KMAN PUBLISHING INSTITUTE

Article history:
Received 06 June 2024
Revised 11 August 2024
Accepted 21 August 2024
Published online 01 September 2024

Journal of Resource Management and Decision Engineering

Volume 3, Issue 3, pp 21-32

The Zero Trust Security Model and Its Application in Organizations

Anoosheh Motamed[1*]

[1] Master's Degree in Information Technology, University of Guilan, Guilan, Iran

*** Corresponding author email address**: Anoosheh_motamed2005@yahoo.com

A r t i c l e I n f o

Article type:
Original Research

How to cite this article:
Motamed, A. (2024). The Zero Trust Security Model and Its Application in Organizations. *Journal of Resource Management and Decision Engineering, 3*(3), 21-32.
https://doi.org/10.61838/kman.jrmde.3.3.3

A B S T R A C T

This article aims to examine the conceptual foundations, architectural components, and practical applications of the Zero Trust security model within diverse organizational contexts, highlighting both its strategic benefits and implementation challenges. A narrative review methodology with a descriptive analysis approach was used to synthesize recent academic and industry literature published between 2022 and 2025. Sources were selected based on relevance to Zero Trust principles, implementation strategies, technological components, and behavioral considerations. The review focuses on key themes including identity and access management, continuous authentication, policy enforcement, and user behavior within cybersecurity frameworks. The Zero Trust model redefines organizational security by eliminating implicit trust and requiring continuous verification for every access request. Key components such as identity verification, multi-factor authentication, micro-segmentation, and real-time monitoring work together to prevent lateral movement and minimize the attack surface. The model has been effectively applied in government, enterprise, and small-to-medium business environments and has proven particularly valuable in hybrid cloud and remote work settings. Benefits include improved security posture, regulatory compliance, and adaptability to evolving digital infrastructures. However, organizations face challenges related to technical complexity, implementation costs, workforce resistance, and skills shortages. Despite these obstacles, phased adoption and cultural alignment can facilitate successful deployment. Zero Trust represents a significant shift from perimeter-based security toward a dynamic, behavior-aware, and policy-driven model that addresses the demands of modern cybersecurity threats. Its comprehensive and flexible architecture provides organizations with the tools to build resilient and adaptive security environments, though successful implementation requires strategic planning, investment, and ongoing education.

Keywords: *Zero Trust, cybersecurity, identity and access management, network segmentation, remote work security.*

1. Introduction

In recent years, the landscape of organizational cybersecurity has undergone dramatic transformation due to the proliferation of sophisticated cyber threats, the expansion of cloud-based services, and the rapid shift toward remote work environments. Organizations today operate in an ecosystem characterized by distributed endpoints, diverse digital infrastructures, and a heightened dependency on digital communication and data exchange. As a result, traditional models of cybersecurity—especially those based on perimeter defense—have proven increasingly inadequate in safeguarding critical assets. Breaches have become more frequent and complex, often leveraging insider threats, compromised credentials, or lateral movement across networks (Molleti & Khanna, 2025; Süzen & Ceylan, 2024). In such a dynamic threat environment, the effectiveness of legacy security strategies has come under critical scrutiny, compelling security architects to explore more resilient and adaptive frameworks.

Traditional perimeter-based models of cybersecurity rely on the assumption that threats originate externally and that once users and devices are authenticated within the internal network, they can be trusted implicitly. This security architecture, often described as a "castle-and-moat" model, focuses on building strong external defenses while allowing relatively unrestricted access within the internal network. While this approach may have been effective when corporate infrastructures were centralized and static, it is ill-suited to contemporary environments marked by mobility, cloud integration, and supply chain interconnectivity. Recent incidents have highlighted how attackers can exploit trusted network components and escalate privileges once inside the network. Furthermore, the insider threat—whether intentional or accidental—remains one of the most damaging and difficult to detect, as trust is conferred too broadly under the perimeter model (Dhiman et al., 2024; Huber & Kandah, 2024; Jensen, 2024).

Several studies have emphasized the vulnerability inherent in this architecture. For instance, Langdon et al. (2020) illustrated how digital health systems relying on traditional defenses often fail to ensure secure user engagement and adherence in the context of sensitive applications like opioid use disorder treatment (Langdon et al., 2020). Similarly, Kechter et al. (2021) noted that when systems are designed without considering users' psychological capacity to manage stress and distress, they are more susceptible to misuse, errors, or neglect, which in turn compromises security (Kechter et al., 2021). This body of research underscores that both technical and human dimensions of organizational security require a paradigm shift.

The emergence of the Zero Trust Security Model represents this critical shift. First conceptualized by John Kindervag at Forrester Research in 2010, Zero Trust is based on the fundamental principle of "never trust, always verify." It operates on the assumption that threats exist both inside and outside the organizational perimeter and therefore mandates continuous verification of users, devices, and access requests, regardless of their location or role. Unlike perimeter-based models, Zero Trust does not automatically trust any entity—whether internal or external—without rigorous identity validation, contextual analysis, and real-time access controls.

Over the last decade, and particularly in the post-2020 environment accelerated by the COVID-19 pandemic, Zero Trust has transitioned from theory to operational priority across industries. The dramatic expansion of hybrid workforces, cloud computing, and edge devices has catalyzed a deeper interest in adaptive and scalable cybersecurity frameworks. Zero Trust has found growing relevance in these settings, where conventional firewalls and static access rules fall short. The model's appeal lies in its granular control mechanisms, including micro-segmentation, least-privilege access, behavioral analytics, and real-time policy enforcement. As Anderson et al. (2024) suggest, in diverse global settings where security and trust vary significantly, a context-sensitive and behavior-aware security model like Zero Trust is crucial to reduce vulnerabilities and prevent policy failures (Anderson et al., 2024).

