Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH
AND DEVELOPMENT

| RESEARCH ARTICLE

Demystifying Zero Trust Security: The No-Trust Network Paradigm

Vaibhav Anil Vora
Amazon Web Services, USA
Corresponding Author: Vaibhav Anil Vora, **E-mail**: voravaibhavanil@gmail.com

| ABSTRACT

Zero trust security represents a paradigm shift in cybersecurity architecture that challenges traditional perimeter-based defense models by eliminating implicit trust and requiring continuous verification for all network interactions. As organizations navigate increasingly complex digital ecosystems characterized by cloud computing, mobile workforces, and interconnected supply chains, conventional security boundaries have dissolved, necessitating a more dynamic approach to protection. This architectural framework implements fundamental principles, including least privilege access, micro-segmentation, continuous monitoring, and data-centric security to establish comprehensive protection across distributed environments. The evolution of zero trust incorporates advanced technologies such as artificial intelligence, machine learning, and cloud-native security controls to enhance detection capabilities and adaptive response mechanisms. Through structured implementation strategies that prioritize assessment, phased deployment, and thoughtful integration with existing infrastructure, organizations can transform security postures to align with contemporary threat landscapes while maintaining operational efficiency.

| KEYWORDS

Continuous Verification, Micro-segmentation, Least Privilege Access, Data-centric Security, Adaptive Authentication

| ARTICLE INFORMATION

ACCEPTED: 12 April 2025 **PUBLISHED:** 01 May 2025 **DOI:** 10.32996/jcsts.2025.7.3.15

I. Introduction

The cybersecurity landscape has experienced a fundamental shift as organizations increasingly move beyond traditional perimeter-based security architectures. Conventional network security models operated on the assumption that external networks were untrusted while internal networks could be considered secure—a paradigm that created clearly defined boundaries between protected and unprotected zones [1]. This approach, which dominated network security thinking for decades, established a security perimeter that functioned as the primary defensive barrier, with resources inside this boundary enjoying a presumed level of trust and protection. However, as digital transformation initiatives have accelerated, this model has revealed significant limitations in addressing contemporary security challenges [2].

Zero trust security represents a comprehensive architectural approach that eliminates the concept of trusted networks, devices, or users based solely on location or network positioning. Instead, zero trust implements continuous verification processes that authenticate and authorize every access attempt before granting resource permissions [1]. This security framework operates on the fundamental principle that organizations should "never trust, always verify"—treating each network request as potentially hostile regardless of its origin. The architecture requires robust identity verification mechanisms for all entities attempting to access resources, strict enforcement of least privilege access controls, and comprehensive monitoring capabilities that examine all network traffic [2]. Zero trust recognizes that threats may originate from both external and internal sources, necessitating verification processes that apply uniformly across the entire digital environment [1].

The significance of adopting zero trust principles has grown considerably as organizations navigate increasingly complex digital ecosystems. The rise of cloud computing, mobile workforces, remote access requirements, and interconnected supply chains has effectively dissolved traditional network boundaries, creating distributed environments where perimeter-focused security measures provide inadequate protection [1]. These evolving operational models have dramatically expanded attack surfaces, introducing new vulnerabilities that sophisticated threat actors can exploit to gain unauthorized access to sensitive resources [2]. As organizational data and applications have become distributed across multiple environments—including on-premises data centers, public cloud platforms, and edge computing locations—security architectures must evolve to provide consistent protection regardless of resource location or access point [1].

Zero trust architecture represents a transformative approach to network security that aligns protection strategies with the realities of modern computing environments. By implementing microsegmentation techniques, organizations can establish granular containment boundaries around critical assets, limiting lateral movement opportunities for potential attackers [1]. Continuous monitoring and verification processes enable more dynamic security responses that can adapt to changing circumstances and emerging threats [2]. Through these and other zero trust principles, organizations can establish more resilient security frameworks capable of protecting distributed resources while supporting business innovation. The architectural approach focuses on securing critical data and applications through consistent policies applied across hybrid environments, enabling organizations to maintain security effectiveness even as technology landscapes continue to evolve [1].

