IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 27, Issue 6, Ser. 3 (Nov. – Dec. 2025), PP 50-64
www.iosrjournals.org

Zero Trust For Small Businesses: Practical Implementation Models For Post-Perimeter Security

Olamide Oluwasegun Oloyede

Abstract
Small and medium-sized enterprises (SMEs) in the United States face a rapidly increasing cyber threat, intensified by cloud adoption, remote work environments, and sophisticated adversarial tactics. Traditional perimeter-based security is inadequate to resolve this, particularly for resource-constrained organizations without dedicated security operations capacity. This paper presents a structured, evidence-based examination of Zero Trust Architecture (ZTA) as an attainable and strategically critical cybersecurity paradigm for SMEs. Drawing on verified academic and industry sources, it advances a phased Zero Trust adoption framework aligned with NIST SP 800-207, emphasizing identity-centric access controls, micro-segmentation, continuous authentication, and managed security service integration. Real-world case analyses across retail, fintech, and healthcare demonstrates measurable improvements in intrusion prevention, compliance readiness, and operational resilience when SMEs deploy incremental Zero Trust controls. The study also identifies key challenges including budget limitations, workforce capacity gaps, legacy technology dependencies, and ethical considerations in continuous monitoring, while proposing policy and capability-building pathways to support sustainable adoption. Synthesizing practitioner insight, empirical findings, and policy direction, the paper shows that Zero Trust is both feasible and foundational for SMEs, securing digital assets, ensuring regulatory compliance, and reinforcing economic continuity in today's U.S. business ecosystem. Future research should focus on scalable automation, adaptive maturity models, and ethical guidelines that refine Zero Trust implementation in small-enterprise ecosystems.

Keywords And Phrases: *Zero Trust Architecture (Zta), SMES, Cybersecurity, NIST SP 800-207, Identity Access Management, Micro-Segmentation, Managed Security Services, Compliance, U.S. Digital Economy, Resilience*

Date of Submission: 04-12-2025 Date of Acceptance: 14-12-2025

I. Introduction

The field of cybersecurity over the years has experienced several changes over the past decade thereby reshaping how we protect and think about our digital lives. Traditional perimeter-based defense models are proving increasingly insufficient in today's dynamic and distributed cybersecurity landscape (FNU Jimmy, 2022). These systems, once reliant on firewalls and intrusion detection at the network's edge, now face challenges as cloud computing, remote work, SaaS platforms, and hybrid environments blur traditional network boundaries. In response, Zero Trust Architecture (ZTA) has emerged as a transformative model that rejects the assumption of trusted internal traffic, instead embracing the principle of "never trust, always verify" through continuous authentication, identity-based access controls, micro-segmentation, and least-privilege enforcement (Nasiruzzaman et al., 2025).

Small and medium-sized enterprises (SMEs) are increasingly exposed to a wide range of cyber threats such as phishing, malware, data breaches, and ransomware largely due to limited resources, low cybersecurity awareness, and insufficient protective measures (Benjamin et al., 2024). Phishing continues to be the most common entry point for cyberattacks against SMEs, with the Techn22 (2024) Cyber Security Breaches Survey revealing that 83% of UK businesses that experienced a breach identified phishing as the initial attack vector, typically involving deceptive emails that lure employees into clicking malicious links or divulging sensitive information. Ransomware has likewise become a significant threat: a survey found that over 60 % of SMEs had experienced a cyber-attack in the last year (CIO World Asia, 2022). The proliferation of supply-chain attacks further amplifies exposure: a single weak vendor can compromise the networks of multiple small enterprises as expressed by Synergy Managed IT Services (2025).

SMEs typically lack the large cybersecurity infrastructure, dedicated personnel, and financial resources that larger organizations can afford, leaving them more exposed to changing digital threats. They may lack dedicated IT security teams, have constrained budgets for advanced tools, and be burdened with supporting legacy systems lacking modern security posture. As one commentary puts it, "cybercriminals see SMEs as

low-risk, high-reward targets." (Keepnet Labs, 2025). These resource constraints create a dual problem: high vulnerability and low capacity to respond or recover effectively.

In this regard, the core research problem addressed in this paper questions how small businesses can adopt Zero Trust principles effectively despite limited budgets and restricted IT or cybersecurity resources. This paper aims to present practical and scalable Zero Trust Architecture models tailored for SMEs, focusing on identity-driven access control, micro-segmentation, continuous authentication, and cloud-based security orchestration. In doing so, the paper aims to bridge the gap between enterprise-grade ZTA frameworks and the realities of resource-constrained small businesses, providing pathways for adopting strong post-perimeter security without prohibitive cost or complexity.

II. Literature Review

Evolution of cybersecurity paradigms

Historically, network security was dominated by a perimeter-based "castle-and-moat" model that relied on strong edge defenses like firewalls and IDS/IPS to block external threats while implicitly trusting internal traffic, a paradigm shaped by the assumption that cyber threats originated outside the network (CNWR, 2024; Ravi et al., 2025). The rise of cloud computing, mobile workforces, SaaS platforms, and widespread third-party integrations has steadily blurred traditional network boundaries, challenging long-held trust assumptions and driving a shift toward more adaptive security models. Cloud computing is typically categorized into three main service models which are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), each offering distinct levels of control, flexibility, and management for users (Salah et al., 2023).

The National Institute of Standards and Technology (NIST) formally articulated this paradigm shift in its Special Publication 800-207, which defines Zero Trust Architecture (ZTA) as a set of principles and deployment models that prioritise identity, device posture, and continuous verification at the centre of access decisions (Rose et al., 2020). ZTA represents a foundational transformation in cybersecurity, replacing implicit trust with continuous verification across users, devices, and networks. Guided by the principle of "never trust, always verify," it assumes that no entity—internal or external—should be automatically trusted. According to NIST SP 800-207, Zero Trust strengthens security through least-privilege access, micro-segmentation, and real-time policy enforcement (Mushtaq et al., 2025).

An empirical study of twelve large-scale organisations by Fadare (2025) reported that comprehensive ZTA adoption yielded an average 67 % reduction in overall security incidents, a 78 % decline in critical incidents requiring executive or regulatory attention, a 43 % improvement in mean time to detection (MTTD), with top performers exceeding 60 %, and up to an 87 % reduction in exploitable east-west network connections through micro-segmentation and software-defined-perimeter technologies. Multiple systematic reviews and surveys confirm that ZTA is more than a marketing construct. It constitutes an architectural re-orientation from network-centric to identity- and context-centric controls. Collectively, these studies show that ZTA integrates diverse technologies including identity and access management (IAM), Zero Trust Network Access (ZTNA), micro-segmentation, continuous monitoring, and policy orchestration into a cohesive and interoperable security posture (Dhiman et al., 2024).

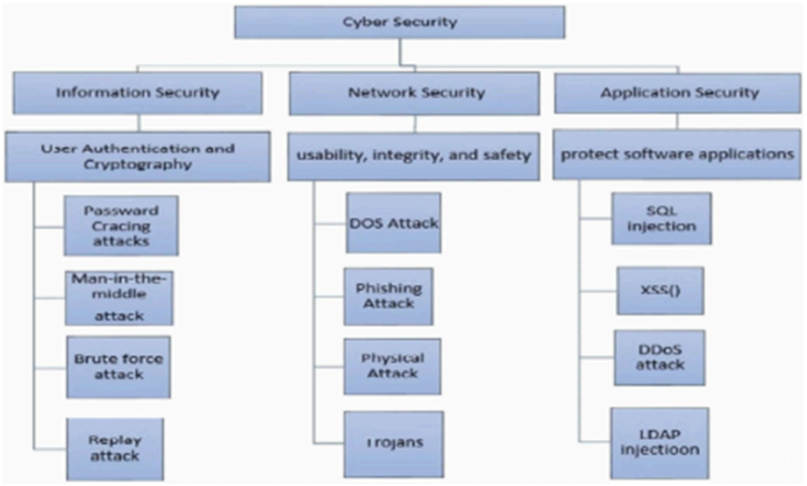

Fig. 1. Classification of cyber security with attacks

Figure 1: Classification of Cyber Security with Attacks
Source: Qureshi & Shandilya (2021)

Zero Trust fundamentals

At the conceptual core of Zero Trust Architecture (ZTA) lie several enduring principles: "never trust, always verify," least-privilege access, micro-segmentation of resources, continuous authentication and authorization, and the prioritization of identity and device posture in access decisions (Mushtaq et al., 2025). According to Microsoft Learn (2025), the Zero Trust model assumes breach and validates every access request as if it originated from an untrusted network, protecting users, devices, applications, and data regardless of location as an approach designed to reflect the realities of a mobile and cloud-centric workforce.

In practice, these principles are operationalized through controls such as strong authentication (ideally multi-factor), fine-grained authorization (role-, attribute-, or just-in-time-based), encryption of east–west traffic within data centres and cloud environments, and automated policy enforcement driven by telemetry and dynamic risk scoring. Contemporary analyses of ZTA emphasize that technology alone is insufficient, effective implementation requires stronger organizational processes, governance structures, and clearly defined migration pathways (Kang et al., 2023). Also, evolving legal and regulatory mandates are accelerating Zero Trust adoption. As noted in an IBM report by Lindemulder and Kosinski (2023), these mandates are reshaping enterprise security priorities, most notably following the 2021 Executive Order issued by U.S. President Joseph Biden, which directed all federal agencies to adopt Zero Trust Architecture as a strategic imperative.

