International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

Zero-Trust-Based Cybersecurity Framework for Large-Scale Corporate Networks

Kang Geol

Senior Security Architect, Hyundai Autoever America, Fountain Valley, California, USA

Abstract: ***The article examines a cybersecurity framework for an extensive, distributed corporate network, constructed on the principles of zero-trust architecture. The objective is to substantiate the transition from a perimeter-centric model to a systemic zero-trust architecture, given blurred network boundaries, multi-cloud infrastructure, and the escalating costs of cyber incidents. The study's relevance is driven by the dominance of web applications and DDoS attacks in the incident landscape, the heterogeneity of internal endpoints, and mounting regulatory pressure. The novelty of the work lies in the synthesis of a multi-layer framework that integrates a standardized corporate web application firewall and a global DDoS mitigation program, a network access control platform, cloud security posture management tools, privileged access management, and contextual data access control, all bound together by a unified model of identity, policy, and telemetry. The framework is grounded in an empirical case of a large-scale network and formalized as a stepwise implementation roadmap. It is shown that the proposed approach ensures the practical feasibility of zero trust architecture at the scale of hundreds of domains and thousands of connections, transforming fragmented perimeter-hardening measures into a coherent model of continuous verification and microsegmentation. The article is intended for cybersecurity architects, IT and information security leaders, and researchers of corporate networks.***

Keywords: zero trust architecture, cybersecurity, large corporate networks, network access control

1. Introduction

Zero-trust architecture emerges as a response to the misalignment of the classical perimeter model with the contemporary structure of corporate networks. Perimeter-centric logic presupposes a rigid boundary between the internal and external environment, within which traffic and subjects are to a large extent, trusted by default. Under conditions of widespread remote work, mobile access, bring-your-own-device models, and intensive use of public and private clouds, such a boundary becomes blurred: a significant share of resources and workloads resides outside the formal perimeter, and users connect to them from unpredictable network contexts. Standardization bodies emphasize that a node's position in the network is no longer a reliable indicator of its trustworthiness. That protection must shift from network segments to specific resources and access subjects [1].

At the same time, the economic consequences of incidents exert additional pressure on infrastructure. According to an annual study of major confidentiality breaches, the average cost of a single incident in 2023 reached 4.45 million USD, reflecting a persistent upward trend over recent years and demonstrating the inadequacy of purely perimeter-based approaches amid an increasingly complex threat landscape [2].

The zero-trust concept rests on several interrelated principles that radically revise the assumptions of the classical model. Central among them is the requirement to never trust automatically and always verify. Every request to a resource, irrespective of the user's or device's network location, must be accompanied by strict authentication and authorization based on up-to-date context. Research surveys emphasize that this is complemented by the principle of least privilege, whereby entitlements are provisioned according to a minimally sufficient set and adjusted as roles, tasks, and risk levels evolve, as well as by microsegmentation, which constrains lateral movement of an adversary within the infrastructure and disrupts traditional flat internal networks [3].

Another foundational element is the assumption of compromise: protection is engineered as though an attacker is already present in the system, which necessitates continuous monitoring of subject behavior and traffic and reliance on telemetry from multiple components. Systematic literature reviews show that zero-trust architectures constitute a distinct research direction, for which typical taxonomies, lists of involved technologies, and catalogues of characteristic implementation challenges have already been formulated [4].

The specific characteristics of large corporate networks further accentuate the relevance of this shift. Organizations operating across dozens of geographically distributed offices and branches, with thousands of users and service devices, hundreds of corporate and customer domains, and heterogeneous multi-cloud infrastructure, are characterized by continuous growth in network topology complexity and access chains. Extensive use of cloud services results in the vast majority of enterprises integrating public and private clouds into their operations, with the projected share of workloads migrated to the cloud environment exceeding 80%, further eroding the boundaries of the classical perimeter and enlarging the attack surface.

