EBOOK

The State of ITDR 2026: prevention and recovery

Key findings from a global survey of 650 IT and security practitioners and executives on how organizations approach identity threat detection and response (ITDR).

Quest

Introduction

ITDR is expanding, and expectations are changing

Identity threat detection and response (ITDR) has become a core part of modern security programs. Identity systems now sit at the center of most environments, connecting users, applications, data, automation, and cloud services. When those systems are compromised, attackers gain immediate access and, in many cases, control over how quickly an organization can respond and recover.

ITDR was initially defined by Gartner as a set of capabilities focused on preventing, detecting, and responding to identity-based threats targeting platforms like Active Directory and Entra ID. That definition shaped early ITDR programs, which tended to overweight prevention and detection, and treat recovery as a downstream concern.

More recent guidance broadens that view. Gartner now aligns ITDR more closely with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and explicitly recognizes recovery as a necessary component of identity security. This shift reflects how identity-based attacks play out today. Prevention and detection still matter, but when identity controls fail, the ability to respond and recover determines the extent of the damage that follows.

Organizations increasingly overestimate their identity security posture by placing too much confidence in preventative controls and alerting, while underinvesting in response and recovery readiness. Survey findings closely mirror this shift in thinking. Recovery readiness remains one of the largest blind spots in modern ITDR programs.

This report presents findings from a global survey of 650 IT and security practitioners and executives. It examines how organizations are attempting to operationalize ITDR in an environment characterized by AI-driven attacks, hybrid identity infrastructures, non-human identity sprawl, and growing recovery risk. The findings highlight where those efforts fall short and what those gaps mean when identity attacks succeed.

Why identity security is under pressure

Identity has become the most consistent entry point for modern attacks. Hybrid Active Directory and Entra ID, cloud adoption, and a growing number of non-human identities have expanded the identity attack surface faster than most organizations can manage. As identity environments grow more complex, maintaining consistent governance becomes harder. Attackers take advantage of this complexity to move quickly once access is gained, and recovery becomes slower and more disruptive.

Survey responses highlight a core tension. Despite increased ITDR adoption and rising confidence, organizations continue to struggle to identify, protect, detect, respond, and recover when an attack succeeds.

Quest Software's perspective

To understand how organizations are approaching identity threat detection and response today, Quest Software conducted a global survey examining where organizations are in their ITDR journey and whether they are achieving the results they expect.

Quest brings decades of expertise in identity security, recovery, management, and modernization, supporting more than 45,000 organizations worldwide, including over 90% of the Fortune 500. For more than 25 years, Quest has worked alongside Microsoft in the Active Directory space – longer than any other vendor – giving our teams deep, sustained exposure to how identity environments evolve and fail over time.

Gartner has consistently recognized Quest as an example vendor across ITDR-related categories, including 11 areas spanning Active Directory security, management, and migration. That's more than double the amount of any other vendor (even Microsoft). Quest also hosts The Experts Conference (TEC), a long-running global practitioner community and education event focused on hybrid Active Directory and Microsoft 365, bringing together over 20,000 participants and hundreds of Microsoft MVPs.

Survey methodology

The 650 survey respondents represent a mix of organizations across industries and regions, drawn from the Quest Software customer base and the TEC community. Data collection and validation were performed using User Evidence, a trusted customer research platform.

Where organizations fall short

While ITDR adoption continues to grow, the way it is implemented often fails to deliver what real-world incidents demand. Many programs are built around individual tools or capabilities, and detection is typically the most mature area, while identification, protection, and recovery receive less consistent attention. This imbalance leaves teams unprepared to contain and recover from identity-driven attacks.

Survey findings reveal that many teams still focus most of their efforts on prevention and detection, and don't give the same attention to response and recovery readiness. As a result, organizations may believe they are well protected yet struggle when identity controls fail. Effective ITDR requires an integrated, lifecycle-based approach rather than a collection of disconnected tools.

