Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2023, 10(6):87-94

Research Article ISSN: 2394 - 658X

Zero Trust Security Architecture: A Paradigm Shift in Data Protection and Access Control

Venkata Baladari

Software Developer, Newark, Delaware, USA
vrssp.baladari@gmail.com

ABSTRACT

A contemporary cybersecurity strategy known as the Zero Trust Security Model aims to eradicate implicit trust and ensure uninterrupted authentication for every user, device, and application. Zero Trust security models diverge from conventional perimeter-based security by anticipating threats within and beyond the network, necessitating rigorous authentication and limitations on user access privileges. Components like Multi-Factor Authentication (MFA), Zero Trust Network Access (ZTNA), micro-segmentation, and AI-driven threat detection strengthen security by reducing vulnerabilities and stopping unauthorized access. The integration of Artificial Intelligence and Machine Learning enhances Zero Trust by facilitating real-time risk assessment and automated reaction to security incidents. Implementation of Zero Trust security comes with its own set of difficulties, such as the intricacies of deployment, problems with integration, and worries about the user experience. As cyber threats become increasingly complex, organizations must place a high priority on implementing Zero Trust to guarantee robust security in cloud-based and hybrid work environments. This study examines the core concepts of Zero Trust, its fundamental technologies, deployment methods, and practical examples to demonstrate its efficacy in safeguarding digital resources. By implementing a Zero Trust model, businesses can substantially lower their cybersecurity vulnerabilities and enhance adherence to regulatory requirements. The research indicates that Zero Trust is a fundamental security strategy for contemporary businesses, providing sustained defense against progressively sophisticated threats.

Keywords: Cybersecurity, Environments, Authentication, Cloud, Security

---

INTRODUCTION

Background and Importance of Cybersecurity

The rapid development of digital technologies has resulted in an exponential rise in cyber threats aimed at individuals, businesses, and government institutions. The increasing use of cloud computing, remote work, and interconnected systems has made traditional security methods relying on perimeter-based defenses inadequate. Cyber attackers are utilizing advanced methods, including ransomware, phishing, and advanced persistent threats (APTs), to evade conventional security systems [1],[2],[3]. Protecting sensitive data and ensuring business continuity is now a top concern that necessitates the implementation of robust cybersecurity plans to safeguard digital assets.

Evolution of Traditional Security Models

Traditionally, organizations have depended on perimeter-based security frameworks, commonly referred to as the "castle-and-moat" method. Within this model, various security measures including firewalls, intrusion detection systems (IDS), and virtual private networks (VPNs) were implemented to establish a robust boundary around an organization's internal network [4],[5]. It was initially considered that any entity that gained access to the network would be trustworthy.

This traditional security model has become outdated due to the growth of cloud services, the implementation of bring-your-own-device policies, and the adoption of hybrid work environments [6]. Modern distributed IT systems pose a significant challenge for traditional security architectures, as threats are now often launched from within the system as well as from outside. Conventional security methods have been shown to be inadequate including insider threats, compromised credentials, and the ability of attackers to move laterally within networks. A change in perspective is now required for how organizations handle cybersecurity measures.

Introduction to Zero Trust Security

This modern cybersecurity framework is based on the guiding principle that trust should never be assumed, and all connections and data should be constantly verified. Traditional models, which typically assume that entities within a network are inherently trustworthy, are contradicted by the Zero Trust approach, which consistently enforces rigorous access controls, verification, and real-time surveillance for every user, device, and application, regardless of their physical location.

This approach combines multi-factor authentication (MFA), identity and access management (IAM), micro-segmentation, and least privilege principles to reduce vulnerability and prevent security breaches. Adopting Zero Trust models enables organizations to experience increased security resilience, lower risk exposure, and better adherence to regulatory requirements. As cyber threats become more sophisticated, Zero Trust Security has become a key approach to protecting digital systems in a rapidly growing threat environment.

