semperis

Evaluating Identity Threat Detection & Response (ITDR) Solutions

A SURVEY OF IDENTITY-CENTRIC SECURITY LEADERS

New cybersecurity solution category emerges: **Identity Threat Detection & Response**

In the wake of rampant cyberattacks targeting Active Directory (AD)—the primary identity store for 90% of organizations worldwide—cybersecurity analysts have identified the critical need for AD-specific security and recovery solutions. Gartner not only named identity system defense as one of the 2022 top trends in cybersecurity but also devised an entirely new category—Identity Threat Detection & Response (ITDR)—to describe products and solutions that address identity system attacks.

It's now common knowledge that AD is a prime attack target for cybercriminals. In fact, AD is involved in 9 out of 10 cyberattacks. But how can organizations best protect their enterprise identity infrastructures? To better understand how organizations are evaluating identity system defense solutions, Semperis surveyed IT and security leaders at more than 50 enterprise organizations across all major vertical industries.

Key takeaway: Organizations are looking for solutions that address threats **across the entire AD attack lifecycle—before, during, and after an attack**. The top ITDR capabilities that leaders seek include capabilities for preventing, detecting, remediating, and recovering from an attack on hybrid identity systems.

Most important ITDR capabilities:

- ✓ Security posture assessment and real-time monitoring
- ✓ Fast, malware-free AD forest backup and recovery
- ✓ Automatic remediation of detected threats

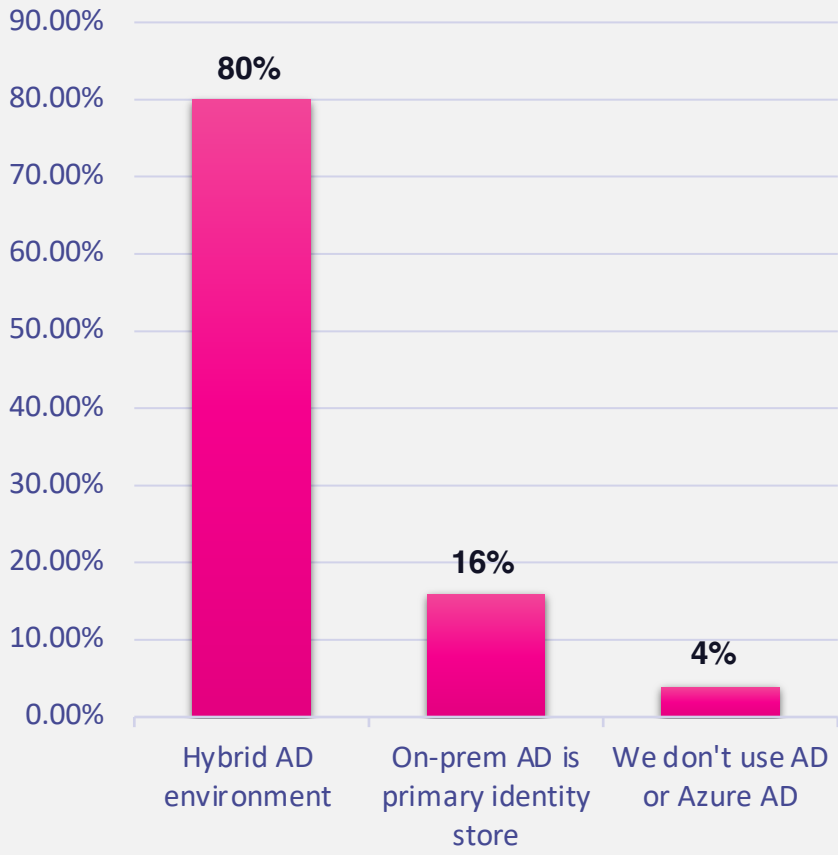
Organizations primarily use **hybrid identity stores**

Our findings reinforce Gartner's prediction that only 3% of organizations will migrate completely from on-premises AD to a cloud-based identity service by 2025. In our survey, 16% of respondents said that on-prem AD is their primary identity store. Another 80% said they either use on-prem AD synchronized to Azure AD or use several different identity systems, including AD and/or Azure AD. Only 4% said they don't use AD or Azure AD at all.