Small business cybersecurity landscape: vulnerabilities and constraints

There is a structural imbalance in the cybersecurity readiness of SMEs, a condition where awareness is rising, yet practical capacity to defend remains severely limited. Empirical research consistently demonstrates that small and medium-sized enterprises (SMEs) experience disproportionately high exposure to cyber incidents while remaining critically underprepared to respond effectively. Marta et al. (2024) emphasize that SMEs are often constrained by limited financial resources and scarce cybersecurity expertise face mounting challenges in countering increasingly sophisticated cyber threats. Their heightened vulnerability stems from extensive reliance on third-party vendors, legacy systems, and supply chain integrations, which collectively make them appealing targets in today's hyperconnected digital economy.

Nisha et al. (2023) note that despite initiatives such as the Welsh Government's Cyber Action Plan, designed to improve SME cybersecurity awareness and resilience through funding and training, many firms continue to face persistent obstacles. These include inadequate understanding of cyber risks, difficulty accessing qualified security professionals, and the prohibitive costs of advanced defense solutions. National and cross-sectoral studies further indicate that over 40% of SMEs have suffered a successful cyberattack in recent years, while a majority admit they would struggle to maintain business continuity following a major breach (Marta et al., 2024; GOV.UK, 2023). These findings underscore the fragile operational resilience of SMEs and their attractiveness to financially motivated attackers.

Tetteh (2024) observes that SME vulnerability profiles are shaped by structural constraints, most notably the absence of dedicated IT and security staff, limited budgets, outdated or unpatched software, and heavy dependence on third-party cloud or supply-chain partners without adequate governance oversight. Such limitations manifest in tangible security gaps, including low adoption of multi-factor authentication (MFA), weak or shared credentials, minimal network segmentation, and insufficient telemetry, all of which create high-value opportunities for adversaries. Ashish et al. (2024) similarly report a pronounced disparity between recommended security controls and operational practices: nearly two-thirds of SMEs have yet to implement MFA, and despite the superior protection offered by Physical Authentication Devices (PADs), adoption remains low due to persistent usability concerns and perceived implementation complexity.

Research Gaps

The academic and standards literature on Zero Trust Architecture (ZTA) is extensive, anchored by the National Institute of Standards and Technology's Special Publication 800-207 (Rose et al., 2020), which defines core principles such as micro-segmentation, policy orchestration, and identity-centric access control. Yet, as systematic reviews observe, most studies are situated in enterprise-scale contexts, organizations with mature governance, dedicated cybersecurity teams, and established identity infrastructures. These assumptions diverge sharply from the realities of small and medium-sized enterprises (SMEs), which typically operate with constrained budgets and generalist IT staff.

Despite ZTA's theoretical maturity, its translation to SME environments remains limited. Existing research provides the conceptual "why" and "what" of Zero Trust but offers little empirical evidence on the "how" for smaller firms. Reviews consistently note a lack of resource-sensitive frameworks that adapt enterprise blueprints into lean, incremental, and affordable adoption pathways. While quantitative studies such as Zillah et al. (2022) show that Zero Trust migration can yield long-term risk reduction sufficient to justify costs when phased, the literature cautions that skills shortages, integration complexity, and upfront investment continue to hinder practical adoption in resource-limited settings.

Evidence of partial adoption and scalability challenges

A consistent pattern in the literature is that small and medium-sized enterprises (SMEs) tend to adopt discrete elements of the Zero Trust Architecture (ZTA) framework rather than deploying complete, end-to-end implementations. Kumar (2025) finds that selective adoption of Zero Trust controls enhances SME security posture by reducing attack surfaces through least-privilege access and continuous identity verification, while strengthening compliance via rigorous logging, segmentation, and secure integration of cloud platforms and mobile workforces through consistent, perimeter-independent enforcement. Similarly, Adelusi et al. (2022) argue that contemporary cybersecurity paradigms that include Zero Trust, AI-driven threat detection, Security-as-a-Service (SECaaS), decentralized identity management, and blockchain-based authentication are transforming SME defense capabilities. These innovations enable continuous authentication, real-time risk evaluation, and automated threat mitigation, yet their adoption remains constrained by the need for scalable and cost-efficient implementation models that can sustain both enterprise resilience and digital trust across rising markets.

Field studies and operational surveys show that most SMEs implement isolated Zero Trust-aligned controls such as multi-factor authentication (MFA), cloud-based identity providers (IdPs), single sign-on (SSO), and cloud-native secure web gateways, while omitting advanced practices like fine-grained micro-segmentation, continuous authorization, or centralized policy orchestration. Akharchaf (2025) emphasizes that strict identity and asset management form the nucleus of ZTA, IdPs authenticate users through MFA, issue signed tokens or certificates to policy engines, and integrate with device-management systems to ensure only compliant endpoints obtain access. Policy enforcement points (PEPs) then broker verified application sessions, while network micro-segmentation, achieved through software-defined networking (SDN) and service meshes, isolates workloads, treating each application domain as a gated enclave. Hariharan (2025) adds that in cloud environments, attackers frequently exploit IAM misconfigurations or over-privileged service accounts to move laterally toward critical assets, while however, least-privilege design, micro-segmentation, and tightly scoped IAM policies can significantly reduce these escalation pathways.

Although these piecemeal adoptions yield measurable improvements, MFA alone dramatically curtails credential-based compromises, they simultaneously expose a scalability paradox, without unified identity governance, centralized telemetry, and coordinated segmentation, residual lateral movement and misconfiguration risks persist. Dakić et al. (2025) and Owen (2025) identify recurring barriers to deeper ZTA implementation within SMEs, including user-experience friction, legacy-system incompatibilities, procurement overhead, and shortages of internal expertise. Such limitations often result in fragmented deployments and operational inefficiencies, closely mirroring the administrative complexity observed in enterprise-scale frameworks like Microsoft's Azure Zero Trust systems, where navigating multi-service control planes requires sustained technical capacity.

Synthesis and implications for this study

Evidence from existing literature shows that although SMEs are increasingly adopting Zero Trust principles, progress remains gradual and limited by cost, scalability, and cybersecurity skill constraints. The research demonstrates strong conceptual support for Zero Trust but highlights a practical adoption gap, as most guidance is oriented toward enterprise-scale capabilities rather than SME realities. While widely endorsed elements such as IAM, MFA, and cloud-native security services provide valuable building blocks, they are rarely presented as structured, stepwise roadmaps suitable for resource-constrained environments. This gap underscores the need for context-sensitive, incremental adoption models. Accordingly, this study synthesizes current insights to develop scalable and financially viable Zero Trust pathways tailored to SMEs, framing implementation as a progressive maturity journey that enables meaningful risk reduction without enterprise-level resources.

III. Methodology

This study employs an analytical and comparative research approach to evaluate the applicability of Zero Trust Architecture (ZTA) in U.S. small and medium-sized enterprises. It synthesizes established Zero Trust frameworks including NIST SP 800-207, Microsoft's Zero Trust Adoption Model, and Google's BeyondCorp paradigm to identify principles adaptable to SME environments. Primary data sources include industry threat intelligence reports and cybersecurity readiness surveys such as the Verizon Data Breach Investigations Report (DBIR) and IBM Threat Intelligence Index, alongside documented SME case studies across healthcare, fintech, and retail sectors. The evaluation framework assesses ZTA components based on cost efficiency, scalability, and integration feasibility within resource-constrained environments. The output of this study is a structured conceptual roadmap demonstrating phased, cost-aware Zero Trust adoption designed for SMEs, highlighting practical controls, service-leveraging opportunities, and measurable security outcomes.