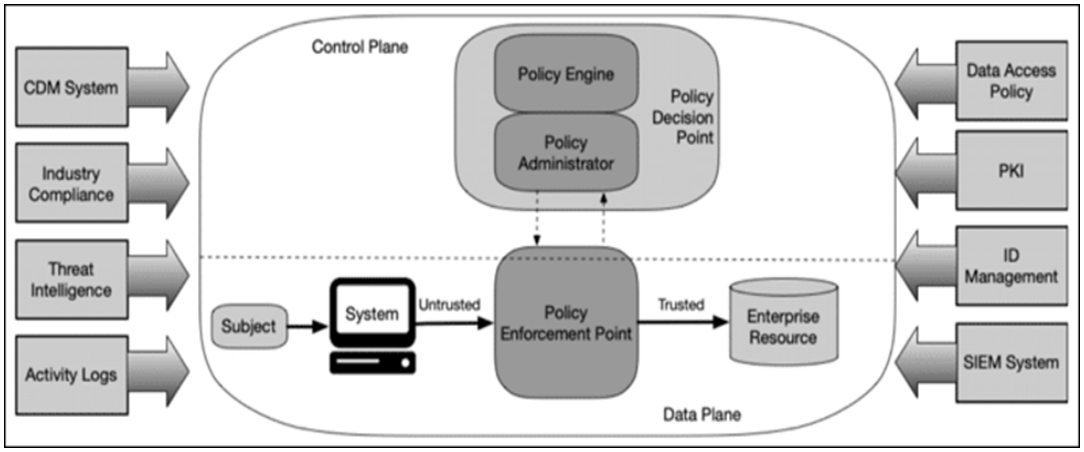

Figure 1: Zero-Trust-Architecture
(Accessed from https://www.ssl.com/blogs/zero-trust-architecture-a-brief-introduction/)

FUNDAMENTALS OF ZERO TRUST ARCHITECTURE

Core Principles of Zero Trust model

Several fundamental principles guide the Zero Trust model, setting it apart from traditional security models. The fundamental idea is to exercise caution and cross-check information. All access requests, whether coming from inside or outside the company, require thorough verification and approval procedures to be completed before granting access. The principle of least privilege restricts access is to provide the permissions and rights required by users, devices, and applications to complete their assigned tasks. This substantially decreases the likelihood of escalated privileges and unauthorized access to confidential information [9].

Key Components and Technologies

Implementing a Zero Trust model effectively demands the integration of multiple technologies, which must collaborate to enforce strict security protocols and reduce the likelihood of security vulnerabilities. Ensuring secure access to systems and data is a primary function of Identity and Access Management (IAM), with the goal of restricting access to only authenticated and authorized users. IAM solutions frequently include Multi-Factor Authentication (MFA), necessitating users to confirm their identity through several authentication methods, such as passwords, biometrics, or a one-time passcode. This substantially lessens the likelihood of attacks that exploit compromised credentials [7],[8],[9].

Traditional Virtual Private Networks (VPNs) are being replaced by Zero Trust Network Access (ZTNA) technology. Unlike virtual private networks, which offer comprehensive network access to users who have been authenticated, Zero Trust Network Access grants access solely to specific applications and resources in accordance with established security protocols [10]. This approach to network security involves isolating various sections of the infrastructure through micro-segmentation, thereby preventing potential unauthorized lateral movement in the event of a security breach.

Organizations bolster their Zero Trust posture by implementing endpoint security and device posture assessment tools that provide ongoing monitoring of devices accessing the network. Access to a device can be limited if it is discovered to be compromised or not adhering to established security protocols. Behavioral analytics and artificial intelligence-driven security systems are crucial for identifying suspicious activities and potential threats in real-time. By examining user behavior and access patterns, advanced AI-driven security systems can detect irregularities and activate preset responses to help prevent potential threats. Cloud security and Secure Access Service Edge (SASE) bring Zero Trust principles into cloud environments, thereby providing secure access to cloud-based

applications and services. These technologies collaborate to establish a robust Zero Trust environment that effectively counters cybersecurity threats.