Simultaneously, the density of inter-service dependencies, the volume of data exchanged, and the number of regulatory requirements all increase, rendering ineffective any attempt to strengthen only the external protective shell. Under these conditions, zero trust architecture functions as a systemic foundation that enables the coordinated redefinition of authentication, authorization, segmentation, and monitoring mechanisms across all layers, from network infrastructure and cloud platforms to application services and protected data, which is elaborated sequentially in the following sections.

2. Literature Review

The research corpus on zero trust architectures demonstrates an evolution from conceptual frames toward detailed taxonomies and applied models for corporate networks: the baseline NIST SP 800-207 architecture formulates the key principles of rejecting perimeter logic, continuous verification, least privilege, and assumed compromise design [1], while subsequent reviews develop these propositions by offering comparative analyses of implementations and typical deployment patterns in corporate environments [3, 4, 8]. Against the backdrop of steadily rising incident costs and an expanding attack surface due to cloud adoption and remote work [2], the literature records a shift in the attack vector from classical network services to the application layer: web applications have become the dominant channel of compromise, making web application firewalls and associated context-aware request control policies a pivotal element of zero trust at the service boundary [5].

In parallel, industry reports on DDoS emphasize a qualitative shift toward multivector, long-running campaigns that demand distributed mitigation programs and tight coupling of network and application-layer filtering with behavioral analytics [6, 7]. At the internal network layer, work on network access control evolution shows a transition from static port-based control to dynamic NAC platforms that act as central decision points for access control and implement microsegmentation and context-aware connection management in the spirit of zero trust [9, 10, 11]. Finally, contemporary guidelines on SIEM and SOAR emphasize the role of centralized telemetry collection and response orchestration as the connective tissue that binds disparate protection tools, perimeter, network, cloud, and application, together into a unified implementation of the zero trust framework for large-scale corporate networks [12].

3. Problem Definition

The problem addressed in this work is that the classical perimeter model of cybersecurity is methodologically misaligned with the actual complexity of large corporate networks featuring thousands of heterogeneous endpoints, hundreds of internal and external domains, and multi-cloud infrastructure in which a significant portion of workloads is located beyond the formal perimeter [1, 2]. In practice, this leads to a situation where, even when individual defensive contours, firewalls, VPNs, traditional filtering and monitoring tools, are reinforced, the organization remains vulnerable to dominant attack types, including exploitation of web application vulnerabilities, multivector DDoS campaigns, and lateral movement of an adversary within the network after initial compromise [5–7, 8].

Existing research and standards on zero trust architectures formulate the principles of rejecting automatic trust, enforcing least privilege, and assuming compromise, but predominantly describe either high-level conceptual models or narrowly focused technological solutions (NAC, WAF, SIEM/SOAR, cloud security) without integrating them into a scalable, practice-oriented framework for large, distributed networks [1, 3, 4, 9–12]. As a result, large organizations lack a systematized architectural blueprint that demonstrates how, based on zero trust principles, to integrate perimeter, network, cloud, and application security controls coherently, define unified decision points for access, telemetry flows, and automated response mechanisms, and implement a phased roadmap for transitioning from fragmented measures to a holistic zero trust architecture.

4. Methodology

Methodologically, the study employs a multi-layered approach that combines a systematic literature review with constructive architectural synthesis and applied case analysis. At the first stage, existing zero trust taxonomies and typical architectural patterns [1, 3, 4, 8, 11] were compared against the empirical model of an extensive corporate network, which made it possible to derive an invariant set of principles (continuous verification, least privilege, assumed compromise) and project them onto the perimeter, internal network, cloud plane, and data domains.

At the second stage, a comparative analysis was carried out for technology classes, web application firewalls and global DDoS mitigation programs, network access control platforms, cloud security posture management tools, privileged access management systems, and centralized monitoring solutions, assessing their ability to operationalize zero trust principles under scaling to hundreds of domains and thousands of connections [5–7, 9–12].

