Infosys cobalt

VIEW POINT

NAVIGATING CLOUD SECURITY AND IDENTITY MANAGEMENT IN THE MODERN WORLD

Quest

Infosys®
Navigate your next

The Dynamic Security Landscape: Navigating the Cloud-first World

Today, 'cloud-first' isn't just a buzzword but a business imperative, fundamentally shifting the rules of security. According to recent studies, over 80% of companies have experienced at least one cloud-related security incident in 2024[1]. High-profile breaches have exposed sensitive customer data, disrupted operations, and eroded trust, underscoring the urgency of a modernized security approach. These aren't isolated incidents but stark reminders that traditional security paradigms struggle to keep pace.

The core problem? Modern threats are complex, dynamic, and intimately intertwined with the very fabric of cloud environments. We're no longer dealing with a static perimeter. Instead, we're navigating a rapidly expanding attack surface fueled by ubiquitous connectivity, frictionless data sharing, and the rise of remote work.

The question is no longer if an attack will happen, but when and how prepared an enterprise is to mitigate its impact. That's why this paper explores the critical role of cloud security and identity management in this dynamic landscape, offering insights and strategies to navigate these complex challenges.

The Modern Attacker

We must first understand the adversary to effectively combat the challenges they present. The modern attacker is not the lone hacker in a basement that we see in movies; they are sophisticated, well-funded, and remarkably adaptable cybercriminals who leverage automation, AI-driven tools, and social engineering tactics to bypass traditional defenses. They operate with professionalism and persistence that demands a similarly advanced defense. Their arsenal is constantly evolving, targeting vulnerabilities across the entire cloud ecosystem.

[1] *50 Cloud Security Stats You Should Know In 2025 | Expert Insights*

Five Key Security Considerations

Modern attacks exploit weaknesses across these five layers:

Infrastructure

- Cloud misconfigurations, exposed APIs, and unpatched vulnerabilities in virtual machines or containers create easy entry points for attackers.

Data

- Sensitive customer and business data stored in the cloud are prime targets for ransomware and data exfiltration.

Endpoint Devices

- The proliferation of IoT and edge computing introduces new risks.

Identity

- With cloud adoption, identity is now the primary attack vector. Phishing, credential stuffing, and MFA fatigue attacks are increasing, targeting users rather than infrastructure.

Applications

- Web and mobile applications are gateways to critical systems, making them attractive targets for zero-day exploits and injection attacks.

To truly protect our digital assets, we must recognize the interconnectedness of these five aspects.

Furthermore, the proliferation of technology-related threats has exponentially increased the possibilities of attack. Imagine a compromised IoT device embedded within a critical mining or manufacturing machine. This could not only lead to data breaches but also physical disruption and even safety hazards. These devices, integral to modern operations, expand the attack surface significantly. Cloud computing has compounded these challenges through shared responsibility models, multi-cloud complexity, and widespread misconfigurations that now represent leading causes of data breaches.

In the past, attackers primarily focused on breaking into infrastructure—hacking firewalls, exploiting servers, and breaching data centers. But in the cloud-first era, identity has become the new perimeter. Threat actors are shifting their strategies to compromise credentials and manipulate access controls. Attackers exploit cloud-specific vulnerabilities—from lateral movement and privilege escalation to supply chain and CI/CD pipeline attacks. Manual processes can't keep up, making a robust identity-centric security strategy no longer optional but necessary.

That's where Microsoft Entra ID can help —providing intelligent, automated identity and access management across cloud environments. As AI and cloud-native development accelerate, securing APIs, machine identities, and development pipelines is just as critical.

In short, modern cloud security isn't just about tools—it's about a proactive, identity-first mindset.

Entra ID: Microsoft's Solution to Identity Security

Microsoft Entra ID is a comprehensive cloud-based identity and access management service. Far beyond a traditional directory service, Entra ID is a critical control plane that secures access to cloud environments across the entire digital estate – internal and external. Its powerful capabilities significantly enhance cloud security posture:

- **Single Sign-On (SSO)**
- **Multi-Factor Authentication (MFA)**
- **Conditional Access**

- **Identity Protection & AI-powered Threat Detection**
- **Privileged Identity Management (PIM)**

Microsoft Entra ID plays a critical role in mitigating common security threats, such as:

Phishing and Credential-Based Attacks

Eliminate password risks with phishing-resistant MFA and passwordless options (like FIDO2 and Windows Hello).