2. Theoretical Foundations of Zero Trust Architecture

The historical development of zero trust architecture can be traced to the recognition that traditional perimeter-based security models were becoming increasingly ineffective in the face of evolving threat landscapes. The concept emerged as security professionals observed that conventional approaches created an implicit trust zone once users or systems were authenticated at the perimeter, allowing potential adversaries who breached external defenses to move laterally throughout networks with minimal resistance [3]. This conceptual shift gained momentum as organizations began experiencing sophisticated attacks that bypassed perimeter controls yet remained undetected within internal networks for extended periods. The zero trust model was developed as a response to these challenges, proposing that organizations should verify anything and everything attempting to connect to systems before granting access. This approach acknowledges that threats can originate from both outside and inside traditional network boundaries, requiring security controls that do not rely on location as a primary trust factor [4].

The core security principles underlying zero trust architecture establish a framework fundamentally different from conventional security approaches. The primary principle maintains that all network traffic must be authenticated and authorized, regardless of origin or destination. Zero trust architecture implements strict verification processes for every access request, ensuring that identity becomes the new network perimeter rather than physical or network boundaries [3]. The architecture enforces micro-segmentation strategies that divide networks into isolated zones, limiting the potential blast radius of security incidents by restricting lateral movement opportunities. Dynamic policy enforcement represents another critical principle, enabling the continuous evaluation of risk factors during sessions rather than relying solely on point-in-time authentication events. Additionally, zero trust emphasizes comprehensive monitoring and logging capabilities that provide visibility into all network activities, establishing a foundation for threat detection and incident response [4].

Traditional security models operate on fundamentally different assumptions when compared to zero-trust architecture. Conventional approaches focus on establishing strong perimeter defenses while maintaining relatively open internal networks, creating distinct trusted and untrusted zones separated by security controls like firewalls and intrusion prevention systems [3]. This model typically grants excessive privileges to users once they authenticate at the perimeter, enabling broad network access that can be exploited by attackers who successfully breach external defenses. Traditional architectures often implement security controls inconsistently across environments, creating protection gaps as resources migrate between on-premises and cloud platforms. In contrast, zero trust assumes breach as a default position, implementing consistent verification processes for all access requests regardless of source or network location. This approach establishes a security model that can adapt to modern distributed environments by focusing on protecting resources rather than network segments [4].

The implementation of zero trust architecture requires several interconnected components working in concert to create a cohesive security ecosystem. Strong identity verification mechanisms serve as the foundation of this architecture, providing the authentication capabilities necessary to verify user and device identities before access decisions [3]. Micro-segmentation technologies enable organizations to establish granular network divisions that contain sensitive resources within protected zones, limiting the potential impact of security incidents. Security information and event management systems provide the visibility needed to monitor activity across environments, detecting potential threats through behavioral analysis and anomaly detection. Policy enforcement points serve as the control mechanisms that evaluate access requests against established security policies, making authorization decisions based on identity, device status, request context, and other relevant factors. These components must operate together seamlessly, creating a unified architecture that implements consistent security controls across distributed environments while maintaining operational efficiency [4].

