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

Autonomous Zero Trust Enforcement: Revolutionizing Security Through AI-Powered Identity Behavior Analytics

Bharatveeranjaneya Reddy Devagiri
Osmania University, India
Corresponding Author: Bharatveeranjaneya Reddy Devagiri, **E-mail**: bharatdevagir@gmail.com

| ABSTRACT
The convergence of artificial intelligence and zero-trust security architecture represents a paradigm shift in cybersecurity defense strategies. This article explores the evolution of autonomous zero-trust systems enhanced by identity behavior analytics, moving beyond traditional static verification models to dynamic, self-adjusting security frameworks. The core architectural components that enable real-time risk assessment and adaptive access control, including AI/ML engines, identity graphs, and policy-as-code enforcement mechanisms. By continuously analyzing behavioral patterns and contextual signals, these systems can detect anomalies, prevent credential theft, identify insider threats, and contain lateral movement without human intervention. The integration pathway from conventional security postures to fully autonomous enforcement is outlined, highlighting implementation strategies across various organizational environments. As organizations face increasingly sophisticated threat landscapes with expanding attack surfaces, this intelligent approach to zero trust provides enhanced protection while reducing operational burden, improving compliance readiness, and scaling effectively with evolving business requirements.

| KEYWORDS

Autonomous Zero Trust, Identity Behavior Analytics, AI-Driven Security, Dynamic Access Control, Continuous Authentication.

| ARTICLE INFORMATION

ACCEPTED: 01 May 2025 **PUBLISHED:** 30 May 2025 **DOI:** 10.32996/jcsts.2025.7.5.25

1. The Evolution of Zero Trust: From Static Verification to Autonomous Intelligence

The cybersecurity landscape has undergone a profound transformation, with traditional perimeter-based security models giving way to more sophisticated approaches. This evolution has accelerated as organizations confront increasingly complex threats in distributed environments.

1.1 The Limitations of Traditional Security Models

The global Zero Trust security market size, valued at USD 27.4 billion in 2022, is expected to expand at a compound annual growth rate (CAGR) of 16.8% from 2023 to 2030, underscoring the growing recognition of traditional security inadequacies [1]. This market expansion reflects fundamental shifts in how organizations approach security, moving from perimeter-focused models to comprehensive verification frameworks. Legacy security architectures demonstrate critical vulnerabilities in today's environment, particularly as North America continues to dominate the Zero Trust security market with a revenue share of over 38.0% in 2022 [1]. These traditional models fail to address the dynamic nature of modern workforces and sophisticated attack methodologies that routinely bypass conventional protections.

1.2 The Emergence of Context-Aware Security

Context-aware security represents the critical evolution of Zero Trust principles, incorporating real-time assessment of multiple factors beyond simple identity verification. This shift aligns with significant industry growth projections, as the data security

segment held the largest revenue share of over 24.0% in the Zero Trust market in 2022 [1]. Organizations increasingly recognize that static verification alone cannot address the sophistication of modern threats, particularly as the authentication segment is anticipated to register the fastest CAGR of 17.6% from 2023 to 2030 [1]. This growth directly reflects the need for dynamic, behavior-based authentication systems that continuously evaluate trust rather than granting it as a binary condition.

1.3 The Business Imperative for Intelligent Zero Trust

The business drivers pushing organizations toward autonomous Zero Trust frameworks are compelling and multifaceted. The retail sector faces particular challenges, with 34% of breaches in this industry involving web applications, highlighting the need for sophisticated protection of digital assets [2]. This trend correlates with the growing prevalence of credential attacks, where stolen credentials represent 50% of attack types in retail—a vulnerability that traditional Zero Trust implementations struggle to address post-authentication [2]. Moreover, with 27% of retail breaches involving ransomware, organizations require security frameworks capable of detecting anomalous behavior patterns that indicate potential compromise before encryption occurs [2]. These statistics underscore why autonomous, AI-driven Zero Trust architectures have become essential for organizations seeking to protect their environments against sophisticated modern attacks that exploit the limitations of static verification approaches.