Detect account takeovers through lateral movement, brute-force attacks, and monitoring of unusual behavior via Defender for Identity.

Credential Stuffing & MFA Fatigue

Microsoft Entra ID's Identity Protection uses AI to detect and block credential stuffing by flagging unusual logins and suspicious activity.

A Holistic Approach to Modern Security

While Microsoft Entra ID is a cornerstone of modern cloud security, it's crucial to understand that it's a vital piece of a broader strategy, not a singular solution. A truly robust defense requires a multi-layered, **'defense in depth'** approach, encompassing both precautionary and post-breach measures.

Precautionary Steps

Zero Trust Security Model

- The "never trust, always verify" approach ensures that access is continuously validated based on risk levels, device compliance, and contextual factors. In addition, policies, configurations, and any dependencies on on-prem infrastructure must be evaluated.

Identity-first Security Approach

- This includes Passwordless Authentication through biometrics, FIDO2 security keys, and certificate-based authentication, and Automated Identity Governance that uses AI-driven insights to detect anomalies, enforce least privilege access, and automate user lifecycle management.

Proactive Identity Threat Detection & Response

- Microsoft Defender and Microsoft Entra ID enable real-time monitoring and AI-driven threat detection. Additionally, Microsoft Sentinel enhances security analytics and automation, enabling faster responses to potential threats.
- Furthermore, Microsoft Security Copilot adds natural language insights and guided responses, boosting security team efficiency and confidence.
- Identity Threat Detection and Response (ITDR) is essential to strengthen this ecosystem—particularly in hybrid identity environments that span both on-premises Active Directory and Microsoft Entra ID. Quest Security Guardian is a purpose-built hybrid ITDR solution that integrates seamlessly across on-premises and cloud identity infrastructure and also includes the first-to-market Active Directory Security (AD) Copilot plugin, allowing security teams to leverage natural language capabilities and guided remediation for AD threats.

Backup and Recovery

- A robust defense-in-depth strategy implies creating and securely maintaining backups of Microsoft Entra ID configurations and data as a contingency measure
- While backup and recovery in Microsoft Entra ID is a shared responsibility between organizations and Microsoft, it's important to note that certain critical attributes—such as group memberships and Conditional Access policies like MFA—are not fully covered by native recovery options. Solutions like Quest On Demand Recovery provide enhanced protection, offering comprehensive backup and recovery capabilities beyond the default 30-day retention in Microsoft's recycle bin. On Demand Recovery backs up 4.2 billion Microsoft Entra ID objects monthly, totalling over 37 billion objects annually, and supports automation and advanced restore options to ensure rapid recovery and business continuity.

Security Awareness & User Training

- Human error remains the weakest link, so continuous security training helps employees recognize phishing attempts, social engineering tactics, and credential theft risks.

Post-Breach Steps

Rapid and decisive action is paramount in the unfortunate event of a breach.

Containment & Immediate Response

- **Force User Sign-outs:** Revoke active sessions and force re-authentication to limit attacker access.
- **Reset Compromised Credentials:** Force password resets for impacted accounts and enforce Passwordless authentication (FIDO2, biometrics) for high-privilege users.
- **Block or Restrict Affected Accounts:** Disable compromised accounts or apply risk-based access controls to limit exposure.
- **Remove Malicious App Access:** Terminate unauthorized OAuth apps and revoke suspicious consent grants.
- **Block Risky IPs and Locations:** Restrict access from suspicious IPs or geographies based on sign-in activity.

Recovery & System Hardening

- **Strengthen Identity Protection:** Enforce MFA for all users, especially privileged accounts; auto-block high-risk logins.
- **Secure Privileged Access:** Apply just-in-time access controls and monitor high-privilege role activations.
- **Disable Legacy Protocols:** Block outdated authentication methods to reduce attack surfaces.
- **Harden Access Policies:** Enforce device compliance, IP restrictions, and MFA for external users.
- **Implement Real-time Risk Response:** Enable continuous access evaluation to revoke access immediately when threats are detected.