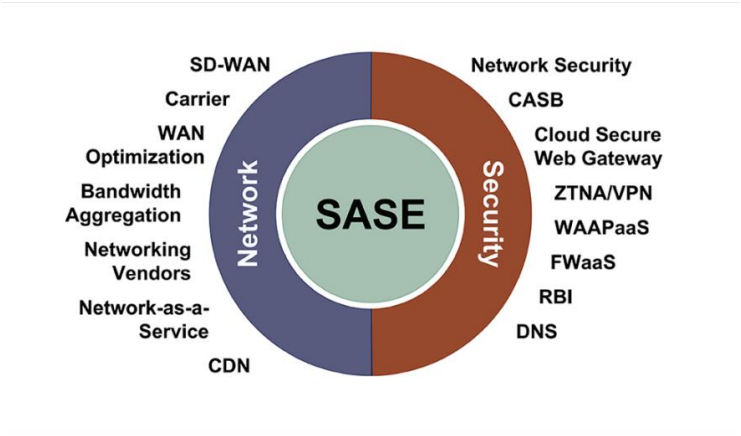

Figure 2: Secure Access Service Edge (SASE)Architecture
(Accessed from https://www.nffinc.com/webinar-essential-elements-to-achieving-secure-access-secure-edge-sase-september-30-2021/)

Zero Trust vs. Perimeter-Based Security

Conventional security frameworks based on perimeter control have traditionally formed the cornerstone of an organization's cybersecurity. These models assume that threats to the network are typically located outside it, with users and devices within the network considered inherently trustworthy. This approach heavily depends on firewalls, intrusion detection systems, and Virtual Private Networks (VPNs) to safeguard internal assets from external hazards. With the growing adoption of cloud services, remote work arrangements, and Internet of Things (IoT) devices, the definition of the traditional perimeter has become increasingly challenging, rendering perimeter-based security less capable of thwarting contemporary cyber threats [9],[11].

Contrary to traditional approaches, Zero Trust rejects the concept of automatic trust and instead imposes rigorous access restrictions based on ongoing user validation. Zero Trust architecture verifies every access request from internal users by evaluating it against various contextual factors, which include device health, user activity, and current risk levels in real-time. Traditional security models typically allow attackers to move laterally within a network after initial access, but Zero Trust counteracts this vulnerability by implementing micro-segmentation and limiting access to the minimum required resources.

A key distinction is evident in the handling of threat detection and response. Security models centered on a perimeter typically rely on fixed defenses and predetermined security protocols, which leave them susceptible to emerging cyber threats. In contrast, Zero Trust employs a dynamic and adaptive security approach, utilizing AI-driven behavioral analytics and ongoing monitoring to identify and react to potential threats as they occur. Inherently, Zero Trust architecture is tailored for cloud-based and hybrid environments, whereas conventional security frameworks face challenges in delivering consistent security measures across on-premises and cloud infrastructure.

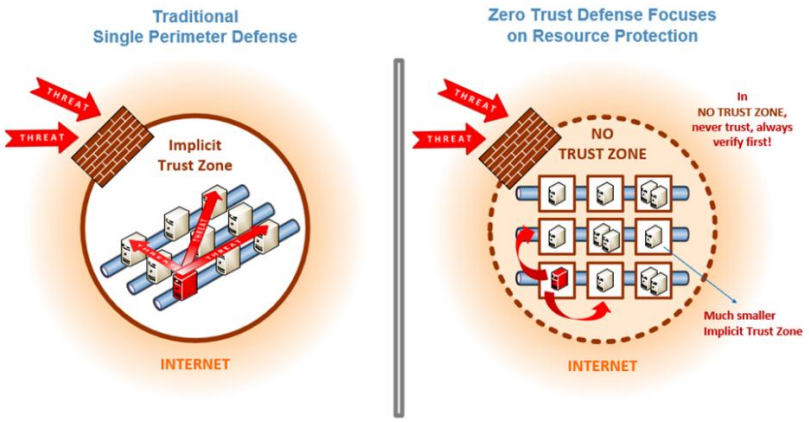

Figure 3: Traditional Vs Zero Trust Vs Defense
(Accessed from https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify)

