The state of ITDR: adoption, maturity and effectiveness

Key finding from a recent survey of 373 organizations to explore their experiences with identity threat detection and response (ITDR).

Introduction: Survey reveals that ITDR measures work.

84% of organizations with an identity threat detection and response (ITDR) practice — even if it's not complete — say they are reaping benefits. In fact, over a third report that their expectations have been fully met (26%) or exceeded (10%).

These valuable insights about ITDR come from a September 2024 survey of 373 IT pros, managers and executives.

The survey found that organizations are reaping benefits even if they are just starting on their ITDR journey. However, we found areas of improvement that can have immediate impact if prioritized in an ITDR strategy. For example, nearly 100% of respondents agree that identity security requires effective hygiene and prevention measures. Surprisingly, however, only half utilize an identity infrastructure security tool.

This report provides a deeper dive into these and other key findings of the survey. We'll cover ITDR adoption, maturity and effectiveness, and then offer other valuable insights from the study. Last, we'll offer additional recommendations for improving your organization's identity security.

> **Nearly 100% of respondents agree that identity security requires effective hygiene and prevention measures. Surprisingly, however, only half utilize an identity infrastructure security tool.**

Introduction: What is ITDR and why is it critical today?

Organizations are facing increasingly sophisticated threats to their identity infrastructure — Active Directory (AD) and Entra ID. According to a 2024 Gartner report, over 90% of all organizations worldwide use Active Directory. The report adds, "Arguably, AD is one of the most valuable IT assets organizations possess. However, Active Directory is complex."[1]

Indeed, Microsoft reports that credential misuse is now a factor in 99% of the 600 million daily identity attacks against Entra ID.[2] Traditional identity and access management (IAM) controls are insufficient in the face of these advanced attacks. In response, Gartner has identified identity threat detection and response (ITDR) as one of the top cybersecurity trends for 2024.[3]

ITDR focuses on enhancing an organization's ability to prevent, detect, investigate and respond to identity-related threats in order to ensure the integrity and availability of critical systems. As adversaries grow more adept at exploiting vulnerabilities in identity systems, ITDR has become a crucial layer of defense for modern organizations.

Credential misuse is now a factor in 99% of the 600 million daily identity attacks against Entra ID.

[1] Gartner, Inc., "Implement IAM Best Practices for Your Active Directory," 2024.
[2] Microsoft Digital Defense Report 2024.
[3] Gartner, Inc., "Emerging Tech Impact Radar: Security," 2024.

Introduction: Quest's unique vantage point

To gain insight into the current state of ITDR, Quest decided to conduct a survey to find out where organizations stand on their ITDR journey and whether they are achieving the benefits they expect.

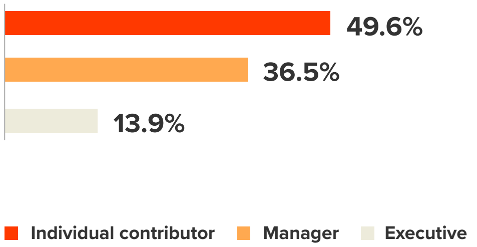
Quest is the leader in identity security, recovery, management and modernization, with more than 130,000 customers and 15,000 partners. We have partnered with Microsoft in the Active Directory space for over 25 years, which is twice as long as any other vendor. Indeed, our team has some 7,000 years of combined AD experience. Year after year, Gartner recognizes Quest as an example vendor for ITDR-related categories; in fact, in 2022 and 2023, Quest is listed in 11 areas of Active Directory security, management and migration — more than double that of any other vendor and even more than Microsoft itself.

Quest is also the host and sponsor of The Experts Conference (TEC). This industry-leading education conference and global community for hybrid AD and Microsoft 365 includes over 20,000 participants and more than 225 Microsoft MVPs.

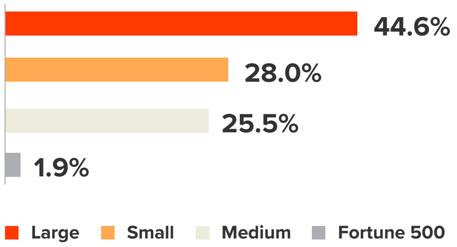
Introduction: Survey methodology and demographics

The 373 survey respondents come from the Quest customer base and the The Experts Conference (TEC) global community. UserEvidence, a leading customer evidence platform, was used to gather the data and validate the responses.