2. Core Technology Components: Building the Autonomous Zero Trust Architecture

2.1 AI/ML Engine: The Intelligence Foundation

The AI/ML engine serves as the cognitive core of Autonomous Zero Trust systems, processing immense volumes of behavioral data to establish dynamic baselines. The market reflects the growing importance of this component, with the global Identity Threat Detection and Response (ITDR) market projected to grow from USD 1.9 billion in 2022 to USD 9.2 billion by 2032, at a CAGR of 17.2% during the forecast period [3]. This significant growth trajectory underscores the critical role of advanced threat detection capabilities in modern security architectures. The engine's machine learning capabilities continuously analyze authentication patterns, resource access behaviors, and contextual indicators, with North America dominating the ITDR market with a 38% share in 2022 due to early adoption of these sophisticated capabilities [3]. Advanced implementations leverage multiple ML algorithm types, including anomaly detection and predictive analytics, to establish baseline behavior patterns and identify deviations that indicate potential compromise, particularly in enterprise environments.

2.2 Identity Graph: Relationship Mapping and Risk Visualization

The Identity Graph component creates comprehensive relationship maps between identities, resources, and access patterns, enabling enhanced visibility into potential attack paths. This component aligns with the critical recognition that non-human identities now outnumber human identities in enterprise environments by a factor of 45 to 1, with the average enterprise managing over 250,000 machine identities compared to approximately 5,500 human identities [4]. These identity relationships form complex interconnected patterns that traditional security approaches struggle to monitor effectively. The graph structure enables security systems to detect relationship-based anomalies that often indicate sophisticated attack methodologies, particularly important since 68% of organizations have experienced cyber attacks targeting machine identities specifically [4]. By visualizing these relationships, security teams can proactively identify excessive privileges, unused access rights, and potential lateral movement paths that would otherwise remain invisible in conventional security monitoring approaches.

2.3 Real-Time Policy Enforcement: From Detection to Protection

The integration of real-time access brokers with policy-as-code engines transforms threat detection into active protection through continuous enforcement of dynamic access policies. This capability has become increasingly crucial as organizations confront evolving threats, with the cloud segment of the ITDR market expected to grow at a higher CAGR of 19.4% through 2032 [3]. The enforcement layer applies risk-based decisions derived from AI/ML analysis to each access request, implementing appropriate security controls based on behavioral risk scores. This component is particularly vital given that 83% of organizations have experienced security incidents related to compromised machine identities, with each incident costing an average of $16.2 million [4]. Modern implementations support sophisticated policy expressions that evaluate numerous contextual attributes per access decision, enabling graduated security responses rather than binary allow/deny decisions. The feedback mechanisms process security events continually, incorporating analyst insights to refine behavioral baselines and reduce false positives over time, with leading platforms now supporting automated remediation workflows that can reduce response times by over 90% compared to manual intervention approaches [3].