At the third stage, based on the established threat–control correspondences and the constraints of a large organization, an integrated framework was synthesized: access decision points were defined at various levels, along with the identity and policy model, required telemetry flows, and typical automated response chains; subsequently, a phased implementation roadmap was developed that aligns quick wins with profound architectural transformation.

5. Results and Discussion

In the second half of the previous decade, web applications finally became the dominant attack vector against corporate infrastructure, particularly for large organizations with hundreds of external and internal domains. According to a data breach investigation report, web applications featured in a substantial share of incidents and leaks, and separate studies indicate that they accounted for up to eighty percent of recorded incidents and sixty percent of confirmed breaches in 2023, reflecting a shift of attackers away from classical network services toward the application layer [5].

Against this backdrop, the web application firewall is regarded as the primary line of defense for Internet-facing infrastructure, and comparisons of different implementations show that, despite variations in accuracy and false positive rates, most solutions can effectively block a significant fraction of common application attacks. In the terminology of zero-trust architecture, this implies moving control from the abstract network perimeter to the boundary of a specific service, where every request to a resource traverses a policy layer tailored to the request's context and client characteristics.

In a large, distributed organization with hundreds of corporate and customer domains, this necessitates a standardized corporate web application firewall deployed as a unified service. Such consolidation enables uniform filtering policies, virtual patching of vulnerabilities before code updates, differentiated regimes for critical financial and customer services versus less stringent ones for auxiliary resources, and centralized telemetry collection for subsequent analysis in event correlation and behavioral analytics systems. From a zero-trust perspective, this transforms each incoming application request into a separate decision point: authentication and authorization are complemented by content filtering and checks against profiles of normal behavior, thereby reducing the probability of exploiting configuration errors and vulnerabilities in the application stack.

Alongside application integrity, zero-trust architecture requires that availability be treated as an equal component of security, especially given the evolution of distributed denial-of-service attacks. Industry reports record a significant increase in the intensity and volume of such attacks, up to multiple terabits per second, and characterize 2023 as a period of qualitative change in the threat landscape, when multivector and long-duration campaigns become the norm rather than an exception [6]. Figure 1 illustrates pronounced interannual and intra-annual variability of the indicator: in all years, maxima are observed in the spring months (predominantly March) and early autumn, while minimum values are recorded in the winter months and mid-summer. The most anomalous spikes occur in March 2020 and September 2022 (around 25–30%), whereas 2023 is characterized by an unusually high level already in January, followed by a relative smoothing of the curve within the 6–15% range.

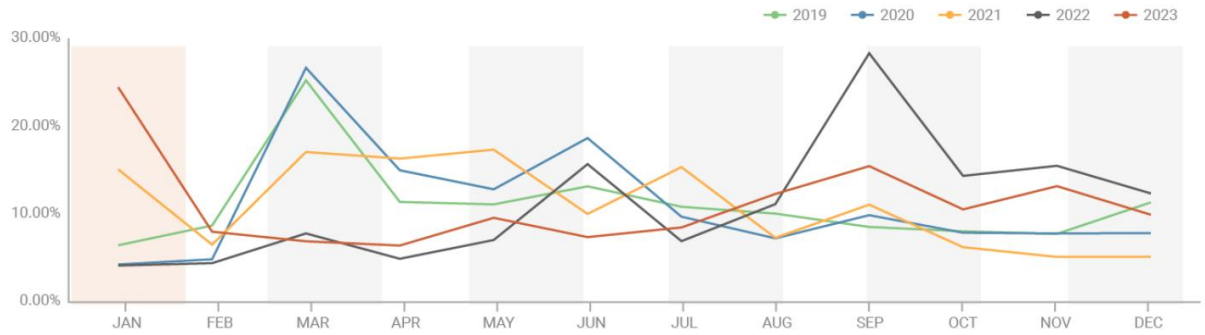

Figure 1: DDoS Attack Trends from 2019 to 2023 [6]