Protecting those hybrid AD systems is top of mind: Survey respondents indicated that the most important capability for **preventing** attacks in their organizations was **continuous monitoring for AD and Azure AD vulnerabilities and risky configurations**.

80% of survey respondents use **hybrid identity systems**—only 4% don't use AD or Azure AD at all.

Use of on-prem AD and Azure AD

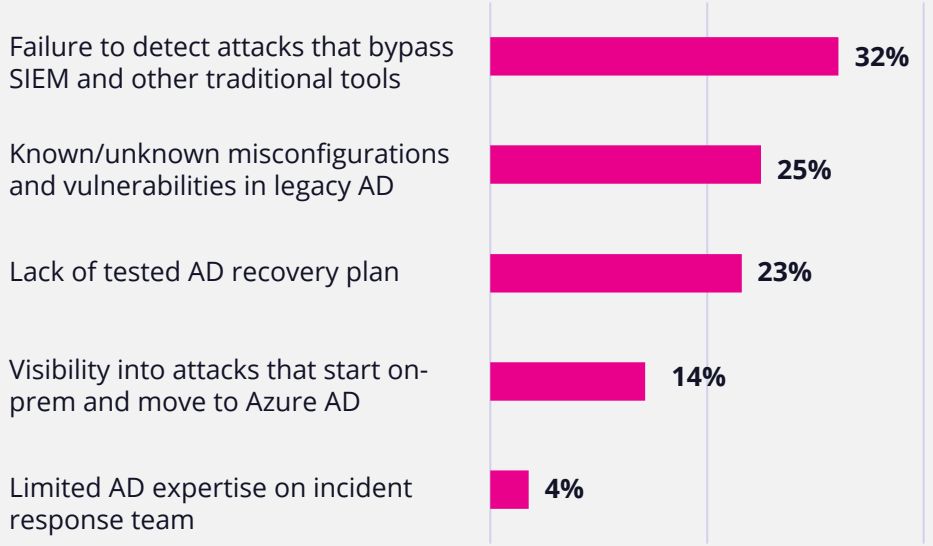


Concerns span protecting hybrid AD systems across **cyberattack lifecycle**

In response to questions about the demands of protecting their hybrid identity systems against attacks, organizations cited issues across the entire Active Directory (AD) cyberattack lifecycle, including preventing, detecting, remediating, and recovering from threats that target AD. Participants' responses indicated a general lack of confidence in their ability to meet the challenges of the current threat landscape. Top concerns included inadequacy of existing solutions, lack of visibility into vulnerabilities, and limited identity security skillsets.

Failure to **detect attacks that bypass SIEM** and other traditional tools was the top concern regarding identity threats.

