Enterprise Network Zero Trust Security Model

A.O. Oronti, B.K. Alese, O. Olabode, O.A. Akinsowon
Cyber Security Department, School of Computing
Federal University of Technology, Akure
Nigeria

Abstract

In recent times the complexity that comes with enterprise data and resources protection has become overwhelming with users requiring access from anywhere, at any time, and from any device, while data is created, stored, transmitted, and processed across diverse environments, spanning on-premises and multiple cloud platforms. Setting the record straight traditional perimeter-based security approaches are no longer effective, as they assume all users and devices within the enterprise environment can be trusted. To mitigate against these, Zero-Trust Architecture (ZTA) has emerged as a robust security framework, enabling secure, authorized access to assets, including machines, applications, services, and associated data and resources, regardless of location. ZTA verifies the context of each access request, including static user profile information and non-person entity information, as well as dynamic information such as geolocation, device health, credentials, resource sensitivity, and access pattern anomalies. If the defined policy is met, a secure session is established to protect all information transferred, with real-time, risk-based assessments and continuous policy evaluations ensuring access remains authorized and secure. Moreover, ZTA protects enterprise from external threats originating from non-organizational resources, providing an additional layer of security. By adopting ZTA, organizations can effectively address the complexities of modern day security threats and ensure the protection of their sensitive assets.

1. Introduction

In the realm of enterprise security, traditional perimeter models have long dominated. These models grant devices access to services and resources by connecting to a privileged network. When employees work within the corporate office, on an appropriate network, services become directly accessible. However, remote work or branch offices —often necessitate the use of a VPN to penetrate the enterprise firewall. This method has served as the cornerstone of organizational protection. However, by 2011, Google recognized that this approach was inherently flawed. The time had come to reevaluate how enterprise services are accessed and safeguarded. The realization marked a pivotal moment in the evolution of enterprise security strategies, also in the contemporary landscape, the traditional perimeter-based security model has proving inadequate. With the upsurge of sophisticated cyber threats, combined with the proliferation of remote work and cloud services has brought about a paradigm shift in cybersecurity strategies. The Zero Trust Framework fundamentally redefines the concept of trust within an Enterprise Network, unlike conventional security models that assume trustworthiness for all users and devices within the network perimeter, Zero Trust operates on the principle that no entity, whether inside or outside the network, should be trusted by default. This model mandates continuous verification of every access request, regardless of its origin, thereby minimizing the risk of unauthorized access and data breaches[1]. Remote locations connect to the headquarters which generate fresh data whose repository is either stored in the cloud or on-premise.

The data collection process involves multiple networks, systems, and applications, each playing a crucial role in managing and storing information. However, these interconnected systems can sometimes harbor vulnerabilities. When cyber attackers identify and exploit known weaknesses, they infiltrate the system, leading to unauthorized access and data breaches. Also, the frequent turnover of individuals within the organisation—due to quest to know more, new enrollments, and staff changes—creates a continuous influx of new data and this constant cycle not only amplifies the volume of sensitive information but also broadens the potential points of entry for cyber threats. Consequently, the dynamic nature of these environments significantly heightens data risk and expands the overall attack surface, making it more challenging to safeguard against breaches. [21] Zero trust provides stronger protection by focusing security directly around data, workloads, and user access patterns rather than physical infrastructure. It limits lateral movement, reduces the attack surface, and contains breaches before they escalate. Continuous traffic inspection and analytics offer deep visibility, enabling organizations to detect anomalies, uncover inefficiencies, and respond faster to threats. Beyond technology, zero trust also addresses human and

 | DOI: 10.20533/ijds.2040.2570.2025.0250

organizational challenges. It reduces reliance on specialized cybersecurity expertise by enforcing automatic least-privilege access and deny-by-default policies, ensuring that employees, contractors, and third parties only have access to what they need. This minimizes accidental exposure and malicious exploitation while providing opportunities for better security awareness. With adaptive authentication, strong identity management, micro-segmentation, and encrypted communication, zero trust strengthens compliance and privacy outcomes while supporting operational flexibility. Ultimately, zero trust represents a shift from reactive security to proactive resilience. By assuming compromise, continuously verifying trust, and safeguarding data wherever it resides, organizations gain a more robust defense model suited for modern digital infrastructures.