IMPLEMENTATION STRATEGIES FOR ZERO TRUST SECURITY

Identity and Access Management (IAM)

At the heart of Zero Trust Security is Identity and Access Management (IAM), designed to guarantee that only verified and permitted users can access particular resources. IAM requires a thorough verification process, checking user identities with various methods including passwords, biometrics, and mobile apps, as well as smart cards, to ensure secure access to sensitive systems. Multi Factor Authentication (MFA) is a key part of IAM, significantly decreasing the threat of credential-based attacks by necessitating users to supply more than one form of verification before accessing protected systems [7],[8],[9].

Beyond authentication, IAM imposes Role-Based and Attribute-Based Access Control (RBAC & ABAC) requirements, guaranteeing user permissions that match only their designated roles. This safeguards against over-privileged access, thereby minimizing the potential attack surface in scenarios where credentials have been compromised [12]. Single Sign-On (SSO) solutions expand the functionality of Identity and Access Management (IAM) by enabling users to access numerous applications securely with a single set of credentials, thereby enhancing both security and user experience [13]. To effectively implement Zero Trust architecture, organizations should give priority to IAM systems that utilize real-time risk evaluation, combining the capabilities of Artificial Intelligence (AI) and Machine Learning (ML) to identify and prevent suspicious login attempts or potential malicious activity.

Micro-Segmentation and Network Security

Zero Trust Security relies on micro-segmentation as a primary approach for safeguarding critical assets against cyber threats. Traditional security frameworks for networks rely heavily on generalized trust principles, which allow users or devices to navigate a network with limited barriers once they have gained access. However, micro-segmentation mitigates the vulnerability by partitioning the network into distinct, isolated sectors, thereby preventing an attacker from accessing other parts of the network.

Data movement between segments is controlled using Software-Defined Networking (SDN) and firewall policies that implement micro-segmentation [14]. Real-time threat intelligence and user behavior inform dynamic segmentation, further bolstering security through adaptive access policy adjustments. In cloud computing, Zero Trust Network Access (ZTNA) supplants traditional Virtual Private Networks (VPNs), enabling users to solely access the particular applications they require, rather than unveiling the entire network [10].

A key component of Zero Trust Network Security is the enforcement of endpoint security measures. All devices attempting to join the network must adhere to rigorous security protocols, patching, malware safeguards, and encryption guidelines. Any device identified as being compromised is isolated right away, thereby preventing it from accessing vital systems and resources. By utilizing micro-segmentation and real-time network monitoring, companies can substantially decrease the likelihood of both internal and external cyber security threats.

Continuous Authentication and Monitoring

Continuous authentication and monitoring form the foundation of Zero Trust Security, which assumes security measures remain in effect even after users login. Unlike conventional security frameworks, which depend on a single authentication event, Zero Trust necessitates ongoing validation of user identities, device integrity, and network activity throughout the duration of a session.

Firms employ continuous authentication by utilizing behavioral analytics, machine learning, and real-time risk assessment techniques. Security systems examine various factors, including keystroke patterns, mouse movements, login patterns, and network activity, to identify anomalies in typical user behavior. Automated security protocols are activated in response to suspected malicious activity, which can include unusual login attempts from outside the country or unauthorized data access, resulting in measures such as session termination, extra verification steps, or access removal.

A vital component of ongoing monitoring is logging and auditing security events. Security teams employ Security Information and Event Management (SIEM) systems and User and Entity Behavior Analytics (UEBA) software to gather, process, and link security information continuously. These tools assist in identifying insider threats, data breaches, and potential cyberattacks before they develop into significant security incidents [15],[16].

Organizations can respond to threats more quickly with the aid of automated incident response mechanisms driven by artificial intelligence. Security Orchestration, Automation, and Response (SOAR) solutions simplify threat detection, analysis, and mitigation through automation, minimizing human involvement and enhancing response times for security incidents [17].

