

EBOOK

Perspectives on Modernizing Identity in a Cloud and AI Era: A Security-First Approach

Executive summary

Identity modernization has become a strategic imperative for organizations embracing cloud services, hybrid environments, and AI-driven initiatives. At the same time, identity has emerged as the primary attack surface for modern adversaries. The convergence of these forces means that identity change — whether migration, consolidation, or modernization — is no longer a routine IT task. It can be one of the highest-risk moments in the security lifecycle.

Many organizations approach identity modernization with an understandable focus on speed, scale, and minimizing disruption. But identity systems are not just directories or authentication services. They control access to data, devices, applications, and administrative power. During periods of change, privileges shift, policies evolve, and trust relationships are redefined. These conditions create opportunity for attackers if identity security is not treated as foundational.

This e-book shares Quest's perspective on identity modernization in a cloud and AI era. It explores why identity changes during migration must be treated as significant security events, examines the emerging risks organizations face, and outlines the principles required to modernize identity safely while preserving productivity and strengthening long-term resilience.



Perspective 1

Identity is the new security perimeter

For years, security strategies focused on protecting networks, endpoints, and applications. Today, that perimeter has collapsed. Identity, both human and non-human, has become the control plane that governs nearly every digital interaction.

Attackers understand this. Rather than attempting to breach hardened infrastructure directly, they focus on compromising credentials, exploiting misconfigurations, and abusing excessive privileges. Once identity is compromised, lateral movement becomes trivial. Administrative access can be escalated, and trust can be exploited.

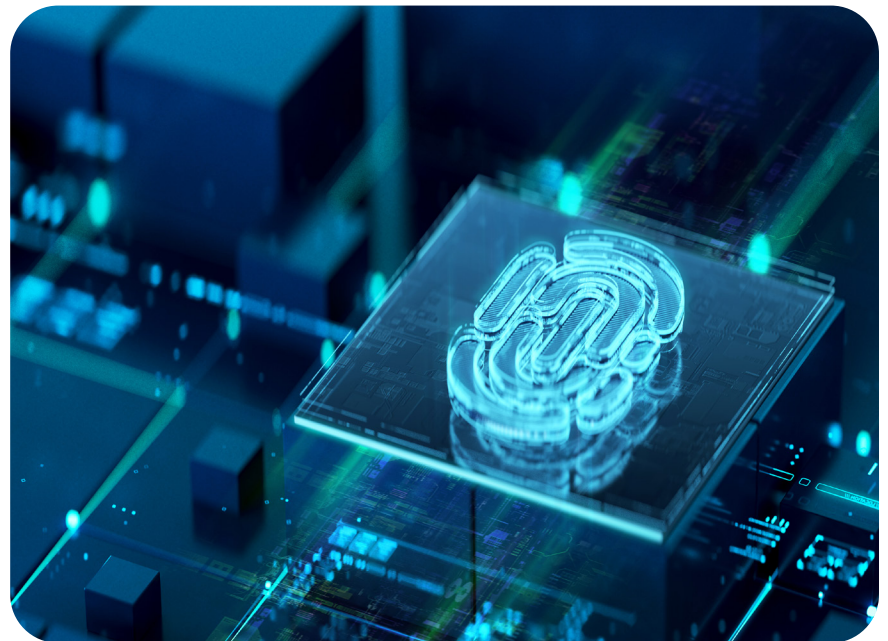
Modern enterprises rely on a complex identity ecosystem:

- On-premises directories alongside cloud identity platforms
- Multiple tenants and domains from historical decisions or M&A
- Devices, applications, and APIs tied to identity policies
- Increasing numbers of automated and AI-driven workloads

Identity modernization is about rationalizing and improving this ecosystem. Doing so safely requires recognizing identity as the foundation of security, not a supporting component.

Ask yourself...

If a privileged identity were compromised today, how quickly would we know?



Perspective 2

Why identity modernization is a high-risk moment

Identity modernization initiatives like directory consolidation, tenant migration, and cloud adoption often coincide with periods of intense operational change. Unfortunately, these same moments also create elevated security risk.

During identity transitions:

- Privileges are reassigned and often temporarily expanded
- Policies may diverge between source and target environments
- Coexistence introduces parallel authentication paths
- Visibility is fragmented across tools and platforms

What's often described as a "controlled migration" frequently feels more like controlled chaos. Highly sensitive assets such as identities, credentials, and access rights are all in motion at once.

A common mistake is treating migration as a neutral activity, something that only becomes a security concern once it's finished. In reality, the migration window itself is prime time for misconfigurations, orphaned access, and attacker opportunity.

Organizations that approach identity modernization with a "move first, secure later" mindset often discover they have carried legacy risk forward — sometimes amplifying it in the process.

Ask yourself...

How will you maintain consistent security controls while identities, access, and policies are in motion?



Perspective 3

The expanding identity surface – AI and non-human identities

One of the most underestimated aspects of identity modernization today is the rise of non-human identities.

Service principals, application identities, automation accounts, and AI agents now outnumber human users in many environments. These identities often:

- Operate without interactive authentication
- Use long-lived credentials
- Possess broad or poorly understood permissions
- Lack clear ownership

Unlike human users, non-human identities don't trigger MFA prompts or password resets. When compromised, they can operate quietly and at machine speed, enumerating environments, exfiltrating data, or persisting unnoticed.