2. Literature Review

Comparitech [7] reports that the year 2023 witnessed a significant increase in security breaches, having a record 954 incidents reported. A substantial escalation from the 139 breaches documented in 2022 and 783 breaches in 2021. The primary driver of this surge was identified as vulnerabilities associated with the a file transfer software, which impacted over 800 organisations. In terms of compromised records, year 2023 saw a dramatic rise to nearly 4.3 million records, in contrast to the approximately 2.6 million records compromised in both 2021 and 2022. Specifically, 1.7 million records were compromised in incidents involving third-party breaches, while 1.9 million records were affected by 65 ransomware attacks. The research conducted by Comparitech, analyzed data spanning the past 19 years, highlighted significant trends and hotspots for breaches within the education sector. Organizations were disproportionately affected, accounting for 60% of the total breaches, largely due to incident. Furthermore, 83% of the compromised records originated from institutions, underscoring the heightened vulnerability of this sector to cyber threats. The evolving landscape of cybersecurity necessitates a re-evaluation of traditional security measures. Traditional perimeter security measures, including Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), firewalls, and web gateways, are becoming increasingly impractical due to the sophistication and pervasiveness of cyber-attacks and breaches of computer network perimeters. This shift underscores the need for more robust and adaptive security frameworks capable of addressing contemporary threats [2].

The "never trust" mindset, is a concept that harmonies nodes in and out of a domain i.e. looking beyond the perimeter; is the major backbone of zero-trust framework, which outrightly resolve trust-based vulnerabilities. This concept was conceived by Stephen Paul Marsh in his research work on computer security, and years down the line in 2010 a researcher at the Forrester Research Institute named John Kindervag adopted it as a security tool [3].

A related study at Stafford examined the application of Zero Trust Architecture (ZTA) principles in the planning of enterprise and industrial workflows and infrastructure. The report states that ZTA operates on the premise that no implicit trust is granted to user accounts or assets based solely on their network or physical location. Instead, authorization and authentication—both for devices and subjects—are distinct processes conducted prior to any session involving the development of enterprise resources. Zero trust primarily addresses various contemporary enterprise network trends, such as cloud-based assets, bring-your-own-device (BYOD) policies, and remote users, which exist outside the traditional enterprise-owned network boundaries.

Furthermore, zero trust prioritizes the protection of resources, including network accounts, services, workflows, and assets, rather than focusing on network segments. This shift in focus arises from the recognition that network location is no longer the central element of a security posture [4]. Hackers often target the weakest link in a domain to gain unauthorized access and exploit vulnerabilities to their advantage. The vulnerabilities can manifest as insiders within the organization or as porous network surfaces. Numerous studies [5], [6] have identified insiders as the most significant attack surface in information security, highlighting the critical need for robust internal security measures. Insiders, defined as individuals with authorized access to an organization’s systems and data, pose a unique threat due to their legitimate access rights. This group includes current and former employees, contractors, and business partners.

The National Institute of Standards and Technology (NIST) describes insiders as entities capable of causing harm through the destruction, disclosure, modification of data, or denial of service [7]. Research indicates that insider threats have increased significantly in recent years. For instance, it is reported that Ponemon Institute records a 47% rise in insider threat incidents between 2018 and 2020, with the average cost of such attacks estimated at $11.45 million [7]. These threats are often challenging to detect and mitigate, requiring sophisticated security measures and continuous monitoring. Moreover, the shift towards remote work and the adoption of cloud-based technologies have exacerbated these vulnerabilities.

The increased reliance on remote access and personal devices has expanded the attack surface, making it more difficult to secure organizational networks[8]. Consequently, institutions must prioritize the protection of internal resources and

 | DOI: 10.20533/ijds.2040.2570.2025.0250

implement comprehensive security strategies to address these evolving threats.

3. Enterprise Network Zero Trust Security Model

Infrastructures in the Enterprise domain present specific Zero Trust Architecture (ZTA) for example, networking equipment, printers, and others offer limited options for authentication, visibility, and security[9].

The technological landscape for devices continues to change, and as enterprises incorporate additional devices into their terrain, administrators will continue to manage the evolving risks associated with these devices [10]. However, despite these evolving risks enterprise continue moving to cloud an environment that creates new considerations and opportunities for managing and tracking most cloud assets and virtual assets [4]. Cloud assets include computing resources (e.g., virtual machines, servers, or containers), storage resources (e.g., block storage or file storage), platform assets (e.g., databases, web servers, message buses/queues), and network resources (e.g., virtual networks, VPNs, gateways, DNS services, etc.) and virtual resources associated with other managed cloud services (e.g., artificial intelligence models) [17].