The relevance of Zero Trust in high-stakes environments is also increasingly documented. For example, Chaleshtori et al. (2022) emphasized the need for robust identity verification and emotional resilience mechanisms when dealing with at-risk populations such as adolescents with drug-addicted parents, suggesting that security frameworks must account for both digital and behavioral vulnerabilities (Chaleshtori et al., 2022). In another study, Henschel et al. (2021) linked security failures in prescription systems to low distress tolerance and lack of contextual safeguards, indicating how Zero Trust's emphasis on continuous monitoring can mitigate such human-centered risks (Henschel et al., 2021).

Despite its clear conceptual strengths, the implementation of Zero Trust is neither uniform nor without challenges. It

requires a fundamental rethinking of network architecture, organizational policies, and cultural attitudes toward trust and access. The transformation is not merely technical but strategic, implicating governance structures, human behavior, and inter-organizational coordination. As Hayes et al. (2023) observe, psychological stress, coping mechanisms, and perceived support all influence how users engage with security systems—highlighting the necessity of integrating human-centered design into Zero Trust implementations (Hayes et al., 2023). Similarly, Baker et al. (2023) reveal that low distress tolerance and high experiential avoidance in users are strong predictors of system misuse or security non-compliance, which reinforces the need for adaptive, real-time validation and policy enforcement (Baker et al., 2023).

This review aims to critically examine the Zero Trust security model and its application in organizational contexts through a descriptive analytical lens. The primary objective is to explore how Zero Trust has emerged as a response to the limitations of perimeter-based models, how it is conceptually and architecturally defined, and how it is being implemented in various organizational settings. The review further seeks to identify the core components and mechanisms of Zero Trust, assess its practical advantages, highlight implementation challenges, and map emerging trends for future application.

Accordingly, this review addresses several key research questions: What are the fundamental principles and architectural elements that define Zero Trust? How does the model address the shortcomings of traditional perimeter-based security frameworks? In what ways have organizations applied Zero Trust in practice, and what outcomes have they reported? What barriers—technical, psychological, cultural—impede the widespread adoption of Zero Trust? And finally, what future directions, including technological innovations and policy frameworks, are likely to shape the evolution of Zero Trust in organizational cybersecurity?

By addressing these questions, this article seeks to contribute to the growing academic and professional discourse surrounding cybersecurity modernization. As digital ecosystems grow in complexity and threat actors become more adaptive, understanding the theory and practice of Zero Trust will be essential for developing resilient, secure, and user-aware organizational environments.

2. Methods and Materials

This study adopts a narrative review methodology with a descriptive analysis approach to explore the Zero Trust security model and its application in organizational settings. Narrative reviews are particularly suited for synthesizing evolving concepts and emerging trends in rapidly changing technological domains such as cybersecurity. Unlike systematic reviews that rely on strict inclusion and exclusion criteria and quantitative synthesis, narrative reviews are more flexible in scope and emphasize the interpretive integration of diverse sources to construct a comprehensive conceptual understanding. Given the objective of this research—to trace, describe, and interpret the key features, components, challenges, and organizational implications of the Zero Trust model—this method was deemed most appropriate.

The descriptive analysis method was employed to systematically extract, categorize, and interpret key themes from the selected literature without conducting statistical meta-analysis. The focus was on identifying the foundational principles of Zero Trust architecture, the main components involved in its implementation, and its practical applications across various organizational environments. This method facilitates the identification of recurring patterns, emerging themes, and divergent viewpoints, enabling a structured yet interpretive synthesis of the literature.

To ensure the relevance and contemporaneity of the reviewed material, the literature search was limited to academic and professional publications from January 2022 to May 2025. This timeframe was selected to capture the most recent developments and implementations of Zero Trust, especially given the acceleration of cybersecurity reforms post-pandemic and the growing reliance on cloud and hybrid work infrastructures. The search was conducted across multiple reputable electronic databases, including IEEE Xplore, Scopus, ScienceDirect, SpringerLink, and Google Scholar. In addition to peer-reviewed journal articles, white papers, industry reports, and official cybersecurity frameworks such as NIST Special Publication 800-207 were also included to enrich the theoretical and practical dimensions of the analysis.

The search strategy involved using keyword combinations such as “Zero Trust architecture,” “Zero Trust security model,” “organizational cybersecurity,” “identity-based access control,” and “Zero Trust implementation in enterprises.” Only English-language sources were considered, and preference was given to articles that discussed the conceptual design, real-world deployments,

strategic value, and barriers to adoption of Zero Trust models in public or private organizations. To enhance the rigor of the selection process, articles were screened based on their relevance to at least one of the following themes: (1) conceptual foundations of Zero Trust, (2) implementation architecture and technologies, (3) organizational use cases, and (4) future trends in Zero Trust strategies.

A qualitative coding strategy was applied to thematically organize the literature and identify critical insights. Sources were analyzed to extract recurring concepts, contradictions, innovative frameworks, and recommendations related to Zero Trust. The descriptive synthesis process followed an iterative review of the materials, allowing for refinement of thematic categories such as identity governance, micro-segmentation, continuous monitoring, and policy enforcement.

3. Conceptual Foundations of Zero Trust

The Zero Trust security model is fundamentally defined by the principle “never trust, always verify.” Unlike traditional perimeter-based security frameworks that implicitly trust users or devices once they are authenticated within a defined network boundary, Zero Trust assumes that no actor—internal or external—should ever be trusted by default. Every attempt to access organizational resources must be verified dynamically based on multiple contextual factors, including user identity, device status, location, time, and behavioral patterns. The core philosophy of Zero Trust recognizes that modern threats often bypass traditional defenses by exploiting trusted credentials or infiltrating internal systems, thereby rendering perimeter-centric approaches insufficient.

Central to the Zero Trust architecture is the concept of identity verification. Access to data and systems is granted only after rigorous authentication of the user and device attempting to initiate the request. Authentication mechanisms typically involve multi-factor authentication (MFA), contextual behavioral analytics, and continuous risk assessment. In environments where security is highly dependent on user behavior, studies have shown that emotional regulation and psychological readiness also influence how reliably users interact with security controls. For instance, Anderson et al. (2023) observed that users with higher distress tolerance exhibited more responsible engagement with digital systems and had fewer problems related to misuse or error-prone behaviors (Anderson et al., 2023). Such findings reinforce the importance of dynamic identity verification that considers not only static credentials but also behavioral indicators.