Academic work underscores that traditional perimeter tools, including general-purpose network firewalls, struggle to detect and filter modern DDoS campaigns and proposes integrating zero-trust principles and behavioral analysis to improve detection and mitigation effectiveness [7]. In this logic, a global DDoS mitigation program designed to protect critical customer services, such as access to online functions of an automotive manufacturer in the US market, relies on distributed traffic scrubbing centers at the carrier level, multi-layer filtering at the network and application layers, and tight coupling between web application firewalls and the monitoring system. Incoming traffic passes through a chain of coordinated control points, where decisions are made not only based on volume and protocol characteristics, but also on behavior, request history, and the aggregate of risk signals; all telemetry is fed into a centralized analytics system that supports the zero trust model and ensures coherence between perimeter and application protection and the subsequent architectural layers discussed below.

Even with strengthened perimeter protection, as described in the previous section, the internal network of a large organization remains vulnerable if it is still treated as a homogeneous, trusted zone. Classical security models assume that any subjects within the corporate boundary deserve more trust than those outside, which directly contradicts the principles of a zero-trust architecture, where network location is not a basis for granting privileges. Research on zero-trust architectures emphasizes that automatic trust in internal participants and the absence of strict verification for every network connection create conditions for unhindered lateral movement by an adversary after initial compromise [8].

In large enterprises where the internal environment comprises thousands of heterogeneous endpoints, corporate laptops, employees' personal devices, specialized equipment, and Internet-of-Things elements, the simple dichotomy of internal versus external zones becomes methodologically untenable. This compels a shift in emphasis away from guarding an abstract perimeter toward strict control of every network connection, regardless of which office, wiring closet, or wireless segment it originates from.

In this context, network access control systems based on port control standards and acting as a single decision point for admission are considered a fundamental mechanism for implementing zero-trust principles at the network layer. Network access control verifies both user credentials and device characteristics. It can enforce specific network contexts, virtual local area networks, security group tags, and access control lists, based on the user's role, the device's technical state, and the current risk level. Industry reviews of the evolution of such solutions demonstrate a transition from first-generation tools focused on basic authentication and blocking toward multifunctional platforms that provide dynamic access management, support for guest and temporary connections, and deep integration with other security components [9].

In the architecture under consideration, this class of solutions, implemented in particular using the Cisco Identity Services

Engine platform, is deployed across dozens of geographically distributed offices and branches, covering thousands of wired and wireless connections. According to technical documentation, this platform is positioned as a central element of zero trust architecture for the workplace: it makes decisions on network admission based on a combination of user and device attributes, profiles endpoints, assigns them security group tags, and implements segmentation according to the principle of least privilege [10]. Cisco ISE license packages are shown in Figure 2.