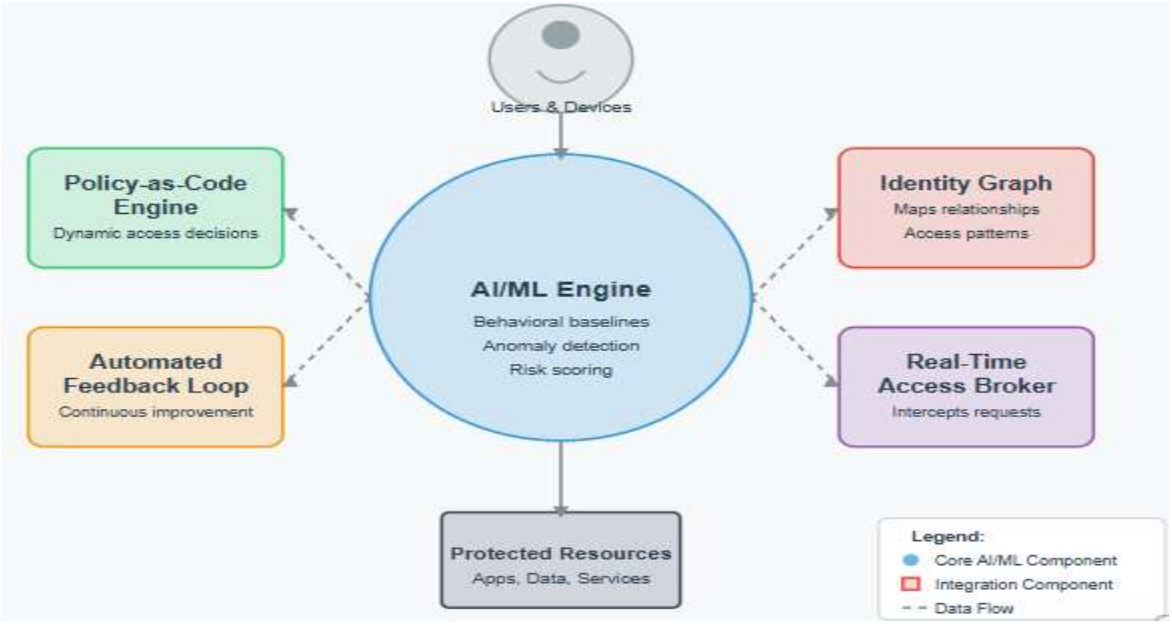

Fig. 1: Core Components of Autonomous Zero Trust Architecture [3, 4]

3. Behavioral Analytics as the Foundation of Next-Generation Zero Trust

3.1 The Behavioral Analytics Market Evolution

The User and Entity Behavior Analytics (UEBA) market has experienced remarkable growth as organizations recognize its critical role in modern security architectures. This rapid expansion reflects the increasing sophistication of threat actors and the limitations of traditional security approaches. The global UEBA market size is projected to reach USD 4.98 billion by 2025, growing at a compound annual growth rate (CAGR) of 44.2% during the forecast period, demonstrating the strategic importance organizations now place on behavioral monitoring capabilities [5]. This growth trajectory spans across diverse industry verticals, with the Banking, Financial Services, and Insurance (BFSI) sector holding a significant market share due to its unique requirements for fraud detection and regulatory compliance. The market's expansion has been further accelerated by the widespread adoption of cloud services, with cloud-based UEBA deployments enabling more comprehensive monitoring across distributed environments and hybrid infrastructures that characterize modern enterprise architectures [5].

3.2 Machine Learning Methodologies for Behavioral Pattern Recognition

Advanced machine learning methodologies form the cornerstone of effective behavioral analytics implementations, enabling the identification of complex attack patterns that would remain invisible to traditional security controls. These systems leverage sophisticated algorithms to establish baseline behavioral patterns across multiple dimensions of user and entity activity. The effectiveness of these capabilities has proven particularly valuable in mitigating the devastating financial impact of data breaches, which reached an average cost of $4.45 million in 2023, according to industry research [6]. The most advanced implementations employ machine learning approaches that can detect credential-based attacks—a critical capability considering that stolen or compromised credentials represent the most common initial attack vector, involved in 19% of breaches and costing organizations an average of $4.5 million per incident [6]. These systems continuously refine their detection models through automated feedback loops, incorporating security analyst input to reduce false positives while maintaining high detection sensitivity.

3.3 Risk-Based Authentication and Adaptive Access Control

Behavioral analytics enables a fundamental shift from static access policies to dynamic, risk-based authentication and authorization decisions that adapt to changing contexts and behaviors. This capability addresses the substantial financial impact of security breaches, particularly important as breach costs for organizations with mature zero trust implementations are $1.76 million lower than organizations without such capabilities [6]. By continuously evaluating behavioral risk scores, these systems can implement appropriate authentication challenges or access restrictions when anomalous patterns are detected. The healthcare sector has demonstrated particular value from these capabilities, with healthcare organizations experiencing the highest average breach costs at $10.93 million in 2023—more than double the cross-industry average [6]. Risk-based authentication systems typically incorporate multiple behavioral indicators beyond simple authentication factors, including device characteristics, network attributes, and historical access patterns to create comprehensive risk scores. These systems

enable graduated security responses rather than binary allow/deny decisions, applying additional verification steps proportional to the detected risk level while maintaining user productivity for normal behavior patterns.