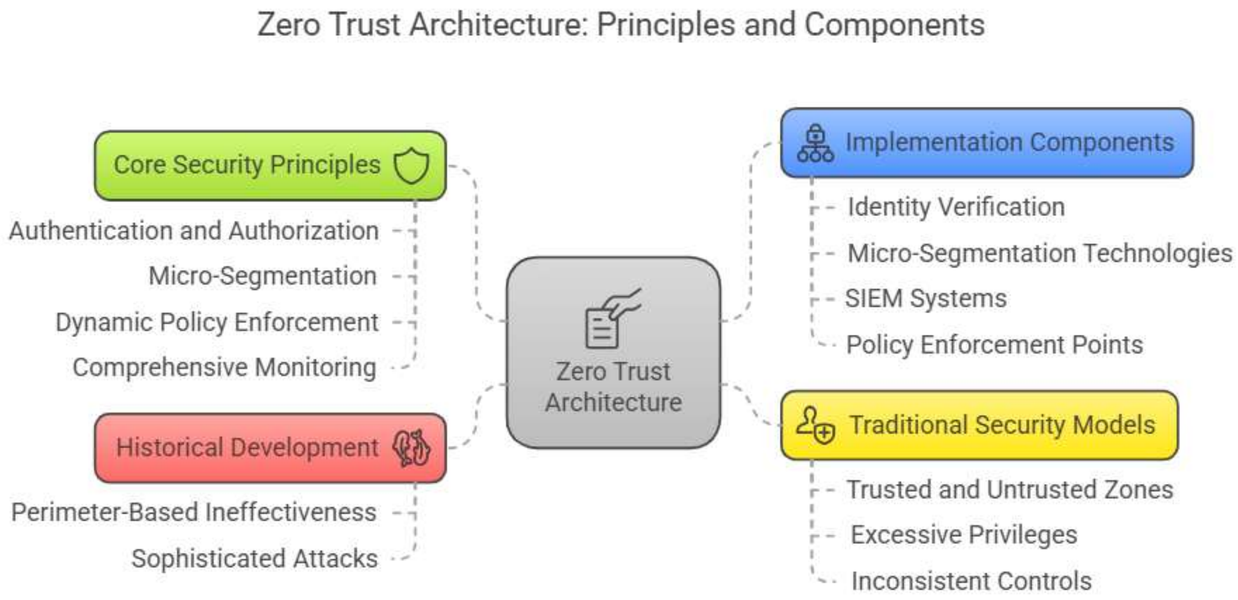
Zero Trust Architecture: Principles and Components
Core Security Principles
Authentication and Authorization
Micro-Segmentation
Dynamic Policy Enforcement
Comprehensive Monitoring
Historical Development
Perimeter-Based Ineffectiveness
Sophisticated Attacks
Zero Trust Architecture
Implementation Components
Identity Verification
Micro-Segmentation Technologies
SIEM Systems
Policy Enforcement Points
Traditional Security Models
Trusted and Untrusted Zones
Excessive Privileges
Inconsistent Controls

Fig 1: Zero Trust Architecture: Principles and Components [3, 4]

3. Essential Components of Zero Trust Implementation

Least privilege access control frameworks establish a critical foundation for zero trust security by ensuring that users, systems, and applications receive only the minimum permissions necessary to perform legitimate functions. This principle directly challenges traditional security models that often grant excessive access rights based on role or network location rather than actual operational need. Effective implementation requires mature identity governance programs capable of continuously evaluating access requirements and revoking unnecessary privileges. According to the zero trust maturity model developed by governmental security agencies, organizations should implement attribute-based access control systems that dynamically assess multiple contextual factors during authorization decisions [5]. These systems consider variables including user identity, device health, resource sensitivity, authentication strength, and behavioral patterns before granting access to protected resources. The most mature implementations incorporate just-in-time and just-enough access protocols, providing temporary elevated privileges for specific administrative tasks rather than maintaining persistent administrative access. Organizations implementing comprehensive least privilege frameworks must establish automated provisioning and de-provisioning processes to manage access throughout the entire user lifecycle, revoking permissions immediately when roles change or employment ends. This approach significantly reduces the attack surface available to potential adversaries, limiting lateral movement opportunities even when initial network access has been achieved [6].

Micro-segmentation strategies enable organizations to implement granular security boundaries around protected resources, replacing broad network segments with precisely defined security zones. This approach acknowledges that traditional network divisions often create excessively large trust zones that permit substantial lateral movement once perimeter defenses are breached. According to established maturity models, advanced zero trust implementations require network environments capable of dynamically creating and enforcing security boundaries that protect individual workloads rather than entire subnets [5]. Software-defined networking technologies facilitate this granularity by separating security policy definition from underlying infrastructure, enabling consistent control enforcement across diverse environments, including on-premises data centers and cloud platforms. Organizations advancing along the zero trust maturity spectrum increasingly implement application-layer segmentation that restricts communications based on software identity rather than network addressing, providing protection that remains consistent despite infrastructure changes. The most sophisticated implementations incorporate workload isolation techniques that establish security boundaries at the container or process level, minimizing the potential blast radius from security incidents. This granular protection requiresa comprehensive understanding of application dependencies and communication patterns, necessitating advanced discovery tools that map legitimate workflow requirements and identify potential security exceptions [6].

