant challenges remain, particularly regarding organizational resistance, expertise shortages, and integration complexities, which must be addressed to achieve widespread implementation.

Looking ahead, advancements in artificial intelligence, machine learning, and identity management technologies are expected to further strengthen Zero Trust capabilities and simplify its deployment. As organizations continue to face sophisticated cyber threats and adopt hybrid and cloud-based infrastructures, Zero Trust is poised to evolve from a security framework into a pervasive security operating model embedded throughout enterprise environments. Given current trends and expert forecasts, Zero Trust is likely to become the dominant cybersecurity model in the coming decade, providing a resilient and adaptive foundation for future cyber defense.

Acknowledgment

The authors would like to express their sincere gratitude to all the participants of the survey who contributed valuable insights to this study. We would also like to thank the staff of the Department of Digital Technologies and Applied Informatics of the Azerbaijan State University of Economics for their support and resources throughout this research.

Authors' Declaration

Conflicts of Interest: The authors declare that there is no conflict of interest regarding the publication of this article.

Authors' Contribution Statement

Guliyeva Asya Mammadkarim: Supervised the research, provided academic guidance throughout the process, reviewed the article drafts, and contributed to the final revisions.

Guliyeva Goncha Ikram: Conceived the idea for the article, conducted the survey, analyzed the data, and wrote the majority of the article.

References

1. Ojha, Nitish, and Abhishek Vaish. "Why Perimeter Security is No Longer Enough: Observations and Open Challenges." *Zero-Trust Learning*. Apple Academic Press, 2025. 305-328. [Online]. Available: https://www.taylorfrancis.com/chapters/edit/10.1201/9781779643575-15/perimeter-security-longer-enough-observations-open-challenges-nitish-ojha-abhishek-vaish
2. Sharma, Amit, et al. "Advanced persistent threats (apt): evolution, anatomy, attribution and countermeasures." Journal of Ambient Intelligence and Humanized Computing 14.7 (2023): 9355-9381. https://doi.org/10.1007/s12652-023-04603-y
3. IBM, "Cost of a Data Breach Report 2024," [Online]. Available: https://www.ibm.com/reports/data-breach , 2024.
4. Capili, Mirene. *Simulation-Based Evaluation of Perimeter-Based and Zero Trust Security Implementation on Internet of Things*. Diss. The George Washington University, 2024. [Online]. Available: https://www.proquest.com/openview/7c58a16d2f8f82d1f9e91446a90151d0/1?pq-origsite=gscholar&cbl=18750&diss=y
5. Adamson, Kazeem Mutiu, and Amna Qureshi. "Zero Trust 2.0: Advances, Challenges, and Future Directions in ZTA." (2025). https://doi.org/10.21203/rs.3.rs-6602547/v1
6. Adahman, Z., Malik, A.W. and Anwar, Z., 2022. An analysis of zero-trust architecture and its cost-effectiveness for organizational security. *Computers & Security*, *122*, p.102911. https://doi.org/10.1016/j.cose.2022.102911