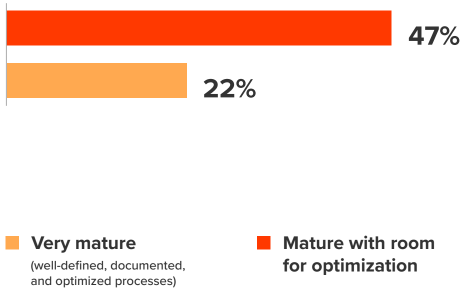
Seniority



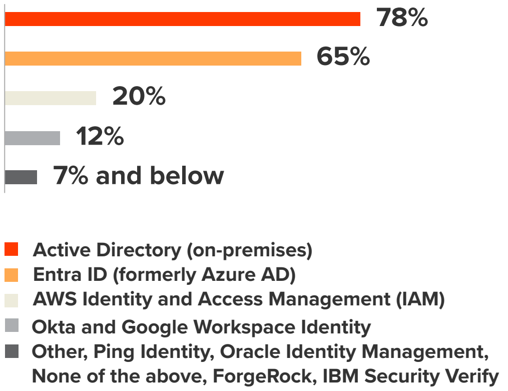
Company size



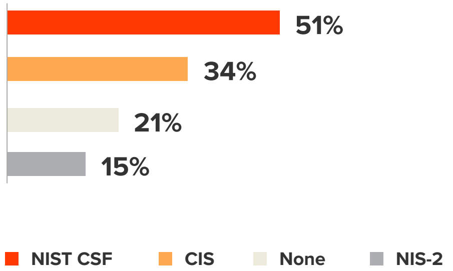
Maturity of security practice



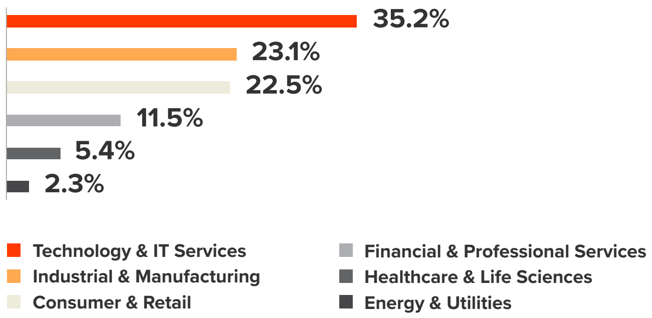
Identity systems



Cybersecurity frameworks



Industry



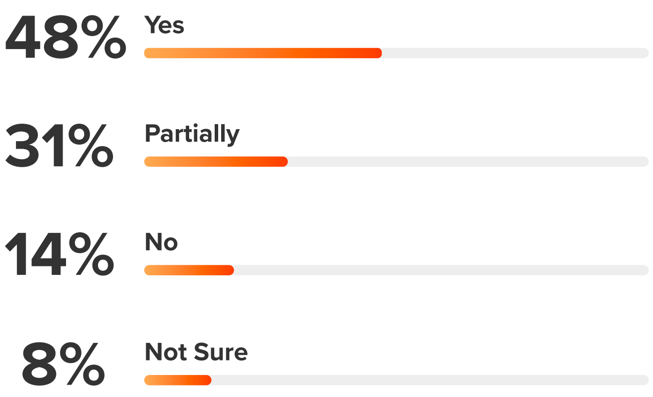
1. Adoption: Implementation rate

Most organizations have begun their ITDR journey, and almost half say their practice is in place.

Organizations today clearly recognize the critical importance of threats to their identity infrastructure.

Indeed, nearly half of respondents (48%) say their organization has an ITDR practice in place, and another third (31%) say they are in the process of implementing one.

Does your organization currently have an ITDR (identity threat detection and response) practice in place?



