© APR 2025 | IRE Journals | Volume 8 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV8I10-1718630

Zero Trust Architecture in Corporate Networks: Reduced VPN Dependence, Threat Containment, and Access Governance in Hybrid Environments

VALDIR DE ESPÍNDULA

Abstract- ***Zero Trust Architecture has been proposed as a structural response to the erosion of perimeter-based security in corporate networks characterized by remote work, cloud migration, heterogeneous endpoints, and the rising frequency of ransomware and lateral-movement attacks. Unlike the traditional perimeter-centric model, Zero Trust assumes that no user, device, or session should be trusted by default, even when the connection originates from an apparently internal environment. This article discusses, based on scientific literature and a major technical reference document, the conceptual foundations of Zero Trust, its relationship with Zero Trust Network Access (ZTNA), its differences from legacy VPN models, and its implications for access control, operational performance, and regulatory alignment. The analysis indicates that contextual policies, strict enforcement of least privilege, logical segmentation, and continuous verification can reduce unnecessary exposure to corporate resources while improving threat containment without necessarily increasing operational friction. The paper concludes that Zero Trust should not be understood merely as a tightening of controls, but as an architectural reorganization of security around identity, context, and continuous resource protection.***

Keywords: Zero Trust, ZTNA, VPN, Network Security, Access Control.

I. INTRODUCTION

Corporate network security has shifted away from the traditional perimeter-based model, in which the main protection strategy relied on separating a trusted internal network from an untrusted external environment. This design was reasonably effective while users, applications, and data were concentrated in on-premises datacenters and connected through predictable topologies. However, the expansion of remote work, cloud computing, distributed applications, and personal-device usage has weakened the assumption that network location alone can serve as a reliable proxy for trust. (see the generated image above)

In this context, Zero Trust Architecture has gained prominence by proposing a different logic of access control. Instead of assuming that an authenticated user or a connected device may move broadly across the corporate environment, Zero Trust requires explicit authentication, contextual authorization, and continuous evaluation before and during access to specific resources. (see the generated image above) Trust is no longer derived from the user's position within the network, but from verifiable attributes such as identity, device integrity, resource sensitivity, observed behavior, and policy consistency throughout the session. [2–5]

The most robust literature on the subject emphasizes that Zero Trust is not a standalone product, but an architectural model composed of interdependent mechanisms such as identity and access management, multifactor authentication, context-based policy enforcement, microsegmentation, telemetry, encryption, and continuous monitoring. [1–6] This is important because it counters the oversimplified view that implementation merely involves replacing a legacy tool with a more modern one. In practice, Zero Trust adoption requires reassessment of access flows, asset classification, attack-surface visibility, and integration between policy-decision and policy-enforcement points.

This article critically examines the role of Zero Trust in corporate networks, with emphasis on three dimensions: the transition from traditional VPN models to Zero Trust Network Access (ZTNA), the architecture's capacity to contain threats in hybrid environments, and its relevance for governance and compliance. The purpose is not to support absolute

© APR 2025 | IRE Journals | Volume 8 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV8I10-1718630

claims about risk elimination, but to discuss, based on bibliographic evidence, the extent to which Zero Trust offers architecturally consistent advantages over implicit-trust models. [1–8]

II. METHODOLOGY

This paper was developed as a narrative literature review focusing on review studies, academic surveys, a key normative reference document, and recent works on Zero Trust, ZTNA, cloud security, and remote-service protection. Sources with stronger technical recognition and clearer bibliographic traceability were prioritized, especially NIST SP 800-207, surveys published in IEEE Access, systematic literature reviews, and studies addressing Zero Trust in corporate and distributed settings. [1–8] Excessively promotional claims and weakly supported evidence were excluded from the core argument. As a result, the article was rewritten to strengthen conceptual coherence, terminological precision, and academic credibility while preserving the thematic emphasis on corporate networks, remote access, reduced VPN dependence, and threat containment.

III. RESULTS AND DISCUSSION

A recurring finding in the literature is that Zero Trust changes the object of defense itself. In traditional models, protective effort is concentrated on maintaining a boundary between internal and external space. Under Zero Trust, the priority becomes the continuous protection of resources, data, applications, and services regardless of where they are hosted or where the request originates. (see the generated image above) This shift is especially relevant in hybrid environments, where corporate applications may coexist across public cloud, private infrastructure, third-party platforms, and remotely accessed endpoints. Conceptually, this shift from perimeter-bound to resource-centric protection can be illustrated by the transition from VPN-centric access to Zero Trust Network Access (ZTNA) in hybrid environments, as depicted in Figure 1.

