Identity as the New Perimeter: Conditional Access, MFA, and Zero Trust Adoption Across Distributed Microsoft 365 Environments

Kelly Okogbenin*, Tedun Awi Daniel
Independent Researcher
*Corresponding author: okogbeninkelly@gmail.com

Abstract

This review examines the transformation of enterprise security as identity replaces the traditional network perimeter across distributed Microsoft 365 environments. Its purpose is to evaluate how Conditional Access, multi-factor authentication, and Zero Trust principles collectively address the risks created by remote work, cloud collaboration, unmanaged devices, credential compromise, privileged access, and fragmented policy enforcement. A structured narrative review method was adopted, drawing on scholarly and authoritative literature published up to 2024 and organizing evidence around perimeter dissolution, identity risk, authentication and authorization, policy enforcement, Zero Trust architecture, governance, usability, compliance, and future research.

The findings show that identity-centric security is most effective when authentication strength, device posture, application sensitivity, location, session context, privilege, and behavioral risk are evaluated together rather than through isolated controls. Conditional Access provides the principal policy-enforcement layer, while MFA strengthens identity assurance and Zero Trust supplies the architectural logic of explicit verification, least privilege, assumed breach, segmentation, and continuous trust evaluation. The review also finds that governance maturity, telemetry, user acceptance, accessibility, security culture, administrator cooperation, and change management materially influence technical effectiveness.

The study concludes that resilient Microsoft 365 security requires an integrated operating model in which trust is continuously assessed and access is dynamically constrained according to risk. It recommends phishing-resistant authentication, stronger privileged-access governance, device-compliance enforcement, service-identity oversight, policy auditing, user-centered implementation, and measurable Zero Trust maturity. Future research should prioritize longitudinal validation of policy effectiveness, AI-assisted identity-risk decisions, passwordless authentication, usability-security trade-offs, and cross-sector evidence on organizational adoption and resilience. These priorities can strengthen accountability, operational continuity, and evidence-based security decision-making across increasingly distributed digital enterprises.

Keywords: Identity-centric security; Conditional Access; Multi-factor authentication; Zero Trust; Microsoft 365; Distributed environments.

DOI: 10.21590/ijhit.06.04.23

1. Introduction

1.1 Distributed Work and Identity-Centric Security

The expansion of distributed work has altered the assumptions on which enterprise security was historically built. Conventional architectures treated the corporate network as a defensible boundary: users, devices and applications operating inside it were granted comparatively greater trust, while external connections were subjected to stronger scrutiny. Cloud computing, software-as-a-service platforms, mobile endpoints and geographically dispersed workforces have weakened that distinction because organizational activity now occurs across homes, branch offices, partner environments and unmanaged networks. Nigerian research on distributed operations similarly shows that geographically dispersed enterprises depend increasingly on coordinated digital capabilities, adaptive workforce structures and information flows that transcend individual sites (Falemi et al., 2020). In this environment, location can no longer serve as a reliable proxy for legitimacy.

The operational consequences are particularly visible in multi-site enterprises, where resources, personnel and decision processes are interconnected through digital platforms. Data-driven coordination can improve visibility and responsiveness across distributed locations, but it also increases dependence on persistent access to shared information systems and cloud services (Akin-Oluyomi& Akhigbe, 2023). For Microsoft 365 environments, this transformation is significant because Exchange Online, SharePoint, Teams, OneDrive and related services are designed to be accessed beyond a single organizational network. Security therefore shifts from protecting a fixed gateway toward determining, at each access event, whether the requesting identity, device and context present an acceptable level of risk.

Remote and hybrid work also expand the attack surface by relocating routine organizational activity to networks and endpoints that security teams may not fully control. Evidence from South African industries indicates that rapid work-from-home adoption intensified cybersecurity challenges and exposed weaknesses in organizational security culture, policy awareness and remote-working practices (Shibambu&Moganedi, 2022). The implication is that distributed work is not merely a change in work location; it is a redistribution of trust relationships. Users may authenticate from different devices, networks, and jurisdictions, while compromised credentials can provide adversaries with access that resembles legitimate employee activity.

Zero Trust responds to this condition by rejecting implicit trust based solely on network location. Cloud-oriented research demonstrates that work-from-home environments require access decisions capable of differentiating legitimate requests from traffic originating through potentially untrusted networks and devices (Mandal et al., 2021). NIST consequently frames Zero Trust as a movement away from static network perimeters toward protection focused on

users, assets, and resources, with authentication and authorization applied before access to enterprise resources is established (Rose et al., 2020). Identity consequently becomes a principal control plane through which distributed access can be evaluated consistently.

This identity-centric orientation extends security beyond the initial sign-in. Once users operate across mobile devices and cloud services, a successful login cannot by itself establish continuing legitimacy for an entire session. Continuous authentication research emphasizes that access-control mechanisms must account for the possibility that an authenticated session may later be misused or an identity impersonated, particularly as mobile and cloud architectures dissolve conventional perimeter assumptions (Junquera-Sánchez et al., 2021). Within Microsoft 365, this logic creates a conceptual foundation for combining identity assurance with device posture, contextual signals, session conditions, and risk-responsive policy enforcement.

The resulting security model is therefore less concerned with distinguishing "inside" from "outside" than with determining whether a particular identity should receive a particular level of access under prevailing conditions. Zero Trust scholarship reinforces this shift by showing that neither internal nor external networks should be inherently trusted and that modern security must accommodate technical, organizational, and user dimensions simultaneously (Buck et al., 2021). For distributed Microsoft 365 environments, identity becomes the new perimeter because it accompanies the user across locations, devices and cloud workloads. Effective protection consequently depends on verifying identities strongly, limiting access according to context and privilege, and continually reassessing trust as conditions change. This transformation provides the conceptual basis for Conditional Access, multi-factor authentication and broader Zero Trust adoption as mutually reinforcing mechanisms for governing access across a perimeterless enterprise. Accordingly, distributed collaboration makes identity governance foundational to security resilience, accountable access, and organizational continuity across modern cloud-dependent enterprises worldwide.

1.2 Microsoft 365 Threat and Trust Landscape

Microsoft 365 environments concentrate communication, collaboration, storage, and identity-mediated access within an interconnected cloud ecosystem, making compromised identities consequential. Rather than attacking a single workstation, adversaries can exploit valid accounts to traverse Exchange Online, SharePoint, Teams and OneDrive while appearing to operate through legitimate authentication channels. Empirical analysis of Microsoft 365 login activity shows that malicious access attempts frequently intersect with previously compromised email addresses, password spraying, credential stuffing, phishing and other adversarial techniques, demonstrating how cloud identity has become a central attack surface (Rich, 2023).

Credential compromise is particularly dangerous because an email identity often functions as a root of trust for services. Large-scale research into stolen credentials found that phishing kits, keyloggers and breached password datasets can enable account hijacking, while contextual risk signals such as device profiles and historical geolocation can strengthen authentication decisions against impersonation (Thomas et al., 2017). Within Microsoft 365, this risk is magnified by the breadth of resources associated with a single organizational identity: successful takeover may expose communications, shared files, collaboration spaces, and downstream business processes without requiring network intrusion.

The resulting threat landscape also changes how trust should be conceptualized. Cloud adoption research in South Africa demonstrates that information-security concerns and trust remain closely intertwined when organizations depend on externally hosted computing services, particularly where institutional control over infrastructure is reduced (Van der Schyff& Krauss, 2014). For distributed Microsoft 365 tenants, trust therefore cannot rest solely on successful credential presentation or presumed safety derived from organizational membership. It must account for the conditions surrounding access, including user legitimacy, device state, location, session characteristics and indications of abnormal behaviour.

Comparable cybersecurity research from Nigeria reinforces the limitations of centralized trust assumptions in increasingly interconnected digital systems, emphasizing integrity, auditability, resilience and verifiable exchange as essential properties of secure architectures (Shittu et al., 2022). Applied to Microsoft 365, these principles support a transition from static authentication toward continuously evaluated trust. Conditional Access and MFA consequently become architectural controls rather than optional safeguards: they introduce additional verification and contextual decision points that reduce reliance on passwords alone, constrain compromised identities, and align cloud access with a Zero Trust posture across distributed organizational environments.

1.3 Review Scope, Questions, and Objectives

This review addresses the growing inadequacy of network-centred security models within distributed Microsoft 365 environments, where users, devices, applications, and organizational data increasingly operate beyond conventional enterprise boundaries. The central problem is that authentication alone no longer provides sufficient assurance that an access request remains legitimate throughout a cloud session. Consequently, the review examines identity as an emerging security perimeter and evaluates how Conditional Access, multi-factor authentication, and Zero Trust principles can collectively strengthen trust decisions across geographically dispersed, hybrid, and cloud-dependent organizations. Its scope encompasses identity risk, authentication assurance, device context, access-policy enforcement, privilege, session

monitoring, and continuous verification while excluding detailed product configuration and implementation tutorials.