As AI adoption accelerates, this problem compounds. Agents create agents. Workloads spin up dynamically. Identity inventories grow faster than governance models can evolve.

Modernizing identity without accounting for non-human identities isn't just incomplete. It's risky.

Ask yourself...

Who owns these identities, and how often is their access reviewed?



Perspective 4

Modernizing authentication and access control

Authentication and access control have evolved significantly in recent years, but many environments still rely on outdated assumptions.

Static credentials, long-standing permissions, and one-time access decisions are increasingly misaligned with modern threat realities. Phishing-resistant authentication, device-bound credentials, and continuous risk evaluation are becoming table stakes.

Equally important is recognizing that access control is not a one-time configuration exercise. It is a continuous process that must evolve as identities, devices, and workloads change.

A modern access strategy balances:

- Strong authentication without excessive friction
- Risk-based enforcement rather than blanket controls
- Protection of privileged users and roles first
- Productivity alongside security

Identity modernization creates an opportunity to realign access models, but only if those controls are preserved and strengthened during the transition.

Ask yourself...

Are our strongest authentication controls enforced consistently during change?



Perspective 5

Visibility, inventory, and governance must come first

One consistent theme across successful identity modernization efforts is this: you cannot secure what you cannot see.

Before identities are migrated, consolidated, or reorganized, organizations must understand:

- What identities exist
- What they have access to
- Which identities represent high-value targets
- Where trust relationships and dependencies lie

This includes human users, devices, applications, and non-human identities. It also includes legacy artifacts that may no longer serve a business purpose but continue to carry risk.

Effective identity modernization begins with assessment and governance. Migration then becomes an opportunity not just to move identities, but to reset practices, retire outdated constructs, and reduce long-term exposure.

Skipping this step often leads to unpleasant surprises mid-migration, when rollback options are limited and business impact is high.

Ask yourself...

Do we know exactly which identities, permissions, and trusts are in scope for migration?



Perspective 6

Incident response during identity change

Security incidents don't pause for modernization projects. In fact, identity changes during migration often increase the likelihood that something will go wrong.

Effective identity incident response during modernization requires preparation:

- Clear playbooks for human user and non-human identity compromise
- The ability to contain threats without destabilizing services
- Confidence-based response, not panic-driven disruption
- Recovery paths that return environments to known-good states

Disabling identities indiscriminately or tearing down access without understanding impact can cause more harm than the original threat. Mature organizations balance containment with continuity, acting decisively while preserving operations.

Modern identity platforms provide telemetry, but that telemetry is only valuable if it is unified, monitored, and actionable throughout the migration lifecycle.

Ask yourself...

If an identity-related incident occurred mid-migration, what would we do first?



Perspective 7

Secure migration as the foundation for modern identity

The most successful identity modernization initiatives share a common approach: security is embedded before, during, and after change.

Secure migration does not mean slowing down modernization. It means:

- Assessing identity risk upfront
- Preserving access controls and visibility during transition
- Protecting privileged access and trust boundaries
- Enabling rollback and recovery when assumptions fail
- Delivering a stronger security posture at the end — not just a new architecture

When security is treated as foundational rather than reactive, migrations become more predictable, less disruptive, and more valuable long-term.

Ask yourself...

Are we reducing identity risk or simply relocating it?

Organizations emerge with:

- Fewer identities and directories
- Cleaner access models
- Reduced attack surface
- Greater confidence supporting cloud, Zero Trust, and AI initiatives

Treat identity modernization as a significant security event

Identity modernization is not simply about where identities live. It's about how trust is established, enforced, and protected.

Every migration, consolidation, or modernization initiative represents a rare opportunity to improve security, but also a period of elevated risk if mishandled. The difference lies in approach.

Organizations that treat identity change as a significant security event — planned, governed, and protected — build a more resilient foundation for the future. Those that don't often find themselves carrying old problems into new platforms.

Modernization doesn't have to introduce risk or additional time to the project. With the right mindset, preparation, and expertise, it can do the opposite.

The Quest approach: Security and resilience built into every migration

Quest Secure Migration

Quest Secure Migration provides an end-to-end solution for modernizing your identity and collaboration environment across Active Directory, Entra ID, and Microsoft 365. Rather than stitching together point tools, Quest unifies identity, device, and workload transitions with security and resilience built in.

Real-time auditing protects change windows, while updating profiles and credentials without desk-side intervention. User continuity is maintained as you consolidate tenants, retire legacy domains, and reduce long-term operational risk. Delivered through an enterprise-grade SaaS platform with regional data residency and leading certifications — and backed by decades of identity expertise, 24/7 support, and AI-assisted troubleshooting — Quest helps you modernize with confidence, creating a cleaner, more resilient identity foundation for Zero Trust, tenant hygiene, and AI-driven initiatives.

Learn more about Quest Secure Migration at <https://www.quest.com/solutions/migration> or ask your Quest account team.

About Quest Software

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on X (formerly Twitter) and LinkedIn.

Explore our solutions →