Biggest concerns regarding identity threats

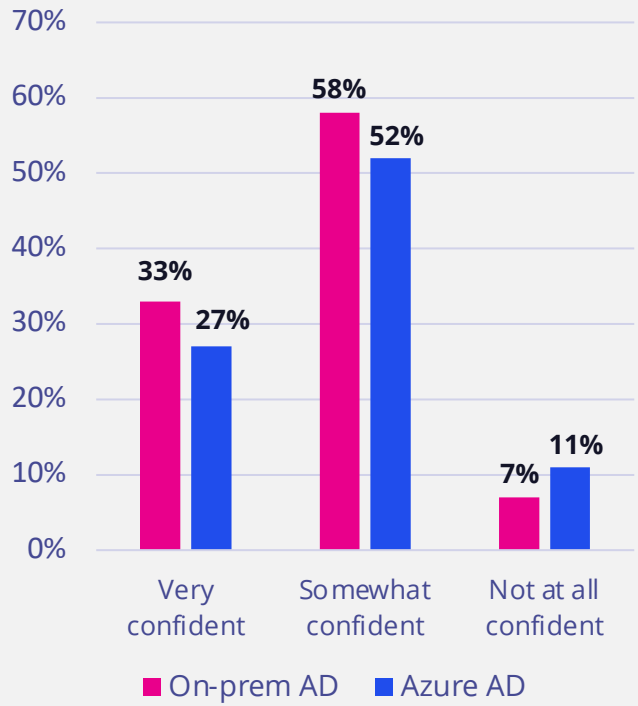


Organizations lack confidence that they can **prevent hybrid AD attacks**

As more organizations adopt hybrid cloud environments, preventing attacks that move from on-prem AD to Azure AD—or vice versa, as in the SolarWinds attack—has emerged as a key concern for many organizations. As cited earlier, most respondent organizations use hybrid identity systems comprising AD, Azure AD, and other cloud systems. Once an organization embraces the cloud, the notion of the traditional network perimeter ceases to exist. In a hybrid identity environment, organizations now must be prepared to guard against an endless array of possible entry points. The acknowledged difficulty in mastering a new security model was reflected in these results: Only 33% of respondents said they were very confident they could prevent on-prem AD attacks, and only 27% said they were very confident they could prevent Azure AD attacks.

Lack of visibility into attacks that **start in on-prem AD and move vertically to Azure AD** drives concern about the ability to prevent attacks

Confidence level in preventing attacks



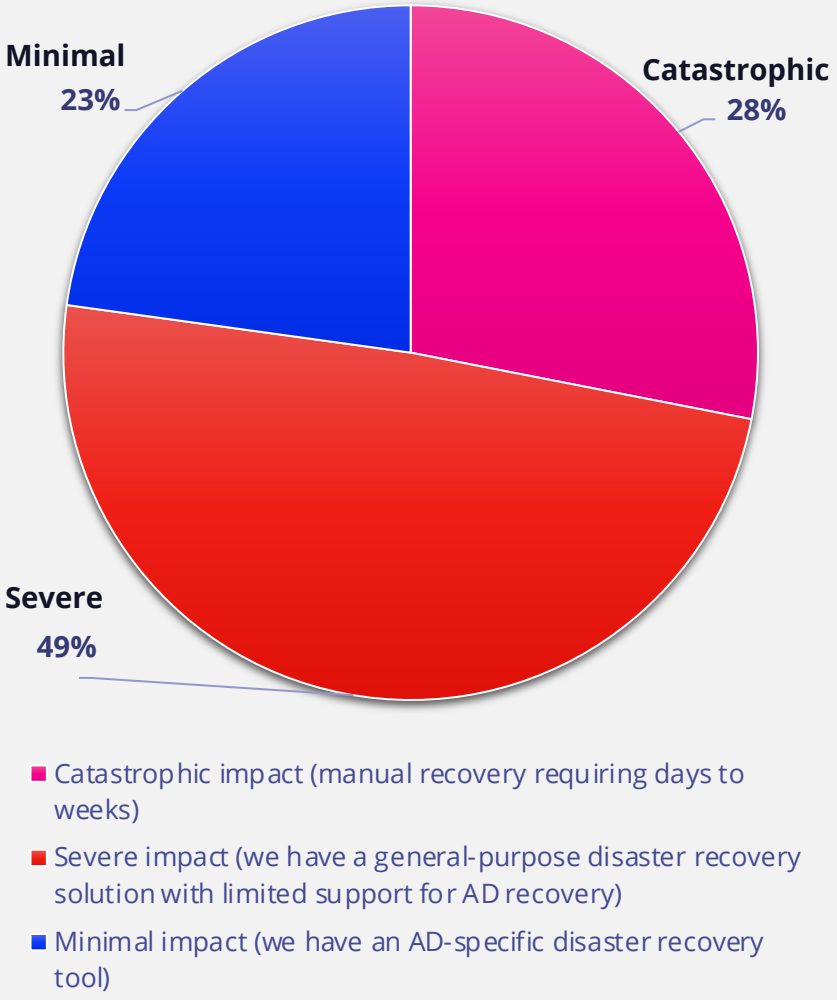
Perceived impact of cyberattacks tied to **concerns about timely recovery**

Most business leaders and their security and IT ops teams recognize that no entity can eliminate the possibility of a cyberattack. Survey respondents expressed a pessimistic view about their ability to recover from a cyberattack that took down AD.

