

WHITE PAPER

5 critical challenges in identity security

Why identity is critical for modern businesses

Quest

Introduction

Active Directory (AD) and Entra ID comprise the backbone of modern identity management. In addition to serving as the primary identity store for most organizations today, AD and Entra ID provide vital authentication and authorization services that enable users to access the corporate resources they need to do their jobs — and keep everyone else out.

These critical functions make AD and Entra ID a top target of attackers. A hacker who compromises the credentials of a legitimate user can slip into the network and begin quietly escalating their privileges to reach increasingly sensitive data and systems. If they manage to acquire admin credentials, they can start wreaking havoc immediately."

Even worse, if attackers manage to bring down your identity infrastructure altogether, the business comes to a screeching halt. No one can log on, let alone perform mission-critical functions like processing transactions or serving customers.

The cost can be astronomical — a study by Forrester Consulting pegs the cost of AD downtime at US$730K per hour. The expenses can include lost productivity, theft or encryption of important data such as intellectual property (IP), lasting reputation damage, compliance penalties, and lawsuits and other legal expenses.

Unfortunately, many organizations today are far too exposed to these risks because they lack effective identity threat detection and response (ITDR) capabilities. This white paper explores the five key challenges involved in identity security and offers a strategy for overcoming them.

Challenge 1: Identity threats are exploding.

According to Microsoft, Entra ID suffers 600 million identity attacks per day (7,000 per second), and more than 99% of them are password-based. Credential theft has become one of the most common ways for attackers to gain access to corporate networks. By obtaining valid usernames and passwords through tactics like phishing or credential stuffing, adversaries can bypass traditional defenses and enter a system undetected. Moreover, organizations often use third-party federated identity providers that hook into Active Directory or Entra ID for authentication and authorization, and adversaries can use that connection to traverse into the organization's network.

> Entra ID suffers 600 million identity attacks per day, more than 99% of which are password-based.

Having valid credentials enables attackers to move laterally between systems and escalate their privileges with less chance of detection. Research shows that adversaries often lurk undetected in the network for days or even months until they are ready to complete their mission; for instance, Mandiant M-Trends Report 2025 pegs global median dwell time at 11 days.

In hybrid environments, lateral movement can include shifting between on-premises and cloud systems. For instance, Octo Tempest (formerly DEV-0875) is a cybercriminal group that has recently targeted a wide range of sectors, including retail, food services, hospitality, insurance companies and airlines. The group is known for using sophisticated social engineering, SMS phishing messages, SIM swapping and other tactics to gain initial access to an environment. Once inside, they proceed to lateral movement, privilege escalation and defense evasion techniques, and finally exfiltrate sensitive data and unleash ransomware. Researchers have evidence of the group using cloud credentials to pivot to on-premises networks, as well as compromising on-prem systems before moving to the cloud.

One common source of identity risks is configuration issues. According to Microsoft, 80 percent of organizations have a direct path to a critical vulnerability or critical asset that's vulnerable to exposures. Misconfigurations can be the result of mistakes by insufficiently trained admins, or even by experienced admins who need to address something quickly and forget to come back and complete the work properly. Misconfigurations also tend to creep in over time; for instance, security groups created for projects may not get removed when the projects end, leaving excessive privileges that can be abused. Another common example is improper configuration of certificate services, which can enable an attacker to impersonate a domain controller, feeding false information to all the machines on the network that begin authenticating against it. It's akin to taping the keys to the outside of your car door.

Another factor in today's growing identity is that adversaries are quickly adopting new tactics. While phishing campaigns remain popular, ransomware operators and other attackers are also taking advantage of AI-powered video and audio to trick users into giving up their credentials or completing other risky actions. For instance, they may impersonate IT support over the phone or Microsoft Teams and convince users to launch Microsoft Quick Assist, which gives them remote access that they can use to perform reconnaissance and move laterally in order to deploy the ransomware payload for maximum damage. It's not surprising that Microsoft Digital Defense Report 2024 reported a 2.75x increase in ransomware attacks compared to the previous year.

Challenge 2. Prioritizing true risks is difficult.

