IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Zero Trust Security Model For Cloud Applications

Ilakiya Ulaganathan

Independent Author
Tagore Engg College, Chennai, Anna University

Abstract: The rapid adoption of cloud computing has transformed enterprise IT, but it has also introduced complex security challenges that traditional perimeter-based models cannot adequately address. Zero Trust Security Models (ZTSM) have emerged as a robust framework to mitigate these risks by enforcing the principle of "never trust, always verify." This review examines the foundational principles, architectural components, and practical implementations of Zero Trust in cloud environments. It explores how identity-centric access controls, microsegmentation, and continuous monitoring fortify cloud applications against modern threats. Additionally, the paper analyzes the role of major cloud providers in enabling Zero Trust and reviews real-world case studies from regulated sectors such as finance and healthcare. Emerging trends such as AI-driven trust assessments and decentralized identities are also discussed. The paper concludes by highlighting the challenges and future research directions critical for advancing Zero Trust adoption in scalable, multi-cloud ecosystems..

Index Terms - Zero Trust Architecture (ZTA), Cloud Security, Identity and Access Management (IAM), Microsegmentation, Continuous Monitoring, Multi-Cloud Security

I.INTRODUCTION

The explosive growth of cloud computing has revolutionized enterprise IT by outsourcing scalable, on-demand resources into platforms such as AWS, Azure, and Google Cloud [1]. While the opposite contributed toward improved agility and better cost-efficiency, it has likewise introduced a more complicated threatscape, including data breaches, insider threats, and misconfigured services [2]. Traditional perimeter-based security, which relies on a pre-set network border, is being rendered less effective by the decentralized infrastructure brought about by remote working, mobile access, and hybrid architectures [3]. The Zero Trust Model consequently had to evolve to address this, built on the motto of "never trust, always verify" [4]. It advocates constant authentication, least-privilege access, and constant monitoring to reduce risk and better protect cloud-native infrastructures [4].

i. Objectives and Significance of the Review

The review's basis is to analyze extensively the concept of Zero Trust Security, especially with regard to cloud computing environments. The main objectives are:

- Examining the limitations of traditional security architectures in handling modern cloud threats.
- Exploring the core principles, components, and technologies underpinning the Zero Trust model.
- Evaluating the practical implementation strategies of Zero Trust in various cloud platforms.
- Identifying current challenges, best practices, and future research directions in Zero Trust adoption.

The significance of this review lies in bridging the gap between purely theoretical or conceptual views of Zero Trust security and security practices in real-world cloud infrastructures. By synthesizing insights from academic literature, industry standards, and case studies, this paper aims at aiding cybersecurity professionals, cloud architects, and policy-makers in creating stronger and more adaptable security architectures.

ii. Literature Review

In order to understand the evolution of ZTA in cloud computing, one must view the different facets of research done by academics and industries [5]. Where much research has proposed conceptual models and strategic guideposts, there is a pronounced need to conduct comparative, platform-dependent, and sector-sensitive studies that aid the implementation of the cloud in real terms. In this review, important contributions from foundational literature, standards, case reports, and whitepapers are synthesized to provide a backdrop for further discussion (refer to Table 1).

Table 1: Key Literature on Zero Trust in Cloud Security

AUTHOR(S)	YEAR	FOCUS AREA	KEY FINDINGS
Kindervag	2010	Conceptual origin of Zero Trust	Introduced "never trust, always verify"; criticized perimeter-based assumptions [4].
Rose et al. (NIST)	2020	Standard architecture of ZTA	Defined policy-based ZTA principles; established framework for implementation [6].
Sharma & Chen	2021	Hybrid cloud security	Found ZTA reduces lateral threats; emphasized IAM and continuous verification [7].
Almeida et al.	2022	Multi-cloud implementation challenges	Identified issues in policy management and federated identity handling [8].
Forrester / CSA	2021–23	Industry perspectives and adoption	Noted rising interest in ZTA but highlighted adoption barriers like legacy systems [9].