A clear majority (77%) indicated that such an attack would have either a severe impact (as they have a general disaster recovery solution but no specific support for AD) or a catastrophic impact (they would need to conduct a manual recovery using their backups, which would require days or weeks). The loss in business revenue, reputational damage, and—in the case of healthcare organizations—patient health and safety from a prolonged recovery can be a business-ending event.

77% of survey respondents indicated they would experience a **severe or catastrophic** impact if AD was down.

Impact of cyberattack that takes down AD



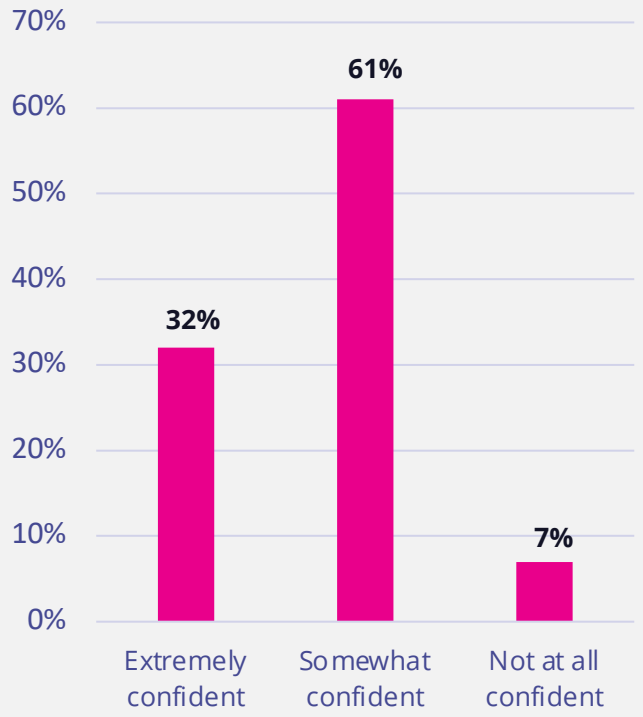
Organizations lack confidence that they can **recover from an AD attack**

The concern about the impact of an AD attack cited earlier is tied to respondents' general lack of confidence that their organizations could quickly recover from a large-scale AD attack. Only 32% of respondents indicated they were "extremely confident" they could recover; 61% of respondents were only "somewhat confident" and 7% were "not at all confident."

Concern about the ability to quickly recover AD was reflected in responses to questions about overall AD security concerns and the capabilities that respondents prioritized when evaluating recovery solutions. These priorities include the need for automated, multi-forest AD recovery; the ability to quickly provision an isolated recovery environment for drills; and AD expertise in incident response.

Only **32%** of respondents indicated they were **extremely confident** they could quickly recovery from a large-scale AD attack.

Confidence level in quickly recovering AD from a large-scale attack



Organizations prioritize ITDR capabilities that **span the attack cycle**

Respondents' rankings of Identity Threat Detection & Response (ITDR) capabilities by importance pointed to solutions that would help them protect Active Directory (AD) before, during, and after an attack—with the top priority being security posture assessment and real-time monitoring for 40% of respondents. In perhaps an acknowledgement that sophisticated attackers are constantly devising new ways to compromise AD, 27% prioritized fast, malware-free AD forest backup and recovery and 20% chose automatic remediation of detected threats.