1. Adoption: Core drivers

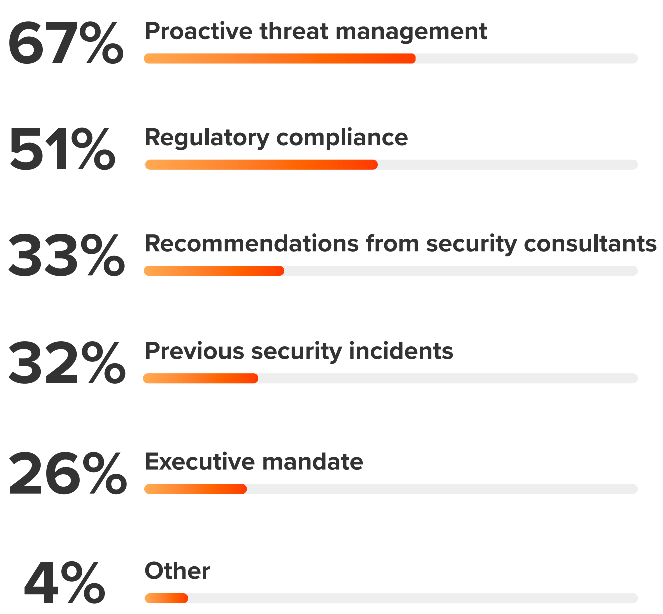
Most organizations implement ITDR to proactively improve security and compliance, rather than in response to security breaches.

The top reason that organizations adopt ITDR is proactive threat management, cited by 2/3 of respondents.

The other major driver is regulatory compliance, named by over half (51%) of respondents.

Interestingly, only a third (32%) of organizations report implementing ITDR because of a previous security incident, and just a quarter (26%) say executive mandate was a primary driver.

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



1. Adoption: Top challenges

The top roadblock to ITDR adoption is lack of budget and expertise for such a complex project.

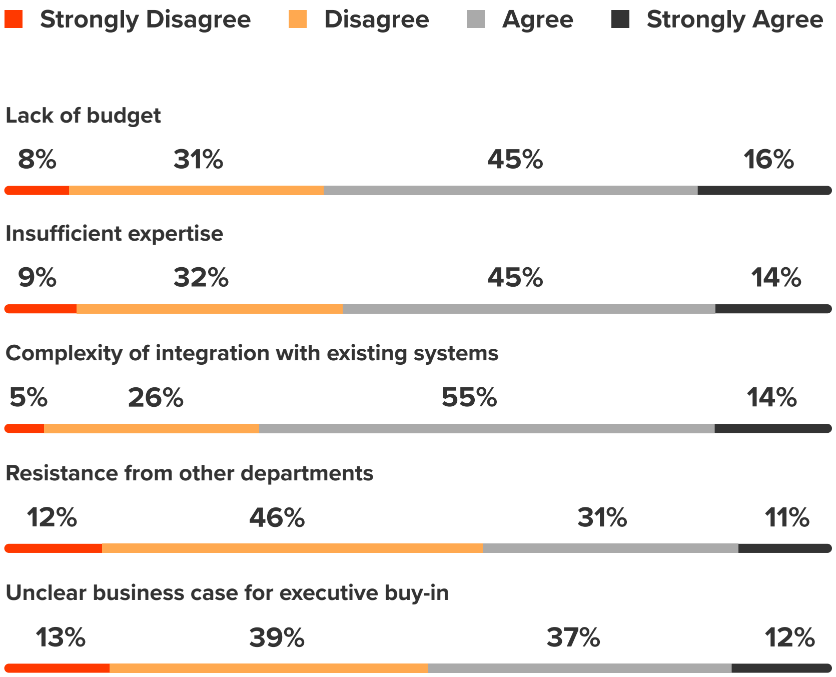
The key reason that organizations are struggling to implement ITDR is simple: It's a complex job that requires proper funding and expertise.

Indeed, the top three hurdles reported by respondents are the complexity of integrating ITDR with existing systems (69%), lack of budget (61%) and insufficient expertise to carry the work (59%).

> **"Challenges include the complexity of integrating ITDR solutions with existing security infrastructure, managing false positives and ensuring privacy while monitoring user behavior."**

Exchange/Mail Administrator,
Large Enterprise Professional Services Company

What has been the biggest challenge in embracing ITDR in your organization?



1. Adoption: The core underlying issue

Underlying the key roadblocks to ITDR adoption is one core issue: lack of executive buy-in.

Why don't IT teams have the budget and skills they need? Nearly half of respondents point to the same factor: an unclear business case for executive buy-in.