Quest brings decades of expertise in identity security, recovery, management, and modernization, supporting more than **45,000 organizations** worldwide, including over **90%** of the **Fortune 500**

Key Findings

1

Recovery & resilience have emerged as ITDR's defining gap

While prevention and detection remain foundational, recovery readiness has emerged as one of the clearest indicator of true ITDR maturity. Organizations often believe their programs are strong because alerts are firing and preventative controls are in place. Yet when identity controls fail, the ability to restore authentication systems quickly and cleanly determines the real outcome. Unfortunately, survey findings show that recovery remains one of the least mature and least exercised components of ITDR programs.

Only 24% of organizations test identity disaster recovery every six months, even though biannual testing is widely considered the minimum recommended standard across incident response frameworks, cyber insurers, and regulatory guidance. For most organizations, identity recovery remains more theoretical than practical.

Only **24% of organizations** test identity disaster recovery every six months.

Quest Expert Insight

Quest's incident recovery teams have supported some of the largest and most complex identity restorations in the world, and one truth stands out: recovery determines survival. In the majority of real incidents we assist with, the organization had preventive controls and detection but had never validated identity recovery end-to-end. As a result, Domain Controllers could not be restored, backups were incomplete or contaminated, conditional access policies prevented admin access, or recovery systems had been disabled by attackers hours before ransomware deployment. Identity recovery is not theoretical. It is operational muscle memory. Organizations that test recovery regularly experience dramatically shorter outages, lower business impact, and far greater resilience during identity-focused attacks.

Recommendation: respond and recover

- Treat identity recovery as a core ITDR capability, not a contingency plan
- Regularly test and validate recovery across multiple ransomware and identity compromise scenarios
- Build operational muscle memory to reduce downtime and recovery risk when an incident occurs
- Ensure flexibility in recovery options so teams can choose the appropriate method for the specific incident, whether that be granular object level or full domain recovery

How often do you practice your **identity disaster recovery plan** (not just a tabletop exercise, but an actual test)?

uevi.co/4083ONQS

2

Identity identification gaps create systemic ITDR risk

While recovery is key for survivability during an incident, preventing compromise in the first place remains essential. Strong identification, protection, and detection capabilities reduce blast radius and improve the effectiveness of recovery when it is required.

Survey respondents did not identify any specific identity area as significantly more difficult to secure than others. Instead, difficulty remains consistently high across different aspects of Active Directory and Entra ID. This shows that identity challenges are systemic, not isolated to one platform or technology.

Non-human identities do stand out as a growing concern. Their rapid growth, unclear ownership, and limited visibility make them difficult to govern. Organizations struggle to clearly define their identity attack surface across on-premises Active Directory serviceaccounts, cloud-based Entra ID, and hybrid identity environments.
When factoring in these prevalent non-human identities, which often vastly outnumber human identities, organizations can be left in a state of, “We don’t even know, what we don’t know.”

Without continuous discovery and inventory, ITDR programs lack a reliable foundation. Detection and response capabilities cannot compensate for gaps in understanding what identities exist or how they are being used.

Non-human identities do stand out as a growing concern. Their rapid growth, unclear ownership, and limited visibility make them difficult to govern.