Figure 1. Conceptual transition from VPN-centric access to Zero Trust Network Access in hybrid corporate networks

Source: Created by author.

This reorientation helps explain the growing relevance of Zero Trust Network Access. Traditional VPNs still function effectively as encrypted tunneling mechanisms, but they often operate with a relatively broad logic of connectivity. In many scenarios, once initial authentication is completed, the user gains visibility into or reachability across large portions of the internal network, even though legitimate activity may require access only to specific applications. This design can enlarge the attack surface if credentials are compromised or endpoints are exploited by malicious actors. The core issue is not the encryption of the tunnel, but the operational assumption of relatively broad trust after entry has been granted.

ZTNA, by contrast, seeks to reduce that exposure through finer-grained mediation. Instead of connecting the user to the network as a whole, the architecture tends to connect the user only to the authorized resource according to identity, context, endpoint posture, and asset sensitivity. (see the generated image above) This distinction is relevant for lateral-movement containment, because it reduces the likelihood that an initial compromise can expand to systems unrelated to the user's legitimate task. The literature suggests that this model is especially compatible with remote-work settings and with organizations operating across both cloud and on-premises environments.

Another important point is that Zero Trust should not be described as a magical solution or as universally simple to deploy. Although surveys and reviews consistently report benefits related to minimizing excessive privilege, improving visibility, and strengthening access governance, the same authors emphasize that architectural effectiveness depends on institutional maturity and technical integration. Without accurate asset inventories, proper resource classification, coherent identity governance, and reliable telemetry, the adoption of Zero Trust language may result only in an additional layer of complexity without meaningfully reducing implicit trust within the environment.

The literature also indicates that microsegmentation and continuous verification play a central role in limiting the operational range of attacks. In traditional architectures, segmentation is often insufficient or overly broad, allowing malicious actors to move laterally after obtaining an initial foothold. In a Zero Trust model, the combination of logical segmentation, dynamic policy enforcement, and session-context reevaluation makes such movement more difficult because access is not assumed to be either permanent or generalized. (see the generated image above) In ransomware-prone environments, this point is especially important, since rapid containment of propagation may be just as important as preventing the initial intrusion.

There is also an operational dimension that requires more precision than is typically found in generic discussions of the topic. It is not appropriate to claim that Zero Trust always improves performance or always reduces friction in every implementation. What the literature supports is a narrower and more defensible statement: by replacing broad connectivity with contextual, application-oriented access, the architecture can rationalize authentication flows and reduce unnecessary exposure, provided that it is well-designed and properly orchestrated. In a recent study on software-defined perimeter protection for remote services, effective brute-force mitigation was observed alongside preserved throughput and improved latency under specific attack conditions, suggesting that, in certain configurations, stronger security and operational efficiency are not necessarily incompatible goals. Even so, these findings should be interpreted within the scope of the study rather than generalized as universal performance gains.

Regulatory alignment is another recurring theme. Zero Trust does not replace governance programs, nor does it guarantee full compliance on its own. However, its emphasis on least privilege, auditability, strong authentication, data protection, and contextual access control may support better demonstrations of due care and lower unnecessary exposure of sensitive information. (see the generated image above) This is especially relevant in corporate environments subject to data-protection obligations and access traceability requirements. According to multiple survey-based studies of ZTNA implementations, organizations deploying these controls tend to report improved auditability and more granular justification for who accessed a given resource, under which conditions, and with what authorization level.

A further conceptual advance lies in understanding Zero Trust as an adaptive architecture rather than a static rule set. Recent work highlights the importance of automation and orchestration so that contextual signals, including behavioral anomalies, changes in device state, or unusual location patterns, can be translated into access decisions in near real time. This increases the model's defensive potential, but it also reveals its dependence on integration across identity systems, observability layers, policy engines, and enforcement points. The quality of implementation is therefore as important as nominal adherence to the framework.