IV. The Need For Zero Trust In The Sme Ecosystem

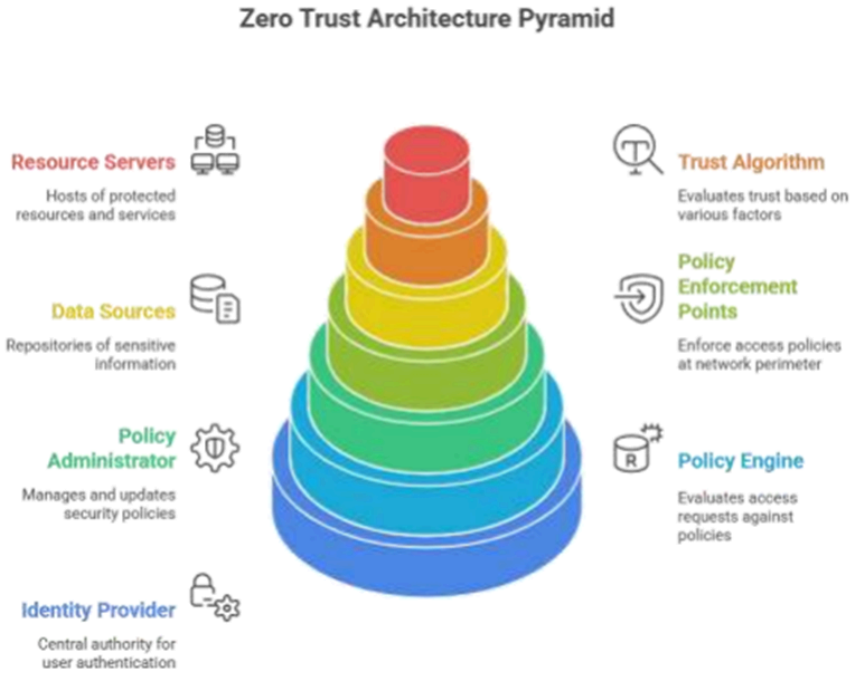

Figure 1: Zero Trust Architectural Pyramid
Source: Fadare et al., 2025

Small and medium-sized enterprises (SMEs) are increasingly exposed to a threat environment once thought to be the preserve of large organisations. Industrial analysis by Joe Ashley (2024) listed that despite 50% of UK businesses, including 18% of micro, 25% of small, and 43% of medium enterprises being targeted by cyberattacks in 2024, with approximately 612,000 firms still affected even after a slight decline from previous years, many SMEs continue to operate under the dangerous misconception that their size makes them unattractive to cybercriminals. This perception gap shows a critical behavioural and strategic vulnerability across the SME sector.

A diverse ecosystem of cybersecurity risk management frameworks such as FAIR (Factor Analysis of Information Risk), NIST SP 800, CVSS (Common Vulnerability Scoring System), TARA (Threat Analysis and Risk Assessment), OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), and CORAS (Model-based Risk Analysis of Security) offer structured methodologies for identifying, analysing, and mitigating cyber risks. These frameworks differ in focus, FAIR quantifies risk based on probability and financial impact, NIST emphasises control-based threat mitigation, CVSS prioritises vulnerability scoring, TARA focuses on threat prioritisation, OCTAVE integrates asset mapping with vulnerability assessment, and CORAS employs model-driven analysis to visualise threat scenarios (Perera et al., 2022). These frameworks provide comprehensive guidance for developing risk-informed security postures. The structural vulnerabilities of SMEs are compounded by their limited budgets, outdated systems, weak identity management, and minimal defensive layering, making them prime targets for financially motivated cyberattacks, reinforcing the need for Zero Trust frameworks that provide proportionate protection without requiring enterprise-scale resources (Tetteh, 2024).

Expanded attack surface: third-party breaches & remote work

The expansion of remote work and increased dependence on third-party vendors have significantly widened the attack surface for SMEs, as remote access tools, personal devices, and unsecured home networks frequently bypass corporate security controls, creating vulnerable entry points for cyber threats. Bispham et al. (2021) report that the rapid adoption of remote work during the COVID-19 pandemic exposed critical vulnerabilities in collaboration and video-conferencing platforms, leading to incidents such as “Zoom-bombing” and man-in-the-middle attacks. Their study found that 91% of executives observed heightened cyber threats, while 85% acknowledged that their organizations were unprepared for the shift, with secondary effects

including user data compromise, still underexamined amid rising cybercrime marketplace activity. Similarly, Bhagat (2023) noted that 70% of organizations experienced cybersecurity breaches linked to remote access technologies, with unmanaged personal devices and increased dependence on cloud infrastructure compounding vulnerabilities due to limited visibility and the complexities of shared responsibility models.

Recent cybersecurity data confirm that these risks extend deeply into third-party ecosystems. A report by BDEmerson (2024) noted that 59% of companies experienced data breaches attributable to third-party vendors or partners, and human error accounted for 95% of these incidents. The report further notes that among SMEs specifically, malware remains the most prevalent attack vector (18%), followed by phishing (17%), data breaches (16%), website hacking (15%), distributed denial-of-service (DDoS) attacks (12%), and ransomware (10%). These dynamics reveal that SMEs now function within an intricately interconnected digital ecosystem, where even minor weaknesses can escalate into systemic risks, including the need for security architectures like Zero Trust that assume breach and minimize implicit trust across networks and partners.

Financial and reputational impacts

Cyberattacks impose diverse severe consequences on small and medium-sized enterprises (SMEs), often threatening their financial viability and reputational integrity. Tetteh (2024) highlights that despite 63% of U.S. small businesses identifying as cyber intermediates and only 4% as experts, 41% suffered attacks in the past year. Ransomware alone cost victims an average of over $16,000 per incident, with only half recovering their data, phishing (53%), unpatched servers or VPNs (38%), and credential theft (29%) remain the most common entry points. In the United Kingdom, SMEs collectively lose more than £3.4 billion annually due to insufficient cybersecurity measures, with over 30% operating without any protections and more than a quarter suffering repeated attacks each year (Scroxton, 2025).

ElectroIQ (2025) projects that cybercrime will cost the global economy approximately US $10.5 trillion by 2025. Among breached businesses, 29% permanently lose customers, 42% incur direct financial losses, and 40% lose critical data, alarmingly, 60% of small businesses close within six months of a major cyber incident. Although many SMEs acknowledge reputation as a key strategic asset, 60% of UK-based SMEs have already experienced a cyber breach—illustrating a dangerous underestimation of both the likelihood and the enduring impact of such events on financial stability, customer trust, and growth potential.

For smaller firms, cyber incidents can trigger serious effects through direct and indirect losses that can range from tens to hundreds of thousands of dollars, sums far more absorbable by large enterprises than by SMEs (Marta et al., 2024). These breaches threaten the confidentiality, integrity, and availability of sensitive data, but for SMEs, the consequences go far beyond operational disruption, posing existential risks through reputational damage, customer loss, and financial strain, thereby underscoring the urgent need for scalable, architecture-based solutions like Zero Trust that align with their limited resources and heightened exposure.

Zero Trust: necessity not luxury

In today's hyperconnected threat environment, adopting a Zero Trust Architecture (ZTA) has moved from being a strategic option to a pragmatic necessity for small and medium-sized enterprises (SMEs). Zero Trust redefines contemporary cybersecurity by dismantling implicit trust within networks and enforcing the principle of "Never Trust, Always Verify", ensuring that every user, device, and application is authenticated, authorized, and continuously validated before access is granted (Rathore, 2024).

As WebNIC (2025) explains, Zero Trust eliminates perimeter-based assumptions by applying rigorous verification to all access requests, regardless of their origin or network location. In practice, this means that every interaction between entities—human or machine—is mediated through contextual policy enforcement and continuous authentication mechanisms. This approach is particularly critical in an era dominated by remote work, cloud adoption, and complex third-party ecosystems, where a single misconfigured identity or unsecured endpoint can expose entire systems.

Sophie (2025) argues that Zero Trust Architecture has become indispensable for protecting modern digital infrastructures, especially given the proliferation of remote workforces and Internet of Things (IoT) devices. However, its adoption remains hindered by technical, organizational, and financial constraints. By treating trust itself as a vulnerability, Zero Trust enforces a security posture grounded in continuous verification and least-privilege access, requiring structured implementation pathways to overcome integration and cost barriers. Zero Trust offers SMEs a sustainable path to cyber resilience by enforcing least-privilege access, continuous verification, and adaptive controls that directly counter threats like credential compromise, lateral movement, and insecure vendor links (Kumar, 2025).

V. Core Components Of Zero Trust For Small Businesses

Zero Trust Architecture (ZTA) provides SMEs with a modular, scalable security framework that can be customized to fit their specific operational needs and financial constraints, enabling practical and resilient cyber

defense (Kumar, 2025; Perera et al., 2022). Instead of relying on monolithic enterprise systems, SMEs can adopt Zero Trust incrementally through five interdependent layers which include identity-centric access control, micro-segmentation, continuous authentication, device trust, and cloud security orchestration, each reinforcing least-privilege access and contextual verification to maintain strong protection within limited resources.

Identity-Centric Access Control

Identity forms the foundation of Zero Trust security, ensuring continuous authentication, authorization, and verification before granting access to resources. Identity, Credential, and Access Management (ICAM) structures enforce secure identity lifecycle controls through authentication mechanisms including biometrics, passwords, and multi-factor tokens (Ologunde, 2025). For SMEs, the most feasible entry point into Zero Trust is adopting cloud-based IAM tools such as Microsoft Entra ID, which provides centralized identity lifecycle management, SSO, MFA, Conditional Access, and Identity Protection, with support for OAuth, SAML, and WS-Federation, delivering enterprise-grade controls without infrastructure overhead (LogicMonitor, 2024).

Zero Trust shifts IAM from static RBAC and ABAC toward continuous, context-aware access reinforced by OpenID Connect, MFA, and ML-based behavioral analytics to counter identity-driven threats (Fadare, 2025). Continuous validation is essential, as Ji et al. (2025) emphasize that every request, whether internal or external, must be re-authenticated to prevent credential misuse and lateral movement. MFA significantly reduces unauthorized access attempts, underscoring its value in SME defense strategies (Hossain & Raza, 2023). Least-privilege enforcement via RBAC and ABAC supports precise access management, with ABAC offering flexible contextual controls, though its complexity may challenge smaller businesses (Pernul et al., 2025). Cloud IAM also improves operational efficiency and user experience through automated provisioning, centralized policy enforcement, SSO, and MFA—making identity-first Zero Trust adoption financially and operationally viable for SMEs (Saeed & Jasmine, 2022).