Continuous monitoring and adaptive authentication mechanisms provide the visibility and dynamic response capabilities essential for maintaining security in zero-trust environments. Unlike traditional security models that authenticate users primarily at session establishment, zero trust requires ongoing verification throughout resource interactions to detect changing risk conditions. Mature implementations develop comprehensive monitoring architectures that collect and analyze telemetry data across endpoints, networks, applications, and identity systems [5]. These monitoring capabilities establish baseline behavioral patterns for users and entities, enabling the detection of anomalous activities that may indicate compromise or credential theft. Advanced implementations incorporate real-time risk assessment engines that evaluate multiple signals during access requests, adjusting authentication requirements based on detected risk factors. When suspicious conditions are identified, adaptive authentication systems may require additional verification through supplemental authentication factors, reputation checks, or behavioral analysis. Mature zero trust implementations integrate monitoring data with automated response capabilities that can modify access permissions, initiate session termination, or implement additional controls when potential threats are detected. This continuous evaluation approach replaces point-in-time access decisions with dynamic security that adapts to changing conditions throughout user sessions [6].

Data-centric security approaches focus protection efforts directly on sensitive information rather than the infrastructure processing or storing that data. This perspective recognizes that traditional security models often emphasize network and system protection while leaving data insufficiently secured as it moves between environments. According to established maturity frameworks, advanced zero trust implementations require comprehensive data security programs that discover, classify, and protect sensitive information across distributed environments [5]. These programs implement data discovery tools that identify regulated and sensitive information across storage repositories, enabling security teams to apply appropriate controls based on data classification. Encryption represents a foundational protection mechanism within data-centric security, ensuring that information remains protected even when underlying systems are compromised. The most mature implementations apply encryption consistently across environments, protecting data during storage, transmission, and processing phases. Data access governance systems monitor and control information usage, ensuring that appropriate authorization decisions consider data sensitivity alongside user identity and access context. Advanced implementations incorporate technologies that maintain protection as data moves outside organizational boundaries, including digital rights management solutions that enforce usage policies regardless of file location. By focusing security efforts directly on protecting information assets, data-centric approaches maintain consistent protection across increasingly distributed and hybrid environments [6].

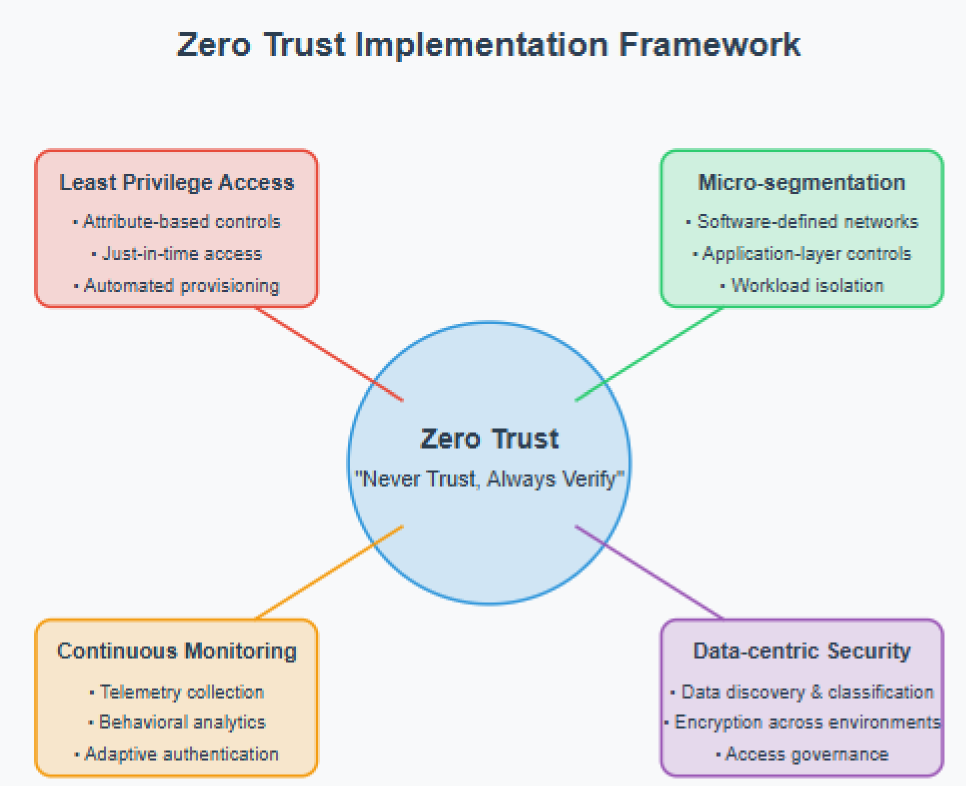
Zero Trust Implementation Framework
Least Privilege Access
• Attribute-based controls
• Just-in-time access
• Automated provisioning
Micro-segmentation
• Software-defined networks
• Application-layer controls
• Workload isolation
Zero Trust
"Never Trust, Always Verify"
Continuous Monitoring
• Telemetry collection
• Behavioral analytics
• Adaptive authentication
Data-centric Security
• Data discovery & classification
• Encryption across environments
• Access governance