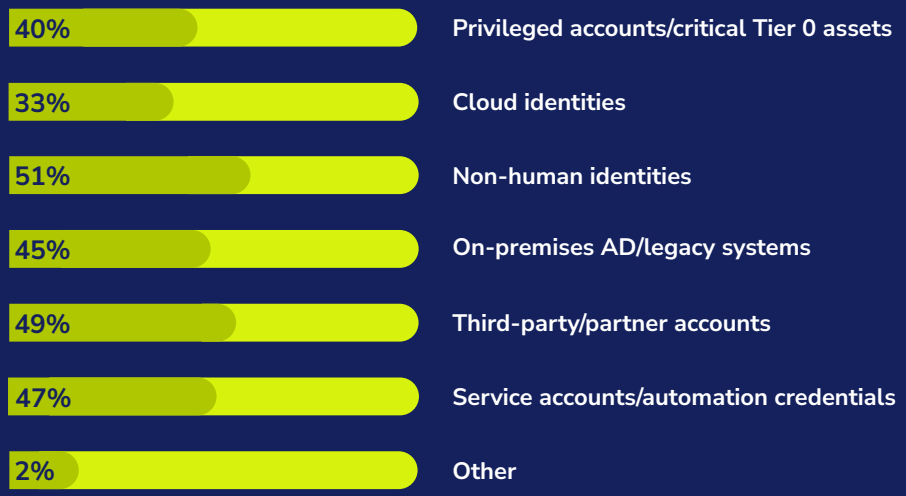
Quest Expert Insight

In nearly every compromise assessment we perform, the root cause traces back to identity visibility gaps across hybrid AD and Entra ID. Organizations often believe they have a complete inventory, yet when telemetry is analyzed, 30–60% of privileged or high-impact identities turn out to be misclassified, unknown, or unmanaged — especially non-human identities. These blind spots give attackers quiet footholds they can escalate from without triggering alarms. We consistently see that when identity discovery is incomplete, every ITDR control that follows — protection, detection, response, and recovery — stands on an unstable foundation. For most organizations, improving identity discovery and classification is the single highest-leverage action to reduce real-world breach impact.

Recommendation: respond and recover

- Establish continuous discovery across hybrid Active Directory and Entra ID environments
- Maintain a current inventory of both human and non-human identities, including on-prem service accounts and cloud-based identities
- Use discovery results to clearly define the identity attack surface

Which areas of your **identity infrastructure** are most difficult to monitor or secure? (Select all that apply)



uevi.co/9223NCGW

3

Blast radius remains high without Tier 0 protection

Organizations report increased investment in identity prevention tools, yet many still experience significant impact when identity attacks occur. This reflects a disconnect between ITDR adoption and actual risk reduction.

Many organizations lack the skills or tools required to reliably identify and secure the identities that control authentication and recovery. This challenge is compounded by the retirement of experienced Active Directory administrators, leaving fewer practitioners with deep Tier 0 expertise.

Identity systems face hundreds of millions of attacks daily, and nearly 80% of organizations remain vulnerable to identity-related threats due to complexity and inadequate tools. When Tier 0 identities are compromised, attackers can rapidly escalate privileges, expand access, disable recovery controls, dramatically increasing blast radius during ransomware attacks.

Many organizations lack the skills or tools required to reliably **identify** and **secure** the identities that control authentication.

Quest Expert Insight

Across thousands of customer engagements, Quest sees the same pattern: security investments increase, yet blast radius remains dangerously high because Tier 0 is either misunderstood or unprotected. Most organizations can identify Domain Admins, but far fewer can identify the extended chain of identities and systems that effectively hold Domain-level control — backup servers, automation tools, legacy delegation paths, cloud sync agents, and high-privilege app registrations. These “Tier 0 by consequence” identities are frequently the ones attackers compromise first. When Tier 0 is not clearly defined and consistently protected, prevention becomes irrelevant, and recovery becomes optional — because attackers will disable it. Strengthening Tier 0 governance is the most reliable way to shrink blast radius and contain identity-driven attacks.

Recommendation: respond and recover

- Identify and formally classify Tier 0 identities
- Apply focused protections, auditing and alerting to Tier 0 accounts
- Reduce identity blast radius by limiting privilege and unnecessary trust relationships
- Address misconfigurations that expose critical identities

What factors have been the primary drivers for your organization to **implement ITDR?**

uevi.co/7761NLMQ

4

Detection is strained by attack surface growth, alert fatigue, and skills gaps

Active Directory remains difficult to secure due to legacy configurations, sprawl, and technical debt. As identity environments expand, security teams are overwhelmed with disconnected signals and alerts, making it difficult to distinguish meaningful threats from background noise.

79% of respondents believe that AI can improve ITDR effectiveness. Organizations increasingly see AI as essential to managing broad identity attack surfaces, reducing alert fatigue, translating technical signals into meaningful risk context, and addressing limited AD and identity security skills.

79% of respondents believe that AI can improve ITDR effectiveness.