Three scholarly questions guide the analysis. First, how has distributed work transformed the role of identity within Microsoft 365 security architectures? Second, how effectively can Conditional Access and multi-factor authentication mitigate credential compromise, unauthorized access, and account takeover without creating disproportionate operational friction? Third, how can Zero Trust principles integrate identity, device, contextual, and behavioural signals into adaptive, least-privilege access governance across heterogeneous enterprise environments?

The review therefore pursues four objectives: to clarify the transition from network-based to identity-centric security; assess the security functions and limitations of Conditional Access and multi-factor authentication; examine Zero Trust as an integrating framework for continuous verification and access governance; and identify technical, organizational, usability, and policy constraints affecting adoption. Analytically, the review remains centred on Microsoft 365 and closely associated identity-management practices rather than cloud security in general. Its contribution to cybersecurity literature lies in connecting authentication controls, contextual access decisions, governance requirements, and Zero Trust principles within a unified analytical framework for distributed enterprise environments, thereby exposing implementation gaps and research priorities requiring further empirical investigation.

1.4 Review Method and Analytical Boundaries

This review adopts a structured narrative methodology to examine identity-centric security across distributed Microsoft 365 environments. Literature selection is guided by the study's central themes of Conditional Access, multi-factor authentication, Zero Trust, cloud identity, authentication risk, authorization, privilege management, adaptive access, remote work, and distributed enterprise security. Relevant studies are drawn from major scholarly databases and indexing platforms commonly used in cybersecurity and information-systems research, including Google Scholar, Scopus, Web of Science, IEEE Xplore, ScienceDirect, SpringerLink, and ACM Digital Library. Priority is given to peer-reviewed journal articles, conference papers, standards, and authoritative technical publications that demonstrate clear relevance to identity governance, cloud-access control, or Zero Trust implementation.

The literature-selection process emphasizes topical relevance, methodological credibility, publication quality, and applicability to contemporary cloud-security environments. Studies are included where they contribute directly to understanding identity assurance, contextual access decisions, credential compromise, continuous verification, distributed work, device trust, privilege, or organizational adoption. Sources lacking a defensible connection to these analytical

concerns are excluded. The review further prioritizes literature published up to 2024, thereby establishing a defined temporal boundary while capturing both foundational and recent developments.

For analysis, the literature is organized into four principal categories: perimeter transformation and distributed work; identity and authentication risk; Conditional Access and MFA enforcement; and Zero Trust governance and adoption. These categories support systematic comparison between technical controls, organizational practices, and broader security architectures.

The review is bounded primarily to Microsoft 365 and closely related identity-management environments. It excludes detailed configuration guidance, penetration-testing procedures, vendor comparisons, and product-performance benchmarking. Methodological limitations include the dependence on published literature, uneven empirical coverage across regions and sectors, rapidly evolving Microsoft capabilities, and variation in how Zero Trust is operationalized across studies. These constraints are acknowledged to preserve interpretive transparency and analytical discipline.

2. Identity as the Security Perimeter

2.1 Perimeter Dissolution in Cloud Collaboration

Cloud collaboration has progressively dissolved the architectural assumptions that once allowed enterprises to equate security with a clearly bounded corporate network. Traditional perimeter models concentrated defensive controls at network ingress and egress points, presuming that users, devices, and applications operating inside the boundary possessed a comparatively higher level of trust. This distinction has become increasingly unstable as organizations distribute workloads across software-as-a-service platforms, public and private clouds, mobile endpoints, branch locations, and remote users. Evidence from Nigerian small and medium-sized enterprises illustrates how cloud adoption shifts organizational computing away from locally controlled infrastructure toward remotely delivered resources and services, thereby changing where control, visibility, and responsibility reside (Abubakar, Bass & Allison, 2014).

Cloud collaboration also redistributes data and business processes across infrastructures that may span providers, jurisdictions, and organizational domains. Research from Ghana shows that cloud adoption is shaped partly by institutional expectations and concerns surrounding data transfer, emphasizing that cloud migration is not merely a technical relocation but an alteration of governance relationships and organizational dependencies (Adjei, Adams &Mamattah, 2021). For Microsoft 365 environments, these dynamics are particularly consequential because email,

document repositories, meetings, messaging, identity services, and collaborative workflows are accessed continuously from locations that no longer correspond to a single trusted network.

This erosion of the fixed perimeter requires security architecture to move closer to the entities that actually request, process, and store organizational resources. Software-defined perimeter research demonstrates the value of authenticating devices and users before exposing application infrastructure, thereby replacing broad network visibility with need-to-know access and dynamically controlled connectivity (Moubayed, Refaey& Shami, 2019). The architectural implication is that network location alone cannot establish legitimacy; identities, endpoints, applications, and resource sensitivity must become first-class security variables.

Zero Trust extends this logic by eliminating assumptions of implicit trust and subjecting access to explicit verification and policy enforcement. In cloud environments, static trust relationships are inadequate because users, services, and workloads interact dynamically across changing infrastructure conditions, making continuous and policy-based trust assessment more appropriate than one-time perimeter admission (Mehraj & Banday, 2020). Accordingly, the security boundary becomes logical and contextual rather than primarily physical.

Contemporary Zero Trust research further emphasizes that authentication, authorization, micro-segmentation, encryption, automation, and risk evaluation must operate together to reduce excessive trust within complex enterprise systems (Syed et al., 2022). This is particularly relevant to Microsoft 365, where a valid identity may interact with multiple applications and data stores during a single working session. Protecting the environment therefore requires controls capable of restricting what authenticated entities can reach, under which conditions, and for how long.

Cloud-focused Zero Trust studies similarly show that modern enterprise networks require greater visibility, intelligent orchestration, and behavioral trust evaluation because cloud resources exist beyond conventional organizational boundaries (Sarkar et al., 2022). The perimeter consequently fragments into multiple enforcement points surrounding identities, devices, applications, data, sessions, and workloads rather than remaining concentrated at a corporate gateway.

This architectural transition also extends to cloud-native services. NIST guidance for multi-location applications argues that Zero Trust requires movement from segmentation based predominantly on IP addresses, subnets, and network boundaries toward policies grounded in user, application, service, and workload identities (Chandramouli & Butcher, 2023). Such an approach is directly compatible with distributed Microsoft 365 environments, where resource access frequently occurs independently of an organization-owned network.

Resilience additionally requires assuming that trusted components themselves may fail or become compromised. Survivable Zero Trust research therefore advocates access control for every request while avoiding implicit trust derived from physical location and strengthening architectures against failures and successful intrusions (Ferretti et al., 2021). Across Microsoft 365, perimeter dissolution thus represents an architectural redistribution of security: identity establishes who is requesting access, endpoint posture informs device assurance, application controls constrain pathways, data protections preserve resource sensitivity, and cloud workload policies govern service interactions. Conditional Access, MFA, and Zero Trust consequently operate as complementary mechanisms for enforcing security wherever collaboration occurs. This redistribution is essential for secure collaboration without recreating obsolete assumptions about trusted network location.

2.2 Identity Risk Across Distributed Environments

Distributed Microsoft 365 environments expose identity systems to risks amplified when users authenticate across home networks, personal devices, branch offices, mobile connections, and cloud applications. In such settings, identity compromise can transform a legitimate account into an adversarial access channel, while defenders may struggle to distinguish authorized activity from malicious use. Evidence from Nigerian banking environments shows that bring-your-own-device practices create overlapping technical and mobility threats where employees access organizational resources through devices and networks outside institutional control (Ofusori& Subramaniam, 2022). These conditions make identity assurance dependent not only on credentials, but also on endpoint trust, connection context, and access behaviour.

Unmanaged devices represent a parallel risk because they may lack configuration, monitoring, patching, encryption, or security enforcement. A systematic review of BYOD security identifies vulnerabilities spanning people, process, and technology, demonstrating that remote-working flexibility can expand organizational exposure when device governance and security controls are fragmented (Mayayise, 2023). Within Microsoft 365, an authenticated user connecting from an unmanaged endpoint may present a different risk profile from the same user accessing services through a compliant device.

Identity risk also extends beyond initial sign-in. Modern identity and access management increasingly requires authentication, authorization, auditing, and monitoring to operate as interconnected functions, as cloud computing, remote work, mobile applications, and interconnected devices multiply access pathways (Aboukadri, Ouaddah&Mezrioui, 2024). Compromised credentials may facilitate unauthorized access, while excessive permissions can enable privilege escalation; persistent sessions can prolong exposure after authentication if risk conditions are not reassessed. Unusual access, impossible travel patterns, unfamiliar devices,

abnormal application use, and atypical privilege requests become signals for adaptive decision-making.