These results indicate that organizations are fully aware that AD is a prime target for attackers. An effective defense must encompass solutions for preventing, remediating, and recovering from attacks.

Rankings of ITDR capabilities reflect the acknowledged need for a **layered defense strategy** that can protect AD before, during, and after an attack.

Ranking of ITDR capabilities by importance to respondents

1. Security posture assessment and real-time monitoring
2. Fast, malware-free AD forest backup and recovery
3. Automatic remediation of detected threats
4. Risk scoring, risk prioritization, and remediation guidance
5. Post-breach forensics analysis

Organizations seek AD-specific ITDR solutions that **span the AD attack lifecycle**

Given the proliferation of attacks that target Active Directory (AD), security and IT operations leaders understand that protecting the enterprise identity infrastructure is imperative to the business. According to Gartner, "Misused credentials are now the top technique used in breaches. Nation-state-level attackers are targeting Active Directory and the identity infrastructure with phenomenal success."

- A hybrid AD environment is the primary identity infrastructure for most businesses and is involved in 9 out of 10 attacks.
- Given the escalation in cyberattacks against AD, organizations need a layered defense strategy to protect against business-damaging compromises.
- Organizations' concerns about protecting AD encompass the entire lifecycle.
- Top priorities for Identity Threat Detection & Response (ITDR) solutions are vulnerability assessments and continuous monitoring; fast, malware-free full AD forest recovery; and automatic remediation of malicious threats.

Organizations are fully aware that a layered defense strategy provides the optimal protection. ITDR solutions that don't address each phase of the AD attack lifecycle will leave organizations vulnerable to devastating attacks.

Need help?

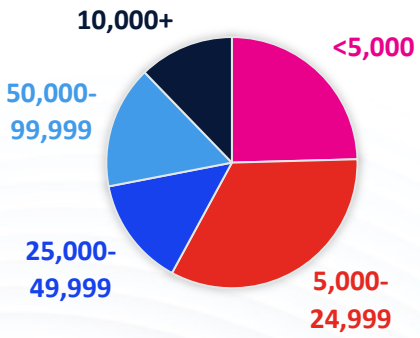
Semperis ITDR solutions protect AD before, during, and after an attack

- Stop attackers from gaining access to hybrid AD environments
- Capture AD changes that bypass SIEMs and other security logging tools
- Automatically remediate malicious changes
- Shorten AD cyber disaster recovery time by 90%
- Harden Active Directory against cyber attacks leading to improved security posture
- Mitigate and recover from AD attacks with guidance from battle-tested incident response team

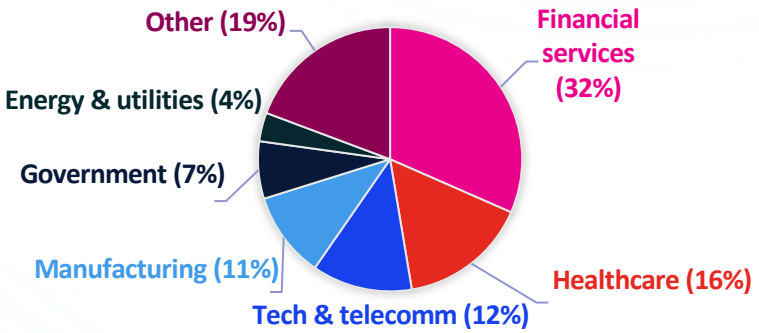
Methodology

At the 2022 Gartner IAM Conference in Las Vegas, we surveyed enterprise IT and security leaders about their identity system defense concerns and their priorities when evaluating Identity Threat Detection & Response (ITDR) products and services. More than 50 organizations, mostly from mid-sized and large enterprises across all industries, provided responses. Respondents received a $25 gift card in appreciation for their participation.