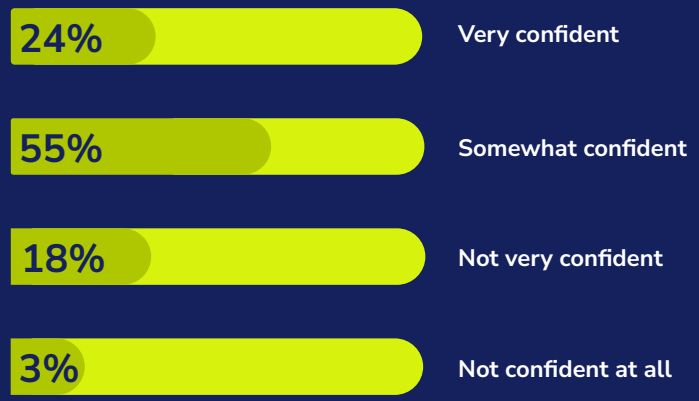
Quest Expert Insight

The gap between the volume of identity activity and the number of people qualified to interpret it has never been wider. Blue teams today face millions of hybrid identity signals across AD, Entra, Azure, M365, and SaaS platforms — far too many to triage manually. In our field work, the detection failures that lead to compromise are rarely due to “no signals”— they’re due to too many signals with too little context. AI-driven detection is no longer a luxury; it’s essential to translate raw events into meaningful risk stories and uncover subtle privilege escalation activity. Organizations that successfully modernize ITDR almost always do so by reducing noise, correlating identity signals across platforms, and automating analysis to compensate for deep AD/Entra expertise shortages.

Recommendation: respond and recover

- Continuously monitor identity activity across hybrid environments to surface suspicious behavior
- Use AI to triage alert noise and help prioritize high-risk identity events
- Correlate identity signals with broader security telemetry to add contextAddress misconfigurations that expose critical identities
- Compensate for identity and AD skills gaps by automating routine detection and analysis

How confident are you that AI tools can improve your **ITDR** effectiveness?



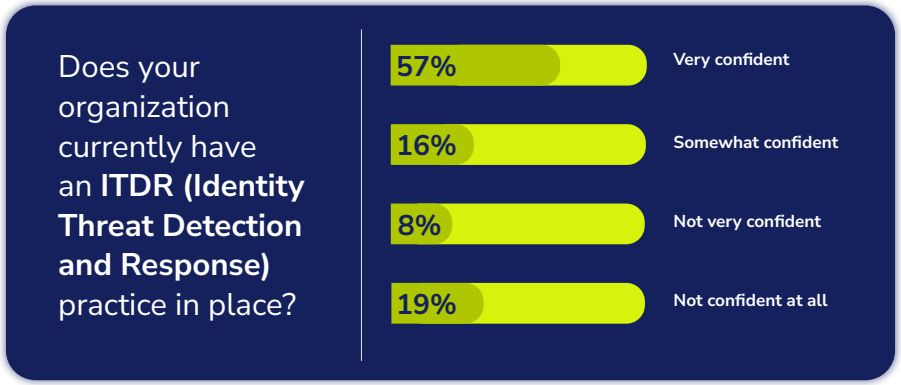
uevi.co/5853VFKI

Additional Insights

Identity adoption is rising, but effectiveness varies

ITDR adoption increased from 48% to 57% year over year. Among organizations with an ITDR practice, 92% report achieving some level of benefit, indicating that even partial implementation can deliver value.

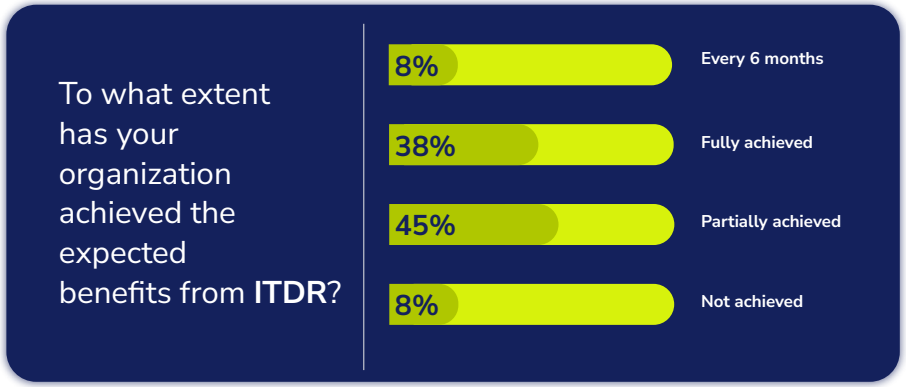
But across respondents, many still describe their ITDR programs as mature, despite gaps in identification, protection, and recovery.