Distributed infrastructures also demonstrate the value of continuous sensing and adaptive protection when cyber and operational conditions change. Research on cyber-physical resilience emphasizes real-time monitoring, intelligent devices, communication security, and adaptive protective responses as mechanisms for sustaining trustworthy operation within highly interconnected environments (Shittu, Olagunju & Shittu, 2024). Applied to Microsoft 365, this logic supports identity-centric controls that continually evaluate users, endpoints, sessions, and privileges. Conditional Access, MFA, device compliance, session controls, and least-privilege administration can thereby constrain compromised identities before they propagate risk across cloud resources, while preserving secure access for a geographically distributed workforce.

2.3 Authentication, Authorization, and Continuous Trust

Authentication, authorization, and continuous trust constitute an interdependent security architecture for governing access across distributed Microsoft 365 environments. Authentication answers the initial question of whether a claimant can provide sufficient evidence of identity, whereas authorization determines the resources, applications, data, and operations available to that authenticated principal. This distinction is fundamental because successful authentication does not establish that every subsequent action should be trusted. Evidence from remote-access environments in Ghana indicates that supplementing passwords with an additional authentication factor can materially strengthen identity assurance, although authenticated endpoints may continue to introduce security exposures requiring further safeguards (Yeboah-Boateng & Kwabena-Adade, 2020). Authentication should therefore be understood as the beginning of a trust decision rather than its permanent resolution.

Authorization converts established identity into bounded access rights. In distributed cloud environments, conventional role assignments can become overly permissive because users, devices, workloads, and applications interact under changing operational conditions. Research from Nigeria demonstrates that attribute-based access mechanisms can combine identity characteristics and repeated validation to strengthen cloud data protection, supporting a transition from broad permissions toward more granular and policy-sensitive decisions (Oyeyinka, Idowu &Kuyoro, 2021). Within Microsoft 365, authorization should consequently reflect not only organizational role, but also resource sensitivity, privilege level, device condition, sign-in context, and prevailing risk.

Attribute-driven controls provide a further mechanism for translating entitlement requirements into enforceable restrictions. Protected information can be made accessible only when defined user attributes satisfy predetermined policy conditions, thereby binding access to verifiable

characteristics rather than authentication status alone (Shittu & Nabil, 2023). This approach reinforces least privilege by ensuring that possession of a valid account does not automatically confer unrestricted access across Exchange Online, SharePoint, Teams, OneDrive, administrative portals, or connected workloads.

Table 1. Identity-Control Lifecycle in Distributed Microsoft 365 Environments

Security layer	Principal question	Typical decision inputs	Microsoft 365 relevance	Expected control outcome
Authentication	**Is the claimant legitimate?**	**Credentials, MFA method, authentication strength**	**User and administrator sign-in**	**Establish initial identity assurance**
Authorization	What may the identity access?	Role, attributes, privilege, resource sensitivity	Applications, data, administrative functions	Restrict access to approved entitlements
Contextual assessment	Is access appropriate now?	Device posture, location, sign-in anomalies, application risk	Conditional Access evaluation	Permit, challenge, restrict, or deny
Least privilege	Is the granted access minimal?	Role necessity, task requirements, privilege duration	Administrative and sensitive operations	Limit exposure and lateral movement
Continuous verification	Does trust remain justified?	Session behaviour, device changes, emerging risk signals	Active cloud sessions and token use	Reassess or revoke access dynamically
Adaptive enforcement	What response matches current risk?	Combined identity, device, behavioural, and session telemetry	Conditional Access and Zero Trust controls	Apply proportionate security action

Continuous trust extends authentication and authorization beyond the point of initial access. Zero Trust research demonstrates that user and device security profiles can be reassessed over time, allowing permissions to be maintained, restricted, or withdrawn as relevant security characteristics change (García-Teodoro et al., 2022). This principle is especially important in Microsoft 365 because users may transition between devices, networks, locations, applications, and privilege states during a single working period. Device compliance, unfamiliar sign-in patterns, geographic anomalies, application sensitivity, session characteristics, and privilege changes can therefore serve as signals for adaptive policy enforcement after authentication has occurred.

Continuous authentication addresses the related possibility that a legitimate session may subsequently be hijacked, transferred, or otherwise misused. Behavioural, physiological, and contextual indicators can provide additional evidence that the authenticated user remains the legitimate operator, although such mechanisms must balance security effectiveness with privacy, usability, and implementation complexity (Baig & Eskeland, 2021). The architectural objective is not perpetual user interruption, but persistent confidence that trust remains justified.

Accordingly, authentication, authorization, contextual risk assessment, least privilege, and continuous verification should operate as a unified trust lifecycle. In distributed Microsoft 365 environments, this lifecycle enables access to become conditional, proportionate, and revocable rather than static. Identity is verified, permissions are constrained, contextual conditions are evaluated, privileges are minimized, and sessions are reassessed as risk changes. Such integration provides the technical foundation upon which Conditional Access, MFA, identity protection, and broader Zero Trust controls can govern cloud access without assuming that trust, once granted, should remain indefinitely valid.

3. Conditional Access and MFA Architectures

3.1 Policy Signals, Context, and Enforcement

Conditional Access in distributed Microsoft 365 environments operates most effectively when access decisions are informed by multiple policy signals rather than credentials alone. Identity-centric enforcement evaluates who is requesting access, the resource requested, device state, network and location, observed behaviour, and session sensitivity. Context-aware access-control research demonstrates that cloud environments require policies incorporating user, resource, and environmental attributes because static role or location assumptions cannot adequately reflect changing conditions (Kayes et al., 2020). For Microsoft 365, a sign-in event therefore becomes a policy-evaluation point rather than an automatic gateway to organizational resources.

Identity and sign-in risk provide another layer of intelligence by estimating whether an authentication attempt is consistent with expected behaviour. Risk-based authentication can use device recognition, behavioural patterns, geolocation anomalies, and digital-footprint indicators to vary authentication requirements dynamically when suspicious conditions emerge (Kolawole, Rahmon &Osoko, 2024). Such signals are valuable in distributed organizations because legitimate employees may connect from multiple countries, networks, and endpoints, while attackers may imitate valid users through compromised credentials. Policy design must distinguish ordinary mobility from anomalous access without treating location itself as definitive evidence of trust.

Device posture further refines this assessment. A correctly authenticated user connecting from an unmanaged, non-compliant, or compromised endpoint presents a different exposure from the same user using a managed device satisfying enterprise requirements. Zero Trust research emphasizes that access policies should combine identity, device, behavioural, and environmental context and validate access on a per-session basis rather than extending implicit trust after authentication (Xiao et al., 2022). These attributes allow Conditional Access policies to impose stronger authentication, restrict functionality, require compliant endpoints, or deny access when risk exceeds tolerance.

Applications and resources must also influence policy outcomes because cloud assets vary in sensitivity. Risk-based access-control frameworks show that cloud authorization can combine role or attribute models with risk metrics and decision thresholds, enabling policies to reflect both the requester and potential consequences of access (dos Santos et al., 2016). Within Microsoft 365, routine collaboration content may therefore justify a different response from privileged administration, sensitive financial records, executive communications, or regulated data.

Location remains useful when treated as contextual evidence rather than a trusted perimeter. Network origin, unusual geographic movement, unfamiliar infrastructure, and deviations from historical access patterns can contribute to risk scoring, but policies must accommodate travel, VPN use, mobile connectivity, and remote work. User and Entity Behaviour Analytics can distinguish normal from abnormal activity by constructing behavioural or session fingerprints and detecting deviations within federated identity environments (Martín et al., 2021). Such telemetry strengthens enforcement after sign-in by making unusual session behaviour visible to the identity-control plane.

Session conditions are therefore critical to continuous trust. A policy decision reasonable at authentication may become unsafe if device posture changes, anomalous activity appears, privilege increases, or the session accesses sensitive resources. Practical implementations of risk-based authentication in cloud platforms demonstrate how contextual risk can be translated into

stepped authentication responses rather than relying exclusively on passwords or universally imposing additional friction (Unsel et al., 2023). This adaptive model suits Microsoft 365 because controls can remain proportionate to evolving access circumstances.

Effective enforcement also depends on translating policy intent into reliable technical action. Zero Trust policy-enforcement research demonstrates the importance of connecting user and device profiles, contextual information, risk-based decision logic, policy languages, and enforcement mechanisms so decisions are implemented consistently at access points (Vanickis et al., 2018). Conditional Access therefore requires more than signal collection; organizations must define coherent rules governing when access is granted, challenged, limited, or blocked.