5. System Design Model and Architecture

Based on NIST SP 800-207 Figure 1 is based on the ZTA reference architecture [20] which describes it’s components and major operations. The components in the general ZTA may be operated as either on-premises or cloud-based services. The core components of Zero Trust Architecture (ZTA) include:

Policy Engine (PE): The PE is responsible for making the final decision to grant, deny, or revoke access to a resource for a specific subject. It calculates [18] trust scores and confidence levels, and makes access decisions based on enterprise policies and information from supporting components. The PE executes a trust algorithm to evaluate each resource request it receives. It can function as a single system or a federation of systems (a "system of systems") that manage different sectors of the ZTA. Each PE within the federation is accountable for its sector, guided by the overall enterprise policies.

Policy Administrator (PA): The PA implements the decisions made by the PE by sending commands to the Policy Enforcement Point (PEP) [18] to establish or terminate the communication path between the subject and the resource. It also generates session-specific authentication and authorization tokens or credentials that the subject uses to access enterprise resources.

Policy Enforcement Point (PEP): The PEP secures the trust zone hosting one or more [18] enterprise resources. It is responsible for enabling, monitoring, and eventually terminating connections between subjects and enterprise resources. The PEP operates based on commands received from the PA.

As delineated by Figure 1 the high-level logical architecture of the general Zero Trust Architecture (ZTA) reference model, which remains agnostic to specific deployment scenarios. This model is constituted by three principal components: Policy Engines, Policy Administrators, and Policy Enforcement Points. Additionally, it encompasses several ancillary components that facilitate the policy engine's decision-making processes by supplying data and policy rules pertinent to Identity, Credential, and Access Management (ICAM), endpoint security, security analytics, data security, and resource protection. The detailed functionalities of these ancillary components are expounded upon in subsequent sections. The diverse sets of information, either generated through policy or amassed by these ancillary components and utilized as inputs for ZTA policy decisions, are designated as Policy Information Points (PIPs).

Imperatively, the logical components within the reference architecture [19] do not necessarily correspond directly to physical (hardware or software) entities. Although the architecture's apparent simplicity might suggest that the ancillary components function as straightforward plug-ins responding in real-time to the Policy Decision Point (PDP), in practice, the ICAM, Endpoint Detection and Response (EDR)/Endpoint Protection Platform (EPP), security analytics, and data security PIPs often embody complex infrastructures. Certain ZTA logical component functions may be executed by multiple hardware or software entities, or conversely, a single software entity may perform multiple logical functions. Subjects, [19] encompassing human users, devices, applications, servers, and other non-human entities that request access to resources, engage with the ZTA to obtain access to enterprise resources. Both human and non-human subjects undergo authentication and are safeguarded by endpoint security measures. Enterprise resources may reside on-premises or within cloud environments. While existing enterprise subjects and resources are not inherently part of the reference architecture, any requisite modifications to existing endpoints, such as the deployment of ZTA agents, should be considered integral to the reference architecture.

6. Case Study: Palo Alto Networks

Palo Alto Networks [20] is at the forefront of shaping a cloud-centric future, leveraging cutting-edge advancements in AI, analytics, automation, and