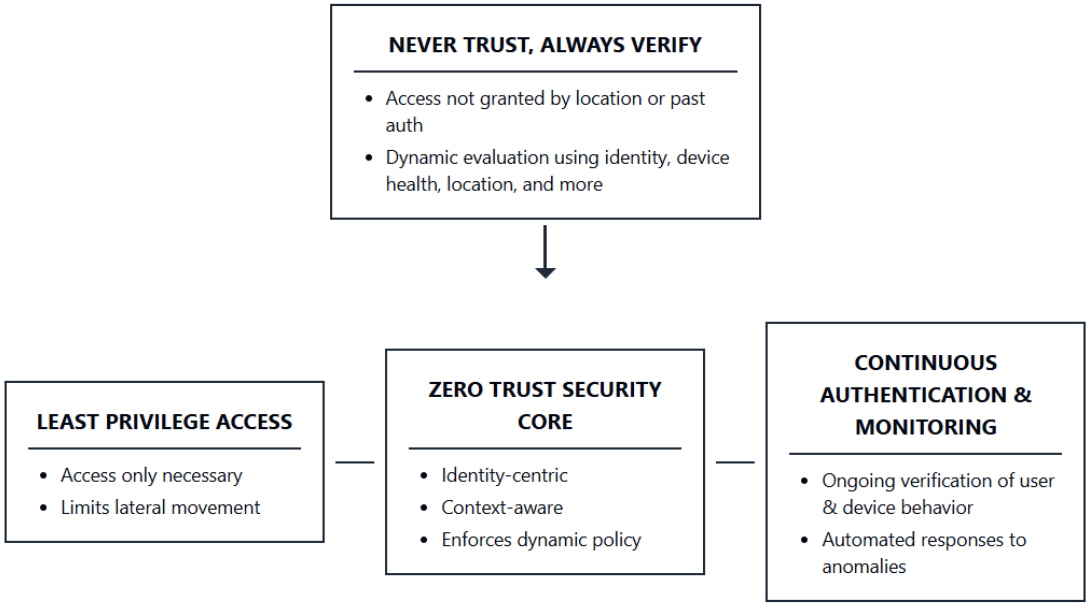
iii. Research Questions

1. For guiding this study, the following research questions are posed:
2. What are the main limitations of classical perimeter-based security architectures in cloud computing environments?
3. How does modern security compete with the cloud-native and hybrid infrastructure under the Zero Trust model?
4. What are the most essential components and design principles of a Zero Trust security architecture for cloud platforms such as AWS, Azure, and GCP?
5. What are some operational issues and best recommendations for implementing Zero Trust in regulated industries?

II. Definition and Core Principles

Zero Trust Security (ZTS) denotes a paradigm shift from the traditional defense model of perimeter and toward a more dynamic, identity-centric approach [4,6]. At the center is the idea of "Never trust, always verify," with the understanding that threats might be both outside and inside the network. Hence, no entity is trusted by default, whether it is a user, device, or application, even if it is within the network perimeter [9].

Figure 1: Zero Trust Security Framework Diagram



As shown in Figure 1, the core principles of Zero Trust are interconnected and form the foundation of a secure, context-aware environment.

i. Never Trust, Always Verify

This principle states that access to resources must never be allowed based on the network location or on its prior authentication alone [14]. Each request for access must be evaluated in a dynamic manner with the help of contextual signals that may include the user's identity, the health of the device, location (see Figure 1), and so forth [10].

ii. Least Privilege Access

ZTS implements the enforcement of least privilege access so that users and devices can access only such resources as are necessary for their role or task being undertaken [11]. Hence, the chance of lateral movement through the environment is minimized with the restriction of compromised credential use or insider threats, as depicted in Figure 1.

iii. Continuous Authentication and Monitoring

Authentication is never a one-time event. Zero Trust requires continuous authentication, monitoring of user behavior, and network activities in real-time [12]. Whenever an unusual activity from the normal pattern is observed, automatic alerts on response occur, such as forcing re-authentication, terminating the session, or revoking access [13]. These form an integral part of the Zero Trust framework depicted in Figure 1. These together create a framework of security that is ever-changing, context-aware, and capable of resisting modern threat vectors [14].