Fig 2: Zero Implementation Framework [5, 6]

4. Practical Implementation Strategies

Assessment and planning methodologies establish the foundation for successful zero trust implementation by documenting current architectures and defining strategic migration paths. Effective assessment approaches begin with comprehensive resource documentation that identifies critical assets, data flows, and existing security controls across environments. This process should include a thorough examination of subjects (users, service accounts, and automated processes), enterprise assets (devices, systems, and applications), and resources (data, services, and workflows) that require protection under the zero trust model [7]. Organizations must develop a detailed understanding of legitimate communication patterns between components, establishing baseline behavioral expectations that can inform subsequent security policy development. The assessment phase should evaluate current policy enforcement mechanisms, identifying existing components that can support zero trust principles while highlighting capability gaps requiring remediation. This evaluation extends beyond technical architecture to include organizational processes, governance structures, and operational procedures that influence security implementation. The planning methodology transitions from current state assessment to target architecture definition, establishing a conceptual framework that aligns zero trust implementation with organizational security requirements. Mature planning approaches incorporate policy formulation processes that define baseline security expectations across environments, creating consistent security standards that can be applied through technical controls [8].

Phased implementation approaches enable organizations to transition methodically from traditional security architectures to comprehensive zero-trust deployments. Effective implementation strategies typically begin by establishing candidate deployment scenarios that reflect organizational priorities, focusing initial efforts on high-value or high-risk environments that will deliver substantial security benefits [7]. Many organizations implement initial zero trust capabilities for specific high-risk applications or user populations, creating controlled environments where security teams can validate architectural approaches and operational procedures before broader deployment. Early implementation phases often emphasize identity and access management enhancements, establishing the strong authentication capabilities necessary for subsequent zero-trust controls. Network architecture transformations typically progress from traditional segmentation to increasingly granular micro-segmentation as organizations develop a deeper understanding of legitimate communication requirements. Resource protection mechanisms evolve throughout implementation phases, with initial controls focused on sensitive data repositories before expanding to broader resource categories. Organizations should establish explicit success criteria for each implementation phase, enabling objective evaluation of deployment effectiveness and identification of potential improvement opportunities. The phased approach creates progressive security enhancement while allowing operational processes and support structures to mature alongside technical capabilities [8].

Integration with existing infrastructure presents significant challenges during zero trust implementations, requiring adaptation strategies that enhance security without disrupting critical operations. Organizations must evaluate how legacy systems interact with zero trust components, identifying potential compatibility limitations that may necessitate architectural accommodations [7]. Integration approaches often incorporate gateway technologies that mediate interactions between modern zero-trust environments and legacy systems that cannot directly support advanced authentication mechanisms. Proxy architectures provide alternative integration options, enabling security policy enforcement without requiring modifications to underlying applications or systems. Security monitoring infrastructure typically requires significant enhancement during zero trust implementation, expanding visibility capabilities to support the continuous assessment processes fundamental to the security model. Organizations may implement temporary policy enforcement points during transition phases, gradually replacing traditional security controls with zero-trust mechanisms as implementation progresses. Integration strategies should address operational concerns, including performance impacts, user experience considerations, and potential failure scenarios that might occur during migration periods. Effective implementations acknowledge that certain legacy components may require enclave-based protection approaches when direct zero trust integration proves infeasible, creating isolated environments with strictly controlled access points [8].