The quality of these decisions depends on control effectiveness and residual risk. Access-control design research from South Africa emphasizes assessing invalid-access probability and anomaly detection when evaluating whether controls provide protection (Goncalves, 2023). Applied to distributed Microsoft 365 environments, policy governance should monitor false positives, false negatives, authentication friction, exceptions, privileged-access exposure, and enforcement consistency. Identity signals, sign-in risk, device posture, application sensitivity, location, telemetry, and session state must converge into transparent, auditable decisions, allowing Conditional Access to function as an adaptive enforcement layer within Zero Trust architecture.

3.2 MFA Strength, Methods, and Resistance

Multi-factor authentication (MFA) strengthens identity assurance by requiring users to present evidence from more than one authentication category, thereby reducing dependence on passwords as a single point of compromise. In distributed Microsoft 365 environments, however, MFA should not be treated as a uniform security control. Its protective value depends on the independence and strength of the factors employed, their resistance to interception and social engineering, the reliability of recovery processes, user acceptance, device availability, and the consistency with which authentication requirements are enforced. Nigerian research combining fingerprint biometrics with cryptographically secured smart cards demonstrates how possession and inherence factors can be combined to make impersonation more difficult than password-only authentication (Oke et al., 2021). The relevant question is therefore not simply whether MFA is enabled, but whether the selected method provides assurance proportionate to the sensitivity of the account and resource.

MFA strength varies considerably across authentication methods. Passwords supplemented by SMS or one-time passcodes provide greater protection than passwords alone, but such approaches remain dependent on transferable codes and user judgement. Push-based authentication can improve convenience, yet repeated approval prompts may create opportunities for inattentive or manipulated responses. By contrast, cryptographic authenticators can bind

authentication to a specific device and service, reducing exposure to credential replay and phishing. FIDO2 exemplifies this stronger model by using public-key cryptography instead of reusable shared secrets, offering substantial security and deployability advantages while retaining practical usability challenges such as unfamiliar workflows and concerns over authenticator loss (Lyastani et al., 2020).

Table 2. Comparative MFA Strength and Deployment Considerations

MFA method	Assurance characteristics	Principal strengths	Key limitations	Appropriate Microsoft 365 use
SMS or voice OTP	Password plus possession channel	Simple deployment; broad device availability	Vulnerable to interception, social engineering, and number compromise	Lower-risk or transitional use
Authenticator OTP	Password plus app-generated code	Avoids dependence on SMS delivery	Codes remain transferable and phishable	General workforce access
Push notification	Password plus device approval	Fast and convenient for users	Approval fatigue and deceptive prompts may reduce resistance	Routine access with risk controls
Biometrics plus possession factor	Inherence combined with device or token	Stronger impersonation resistance	Device dependence, privacy, enrollment, and recovery concerns	Managed devices and higher-assurance access
FIDO2/security keys	Public-key, phishing-resistant authentication	Strong replay and phishing resistance	Hardware, enrollment, recovery, and compatibility considerations	Privileged and sensitive accounts
Passwordless platform credentials	Device-bound cryptographic authentication	Reduced password exposure and improved user experience	Legacy integration and lifecycle complexity	Modern managed Microsoft 365 estates

Security effectiveness must also be considered alongside usability. Authentication mechanisms that are technically robust can fail operationally if employees find them confusing, intrusive, inaccessible, or excessively time-consuming. Evidence from South African online-banking users indicates that authentication usability differs across user characteristics and experience levels, reinforcing the need to design security controls that can be completed reliably by diverse populations without undermining assurance objectives (Mujinga, 2024). This consideration is particularly important in Microsoft 365 environments serving remote workers, contractors, administrators, mobile users, and employees using heterogeneous devices.

The strongest authentication method is therefore not automatically the most appropriate for every access event. Privileged administrators, high-value applications, sensitive data, and elevated-risk sessions warrant stronger, phishing-resistant authentication, whereas ordinary workforce access may require methods that balance assurance with accessibility and continuity. Authentication design should also account for account recovery, device loss, enrollment, hardware replacement, remote onboarding, and emergency access because weaknesses in recovery processes can undermine otherwise strong MFA.

Enterprise adoption studies of FIDO2 further show that technically superior authentication can encounter operational barriers involving legacy applications, identity lifecycle management, remote users, recovery procedures, and exceptional cases that complicate migration from established credentials (Kepkowski et al., 2023). MFA strategy in Microsoft 365 should therefore be tiered, risk-sensitive, and progressively modernized rather than imposed uniformly. Its greatest value emerges when authentication strength is integrated with Conditional Access and Zero Trust, allowing factor requirements to respond to identity risk, device posture, resource sensitivity, privilege level, and session context. In this model, MFA becomes an adaptive component of identity assurance rather than a static one-time challenge, enabling organizations to strengthen resistance to phishing and account takeover while preserving usability, accessibility, and operational resilience.

3.3 Legacy Authentication and Policy Gaps

Legacy authentication and policy gaps remain weaknesses in distributed Microsoft 365 environments because older protocols, inconsistent configurations, and exceptional access paths can circumvent controls systematically designed around modern identity assurance. Password-centric authentication is particularly fragile when it relies on no contextual verification or additional factors. Nigerian research on cloud-based authentication demonstrates that stronger multi-layer and multi-factor mechanisms can materially improve resistance to unauthorized access, highlighting the limitations of security architectures that continue to depend on simpler credential-based controls (Okeke &Orimadike, 2024). In practice, legacy dependencies become

problematic when business applications or integration workflows cannot support stronger authentication requirements, encouraging organizations to preserve weaker access paths.

Policy gaps can also emerge when access rules are unevenly defined or enforced across cloud services. Research from Ghana emphasizes that cloud security requires explicit authorization policies, consistent policy languages, and enforceable controls rather than informal or fragmented governance arrangements (Okoampa-Larbi, Twum &Hayfron-Acquah, 2017). Within Microsoft 365, exclusions created for older applications, emergency accounts, service integrations, or operational convenience can therefore create asymmetric protection. A tenant may appear governed while particular protocols, applications, or identities remain outside Conditional Access, MFA, or device-compliance requirements.

Privileged identities magnify this exposure because compromise can provide broad administrative control over directories, services, and security settings. Enterprise research shows that privileged accounts commonly possess extensive authorization and are attractive targets for password theft, making dedicated management, monitoring, and restriction essential (Sindiren&Ciylan, 2019). In Microsoft 365, standing administrative privileges, shared administrator credentials, poorly governed break-glass accounts, and excessive role assignments can weaken least-privilege objectives. Similar concerns apply to service identities, application principals, and automated accounts, whose permissions may persist long after their original operational purpose.

Configuration inconsistency further complicates enforcement. Enterprise IAM research identifies security, compliance, operability, technology, and user requirements as interdependent, while also showing that complex identity environments are difficult to maintain consistently as organizations scale (Glöckler et al., 2024). Policy effectiveness therefore depends not only on designing strong controls but on ensuring complete coverage, accurate identity lifecycle management, and regular review of exceptions. For distributed Microsoft 365 environments, legacy protocol retirement, privileged-access governance, service-identity oversight, configuration standardization, and continuous policy auditing are necessary to prevent weak exceptions from becoming durable pathways around Zero Trust enforcement.

4. Zero Trust in Microsoft 365

4.1 Zero Trust Principles and Identity Controls

Zero Trust reframes enterprise security around explicit verification rather than inherited confidence in network location. Within distributed Microsoft 365 environments, every access request should be evaluated as a discrete transaction involving an identity, device, resource, and prevailing risk context. Zero Trust implementation research emphasizes precise authentication,

minimal authorization, and continuous verification so legitimacy is repeatedly established rather than assumed after sign-in (Tsai et al., 2024). Identity therefore becomes the control plane through which trust is asserted, challenged, and revoked.

Identity protection within this model requires more than validating credentials. It demands assurance that the requesting principal is legitimate, appropriately privileged, and operating under acceptable conditions. Nigerian and Ghanaian research on Zero Trust implementation in distributed infrastructure highlights identity credentialing, policy-based access control, micro-segmentation, and continuous monitoring as mutually reinforcing mechanisms for reducing implicit trust across dispersed assets (Ogborigbo& Gadah, 2021). Applied to Microsoft 365, users, administrators, applications, and service principals should receive access only after policy evaluates relevant identity and resource conditions.

Least privilege gives this verification model operational discipline. Permissions should be restricted to what is necessary for a defined task, role, or session, reducing the damage possible when an account is compromised. Migration research shows that Zero Trust architectures depend on granular authorization, dynamic policy enforcement, and careful transition from legacy trust assumptions rather than simply adding stronger authentication to existing networks (Teerakanok et al., 2021). In Microsoft 365, least privilege therefore extends to administrative roles, application permissions, delegated access, privileged sessions, and sensitive collaboration resources.

Device trust is equally consequential because a valid user can still introduce risk through a compromised, unmanaged, or non-compliant endpoint. Contemporary Zero Trust research stresses that user identity, device health, location, and behaviour should influence access decisions and that these conditions should be continuously reassessed as circumstances change (Azad et al., 2024). Conditional Access can operationalize this logic by differentiating managed and unmanaged devices, requiring stronger authentication for elevated risk, and restricting sensitive resources when device assurance is inadequate.