Micro-Segmentation

Micro-segmentation divides networks into granular, isolated zones to limit lateral movement and reduce attack surfaces. Palo Alto Networks defines it as a Zero Trust–aligned model that enforces least-privilege controls between workloads and can scale down to individual virtual machines, improving breach containment and policy precision. Empirical evidence shows micro-segmentation is more effective and faster to deploy in cloud-native and microservices environments than in legacy, monolithic infrastructures, where implementation complexity and success rates vary widely (Fadare, 2025). Segmented architectures enhance resilience by isolating threats and improving defense posture, particularly in multi-tenant cloud environments like Platform-as-a-Service (Ryan and Stephen, 2025).

The Software-Defined Perimeter (SDP) extends this model through identity-based, dynamic trust provisioning, hiding resources until verification occurs and replacing static perimeter defenses (Horne, 2022). While enterprise-grade SDP systems can be costly, SMEs can adopt practical segmentation using VLANs, host-based firewalls, AWS Security Groups, and Azure Network Security Groups, making Zero Trust segmentation feasible without prohibitive investment.

Akharchaf (2025) highlights that micro-segmentation in cloud and hybrid systems relies on Policy Enforcement Points (PEPs), including API gateways and service mesh sidecars—to restrict access at the resource level. SDN and virtual network policies further create autonomous micro-enclaves that require explicit authorization. Even lightweight segmentation, such as separating user, server, and administrative subnets, substantially reduces breach propagation risk. Micro-segmentation also increases visibility into east–west traffic, allowing SMEs to detect anomalies and contain threats before escalation (Adudotla, 2025).

Continuous Authentication and Verification

Continuous authentication builds on least-privilege principles by verifying user identity, context, and behavior throughout the session rather than relying on a single login event. Hussain (2025) notes that behavioral biometrics and contextual intelligence now enable real-time anomaly detection, preventing unauthorized access even after initial authentication. Advances in AI and behavioral analytics assess device posture, geographic activity, historical patterns, and contextual signals to identify insider threats or credential misuse, with machine learning and deep learning models providing adaptive behavioral profiling (Smith et al., 2025).

This model closes security gaps left by static MFA, which validates only at login. Yakushkin (2022) highlights that continuous verification correlates anomalies during the session with contextual activity to mitigate post-login compromise risks. Deep learning techniques outperform traditional methods in insider threat detection, Nasir et al. (2021) demonstrate that frameworks such as LSTM-CNN, XGBoost, Improved Hidden Markov Models, and Random Forests analyze behavioral logs and temporal sequences to flag deviations, while systems like Insider Catcher exemplify high-precision DL-driven threat monitoring.

For SMEs, continuous authentication is increasingly attainable through adaptive cloud services. Microsoft Entra ID Protection offers real-time risk-based detections and dynamic access enforcement

(Microsoft, 2025), while Google BeyondCorp Enterprise enables context-aware verification with phishing-resistant controls integrated across user sessions (Goodison, 2021). These cloud-native services allow SMEs to embed continuous, behavior-driven identity assurance without on-premises complexity, aligning with Zero Trust by ensuring validation persists throughout every interaction.

Figure 2: Insider Attack Motivations
Source: Nasir et al., (2021)

Device Trust and Endpoint Protection

In Zero Trust environments, every endpoint is untrusted until verified, requiring continuous assessment of device integrity, patch levels, and configuration compliance (Lund et al., 2024). NIST SP 800-161 Revision 1 outlines supply-chain security risks such as counterfeit components and embedded malicious code, noting persistent visibility gaps in vendor practices and downstream device integrity challenges (Olzak, 2025). Zero Trust implementation in hybrid and multi-cloud infrastructures increasingly uses machine learning to refine Conditional Access and contextual verification, enabling adaptive device trust that aligns with continuous authentication principles (Dakić et al., 2025).

For SMEs, device trust is achievable through accessible EDR platforms such as SentinelOne, CrowdStrike Falcon Go, and Microsoft Defender for Business, which offer automated patching, ransomware recovery, behavioral analytics, and integration with identity systems (Ron Samson, 2025). Automated patching remains essential, as Ahmadi et al. (2023) show it mitigates exploitable vulnerabilities frequently seen in small-business attacks. For organizations with limited internal expertise, MDR services provide continuous monitoring and incident response without the cost of dedicated SOCs (Cynet, 2025). These mechanisms operationalize the Zero Trust principle of explicit verification by continuously validating endpoint posture—across laptops, mobile devices, and IoT nodes, thereby strengthening breach containment and enabling SMEs to sustain strong security within constrained budgets.

Cloud Security Orchestration

Cloud Security Orchestration, Automation, and Response (SOAR) platforms centralize security controls across hybrid and multi-cloud environments, enabling SMEs to streamline detection, automate routine defense actions, and accelerate incident response, reducing downtime and security spending. IBM (2025) shows that containing breaches within 200 days lowers costs by 23%, highlighting the financial value of rapid response.

Modern SaaS-based SOAR solutions such as Palo Alto Cortex XSOAR and Microsoft Sentinel integrate automated detection, response playbooks, and compliance reporting for enterprise-grade protection (Sentinel One, 2025). Empirical findings confirm that SOAR deployment enhances response speeds, operational

efficiency, and regulatory alignment in cloud settings through automated workflows and tool orchestration (Peterson et al., 2023).

Machine-learning-enabled SOAR continues to evolve toward predictive defense, though hybrid environments still face challenges around data residency and cross-platform communication. As Vemula (2023) notes, security controls like cloud firewalls and automated detection tools often suffer from provider-specific limits, making orchestration crucial for consistent visibility and policy enforcement. Compared with traditional on-prem SIEM systems, cloud-based orchestration delivers faster response cycles and lower total cost of ownership (Amisha, 2024). For SMEs, lightweight SOAR deployments offer a cost-efficient path to continuous security monitoring, automation-driven resilience, and compliance with regulations such as GDPR, PCI-DSS, and SOC 2.

VI. Implementation Models And Frameworks

To effectively implement Zero Trust Architecture (ZTA) in small and medium-sized enterprises (SMEs), a flexible and context-specific approach is required. While the core principle of Zero Trust "never trust, always verify" remains constant, organizations vary in their infrastructure maturity, cloud adoption level, and security resources. Accordingly, three primary models have become viable pathways for SMEs, these models include Cloud-Native Zero Trust Adoption Model, the Hybrid Zero Trust Framework, and the Managed Security Service Model. Each represents a different balance of control, scalability, and cost efficiency, yet all follow a phased implementation structure through Assessment → Integration → Optimization.

Model 1: Cloud-Native Zero Trust Adoption

Verma (2025) defines Zero Trust Architecture (ZTA) as essential for securing cloud-native environments through continuous, adaptive verification of users, devices, and services to counter identity-driven threats and secret-management risks. The model adopts microservices-aware security, shift-left practices, and AI-enhanced intelligence to support scalable, compliant protection without compromising cloud agility. This Cloud-Native Zero Trust Adoption Model operationalizes Zero Trust through existing SaaS and Identity and Access Management (IAM) platforms, avoiding heavy capital expenditure. As Nalla (2024) notes, identity forms the core, enforcing "never trust, always verify" through ongoing authentication, dynamic authorization, and credential lifecycle controls. Combined with least-privilege access and behavioral policies, these tools reduce attack exposure and mitigate credential abuse.

The model aligns closely with SME needs, especially those using Microsoft Azure, AWS, and Google Cloud, where native IAM services enable granular identity-driven access (Alkhatib et al., 2025). Core features such as Azure Conditional Access and AWS Identity Center deliver continuous verification, adaptive authorization, and device-compliance enforcement. Peterson et al. (2023) emphasize that identity-centric controls limit lateral movement, while orchestration platforms like Microsoft Sentinel automate policy refinement and incident response. MFA, device telemetry, and just-in-time (JIT) privileges reinforce context-aware trust across sessions. For SMEs, this approach optimizes cost and operational efficiency by relying on SaaS-based orchestration instead of on-premise architectures, reducing complexity and infrastructure burden (Vemula, 2023; Amisha, 2024). Ultimately, it supports a scalable, identity-first Zero Trust posture that adapts to threat dynamics while enabling enterprise-grade security without disruptive restructuring or high expense.

Model 2: Hybrid Zero Trust Framework

The Hybrid Zero Trust Framework integrates legacy on-premises systems with cloud-native identity, orchestration, and policy enforcement, allowing SMEs to modernize securely without disrupting mission-critical ERP systems, Active Directory domains, or custom legacy applications. Microsoft (2024) highlights that hybrid environments increase the attack surface, making unified Zero Trust design critical for protecting data and communication across cloud and on-premise resources. Evidence supports the value of hybrid Zero Trust in distributed work structures. Zohaib et al. (2024), in a review of 86 studies, show that ZT-VPN models strengthen performance and security in hybrid and remote settings through granular access, continuous validation, and context-driven role-based controls, with dynamic routing and session-aware inspection improving latency and resilience against advanced threats.