Case studies of successful zero trust deployments demonstrate how organizations across various sectors have implemented these security principles despite diverse technical environments and operational requirements. A federal government agency successfully migrated from perimeter-focused security to a zero-trust architecture by implementing candidate scenarios that progressively enhanced protection for sensitive resources [7]. This organization established a dedicated zero-trust planning team that developed detailed migration strategies for each application environment, identifying specific security control requirements and potential integration challenges before implementation. A healthcare organization achieved zero trust implementation while maintaining strict regulatory compliance requirements through a data-centric approach that evaluated resource sensitivity during policy development. This organization implemented enhanced monitoring capabilities across clinical systems, creating the visibility necessary for continuous trust evaluation throughout user sessions. A financial services organization deployed a trust architecture for customer-facing applications by implementing tiered access policies that scale authentication requirements according to resource sensitivity and transaction risk levels. This approach enhanced security while maintaining positive user experiences for routine interactions. A manufacturing organization successfully implemented zero trust principles across operational technology environments by establishing clear security boundaries around control systems and implementing strict access verification for all management interfaces [8]. These implementations demonstrate that successful zero trust deployments require comprehensive planning, appropriate technology selection, and organizational alignment throughout the transformation process.

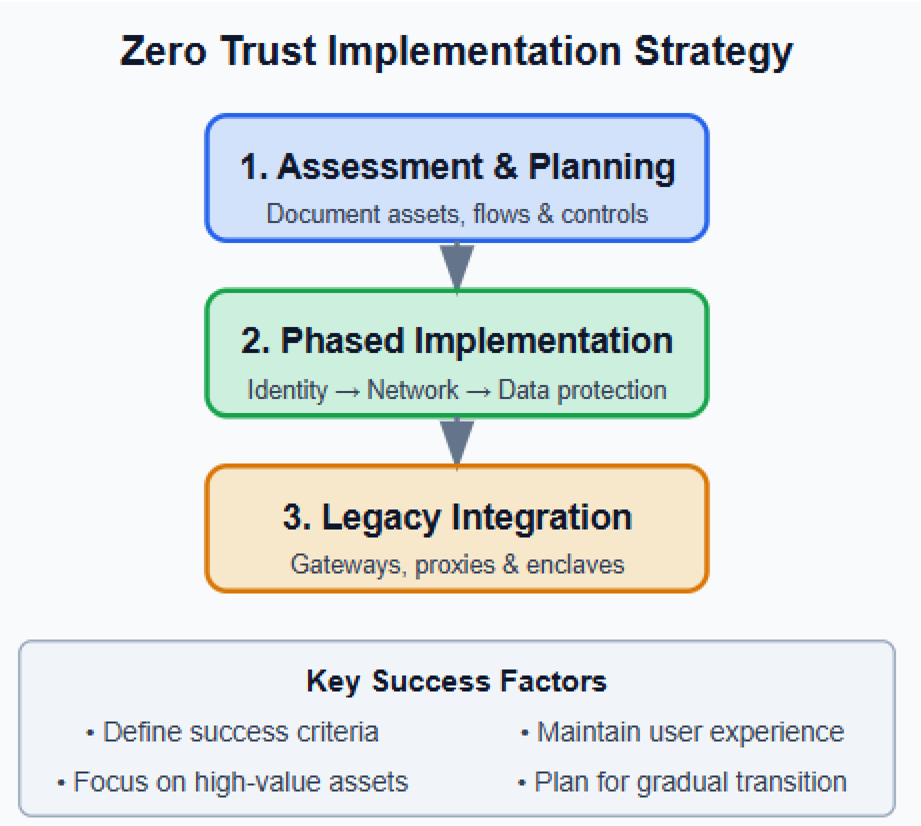
Zero Trust Implementation Strategy
1. Assessment & Planning
Document assets, flows & controls
2. Phased Implementation
Identity → Network → Data protection
3. Legacy Integration
Gateways, proxies & enclaves
Key Success Factors
• Define success criteria
• Maintain user experience
• Focus on high-value assets
• Plan for gradual transition