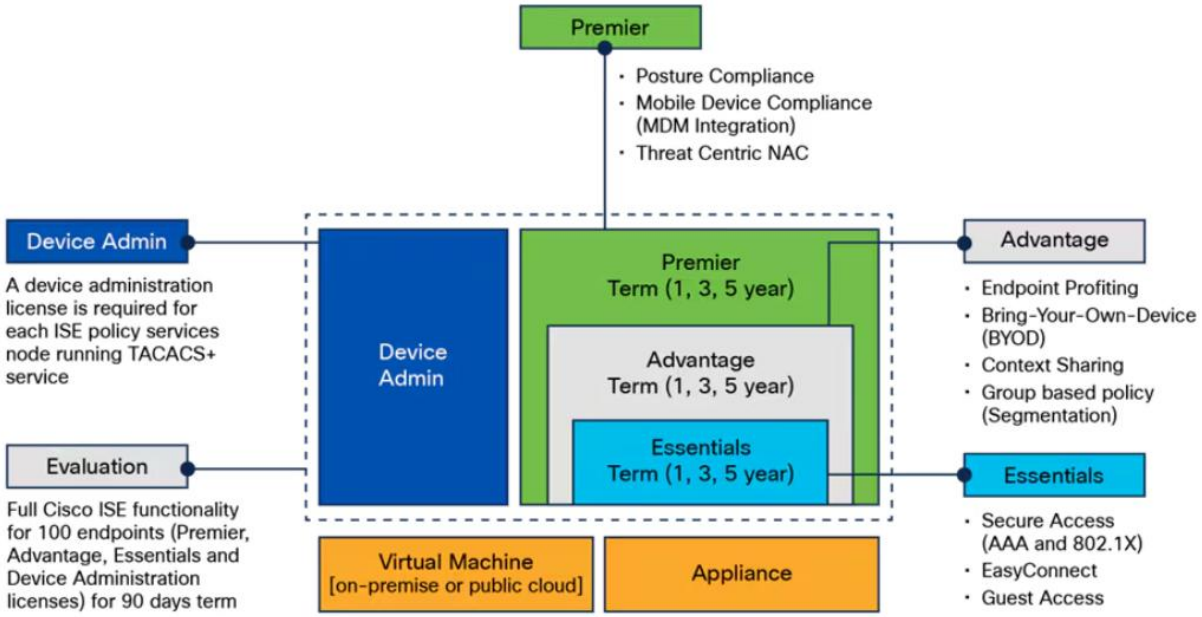

Figure 2: Cisco ISE license packages [10]

Scaling to thousands of nodes and hundreds of switching points is achieved through a distributed architecture, automated profiling, and tight integration with wired and wireless communication infrastructure.

In a zero-trust architecture, not only the moment of initial admission but also the subsequent operation of network access control as a telemetry source and an operational response lever are critical. Modern guidelines for designing zero-trust architectures emphasize the importance of continuous trust assessment across multiple attributes, from device parameters to behavioral characteristics, as reflected in research on dynamic access management models grounded in integrated risk and trust scores for each resource request [11].

In practice, this is implemented by integrating the network access control platform with the identity management system, endpoint detection and response tools, and a centralized event collection and correlation system, where data on every connection and device state change form part of the overall picture. Recommendations for deploying centralized monitoring systems highlight the need to include network access control logs among the priority sources, as they record the details of all network access attempts and enable automated isolation and quarantine segmentation of devices when anomalies and incidents are detected [12]. As a result, network access control and solutions such as Cisco Identity Services Engine evolve from an auxiliary connection-control component into a supporting element of the zero-trust architecture, providing microsegmentation, selective admission, and managed isolation of compromised devices at scale across the entire corporate network.

The transition to a zero-trust architecture across an extensive corporate network remains incomplete if it affects only the perimeter and the internal network while ignoring cloud platforms and environments where the most valuable data is processed. The cloud infrastructure of such organizations encompasses numerous accounts, projects, and subscriptions across multiple public and private clouds, where new virtual machines, container clusters, and serverless functions are constantly created. Under these conditions, manual control of configurations and security policies is practically impossible, and individual misconfigurations become tantamount to creating hidden entry points. Specialized cloud security posture management and cloud workload protection platforms introduce continuous automated auditing of parameters for network access, encryption, key management, interservice communication, and access rules, benchmarking them against internal policies and international information security standards. Simultaneously, they analyze the behavior of virtual machines, containers, and serverless functions, as well as traffic within cloud segments, to limit lateral movement and identify anomalous interactions between services. Thus, the principles of least privilege and continuous verification previously described for the perimeter and local network are directly extended into the cloud plane.