The model embeds Zero Trust across hybrid stacks via micro-segmentation, identity federation, and secure API mediation. Micro-segmentation restricts lateral movement and enables east-west traffic monitoring, while identity federation connects on-premises directories to cloud IAM platforms, enabling unified authentication, Conditional Access, and adaptive authorization (Amisha, 2024; LogicMonitor, 2024; Akharchaf, 2025). SDPs and CASBs add encryption, least-privilege enforcement, and visibility across hybrid applications (Hornes, 2022; Check Point Software Technologies, 2023). IBM (2025) reports that firms adopting Zero Trust in hybrid systems achieve higher breach-containment and lower incident costs due to unified policies and

telemetry-driven risk evaluation. However, achieving maturity requires careful coordination to manage interoperability, identity sprawl, and latency through phased modernization, legacy hardening, and continuous monitoring to adapt trust boundaries as environments evolve.

Model 3: Managed Security Service Model

The Managed Security Service Model enables SMEs to implement Zero Trust by outsourcing core security operations to managed service providers, avoiding the cost and expertise required to build internal SOC capabilities. MSSPs oversee identity governance, endpoint and network monitoring, threat detection, and incident response, aligning their services with key Zero Trust principles such as continuous verification and least-privilege access (Marinos et al., 2025). Subscription-based delivery gives SMEs access to enterprise-grade tools and automation, including platforms such as Cortex XSOAR and SentinelOne-enabled MDR services, which integrate identity-centric controls, AI-driven anomaly detection, and rapid response orchestration (SentinelOne, 2025). This model is particularly beneficial for SMEs facing technical and staffing limitations, as it provides 24/7 surveillance, proactive threat hunting, and compliance alignment without expanding internal security teams. However, success depends on rigorous vendor governance, clear shared-responsibility frameworks, and contractual guarantees covering data stewardship, regulatory compliance, and incident reporting. When properly managed, MSS-driven Zero Trust adoption offers scalable, intelligence-based security maturity and cost-efficient resilience for SMEs operating in dynamic threat environments.

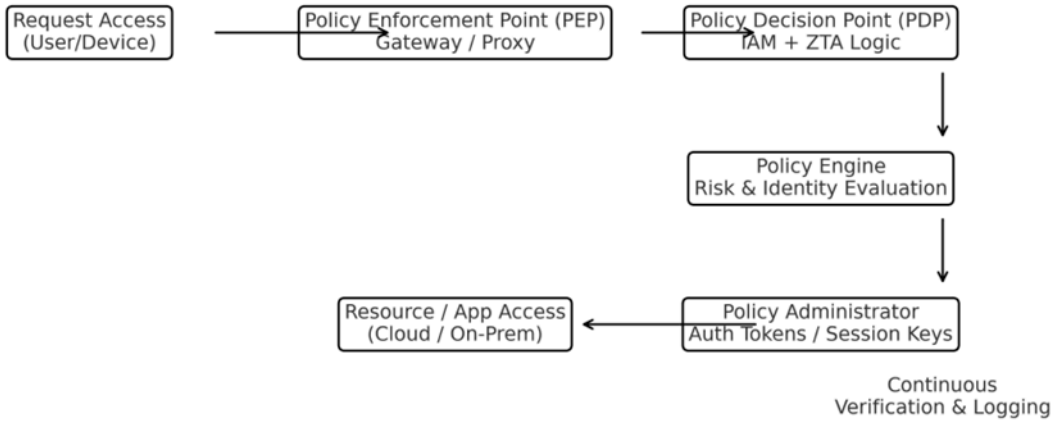

Figure 3: NIST SP 800-207-aligned Zero Trust flowchart

VII. Case Studies

While comprehensive public case-studies of full Zero Trust Architecture (ZTA) adoption in SMEs remain limited, several reports and practitioner white-papers illustrate how smaller organisations have implemented partial or full ZTA measures with measurable results.

Kumar (2025) highlights how SMEs are adopting identity-centric Zero Trust strategies such as multi-factor authentication (MFA), micro-segmentation, and continuous authentication by focusing on account security, lateral movement restriction, and context-aware access enforcement. These incremental measures have led to fewer intrusion attempts and improved operational continuity during suspicious events, demonstrating that identity governance and segmentation can significantly enhance cyber resilience in resource-constrained environments. Supporting this, Lookout's Continuous Conditional Access (CCA) highlights how unified telemetry involving correlating device health, user behavior, and cloud-app access enables dynamic risk evaluation and real-time enforcement, as illustrated by an incident where a risky mobile app triggered immediate data access denial and remediation instructions. Similarly, the integration of Okta Identity Cloud with LogRhythm SIEM reveals how combining identity logs with behavioral analytics can detect insider threats, improve detection times, and automate forensic visibility, offering SMEs enterprise-grade Zero Trust monitoring without the need for a dedicated security operations center.

Anurag Agrawal (2024) vendor-ecosystem survey shows that small and mid-market firms adopting Zero Trust report stronger compliance readiness, smoother audit preparation, and clearer vendor-risk governance. Revealing a maturity gradient where small businesses deploy Zero Trust reactively to reduce endpoint threats and respond to incidents, while core mid-market firms balance compliance and hybrid-IT risks, and upper-mid-market firms emphasise proactive data protection and breach prevention. Techaisle's research reveals that Zero Trust (ZT) awareness and perceived importance vary significantly by organization size, with

only 8% of small businesses familiar with ZT and just 29% considering it more than moderately important, compared to 46% awareness and 90%–93% importance ratings among core and upper midmarket firms. While 30% of upper midmarket organizations are actively engaged in ZT access projects, 45% of small businesses have no immediate plans, though deployment rates still show momentum across segments—86% in upper midmarket, 69% in core midmarket, and 42% among small businesses. The findings demonstrate a tangible cultural shift toward preventative security, often accelerated through Zero Trust-XDR synergies and continuous verification practices.

Meegle (2024) presents three compelling cases illustrating the practical benefits of Zero-Trust security for small and mid-sized organizations. A small retail business fortified its payment environment with MFA, network segmentation, encryption, and device access controls, successfully thwarting a ransomware attack shortly after deployment highlighting the effectiveness of layered Zero-Trust defenses in protecting transactional systems. A mid-sized marketing agency, operating with a distributed workforce, adopted Zero-Trust measures including MFA, endpoint security, and behavioral monitoring, resulting in a marked reduction in phishing incidents and improved resilience in remote operations. Meanwhile, a private healthcare clinic implemented role-based access and real-time activity monitoring to secure electronic health records, enabling early detection and mitigation of insider threats, and demonstrating the critical role of Zero-Trust in safeguarding sensitive data within compliance-driven sectors.

Cross-Sector References & Outcomes

In the healthcare SME-clinic segment, Zero-Trust Security for Resource-Constrained SMEs and Healthcare Providers documents how small medical practices deployed network segmentation, access governance, and continuous activity monitoring to safeguard electronic patient records. Luna (2025) reports measurable reductions in unauthorized internal access attempts and enhanced audit traceability, illustrating how Zero-Trust controls reinforce confidentiality and regulatory accountability in resource-limited clinical environments. This shift has been driven by the growing targeting of SMEs and healthcare providers by cybercriminals who exploit limited cybersecurity capacity, exposing the insufficiency of perimeter-based defenses and accelerating the adoption of Zero-Trust Security (ZTS). While effective, ZTS implementation remains constrained by financial and technical barriers that make comprehensive adoption appear complex for smaller healthcare operators.

In the fintech SME-startup, individual implementations are less frequently disclosed due to regulatory confidentiality. However, guidance from the Cloud Security Alliance indicates that rising financial-technology firms have accelerated compliance readiness for frameworks such as PCI-DSS and SOC 2 by deploying identity-centric controls, multi-factor authentication (MFA), and real-time security telemetry. Blockchain adoption further shapes fintech security posture by enabling secure and transparent transaction mechanisms, yet introducing risks tied to smart-contract vulnerabilities and transactional anonymity. Ajayi et al. (2025) note that privacy-preserving innovations such as multi-signature authentication and zero-knowledge proofs are strengthening regulatory compliance and cybersecurity resilience in blockchain-based systems. Complementarily, industry commentary emphasizes that AI-driven security automation, Zero-Trust frameworks, and quantum-resistant encryption are emerging as strategic levers that enable cybersecurity startups to enhance threat intelligence, attract investment, and align security solutions with global resilience imperatives (Female Switch, 2025). In this dual healthcare and fintech SME environments, Zero-Trust measures have supported earlier detection of credential misuse, reduced audit preparation times, and promoted a transition from reactive defense to proactive cyber-governance cultures.

Professional Insight

Drawing Practical field experience with SMEs shows that successful Zero Trust adoption hinges on incremental execution and business-aligned implementation. Beginning with identity and device trust, strong identity proofing, adaptive authentication, and verified endpoint posture, enables SMEs to build security maturity without operational strain before advancing to segmentation, granular authorization, and automation. Positioning Zero Trust as a business resilience strategy rather than a purely technical initiative is equally critical. As emphasized by Microsoft (2025), framing Zero Trust around continuity, supply-chain integrity, and regulatory strength ensures leadership buy-in and aligns security with enterprise value.