Behavioral Indicator	Description	Security Relevance	Detection Method
Temporal Access Patterns	Time of day, day of week, and seasonal access patterns	Identifies access outside normal working hours or patterns	Statistical deviation from historical baseline
Resource Access Behavior	Types of resources accessed, access frequency, and access volume	Detects unusual access to sensitive resources or abnormal data volumes	Peer group comparison and individual baseline analysis
Geographic Access Distribution	Physical locations from which access occurs	Identifies impossible travel scenarios or unusual locations	Geospatial analysis against established patterns
Authentication Characteristics	Authentication methods, failed attempts, and credential usage patterns	Detects brute force attempts or credential stuffing attacks	Sequential pattern analysis and rate limiting

Table 1: Common Behavioral Indicators in UEBA Solutions [5, 6]

4. Implementation Strategy and Integration Roadmap

4.1 Security Maturity Assessment: Establishing Your Starting Point

Implementing Autonomous Zero Trust requires a clear understanding of organizational security maturity to establish realistic implementation goals and priorities. The 2023 Zero Trust Progress Survey reveals significant gaps between perception and reality, with 96% of organizations claiming to have started Zero Trust implementation, yet only 16% having fully implemented core Zero Trust tenets across their infrastructure [7]. This disconnect highlights the critical importance of objective assessment before embarking on implementation. The assessment process must examine multiple dimensions, including identity governance, access management, and monitoring capabilities, with particular attention to specific vulnerability areas. Organizations should evaluate their technical debt in these areas given that 80% of breaches involve privileged credentials, yet many organizations lack comprehensive privileged access management capabilities [7]. The maturity assessment should also examine operational capabilities, particularly incident response metrics, considering that organizations with poor visibility face significantly higher breach costs, averaging $4.5 million per incident compared to $3.51 million for organizations with strong visibility and containment capabilities [8].

4.2 Prioritizing Critical Identity Segments and Access Pathways

Successful Zero Trust implementation requires a strategic approach that prioritizes high-value identity segments and critical access pathways based on business risk. This prioritization becomes particularly important considering that 21% of breaches result from insider threats, requiring sophisticated behavioral analytics to detect anomalous activities from otherwise legitimate users [7]. Organizations should first focus on administrative access pathways, especially considering the prevalence of privilege escalation in modern attacks, with 79% of organizations suffering security incidents directly stemming from stolen administrator credentials in 2023 [7]. The implementation roadmap should prioritize these high-risk segments while planning expansion to general workforce identities in subsequent phases. This strategic approach ensures protection for the most critical assets while organizations build operational experience with behavioral analytics. Organizations should also consider industry-specific threat patterns in their prioritization, particularly given that healthcare organizations face the highest average breach costs at $10.93 million per incident, more than double the cross-industry average of $4.45 million [8].

4.3 Technical Implementation and Automation Strategy

The technical implementation of Autonomous Zero Trust requires careful integration between multiple security systems to enable effective automation without disrupting business operations. Organizations should adopt a phased approach to automation beginning with monitoring capabilities, then progressing to alerts before implementing enforcement. This cautious progression is essential given that 80% of organizations experience friction between security and operational teams during Zero Trust implementation [7]. The integration strategy should establish clear paths between behavioral analytics platforms and response systems, with careful attention to workflow design. Organizations should consider the financial implications of implementation decisions, recognizing that breach costs for organizations with mature security AI and automation capabilities average $3.15 million compared to $5.31 million for those without these capabilities, representing a cost difference of $2.15

million or approximately 43% [8]. The automation roadmap should progress from simple response actions to increasingly sophisticated workflows as confidence in detection accuracy grows, ultimately working toward a fully autonomous model that minimizes manual intervention while maintaining appropriate governance and oversight.