Another critical principle of Zero Trust is least privilege access, which ensures that users and devices are granted only the minimum levels of access necessary to perform their specific tasks. By narrowing access rights and continually validating them, the Zero Trust model limits the potential impact of compromised accounts or malicious insiders. Felton et al. (2019) highlighted that users with low distress tolerance and impulsivity were more prone to risk-taking behavior, such as unauthorized data access or misuse of privileged roles (Felton et al., 2019). Therefore, reducing access privileges minimizes the probability of such vulnerabilities being exploited. Least privilege policies also facilitate better audit trails and anomaly detection, as deviations from baseline permissions can be quickly flagged for investigation.

Micro-segmentation, a third foundational element of Zero Trust, refers to the practice of dividing networks into smaller, logically isolated zones so that access between them can be tightly controlled. This segmentation prevents lateral movement within the network, a common technique used by attackers after an initial breach. Once a malicious actor gains entry into one part of the network under the traditional model, they can often move undetected across systems. In contrast, micro-segmentation in a Zero Trust environment ensures that even if one segment is breached, other segments remain protected. Kline et al. (2021) emphasized the value of compartmentalized access control when studying aggression and risk behaviors; their findings suggest that limiting overexposure to risky environments reduces the likelihood of policy violations and erratic behavior (Kline et al., 2021). Translated into cybersecurity terms, this supports the rationale for network micro-segmentation, which reduces exposure and improves containment in the event of a breach.

The Zero Trust model contrasts sharply with traditional network security frameworks, which are often referred to as "trust but verify" architectures. These conventional models rely heavily on boundary firewalls and demilitarized zones (DMZs) to regulate access, with internal traffic assumed to be safe. This model has been increasingly criticized due to its vulnerability to insider threats, supply chain compromises, and credential theft. Wolitzky-Taylor et al. (2016) demonstrated that assumptions of internal safety could be misplaced, especially when users face psychological pressures or distractions that affect judgment and compliance (Wolitzky-Taylor et al., 2016). Likewise,

Zapolski et al. (2018) highlighted how adolescents with low distress tolerance are more susceptible to impulsive behaviors, including system misuse, suggesting that implicit trust within a network can lead to critical security oversights (Zapolski et al., 2018).

The historical development of the Zero Trust model can be traced to John Kindervag's work at Forrester Research in 2010, where the concept was first articulated as a way to address the failings of perimeter-based models. Since then, the model has gained traction among security professionals and policymakers, especially as cyberattacks have become more sophisticated and identity-based threats have surged. The National Institute of Standards and Technology (NIST) significantly advanced the formalization of Zero Trust by publishing Special Publication 800-207, which provides a comprehensive framework for implementing Zero Trust architecture across federal and private organizations. This document outlines key components such as policy enforcement points, trust algorithm engines, and continuous diagnostics, offering a blueprint for scalable and context-aware security controls.

Further elaborating on the Zero Trust framework, Veilleux (2022) proposed a theory of momentary distress tolerance to explain how individuals make split-second decisions about whether to engage with or avoid security prompts and procedures (Veilleux, 2022). This aligns with Zero Trust's emphasis on continuous verification—the notion that authentication is not a one-time event but a persistent process, constantly updated as user behavior or environmental variables change. When implemented properly, this real-time approach strengthens the system's ability to detect anomalies, thwart lateral movement, and prevent privilege escalation.

Moreover, Zero Trust's focus on dynamic verification is supported by findings from Ghanbari et al. (2020), who compared behavioral therapies in high-risk populations and observed that ongoing monitoring and adjustment led to more sustainable outcomes (Ghanbari et al., 2020). In cybersecurity contexts, such adaptive strategies manifest as automated threat responses, AI-powered risk assessments, and context-sensitive access decisions—all of which are core features of modern Zero Trust platforms.

Notably, the adoption of Zero Trust has been bolstered by its flexibility across different organizational environments. For example, Sease et al. (2024) found that individuals involved in justice systems who experienced trauma were more likely to benefit from structured, rule-based environments (Sease et al., 2024). A similar principle applies in cybersecurity, where deterministic access policies can provide clarity and consistency in access control, especially in high-risk sectors such as healthcare, finance, and government.

The Zero Trust model is also uniquely suited to accommodate human psychological variability. Yıldız and Büyükfırat (2024) found that psychological flexibility and distress tolerance significantly influenced individuals' ability to cope with high-stress environments, a factor that translates into how users interact with security protocols and system prompts (Yıldız & Büyükfırat, 2024). In this context, Zero Trust serves not only as a technological architecture but also as a behavioral alignment mechanism, ensuring that security policies are responsive to users' cognitive and emotional states while still maintaining strict access governance.

Over time, the conceptual framework of Zero Trust has matured into an integrative security model that unites technical controls, behavioral analytics, and policy enforcement. Reese et al. (2019) emphasized the importance of post-treatment trajectories in behavioral compliance, suggesting that security systems too must accommodate long-term patterns rather than static profiles (Reese et al., 2019). Zero Trust captures this insight by continuously adapting to user behavior, system health, and environmental signals in real time.

In sum, the conceptual foundations of Zero Trust lie in its unwavering skepticism toward implicit trust, its architectural emphasis on identity and behavior-based validation, and its commitment to adaptive security controls that respond dynamically to shifting risk landscapes. This model challenges outdated assumptions of internal safety and offers a proactive, intelligent framework designed for the demands of modern digital ecosystems. As threats become more nuanced and human factors more influential, the Zero Trust philosophy offers not just an architectural remedy but a paradigm shift in how organizations conceptualize and operationalize trust.

4. Components and Architecture

The architecture of the Zero Trust model is structured around a series of interdependent components that work collectively to ensure rigorous access control, visibility, and adaptability across an organization's digital infrastructure. At the core of this architecture is the commitment to context-driven trust decisions, wherein every request for access must be continuously evaluated based on a set of dynamic and

multi-layered factors. These components are designed not only to verify identity and restrict access, but also to monitor behavior, enforce policy, and adapt in real time to changing conditions and emerging threats.