Cloud-based and managed security services function as key accelerators for resource-constrained SMEs, enabling adoption of enterprise-grade IAM, endpoint protection, and managed detection without capital-intensive investment. This model supports predictable spending and faster deployment. Success must be measurable, reflected in metrics such as reduced privileged access exposure, enhanced threat detection speed, limited lateral movement, and fewer audit exceptions. Supply-chain risk warrants urgent attention as SMEs depend extensively on third-party providers, making it essential to extend Zero Trust principles, least privilege, continuous verification, and segmentation to vendor access for comprehensive protection. Lastly, organizational

culture underpins technical controls, making ongoing workforce training and reinforcement of least-privilege behavior indispensable to sustain Zero Trust maturity.

VIII. Challenges And Limitations

Despite growing momentum toward Zero Trust adoption among SMEs, several constraints continue to hinder full and sustainable implementation. Financial limitations remain one of the most significant barriers, as many small organisations struggle to allocate sustained budgets for identity-security platforms, device-trust systems, and advanced monitoring tools required to safeguard against cyberattacks (Marta et al., 2024). These pressures are compounded by a shortage of skilled cybersecurity personnel, forcing SMEs to choose between investing in critical security capability development or maintaining day-to-day business operations (Ejaz et al., 2024). Technical integration challenges further complicate adoption, particularly where legacy IT systems lack compatibility with granular access controls and continuous authentication mechanisms, this often necessitates phased upgrades or middleware solutions, increasing implementation complexity and timelines. Integrating new digital infrastructure with outdated systems can also weaken operational efficiency, as fragmented connectivity between platforms elevates both security and cost burdens (Bradač & Huđek, 2023). A persistent misconception that Zero Trust is excessively complex or resource-intensive discourages many SMEs from engaging in early, structured planning, leading instead to reactive cybersecurity practices. Reliance on cloud-delivered security services can additionally expose SMEs to vendor lock-in risks, where critical identity and monitoring functions become overly dependent on single providers, reducing operational flexibility and increasing long-term switching costs. Data confidentiality presents another formidable challenge, as insufficient access controls, weak encryption, and reliance on insecure third-party systems make adherence to regulatory obligations such as GDPR and PCI DSS more difficult, particularly for cross-border SMEs in sensitive sectors like healthcare (Isabirye, 2024). While continuous monitoring remains central to Zero Trust, it introduces ethical and privacy concerns, SMEs must carefully balance behavioural analytics and verification with transparent governance, employee trust, and compliance with data-protection frameworks to avoid disproportionate surveillance practices. Taken together, these limitations underscore the need for phased implementation, strategic vendor management, and capability development to support effective and lasting Zero Trust maturity within resource-constrained SME environments.

IX. Policy Recommendations And Strategic Pathways

Strengthening Zero Trust adoption among SMEs requires coordinated policy design and cross-sector collaboration. Public-private partnerships should expand subsidized cybersecurity training, certifications, and financial incentives to help small enterprises build resilient digital infrastructures, mitigate evolving cyber threats, and support leadership alignment toward performance gains in the digital economy (Olaosegba et al., 2024). U.S. federal agencies should further translate NIST SP 800-207 guidance into a simplified, tiered Zero Trust maturity framework tailored to SMEs, supported by streamlined reporting criteria to reduce compliance complexity and enhance implementation feasibility.

Promoting AI-enabled security automation through innovation grants, marketplace validation programs, and vendor-neutral evaluation platforms can reduce operational burdens by equipping SMEs with trusted tools for identity assurance, anomaly detection, and incident response. Consistent with ENISA's guidance for SMEs, which emphasizes workforce readiness, secure processes, and strong technical safeguards, including access controls, timely software patching, cloud adoption, and structured incident response planning (ENISA, 2021), ethical oversight and transparency must accompany automation to avoid excessive monitoring and preserve stakeholder trust. A phased SME cybersecurity maturity roadmap prioritizing identity and device trust, progressive segmentation, cloud-based security services, and measurable risk-reduction outcomes will support a transition from reactive defense to proactive cyber resilience, enabling sustainable Zero Trust adoption across the U.S. SME ecosystem.

X. Conclusion

Zero Trust has evolved from an enterprise-centric concept into a practical, essential security strategy for SMEs operating in an increasingly aggressive cyber environment. Its implementation strengthens digital asset protection, customer confidence, and business continuity. This study shows that phased adoption, hybrid deployment models, and managed service integration enable SMEs to enhance security without overwhelming financial or operational demands. Evidence demonstrates that even partial Zero Trust maturity delivers measurable gains, including reduced intrusion success, improved compliance readiness, and greater operational resilience.

The study's core insight emphasizes that SME-aligned Zero Trust programs are most effective when anchored in identity-first controls, progressive network segmentation, automated continuous monitoring, and cloud-orchestrated security services. These approaches not only reduce cyber risk but also support strategic

independence by helping SMEs safeguard data, maintain customer trust, and remain competitive in regulated and data-driven markets. Meaningful scaling, however, requires policy support through skills-building initiatives, simplified compliance pathways, and innovation in AI-enabled security tools.

Future research should prioritize adaptive Zero Trust frameworks tailored to SME realities, including legacy technology constraints, distributed workforces, and cloud-first models. Continued examination of cost-efficient implementation, ethical monitoring guidelines, and interoperable automation will enable more inclusive and realistic adoption pathways. Ultimately, Zero Trust is both a technical architecture and a governance philosophy that transforms SMEs from reactive defenders into proactive, resilient participants in the digital economy.

Reference

[1]. Adelusi, Bamidele & Uzoka, Abel & Ojika, Favour. (2022). Advances In Cybersecurity Strategy And Cloud Infrastructure Protection For Smes In Emerging Markets. Journal Of Frontiers In Multidisciplinary Research. 03. 467-482. 10.54660/.JFMR.2022.3.1.467-482.

[2]. Adudotla, Poorna Chandra Reddy. (2025). Employing Micro-Segmentation For Securing Multi-Tenant Cloud Environments.

[3]. Ahmadi Mehri, Vida & Arlos, Patrik & Casalicchio, Emiliano. (2023). Automated Patch Management: An Empirical Evaluation Study. 10.1109/CSR57506.2023.10224970.

[4]. Ajayi, Olanrewaju & Alozie, Chisom & Abieba, Olumese & Akerele, Joshua & Collins, Anuoluwapo. (2025). Blockchain Technology And Cybersecurity In Fintech: Opportunities And Vulnerabilities. 11. 1334-1345.

[5]. Akharchaf, Youssef. (2025). Zero Trust Architecture In Cloud Security: Challenges And Implementation. 10.13140/RG.2.2.26671.04000.

[6]. Alkhatib, Ahmad & Shaheen, Ameen & Albustanji, Rand. (2025). A Comparative Analysis Of Cloud Computing Services: AWS, Azure, And GCP. International Journal Of Computing And Digital Systems. 18. 1-15. 10.12785/Ijcds/1571111846.

[7]. Amisha Sinha. (2024). Challenges And Best Practices For Integrating Security Orchestration, Automation, And Response (SOAR) Platforms With Cloud Infrastructure Creative Component Master Of Science In Information Systems. Https://Dr.Lib.Iastate.Edu/Server/Api/Core/Bitstreams/48ab713c-0f6c-472a-9564-9d6bee1b394b/Content

[8]. Anurag Agrawal. (2024). Zero Trust Adoption In The SMB And Midmarket: Drivers, Challenges, And Partner Ecosystem. Techaisle Https://Techaisle.Com/Blog/552-Zero-Trust-Adoption-In-The-Smb-And-Midmarket-Drivers-Challenges-And-Partner-Ecosystem

[9]. Ashish Nanda, Jongkil Jay Jeong, Syed Wajid Ali Shah, Mohammad Nosouhi, Robin Doss. (2024). Examining Usable Security Features And User Perceptions Of Physical Authentication Devices. Computers & Security, Volume 139, 103664, ISSN 0167-4048. Https://Doi.Org/10.1016/J.Cose.2023.103664.

[10]. Assion K. Tetteh. (2024). Cybersecurity Needs For Smes. Issues In Information Systems Volume 25, Issue 1, Pp. 235-246, 2024 235 DOI: Https://Doi.Org/10.48009/1_Iis_2024_120

[11]. Bdemerson. (2024). Small Business Cybersecurity Statistics. Https://Www.Bdemerson.Com/Article/Small-Business-Cybersecurity-Statistics

[12]. Benjamin, Lucky & Adegbola, Ayodeji & Amajuoyi, Prisca & Adegbola, Mayokun & Adeusi, Kudirat. (2024). Digital Transformation In Smes: Identifying Cybersecurity Risks And Developing Effective Mitigation Strategies. Global Journal Of Engineering And Technology Advances. 19. 134-153. 10.30574/Gjeta.2024.19.2.0084.