uevi.co/4083ONQS

Identity remains the primary attack surface

Hybrid identity infrastructures, automation, and cloud services continue to expand the number of identities that need protection. Non-human identities frequently outpace visibility and governance, while attackers continue to prioritize identity compromise because it provides efficient access and control. As a result, identity security increasingly determines the scope and severity of modern attacks.



uevi.co/5983DJOT

Conclusion

Stronger identity resilience starts with a complete ITDR strategy

Survey findings make one point clear: while organizations are making progress in detection and prevention, gaps in identification, Tier 0 protection, and especially recovery resilience create broad, interconnected challenges for attaining true identity threat detection and response.

Recovery testing remains inconsistent. Tier 0 identities are frequently misunderstood or incompletely protected. Non-human identities expand faster than governance models can keep up. Detection capabilities are improving, but teams remain strained by alert fatigue, hybrid complexity, and skills shortages.

Individually, each of these challenges introduce risk. Collectively, they expose a larger issue: many ITDR programs are still built around tools and signals rather than lifecycle resilience.

As ITDR evolves beyond its original prevention and detection focus, organizations must align identity security to a more complete model and strategy. Gartner's alignment with the National Institute of Standards and Technology Cybersecurity Framework reinforces that identity resilience depends on coordinated maturity across identification, protection, detection, response, and recovery.

As **ITDR evolves** beyond its original prevention and detection focus, organizations must align identity security to a more complete model and strategy.

A modern ITDR strategy therefore demands:

- Continuous visibility into hybrid identity environments
- Clear Tier 0 governance to reduce blast radius
- Intelligent detection that reduces noise and adds context
- Proactive containment to mitigate attacks and disruption
- Constant updating of identity infrastructure to stay ahead of changes and evolving threatsIntelligent detection that reduces noise and adds context
- Validated, flexible recovery processes that are regularly tested and operationalized

Quest identity security and resilience is delivered from a unified, mature, and scalable SaaS solution, built to lead organizations towards true ITDR. Built to cover the full NIST Cybersecurity Framework, the solution provides continuous visibility into hybrid identity environments and deep, contextual insight into every significant AD and Entra ID change. Integrated AI translates technical activity into human-readable risk context, while embedded Quest and Microsoft identity expertise productizes decades of field experience, accelerating response and reducing reliance on scarce specialists.

Proactive threat containment stops attackers in real time, preventing lateral movement and unauthorized changes, while clear Tier 0 governance and auditing minimize catastrophic risk.

Phased recovery restores the most critical systems first, and flexible recovery options, from granular fixes to full environment rebuilds, ensure organizations can recover in any scenario. Automated recovery workflows provide full visibility at every step, keeping backups clean so malware does not return with restored data. Together with Recovery-as-a-Service, including 24/7 expert guidance, monthly health checks, and ongoing readiness support, Quest enables organizations to operationalize ITDR as a complete lifecycle discipline.

By continuously modernizing their identity infrastructure while addressing visibility, protection, detection, and recovery gaps, organizations are best positioned to withstand, contain, and recover from today's identity-driven attacks.

In a world where identity is the primary attack surface, resilience is no longer optional. Organizations that treat ITDR as an end-to-end discipline – not a collection of tools – will be best positioned to withstand, contain, and recover from the identity-driven attacks that define today's threat landscape.

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.

Ebook-Quest_Ebook_eBook-New-State of ITDR 2025-HO-101120

Explore our solutions →

Quest