A core IT security best practice and Zero Trust principle is to take an assume-breach posture. That is, no matter how well secured the IT environment is, organizations need to recognize that a certain percentage of attacks will get through — and that both malicious and negligent users are already inside. Accordingly, it's vital to continually monitor for suspicious activity and alert security teams when threats are detected.

However, IT ecosystems are highly dynamic, and it's hard to spot suspicious behavior in the sea of activity. In modern distributed environments, organizations often collect terabytes of log data per day, most of which represents legitimate activity. In particular, identity platforms like Entra ID and traditional on-premises AD generate vast amounts of telemetry, from sign-in attempts and password changes to privilege modifications and potential policy violations. As a result, security teams — who are already stretched thin — must often sift through hundreds or thousands of alerts on a daily basis. Trying to identify true threats in all the noise is a Herculean task.

It's hard to spot truly suspicious behavior in today's highly dynamic IT ecosystems.

The problem is not limited to the sheer volume of alerts. All too often, the notifications themselves lack the contextual details required for effective analysis and prioritization. For example, an alert might indicate that a privileged user has been added to a powerful AD group but fail to provide actionable details like who made the change, whether the action aligns with a change request and which systems were accessed afterwards. Instead, analysts are forced to manually correlate data across multiple logs and platforms to triage the alert.

Investigations can therefore be exceedingly difficult and time-consuming, and security teams can end up spending too much of their day chasing false positives. Over time, this constant barrage of low-quality alerts can desensitize teams, leading to slower response times and even truly suspicious activity being missed or ignored altogether. After all, even if you have a crack squad of firefighters, you need to be able to quickly send them to the actual fire and not to the building where someone accidentally burnt their lunch or pulled the alarm for a lark.

Challenge 3: AD expertise is increasingly difficult to find.

A significant number of cyberattacks today are directed at Active Directory. One reason is its ubiquity: Even as organizations embrace a variety of cloud workloads, most of them still maintain their on-prem directory for technological, business, compliance and other factors. For instance, they might be subject to regulatory requirements around data sovereignty, rely on legacy or custom-built applications that require AD for authentication and authorization, or utilize highly sensitive data and processes that require strict control.

Another factor is that AD is over 25 years old and Microsoft has not provided significant updates in recent years. Therefore, the nuances and weaknesses of AD are well understood by attackers. There are even open-source tools like Mimikatz that can help uncover attack paths in a specific victim environment. In recent years, Microsoft has been focusing its attention on its cloud solutions, so although AD continues to be supported, identity security enhancements are concentrated in Entra ID.

While AD is not inherently insecure, many AD environments have built up considerable technical debt over the years or decades. As a result, keeping everything running properly and securely requires an experienced hand. However, organizations have less expertise available to combat the attacks on their AD identity infrastructure. Deep and broad knowledge of AD is concentrated among older IT professionals, many of whom have either reached retirement age or are rapidly approaching it.

That expertise is difficult to replace. As of 2021, Microsoft has completely retired the exams for its Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Solutions Developer (MCSD) and Microsoft Certified Solutions Expert (MCSE) training tracks. And it's not just exams; many courses that deal with fundamental skills, such as Windows Server 2019 administration, have been retired already or will be soon. Indeed, Microsoft's current recommended role-based certification path is based entirely on Microsoft cloud technologies, with options like Azure Solutions Architect Expert, Teams Administrator Associate, Azure Data Engineer Associate and Azure Developer Associate.

Microsoft has retired many courses and exams that deal with fundamental AD skills.

In short, while younger members of the IT workforce might hold some of the base Azure certifications from Microsoft, but they have no way to become certified in on-premises Active Directory — just as their older counterparts with that experience are retiring. This growing AD knowledge gap puts organizations at increasing risk of critical identity security gaps.

Challenge 4: AI-powered threats are on the rise.

Adversaries also have a new and powerful tool for creating and executing identity-based attacks: generative AI (GenAI). GenAI utilizes techniques

like deep learning, natural language processing and reinforcement learning to tackle complex tasks and deliver improved performance over time. Cybercriminals are eagerly abusing generative AI to create increasingly adaptive and effective attacks. Indeed, Gartner expects that by 2027, 17% of all cyberattacks will involve GenAI.

By 2027, 17% of all cyberattacks will involve GenAI, according to Gartner.