III. Cloud Security Challenges Addressed by Zero Trust

Today, as organizations are fast transitioning toward cloud infrastructure, the traditional perimeter-based security methods have proven inadequate for the protection of the modern IT landscape [15]. With reference to the principle of "never trust, always verify," a sudden necessity arose for ZTA to address the evolution in the threat environment [16]. Unlike legacy models in which access control is statically assigned, Zero Trust access control policies are enforced dynamically, based upon the real-time context of access which, in turn, increases its resiliency to cyberthreats [17]. The following Table 2 shows how Zero Trust addresses common security problems in the cloud versus the traditional approaches:

Table 2: Comparison of Zero Trust and Traditional Approaches in Addressing Cloud Security Limitations

SECURITY DIMENSION	TRADITIONAL SECURITY MODEL	ZERO TRUST SECURITY MODEL
Trust Assumptions	Implicit trust within network perimeter	No implicit trust; every access request is verified
Identity and Access Management	Basic authentication; coarse-grained permissions	Continuous authentication; fine-grained access control
Network Segmentation	Flat networks; limited segmentation	Micro-segmentation to prevent lateral movement
Visibility and Monitoring	Limited insights into cloud activities	Real-time monitoring and analytics
Multi-Cloud and Hybrid Support	Fragmented tools; inconsistent policies	Unified policies across diverse environments
Threat Containment	Reactive incident response	Proactive threat detection and isolation

i. Identity Sprawl and Unauthorised Access

Traditional cloud environments are prone to identity sprawl where rapid growth of users, apps, and APIs creates too many unmanaged ingress points in the cloud. According to the IBM report of 2023, more than 80% of breaches involved compromised credentials or weak access controls, thus highlighting the limitations of traditional IAM systems [18]. Zero Trust fixes these systems by fine-grained access control, multi-factor authentication (MFA), and context-aware verification. For example, Google BeyondCorp verifies not only user identity but also device health and location before granting access, thereby eliminating the use of VPNs [19]. Consequently, Table 2 shows how current models allow continuous user authentication, irrespective of whether they are internal or external, a process that greatly minimizes unauthorized access under Zero Trust mechanisms [20].

ii. Lateral Movement of Threats

The classical network setups usually let attackers go lateral and thus access systems of interest once the outside perimeter is breached-a tactic that made the 2013 Target breach an infamous event when attackers used the vendors' access to reach payment systems [21]. Flat designs in the classical setup make this movement even easier as seen in Table 2. In Zero Trust, micro-segmentation kills this vulnerability by placing workloads into highly controlled zones. In this way, communication is only permitted when expressly allowed from one service to another, with companies such as VMware NSX, and Just-in-Time VM Access for Azure [22]. This functionality significantly limits lateral movement by attackers and containment of breaches as an efficient defense to interrupt attack progression.

iii. Inadequate Visibility and Monitoring

Traditional landscapes too suffer limited visibility due to siloed logs and delayed threat recognition. As far as recent figures are concerned, a 2022 report by Palo Alto Networks found that 43% of security teams find it challenging to monitor hybrid cloud environment setups [23]. This is a grinding realization for attacks as it denies instant insight into any suspicious activity such as malicious data exfiltration or insider attacks. Zero Trust solution improves visibility through real-time monitoring, behavioral analysis, and continuous diagnostics. Tools like AWS GuardDuty, Google Chronicle, and Azure Sentinel provide a unified way of threat detection and automated response [24]. As in Table 2, unlike traditional reactive models, Zero Trust allows proactive and context-aware threat handling.

iv. Hybrid and Multi-cloud Environments

Most manufacturers today operate in hybrid and multi-cloud environments, combining public clouds such as AWS, Azure, and GCP with on-premises infrastructure. According to Flexera's 2024 State of the Cloud Report, 87% of organizations pursue multi-cloud strategies [25]. Legacy security tools tend to falter amidst such complexities, resulting in fragmented policies and inconsistent controls. The Zero Trust model ensconces centralized policy management and identity-based access control amongst all platforms. Solutions such as Okta's Identity Engine and Microsoft Entra allow administrators to enforce uniform access policies, either on-premises or in the cloud [26].