 | DOI: 10.20533/ijds.2040.2570.2025.0250

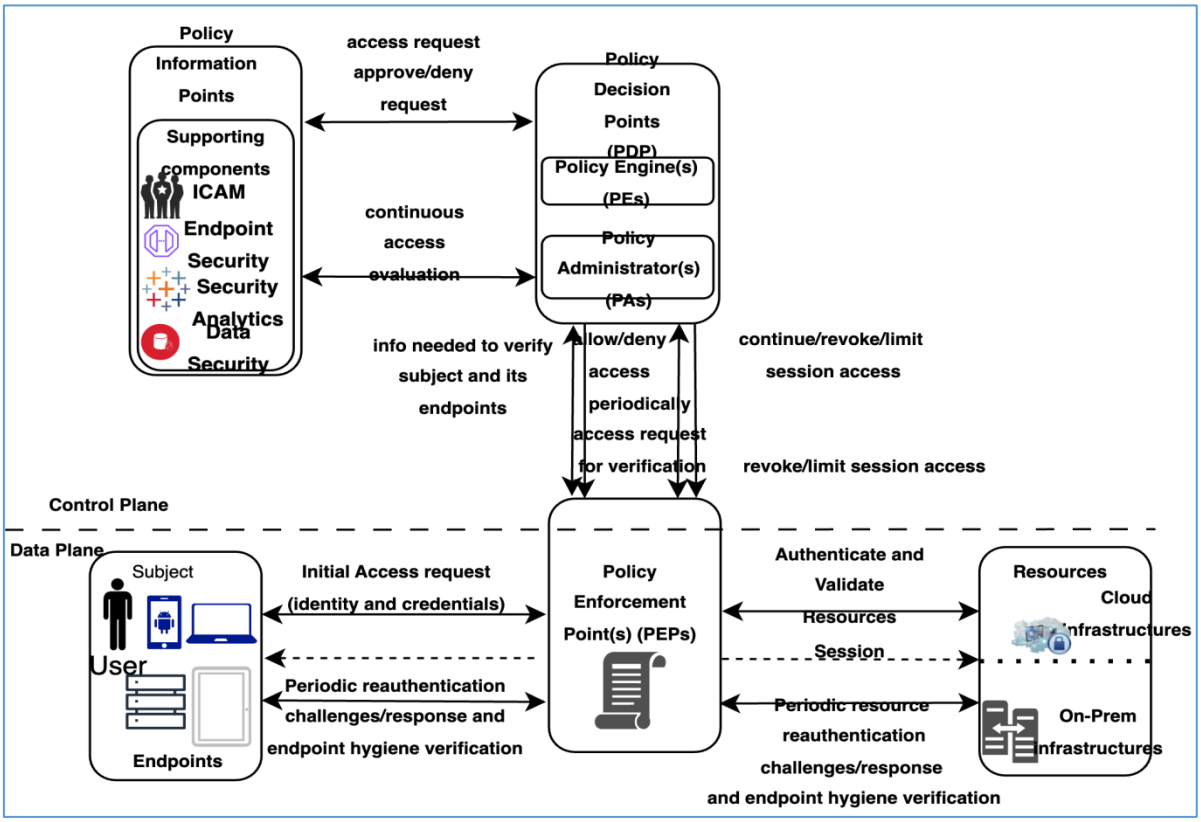

Figure 1. Reference Architecture Zero Trust

orchestration to revolutionize the way individuals and organizations function. By offering an integrated platform and fostering a robust ecosystem of partners, Palo Alto Networks' security technologies empower organizations to implement consistent security controls across various environments, including clouds, networks, endpoints, and mobile devices. Their core capabilities [20] encompass comprehensive traffic inspection, covering all applications, threats, and content, and associating this traffic with the user, irrespective of their location or device type. This integration ensures that users, applications, and content—the critical elements driving your business—are seamlessly incorporated into your enterprise's zero trust security policy.

To achieve this, Palo Alto Networks' Next Generation Firewall (available in hardware-based, VM, and containerized formats) and Prisma Access offer consistent core capabilities essential for enforcing zero trust policies, including User-ID, App-ID, and Device-ID.

- User-ID technology is a powerful tool for organizations, allowing them to identify users across various locations and devices. By focusing on users and groups instead of IP addresses, it provides detailed visibility into application activity. This approach helps ensure that applications are used safely and in line with business needs.
- App-ID technology enables organizations to precisely identify applications within all network traffic, even those that are disguised, use dynamic ports, or are encrypted. This technology helps organizations understand and manage applications by distinguishing between their specific functions, such as video streaming versus chat, upload versus download, and screen-sharing versus remote device control.
- Device-ID technology enables organizations to enforce policy rules based on the device itself, irrespective of changes to its IP address or location. By offering traceability for devices and associating network events with specific devices, Device-ID provides context for how events relate to devices, allowing organizations to create policies tied to devices rather than users, locations, or IP addresses, which can change over time.

7. Conclusion

Our study explored the efficacy of Zero Trust Architecture (ZTA) in an Enterprise architecture and illustrates how a manufacturer implements for an

 | DOI: 10.20533/ijds.2040.2570.2025.0250

enterprise. Findings indicate that ZTA provides a framework for enhancing network security by moving the security paradigm from default perimeter-based approach to one that assumes no implicit trust within an enterprise. This approach is important for all enterprise, which are characterized by a diverse user base and a high degree of resource sharing. The deployment of ZTA on networks addresses several critical security challenges, including unauthorized access, data breaches, and insider threats. By continuously verifying the identity and integrity of devices and users, ZTA ensures that only authenticated and authorized entities can access network resources. Future work should focus on making comparative analysis of how various manufacturers implement ZTA.