TECHNOLOGIES ENABLING ZERO TRUST

Role of Multi-Factor Authentication (MFA)

Within a Zero Trust framework, Multi-Factor Authentication (MFA) is crucial for enhancing identity verification processes. Authentication methods based solely on passwords are extremely susceptible to cyber threats, such as phishing, stolen login credentials, and brute-force assaults. This risk is mitigated by the MFA, which necessitates users to authenticate using various verification methods. MFA usually consist of something the user is familiar with

(such as a password), something they possess (such as an authentication token or a smartphone application), and something they are (like biometric verification through fingerprints or facial recognition) [18].

Adaptive multi-factor authentication increases security by evaluating relevant risk elements before authorizing access. In cases where a login attempt originates from an unfamiliar location, device, or IP address, the system might request further verification from the user, possibly through a one-time passcode or biometric authentication methods. This method prevents unauthorized access, even if attackers acquire valid login credentials. Organizations can substantially minimize the threat of identity-related cyber-attacks by implementing Multi-Factor Authentication and guarantee that users whose identities have been verified alone can access sensitive systems and data.

Figure 4: Multi-Factor Authentication
(Accessed from https://blog.typingdna.com/what-is-multi-factor-authentication-mfa-and-why-passwords-arent-enough/)

Zero Trust Network Access (ZTNA)

Traditional Virtual Private Networks (VPNs) are being replaced by a more secure approach, known as Zero Trust Network Access (ZTNA), which offers a more granular access control model. This new approach reduces the risk of lateral movement by attackers if credentials are compromised, as VPNs often grant users broad access to an organization's internal network following authentication. In contrast to a completely open network, ZTNA guarantees that users can only access specific applications or resources for which they have explicit permission, rather than providing unrestricted access to the network [10].

ZTNA functions on a system of continuous verification of user identities and real-time authorization checks, with every access request being assessed based on the user's identity, device condition, geographical location, and current security status. Unlike conventional network access methods, ZTNA conceals internal applications from public visibility, rendering them imperceptible to attackers who identify potential entry points. This substantially decreases the attack surface and stops unauthorized users from accessing vital resources. For organizations with remote staff, flexible work arrangements, and cloud-based systems, ZTNA offers a secure, expandable, and streamlined approach to managing network security.

Cloud and Endpoint Security

As more organizations move their operations to cloud environments, securing cloud-based resources and endpoints has become a critical component of a Zero Trust security strategy. Conventional security models that rely on perimeter-based approaches often find it challenging to offer uniform protection in complex multi-cloud and hybrid infrastructure settings. In contrast, Zero Trust Cloud Security implements rigorous access restrictions, requiring continuous authentication of users and devices prior to their interaction with cloud assets.

Organizations secure their cloud applications by using Cloud Access Security Brokers (CASBs), which monitor and enforce security policies in cloud environments. These solutions aid in preventing data leakage, unauthorized access, and cloud misconfigurations which may lead to sensitive information being exposed. Even if cloud data is intercepted, it is encrypted, tokenized, and continuously monitored to prevent unauthorized access, thus keeping it inaccessible to those who do not have permission [18].

Zero Trust incorporates endpoint security as a vital element, with endpoints like laptops, smartphones, and IoT devices frequently being the focus of cybercriminal attacks. Companies implement Endpoint Detection and Response (EDR) systems to track device activity, identify malware infections, and block unauthorized access [19]. Conducting device authentication and security posture evaluations is also crucial, guaranteeing that only compliant and secure devices can access corporate networks. When an endpoint is determined to be compromised, Zero Trust protocols immediately limit its access in order to prevent further disruption.