[13]. Bhagat, Nikhil. (2023). Cybersecurity In A Remote Work Era: Strategies For Securing Distributed Workforces. Journal Of Mathematical & Computer Applications. 1-5. 10.47363/JMCA/2023(2)E137.

[14]. Bispham, Mary & Creese, Sadie & Dutton, William & Esteve-Gonzalez, Patricia & Goldsmith, Michael. (2021). Cybersecurity In Working From Home: An Exploratory Study. SSRN Electronic Journal. 10.2139/Ssrn.3897380.

[15]. Bradač Hojnik, B., & Hudek, I. (2023). Small And Medium-Sized Enterprises In The Digital Age: Understanding Characteristics And Essential Demands. Information, 14(11), 606. Https://Doi.Org/10.3390/Info14110606

[16]. Check Point Software Technologies. (2023). CASB Vs. ZTNA: What's The Difference And Which Is Better For Zero Trust? Https://Sase.Checkpoint.Com/Blog/Zero-Trust/Casb-Vs-Ztna

[17]. CIO World Asia. (2023). Over 60% Of Smes Are At Risk For A Ransomware Attack. Https://Cioworldasia.Com/2023/06/27/Over-60-Of-Smes-Are-At-Risk-For-A-Ransomware-Attack

[18]. CNWR. (2024). From Castle And Moat To Zero Trust: A Paradigm Shift In Cybersecurity. Https://Cnwr.Com/Blog/From-Castle-And-Moat-To-Zero-Trust-A-Paradigm-Shift-In-Cybersecurity?Hs_Amp=True

[19]. Cynet. (2025). MDR Service Vs. In-House SOC: Finding The Right Approach. Cynet. Https://Www.Cynet.Com/Mdr/Mdr-Service-Vs-In-House-Soc-Finding-The-Right-Approach/

[20]. Dakić, V., Morić, Z., Kapulica, A., & Regvart, D. (2025). Analysis Of Azure Zero Trust Architecture Implementation For Mid-Size Organizations. Journal Of Cybersecurity And Privacy, 5(1), 2. Https://Doi.Org/10.3390/Jcp5010002

[21]. Dhiman P, Saini N, Gulzar Y, Turaev S, Kaur A, Nisa KU, Hamid Y. A Review And Comparative Analysis Of Relevant Approaches Of Zero Trust Network Model. Sensors (Basel). 2024 Feb 19;24(4):1328. Doi: 10.3390/S24041328. PMID: 38400486; PMCID: PMC10892953.

[22]. Ejaz, Umair & Gimah, Mathew & Iseal, Sheed. (2024). Cybersecurity Talent Shortage In Smes: Innovative Approaches To Recruitment And Retention.

[23]. Electroiq. (2025). Small Business Cyber Attack Statistics. Https://Electroiq.Com/Stats/Small-Business-Cyber-Attack-Statistics/

[24]. European Union Agency For Cybersecurity (ENISA). (2021). Cybersecurity For Smes: Challenges And Recommendations. Https://Www.Enisa.Europa.Eu/Sites/Default/Files/Publications/ENISA%20Report%20-%20Cybersecurity%20for%20SMES%20Challenges%20and%20Recommendations.Pdf

[25]. Female Switch. (2025). Cybersecurity Startups: Top Trends And Opportunities. Https://Www.Femaleswitch.Com/Playbook/Tpost/Yacsj9n991-Cybersecurity-Startups-Top-Trends-And-Op

[26]. FNU Jimmy.. (2022). Zero Trust Security: Reimagining Cyber Defense For Modern Organizations. International Journal Of Scientific Research And Management (IJSRM), 10(04), 887-905. Https://Doi.Org/10.18535/Ijsrm/V10i4.Ec11

[27]. Goodison, D. (2021). Google Cloud Unveils New Beyondcorp Zero Trust Security Platform. CRN. Https://Www.Crn.Com/News/Cloud/Google-Cloud-Unveils-New-Beyondcorp-Zero-Trust-Security-Platform

[28]. GOV.UK. (2023). Cyber Security Breaches Survey 2023. Department For Science, Innovation And Technology (2023). Https://Www.Gov.Uk/Government/Statistics/Cyber-Security-Breaches-Survey-2023/Cyber-Security-Breaches-Survey-2023

[29]. Hariharan, Ramanan. (2025). Zero Trust Security In Multi-Tenant Cloud Environments. Journal Of Information Systems Engineering And Management. 10. 623-644. 10.52783/Jisem.V10i45s.8899.

[30]. Himmat Rathore. (2024). Zero Trust Frameworks: Redefining Perimeter Security For Decentralized Networks. IRE Journals | Volume 7 Issue 9 | ISSN: 2456-8880

[31]. Horne, Dwight. (2022). Leveraging Software Defined Perimeter (SDP), Software Defined Networking (SDN), And Virtualization To Build A Zero Trust Testbed With Limited Resources.

[32]. Hossain, Mohammad & Raza, Md Adil. (2023). Exploring The Effectiveness Of Multifactor Authentication In Preventing Unauthorized Access To Online Banking Systems. SSRN Electronic Journal. 1. 8-12. 10.2139/Ssrn.5207142.

[33]. Hussain, Shafiq. (2025). Behavioral Biometrics And Continuous Authentication In Cybersecurity Systems. 10.13140/RG.2.2.35971.41763.

[34]. IBM. (2025). What Is SOAR (Security Orchestration, Automation And Response)? IBM. Https://Www.Ibm.Com/Think/Topics/Security-Orchestration-Automation-Response

[35]. Isabirye, Edward. (2024). Cloud Adoption And Digital Transformation Cybersecurity Consideration For Smes. IRE Transactions On Engineering Management. Volume 7 Issue 10.

[36]. Ji, E. , Jin, J. And Zhang, Q. (2025) The Evolution Of Cloud Security Frameworks: Identity Management And Zero Trust Implementation In Distributed Systems. Journal Of Computer And Communications, 13, 1-13. Doi: 10.4236/Jcc.2025.137001.

[37]. Joe Ashley (2024). Cyber Attacks And Smes. Focus Group. Https://Focusgroup.Co.Uk/Resources/Blog/Cyber-Attacks-And-Smes/

[38]. Kang H, Liu G, Wang Q, Meng L, Liu J. (2023). Theory And Application Of Zero Trust Security: A Brief Survey. Entropy (Basel). 2023 Nov 28;25(12):1595. Doi: 10.3390/E25121595. PMID: 38136475; PMCID: PMC10742574.

[39]. Keepnet Labs. (2025). Why Smes Are Prime Targets For Ransomware & How To Protect Against Attacks. Https://Keepnetlabs.Com/Blog/Ransomware-And-Smes

[40]. Kehinde Olakunle Fadare (2025). Optimizing Data Center Security With Zero Trust Architecture, International Journal Of Engineering And Advanced Technology Studies, 13 (3), 71-96. : Https://Doi.Org/10.37745/Ijeats.13/Vol13n37196

[41]. Kumar, Prince. (2025). Zero Trust Architecture For Sme Cybersecurity: Enhancing Resilience In The Digital Transformation Era. International Journal Of Progressive Research In Engineering Management And Science. Vol 5. 2791-2819.

[42]. Lindemulder, G., & Kosinski, M. (2025). What Is Zero Trust? IBM Think. Https://Www.Ibm.Com/Think/Topics/Zero-Trust

[43]. Logicmonitor. (2024). What Is Microsoft Entra ID (Formerly Azure Active Directory?) Https://Www.Logicmonitor.Com/Blog/What-Is-Azure-Active-Directory#:~:Text=Microsoft%20Entra%20ID%2C%20formerly%20known,Holistic%20approach%20to%20identity%20management.

[44]. Lund, B. D., Lee, T.-H., Wang, Z., Wang, T., & Mannuru, N. R. (2024). Zero Trust Cybersecurity: Procedures And Considerations In Context. Encyclopedia, 4(4), 1520-1533. Https://Doi.Org/10.3390/Encyclopedia4040099

[45]. Marinos, Louis & Nasi, Greta & Portesi, Silvia. (2025). MSS MARKET ANALYSIS: An Analysis Of The Managed Security Service Market. 10.2824/7566738.

[46]. Marta F. Arroyabe, Carlos F.A. Arranz, Ignacio Fernandez De Arroyabe, Juan Carlos Fernandez De Arroyabe. (2024). Revealing The Realities Of Cybercrime In Small And Medium Enterprises: Understanding Fear And Taxonomic Perspectives. Computers & Security, Volume 141, 103826, ISSN 0167-4048. Https://Doi.Org/10.1016/J.Cose.2024.103826.

[47]. Meegle. (2024). Zero-Trust Security For Small Businesses. Https://Www.Meegle.Com/En_Us/Topics/Zero-Trust-Security/Zero-Trust-Security-For-Small-Businesses

[48]. Mercy, Olaosegba & Bayya, Anil Kumar & Ejjami, Rachid & Mansour, Fedaa. (2024). The Role Of Public-Private Partnerships In Enhancing SME Cyber Security.

[49]. Mia Luna. (2025). Zero-Trust Security For Resource-Constrained Smes And Healthcare Providers: Implementing Robust Protection On A Limited Budget.