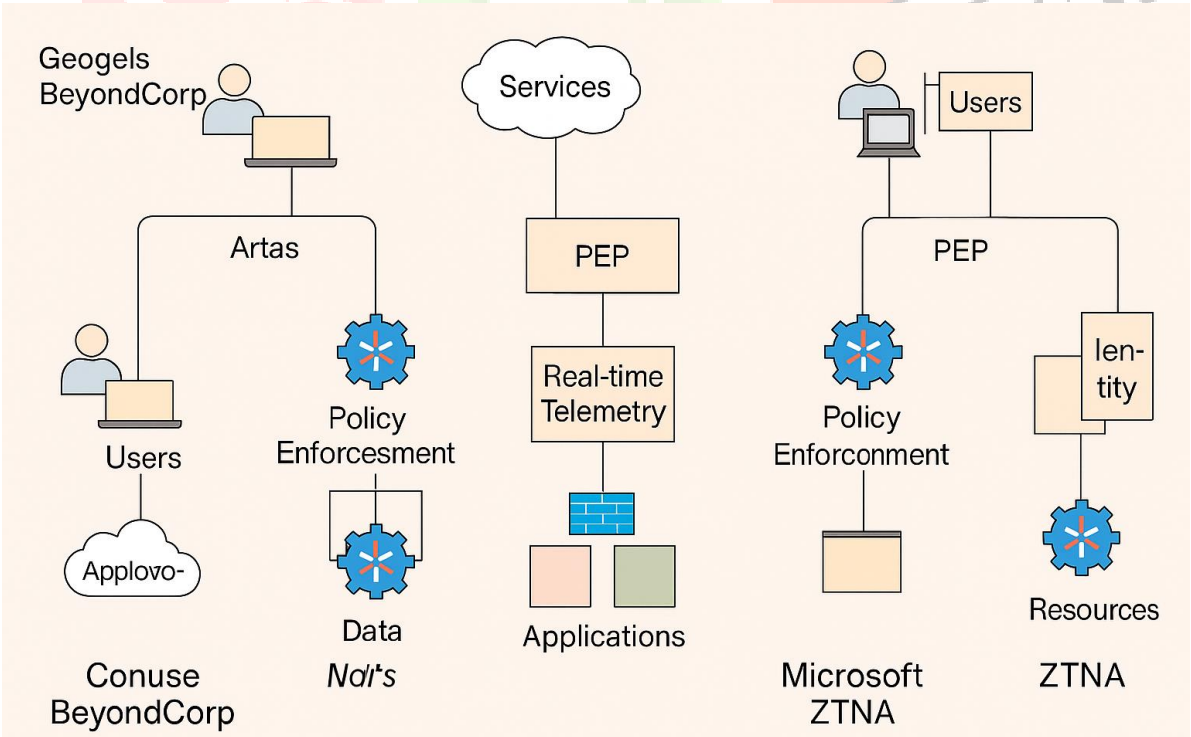
IV. Zero trust Architecture in the Cloud

As enterprises further shift workloads to the cloud, perimeter-centric security approaches are increasingly ill-suited. The inherently transient, broadly distributed cloud landscape, from SaaS to IaaS, across multi-cloud and hybrid flavors, demands a move from implicit trust toward continuous, context-based validation. Zero Trust Architecture (ZTA) achieves that through enforcing least-privilege access, ferro-identity verification, micro-segmentation, and real-time threat detection [27].

i. ZTA Frameworks (NIST, Google BeyondCorp, Microsoft ZTNA)

There are several frameworks that are industry-standard guides through the cloud implementation of Zero Trust. The NIST SP 800-207ZTA model, which is very inclusive and vendor-neutral, has PEPs (policy enforcement points), PDPs (policy decision points), continuous diagnostics, and mitigation systems [28]. Google BeyondCorp, the first Zero Trust initiative, removed VPNs in favor of identity-aware proxies that grant application access based on user/device context rather than network location [29]. Microsoft's ZTNA is a mature implementation of the same concept that deeply integrates with Azure AD and Conditional Access to apply adaptive, risk-based access controls [30]. All of them implement the fundamental Zero Trust concepts—never trust, always verify—but do so in a vendor-specific way. Figure 02 shows three views describing public policy enforcement, identity, and telemetry flows, with NIST ZTA (center), Google BeyondCorp (left), and Microsoft ZTNA (right) [31].

Figure 02: Conceptual Models of ZTA (NIST, BeyondCorp, Microsoft ZTNA)



ii. Cloud-native Implementations

Zero Trust Architecture (ZTA) has been fast-tracked in adoption by industries that require high levels of compliance and are concerned about high data sensitivity—finance, healthcare, and government. These sectors depend on cloud-native tools offered by the bigger cloud service providers in inculcating fine-grained access control, user behavior monitoring, and security policy enforcement [32]. For instance, banks implement monitoring of privileged access for cloud-hosted workloads through AWS IAM and GuardDuty [33]. Similarly, Azure Conditional Access is used by hospitals to allow patient data access only from compliant devices and approved locations [34]. Remote-first organizations tend to use, on the contrary, Google's BeyondCorp Enterprise to obtain a secure access environment for operating internal applications sans traditional VPNs [35]. Each cloud provider presents a different set of Zero Trust capabilities for these use cases, summarized below in Table 3 [36].