An equally important dimension of zero trust architecture is privileged access management and data access control in critical development and financial analysis environments. These domains house confidential algorithms, engineering specifications, economic models, and aggregated customer data, whose loss or tampering would have disproportionately severe consequences. The traditional model, in which administrative accounts are permanent and have broad entitlements, is overly susceptible to misuse and compromise. Privileged access management systems transform this area into a just-in-time regime: an administrator or engineer receives elevated privileges only for a limited interval and

strictly for a specific task. At the same time, the credentials themselves are stored in a protected secrets vault, and all session activity is recorded for subsequent analysis. In parallel, data access management systems introduce finer-grained entitlements at the level of datasets and data fields, taking into account not only the user's formal role but also the context of the request: from which environment the user connects, on which device they operate, how sensitive the requested information is, and whether their behavior deviates from typical patterns. This combination of privileged and context-aware data control significantly reduces the risk of external intrusions leveraging internal accounts and of intentional or unintentional insider actions.

The entire system is part of a single, integrated zero-trust architecture that includes web application firewalls, global denial-of-service protection, network access control systems, and protection for cloud and critical systems, as mentioned above. Smoothly integrated through a single identity and policy model, every user, device, service, and dataset is understood in terms of a standard, consistent set of attributes and trust level, and every access decision is taken at all boundaries and data flows, from the instant of network connection through to the request for the specific resource in the cloud. Centralized logging and telemetry collection in a security event and behavioral analytics platform provide a holistic view of network access attempts, web application requests, configuration changes to cloud resources, the issuance of privileged rights, and operations involving sensitive data. On this basis, automated response methods are constructed, whereby an incident orchestration platform, upon detecting anomalies, tightens rules on the web application firewall, moves suspicious devices into a quarantine segment, revokes privileged sessions, and initiates remediation of unsafe settings in cloud accounts.

For a large organization, the transition to such a model cannot be instantaneous, necessitating a phased implementation roadmap. The next step is to produce an inventory of existing resources, access flows, and security tools, rank order the most meaningful gaps between existing practice and zero trust principles, and identify quick wins, where significant benefits can be obtained without meaningful architectural changes in the short term. These include initial steps such as adding web application firewall protection, implementing basic network access controls, and performing configuration auditing. Later designs may involve more advanced changes, such as centralized privileged access management, context-based data controls, global DDoS protection, and consolidating all components into a single analytics and orchestration platform that closely integrates the different security controls (see Figure 3).

