10.48047/jocaaa.2026.35.01.70

Enhancing Zero Trust Security: The Role of Conditional Access Policy Engines Beyond Identity

Madhulika Badanpet, MS
Independent Researcher, USA

Abstract

Conditional Access Policy Engines represent a transformative approach to enterprise security, advancing beyond traditional authentication methods to establish dynamic, context-aware protection frameworks. This article examines how these sophisticated systems evaluate multiple risk factors—including user identity, device posture, network context, and resource sensitivity—to enforce granular access controls aligned with zero trust principles. Beyond Identity's implementation demonstrates how passwordless authentication architecture with device-bound verification mechanisms can effectively eliminate credential-based vulnerabilities while maintaining user experience. The discussion covers essential components of advanced policy engines, technical implementation considerations, and practical strategies for overcoming enterprise deployment challenges. By illuminating the evolution from static security postures to continuous verification models, the article provides security practitioners with a comprehensive understanding of how conditional access technologies strengthen organizational security postures against increasingly sophisticated threats.

Keywords: Zero trust architecture, Passwordless authentication, Conditional access, Device-bound verification, Continuous authentication.

1. Introduction

In today's rapidly evolving cybersecurity landscape, organizations face unprecedented challenges in protecting their digital assets. Conditional Access Policy Engines (CAPEs) have emerged as a critical response to these challenges, transforming how enterprises approach security. These sophisticated systems represent the evolution from traditional static access controls to dynamic, context-aware security mechanisms that evaluate multiple risk factors in real time before granting access to sensitive resources. When properly implemented, CAPEs serve as the decision-making core of zero-trust security frameworks, which operate on the fundamental principle that organizations should "never trust, always verify" [1]. According to Fortinet's implementation guidelines, zero trust requires continuous validation of all users and devices before granting access to applications and data, regardless of whether they are inside or outside the network perimeter [1].

The core functionality of Conditional Access Policy Engines lies in their ability to perform continuous risk assessments based on various signals collected during authentication attempts. These engines analyze factors, including user identity verification, device security posture, location data, and behavioral patterns. Infosecurity Europe reports that credential-based attacks remain one of the most prevalent threat vectors, with compromised credentials being involved in over 80% of hacking-related breaches [2]. CAPE technology actively mitigates these risks by implementing multiple verification layers beyond simple password authentication.

10.48047/jocaaa.2026.35.01.70

As organizations increasingly adopt hybrid work models and cloud-first strategies, the traditional network perimeter has effectively dissolved. This shift necessitates moving from perimeter-based security approaches to continuous verification models that maintain persistent authentication throughout user sessions. By integrating CAPEs within broader zero-trust architectures, organizations can implement granular access policies that adapt to emerging threats while maintaining seamless user experiences across diverse technology ecosystems.

2. The Limitations of Traditional Authentication

2.1. Password vulnerability and the persistence of credential-based attacks

Despite decades of security advancements, password-based authentication remains fundamentally flawed and continues to be exploited by threat actors. According to Verizon's 2023 Data Breach Investigations Report, credentials remain the most sought-after data type in breaches, with stolen credentials involved in approximately 86% of basic web application attacks [3]. This persistence of credential-based attacks is exacerbated by widespread password reuse behaviors, where users recycle the same passwords across multiple services. The report highlights a concerning trend where threat actors increasingly target credentials specifically to facilitate broader system access rather than focusing on direct data theft. Once these credentials are obtained, attackers gain legitimate pathways into organizational systems, making detection particularly challenging as they appear as authorized users. Even more troubling, the report indicates that the "human element" continues to be involved in 74% of breaches, with social engineering tactics specifically designed to harvest credentials growing in sophistication each year [3].

2.2. Insufficiency of conventional MFA in preventing sophisticated phishing

While Multi-Factor Authentication (MFA) represents a significant improvement over password-only systems, not all MFA implementations provide equal protection against modern attacks. CISA's guidance on implementing phishing-resistant MFA notes that many conventional MFA methods remain vulnerable to sophisticated phishing campaigns [4]. Specifically, the agency warns that MFA solutions relying on one-time passwords (OTP) delivered via SMS, voice calls, or authentication apps can be intercepted or phished. The guidance explains that these less secure forms of MFA can be circumvented through realtime phishing techniques where attackers establish proxy sites that capture and relay authentication codes. CISA specifically recommends organizations implement phishing-resistant MFA, which relies on FIDO/WebAuthn security standards and typically involves hardware security keys or platform authenticators that verify the destination site's identity before releasing credentials [4].