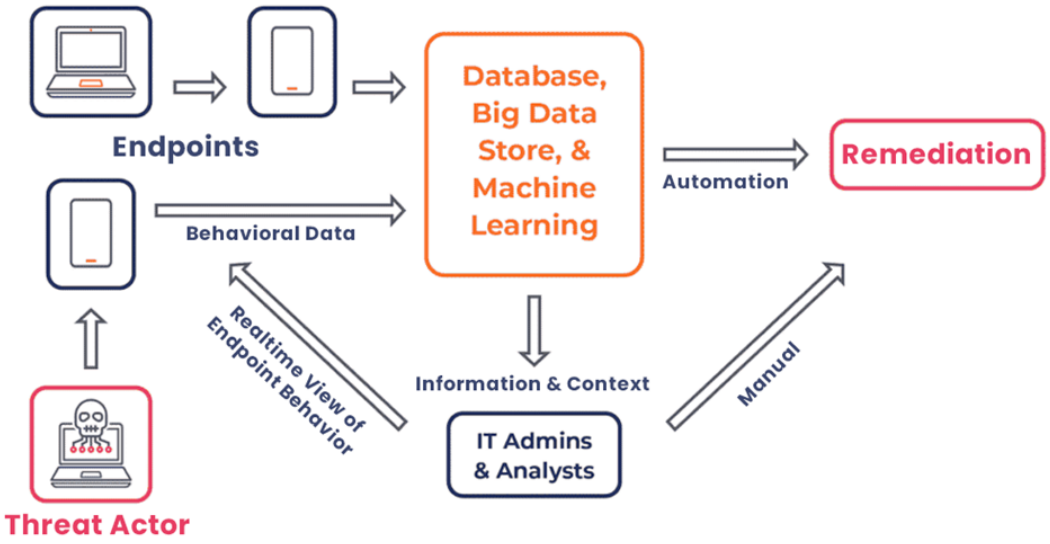

Figure 5: Endpoint Detection and Response
(Accessed from https://www.safeaeon.com/security-blog/endpoint-detection-and-response-edr/)

CHALLENGES AND LIMITATIONS OF ZERO TRUST

Implementation Complexity and Cost

Adopting Zero Trust is hindered by the intricacies involved in its implementation. In contrast to conventional security frameworks that frequently rely on perimeter-based security measures, Zero Trust demands a comprehensive re-evaluation and replacement of existing access control systems, identity authentication processes, and network partitioning tactics. Prior to implementing Zero Trust policies, organizations must initially create a comprehensive map of all users, devices, applications, and data flows, a process that can be both labour-intensive and time-consuming.

Zero Trust security relies on various integrated security technologies, such as Identity and Access Management (IAM), Multi-Factor Authentication (MFA), Zero Trust Network Access (ZTNA), endpoint security solutions, micro-segmentation, and continuous monitoring systems. Implementing and linking these tools necessitates specialized technical knowledge, committed IT personnel, and thorough testing, thereby posing difficulties for organizations with limited cybersecurity capabilities.

In addition to complexity, the financial investment required for Zero Trust deployment can be significant. Companies may have to update their current security systems, invest in modern security tools, educate staff members, and assign funds for continuous supervision and administration. Small and medium-sized enterprises (SMEs) may experience additional financial strain from these costs, making it difficult for them to completely adopt a Zero Trust model. Despite the high upfront costs, the long-term advantages of reduced data breaches, enhanced security resilience, and adherence to compliance standards can potentially outweigh these initial hurdles.

User Experience and Productivity Trade-offs

Prioritizing security above convenience in Zero Trust environments often results in user experience difficulties and productivity compromises. In contrast to conventional security models, which provide users with extensive access permissions once they are within the network, Zero Trust policies mandate ongoing verification, rigorous access restrictions, and instantaneous security evaluations. This may necessitate employees to repeatedly authenticate themselves throughout their work tasks, ultimately resulting in decreased productivity and hindered operational efficiency.

Staff members who had previously been granted unrestricted access to specific software may now encounter extra login requirements, blocked access, or complex verification procedures. These measures can strengthen security, but they may also decrease productivity, cause organizational disruption, and heighten employee dissatisfaction, particularly those who regard them as excessive hurdles.

To minimize productivity losses, businesses need to implement intelligent verification systems, including risk-adjusted adaptive verification, Single Sign-On (SSO), and behavior-based access controls. Implementing these solutions enables a balance between security and user experience, providing unobstructed authentication in low-risk scenarios and heightened security protocols in response to identified anomalies. Providing clear communication and training employees on the significance of Zero Trust security can also help alleviate resistance and enhance user acceptance.