Fig 3: Zero Trust Implementation Strategy [7, 8]

5. Emerging Trends and Future Directions

Artificial intelligence and machine learning technologies represent transformative capabilities within zero-trust architectures, enabling more sophisticated and adaptive security controls. These technologies enhance zero trust implementations by leveraging pattern recognition and anomaly detection to identify subtle deviations from established behavioral baselines across network environments. Machine learning algorithms analyze historical access patterns and contextual factors—including time, location, device characteristics, and resource sensitivity—to establish dynamic risk scores for authentication and authorization decisions [9]. The integration of these technologies enables more nuanced security responses that adapt to changing threat conditions without requiring manual policy adjustments. Behavioral analytics capabilities monitor user interactions with applications and data, establishing normal usage patterns that serve as comparative baselines for detecting potential credential theft or insider threats. Natural language processing enhances security analytics by extracting actionable intelligence from unstructured data sources, improving threat detection capabilities across diverse information repositories. Advanced implementations increasingly leverage reinforcement learning techniques that optimize security policies based on observed outcomes, creating protection mechanisms that continuously improve through operational experience. These AI-enhanced protection systems significantly reduce analyst workload by automating routine security decisions while escalating unusual activities that require human investigation [10].

Zero trust implementation within cloud-native and multi-cloud environments introduces distinctive security considerations as organizations distribute workloads across diverse infrastructure platforms with varying security capabilities. The ephemeral nature of cloud resources aligns naturally with zero trust principles, requiring security controls that focus on protecting workloads and data rather than static network boundaries [9]. Cloud service providers increasingly incorporate native security capabilities that support zero trust implementation, including identity federation services, microsegmentation technologies, and comprehensive API security controls. Software-defined perimeter technologies create protected access pathways to distributed resources, implementing zero trust principles through encrypted micro-tunnels that authenticate both users and devices before permitting resource access. Container security platforms extend protection to microservice architectures, establishing verification processes for individual application components rather than monolithic systems. Cloud security posture management tools provide visibility across diverse environments, enabling consistent policy enforcement despite infrastructure heterogeneity. Organizations achieving the most mature implementations establish unified security control planes that implement consistent verification processes regardless of resource location, eliminating security disparities between cloud providers [10].

Integration of zero trust principles with DevSecOps practices enables organizations to incorporate security throughout application lifecycles, creating systems with embedded protection mechanisms rather than retrofitted controls. This integration emphasizes proactive security approaches that identify and remediate vulnerabilities during development phases, substantially reducing the costs associated with addressing security issues in production environments [9]. Infrastructure-as-code methodologies enable security teams to define protection mechanisms alongside application components, ensuring consistent control implementation across development, testing, and production environments. Automated security testing tools integrate with continuous integration pipelines, identifying potential vulnerabilities during build processes before deployment. Runtime application self-protection technologies extend security into operational environments, implementing continuous verification principles through controls that authenticate and authorize interactions during execution. API security frameworks establish standardized protection for application communications, implementing consistent verification regardless of deployment environment. Security policy-as-code approaches enable automated compliance validation, ensuring that deployed resources maintain required protection levels throughout operational lifecycles. These integrations transform traditional security models that often created friction within development processes, establishing security as an integral component of application delivery rather than a separate validation function [10].