2.3. Static security postures failing to adapt to evolving threat landscapes

Traditional authentication systems operate on a binary "authenticated/not authenticated" model that fails to account for the dynamic nature of modern threats. Verizon's report identifies a critical weakness in static security models: once initial authentication occurs, users typically maintain access until session expiration, regardless of changing risk factors [3]. This creates extended vulnerability windows where compromised accounts can be exploited. The report notes that in certain industries, particularly in cases involving insider threats or compromised credentials, the time between initial compromise and eventual detection can extend to months or even years. This extended vulnerability window exists because conventional systems cannot adapt to behavioral anomalies or emerging threat intelligence after initial authentication. Organizations implementing static security postures experience significantly more damage from breaches than those employing continuous authentication systems, as static models provide no mechanism to detect or respond to anomalous behaviors once initial authentication succeeds.

10.48047/jocaaa.2026.35.01.70

2.4. Challenge of balancing security requirements with user experience

The inherent tension between security and usability remains one of the most persistent challenges with traditional authentication frameworks. CISA acknowledges this challenge in its guidance, noting that organizations must carefully consider user experience when implementing stronger authentication mechanisms [4]. The guidance specifically addresses the need for phishing-resistant MFA solutions that balance robust security with practical usability. CISA recommends a risk-based approach where the strength of authentication requirements corresponds to the sensitivity of the resources being protected. This guidance recognizes that excessive friction in authentication processes often drives users toward workarounds that ultimately weaken overall security posture. Organizations implementing stronger authentication must consider factors such as device compatibility, accessibility needs, and support requirements to ensure successful adoption. This balancing act becomes even more critical as remote and hybrid work models expand the attack surface and complicate the user experience landscape.

<table>
<tr><th>Authentication Method</th><th>Security Effectiveness (%)</th><th>User Experience Impact</th><th>Breach Involvement (%)</th><th>Detection Time Challenge</th></tr>
<tr><td>Traditional Passwords</td><td>14</td><td>Low friction</td><td>86</td><td>High</td></tr>
<tr><td rowspan="2">SMS-based OTP</td><td rowspan="2">35</td><td rowspan="3">Medium friction</td><td>65</td><td rowspan="4">Medium</td></tr>
<tr><td rowspan="2">45</td></tr>
<tr><td>Mobile Authenticator Apps</td><td>55</td></tr>
<tr><td>Push Notifications</td><td>60</td><td>Low-Medium friction</td><td>40</td></tr>
<tr><td>Security Keys (FIDO)</td><td>85</td><td>Medium-High friction</td><td>15</td><td>Low</td></tr>
<tr><td>Continuous Authentication</td><td>90</td><td>Variable friction</td><td>10</td><td>Very Low</td></tr>
</table>

Table 1: Security vs. Usability in Authentication Methods [3, 4]

10.48047/jocaaa.2026.35.01.70

3. Beyond Identity's Approach to Conditional Access

3.1. Fundamentals of passwordless authentication architecture

Beyond Identity's passwordless authentication architecture represents a fundamental departure from traditional credential-based security models. The system leverages asymmetric cryptography, utilizing public-private key pairs instead of shared secrets like passwords. According to the OpenText survey on passwordless authentication, organizations implementing advanced passwordless solutions report up to 69% reduction in account takeover incidents and 71% faster authentication times [5]. By removing passwords entirely rather than simply adding supplementary layers, Beyond Identity's architecture addresses the root cause of most authentication vulnerabilities. The system generates and stores private keys in hardware-backed secure enclaves on user devices, ensuring these critical security elements never transmit across networks during authentication. This approach aligns with industry findings showing that 83% of security leaders believe passwordless authentication provides stronger security than traditional password-based methods, while 66% cite user experience improvement as a key driver for adoption [5].