The assumed-breach principle complements explicit verification by accepting that preventive controls may fail. Instead of presuming internal safety, Zero Trust limits lateral movement and constrains compromise through segmentation, narrowly scoped permissions, and persistent monitoring. Research from Kenya links stronger identity and access management with cyber resilience, underscoring how authentication, access controls, proactive threat detection, and operational oversight collectively strengthen protection in distributed digital environments (Musyoka & Mose, 2024). For Microsoft 365, assumed breach means designing controls so one compromised identity or endpoint does not automatically expose the wider tenant.

Applications and workloads must also be treated as identities rather than passive infrastructure. Zero Trust maturity research identifies identity, endpoints, applications and workloads, data, networks, infrastructure, visibility, analytics, and automation as interdependent dimensions of successful adoption (Yeoh et al., 2023). This is relevant to Microsoft 365 integrations, where service principals, APIs, automation accounts, and connected applications may hold extensive permissions without an active human user. Workload access should therefore be authenticated, authorized, monitored, and periodically reviewed with rigor comparable to human accounts.

Segmentation provides another mechanism for translating least privilege into enforceable architecture. By dividing resources into smaller trust zones and limiting communication according to verified identities and policies, organizations can reduce unrestricted east-west movement after compromise. Research mapping Zero Trust implementation demonstrates that identity and access management, software-defined perimeter mechanisms, and micro-segmentation operate together to create granular isolation and policy enforcement across users, devices, applications, and resources (Liu et al., 2024).

Adaptive controls make these principles sustainable where risk changes continuously. Automation and orchestration research shows that Zero Trust increasingly depends on coordinated policy decisions, telemetry, analytics, authentication, and access-control mechanisms capable of responding dynamically to emerging conditions (Cao et al., 2024). In distributed Microsoft 365 environments, this translates into controls that can require stronger authentication, reduce session capability, revoke access, or trigger investigation as risk increases. Zero Trust therefore functions not as a single product, but as an identity-centred operating model in which explicit verification, least privilege, assumed breach, device assurance, workload governance, segmentation, and adaptive enforcement continuously regulate cloud access.

4.2 Governance, Telemetry, and Adaptive Access

Governance converts identity security from technical controls into an enterprise operating discipline. In distributed Microsoft 365 environments, Conditional Access, MFA, privileged access, device compliance, and session controls require policy ownership, accountability, measurable objectives, and continuous oversight. Cybersecurity governance maturity research from South Africa emphasizes that effective governance must be assessable and reportable to board stakeholders, allowing organizations to determine whether controls are deployed or operating with sufficient consistency and accountability (De Bruin & Von Solms, 2016).

Telemetry provides the evidentiary foundation for such oversight. Identity logs, authentication events, device-state information, application activity, privilege changes, and anomalous session behaviour allow security teams to evaluate whether access policies remain appropriate as conditions evolve. Nigerian research on digital-twin monitoring demonstrates the value of

synchronizing real-time and historical data with analytical models to improve situational awareness and identify abnormal conditions earlier than conventional monitoring (Shittu et al., 2023). In Microsoft 365, comparable telemetry should feed identity protection, audit processes, and policy review rather than remain fragmented across administrative consoles.

Enterprise operationalization also requires automation that converts observations into timely responses. Smart-automation research shows that combining supervisory monitoring with analytics and intelligent control can strengthen transparency, decision-making, resilience, and adaptive governance while introducing cybersecurity and skills requirements requiring oversight (Omoegun et al., 2024). Applied to Microsoft 365, this logic supports automated responses such as requiring stronger authentication, blocking risky sessions, restricting unmanaged devices, revoking tokens, or escalating suspicious activity for investigation.

Adaptive access depends on policies that change as evidence changes. Enterprise-cloud research demonstrates that access-control policies benefit from analysis of user requests, roles, resource utilization, and behavioural patterns, enabling policy redefinition when existing permissions no longer match operational need (Kaur & Verma, 2023). For distributed Microsoft 365 environments, this implies a governance cycle in which telemetry informs risk assessment, risk informs access decisions, and outcomes are reviewed against security and business objectives.

Mature governance therefore requires policy ownership, exception management, escalation pathways, auditability, performance indicators, and periodic validation. Metrics should extend beyond deployment counts to examine enforcement coverage, privileged-access exposure, policy exceptions, risky sign-ins, remediation speed, authentication friction, and unresolved alerts. By connecting telemetry, adaptive access, accountability, and maturity assessment, organizations can transform Zero Trust from an aspiration into a continuously governed enterprise capability.

5. Adoption Challenges and Strategic Priorities

5.1 Usability, Inclusion, and Change Management

Identity-centric security in distributed Microsoft 365 environments succeeds only when protective controls are usable, inclusive, and embedded within organizational change rather than as technical requirements. Conditional Access, MFA, device compliance, and privileged-access controls alter everyday work routines, and their effectiveness depends on whether employees understand, accept, and consistently follow them. Technology-adoption research emphasizes that readiness is shaped by skills, adaptability, psychological acceptance, strategic alignment, capability development, and reinforcement, indicating that organizations should prepare employees before introducing controls that materially change access practices (Akhigbe et al.,

2024). For Microsoft 365, this means pairing security deployment with communication, preparation and support.

Authentication friction is a particularly important adoption variable. Repeated prompts, unfamiliar authenticators, device changes, recovery procedures, and context-sensitive challenges can protect accounts while interrupting workflows. Research on two-factor authentication shows that perceived satisfaction with task-completion time can influence usability more than measured completion time, demonstrating that user experience is shaped partly by expectations rather than technical efficiency alone (Kružíkova et al., 2024). Conditional Access policies should therefore apply stronger authentication proportionately, reserving additional friction for elevated risk, privileged operations, sensitive resources, or anomalous conditions instead of challenging every user uniformly.

Poorly calibrated security demands can also produce fatigue. Users exposed to numerous security decisions may experience resignation, loss of control, risk minimization, or decision avoidance, weakening technically sound controls (Stanton et al., 2016). In distributed Microsoft 365 environments, excessive prompts or confusing policy messages can encourage users to approve requests reflexively, seek workarounds, or perceive security as an obstacle. Administrators should reduce unnecessary prompts, simplify recovery pathways, explain why challenges occur, and make secure actions easier.

Security culture provides the organizational context in which these behaviors develop. Evidence from South Africa demonstrates that information-security culture can be improved through repeated assessment, monitoring, awareness initiatives, and targeted implementation actions, with training contributing materially to behavioral improvement (Da Veiga & Martins, 2015). This is especially important where Microsoft 365 adoption spans offices, contractors, remote employees, and teams. Training should not be confined to generic annual modules; it should address phishing-resistant authentication, suspicious approval requests, device requirements, session risks, privilege use, and escalation procedures.

Workforce diversity further complicates standardized security design. Employees differ in technical confidence, age, accessibility needs, device availability, work location, connectivity, language, and exposure to security practices. Organizational research indicates that security awareness is influenced not only by individual knowledge but also by the surrounding security culture, suggesting that behavioral improvement requires attention to shared norms and institutional expectations (Wiley et al., 2020). Inclusive Microsoft 365 security should therefore provide accessible authentication choices, alternative recovery mechanisms, clear language, and support for users whose circumstances make a single method impractical.

Remote work magnifies these human considerations because employees operate with reduced direct supervision and may depend on personal networks, mobile devices, or unfamiliar technical arrangements. Empirical research on home-working employees shows that organizational training, workplace context, and confidence in defensive measures influence cyber-defense and cyber-risk behaviors, making education and managerial reinforcement important alongside technical controls (Klein & Zwilling, 2024). Change management must extend beyond deployment milestones to reinforce secure behavior as hybrid work evolves.

Operational data can strengthen this process when used to identify where users encounter difficulties rather than merely to measure compliance. Workforce-behavior frameworks show that real-time operational information can reveal performance patterns and support responsive organizational decisions (Akhigbe et al., 2023). In Microsoft 365, help-desk trends, authentication failures, policy blocks, recovery requests, risky sign-ins, and exception patterns can reveal whether controls create avoidable friction or whether particular groups require targeted assistance.

Administrator resistance also requires management. Security teams may prefer broad controls, whereas business units may seek exceptions to preserve legacy workflows, creating tension between assurance and continuity. Effective change therefore requires executive sponsorship, transparent exception governance, pilot testing, feedback channels, phased deployment, and measurable adoption outcomes. Usability and inclusion should not be treated as compromises to Zero Trust; they are conditions for durable enforcement. When users understand access decisions, complete authentication reliably, obtain assistance, and perceive controls as proportionate, identity-centric security becomes sustainable across distributed Microsoft 365 environments.