8. References

[1] Microsoft Learn. (n.d.). Securing identity with Zero Trust. https://www.microsoft.com/en-us/security/business/zero-trust (Access Date: 5 May 2025).

[2] Assunção, P. (2019). A zero-trust approach to network security. In Proceedings of the Digital Privacy and Security Conference (Vol. 2019). Porto Portugal.

[3] Edo, O.C., Tenebe, T., Etu, E., Ayuwu, A., Emakhu, J., and Adebiyi, S. (2022). Zero Trust Architecture: Trend and Impact on Information Security. International Journal of Emerging Technology and Advanced Engineering, 140-147. DOI: 10.46338/ijetae0722_15.

[4] Stafford V. A. (2020). Zero trust architecture. NIST special publication. 207.

[5] Sasse, M. A., Brostoff, S., and Weirich, D. (2021). 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] GSA. (2021). Zero Trust Architecture (ZTA): Buyer guide. Zero Trust Architecture. Buyers Guide v11 20210810 (4).

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

[8] Cyberecurity Insiders. (2019). Zero Trust Adoption Rate. https://www.cybersecurity-insiders.com/portfolio/2019-zero-trust-adoption-report/#:~:text=KeyTakeaways%3A (Access Date: 12 October 2024).

[9] Edlyn, L., and Algirde, P. (2019). Hardware is a cybersecurity risk. Here's what we need to know. World Economic Forus. https://www.weforum.org/agenda/2019/12/our-hardware-is-under-cyberattack-heres-how-to-make-it-safe/ (Access Date: 20 October 2024).

[10] InfoSecurity Magazine. (2024). Data Breaches in US Schools Exposed 37.6M Records. https://www.infosecurity-magazine.com/news/data-breaches-us-sch ools-37m/ (Access Date: 12 October 2024).

[11] Bollmann, S., and Kleinebudde, P. (2021). Evaluation of different segmentation methods of X-ray micro computed tomography images. International Journal of Pharmaceutics, 120880.

[12] IT Security Wire. (n.d.). Risks and challenges of migrating to zero trust architecture. https://itsecuritywire.com/featuredrisks-and-challenges-of-migrating-to-zero-trust-architecture-zta/ (Access Date: 2 June 2024).

[13] NIST Project Overview. (n.d.). Zero Trust Architecture. https://pages.nist.gov/zero-trust-architecture/VolumeA/ProjectOverview.html (Access Date: 14 September 2024).

[14] F5 Networks. (n.d.). What is zero trust architecture zta. https://www.f5.com/labs/learning-center/what-is-zero-trust-architecture-zta (Access Date: 15 August 2024).

[15] Shevchenko, N., Chick, T. A., O'Riordan, P., Scanlon, T. P., and Woody, C. (2018). Threat Modeling: A Summary of Available Methods. Software Engineering Institute, Carnegie Mellon University.

[16] Dildy, T. J. (2016). Network Access Control: Has It Evolved Enough for Enterprises? ISACA Journal.

[17] Haber, M. J. (2022). Applying Access Control Lists in the Cloud. Beyond Trust.

[18] National Institute of Standards and Technology. (2024). Implementing a Zero Trust Architecture: Full Document. NIST Special Publication 1800-35.

[19] Implementing a Zero Trust Architecture Project documentation NIST SP 1800-35 Publication. https://pages.nist.gov/zero-trust-architecture/VolumeB/architecture.html#general-zta-reference-architecture (Access Date: 25 August 2024).

[20] Implementing a Zero Trust Architecture: High-Level Document (2024). Paper Title. https://www.nccoe.nist.gov/sites/default/files/2024-11/zta-nist-sp-1800-35-ipd.pdf (Access Date: 28 November 2024).

[21] Zero Trust Explained: Benefits, Principles, and Technologies https://www.cynet.com/zero-trust/zero-trust-explained-benefits-principles-and-technologies/ (Access Date: 26 November 2025).

 | DOI: 10.20533/ijds.2040.2570.2025.0250