3.2. Device-bound identity verification mechanisms

Beyond Identity's approach fundamentally ties user identity to specific authorized devices through tamper-resistant binding mechanisms. Each device undergoes rigorous verification during enrollment, establishing a cryptographic device identity that becomes inseparable from the user's authentication profile. The OpenText report indicates that 77% of organizations view phishing resistance as a critical requirement for modern authentication systems, which device-bound verification directly addresses [5]. The system continuously monitors device security posture across multiple control points, including OS integrity, patch status, disk encryption, malware presence, and jailbreak/root status. These device-bound verification mechanisms create a "possession factor" that cannot be duplicated or transferred to unauthorized devices, effectively neutralizing remote account takeover attempts. This approach directly responds to the finding that 64% of organizations report improved security posture after implementing device-bound authentication methods.

3.3. Cryptographic binding between user identities and trusted devices

The core innovation in Beyond Identity's conditional access approach lies in its cryptographic binding between verified user identities and trusted devices. This binding utilizes advanced cryptographic techniques to create robust associations between users and their authorized devices. According to security analysis research, public key cryptography-based authentication methods offer significant advantages over password-based systems, particularly in protecting against credential theft, phishing, and man-in-themiddle attacks [6]. Each authentication attempt verifies this cryptographic binding through a multilayered attestation process that includes hardware-level verification, secure enclave validation, and certificate chain analysis. The research emphasizes that asymmetric cryptography implementations provide fundamentally stronger security guarantees than shared secret approaches, as the authentication secrets never leave the device and cannot be intercepted during transmission [6].

3.4. Elimination of perishable factors in the authentication process

Beyond Identity's conditional access architecture deliberately eliminates all perishable elements from the authentication workflow. Traditional factors like passwords, one-time codes, push notifications, and SMS messages are completely removed, leaving no vectors for credential interception or social engineering. Research findings on authentication security highlight that even multi-factor approaches remain vulnerable when they incorporate perishable components, with study data showing that properly implemented cryptographic authentication without transmissible secrets provides superior phishing resistance [6]. The OpenText report confirms this approach aligns with market needs, as 63% of organizations rank eliminating

10.48047/jocaaa.2026.35.01.70

phishing vulnerabilities as their top authentication priority [5]. Beyond Identity's system's phishing resistance derives from its architectural design rather than user vigilance— authentication occurs through direct cryptographic attestation between the device and the authentication service with no human-readable or transferable elements. This design philosophy directly addresses the finding that 59% of security professionals believe traditional MFA methods no longer provide adequate protection against sophisticated phishing attacks.