7. Microsoft, "Zero Trust Adoption Report: How does your organization compare?" [Online]. Available: https://www.microsoft.com/en-us/security/blog/2021/07/28/zero-trust-adoption-report-how-does-your-organization-compare/ , 2021.
8. Stafford, V., 2020. Zero trust architecture. NIST special publication, 800(207), pp.800-207. https://doi.org/10.6028/NIST.SP.800-207
9. Sheikh, N., Pawar, M. and Lawrence, V., 2021, May. Zero trust using network micro segmentation. In IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 1-6). IEEE. https://doi.org/10.1109/INFOCOMWKSHPS51825.2021.9484645
10. Anatias, Lesky Deni Saputra. DESIGN AND IMPLEMENTATION OF A TRUST POLICY DECISION POINT (TRUST PDP). Diss. EINDHOVEN UNIVERSITY OF TECHNOLOGY, 2009. [Online]. Available: https://pure.tue.nl/ws/files/46965635/658578-1.pdf
11. Poirrier, Alexandre, Laurent Cailleux, and Thomas Heide Clausen. "Is Trust Misplaced? A Zero-Trust Survey." Proceedings of the IEEE (2025). https://doi.org/10.1109/JPROC.2025.3555131
12. Hasan, Mahmud. "Enhancing Enterprise Security with Zero Trust Architecture." arXiv preprint arXiv:2410.18291 (2024). https://doi.org/10.48550/arXiv.2410.18291
13. Rebouças Filho, W.L., 2025. The Role of Zero Trust Architecture in Modern Cybersecurity: Integration with IAM and Emerging Technologies. Brazilian Journal of Development, 11(1), pp.e76836-e76836. https://doi.org/10.34117/bjdv11n1-060
14. Carter, Matthew Keith. "Techniques to approach least privilege." IDPro Body of Knowledge 1.9 (2022). https://doi.org/10.55621/idpro.88
15. Basta, Nardine, et al. "Towards a zero-trust micro-segmentation network security strategy: an evaluation framework." NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2022. https://doi.org/10.1109/NOMS54207.2022.9789888
16. A. Herrod, "Why There's No Zero Trust Without Microsegmentation," Illumio, 2023. [Online]. Available: https://www.illumio.com/blog/no-zero-trust-without-microsegmentation
17. Ojo, Samson. "Identity and Access Management (IAM) Authentication Methods: Importance of Multi-Factor Authentication (MFA) and Single Sign-On (SSO) and Access Control Models." (2025). https://doi.org/10.20944/preprints202503.1830.v1
18. González-Granadillo, Gustavo, Susana González-Zarzosa, and Rodrigo Diaz. "Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures." Sensors 21.14 (2021): 4759. https://doi.org/10.3390/s21144759
19. Itodo, Cornelius, and Murat Ozer. "Multivocal literature review on zero-trust security implementation." Computers & Security (2024): 103827. https://doi.org/10.1016/j.cose.2024.103827
20. Ghasemshirazi, Saeid, Ghazaleh Shirvani, and Mohammad Ali Alipour. "Zero trust: Applications, challenges, and opportunities." arXiv preprint arXiv:2309.03582 (2023). https://doi.org/10.48550/arXiv.2309.03582
21. Syed, Naeem Firdous, Syed W. Shah, Arash Shaghaghi, Adnan Anwar, Zubair Baig, and Robin Doss. "Zero trust architecture (zta): A comprehensive survey." IEEE access 10 (2022): 57143-57179. https://doi.org/10.1109/ACCESS.2022.3174679
22. Sarkar, S., Choudhary, G., Shandilya, S.K., Hussain, A. and Kim, H., 2022. Security of zero trust networks in cloud computing: A comparative review. *Sustainability*, *14*(18), p.11213. https://doi.org/10.3390/su141811213
23. Singh, A., 2025. From Past to Present: The Evolution of Data Breach Causes (2005–2025). *LatIA*, *3*, pp.333-333. https://doi.org/10.62486/latia2025333
24. Botwright, Rob. *Zero Trust Security: Building Cyber Resilience & Robust Security Postures*. Rob Botwright, 2023. [Online]. Available:

https://books.google.az/books?id=Tp3fEAAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

25. Kim, Haena, Yejun Kim, and Seungjoo Kim. "A study on the security requirements analysis to build a zero trust-based remote work environment." arXiv preprint arXiv:2401.03675 (2024). https://doi.org/10.48550/arXiv.2401.03675
26. Palo Alto Networks, "Network Detection and Response in Zero Trust Environments.," [Online]. Available: https://www.paloaltonetworks.com/zero-trust.
27. Ismail, M. and Abd El-Gawad, A.F., 2023. Revisiting zero-trust security for internet of things. *Sustainable machine intelligence journal*, *3*, pp.6-1. https://doi.org/10.61185/SMIJ.2023.33106
28. Ofili, B.T., Erhabor, E.O. and Obasuyi, O.T., 2025. Enhancing Federal Cloud Security with AI: Zero Trust, Threat Intelligence, and CISA Compliance. *World Journal of Advanced Research and Review*. https://doi.org/10.30574/wjarr.2025.25.2.0620
29. Rivera, Javier Jose Diaz, Afaq Muhammad, and Wang-Cheol Song. "Securing digital identity in the zero trust architecture: A blockchain approach to privacy-focused multi-factor authentication." *IEEE Open Journal of the Communications Society* (2024). https://doi.org/10.1109/OJCOMS.2024.3391728
30. Paul, Freeman. "From Legacy Systems to Zero Trust: Transitioning Your Organization's Security Model." (2022).
31. Patel, Nimeshkumar. "SECURE ACCESS SERVICE EDGE (SASE): EVALUATING THE IMPACT OF CONVEREGED NETWORK SECURITY ARCHITECTURES IN CLOUD COMPUTING." *Journal of Emerging Technologies and Innovative Research* 11.3 (2024): 12. [Online]. Available: https://scholar9.com/publication/4c2f51af09932024b09ce2eac63e1df0.pdf
32. Kindervag, J., 2010. Build security into your network's dna: The zero trust network architecture. Forrester Research Inc, 27, pp.1-16. [Online]. Available: https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf
33. Khan, M.J., 2023. Zero trust architecture: Redefining network security paradigms in the digital age. *World Journal of Advanced Research and Reviews*, *19*(3), pp.105-116. https://doi.org/10.30574/wjarr.2023.19.3.1785
34. Gartner, "Predicts 2025: Scaling Zero-Trust Technology and Resilience," Available: https://www.paloaltonetworks.com/resources/research/gartner-predicts-2025-zero-trust-and-resilience-sase , 2025.