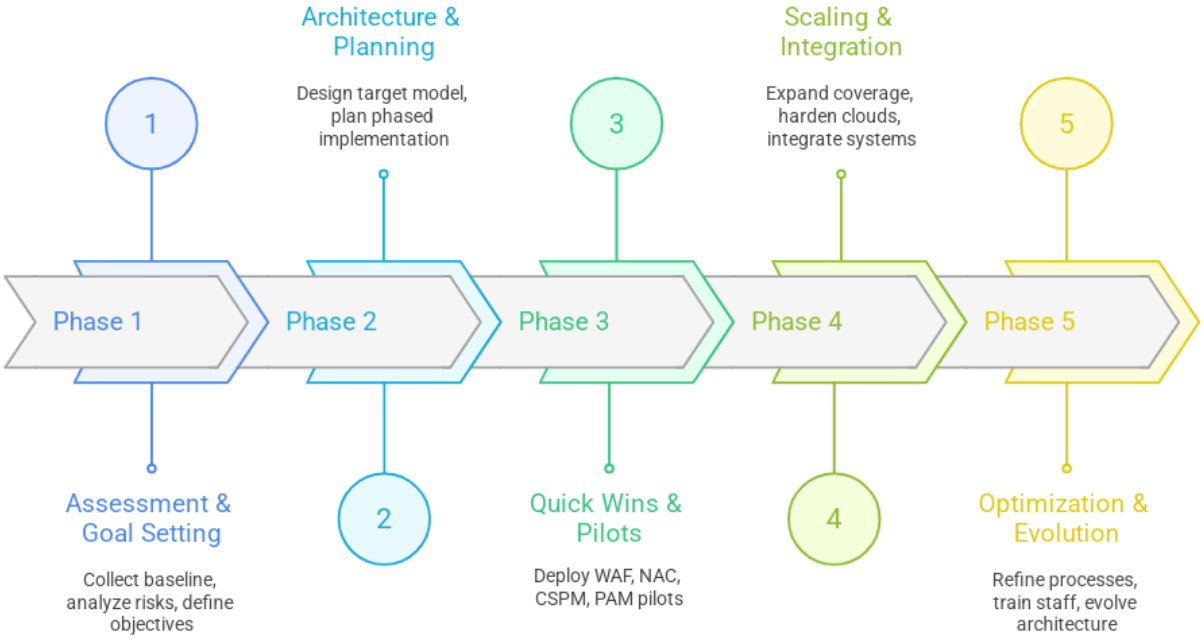

Figure 3: Implementation Roadmap

As a result, the organization gradually shifts from fragmented security to an integrated zero-trust framework, in which every new technology and service is initially embedded within a unified model of identity, policy, and observability. A promising direction for further development is the adoption of zero-trust network access approaches, secure access service edge concepts, and increasingly extensive use of artificial intelligence and machine learning methods to enhance the sensitivity and robustness of analytics to complex, low-obviousness threats.

6. Conclusion

The cybersecurity framework presented in this work demonstrates that the transition to a zero-trust architecture for an extensive, distributed corporate network is feasible only through a comprehensive transformation across multiple planes simultaneously, from the perimeter and internal network to cloud platforms and critical data domains. It is shown that the dominance of web applications in the incident structure, the evolution of distributed denial-of-service attacks, the erosion of the network perimeter by remote work and multi-cloud environments, and the heterogeneity of internal endpoints render the classical trusted boundary model methodologically untenable. Against this backdrop, zero trust

architecture, grounded in the assumption of compromise, the principle of least privilege, microsegmentation, and continuous context verification for each request, functions not as a point enhancement atop existing infrastructure but as a systemic frame into which all security layers must be embedded.

The solution developed in the article concretizes this frame through a set of interrelated mechanisms implemented at the scale of an extensive corporate network. At the perimeter and service boundaries, this is achieved through a standardized corporate web application firewall deployed as a unified service in front of hundreds of domains and providing near-complete coverage of Internet-facing resources, as well as a global DDoS mitigation program with distributed traffic scrubbing centers and multi-layer filtering. The internal network layer is transformed from a trusted zone into a regime of selective, context-dependent access via a network access control platform deployed across dozens of offices and branches that implements dynamic assignment of network contexts, microsegmentation, and managed isolation of compromised devices. The cloud dimension of zero trust architecture is enabled by specialized security posture management and workload protection tools that ensure continuous configuration auditing and analysis of interactions across the multi-cloud environment. For the most sensitive data and processes, the focus is on privileged access management, context, and information-centric data operations, integration through a common identity and policy framework, central telemetry, information security analytics, and automated responses to triggers from incident management platforms that connect these processes.

The phased implementation roadmap, including asset and access-flow inventory, the elimination of the most critical gaps between the current state and zero-trust principles, the realization of quick wins, and subsequent profound changes, illustrates the practical feasibility of the proposed approach within a large organization. Taken together, the results presented show that the transition from fragmented perimeter-hardening measures to a holistic zero trust architecture enables corporate cybersecurity development to be structured as a stepwise enhancement of a unified identity, policy, and observability framework into which new technologies and services are embedded from the outset. The outlined directions for further evolution, zero trust network access, secure access service edge concepts, and the growing role of artificial intelligence and machine learning in behavioral analytics indicate that the architecture described can serve not as an end state but as a stable foundation for the continued development of corporate protection in an increasingly complex threat landscape.

7. Future Scope

Prospects for further research primarily concern deeper formalization of the trust and risk models underpinning the zero-trust architecture in large, distributed networks. A transition is required from heuristically defined policies to formalizable, verifiable decision-making schemes integrated with policy-as-code mechanisms, declarative configuration management, and formal methods for verifying the correctness of access policies. Of particular interest is the development of maturity and observability metrics for zero trust frameworks, enabling quantitative assessment of resource coverage, telemetry density, microsegmentation effectiveness, and the degree of response automation. A separate line of inquiry concerns the application of machine learning and behavioral analytics methods not only for anomaly detection but also for dynamic policy adaptation in a changing threat landscape and a highly variable business environment.