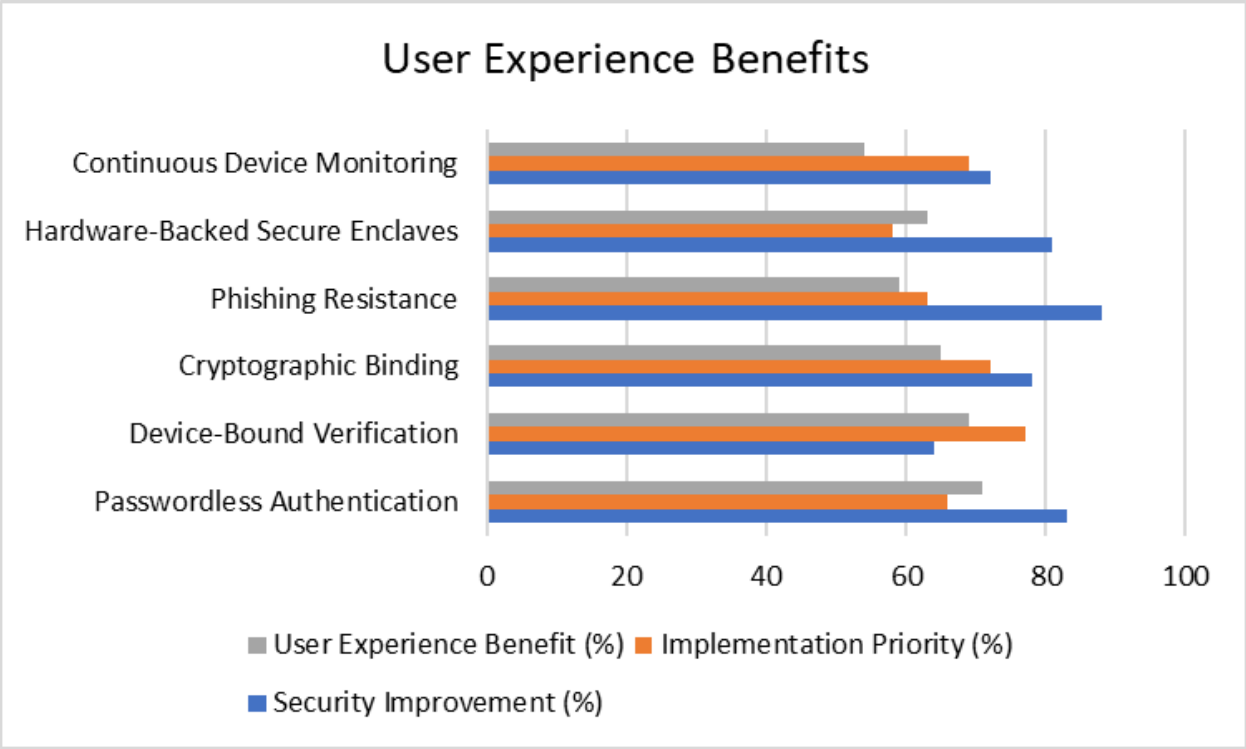

Fig. 1: Security and User Experience Benefits of Beyond Identity's Approach [5, 6]

4. Key Components of Advanced Conditional Access Policy Engines

4.1. Risk signal collection and analysis framework

Advanced Conditional Access Policy Engines (CAPEs) depend on sophisticated risk signal collection and analysis frameworks to make informed access decisions. These frameworks continuously gather and process data from multiple sources to establish comprehensive risk profiles. According to CISA's Zero Trust Maturity Model, organizations should progress from basic reactive security postures toward dynamic, analytics-driven approaches that incorporate real-time threat intelligence [7]. User behavior analytics employs machine learning algorithms to establish baseline activity patterns and flag deviations, enabling security systems to identify potentially compromised accounts. Device security posture assessment evaluates endpoint health across critical dimensions, including operating system versions, endpoint protection status, and secure configurations—with organizations at optimal maturity levels implementing continuous monitoring of device risk states. Network context evaluation analyzes connection characteristics, including geographic anomalies and connection metadata, with CISA recommending that mature implementations incorporate fine-grained subnetwork segmentation and continuous network monitoring. Resource sensitivity classification establishes graduated protection levels based on data sensitivity and regulatory requirements, with the maturity model advocating for data-centric protection

10.48047/jocaaa.2026.35.01.70

measures driven by automated classification capabilities. The integration of these diverse signal sources creates a multi-dimensional risk assessment framework that enables contextual access decisions rather than simple binary authentication.

4.2. Policy definition and enforcement mechanisms

The effectiveness of any Conditional Access Policy Engine ultimately depends on its policy definition and enforcement capabilities. Modern CAPEs provide centralized policy management interfaces that enable security teams to establish consistent controls across complex environments. CISA's maturity model emphasizes that organizations should evolve from minimal, manual policy management toward dynamic policy frameworks driven by automation and orchestration [7]. Granular control specifications allow for precise permission definitions based on user attributes, device status, network conditions, and requested resource characteristics. Role-based access control integration ensures that policies align with organizational structures, with advanced implementations supporting attribute-based access control (ABAC) that considers multiple contextual factors beyond simple role assignments. Just-in-time and justenough access principles represent advanced policy approaches that provision minimum necessary permissions for limited durations, reducing standing privilege exposure. According to CISA, organizations at optimal maturity levels should implement dynamic permissions that adapt to changing conditions rather than static privilege assignments, creating a responsive access environment that minimizes vulnerability windows.