GenAI increases identity risk by enabling established hackers to launch more effective attacks faster. It is enabling less-technical groups and individuals to get into the cyberattack "business". For example, attackers at various skill levels are using AI to create sophisticated spear-phishing emails, highly targeted vishing attacks, and deep-fake audio and video that are virtually indistinguishable from legitimate communications. Moreover, AI helps attackers learn from target environments and continuously adapt their strategies to become harder to identify and neutralize.

Here are some specific examples of how adversaries are abusing the power of GenAI:

- **Automated research and reconnaissance** — Attackers use GenAI to quickly summarize data from databases of breached credentials, dark web forums, or public sources.
- **More effective phishing emails** — GenAI can generate grammatically correct, convincing messages in multiple languages to target victims across geographical locations.
- **Personalized lures** — AI can scrape and synthesize personal data to craft highly targeted messages for spear phishing campaigns.
- **Deepfake voice & video** — Attackers are using AI-generated audio or video to impersonate executives for financial gain.
- **Code generation** — GenAI can help attackers write malware, backdoors and other code.

Moreover, GenAI helps hackers conduct more sophisticated and effective attacks. For instance, it can help them create polymorphic malware that evades traditional signature-based detection, giving hackers more time to move laterally and escalate their privileges in order to maximize the impact of their attack.

Challenge 5: Traditional threat response is too slow.

The fifth key challenge in defending against identity-based attacks is being able to respond quickly enough. With attacks unfolding at machine speed, traditional defensive workflows are woefully insufficient. By the time someone on the security team reads the alert email or message, the damage could already be done, especially if adversaries have been lurking in the environment for weeks or months preparing for the final coup d'etat.

Proper configuration and good security hygiene are foundational. Many organizations do not have a clear understanding of their critical assets, let alone a tiered administrative model that organizes user accounts, computers and other IT assets into different tiers to empower IT teams to better manage and secure them.

The most important tier to define and secure is Tier 0, which comprises the organization's most mission-critical IT assets. Tier 0 includes powerful machines like domain controllers (DCs) and privileged access workstations (PAWs), as well as all accounts and groups that have direct or indirect administrative control over the forest, domains or DCs. Examples include highly privileged security groups like Domain Admins, Account Operators and Backup Operators, along with all accounts that are members of those groups, through either direct membership or indirect paths like group nesting. Adversaries target Tier 0 assets because compromising them grants control over the entire environment. Defining and securing these critical objects must be your top priority.

Adversaries target Tier 0 assets because compromising them grants control over the entire environment. Therefore, defining and securing these critical objects must be your top priority.

While security teams need to respond quickly to any cyberattack, attacks on Tier 0 assets demand instant action. For example, escalation to Domain Admin gives adversaries unrestricted access, so immediate Tier 0 containment is crucial; any delay allows them to trigger attacks that compromise data integrity or operational continuity.