Identity and Access Management (IAM) plays a central role in the Zero Trust framework. IAM systems are responsible for ensuring that only authenticated and authorized individuals are granted access to specific organizational resources. Unlike traditional approaches where access is typically assigned based on roles or departments and rarely updated, IAM in Zero Trust environments operates on a principle of continuous validation. Each user's identity is rigorously verified through credentials, behavioral biometrics, and contextual cues such as device health or geolocation. As Reese et al. (2019) point out, users' access profiles should be treated as evolving trajectories rather than static entries, necessitating ongoing reevaluation to prevent unauthorized access (Reese et al., 2019). IAM systems in Zero Trust must be deeply integrated with user directories, behavioral monitoring tools, and access governance platforms to enable real-time authentication and fine-grained access provisioning.

Behavioral variability plays a critical role in identity verification. As Anderson et al. (2024) observed in a cross-continental study, distress tolerance is linked with the predictability and reliability of user behavior in digital environments (Anderson et al., 2024). This insight reinforces the need for adaptive IAM frameworks that take into account psychological patterns and emotional states, not just credential-based verification. Veilleux (2022) further proposed that decisions to engage with or avoid secure authentication steps are influenced by momentary distress tolerance, which suggests that effective IAM must balance security enforcement with user experience optimization (Veilleux, 2022). Therefore, IAM tools in Zero Trust systems are not only about gatekeeping but also about behavioral modeling and predictive risk scoring.

Complementing IAM is Multi-Factor Authentication (MFA), which introduces additional layers of security by requiring users to present two or more verification factors before access is granted. MFA typically includes combinations of knowledge-based credentials (e.g., passwords), possession-based factors (e.g., smartphones or tokens), and inherence-based identifiers (e.g., biometrics). The use of MFA substantially reduces the risk of account compromise resulting from credential theft or phishing attacks. As highlighted by Batchelder et al. (2017), users exposed to traumatic or high-risk environments are more prone to impulsive actions, making them more vulnerable to social engineering attacks and password reuse (Batchelder et al., 2017). By enforcing MFA, organizations introduce critical friction points that prevent unauthorized access even if one factor is compromised.

Importantly, MFA must be seamlessly integrated into the user journey to reduce fatigue and friction. Hayes et al. (2023) emphasized the delicate balance between psychological stress and system compliance, noting that overly burdensome authentication processes can lead to avoidance behaviors or workarounds (Hayes et al., 2023). Therefore, advanced MFA systems in Zero Trust architectures increasingly rely on adaptive authentication, which dynamically adjusts the required factors based on contextual risk. For example, if a user logs in from a recognized device and location, fewer steps may be required; conversely, login attempts from new or high-risk environments may trigger stricter authentication protocols.

A third foundational component of Zero Trust architecture is network segmentation and the creation of micro-perimeters. Traditional networks operate under the assumption that once access is granted, lateral movement within the network is unrestricted. Zero Trust rejects this premise by segmenting the network into granular zones—each with its own access policies and enforcement mechanisms. This approach, often referred to as micro-segmentation, limits attackers' ability to move laterally and access high-value assets if they do manage to breach one segment. Kechter et al. (2021) illustrated that structured segmentation in user environments reduces the opportunity for escalation of negative behaviors over time, a principle that translates effectively into digital security as well (Kechter et al., 2021). Through enforced isolation of applications, data, and user groups, micro-perimeters strengthen containment and reduce the blast radius of any security breach.

Micro-segmentation also plays a psychological role in reinforcing policy adherence. Shorey et al. (2017) reported that individuals with low distress tolerance are more likely to act on impulses, particularly in poorly monitored environments (Shorey et al., 2017). By creating clearly defined boundaries within the network, Zero Trust architectures reinforce behavioral expectations and provide immediate feedback when boundaries are crossed. These structures serve not only as technical barriers but also as behavioral cues that inform users of permissible zones and restricted access.

Continuous monitoring and analytics form the real-time nervous system of the Zero Trust model. Unlike traditional models that focus on one-time verification at the point of access, Zero Trust requires persistent oversight of user and system behavior throughout the session. Every action—such as file access, data movement, application usage, and login location—is monitored and evaluated for anomalies. Behavioral analytics tools collect and process this telemetry data to generate baseline user profiles and detect deviations that may indicate insider threats or compromised accounts. According to Felton et al. (2019), such deviations often emerge when users experience shifts in distress tolerance or impulse control, making continuous monitoring a critical defense mechanism (Felton et al., 2019).

Machine learning algorithms are increasingly employed in this space to detect subtle behavioral changes that may not trigger traditional alerts. As Ghanbari et al. (2020) noted in the context of therapy for substance abusers, adaptive feedback and continuous assessment yielded better behavioral outcomes than static interventions (Ghanbari et al., 2020). In cybersecurity, this translates into a need for systems that learn from and respond to user behavior over time, adjusting security postures dynamically based on real-time risk assessments. O'Loughlin et al. (2023) demonstrated how peer perceptions and psychological distress can alter user behavior and influence system interactions, underscoring the value of contextual monitoring in preventing both deliberate and accidental breaches (O'Loughlin et al., 2023).

Tying these components together is the policy enforcement engine, supported by orchestration layers that automate decision-making and response. The policy engine determines whether a given access request should be allowed based on predefined policies, contextual data, and real-time analytics. These policies can be as simple as "deny access from unrecognized devices" or as complex as "allow access to sensitive data only if the user is on a managed device, within a known network, during business hours, and exhibits no anomalous behavior." These policies are dynamically evaluated and enforced at every access point, ensuring consistent application of Zero Trust principles.

Chaleshtori et al. (2022) highlighted the necessity of rule-based systems in high-risk contexts, noting that structured environments improved self-regulation and reduced sensation-seeking behaviors in adolescents exposed to addiction (Chaleshtori et al., 2022). Similarly, in cybersecurity, clear and consistently enforced rules help users internalize expectations and reduce unintentional violations. Ali et al. (2017) emphasized that readiness and motivation influence compliance with structured systems, reinforcing the need for policy engines that are both flexible and intelligible to users (Ali et al., 2017).