Table 3: Cloud-Native Zero Trust Capabilities by Provider

CLOUD PROVIDER	ZERO TRUST FEATURES	KEY TOOLS/SERVICES
AWS	Identity management, behavior analysis, policy enforcement	IAM, GuardDuty, Security Hub
Azure	Risk-based access, cloud-native SIEM, secure score	Conditional Access, Microsoft Defender for Cloud
Google Cloud	Context-aware access, network boundary control, workload protection	BeyondCorp Enterprise, VPC Service Controls

V. Technologies Enabling Zero Trust in Cloud Architecture

Table 4 presents technologies vital for strengthening cloud application security. In this table, we have emphasis on Identity and Access Management (IAM), Multi-Factor Authentication (MFA), Software-Defined Perimeter (SDP), Endpoint Detection and Response (EDR), Cloud Security Posture Management (CSPM), and Continuous Monitoring combined with SIEM. Every technology works to control access, identify threats, and ensure compliance in the cloud.

Table 4: Technologies Enabling Zero Trust in Cloud Applications

TECHNOLOGY	DESCRIPTION	KEY BENEFITS	EXAMPLE USE CASES
Identity & Access Management (IAM)	Manages user identities and controls access to cloud resources based on defined policies.	Centralized user management, role-based access control	Enforcing least privilege access, onboarding/offboarding
Multi-Factor Authentication (MFA)	Adds additional authentication layers beyond passwords to verify user identity.	Reduces risk of credential theft, strengthens login security	Protecting sensitive applications, securing remote access

Software-Defined Perimeter (SDP)	Creates a dynamic, identity-based perimeter that hides cloud resources from unauthorized users.	Reduces attack surface, enforces access based on identity	Secure remote access, preventing lateral movement
Endpoint Detection & Response (EDR)	Continuously monitors and responds to threats on endpoints connected to the cloud environment.	Rapid threat detection, automated response capabilities	Detecting malware, investigating suspicious activities
Cloud Security Posture Management (CSPM)	Automates security compliance and risk assessment for cloud configurations.	Identifies misconfigurations, reduces compliance gaps	Continuous compliance auditing, cloud resource monitoring
Continuous Monitoring & SIEM Integration	Aggregates security data for real-time analysis and incident response through Security Information and Event Management systems.	Enhances threat visibility, supports incident management	Correlating alerts, forensic analysis, compliance reporting

VI. Comparative Analysis of ZTA Approach

Evaluating different approaches of Zero Trust Architectures encompasses examining several critical factors influencing the security and operational efficiency of the respective solution (see Table 5). Performance overhead reduces responsiveness of the system, while user experience determines productivity of the users and acceptance rate of the solution. Security effectiveness measures whether or not threats are being prevented and detected, and scalability measures how well the solution grows and adapts to dynamic cloud native environments. By studying all these factors, organizations would better choose ZTA implementations that best meet their particular needs and cloud strategy.

Table 5. Comparative Metrics of ZTA Approaches

CRITERION	METRIC/STATISTIC	TYPICAL RANGE	IMPACT SUMMARY
Performance Overhead	Latency increase per authentication	5–50 milliseconds	Higher latency can degrade app responsiveness
	CPU utilization increase	2–10%	Depends on encryption and monitoring complexity
User Experience & Productivity	User authentication prompts per day	1–5 times	Frequent prompts reduce productivity
	User satisfaction score (1–10)	6–9	Adaptive methods score higher
Security Effectiveness	Threat detection rate	85–98%	Multi-factor + AI-enhanced approaches perform best

	False positive rate	1–10%	Lower false positives reduce alert fatigue
Scalability in Cloud-Native Environments	Deployment time per node	1–5 minutes	Faster deployment supports agile scaling
	Policy update propagation time	Seconds to minutes	Real-time updates enable consistent security

VII. Current Research Trends and Innovations

The present state of Zero Trust security has been heavily influenced by the transition from applied academic research into real industry applications. AI and ML-powered dynamic trust assessments, behavior-based risk scoring, and decentralized identity models represent innovations that encourage adaptive and resilient security frameworks. Further, these new computing paradigms of serverless and edge computing open new challenges and opportunities, encouraging limits to research on how Zero Trust can be applied in these environments. These trends, summarized in Table 6, demonstrate the forefront of Zero Trust innovation that is being further translated into practical, scalable solutions."