Overcoming identity security challenges

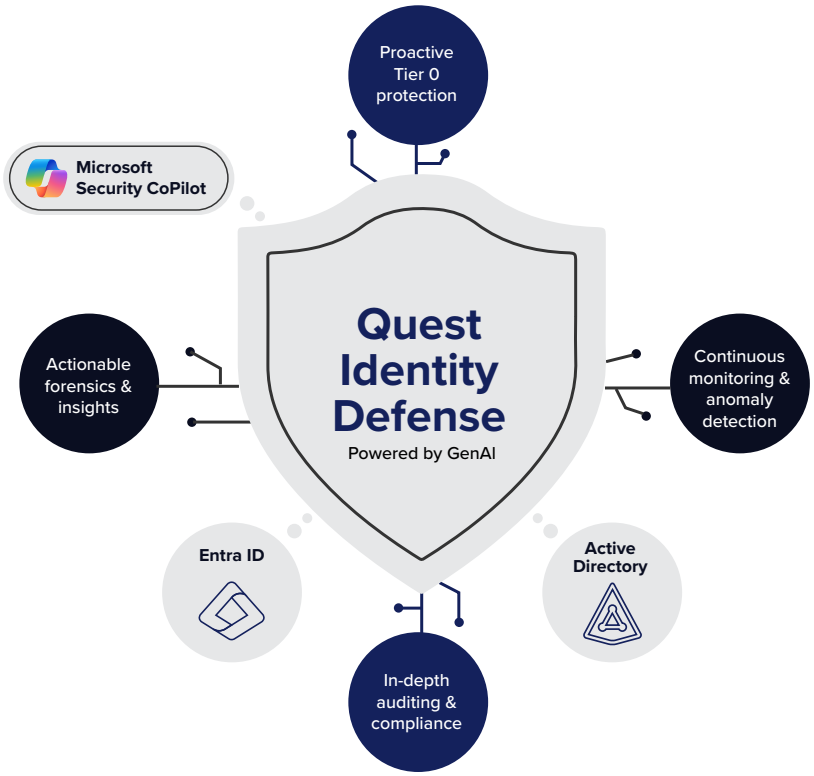
The key to overcoming these challenges and getting the robust identity security required for modern threats is to choose the right tools and the right partner. Quest is the go-to vendor for securing Active Directory and Entra ID. We've been helping to secure AD since its inception and have protected 37 billion Entra ID objects to date. We've earned the prestigious Microsoft Partner of the Year award six times, and our strong strategic partnership with Microsoft gives us early access to their emerging tools and features, such as the Co-Pilot for Security Partner Preview. It's no wonder that 95 percent of Fortune 500 companies rely on Quest for identity security.

With Identity Defense, you can achieve the robust hybrid AD security and ITDR required to defend against modern attacks. It can help you:

- Significantly reduce identity attack surface
- Gain deep visibility and observability of critical identity assets
- Accelerate threat investigation and response
- Protect Tier 0 and stop identity attacks in real time
- Strengthen compliance posture with human-readable auditing

Hybrid identity security and observability

Quest Identity Defense delivers deep visibility into identity posture, activity and exposure across hybrid environments. By surfacing risky configurations, privileged paths and Tier 0 exposures across both human and non-human identities, security teams can clearly see where identity risk exists before attackers exploit it.



Quest Identity Defense reveals existing security vulnerabilities and provides clear remediation guidance.

Identity posture management

Benchmark Active Directory and Entra ID configurations against industry best practices to continuously assess identity posture. Quickly surface vulnerabilities, privilege exposures and configuration drift across critical identity assets, including Tier 0 infrastructure and non-human identities. Built-in remediation guidance provides clear, actionable steps to resolve exposures and strengthen identity hygiene before weaknesses become active compromises.

Real-time threat defense

Activate dynamic Shields Up containment to freeze changes to crown-jewel identity assets during active incidents. By disrupting persistence techniques and lateral movement, including DCShadow-style attacks, Identity Defense stops identity attacks mid-flight and limits blast radius before damage spreads.

Deep AD auditing

Quest Identity Defense delivers human-readable auditing of every significant identity change across Active Directory and Entra ID. Security teams can clearly see the who, what, when, where and workstation behind identity activity, providing the investigation context needed to quickly understand incidents.