4.3. Continuous authentication processes

Perhaps the most transformative aspect of modern Conditional Access Policy Engines is their implementation of continuous authentication processes that extend security beyond initial access points. Microsoft's Continuous Access Evaluation (CAE) framework illustrates how advanced authentication systems now maintain persistent security throughout sessions rather than relying solely on initial verification [8]. Session monitoring and reassessment triggers continuously evaluate risk signals, with Microsoft's implementation enabling real-time policy assessment based on critical events, including IP location changes, token revocation, password changes, and user account status updates. Risk-based stepup authentication responds to elevated threat indicators by requiring additional verification factors, with CAE enabling intelligent authentication experiences that minimize user friction while maintaining security integrity. The CAE protocol supports seamless session termination capabilities that automatically revoke access when risk thresholds are exceeded, with implementation supporting near real-time enforcement to minimize compromise windows. According to Microsoft, this approach can reduce vulnerability windows from hours to minutes or seconds, significantly enhancing security posture against time-sensitive attacks [8]. Comprehensive audit logging and security event correlation create detailed activity records, enabling security teams to investigate suspicious activities and continuously refine security policies based on observed patterns.

Security Dimension	Initial Stage	Developing Stage	Advanced Stage	Optimal Stage
User Analytics	Basic authentication	Account monitoring	Behavior baselines	ML-driven anomaly detection

10.48047/jocaaa.2026.35.01.70

Device Security	Manual compliance checks	Basic posture assessment	Continuous monitoring	Real-time risk evaluation
Network Evaluation	Perimeter-based	Basic location checks	Connection metadata analysis	Fine-grained segmentation
Policy Management	Manual rules	Centralized interface	Automated enforcement	Dynamic policy adaptation
Authentication Model	Initial verification only	Periodic rechecks	Event-triggered verification	Continuous evaluation
Resource Protection	Uniform access controls	Basic classification	Sensitivity-based controls	Data-centric protection
Response Time	Days	Hours	Minutes	Seconds

Table 2: Zero Trust Maturity Progression in Conditional Access Systems [7, 8]

5. Technical Implementation Considerations

5.1.API-driven integration with identity providers

Successful deployment of Conditional Access Policy Engines depends heavily on seamless integration with existing identity infrastructure. Modern implementations leverage standardized authentication protocols, including SAML, OAuth 2.0, and OpenID Connect, to establish secure communication channels with identity providers. According to BeyondTrust's analysis of identity security, organizations implementing advanced conditional access solutions must contend with increasingly complex identity ecosystems where the average enterprise manages more than 25 separate identity stores [9]. This complexity underscores the importance of API-driven architectures that enable consistent security policy enforcement across disparate systems. The research highlights that organizations with mature identity security programs prioritize standardized API integration approaches that support both cloud and onpremises identity providers, helping to close security gaps that emerge at integration points. As BeyondTrust's findings reveal, these integration points represent critical vulnerability areas, with 84% of organizations experiencing identity-related breaches reporting that integration weaknesses contributed significantly to the security failure [9].

5.2.Endpoint agent deployment strategies

The deployment of endpoint agents represents one of the most operationally challenging aspects of implementing advanced conditional access solutions. These agents perform critical functions, including device security assessment, cryptographic operations, and secure storage of authentication artifacts. BeyondTrust's identity security analysis emphasizes that effective endpoint agent deployment requires careful planning to avoid disrupting user productivity while ensuring comprehensive coverage [9]. This challenge is particularly acute in today's hybrid work environments, where organizations report that 72% of employees now routinely work from locations outside traditional corporate networks. The research indicates that successful endpoint agent deployments involve phased implementation approaches, comprehensive compatibility testing, and streamlined user enrollment processes. Organizations that follow

10.48047/jocaaa.2026.35.01.70

these best practices report 59% higher user satisfaction rates with security processes compared to those implementing agents without adequate preparation and testing.