An equally significant area of advancement involves transforming the proposed framework into domain-specific profiles for individual industries and architectural paradigms, from highly regulated financial and telecommunications ecosystems to industrial Internet of Things, 5G/edge scenarios, and distributed supply chains. In this context, there is a need to refine requirements for integrating zero trust with secure access service edge and security service edge (SASE/SSE) concepts, cross-platform identity and access management solutions, and cloud-native protection tools. An additional direction for research will be the development of organizational and process models describing the evolution of roles and competencies in information security and IT departments, the management of technical and social debt during phased migration from perimeter practices to zero trust architecture, and the empirical assessment of how such transformations affect business resilience and regulatory compliance.

References

[1] Rose S, Borchert O, Mitchell S, Connelly S. Zero trust architecture. NIST Special Publication 800-207 [Internet]. 2020 Aug [cited 2025 Nov 1]; Available from: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

[2] Help Net Security. Average cost of a data breach reaches $4.45 million in 2023 [Internet]. Help Net Security. 2023 [cited 2025 Nov 1]. Available from: https://www.helpnetsecurity.com/2023/07/24/ibm-cost-data-breach-report-2023/

[3] Dhiman P, Saini N, Gulzar Y, Turaev S, Kaur A, Nisa KU, et al. A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. Sensors. 2024 Jan 1;24(4):1328.

[4] Gambo ML, Almulhem A. Zero Trust Architecture: A Systematic Literature Review. Journal of Network and Systems Management. 2025 Nov 13;34(1).

[5] Bureau O. Web applications were used in 80% of security incidents and 60% of breaches in 2023: Barracuda [Internet]. ETCIO. 2024 [cited 2025 Nov 4]. Available from: https://ciosea.economictimes.indiatimes.com/news/security/web-applications-were-used-in-80-of-security-incidents-and-60-of-breaches-in-2023-barracuda/107836392

[6] DDoS Statistical Report for 2023 [Internet]. Nexusguard. 2023 [cited 2025 Nov 5]. Available from: https://nexusguard.com/threat-report/ddos-statistical-report-for-2023

[7] Ashfaq F, Wasim M, Shah MA, Ahad A, Pires IM. Enhancing Security in 5G Edge Networks: Predicting

Real-Time Zero Trust Attacks Using Machine Learning in SDN Environments. Sensors. 2025 Mar 19;25(6):1905.

[8] Habash RM, Khalel M. Zero Trust Security Model for Enterprise Networks. Iraqi Journal of Information and Communication Technology. 2023 Aug 31;6(2):68–77.

[9] Fortinet. The Evolution of Network Access Control (NAC) How IoT and Telework Have Changed NAC Solutions [Internet]. Fortinet. Fortinet; [cited 2025 Nov 8]. Available from: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-evolution-of-network-access-control.pdf

[10] Cisco. Cisco Identity Services Engine Data Sheet [Internet]. Cisco. 2025 [cited 2025 Nov 9]. Available from: https://www.cisco.com/c/en/us/products/security/identity-services-engine/ise-ds.html

[11] Bradatsch L, Miroshkin O, Trkulja N, Kargl F. Zero Trust Score-based Network-level Access Control in Enterprise Networks. Arxiv. 2024 Feb 13.

[12] Ministry of Defence. Implementing SIEM and SOAR platforms: practitioner guidance [Internet]. Ministry of Defence. 2025 [cited 2025 Nov 11]. Available from: https://media.defense.gov/2025/May/27/2003722066/-1/-1/0/IMPLEMENTING-SIEM-AND-SOAR-PLATFORMS-PRACTITIONER-GUIDANCE.PDF