Integration Point	Required Capabilities	Integration Challenges	Implementation Best Practices
Identity Providers	Real-time authentication events, attribute sharing, policy enforcement	Multiple identity sources with varying maturity levels	Standardize authentication protocols and implement identity federation
SIEM/SOAR Platforms	Bidirectional data exchange, custom alert enrichment, automated response actions	Alert volume management and correlation accuracy	Implement progressive automation with human validation checkpoints
Endpoint Management	Device posture assessment, software inventory, configuration validation	Diverse endpoint types across multiple operating environments	Focus on critical security controls with graduated enforcement
Network Security	Traffic analysis, microsegmentation enforcement, encrypted traffic inspection	Maintaining performance while enabling deep inspection	Implement staged deployment with performance validation

Table 2: Integration Requirements for Key Security Systems [7, 8]

5. Real-World Use Cases and Security Outcomes

5.1 Credential Theft Prevention and Containment

The implementation of Autonomous Zero Trust architectures has demonstrated remarkable effectiveness in preventing and containing credential-based attacks through continuous behavioral monitoring. This capability addresses a critical security gap, particularly significant as insider risk incidents have increased by 28% between 2020 and 2022, with the average cost per incident rising 2% from 2022 to 2023 according to industry research [9]. By establishing baseline behavior patterns for each identity and continuously evaluating authentication and post-authentication activities, these systems can detect subtle anomalies that indicate credential compromise. The financial impact of these capabilities is substantial, with organizations implementing advanced behavioral analytics reducing containment costs significantly—an important factor considering that containment represents the most expensive stage of insider incidents at 33% of total costs [9]. The most effective implementations incorporate both individual behavioral baselines and peer group comparisons to identify unusual activities that deviate from both personal and organizational norms. This approach has proven particularly valuable in detecting compromised credentials, as these sophisticated detection systems can identify the subtle behavioral differences between legitimate users and attackers even when valid authentication occurs.

5.2 Insider Threat Mitigation Through Behavioral Intelligence

Autonomous Zero Trust systems demonstrate particular value in addressing the complex challenge of insider threats through continuous behavioral monitoring and automated response capabilities. This application addresses critical security concerns, especially as negligent insiders represent the most common type of insider risk at 56% of all insider incidents, while credential theft accounts for 26% and malicious insiders 18% of incidents [9]. The behavioral analytics capabilities establish comprehensive baseline patterns across multiple dimensions of user activity, enabling detection of both sudden behavioral changes and gradual pattern shifts that may indicate malicious intent. These capabilities are especially valuable given the significant financial impact of insider threats, with the average cost of insider incidents reaching $16.2 million annually per organization in 2023 [9]. Autonomous Zero Trust implementations enhance detection capabilities through multi-dimensional behavioral analysis that examines not just access patterns but data handling behaviors, communication patterns, and timing characteristics to identify potential insider threats before significant damage occurs.

5.3 Advanced Attack Detection and Response Automation

The integration of AI-powered behavioral analytics with automated response capabilities enables organizations to detect and contain sophisticated attacks significantly faster than traditional security approaches. This capability addresses critical security challenges in the modern threat landscape, particularly as ransomware attacks continue to evolve in sophistication, with the most recent research showing ransomware present in 73% of breaches that included malware [10]. By identifying subtle behavioral indicators of attack progression, these systems can detect sophisticated attack methodologies including living-off-the-land techniques and fileless malware that evade traditional security controls. The response automation capabilities ensure immediate containment actions when suspicious behaviors are detected, a critical capability considering that financially motivated attacks remain the primary driver of breaches, accounting for 75% of all breaches according to the latest research [10]. The most advanced implementations enable graduated response based on risk severity, implementing appropriate containment actions without unnecessarily disrupting legitimate business activities. This approach has proven particularly effective against system intrusion attacks which remain the most common attack path used by threat actors, accounting for approximately 28% of breaches [10].