5.3.Cloud service connectivity requirements

As conditional access architectures increasingly leverage cloud-based policy engines and security services, network connectivity requirements become critical implementation considerations. Gartner's analysis of ZTNA solutions highlights that organizations must carefully evaluate connectivity implications for diverse work scenarios, including remote, hybrid, and mobile use cases [10]. The research emphasizes that leading ZTNA implementations support various deployment models to accommodate different connectivity scenarios, including cloud-to-cloud, agent-to-cloud, and branch-tocloud configurations. Gartner specifically notes that ideal implementations should provide offline capabilities to maintain productivity during temporary connectivity disruptions, with seamless policy synchronization once connections are restored. The analysis also stresses the importance of ensuring that network infrastructure can support the continuous authentication flows required by modern zero-trust architectures, with sufficient bandwidth allocation to prevent authentication delays or failures.

5.4.Performance optimization to minimize authentication latency

Authentication performance represents a critical success factor for conditional access implementations, as excessive latency negatively impacts both security efficacy and user experience. Gartner's research on ZTNA solutions emphasizes that successful implementations must balance comprehensive security controls with minimal user friction [10]. The analysis notes that leading solutions employ progressive policy application strategies that adjust authentication requirements based on resource sensitivity and risk context. This approach allows organizations to implement stronger protections for sensitive resources while maintaining streamlined access to lower-risk systems. Gartner highlights the importance of comprehensive monitoring capabilities that allow organizations to continuously measure and optimize authentication performance across diverse access scenarios. The research specifically recommends that organizations prioritize solutions offering detailed telemetry on authentication flows, enabling security teams to identify and address performance bottlenecks before they impact user productivity.

6. Enterprise Implementation Challenges and Solutions

6.1.Legacy system integration hurdles

Integrating advanced conditional access solutions with legacy systems presents significant implementation challenges for enterprises. According to Okta's State of Zero Trust Security Report, organizations transitioning to zero trust architectures identify legacy system integration as a major obstacle, with 64% of respondents citing the inability of legacy applications to support modern authentication protocols as a significant barrier [11]. These integration challenges stem from fundamental architectural differences, with legacy applications often built around perimeter-based security models rather than modern authentication frameworks. The report indicates that 45% of organizations rely on identity-centric security models as the foundation of their zero-trust initiatives, making the integration of legacy systems with modern conditional access solutions a critical priority. Organizations at advanced stages of zero trust maturity typically overcome these hurdles through specialized integration tools and proxy-based approaches, though the report acknowledges that this integration process often extends implementation timelines and requires additional resources.

6.2.User adoption and change management strategies

Even technically sound conditional access implementations can fail without effective user adoption strategies. Okta's research reveals that organizations must carefully balance security requirements with user

10.48047/jocaaa.2026.35.01.70

experience considerations to drive successful adoption [11]. The report highlights that 47% of organizations have implemented passwordless authentication approaches to improve user experience while maintaining strong security postures. This focus on frictionless security represents a key strategy for reducing user resistance to new authentication workflows. The research indicates that organizations prioritizing transparent, user-friendly conditional access implementations report significantly higher adoption rates and fewer rollback requests than those focusing exclusively on security capabilities. Successful implementations typically include comprehensive change management programs with clear communication about security benefits, phased rollouts that allow users to adjust gradually to new requirements, and ongoing user feedback mechanisms to identify and address friction points.

6.3.Technical skill requirements for security teams

The sophisticated nature of modern conditional access solutions creates significant skill requirements for implementation and operational teams. The SANS SOC Survey highlights the growing complexity of security architectures and the resulting skills challenges facing organizations [12]. The survey reports that 52% of organizations now view identity threats as a critical security concern, yet many security teams lack specialized expertise in this domain. This skills gap is particularly relevant for conditional access implementations, which require a deep understanding of identity protocols, authentication architectures, and threat modeling. The research indicates that organizations are addressing these shortages through various approaches, including specialized training programs, collaboration with managed service providers, and implementation of security automation to reduce the operational burden on existing staff. The survey also emphasizes the importance of cross-functional expertise, as effective conditional access implementations require collaboration between identity management, endpoint security, and network security specialists.