Standards and frameworks guiding zero trust implementation continue to mature as the model gains broader adoption across industries and regulatory environments. These frameworks establish structured approaches to deployment, creating common reference architectures and capability definitions that facilitate consistent implementation [9]. Industry organizations have developed specialized guidance for specific sectors, including healthcare, finance, and critical infrastructure, addressing unique regulatory requirements and operational constraints. Governmental agencies have published detailed reference architectures that define logical components and integration patterns, providing implementation blueprints for organizations transitioning from traditional security models. Maturity models establish progressive capability levels across multiple security domains—including identity, device, network, application, and data protection—enabling organizations to assess current postures and prioritize enhancement initiatives. Security certification programs increasingly incorporate zero trust principles, acknowledging the effectiveness of continuous verification approaches for protecting sensitive resources across distributed environments. These evolving standards promote implementation consistency while accommodating diverse organizational requirements and technology environments. The standardization of zero trust approaches enables more effective communication between security stakeholders, establishing common terminology and architectural patterns that facilitate collaboration between technology providers, implementation teams, and security governance functions [10].

Technology Component	Primary Function	Business Impact
AI/ML Behavioral Analytics	Anomaly Detection	Reduced Analyst Workload
Cloud Security Posture Management	Multi-Environment Visibility	Consistent Policy Enforcement
Software-Defined Perimeter	Secure Access Pathways	Protected Distributed Resources
Infrastructure-as-Code Security	Embedded Protection	Reduced Remediation Costs
Runtime Application Self-Protection	Continuous Verification	Enhanced Operational Security
Security Policy-as-Code	Automated Compliance	Maintained Protection Levels
Maturity Assessment Frameworks	Progressive Capability Planning	Prioritized Enhancement Initiatives

Table 1: Zero Trust Technology Components and Impact Assessment [9, 10]

6. Conclusion

Zero trust architecture has emerged as a transformative security model that addresses fundamental vulnerabilities in traditional network protection approaches. By implementing continuous verification processes across all digital interactions, organizations establish resilient security frameworks capable of protecting distributed resources in modern computing environments. The core principles of zero trust—least privilege access, micro-segmentation, continuous monitoring, and data-centric protection—create a comprehensive security ecosystem that limits potential attack surfaces while enabling business innovation. As implementation frameworks mature and integration with technologies like artificial intelligence, cloud security, and DevSecOps practices deepens, zero trust capabilities will continue evolving to address emerging threats and operational requirements. Organizations adopting zero trust principles position themselves to maintain effective security postures despite expanding attack surfaces and increasingly sophisticated adversaries, creating protection models that remain effective regardless of where resources reside or how they are accessed.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Chase Cunningham, "The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q3 2020," Forrester, 2020. [Online]. Available: https://f.hubspotusercontent10.net/hubfs/2241716/Zero%20Trust/forrester-ztx-report-2020.pdf

[2] Cybersecurity and Infrastructure Security Agency, "Zero Trust Maturity Model," 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf

[3] IBM Security, "Cost of a Data Breach Report 2024,". [Online]. Available: https://www.ibm.com/reports/data-breach

[4] John Kindervag, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture," Forrester, 2010. [Online]. Available: https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf

[5] Onome Edo et al., "Zero Trust Architecture: Trend and Impact on Information Security," ResearchGate, 2022. [Online]. Available: https://www.researchgate.net/publication/361758378_Zero_Trust_Architecture_Trend_and_Impact_on_Information_Security

[6] Saeid Ghasemshirazi, "Zero Trust: Applications, Challenges, and Opportunities," arXiv:2309.03582, 2023. [Online]. Available: https://arxiv.org/abs/2309.03582

[7] Sandeep Chinamanagonda, "Zero Trust Security Models in Cloud Infrastructure -Adoption of zero-trust principles for enhanced security," Academia Nexus Journal, 2022. [Online]. Available: http://academianexusjournal.com/index.php/anj/article/view/3/3

[8] Scott Rose et al., "Zero Trust Architecture," U.S. Department of Commerce, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

[9] Sumit K, "Zero Trust Security: A Modern Approach to Securing Your Applications," Medium, 2023. [Online]. Available: https://medium.com/google-cloud/zero-trust-security-model-a-new-approach-to-network-security-9dee89564b3e

[10] Tahir, "6 Pillars of DevSecOps: Bridging Security & DevOps," Medium, 2025. [Online]. Available: https://medium.com/@tahirbalarabe2/6-pillars-of-devsecops-bridging-security-devops-2f6fe12ade7b