AI-driven insights

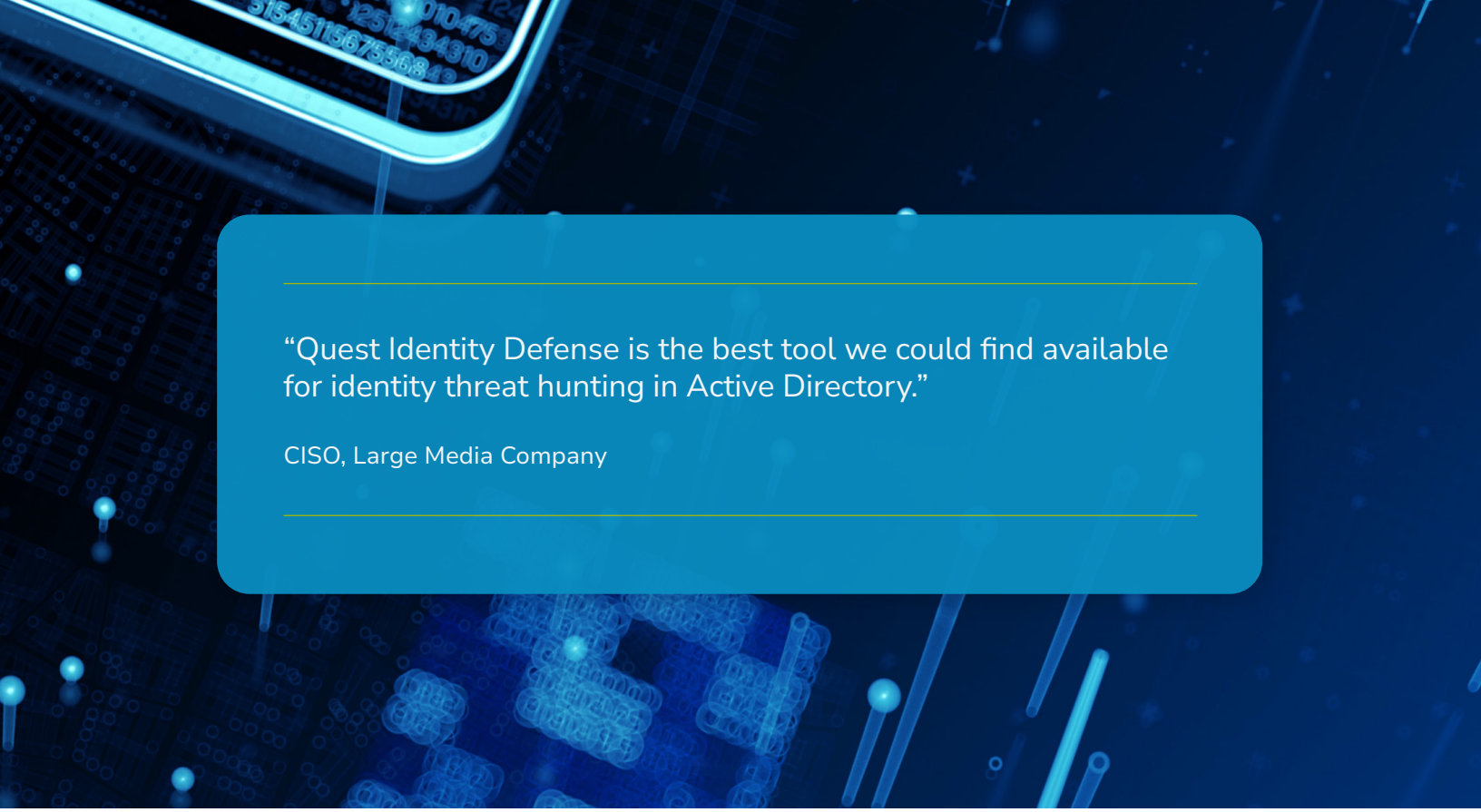
Integrated AI transforms complex identity telemetry into clear, actionable insights that accelerate investigation and response. Identity Defense translates technical identity activity into understandable security and business risk, enabling faster decision-making and clearer communication with leadership. Built-in remediation guidance empowers security teams to take immediate action while reducing reliance on deep Active Directory expertise.

Workload identity protection

Easily discover and secure service accounts and workload identities. Gain full visibility into their activities and prevent their compromise.

Part of a unified ITDR platform aligned to NIST

Aligned to NIST CSF 2.0 security functions, Quest Identity Defense delivers continuous visibility, policy-based protection, and measurable outcomes, such as a 44% improvement in MTTR, while serving as the protection and response foundation of Quest's broader platform for identity recovery and cyber resilience.



> “Quest Identity Defense is the best tool we could find available for identity threat hunting in Active Directory.”
>
> CISO, Large Media Company

Conclusion

Organizations face multiple challenges in implementing effective identity threat detection and response: a growing barrage of attacks, difficulty in spotting true threats in today’s complex and noisy IT ecosystems, lack of AD expertise, increasing AI abuse by cybercriminals, and the speed of modern threats.

Quest Identity Defense (link the product page here) strengthens security across Active Directory and Entra ID by continuously identifying identity risk, protecting critical assets, and containing attacks before they escalate. From a unified workspace, security teams gain deep visibility into identity activity, posture, and exposure across both human and non-human identities, enabling faster investigation and response while reducing operational risk.

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 →

Quest