5.2 Compliance, Privilege, and Operational Resilience

Compliance, privilege governance, and operational resilience are tightly connected in distributed Microsoft 365 environments because security controls must satisfy regulatory obligations while preserving access to business services. Governance requires explicit accountability for identity policies, access reviews, exception handling, data protection, and audit evidence across dispersed users and administrators. Research on governance across distributed operational networks shows that compliance improves when responsibilities, monitoring mechanisms, escalation processes, and quality controls are standardized rather than left to fragmented local practices (Akin-Oluyomi& Akhigbe, 2022). In Microsoft 365, this principle supports consistent Conditional Access baselines, documented policy ownership, entitlement reviews, and traceable remediation of control failures.

Privileged access represents a sensitive governance domain because administrative identities can alter security configurations, assign roles, access protected information, and disable safeguards. Zero Trust guidance on privileged access management emphasizes controlling, monitoring, and reporting elevated access, with high-value administrative resources requiring rigorous protection (Garbis & Chapman, 2021). Accordingly, standing privileges should be minimized, administrative roles separated from routine user activity, and elevation should be time-bound, justified, strongly authenticated, and logged. Service identities and application permissions require comparable scrutiny because excessive non-human privileges can create durable pathways that evade user-focused controls.

Operational resilience depends on linking these access controls to enterprise risk management rather than treating identity security as an isolated technical function. Integrated risk frameworks demonstrate that analytics, cross-functional coordination, and adaptive governance can improve organizational resilience by converting fragmented risk information into proactive decisions (Falemi, Akhigbe & Akin-Oluyomi, 2024). For Microsoft 365, this requires monitoring risky sign-ins, privileged-role changes, policy exclusions, authentication failures, service-account dependencies, configuration drift, and incident-response readiness while maintaining recovery procedures and continuity arrangements.

Compliance also relies on leadership capable of translating formal policies into institutional behavior. African research on technological transformation stresses that ethical leadership and effective policy implementation are central to converting governance objectives into operational practice (Enaifoghe, Dlamini &Agwuna, 2020). This is relevant where business units seek policy exceptions or administrators face pressure to weaken controls for convenience. Mature Microsoft 365 governance should therefore combine regulatory mapping, least privilege, resilient access pathways, emergency-account controls, configuration assurance, auditability, and security operations. These mechanisms allow organizations to sustain secure access during disruption without normalizing exceptions that undermine Zero Trust or weaken accountability.

5.3 Research Gaps and Future Directions

Research on identity-centric security has advanced rapidly, yet gaps remain between Zero Trust principles and demonstrable enterprise outcomes. A weakness concerns maturity measurement. Organizations often assess implementation through capability checklists, although such measures may not establish whether identity controls reduce compromise, privilege abuse, or session risk. A 2024 corporate Zero Trust maturity model proposes structured assessment across segmentation, access control, data protection, and incident response, but standardized outcome measures are needed across sectors and distributed operating models (Ilyas, Akal &Althebyan, 2024). Future studies should connect maturity stages to measurable security, usability, resilience, and governance outcomes within Microsoft 365.

AI-assisted identity risk is another priority. Nigerian research on AI-enabled IAM indicates that machine learning can strengthen authentication, authorization, access control, and adaptive decision-making, while performance remains influenced by computational conditions, transparency, user acceptance, and model improvement (Olabanji et al., 2024). Future Microsoft 365 research should test whether AI-assisted risk scoring reliably distinguishes legitimate mobility from account compromise across remote users, unmanaged endpoints, service identities, and changing locations. Attention is required for explainability, bias, false positives, privacy, adversarial manipulation, and human oversight before automated identity decisions become embedded in access governance.

Organizational readiness also remains underexamined. South African research proposes layered guidance for adopting AI within IAM and highlights interactions among organizational environment, technology, IAM lifecycle processes, user requirements, architecture, and implementation approaches (Masawi & Matthee, 2024). Zero Trust studies should move beyond technical deployment and examine policy ownership, administrator resistance, workforce diversity, skills, accessibility, exception governance, and security culture longitudinally. Comparative research across industries and regions could clarify whether adoption barriers differ between mature cloud enterprises and organizations undergoing hybrid transformation.

Passwordless authentication presents a further research frontier because stronger authentication does not automatically eliminate operational friction. Passwordless single sign-on research demonstrates security and usability benefits while identifying integration and recovery challenges in heterogeneous enterprise environments (Mahnamfar, Bicakci&Uzunay, 2024). Future studies should evaluate passkeys, hardware-backed credentials, recovery pathways, legacy application coexistence, and phishing resistance under real Microsoft 365 workloads. More broadly, controlled experiments and longitudinal field studies are needed to quantify Conditional Access policy effectiveness, authentication burden, exception rates, incident reduction, and user adaptation, enabling identity-centric security claims to be validated empirically rather than inferred from architectural conformity.

Conclusion

This review demonstrated that identity has become the decisive control point for securing distributed Microsoft 365 environments in which users, devices, applications, and workloads operate beyond conventional network boundaries. The analysis showed that Conditional Access, multi-factor authentication, identity protection, device assurance, least-privilege authorization, session controls, and continuous verification are most effective when implemented as interdependent elements of a Zero Trust architecture rather than as isolated safeguards. Conditional Access enables context-sensitive enforcement by incorporating identity, sign-in risk, device posture, location, application sensitivity, and session conditions into access decisions,

while MFA strengthens assurance by reducing dependence on reusable credentials. The findings further established that phishing-resistant authentication, privileged-access governance, workload identity protection, segmentation, and adaptive policy enforcement are essential for constraining account compromise and limiting lateral movement.

Equally, the review confirmed that technical strength alone does not determine successful adoption. Governance maturity, policy ownership, monitoring, accountability, workforce readiness, usability, inclusion, administrator cooperation, and security culture strongly influence whether identity controls remain effective in practice. Telemetry and continuous oversight were identified as critical for detecting anomalies, validating policy performance, managing exceptions, and sustaining operational resilience across geographically dispersed organizations.

The study therefore concludes that resilient Microsoft 365 security requires an integrated identity-centric operating model in which trust is continuously earned, verified, and restricted according to changing risk. Organizations should prioritize phishing-resistant MFA, rigorous Conditional Access baselines, least-privilege administration, service-identity governance, device compliance, policy auditing, and measurable Zero Trust maturity. They should also invest in user-centered change management, accessible authentication options, targeted training, and transparent exception processes. This integration aligns security assurance with business continuity, regulatory accountability, and sustainable digital collaboration. Future research should emphasize longitudinal and cross-sector evaluation of policy effectiveness, AI-assisted identity-risk decisions, passwordless authentication, usability-security trade-offs, and measurable Zero Trust outcomes. Such evidence is necessary to move identity-centric security from architectural principle to demonstrably effective enterprise practice.

References

1. Aboukadri, S., Ouaddah, A. and Mezrioui, A. (2024) ‘Machine learning in identity and access management systems: Survey and deep dive’, Computers & Security, 139, 103729. DOI: 10.1016/j.cose.2024.103729.
2. Abubakar, A.D., Bass, J.M. and Allison, I. (2014) ‘Cloud computing: Adoption issues for Sub-Saharan African SMEs’, The Electronic Journal of Information Systems in Developing Countries, 62(1), pp. 1–17. DOI: 10.1002/j.1681-4835.2014.tb00439.x.
3. Adjei, J.K., Adams, S. and Mamattah, L. (2021) ‘Cloud computing adoption in Ghana; accounting for institutional factors’, Technology in Society, 65, 101583. DOI: 10.1016/j.techsoc.2021.101583.
4. Akhigbe, R., Falemi, A. and Akin-Oluyomi, O.T. (2023) ‘A conceptual model for improving customer experience using workforce behavior and real-time operational data’, International Journal of Multidisciplinary Research and Growth Evaluation, 4(6), pp.