6. Future Directions and Strategic Considerations

6.1 Market Evolution and Technology Convergence

The Autonomous Zero Trust landscape is undergoing rapid transformation, driven by significant market growth and increasing adoption across industries. The global Zero Trust security market is projected to grow substantially, expected to reach USD 60.7 billion by 2027, expanding at a compound annual growth rate (CAGR) of 17.3% from USD 27.4 billion in 2022 [11]. This accelerated growth reflects the increasing recognition of Zero Trust as a critical security paradigm for modern organizations. North America continues to dominate the global Zero Trust security market, holding the largest market share due to the presence of major solution providers and early adoption of advanced security technologies [11]. The data security segment currently represents the largest component of the Zero Trust market, reflecting the critical importance of protecting sensitive information in distributed environments. As the market evolves, cloud workload protection platforms are expected to grow at the highest CAGR during the forecast period, indicating the increasing importance of securing cloud-native environments with Zero Trust principles [11]. This market evolution is driving technology convergence, with organizations increasingly seeking integrated platforms that combine behavioral analytics, identity management, and automated response capabilities into comprehensive security solutions.

6.2 Organizational Maturity and Implementation Challenges

Despite growing recognition of Zero Trust's importance, significant maturity gaps remain across organizations, presenting both challenges and opportunities for security leaders. Recent research indicates that while 97% of organizations report that Zero Trust has increased in priority over the past two years, only 21% of these organizations have implemented at least one Zero Trust initiative [12]. This gap between strategic intent and operational implementation highlights the complexity of Zero Trust adoption and the need for structured implementation approaches. The maturity progression varies significantly by industry, with financial services and technology sectors demonstrating the highest maturity levels while healthcare and manufacturing sectors lag in adoption [12]. Budget limitations represent the most significant barrier to Zero Trust implementation, cited by 28% of organizations, followed by competing priorities at 19% and lack of experienced staff at 17% [12]. These challenges underscore the importance of demonstrating tangible business value throughout the implementation journey, with organizations increasingly focusing on quantifiable security outcomes and operational efficiency improvements to justify continued investment in Zero Trust capabilities.

6.3 Emerging Implementation Priorities and Integration Patterns

As organizations advance their Zero Trust initiatives, clear patterns are emerging regarding implementation priorities and integration approaches. Identity-centric security capabilities represent the foundation of effective Zero Trust architectures, with 96% of organizations planning to integrate MFA across their workforce and 84% focusing on extending access control policies to APIs as key components of their strategy [12]. Server infrastructure and workloads represent the most challenging protection targets, with only 19% of organizations having fully implemented Zero Trust controls for these resources compared to 36% for APIs and 35% for web applications [12]. The implementation approach increasingly emphasizes integration between security domains, with organizations moving beyond siloed security controls toward comprehensive platforms that provide unified visibility and control. This integration trend is particularly evident in cloud environments, where the API Security segment within the Zero Trust market is expected to grow at the highest CAGR during the forecast period [11]. As implementations mature, organizations are increasingly focusing on automation and orchestration capabilities that enable dynamic policy enforcement based on real-time risk assessment, establishing the foundation for truly autonomous Zero Trust architectures that adapt continuously to changing threat landscapes and business requirements.

Technology Trend	Potential Impact on Zero Trust	Integration Opportunities	Implementation Timeline
Quantum-Resistant Cryptography	Fundamental shift in authentication and encryption foundations	Identity provider integration and certificate infrastructure	Long-term planning required with staged implementation
Edge Computing Security	Distributed enforcement points with local decision-making capabilities	Integration with IoT security frameworks and 5G infrastructure	Mid-term implementation focusing on high-value edge cases
AI-Powered Deception Technology	Enhanced threat detection through deliberate decoys and honeypots	Behavioral analytics integration for targeted deception deployment	Near-term implementation for specific high-risk environments
Decentralized Identity (DID)	User-controlled identity with blockchain verification	Federation with traditional identity providers during transition	Phased implementation starting with non-critical applications

Table 3: Emerging Technologies in Autonomous Zero Trust Ecosystems [11, 12]