Lack of understanding of the nature and importance of ITDR by senior management can take different forms. For example, one survey participant notes that their executives believe multifactor authentication (MFA) alone is sufficient for ITDR. And even in organizations that have suffered a security incident, leadership teams may be unconvinced that ITDR solutions are worth the cost.

> **Upper management just isn't serious enough about ITDR. They either think we won't get hit, or think they can handle the situation if we are hit.**
>
> *Support Staff, Professional Services Company*

> **Despite a prior security incident, a distributed organization with multiple IT teams and leaders still has trouble communicating and understanding the importance of ITDR.**
>
> *Enterprise Cloud Administrator, Food Products Company*

2. Maturity: Current status

64% of organizations consider their current ITDR practice to be mature or very mature.

Nearly a quarter of respondents (23%) say that their ITDR practice is very mature, defined as providing comprehensive coverage, continuous monitoring and automated responses.

Another 41% rate their practice as mature, with good coverage through manual monitoring and response.

> **Fully implementing ITDR is a huge challenge when no one on the team is skilled in properly deploying to gain value.**
>
> *IT Architect, Internet Software & Services Company*

How mature is your organization's ITDR practice?

23% **Very mature** (comprehensive coverage, continuous monitoring, and automated responses)

41% **Mature** (good coverage with manual monitoring and response)

24% **Developing** (partial coverage with manual processes)

13% **Early stage** (limited coverage with significant gaps)

2. Maturity: Causes of low ITDR maturity

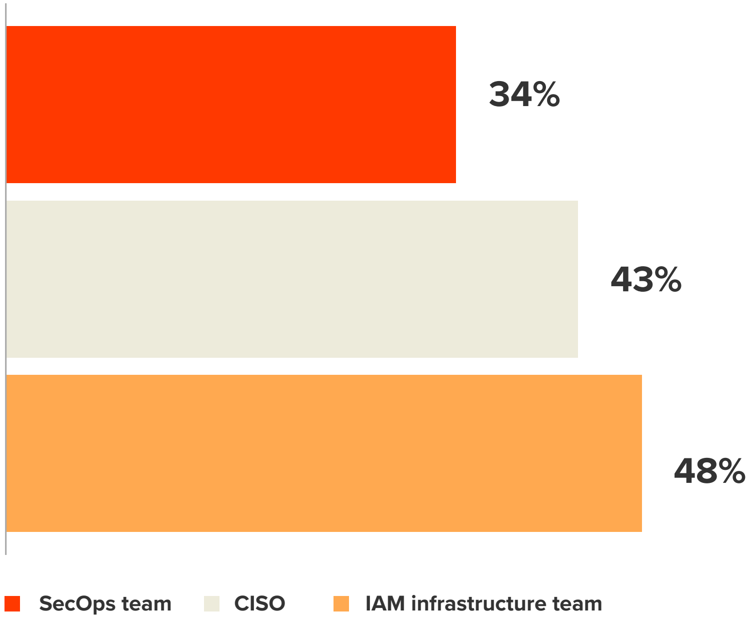
a. Two in three organizations fail to leverage their identity experts

One key reason for lack of ITDR maturity is not putting the right people in charge. Almost half of respondents (48%) say their security operations (SecOps) team has primary responsibility for ITDR, and nearly as many point to the CISO.

Only a third (34%) name their access management (IAM) infrastructure team. However, these identity experts are uniquely positioned to improve ITDR maturity because they live and breathe the complexities of identity hygiene, exposure management and identification of critical Tier Zero assets.

In short, while SecOps and CISOs add important value to ITDR, without the IAM team's expertise, there's a higher risk of misconfigurations, incomplete identity protection strategies and missed opportunities for automation — all of which are necessary for achieving high ITDR maturity.

Who in your organization is responsible for ITDR?



2. Maturity: Causes of low ITDR maturity

b. Over half of organizations lack robust identity threat prevention.

When it comes to identity threats, prevention is just as critical as detection and response. Indeed, Alex Weinert, Vice President of Identity Security at Microsoft, calls prevention the silent "P" in ITDR.[4]

Similarly, a 2024 Gartner report states: "Lapses in IAM data and configuration hygiene directly impact an organization's ability to protect itself from cyberattacks."[5]

This message has been heard loud and clear: Nearly 100% of respondents agree that good identity security requires effective exposure management; secure and consistent configurations and policies; and regular monitoring and auditing.