Investigation & Root Cause Analysis

- **Analyze Logs for Anomalies:** Review sign-in and audit logs for unusual patterns, risky logins, or legacy authentication use.
- **Check for Privilege Escalation:** Investigate unauthorized role changes or admin access assignments.
- **Audit Security Policies:** Ensure policies are correctly applied and identify any unauthorized modifications.
- **Verify MFA and Device Integrity:** Check if attackers registered new MFA methods or compromised trusted devices.

Long-Term Security Improvements & Compliance

- **Conduct a Comprehensive Identity Audit:** Identify stale accounts, over-permissioned users, and unused apps or roles.
- **User & Admin Training:** Provide regular training on phishing, credential hygiene, and privileged account security.
- **Enhance Governance:** Automate access reviews, certification, and identity lifecycle management.

Implementing these comprehensive measures can significantly strengthen enterprise cloud security posture and mitigate the impact of potential breaches. Here are two real-life examples:

A global bank partnered with Quest Solutions to fortify its hybrid IT environment—spanning Active Directory and Cloud Identity. By leveraging Quest's integrated suite for proactive auditing, secure change control, and rapid, tamper-proof recovery, the bank strengthened its security posture, maintained compliance across regions, and ensured operational continuity—even during rigorous red team testing. The result: enhanced cyber resilience and reinforced customer trust.

Meanwhile, a leading wind energy firm elevated its security with Infosys' implementation of Microsoft 365 security tools. The solution safeguarded critical data, identities, devices, and applications across its operations. Infosys deployed Azure AD with MFA and conditional access for identity protection, Microsoft Information Protection (MIP) for data classification, and Intune for unified device management—significantly reducing workplace risk and boosting security maturity.

The Path Forward: Redefining Security for Tomorrow's Enterprise

As cloud adoption accelerates and identity becomes the new security frontier, organizations must rethink their entire approach—from siloed defenses to a unified, adaptive security fabric. Those who act decisively today, embedding identity-first principles into cloud strategies, won't merely survive the next wave of cyber threats—they'll thrive where security becomes a competitive advantage.

About the Authors

Anand Iyer

Vice President and Global Delivery Head, Infosys Microsoft Practice

Anand is an industry veteran with over 25 years of experience in consulting and IT services.
He has a flair for driving synergies and growth for both Infosys and the Microsoft ecosystem and is leading the delivery of innovative and exceptional solutions for digital workplace and business application customers. Anand has a proven track record of leading delivery across geographies for marquee clients of Infosys, including many large customers. He has helped large organizations restructure their teams to achieve better outcomes and efficiencies.

Anand is passionate about leveraging technology to create value for customers and society.
He has also been a champion of change, leading and participating in initiatives across performance management, culture transformation, diversity and inclusion, and next generation production support for organizations. Anand is a thought leader and has been published in several leading media publications.

Sergey Medved

Vice President, Product Management and Marketing, Quest Software

A product management veteran with over 15 years of experience, Sergey is on a mission to help enterprises protect identity infrastructure and discover, analyze, and address cyber security risks. As a VP of Product Management and Marketing at Quest Software, he is spearheading the investment into proactive identity threat detection and response, helping Quest solidify its position as a cyber resilience software market leader.

Sergey's professional background includes various leadership positions at public and private equity owned companies, including Oracle and ClearSlide. Most recently, he led commercial product management at ESW Capital / Trilogy, focusing on buying, strengthening, then growing mature software companies. Sergey started tinkering with Active Directory and Remote Desktop Protocol in High School and was an active contributor for a leading Russian-language technology newspaper.

Infosys Cobalt is a set of services, solutions and platforms for enterprises to accelerate their cloud journey. It offers over 35,000 cloud assets, over 300 industry cloud solution blueprints and a thriving community of cloud business and technology practitioners to drive increased business value. With Infosys Cobalt, regulatory and security compliance, along with technical and financial governance comes baked into every solution delivered

For more information, contact askus@infosys.com

Infosys®
Navigate your next