The orchestration layer acts as the execution arm of the policy engine, integrating inputs from IAM, MFA, behavioral analytics, and endpoint detection systems to automate threat responses. For instance, if a user exhibits suspicious behavior—such as attempting to access restricted files or downloading large datasets—access can be immediately revoked, and alerts triggered without human intervention. Such automation is especially valuable in reducing response times and preventing damage in fast-moving attack scenarios. Henschel et al. (2021) found that individuals with alexithymia—difficulty identifying and expressing emotions—were more likely to misuse systems unintentionally, a risk that can be mitigated through automated orchestration that bypasses human decision-making delays (Henschel et al., 2021).

In summary, the architecture of Zero Trust is built on an intricate web of interconnected components that provide defense-in-depth and contextual decision-making across every layer of the organization's digital environment. Identity and Access Management ensures that users are who they claim to be and that their access is appropriately scoped. Multi-Factor Authentication adds robustness to this process by introducing redundant checks. Micro-segmentation constrains access to discrete zones within the network, reducing the spread of attacks. Continuous monitoring and behavioral analytics enable real-time risk detection, while policy engines and orchestration layers automate enforcement and response. Together, these components form a dynamic, intelligent, and resilient architecture capable of responding to the complexities of modern cyber threats. By embedding both technical and behavioral insights into its design, Zero Trust offers a future-oriented model for secure and adaptive organizational environments.

5. Applications in Organizational Contexts

The practical application of the Zero Trust security model has rapidly expanded across various organizational settings, including government agencies, large enterprises, and small-to-medium businesses (SMBs). As cyber threats evolve in both scale and sophistication, the Zero Trust model has gained traction due to its capacity to mitigate identity-based attacks, prevent lateral movement within networks, and enforce granular access policies. This architectural shift has

become increasingly critical in modern digital environments where organizations are no longer confined to physical offices or traditional infrastructure but operate across cloud platforms, mobile endpoints, and remote workforces.

In the public sector, government agencies have become prominent adopters of Zero Trust frameworks due to heightened concerns around data sovereignty, espionage, and supply chain vulnerabilities. The U.S. federal government, for instance, has mandated agencies to adopt Zero Trust principles in alignment with the NIST SP 800-207 framework. These implementations are motivated not only by rising attack volumes but also by the demand for continuous compliance and real-time visibility into access requests. In high-stakes environments where missteps can lead to national security breaches, Zero Trust's foundational premise—"never trust, always verify"—offers a clear strategic advantage. Kline et al. (2021) observed that individuals in roles involving high stress and decision-making complexity, such as public safety or defense, are more prone to judgment errors under emotional strain, underscoring the value of automated, policy-driven access decisions that eliminate reliance on human discretion (Kline et al., 2021).

Large enterprises, especially those operating in finance, healthcare, and technology, have also moved swiftly to implement Zero Trust architectures. These sectors are frequent targets of cyberattacks due to their high-value data assets and complex interconnectivity. For example, Google's BeyondCorp initiative is among the most cited case studies in the Zero Trust domain. BeyondCorp reimagines enterprise security by enabling employees to work securely from any location without the need for traditional VPNs. Instead, user and device-based trust evaluations are conducted in real time, with access granted dynamically. This initiative has become a model for how Zero Trust can be deployed at scale, decoupling trust from network location and instead anchoring it in identity, device posture, and behavioral context. Reese et al. (2019) emphasized that trust should be viewed as an adaptive trajectory shaped by real-time data rather than a static state, a principle that underpins BeyondCorp's continuous access evaluation (Reese et al., 2019).

Similarly, in the healthcare sector, organizations have adopted Zero Trust to secure sensitive electronic health records (EHRs), comply with HIPAA requirements, and support telemedicine platforms. The complexity of healthcare systems, often characterized by legacy technologies and fragmented infrastructures, makes them particularly vulnerable to insider threats and credential abuse. Hayes et al. (2023) noted that in emotionally demanding environments such as caregiving, stress and cognitive load significantly impact decision-making and system compliance, suggesting the importance of frictionless but robust authentication mechanisms (Hayes et al., 2023). By integrating Multi-Factor Authentication (MFA) and contextual access controls, healthcare institutions can protect against unauthorized data exposure while minimizing disruption to clinical workflows.

Small and medium-sized businesses (SMBs) are also recognizing the benefits of Zero Trust, albeit with different implementation strategies compared to larger organizations. Due to limited resources, SMBs are particularly susceptible to ransomware and phishing attacks. However, Zero Trust principles can be tailored to fit leaner operational structures by focusing on core components such as MFA, identity governance, and cloud-based policy enforcement. Ghanbari et al. (2020) emphasized the value of structured, phased interventions in resource-constrained environments, a perspective that aligns with the progressive adoption of Zero Trust in SMBs through modular and scalable tools (Ghanbari et al., 2020).

One of the key advantages of Zero Trust is its seamless integration with cloud services and hybrid infrastructures. As organizations migrate workloads to platforms like AWS, Microsoft Azure, and Google Cloud, the traditional perimeter dissolves, making static access controls obsolete. Cloud-native Zero Trust tools allow organizations to enforce granular policies across distributed environments, regardless of where data or applications reside. Anderson et al. (2023) highlighted the importance of maintaining policy consistency across geographic regions and infrastructure layers, especially in multinational organizations where data governance and threat models vary considerably (Anderson et al., 2023). These cloud integrations rely heavily on identity federation, risk-based authentication, and continuous telemetry analysis to ensure access decisions are based on the most current and relevant contextual signals.