Overcoming Resistance to Change

Implementing Zero Trust Security necessitates a significant change from conventional security frameworks, potentially resulting in opposition from staff, IT personnel, and executives. Employees who work with technology systems are accustomed to having easy access and may experience frustration when more authentication steps are required. IT departments are concerned about the complexity and resources needed for implementation, whereas senior management might be hesitant due to concerns about expenses and potential decreases in productivity. It is essential for businesses to implement Zero Trust in a seamless and transparent manner.

A frequent misinterpretation is that Zero Trust implies the organization has no faith in its workforce. The objective is to safeguard sensitive data and systems rather than to instill distrust in users, especially in the face of potential security threats. Organizations should make clear the advantages of Zero Trust, such as stopping cyberattacks, mitigating insider threats, and preventing data breaches, in order to decrease resistance. Offering training sessions and awareness programs can educate employees on the importance of these security measures and instruct them on how to work securely with minimal disruption.

Implementing Zero Trust architecture is typically more effective when done gradually to prevent burdening the workforce. Companies can begin by implementing small-scale pilot projects within specific teams, collecting feedback, and revising their policies accordingly, rather than introducing abrupt, enterprise-wide changes. A phased implementation allows employees to adapt to updated security protocols while also enabling IT departments to fine-tune and perfect their rollout process.

Organizations should utilize user-friendly security solutions such as Single Sign-On (SSO), adaptive authentication, and automated security tools to facilitate a smoother transition. These solutions minimize disruptions to employees' workflow by only requiring extra authentication steps when they are truly necessary. By streamlining security procedures, organizations can achieve a harmonious balance between robust security measures and a user-friendly experience.

Establishing a culture prioritizing security is equally crucial. Cybersecurity should be viewed as a collective obligation, rather than simply a duty confined to the IT department. Senior management should foster an environment of security awareness, facilitate the reporting of security-related issues, and engage various departments in security-related conversations. Departments can also have security advocates appointed to them in order to strengthen Zero Trust policies.

CONCLUSION

The Zero Trust Security Model is a contemporary approach to cybersecurity that eliminates the assumption of implicit trust and insists on rigorous verification for every user, device, and access request. In contrast to the conventional approach to network security, which presumes all activity within the network is trustworthy, Zero Trust necessitates ongoing verification and surveillance to deter unauthorized access. Organizations can reduce security risks and safeguard sensitive information from cyber attacks by putting in place essential security measures like Multi-Factor Authentication (MFA), Zero Trust Network Access (ZTNA), micro-segmentation, and least privilege access control. The combination of Artificial Intelligence (AI) and Machine Learning (ML) also boosts real-time threat detection, allowing organizations to take action against security threats ahead of time.

Although Zero Trust offers several benefits, its implementation is complicated by several factors, such as the need to integrate it with current systems and the potential for it to affect user experience. As cyber threats become increasingly sophisticated, organizations must place a high priority on Zero Trust to enhance their overall security stance. Investing in appropriate technologies and business strategies can increase a company's ability to withstand cyberattacks, improve its adherence to regulatory requirements, and establish a safer digital infrastructure. In the future, Zero Trust is set to become a vital component of contemporary cybersecurity, enabling companies to adjust to changing threats and safeguard their networks within a more digital environment.

REFERENCES

[1]. P. Chen, L. Desmet, and C. Huygens, "A study on advanced persistent threats," in Communications and Multimedia Security. CMS 2014, B. De Decker and A. Zúquete, Eds. Berlin, Heidelberg: Springer, 2014, vol. 8735, pp. 63–72. doi: 10.1007/978-3-662-44885-4_5.

[2]. C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, "Ransomware: Recent advances, analysis, challenges and future research directions," Computers & Security, vol. 111, p. 102490, 2021. doi: 10.1016/j.cose.2021.102490.