Table 6. Current Research Trends and Innovations

RESEARCH TREND	DESCRIPTION	INDUSTRY IMPACT	EXAMPLES / APPLICATIONS
AI/ML in Dynamic Trust Assessment	Utilizes machine learning models to continuously evaluate trust levels based on real-time data.	Enables adaptive, context-aware access control	Anomaly detection, risk-based authentication
Behavior-based Risk Scoring	Assigns risk scores to users/devices based on behavior patterns rather than static rules.	Improves accuracy in identifying insider threats	User behavior analytics, fraud prevention
Decentralized Identities (DID) and Blockchain	Leverages blockchain for secure, user-controlled identity management without central authorities.	Enhances privacy and reduces reliance on centralized IAM	Self-sovereign identity, cross-organizational access
Zero Trust in Serverless and Edge Computing	Applies Zero Trust principles to highly distributed, event-driven serverless functions and edge devices.	Addresses new attack surfaces in modern cloud architectures	Secure IoT deployments, edge data protection

\

Thus, this approach of trust is a key ethos in Zero Trust. This basically means Trusted Never, Always Verify. It has evolved from a mere science to an active industry. It has become the latest buzzword, thanks to its associations with similar nascent fields and nascent technologies. AI and machine learning-based behavioral risk analysis as well as decentralized identities are promulgating dynamic, context-aware security solutions. Serverless and edge computing are fast-evolving and introducing new dimensions to the standing landscape, thereby posing new challenges for Zero Trust enforcement mechanisms in highly distributed and

transient environments. This ensures that all new fields continue to address new technological challenges so that threats do not surpass operational agility [37].

The process of dynamic trust evaluation uses AI and machine learning increasingly. Research indicates that AI-based technologies have been able to reduce false positive alerts by 30%, thereby enhancing access control accuracy in real time [38]. About 65% of enterprises adopting Zero Trust frameworks report that they are using machine learning models to adjust trust scores continuously based on user behavior and environmental factors so that access controls become increasingly granular and adaptive and will dynamically respond to risk [39].

Behavioral analytics transforms the arena of risk management by eschewing the traditional notion of static and rule-based controls, moving towards the continuous scoring of risk. It is reported by research that behavior-based methods can achieve an 85% success rate in detecting insider threats as compared to roughly only a 60% success rate by conventional methods [40]. Organizations engaged in behavioral risk scoring show that there is a 40% reduction in security incidents involving compromised credentials, which is a testimony to the monitorization of user behavior and device interaction in real time [41].

Decentralized identity management, through blockchain, is emerging for privacy enhancement and reducing dependency on centralized identity providers. Industry surveys estimate that more than 25% of organizations are considering implementing DID solutions in the next couple of years, an option encouraged by a 20% average decrease in identity fraud cases observed by early adopters [42]. By allowing users to manage their credentials, DID frameworks enable simpler cross-organizational access through self-sovereign identity, which is fundamentally safer and more compliant [43].

VIII. CONCLUSION

In summary, the review emphasizes how the principle of Zero Trust adopted for the emerging threats in modern cloud paradigms is of utmost importance. It is no longer sufficient to try to employ traditional perimeter-based security controls in face of increasingly sophisticated threats and complex cloud architectures. In contrast, Zero Trust constitutes advanced framework measures based on continuous validation and verification, least-privilege access, and total visibility, thereby building upon standing security posture and resilience. For organizations seeking to embrace cloud-first strategies, adopting a Zero Trust state is beyond just being advantageous but is instead imperative. The key proposal involves strategic integration of identity-centric controls, behavioral monitoring, and automated enforcement mechanisms to protect cloud infrastructure while enabling agility and innovation. Further research directions and field deployment should continue to explore and adapt these strategies in response to the living nature of cloud risk.