1322–1338. DOI: 10.54660/.IJMRGE.2023.4.6.1322-1338.Akhigbe, R., Falemi, A. and Akin-Oluyomi, O.T. (2024) 'An advanced framework for technology adoption that

5. supports employee readiness in modern organizations', International Journal of Advanced Multidisciplinary Research and Studies, 4(1), pp. 1637–1659. DOI: 10.62225/2583049X.2024.4.1.5344.
6. Akin-Oluyomi, O.T. and Akhigbe, R. (2022) 'A supply chain governance model for enhancing compliance and operational quality across retail networks', International Journal of Multidisciplinary Research and Growth Evaluation, 3(6), pp. 860–878. DOI: 10.54660/.IJMRGE.2022.3.6.860-878.
7. Akin-Oluyomi, O.T. and Akhigbe, R. (2023) 'An advanced framework for improving multi-site operational efficiency using data-driven performance indicators', International Journal of Advanced Multidisciplinary Research and Studies, 3(1), pp. 1763–1781. DOI: 10.62225/2583049X.2023.3.1.5343. (Multi Research Journal)
8. Azad, M.A., Abdullah, S., Arshad, J., Lallie, H. and Ahmed, Y. (2024) 'Verify and trust: A multidimensional survey of zero-trust security in the age of IoT', Internet of Things, 27, 101227. DOI: 10.1016/j.iot.2024.101227.
9. Baig, A.F. and Eskeland, S. (2021) 'Security, privacy, and usability in continuous authentication: A survey', Sensors, 21(17), 5967. DOI: 10.3390/s21175967
10. Buck, C., Olenberger, C., Schweizer, A., Völter, F. and Eymann, T. (2021) 'Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust', Computers & Security, 110, 102436. DOI: 10.1016/j.cose.2021.102436. (ScienceDirect)
11. Cao, Y., Pokhrel, S.R., Zhu, Y., Doss, R. and Li, G. (2024) 'Automation and orchestration of Zero Trust Architecture: Potential solutions and challenges', Machine Intelligence Research, 21, pp. 294–317. DOI: 10.1007/s11633-023-1456-2.
12. Chandramouli, R. and Butcher, Z. (2023) A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments. NIST Special Publication 800-207A. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-207A.
13. Da Veiga, A. and Martins, N. (2015) 'Improving the information security culture through monitoring and implementation actions illustrated through a case study', Computers & Security, 49, pp. 162–176. DOI: 10.1016/j.cose.2014.12.006.
14. De Bruin, R. and Von Solms, S.H. (2016) 'Cybersecurity governance: How can we measure it?', in 2016 IST-Africa Conference, IST-Africa 2016. Durban, South Africa: IEEE. DOI: 10.1109/ISTAFRICA.2016.7530578.
15. dos Santos, D.R., Marinho, R., Schmitt, G.R., Westphall, C.M. and Westphall, C.B. (2016) 'A framework and risk assessment approaches for risk-based access control in the cloud', Journal of Network and Computer Applications, 74, pp. 86–97. DOI: 10.1016/j.jnca.2016.08.013.

16. Enaifoghe, A., Dlamini, N.P. and Agwuna, L.U. (2020) 'African economic integration development in technological transformation: Assessing the importance of ethical leadership for policy implementation in SADC', Journal of Economics and Behavioral Studies, 12(6), pp. 11–20. DOI: 10.22610/jebs.v12i6(J).3102.
17. Falemi, A., Akhigbe, R. and Akin-Oluyomi, O.T. (2020) 'A conceptual supply chain talent development model for capability building across distributed operations', International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), pp. 439–456. DOI: 10.54660/.IJMRGE.2020.1.5.439-456.
18. Falemi, A., Akhigbe, R. and Akin-Oluyomi, O.T. (2024) 'A conceptual enterprise risk management model that integrates HR strategy with operational analytics', International Journal of Multidisciplinary Research and Growth Evaluation, 5(6), pp. 1730–1753. DOI: 10.54660/.IJMRGE.2024.5.6.1730-1753.
19. Ferretti, L., Magnanini, F., Andreolini, M. and Colajanni, M. (2021) 'Survivable zero trust for cloud computing environments', Computers & Security, 110, 102419. DOI: 10.1016/j.cose.2021.102419.
20. Garbis, J. and Chapman, J.W. (2021) 'Privileged access management', in Zero Trust Security: An Enterprise Guide. Berkeley, CA: Apress, pp. 155–161. DOI: 10.1007/978-1-4842-6702-8_12.
21. García-Teodoro, P., Camacho, J., Maciá-Fernández, G., Gómez-Hernández, J.A. and López-Marín, V.J. (2022) 'A novel zero-trust network access control scheme based on the security profile of devices and users', Computer Networks, 212, 109068. DOI: 10.1016/j.comnet.2022.109068
22. Glöckler, J., Sedlmeir, J., Frank, M. and Fridgen, G. (2024) 'A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity', Business & Information Systems Engineering, 66, pp. 421–440. DOI: 10.1007/s12599-023-00830-x.
23. Goncalves, D.P. (2023) 'Security access control effectiveness design', South African Journal of Industrial Engineering, 34(3), pp. 84–96. DOI: 10.7166/34-3-2954.
24. Ilyas, M., Akal, M. and Althebyan, Q. (2024) 'Maturity model for corporate sector based on Zero Trust adoption', in 2024 International Conference on Engineering and Emerging Technologies (ICEET), pp. 1–7. IEEE. DOI: 10.1109/ICEET65156.2024.10913750.
25. Junquera-Sánchez, J., Cilleruelo, C., De-Marcos, L. and Martinez-Herráiz, J.-J. (2021) 'Access control beyond authentication', Security and Communication Networks, 2021, Article 8146553, pp. 1–11. DOI: 10.1155/2021/8146553. (Wiley Online Library)
26. Kaur, A. and Verma, A. (2023) 'Adaptive Access Control Mechanism (AACM) for enterprise cloud computing', Journal of Electrical and Computer Engineering, 2023, Article 3922393, pp. 1–30. DOI: 10.1155/2023/3922393.
27. Kayes, A.S.M., Kalaria, R., Sarker, I.H., Islam, M.S., Watters, P.A., Ng, A., Hammoudeh, M., Badsha, S. and Kumara, I. (2020) 'A survey of context-aware access

control mechanisms for cloud and fog networks: Taxonomy and open research issues', Sensors, 20(9), 2464. DOI: 10.3390/s20092464.

28. Kepkowski, M., Machulak, M., Wood, I. and Kaafar, D. (2023) 'Challenges with passwordless FIDO2 in an enterprise setting: A usability study', in Proceedings of the 2023 IEEE Secure Development Conference (SecDev), pp. 37–48. DOI: 10.1109/SecDev56634.2023.00017
29. Klein, G. and Zwilling, M. (2024) 'The weakest link: Employee cyber-defensebehaviors while working from home', Journal of Computer Information Systems, 64(3), pp. 408–422. DOI: 10.1080/08874417.2023.2221200.
30. Kolawole, A.F., Rahmon, S.O. and Osoko, E.A. (2024) 'Utilizing digital footprint analysis for end-to-end risk-based authentication in medical billing systems', World Journal of Advanced Engineering Technology and Sciences, 13(2), pp. 166–179. DOI: 10.30574/wjaets.2024.13.2.0553.
31. Kružíkova, A., Muzik, M., Knapova, L., Dedkova, L., Smahel, D. and Matyas, V. (2024) 'Two-factor authentication time: How time-efficiency and time-satisfaction are associated with perceived security and satisfaction', Computers & Security, 138, 103667. DOI: 10.1016/j.cose.2023.103667.
32. Liu, C., Tan, R., Wu, Y., Feng, Y., Jin, Z., Zhang, F., Liu, Y. and Liu, Q. (2024) 'Dissecting zero trust: Research landscape and its implementation in IoT', Cybersecurity, 7, Article 20. DOI: 10.1186/s42400-024-00212-0.
33. Lyastani, S.G., Schilling, M., Neumayr, M., Backes, M. and Bugiel, S. (2020) 'Is FIDO2 the kingslayer of user authentication? A comparative usability study of FIDO2 passwordless authentication', in 2020 IEEE Symposium on Security and Privacy (SP), pp. 268–285. DOI: 10.1109/SP40000.2020.00047
34. Mahnamfar, A., Bicakci, K. and Uzunay, Y. (2024) 'ROSTAM: A passwordless web single sign-on solution mitigating server breaches and integrating credential manager and federated identity systems', Computers & Security, 139, 103739. DOI: 10.1016/j.cose.2024.103739.
35. Mandal, S., Khan, D.A. and Jain, S. (2021) 'Cloud-based Zero Trust access control policy: An approach to support work-from-home driven by COVID-19 pandemic', New Generation Computing, 39(3–4), pp. 599–622. DOI: 10.1007/s00354-021-00130-6. (PubMed Central (PMC))
36. Martín, A.G., Beltrán, M., Fernández-Isabel, A. and Martín de Diego, I. (2021) 'An approach to detect user behaviour anomalies within identity federations', Computers & Security, 108, 102356. DOI: 10.1016/j.cose.2021.102356.
37. Masawi, A. and Matthee, M. (2024) 'Guidelines for the adoption of artificial intelligence in identity and access management within the financial services sector', in Nagar, A.K., Jat, D.S., Mishra, D. and Joshi, A. (eds.) Intelligent Sustainable Systems. Lecture Notes

in Networks and Systems, vol. 812. Singapore: Springer, pp. 111–127. DOI: 10.1007/978-981-99-8031-4_11.