[3]. Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments," Energy Reports, vol. 7, pp. 8176-8186, 2021. doi: 10.1016/j.egyr.2021.08.126.

[4]. A. Khraisat, I. Gondal, P. Vamplew, and others, "Survey of intrusion detection systems: techniques, datasets and challenges," Cybersecurity, vol. 2, no. 20, 2019. [Online]. Available: https://doi.org/10.1186/s42400-019-0038-7.

[5]. Y. K. Sharma and C. Kaur, "The Vital Role of Virtual Private Network (VPN) in Making Secure Connection Over Internet World," International Journal of Recent Technology and Engineering (IJRTE), vol. 8, no. 6, pp. 1234-1240, Mar. 2020.
[6]. Y. Barlette, A. Jaouen, and P. Baillette, "Bring Your Own Device (BYOD) as reversed IT adoption: Insights into managers' coping strategies," Int. J. Inf. Manag., vol. 56, p. 102212, 2021, doi: 10.1016/j.ijinfomgt.2020.102212.
[7]. J. Williamson and K. Curran, "The role of multi-factor authentication for modern-day security," Semiconductor Science and Information Devices, vol. 3, no. 1, pp. 16–23, 2021. doi: 10.30564/ssid.v3i1.3152.
[8]. I. Indu, P. M. R. Anand, and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," Eng. Sci. Technol., Int. J., vol. 21, no. 4, pp. 574–588, 2018, doi: 10.1016/j.jestch.2018.05.010.
[9]. N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," IEEE Access, vol. 10, pp. 57143-57179, 2022, doi: 10.1109/ACCESS.2022.3174679.
[10]. M. Campbell, "Beyond Zero Trust: Trust Is a Vulnerability," Computer, vol. 53, no. 10, pp. 110-113, Oct. 2020, doi: 10.1109/MC.2020.3011081.
[11]. B. Sengupta and A. Lakshminarayanan, "DistriTrust: Distributed and low-latency access validation in zero-trust architecture," Journal of Information Security and Applications, vol. 63, p. 103023, 2021. doi: 10.1016/j.jisa.2021.103023.
[12]. M. P. Singh, S. Sudharsan, and M. Vani, "ARBAC: Attribute-Enabled Role Based Access Control Model," in ISEA Asia Security and Privacy Conference, 2019.
[13]. M. Kihara and S. Iriyama, "Security and performance of single sign-on based on one-time pad algorithm," Cryptography, vol. 4, no. 2, p. 16, 2020. doi: 10.3390/cryptography4020016.
[14]. K. Nisar, E. R. Jimson, M. H. A. Hijazi, I. Welch, R. Hassan, A. H. M. Aman, A. H. Sodhro, S. Pirbhulal, and S. Khan, "A survey on the architecture, application, and security of software defined networking: Challenges and open issues," Internet of Things, vol. 12, p. 100289, 2020. doi: 10.1016/j.iot.2020.100289.
[15]. G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures," Sensors, vol. 21, no. 14, p. 4759, 2021. doi: 10.3390/s21144759.
[16]. M. A. Salitin and A. H. Zolait, "The role of User Entity Behavior Analytics to detect network attacks in real time," 2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakhier, Bahrain, 2018, pp. 1-5, doi: 10.1109/3ICT.2018.8855782.
[17]. R. Vast, S. Sawant, A. Thorbole, and V. Badgujar, "Artificial Intelligence based Security Orchestration, Automation and Response System," 2021 6th International Conference for Convergence in Technology (I2CT), Maharashtra, India, 2021, pp. 1-5, doi: 10.1109/I2CT51068.2021.9418109.
[18]. E. B. Fernández, N. Yoshioka, and H. Washizaki, "Cloud Access Security Broker (CASB): A pattern for secure access to cloud services," 2015.
[19]. H. Kaur and R. Tiwari, "Endpoint detection and response using machine learning," J. Phys.: Conf. Ser., vol. 2062, no. 1, p. 012013, 2021. doi: 10.1088/1742-6596/2062/1/012013.