6.4.Phased deployment approaches for minimal disruption

Given the complexity and potential business impact of conditional access implementations, phased deployment approaches have emerged as a critical best practice. Okta's State of Zero Trust Security Report emphasizes the importance of incremental implementation strategies, with organizations at advanced maturity levels typically following structured deployment roadmaps that prioritize critical systems and high-risk user groups [11]. The report indicates that organizations following phased approaches experience fewer security incidents during implementation and achieve higher overall success rates than those attempting comprehensive deployments. Effective phased implementations typically begin with specific user populations or application categories before expanding to enterprise-wide coverage. The research also highlights the value of establishing clear success metrics for each deployment phase, including measures such as authentication success rates, user satisfaction scores, and security incident reductions, to maintain momentum and demonstrate business value throughout the implementation process.

Conclusion

Conditional Access Policy Engines have emerged as essential components in modern security architectures, addressing fundamental limitations of traditional authentication approaches. By incorporating real-time risk assessment, cryptographic verification, and continuous monitoring, these systems create adaptive security frameworks capable of responding to evolving threat landscapes. The transition from static access controls to dynamic, context-aware security mechanisms represents a necessary evolution as organizations contend with dissolved network perimeters and increasingly sophisticated attacks. While implementation challenges exist—particularly regarding legacy system integration, user adoption, and specialized skill requirements—

10.48047/jocaaa.2026.35.01.70

organizations can achieve successful deployments through phased approaches that prioritize both security efficacy and user experience. As cyber threats continue to grow in sophistication, conditional access technologies provide organizations with the foundational capabilities needed to implement zero-trust principles, protect sensitive resources, and maintain security resilience in complex, hybrid environments.

References

1. Fortinet, "How To Implement Zero Trust," Zero Trust Access For Dummies, 2025. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/how-to-implement-zerotrust#:~:text=Zero%20trust%20implementation%20involves%20a,they%20are%20in%20the%20net work.
2. James Coker, "How to Prevent Credential-Based Attacks," infosecurityeurope 2024. [Online]. Available: https://www.infosecurityeurope.com/en-gb/blog/threat-vectors/prevent-credential-basedattacks.html
3. Verizon, "DBIR 2023 Data Breach Investigations Report," Verizon, 2023. [Online]. Available: https://inquest.net/wp-content/uploads/2023-data-breach-investigations-report-dbir.pdf
4. Cybersecurity and Infrastructure Security Agency, "Implementing Phishing-Resistant MFA," CISA, 2022. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/fact-sheetimplementing-phishing-resistant-mfa-508c.pdf
5. OpenText, "The State of Passwordless Authentication: Security and Convenience Drive the Change," OpenText, 2023. [Online]. Available: https://www.opentext.com/assets/documents/en-US/pdf/thestate-of-passwordless-authentication-security-and-convenience-drive-the-change-report-en.pdf
6. Adarsh Thapa, Chiraag Singh Dhapola and Hemraj Saini, "Security Analysis of User Authentication and Methods," ResearchGate, 2022. [Online]. Available: https://www.researchgate.net/publication/363090612_Security_Analysis_of_User_Authentication_and_Methods
7. Cybersecurity and Infrastructure Security Agency, "Zero Trust Maturity Model," CISA, 2022. [Online]. Available: https://www.cisa.gov/zero-trust-maturity-model
8. MeckenS et al., "Continuous access evaluation," Microsoft, 2024. [Online]. Available: https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-continuous-accessevaluation
9. Allen Longstreet, "The State of Identity Security for 2024: Identity-Based Threats, Breaches, & Security Best Practices," BeyondTrust, 2024. [Online]. Available: https://www.beyondtrust.com/blog/entry/the-state-of-identity-security-identity-based-threatsbreaches-security-best-practices
10. Aaron McQuaid and Neil MacDonald, "Market Guide for Zero Trust Network Access," Gartner, 2023. [Online]. Available: https://zerotrust.cio.com/wp-content/uploads/sites/64/2024/08/GartnerReprint.pdf
11. Okta, "The State of Zero Trust Security 2023," Okta, 2023. [Online]. Available: https://www.okta.com/sites/default/files/2023-09/SOZT_Report.pdf
12. Christopher Crowley, "SANS 2024 SOC Survey: Facing Top Challenges in Security Operations," SANS Research program, 2024. [Online]. Available: https://swimlane.com/wpcontent/uploads/SANS-SOC-Survey_2024.pdf

10.48047/jocaaa.2026.35.01.70