7. Conclusion

Autonomous Zero Trust enforcement powered by AI-driven behavioral analytics represents the natural evolution of security architecture in an era of complex threats and distributed workforces. By moving beyond static rules to intelligent, context-aware security decisions, organizations can significantly strengthen their security posture while simultaneously reducing operational overhead and enhancing user experience. The self-adjusting nature of these systems ensures they adapt to changing behavior patterns, emerging threats, and evolving business requirements without constant manual reconfiguration. While implementation requires thoughtful planning and phased deployment, the resulting capabilities—from automated threat detection to dynamic privilege management—provide a foundation for resilient security that scales with organizational growth. As security teams increasingly face resource constraints amidst expanding attack surfaces, autonomous zero-trust approaches offer a strategic advantage by focusing human expertise on high-value security activities while allowing AI to handle continuous monitoring and enforcement. Organizations embracing this paradigm will be better positioned to meet both current and future security challenges in an increasingly complex digital landscape.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.

References

[1] Abi Tyas Tunggal, "What is the Cost of a Data Breach in 2023," UpGuard, 5 Jan. 2025. [Online]. Available: https://www.upguard.com/blog/cost-of-data-breach.
[2] Arooj Anwar, "Key Insights from the 2024 Verizon Data Breach Investigations Report," CyberPilot, 2024. [Online]. Available: https://www.cyberpilot.io/cyberpilot-blog/key-insights-from-the-2024-verizon-data-breach-investigations-report.
[3] CyberArk, "What is Machine Identity Security?" CyberArk, 2025. [Online]. Available: https://www.cyberark.com/what-is/machine-identity-security/.
[4] GlobeNewswire, "Zero Trust Security Market worth $60.7 billion by 2027, growing at a CAGR of 17.3%," Markets and Markets, 20 June 2023. [Online]. Available: https://www.globenewswire.com/news-release/2023/06/20/2691281/0/en/Zero-Trust-Security-Market-worth-60-7-billion-by-2027-growing-at-a-CAGR-of-17-3-Report-by-MarketsandMarkets.html.
[5] Grand View Research, "Zero Trust Security Market Size & Trends," Grand View Research Insight, [Online]. Available: https://www.grandviewresearch.com/industry-analysis/zero-trust-security-market-report
[6] Holger Schulze, "2023 Zero Trust Progress Report," Ivanti, 2023. [Online]. Available: https://www.ivanti.com/resources/v/doc/ivi/2776/160b264eb465.
[7] Okta, "The State of Zero Trust Security 2023," Okta, 2023. [Online]. Available: https://www.okta.com/sites/default/files/2023-09/SOZT_Report.pdf.
[8] Ponemon Sullivan Privacy Report, "Cost of Insider Risks Global Report 2023," Ponemon Institute, 2023. [Online]. Available: https://ponemonsullivanreport.com/2023/10/cost-of-insider-risks-global-report-2023/.
[9] Research and Markets, "User Entity Behavior Analytics Market - Global Industry Size, Share, Trends Opportunity, and Forecast 2018-2028," Research and Markets, Oct. 2023. [Online]. Available: https://www.researchandmarkets.com/report/entity-behavior-analytics?srsltid=AfmBOooACgMB9asB9LGeoEYIWYu5vWe98sprByakM91hXmP6pylQHpWE.

[10] Spherical Insights, "Global Identity Threat Detection and Response (ITDR) Market Insights Forecasts to 2033," Spherical Insights, 2023. [Online]. Available: https://www.sphericalinsights.com/reports/identity-threat-detection-and-response-itdr-market.
[11] The Hackers News, "Cost of Data Breach Report 2023: Insights, Mitigators and Best Practices," The Hacker News, 21 Dec. 2023. [Online]. Available: https://thehackernews.com/2023/12/cost-of-data-breach-report-2023.html.
[12] Verizon, "2024 Data Breach Investigations Report," Verizon Business, 2024. [Online]. Available: https://www.verizon.com/business/resources/T242/infographics/2024-dbir-retail-snapshot.pdf.