In hybrid environments where on-premises and cloud systems coexist, Zero Trust provides a unifying security framework that ensures continuity and visibility. Traditional security approaches often struggle with fragmented control points and inconsistent enforcement. By contrast, Zero Trust architecture centralizes policy management and decentralizes enforcement through software-defined perimeters and API-driven automation. This model supports interoperability and reduces the attack surface, particularly

in environments where legacy applications cannot be easily re-engineered for the cloud. Felton et al. (2019) discussed how contextual awareness and real-time feedback loops help organizations detect shifts in user behavior that might signal compromise, making Zero Trust's continuous monitoring features especially valuable in hybrid ecosystems (Felton et al., 2019).

The surge in remote work and Bring Your Own Device (BYOD) policies since 2020 has further accelerated the adoption of Zero Trust. With employees accessing corporate systems from personal devices, unsecured networks, and diverse locations, traditional network-centric controls have become functionally obsolete. Zero Trust provides a solution by shifting the focus from securing the network to securing the interaction between user, device, and data. Sease et al. (2024) found that individuals with prior trauma or inconsistent behavioral patterns responded more reliably to systems that enforced structured and transparent access policies (Sease et al., 2024). This insight is especially pertinent in remote work settings where informal or unmonitored behavior can compromise security.

In BYOD contexts, the variability in device health and security posture introduces significant risk. Zero Trust mitigates this risk by requiring endpoint compliance checks before access is granted, such as verifying the presence of antivirus software, patch levels, and disk encryption. Devices that fail to meet these standards can be quarantined or given restricted access. Wolitzky-Taylor et al. (2016) suggested that impulsive behaviors, particularly among younger users, often correlate with reduced adherence to security protocols, making proactive enforcement through device-level policies a critical safeguard (Wolitzky-Taylor et al., 2016). By continuously monitoring device behavior and risk posture, organizations can dynamically adjust access privileges in real time.

Moreover, Zero Trust's adaptability to diverse user populations is essential in inclusive workplaces where employees may have varying degrees of technical proficiency or psychological resilience. Chaleshtori et al. (2022) demonstrated that structured systems with transparent rules improved security behavior among adolescents from high-risk environments, implying that similar frameworks can enhance compliance and reduce friction in adult workforces (Chaleshtori et al., 2022). This is particularly relevant in sectors like education and nonprofit organizations, where workforce diversity and limited IT resources demand a flexible but enforceable security strategy.

The psychological dimensions of security behavior in organizational settings also inform Zero Trust application. Baker et al. (2023) found that experiential avoidance and emotional instability were mediating factors in users' ability to engage with security systems responsibly (Baker et al., 2023). This implies that security architectures must not only be technically sound but also psychologically attuned to user variability. Zero Trust addresses this by reducing the cognitive load on users through automation and by minimizing reliance on manual intervention or ad hoc decision-making. By codifying trust decisions into policy engines and automating enforcement, Zero Trust reduces the opportunity for human error and improves compliance.

In conclusion, the deployment of Zero Trust across different organizational contexts reveals its versatility and strategic importance in securing modern digital environments. From federal agencies concerned with national security to small businesses facing resource limitations, the Zero Trust model provides a scalable and adaptive framework that aligns security with user behavior, device health, and contextual risk. Whether through landmark implementations like Google's BeyondCorp, integrations into hybrid cloud infrastructures, or its role in enabling secure remote work, Zero Trust is redefining how trust is managed and operationalized in the cybersecurity domain. Its success hinges not only on technical implementation but also on its capacity to accommodate human behavior, psychological variability, and dynamic work environments, making it a cornerstone of 21st-century organizational security.

6. Benefits and Opportunities

Zero Trust architecture offers organizations a transformative approach to achieving an enhanced security posture by continuously authenticating users and devices before granting access, thereby reducing the potential for credential misuse or lateral attacks. Reese et al. (2019) emphasized that access models based on ongoing behavior assessments can reduce the probability of breaches by identifying anomalies early (Reese et al., 2019). By implementing strict identity verification and micro-segmentation, organizations significantly reduce their attack surface, limiting the impact of breaches and containing threats before they propagate. Kechter et al. (2021) showed that compartmentalizing exposure to risky behavior reduced escalation patterns, echoing Zero Trust's principle of least privilege and segmentation (Kechter et al., 2021).

Additionally, Zero Trust supports improved compliance and governance through transparent policy enforcement and detailed audit trails. Hayes et al. (2023) demonstrated how systems that enforce clearly defined behavioral and access boundaries promote greater adherence to rules and reduce ambiguity in user interaction (Hayes et al., 2023). Another key advantage is the model's adaptability to modern work environments, including remote work and BYOD scenarios. Sease et al. (2024) reported that structured and dynamically enforced policies lead to more consistent engagement, even in high-risk user populations (Sease et al., 2024). As organizations navigate increasingly distributed and hybrid infrastructures, Zero Trust provides a scalable and context-aware security framework that meets the demands of flexibility without compromising control.

7. Challenges and Barriers

Despite its benefits, the implementation of Zero Trust presents several challenges. One of the most significant is the technical complexity involved in overhauling existing infrastructures, especially in legacy-heavy environments. Felton et al. (2019) noted that systems burdened with outdated architectures often lack the agility required for real-time behavior tracking and policy enforcement (Felton et al., 2019). The financial and resource commitments required for deploying Zero Trust can also be substantial, particularly for SMBs. Ghanbari et al. (2020) discussed how resource-constrained systems require phased adoption and simplified models, reflecting similar trade-offs in Zero Trust implementations (Ghanbari et al., 2020). Another barrier is user experience and resistance; overly rigid or complex authentication processes can lead to avoidance behavior. Veilleux (2022) showed that distress intolerance could result in security non-compliance when users feel overwhelmed by procedural friction (Veilleux, 2022). Lastly, the skills gap poses a serious obstacle, as organizations often lack personnel trained in Zero Trust principles and technologies. Anderson et al. (2023) emphasized that behavioral readiness and technical literacy affect how well users adapt to new access frameworks, highlighting the need for comprehensive training and cultural alignment (Anderson et al., 2023).