However, that knowledge is often not translated into action. Only 50% of respondents utilize an identity infrastructure security tool to identify and remediate misconfigurations, and only 42% monitor their critical assets (Tier Zero).

Identity threat prevention is woefully neglected:

Only 50% of organizations utilize an identity infrastructure security tool to root out misconfigurations, and just 42% identify and monitor Tier Zero assets.

[4] Microsoft on Protecting Identity – The Core of Your Digital Ecosystem," The Practical 365 Podcast S4 E18, 20 Oct 2023.
[5] Gartner, Inc., "Prioritize IAM Hygiene for Robust Identity-First Security," 2024.

2. Maturity: Causes of low ITDR maturity

c. Nearly a third of respondents never test their identity disaster recovery plan.

Every second your identity infrastructure is down, your business is dead in the water, and the costs skyrocket. In fact, research pegs the cost of Active Directory downtime at $730,000 per hour.[6]

Nevertheless, 31% of organizations never test their disaster recovery (DR) plan![7] Amazingly, the percentage is nearly identical for organizations that implemented ITDR because of a previous security incident.

The best practice is to run a real test (not a tabletop exercise) every 6 months, but only 24% of organizations meet this bar. Even among those who say their ITDR practice is mature, it's still just 32% — far below what's expected at that level.

A robust backup and DR solution is critical to ensuring quick restoration of services, and regular practice of the recovery process is also vital for building up muscle memory to help you through a real disaster, when adrenaline, emotions and stress will be at their highest.

31%

of organizations never test their identity disaster recovery plan.

[6] "The Total Economic Impact™ of Quest Recovery Manager For Active Directory Disaster Recovery Edition"

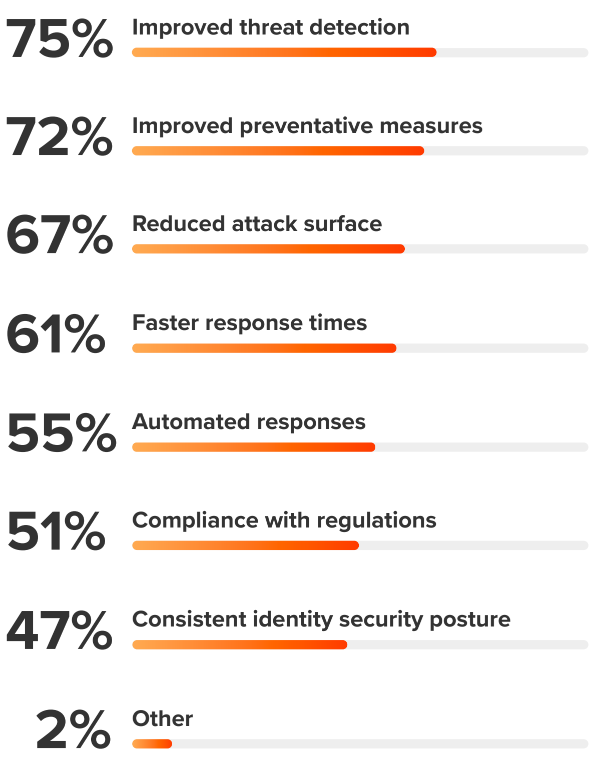
[7] uevi.co/6534ZMGX

3. Effectiveness: Expected benefits

Organizations expect their ITDR program to improve security through threat prevention, detection and response, as well as to facilitate regulatory compliance.

The survey reveals high expectations for implementing an ITDR practice across all of the areas mentioned earlier.

What are the primary benefits your organization expects from ITDR?



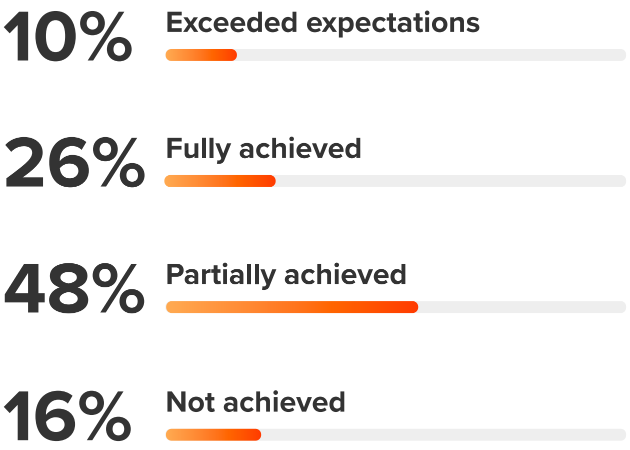
3. Effectiveness: Actual benefits

Adopting ITDR yields significant benefits — even if the program has been only partially implemented.