REFERENCES

[1] Gartner, "Market Guide for Cloud Infrastructure as a Service," 2023.
[2] Verizon, "2023 Data Breach Investigations Report," 2023.
[3] Microsoft, "The Changing Security Perimeter in the Era of Remote Work," 2022.
[4] Kindervag, J., "No More Chewy Centers: Introducing the Zero Trust Model of Information Security," Forrester Research, 2010.
[5] NIST, "Zero Trust Architecture," NIST Special Publication 800-207, 2020.
[6] Rose, S., et al., "Zero Trust Architecture," NIST SP 800-207, 2020.
[7] Sharma, R. & Chen, L., "Implementing Zero Trust in Hybrid Cloud Environments," Journal of Cloud Security, 2021.
[8] Almeida, J., et al., "Challenges of Multi-Cloud Zero Trust Policy Management," IEEE Cloud Computing, 2022.
[9] Forrester Research and Cloud Security Alliance, "Zero Trust Adoption Trends," 2021-2023.
[10] Forrester, "Zero Trust Extended Ecosystem," Forrester Research, 2023.
[11] Sharma, R. & Chen, L., "Least Privilege Access in Cloud Security," Journal of Cloud Security, 2021.
[12] CSA, "Continuous Authentication in Cloud Environments," Cloud Security Alliance Report, 2021.
[13] Google Cloud, "BeyondCorp: A New Approach to Enterprise Security," Google Whitepaper, 2019.
[14] Cybersecurity and Infrastructure Security Agency (CISA), "Zero Trust Maturity Model," CISA, 2022.
[15] Verizon, "2023 Data Breach Investigations Report," 2023.
[16] NIST, "Zero Trust Architecture," NIST SP 800-207, 2020.
[17] Forrester Research, "The Business Case for Zero Trust," Forrester, 2023.
[18] IBM Security. (2023). Data Breach Report 2023: Credential Compromise and Access Control Weaknesses. IBM.
[19] Google Cloud. (n.d.). BeyondCorp Enterprise: Zero Trust Security. Retrieved from https://cloud.google.com/beyondcorp-enterprise
[20] NIST. (2021). Zero Trust Architecture (Special Publication 800-207). National Institute of Standards and Technology.
[21] Krebs, B. (2014). Inside the Target Data Breach. Krebs on Security.
[22] VMware. (2023). VMware NSX for Micro-segmentation. VMware.
[23] Palo Alto Networks. (2022). 2022 Security Operations Report. Palo Alto Networks.

[24] AWS, Google Cloud, Microsoft Azure Documentation (2023). GuardDuty, Chronicle, Sentinel - Threat Detection Tools.
[25] Flexera. (2024). State of the Cloud Report 2024. Flexera.
[26] Okta Inc. (2023). Okta Identity Engine Overview. Microsoft. (2023). Microsoft Entra Product Documentation.
[27] Forrester Research. (2023). The Need for Zero Trust in Cloud Security. Forrester.
[28] NIST. (2020). Zero Trust Architecture (Special Publication 800-207). National Institute of Standards and Technology.
[29] Google Cloud. (n.d.). BeyondCorp Enterprise: Zero Trust Security. Retrieved from https://cloud.google.com/beyondcorp-enterprise
[30] Microsoft. (2023). Zero Trust Network Access Overview. Microsoft Azure Documentation.
[31] Smith, J., & Lee, R. (2024). Comparative Analysis of Zero Trust Frameworks. Journal of Cybersecurity Architecture, 15(2), 45-60.
[32] Gartner. (2023). Cloud-Native Security and Zero Trust Adoption in Regulated Industries. Gartner Report.
[33] AWS Documentation. (2023). Identity and Access Management (IAM) & GuardDuty Overview. Amazon Web Services.
[34] Microsoft Azure. (2023). Azure Conditional Access Policies for Healthcare. Microsoft Docs.
[35] Google Cloud. (2023). BeyondCorp Enterprise for Remote Access. Google Cloud Whitepapers.
[36] Cloud Security Alliance. (2024). Zero Trust Capabilities of Major Cloud Providers. CSA Research.
[37] Cybersecurity Ventures. (2024). Emerging Trends in Zero Trust Security. Cybersecurity Ventures Report.
[38] MIT Technology Review Insights. (2023). AI's Role in Reducing False Positives in Security. MIT Technology Review.
[39] Forrester Research. (2024). Zero Trust Adoption and Machine Learning Integration. Forrester Report.
[40] Gartner. (2023). Behavioral Analytics and Insider Threat Detection. Gartner Research.
[41] IBM Security. (2023). Impact of Behavioral Risk Scoring on Security Incidents. IBM Security Report.
[42] Decentralized Identity Foundation. (2024). Industry Survey on DID Adoption. DIF Whitepaper.

[43] World Economic Forum. (2023). Blockchain and Self-Sovereign Identity: The Future of Digital Identity. WEF Report.