8. Discussion and Conclusion

The Zero Trust security model has emerged as a critical paradigm shift in how organizations conceptualize and enforce digital security in an increasingly complex and interconnected environment. Unlike traditional perimeter-based models that rely on implicit trust within internal networks, Zero Trust operates on the foundational principle that no entity—whether inside or outside the network—should be trusted by default. Every user, device, and application must undergo continuous verification before being granted access to any resource. This approach represents a comprehensive transformation in security strategy, responding to the evolving nature of threats, technological infrastructures, and user behaviors.

The necessity of adopting a Zero Trust approach has become more evident as organizations grapple with sophisticated cyber threats that exploit the limitations of legacy systems. The rise of cloud computing, remote work, mobile access, and bring-your-own-device (BYOD) policies has dissolved the traditional network perimeter. This evolution demands a security architecture capable of enforcing granular access controls, monitoring behavior in real time, and responding adaptively to anomalies. Zero Trust meets these demands through a tightly integrated set of technologies and processes, including Identity and Access Management (IAM), Multi-Factor Authentication (MFA), micro-segmentation, continuous monitoring, and dynamic policy enforcement.

In practice, Zero Trust enables organizations to reduce their attack surface by ensuring that access to critical resources is strictly limited based on contextual risk assessments. By adhering to the principle of least privilege and segmenting network assets, even a successful breach in one area does not automatically grant attackers access to the broader environment. Continuous behavioral analytics allow for real-time detection of deviations from normal usage patterns, adding another layer of defense that is both proactive and intelligent. These capabilities not only improve an organization's resilience to attacks but also support compliance with regulatory standards by offering clear audit trails and enforceable security policies.

The flexibility of the Zero Trust model makes it highly applicable across a wide range of organizational contexts. In government sectors, Zero Trust supports the safeguarding of sensitive national data and reinforces operational continuity in the face of increasingly state-sponsored cyber threats. In enterprise settings, particularly in industries such as finance, healthcare, and technology, Zero Trust offers a way to secure high-value data while maintaining the agility required for innovation and remote collaboration. Small and medium-sized businesses, though often constrained by limited resources, also stand to benefit from adopting Zero Trust

principles incrementally through cloud-based services and modular solutions that prioritize core security functions.

However, the transition to Zero Trust is not without its challenges. The architectural and operational overhaul required for full implementation can be daunting, particularly for organizations reliant on legacy systems or lacking cybersecurity maturity. The cost of deploying and integrating Zero Trust technologies—alongside the demand for skilled personnel—presents both financial and human resource hurdles. Additionally, the emphasis on continuous verification and strict access control, if not properly managed, can introduce user experience issues that lead to friction, resistance, or workarounds that inadvertently compromise security.

To overcome these barriers, organizations must adopt a phased and strategic approach to Zero Trust. This involves aligning the implementation with business goals, prioritizing critical assets and workflows, and investing in user education and change management. Building a culture of security that recognizes the shared responsibility of all stakeholders—from IT teams to end users—is essential. Zero Trust should not be viewed merely as a technical deployment but as an organizational philosophy that redefines how trust is established, maintained, and monitored across digital ecosystems.

Looking ahead, the evolution of Zero Trust will be shaped by advancements in artificial intelligence, machine learning, and automation, all of which enhance its ability to make real-time, risk-informed decisions. As the digital landscape continues to evolve, so too will the threats that organizations face. Zero Trust offers a future-proof security architecture designed not only to defend against current threats but to adapt to those yet to emerge.

In conclusion, the Zero Trust model represents a fundamental rethinking of digital security, emphasizing dynamic validation over static trust, behavioral intelligence over perimeter control, and resilience over convenience. Its holistic, adaptive, and user-aware framework positions it as a cornerstone of organizational security in the modern era. While challenges to implementation exist, the long-term benefits in terms of reduced risk, increased compliance, and improved operational confidence make Zero Trust not only a strategic imperative but a necessary evolution in cybersecurity management.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethics Considerations

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were considered.

References

Ali, B., Green, K. M., Daughters, S. B., & Lejuez, C. W. (2017). Distress Tolerance Interacts With Circumstances, Motivation, and Readiness to Predict Substance Abuse Treatment Retention. *Addictive behaviors*, *73*, 99-104. https://doi.org/10.1016/j.addbeh.2017.04.016

Anderson, G. N., Conway, C., & Bravo, A. J. (2023). Distress Tolerance Predicts Substance Use Motivations and Problems in Young Adults Across Four Continents. https://doi.org/10.31234/osf.io/dq8u3

Anderson, G. N., Conway, C., & Bravo, A. J. (2024). Distress Tolerance Is Linked With Substance Use Motivations and Problems in Young Adults Across Four Continents. *Journal of personality*, *93*(3), 706-723. https://doi.org/10.1111/jopy.12963

Baker, S. N., Burr, E. K., Leon, A. N. D., Leary, A. V., Rozek, D. C., & Dvorak, R. D. (2023). The Mediating Roles of Affect Lability and Experiential Avoidance Between Distress Tolerance and Suicidal Ideation Among College Students. *Psychological Reports*. https://doi.org/10.1177/00332941231216671

Batchelder, A., Ehlinger, P. P., Boroughs, M., Shipherd, J. C., Safren, S. A., Ironson, G., & O'Cleirigh, C. (2017). Psychological and Behavioral Moderators of the Relationship Between Trauma Severity and HIV Transmission Risk Behavior Among MSM With a History of Childhood Sexual Abuse. *Journal of Behavioral Medicine*, *40*(5), 794-802. https://doi.org/10.1007/s10865-017-9848-9

Chaleshtori, M. N., Asgari, P., Heidari, A., Bozorgi, Z. D., & Hafezi, F. (2022). Effectiveness of Mindfulness-Based Stress Reduction Intervention in Distress Tolerance and Sensation-Seeking in Adolescents With a Drug-Addicted Parent. *Journal of Research and Health*, *12*(5), 355-362. https://doi.org/10.32598/jrh.12.5.1889.2

Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. (2024). A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. *Sensors*, *24*(4), 1328. https://doi.org/10.3390/s24041328