Overall, 84% of organizations that have fully or partially implemented an ITDR practice say it has delivered benefits.

What's more, 1 in 10 say the program has exceeded their expectations, and another quarter (26%) say they have fully achieved the expected benefits.

To what extent has your organization achieved the expected benefits from ITDR?



3. Effectiveness: Satisfaction

Satisfaction is high even for organizations that have only partially implemented ITDR.

Full implementation

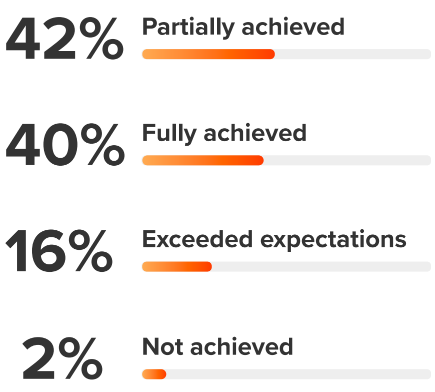
Not surprisingly, satisfaction is highest for organizations that have fully implemented ITDR: 16% say it has exceeded their expectations, and another 40% saying they have full achieved the expected benefits.

Partial implementation

However, even partially implementing ITDR enables organizations to achieve significant benefits: 15% of respondents say they have achieved or exceeded their goals, and another 71% report their practice has partially delivered the expected benefits.

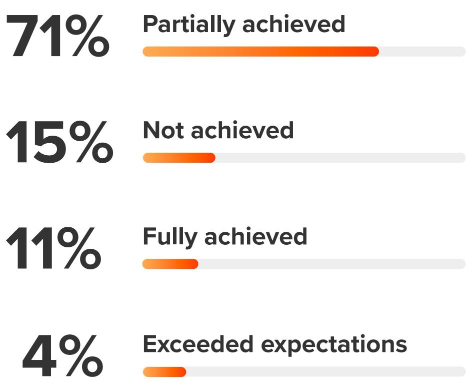
Full implementation

To what extent has your organization achieved the expected benefits from ITDR?



Partial implementation

To what extent has your organization achieved the expected benefits from ITDR?



Additional insights: Strategies for better results

a. Modernize your Active Directory environment.

More than half of organizations (55%) report ITDR improvements after modernizing their Active Directory.

That makes a great deal of sense. After all, as the core identity system for most organizations today, AD provides the vital authentication and authorization services necessary for users to do their jobs and for processes and services to run. However, AD is such a large and complex system that it can easily sprawl out of control, especially in organizations that have undergone mergers, acquisitions and reorganizations.

AD sprawl limits insight into and control over crucial IT assets like accounts, security groups, powerful servers and Group Policy. Adversaries can take advantage of the resulting security gaps to slip into the network, escalate their permissions and move laterally until they reach your sensitive data and systems. The result can be a devastating data breach, hefty ransom demand or costly downtime.

Active Directory modernization is the practice of migrating and consolidating your on-premises AD environment. AD modernization helps organizations reduce their attack surface and makes it easier to quickly detect and respond to security threats.

55%

of organizations report ITDR improvements after modernizing their Active Directory.

Additional insights: Strategies for better results

b. Seize new technologies.

Almost half of respondents are considering using artificial intelligence (AI) and machine learning (ML) capabilities to help them predict and prevent security vulnerabilities in their identity infrastructure. AI-powered solutions like Microsoft Security Copilot are already delivering significant value in enabling organizations to strengthen their security posture and promptly detect and respond to threats.

In particular, choosing an identity infrastructure security tool that integrates seamlessly with Security Copilot enhances ITDR by simplifying security and accelerating response times. By integrating Security Guardian from Quest with Microsoft Security Copilot, organizations can better address the ITDR challenges uncovered by the survey.