IV. CONCLUSION

The reviewed literature supports the view that Zero Trust Architecture constitutes a coherent response to the limits of perimeter-based security in contemporary corporate networks. Its main contribution is not the indiscriminate multiplication of barriers, but the redefinition of access around identity, context, least privilege, and continuous validation. Compared with VPN-centric approaches and models that rely on implicit trust after connection, Zero Trust offers finer access granularity, stronger lateral-movement containment, and better alignment with hybrid, remote, and cloud-oriented environments. [1–8] Even so, the benefits attributed to the model are defensible

only when described with care, avoiding excessive generalization or absolute promises. Zero Trust should therefore be presented as an architecture of governance and continuous resource protection whose effectiveness depends on sound technical design, operational integration, and institutional maturity.

REFERENCES

[1] Rose S, Borchert O, Mitchell S, Connelly S. Zero trust architecture. Gaithersburg: National Institute of Standards and Technology; 2020. doi:10.6028/NIST.SP.800-207.

[2] Syed NF, Shah SW, Shaghaghi A, Anwar A, Baig Z, Doss R. Zero trust architecture (ZTA): a comprehensive survey. IEEE Access. 2022;10:57143-57179. doi:10.1109/ACCESS.2022.3174679.

[3] Sarkar S, Choudhary G, Shandilya SK, Hussain A, Kim H. Security of zero trust networks in cloud computing: a comparative review. Sustainability. 2022;14(18):11213. doi:10.3390/su141811213.

[4] Zohaib SM, Sajjad S, Iqbal Z, Yousaf M, Haseeb M, Muhammad Z. Zero trust VPN (ZT-VPN): a systematic literature review and cybersecurity framework for hybrid and remote work. Information. 2024;15(11):734. doi:10.3390/info15110734.

[5] Cao Y, Pokhrel S, Zhu Y, Doss R, Li G. Automation and orchestration of zero trust architecture: potential solutions and challenges. Mach Intell Res. 2024;21:294-317. doi:10.1007/s11633-023-1456-2.

[6] Nahar N, Andersson K, Schelén O, Saguna S. A survey on zero trust architecture: applications and challenges of 6G networks. IEEE Access. 2024;12:94753-94764. doi:10.1109/ACCESS.2024.3425350.

[7] Ruambo FA, Masanga EE, Lufyagila B, Ateya AA, Almousa M, Abd-El-Atty B. Brute-force attack mitigation on remote access services via software-defined perimeter. Sci Rep. 2025;15(1):18599. doi:10.1038/s41598-025-01080-5.

[8] Gambo ML, Almulhem A. Zero trust architecture: a systematic literature review. J Netw Syst Manage. 2025. doi:10.1007/s10922-025-09998-x.

[9] Pourre, C. B. F. (2024). UMA ANÁLISE BIBLIOMÉTRICA DA PESQUISA DE FRAMEWORK DE CIDADES INTELIGENTES. Revista Sistemática, 14(8), 591–605. https://doi.org/10.56238/rcsv14n8-00926.

[10] [1:19 PM, 19/05/2026] Carlla Furlan Pourre: POURRE, C. B. F. Indicadores de resultados finalísticos como instrumento de diagnóstico do transporte urbano: um estudo de caso do Distrito Federal. 2020. Dissertação (Mestrado em Arquitetura e Urbanismo) – Universidade Federal de Brasília, Brasília, 2020. Disponível em: https://repositorio.unb.br/handle/10482/38743. Acesso em: 23 out. 2025.

[11] Carlla Furlan Pourre: FURLAN, Carlla Brito; SANTOS, Gleys Ially Ramos dos. 2016. A qualidade do transporte público urbano em cidades médias: estudo de caso em Palmas-Tocantins. Revista em Gestão, Inovação e Sustentabilidade. Disponível em: chrome-extension://efaidnbmnnMarecilda; Mello, Cristina de. 2022.

[12] Gotardi Pessoa, E. (2025). Analysis of the performance of helical piles under various load and geometry conditions. *ITEGAM-JETIA*, *11*(53), 135-140. https://doi.org/10.5935/jetia.v11i53.1887

[13] Gotardi Pessoa, E. (2025). Sustainable solutions for urban infrastructure: The environmental and economic benefits of using recycled construction and demolition waste in permeable pavements. *ITEGAM-JETIA*, *11*(53), 131-134. https://doi.org/10.5935/jetia.v11i53.1886