Felton, J. W., Strutz, K. L., McCauley, H. L., Poland, C., Barnhart, K., & Lejuez, C. W. (2019). Delay Discounting Interacts With Distress Tolerance to Predict Depression and Alcohol Use Disorders Among Individuals Receiving Inpatient Substance Use Services. *International journal of mental health and addiction*, *18*(5), 1416-1421. https://doi.org/10.1007/s11469-019-00163-5

Ghanbari, H., Toozandehjani, H., & Nejat, H. (2020). Comparison of the Effectiveness of Acceptance and Commitment Therapy and Quality of Life Improvement Training on Distress Tolerance and Self-Destructive Behaviors in Substance Abusers. *International Journal of Basic Science in Medicine*, *5*(1), 28-32. https://doi.org/10.34172/ijbsm.2020.07

Hayes, A., Dempsey, M., Kells, M., & Murphy, M. (2023). The Relationship Between Social Support, Coping Strategies and Psychological Distress and Positive Mental Well-Being in Carers of People With Borderline Personality Disorder. *Borderline personality disorder and emotion dysregulation*, *10*(1). https://doi.org/10.1186/s40479-023-00237-w

Henschel, A. V., Flanagan, J. C., Augur, I. F., Jeffirs, S. M., & Back, S. E. (2021). Motives for Prescription Opioid Use: The Role of Alexithymia and Distress Tolerance. *American Journal on Addictions*, *31*(1), 55-60. https://doi.org/10.1111/ajad.13230

Huber, B., & Kandah, F. (2024). Zero Trust+: A Trusted-Based Zero Trust Architecture for IoT at Scale. 1-6. https://doi.org/10.1109/icce59016.2024.10444321

Jensen, C. D. (2024). Why Zero Trust Architectures Are Not Replacing Trust. 121-135. https://doi.org/10.1007/978-3-031-76714-2_8

Kechter, A., Barrington-Trimis, J. L., Cho, J., Davis, J. P., Huh, J., Black, D. S., & Leventhal, A. M. (2021). Distress Tolerance and Subsequent Substance Use Throughout High School. *Addictive behaviors*, *120*, 106983. https://doi.org/10.1016/j.addbeh.2021.106983

Kline, N. K., Cabrera, K. B., & Reed, K. M. P. (2021). Predicting Different Types of Intimate Partner Aggression Perpetration: The Roles of Problem Alcohol Use and Distress Tolerance. *Journal of interpersonal violence*, *37*(13-14), NP10962-NP10984. https://doi.org/10.1177/0886260521990830

Langdon, K. J., Ramsey, S. E., Scherzer, C. R., Carey, K. B., Ranney, M. L., & Rich, J. D. (2020). Development of an Integrated Digital Health Intervention to Promote Engagement in and Adherence to Medication for Opioid Use Disorder. *Addiction Science & Clinical Practice*, *15*(1). https://doi.org/10.1186/s13722-020-00189-4

Molleti, R., & Khanna, A. (2025). End to End Well Architected Zero Trust Architecture in Fintech Cloud Environments. *International Scientific Journal of Engineering and Management*, *04*(01), 1-7. https://doi.org/10.55041/isjem00106

O'Loughlin, C. M., Park, Y., & Ammerman, B. A. (2023). Suicide Ideation, Distress, and Peer Perceptions as Predictors of Substance Use. *Substance Use & Misuse*, *58*(4), 560-569. https://doi.org/10.1080/10826084.2023.2177964

Reese, E. D., Conway, C., Anand, D., Bauer, D. J., & Daughters, S. B. (2019). Distress Tolerance Trajectories Following Substance Use Treatment. *Journal of consulting and clinical psychology*, *87*(7), 645-656. https://doi.org/10.1037/ccp0000403

Sease, T. B., Wiese, A. L., & Knight, K. (2024). A Latent Profile Analysis of Substance Use and Post-Traumatic Stress on Substance Use Treatment Outcomes Among People Involved With the Justice System. *Journal of Drug Issues*. https://doi.org/10.1177/00220426241248361

Shorey, R. C., Gawrysiak, M. J., Elmquist, J., Brem, M. J., Anderson, S., & Stuart, G. L. (2017). Experiential Avoidance, Distress Tolerance, and Substance Use Cravings Among Adults in Residential Treatment for Substance Use Disorders. *Journal of Addictive Diseases*, *36*(3), 151-157. https://doi.org/10.1080/10550887.2017.1302661

Süzen, A. A., & Ceylan, O. (2024). The Advantages and Implementation Challenges Within the Scope of the Basic Principles of Transition to Zero Trust Architecture. *International Journal of 3d Printing Technologies and Digital Industry*, *8*(3), 416-427. https://doi.org/10.46519/ij3dptdi.1556319

Veilleux, J. C. (2022). A Theory of Momentary Distress Tolerance: Toward Understanding Contextually Situated Choices to Engage With or Avoid Distress. *Clinical Psychological Science*, *11*(2), 357-380. https://doi.org/10.1177/21677026221118327

Wolitzky-Taylor, K., McBeth, J., Guillot, C. R., Stone, M. D., Kirkpatrick, M. G., Zvolensky, M. J., Buckner, J. D., & Leventhal, A. M. (2016). Transdiagnostic Processes Linking Anxiety Symptoms and Substance Use Problems Among Adolescents. *Journal of Addictive Diseases*, *35*(4), 266-277. https://doi.org/10.1080/10550887.2016.1207969

Yıldız, E., & Büyükfırat, E. (2024). Psychological Flexibility in Individuals With Substance Use Disorder: The Mediating Effect of Distress Tolerance and Stress. *Journal of Psychiatric and Mental Health Nursing*, *32*(3), 610-622. https://doi.org/10.1111/jpm.13140

Zapolski, T. C. B., Rowe, A. T., Banks, D. E., & Faidley, M. T. (2018). Perceived Discrimination and Substance Use Among Adolescents: Examining the Moderating Effect of Distress Tolerance and Negative Urgency. *Substance Use & Misuse*, *54*(1), 156-165. https://doi.org/10.1080/10826084.2018.1512625