For example, they can:

- Make faster and more informed decisions with clear, actionable summaries of complex security alerts.
- Rapidly detect, investigate and mitigate identity threats with guided responses and automated task optimization.
- Uncover overlooked details with a deeper understanding of findings.
- Mitigate the IT skills shortage by automating routine tasks to enable experts to focus on the most critical security challenges and providing step-by-step guidance to grow the team's proficiency.

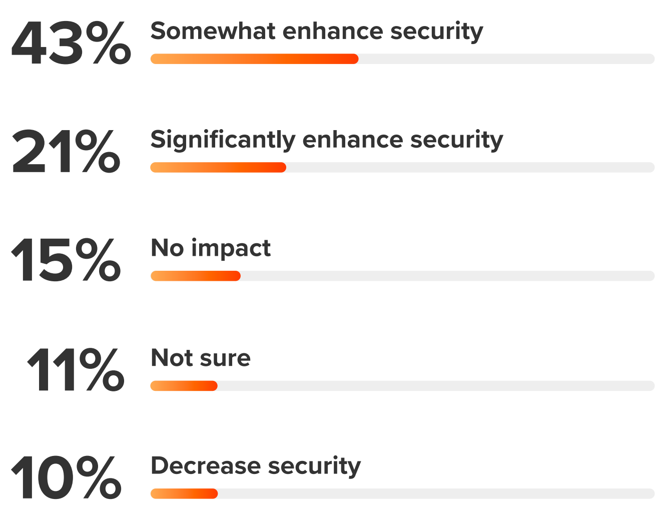
Additional insights: Strategies for better results

c. Consider migrating devices to the cloud.

Nearly two thirds of organizations believe that joining devices to the cloud as part of their ITDR practice enhances security. They are right: Top benefits include single sign-on (SSO) to cloud resources, phishing-resistant authentication, device-based conditional access policies, automatic device licensing, self-service password reset, and centralized device identity management.

Not surprisingly, 58% of organizations have started down this path. However, migrating devices from AD-joined to cloud-joined can be a cumbersome journey. Joining machines to Entra ID requires a complete device reset, frustrating users who must then painstakingly rebuild their profiles, copy their data and reconfigure their desktop settings. Moreover, the process can take 5+ hours — per device. If you have 1,000 devices, that's potentially 5,000 hours of lost productivity!

To what extent do you believe cloud-joined devices enhance security as part of your ITDR practice?

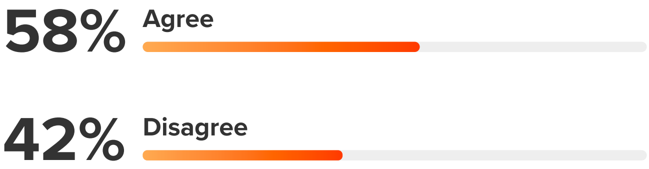


Additional insights: Strategies for better results

c. Consider migrating devices to the cloud.

Fortunately, On Demand Migration makes it fast and easy to move devices from on-premises AD to Entra ID. The tool eliminates the need to wipe and reimage the machines, and it will even automatically restore the user profiles on each device. The entire move takes only about 15 minutes, and as soon as the machine reboots, the user can log on and get right back to work. It's a repeatable process that's easy to learn and perform accurately, time after time.

As part of a modern cloud initiative, for greater security we have started switching to, or plan to switch to, cloud-only devices.



Recommendations

Prevent

- Benchmark your current Active Directory configuration against industry best practices.
- Identify and protect your Tier Zero assets, and prevent malicious or accidental changes to critical objects like privileged security groups and key Group Policy objects (GPOs).
- Map the attack paths in your environment and mitigate them efficiently by addressing their choke points.

Detect

- Continuously monitor for suspicious activity and notify security teams, using threat detection tools that avoid alert fatigue.
- Eliminate blind spots by removing the limitations of system-provided audit logs.

Respond

- Speed incident response with a coherent picture of related events across the hybrid environment.
- Share information between tools, such as your identity security tool, your SIEM and Security Copilot.

Recover

- Regularly create AD backups and store them securely.
- Ensure you can granularly restore individual objects and their properties, including cloud-only attributes.
- Ensure you can promptly restore business operations in case of a disaster with flexible full-forest recovery.

Please visit https://www.quest.com/solutions/itdr/ to learn more about enhancing your ITDR practice.