38. Mayayise, T.O. (2023) 'BYOD security issues and controls framework: An outcome of a systematic literature review', International Journal of Information and Computer Security, 21(1/2), pp. 135–161. DOI: 10.1504/IJICS.2023.131095.
39. Mehraj, S. and Banday, M.T. (2020) 'Establishing a zero trust strategy in cloud computing environment', in 2020 International Conference on Computer Communication and Informatics (ICCCI), pp. 1–6. DOI: 10.1109/ICCCI48352.2020.9104214.
40. Moubayed, A., Refaey, A. and Shami, A. (2019) 'Software-Defined Perimeter (SDP): State of the art secure solution for modern networks', IEEE Network, 33(5), pp. 226–233. DOI: 10.1109/MNET.2019.1800324.
41. Mujinga, M. (2024) 'Usable security of online banking authentication: An exploratory factor analysis', Journal of Information Systems and Informatics, 6(1), pp. 409–420. DOI: 10.51519/journalisi. v6i1.673
42. Musyoka, S.M. and Mose, T. (2024) 'Zero trust maturity model and cyber resilience in mobile money providers in Nairobi City County, Kenya', International Journal of Social Sciences Management and Entrepreneurship, 8(3), pp. 1037–1051.
43. Ofusori, L.O. and Subramaniam, P.R. (2022) 'A study on e-commuting: Alleviating technical and mobility threats in a BYOD-enabled banking environment in Nigeria', African Journal of Science, Technology, Innovation and Development, 14(2), pp. 489–503. DOI: 10.1080/20421338.2020.1856548.
44. Ogborigbo, J.C. and Gadah, J.N. (2021) 'Implementation of Zero Trust Architecture for cybersecurity in Distributed Energy Resources (DERs): A systematic review', World Journal of Advanced Engineering Technology and Sciences, 2(2), pp. 104–132. DOI: 10.30574/wjaets.2021.2.2.0021.
45. Oke, B.A., Olaniyi, O.M., Aboaba, A.A. and Arulogun, O.T. (2021) 'Multifactor authentication technique for a secure electronic voting system', Electronic Government, an International Journal, 17(3), pp. 312–338. DOI: 10.1504/EG.2021.115999
46. Okeke, R.O. and Orimadike, S.O. (2024) 'Enhanced cloud computing security using application-based multi-factor authentication (MFA) for communication systems', European Journal of Electrical Engineering and Computer Science, 8(2), pp. 1–8. DOI: 10.24018/ejece.2024.8.2.593.
47. Okoampa-Larbi, R., Twum, F. and Hayfron-Acquah, J.B. (2017) 'A proposed cloud security framework for service providers in Ghana', International Journal of Computer Applications, 158(1), pp. 17–22. DOI: 10.5120/ijca2017912722.
48. Olabanji, S.O., Olaniyi, O.O., Adigwe, C.S., Okunleye, O.J. and Oladoyinbo, T.O. (2024) 'AI for identity and access management (IAM) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorization, and access control

within cloud-based systems', Asian Journal of Research in Computer Science, 17(3), pp. 38–56. DOI: 10.9734/ajrcos/2024/v17i3423.

49. Omoegun, G.O., Sunday, E.A., Essien, M.A. and Oluokun, O.A. (2024) 'Implementing smart automation solutions in medium-scale industries using SCADA systems', International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(5), pp. 1207–1231. DOI: 10.32628/CSEIT241061242.
50. Oyeyinka, I.F., Idowu, S. and Kuyoro, A. (2021) 'A symbolic attribute-based access control model for data security in the cloud', ITEGAM-JETIA, 7(29), pp. 36–46. DOI: 10.5935/jetia.v7i29.750
51. Rich, M.S. (2023) 'Enhancing Microsoft 365 security: Integrating digital forensics analysis to detect and mitigate adversarial behavior patterns', Forensic Sciences, 3(3), pp. 394–425. DOI: 10.3390/forensicsci3030030.
52. Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020) Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-207. (NIST)\
53. Sarkar, S., Choudhary, G., Shandilya, S.K., Hussain, A. and Kim, H. (2022) 'Security of zero trust networks in cloud computing: A comparative review', Sustainability, 14(18), 11213. DOI: 10.3390/su141811213.
54. Shibambu, A. and Moganedi, S. (2022) 'How working from home has affected South African industries? A cybersecurity culture perspective', in 2022 International Conference on Intelligent and Innovative Computing Applications (ICONIC), pp. 137–143. DOI: 10.59200/ICONIC.2022.015. (Mauricon)
55. Shittu, H. and Nabil, M. (2023) 'Smart supply chain management with attribute-based encryption access control', in 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), pp. 198–204. DOI: 10.1109/CCWC57344.2023.10099268
56. Shittu, H., Olagunju, F. and Shittu, M. (2024) 'Cyber physical resilience in digital substations: IoT-enabled adaptive protection for secure DER integration', International Journal of Science, Architecture, Technology and Environment, 1(3). DOI: 10.63680/ijsate032532.08.
57. Shittu, M.A., Adeniji, I.O., Shittu, H. and Opara, I.S. (2022) 'Blockchain-assisted secure data exchange architectures for SCADA-controlled power systems', Iconic Research and Engineering Journals, 6(3), pp. 359–380. DOI: 10.64388/IREV6I3-1714041.
58. Shittu, M.A., Shittu, H., Adeleke, O.J. and Adedokun, O.J. (2023) 'Digital twin modeling for real-time monitoring and fault detection in smart substations', International Journal of Industrial Engineering Research and Development, 14(2), pp. 25–44. DOI: 10.34218/IJIERD_14_02_003.

59. Sindiren, E. and Ciylan, B. (2019) 'Application model for privileged account access control system in enterprise networks', Computers & Security, 83, pp. 52–67. DOI: 10.1016/j.cose.2019.01.008.
60. Stanton, B.C., Theofanos, M.F., Prettyman, S.S. and Furman, S.M. (2016) 'Security fatigue', IT Professional, 18(5), pp. 26–32. DOI: 10.1109/MITP.2016.84.
61. Syed, N.F., Shah, S.W., Shaghaghi, A., Anwar, A., Baig, Z.A. and Doss, R. (2022) 'Zero Trust Architecture (ZTA): A comprehensive survey', IEEE Access, 10, pp. 57143–57179. DOI: 10.1109/ACCESS.2022.3174679.
62. Teerakanok, S., Uehara, T. and Inomata, A. (2021) 'Migrating to Zero Trust Architecture: Reviews and challenges', Security and Communication Networks, 2021, Article 9947347. DOI: 10.1155/2021/9947347.
63. Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., Markov, Y., Comanescu, O., Eranti, V., Moscicki, A., Margolis, D., Paxson, V. and Bursztein, E. (2017) 'Data breaches, phishing, or malware? Understanding the risks of stolen credentials', in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1421–1434. DOI: 10.1145/3133956.3134067.
64. Tsai, M., Lee, S. and Shieh, S.W. (2024) 'Strategy for implementing Zero Trust Architecture', IEEE Transactions on Reliability, 73(1), pp. 93–100. DOI: 10.1109/TR.2023.3345665.
65. Unsel, V., Wiefling, S., Gruschka, N. and Lo Iacono, L. (2023) 'Risk-based authentication for OpenStack: A fully functional implementation and guiding example', in Proceedings of the 13th ACM Conference on Data and Application Security and Privacy, pp. 237–243. DOI: 10.1145/3577923.3583634.
66. Van der Schyff, K. and Krauss, K. (2014) 'Higher education cloud computing in South Africa: Towards understanding trust and adoption issues', South African Computer Journal, 55, pp. 40–55. DOI: 10.18489/sacj.v55i0.254.
67. Vanickis, R., Jacob, P., Dehghanzadeh, S. and Lee, B. (2018) 'Access control policy enforcement for Zero-Trust-Networking', in 29th Irish Signals and Systems Conference (ISSC 2018), Article 8585365. DOI: 10.1109/ISSC.2018.8585365.
68. Wiley, A., McCormac, A. and Calic, D. (2020) 'More than the individual: Examining the relationship between culture and information security awareness', Computers & Security, 88, 101640. DOI: 10.1016/j.cose.2019.101640.
69. Xiao, S., Ye, Y., Kanwal, N., Newe, T. and Lee, B. (2022) 'SoK: Context and risk-aware access control for Zero Trust systems', Security and Communication Networks, 2022, Article 7026779. DOI: 10.1155/2022/7026779.
70. Yeboah-Boateng, E.O. and Kwabena-Adade, G.D. (2020) 'Remote access communications security: Analysis of user authentication roles in organizations', Journal of Information Security, 11(3), pp. 161–175. DOI: 10.4236/jis.2020.113011

71. Yeoh, W., Liu, M., Shore, M. and Jiang, F. (2023) 'Zero trust cybersecurity: Critical success factors and a maturity assessment framework', Computers & Security, 133, 103412. DOI: 10.1016/j.cose.2023.103412.