[50]. Microsoft. (2024). Improving Hybrid Cloud Security With A Zero Trust Framework. Microsoft. Https://Www.Microsoft.Com/En-Us/Microsoft-365/Business-Insights-Ideas/Resources/Improving-Hybrid-Cloud-Security-With-A-Zero-Trust-Framework

[51]. Microsoft. (2025). Identity Protection Risk Detections In Microsoft Entra ID. Microsoft Learn. Https://Learn.Microsoft.Com/En-Us/Entra/Id-Protection/Concept-Identity-Protection-Risks

[52]. Microsoft. (2025). What Is Zero Trust? Microsoft Learn. Https://Learn.Microsoft.Com/En-Us/Security/Zero-Trust/Zero-Trust-Overview

[53]. Microsoft. (2025). Zero Trust Adoption Framework Overview. Microsoft Learn. Https://Learn.Microsoft.Com/En-Us/Security/Zero-Trust/Adopt/Zero-Trust-Adoption-Overview

[54]. Mushtaq, S., Mohsin, M., & Mushtaq, M. M. (2025). A Systematic Literature Review On The Implementation And Challenges Of Zero Trust Architecture Across Domains. Sensors, 25(19), 6118. Https://Doi.Org/10.3390/S25196118

[55]. Nalla, Kiran. (2024). Building Zero-Trust Security Models In Cloud Environments: Best Practices For Enterprises. World Journal Of Advanced Engineering Technology And Sciences. 11. 424-436. 10.30574/Wjaets.2024.11.1.0009.

[56]. Nasir, Rida & Afzal, Mehreen & Latif, Rabia & Iqabl, Waseem. (2021). Behavioral Based Insider Threat Detection Using Deep Learning. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3118297.

[57]. Nasiruzzaman M., M. Ali, I. Salam And M. H. Miraz. (2025). "The Evolution Of Zero Trust Architecture (ZTA) From Concept To Implementation", 2025 29th International Conference On Information Technology (IT), Žabljak, Montenegro, 19-22 February, 2025, Pp. 1-8. DOI: 10.1109/IT64745.2025.10930254.

[58]. Nisha Rawindaran, Ambikesh Jayal, Edmond Prakash, Chaminda Hewage. (2023). Perspective Of Small And Medium Enterprise (SME's) And Their Relationship With Government In Overcoming Cybersecurity Challenges And Barriers In Wales. International Journal Of Information Management Data Insights, Volume 3, Issue 2, 100191, ISSN 2667-0968. Https://Doi.Org/10.1016/J.Jjimei.2023.100191.

[59]. Ologunde, Ezekiel. (2025). Identity-Centric Zero Trust Architecture: A Comprehensive Framework For Modern Enterprise Security Governance.

[60]. Olzak, Tom. (2025). Verify Device Integrity. Https://Www.Researchgate.Net/Publication/390539503_Verify_Device_Integrity

[61]. Owen, Antony. (2025). Implementing Multi-Factor Authentication In Cloud Services For Smes.

[62]. Palo Alto Networks. (N.D.). What Is Microsegmentation? Https://Www.Paloaltonetworks.Com/Cyberpedia/What-Is-Microsegmentation

[63]. Perera, Srinath & Jin, Xiaohua & Maurushat, Alana & Opoku, De-Graft. (2022). Factors Affecting Reputational Damage To Organisations Due To Cyberattacks. Informatics. 9. 28. 10.3390/Informatics9010028.

[64]. Pernul Günther, Gill Asif Qumer, Khansa Lara, Everett Cath. (2025). Identity And Access Management. Elsevier. Https://Www.Sciencedirect.Com/Topics/Computer-Science/Identity-And-Access-Management

[65]. Peterson, John & Anderson, Michael & Mitchell, Sarah & Thompson, David & James, Andrew & Edmondson, Dale. (2023). Security Orchestration And Automated Response (SOAR) In Hybrid Clouds.

[66]. Prince Kumar. (2025). Zero Trust Architecture For Sme Cybersecurity: Enhancing Resilience In The Digital Transformation Era. International Journal Of Progressive Research In Engineering Management And Science (IJPREMS), Vol. 05, Issue 04, April 2025, Pp : 2791-2819

[67]. Qureshi, Shahana & Shandilya, Shishir K. (2021). Advances In Cyber Security Paradigm: A Review. 10.1007/978-3-030-49336-3_27.

[68]. Ravi, Chetan & Shaik, Mahammad & Saini, Vipin & Chitta, Subrahmanyasarma & Bonam, Venkata Sri Manoj. (2025). Beyond The Firewall: Implementing Zero Trust With Network Microsegmentation. Nanotechnology Perceptions. 21. 560-578.

[69]. Ron Samson. (2025). Endpoint Threat Detection And Response For Small And Medium Enterprises. Clearnetwork. Https://Clearnetwork.Com/Endpoint-Threat-Detection-And-Response-For-Small-And-Medium-Enterprises/Amp/

[70]. Ryan Bredesen And Stephen Mujeye. (2025). Network Segmentation Security With The Implementation Of Threats. In Proceedings Of The 2025 8th International Conference On Software Engineering And Information Management (ICSIM '25). Association For Computing Machinery, New York, NY, USA, 137–141. Https://Doi.Org/10.1145/3725899.3725920

[71]. Saeed, Sultan & Jasmine, Nathaile. (2022). Enhancing Security With Cloud-Based Identity And Access Management Solutions. International Journal Of Cloud Computing.

[72]. Salah, Noor & Abdulrahman, Lozan & Delzy, Mohammed & Abdulkarim, Nasiba & Omar, Marya & Mohammed Ghazi Sami, Teba. (2023). HIGH-PERFORMANCE CLOUD COMPUTING SERVICES AND ITS INFLUENCES BY WEB TECHNOLOGY BASED ON INFORMATION SYSTEMS. Journal Of Biomechanical Science And Engineering. March 2023. 263-303. 10.17605/OSF.IO/KF9XC.

[73]. Scott Rose, Oliver Borchert, Stu Mitchell, VA Sean Connelly. (2020). NIST Special Publication 800-207 Zero Trust Architecture. Https://Doi.Org/10.6028/NIST.SP.800-207

[74]. Scroxton, A. (2025). UK Smes Losing Over £3bn A Year To Cyber Incidents. Computer Weekly. Https://Www.Computerweekly.Com/News/366622019/UK-Smes-Losing-Over-3bn-A-Year-To-Cyber-Incidents

[75]. Sentinelone. (2025). 10 Enterprise Security Solutions: Comparative Analysis 2025. Sentinelone. Https://Www.Sentinelone.Com/Cybersecurity-101/Cybersecurity/Enterprise-Security-Solutions/

[76]. Smith, Samuel & Klaus, Mike & Stephen, Biodun & Hannah, Tessy. (2025). AI-Powered Behavioral Analytics For Predictive Anomaly Detection In Zero Trust Infrastructures.

[77]. Sophie, Emily. (2025). Building Trust By Removing Enterprise-Wide Implementation Barriers For Zero Trust Architecture. 8.

[78]. Synergy Managed IT Services. (2025). The Top 5 Cyber Risks Facing UK Smes In 2025. Https://Synergy.Tech/Insight/The-Top-5-Cyber-Risks-Facing-Uk-Smes-In-2025

[79]. Techn22. (2024). Techn22 Threat Report 2024: Exploiting Weak Defences And Targeting Critical SME Data. Capcon. Https://Www.Capcon.Co.Uk/Wp-Content/Uploads/2024/11/Techn22-2024-Threat-Report-.Pdf

[80]. Vemula, Vamshidhar Reddy. (2023). Multi-Cloud Security Orchestration Using Deep Reinforcement Learning. Https://Www.Researchgate.Net/Publication/386050540_Multi-Cloud_Security_Orchestration_Using_Deep_Reinforcement_Learning

[81]. Verma, Saurabh. (2025). Zero Trust Architecture In Cloud-Native Environments: Implementation Strategies & Best Practices. International Journal Of Computer Trends And Technology. 73. 102-107. 10.14445/22312803/IJCTT-V73I4P114.

[82]. Webnic. (2025). Why Zero Trust Is No Longer Optional. Https://Webnic.Cc/Cyber-Security/Why-Zero-Trust-Is-No-Longer-Optional/

[83]. Yakushkin, V. (2022). Continuous Authentication: What It Is & How It Works. Syteca. Https://Www.Syteca.Com/En/Blog/Continuous-Authentication

[84]. Zillah Adahman, Asad Waqar Malik, Zahid Anwar. (2022). An Analysis Of Zero-Trust Architecture And Its Cost-Effectiveness For Organizational Security. Computers & Security, Volume 122, 102911, ISSN 0167-4048. Https://Doi.Org/10.1016/J.Cose.2022.102911.

[85]. Zohaib, S. M., Sajjad, S. M., Iqbal, Z., Yousaf, M., Haseeb, M., & Muhammad, Z. (2024). Zero Trust VPN (ZT-VPN): A Systematic Literature Review And Cybersecurity Framework For Hybrid And Remote Work. Information, 15(11), 734. Https://Doi.Org/10.3390/Info15110734