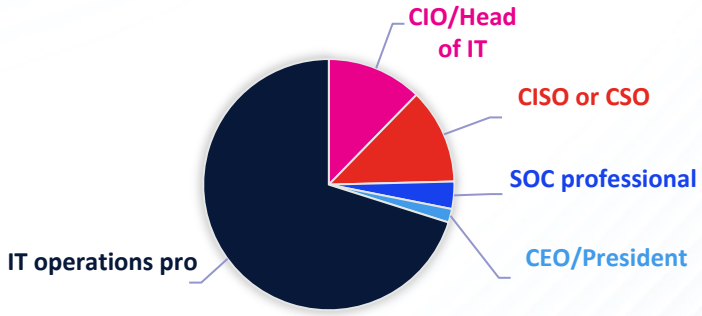
COMPANY SIZE (# OF EMPLOYEES)

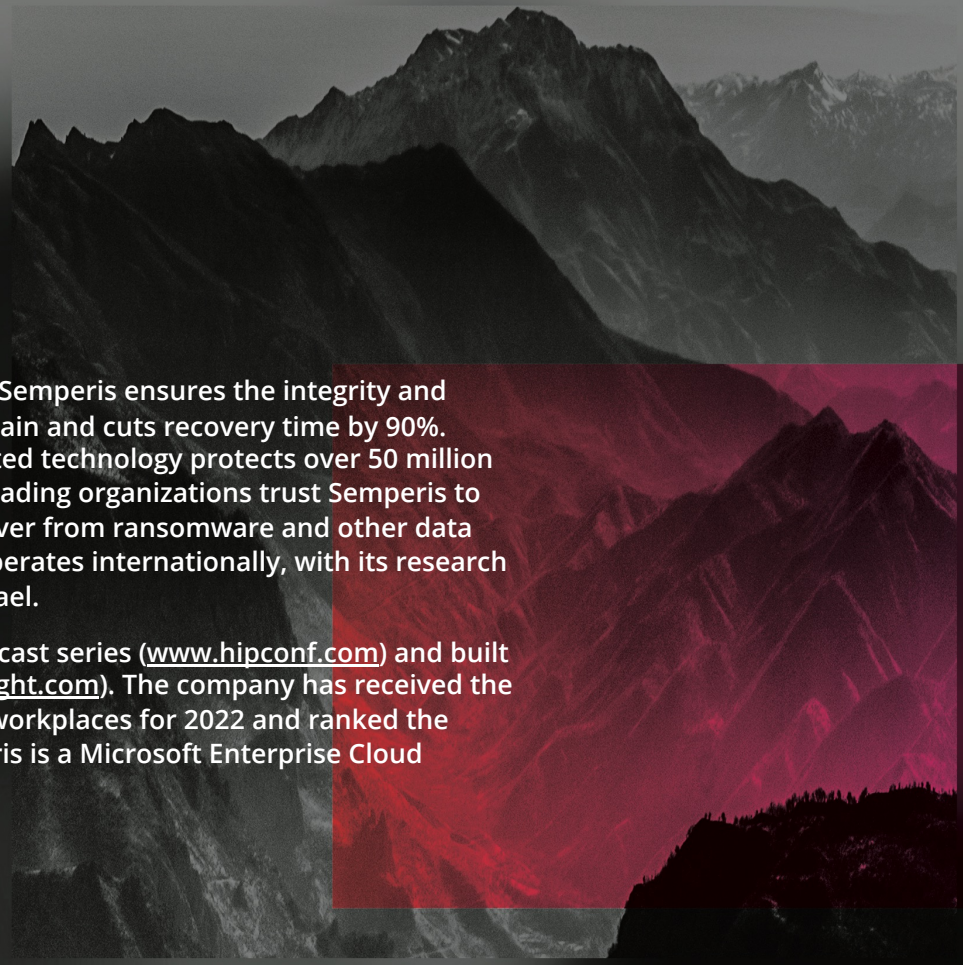


INDUSTRY



TITLE





About Semperis

For security teams charged with defending hybrid and multi-cloud environments, Semperis ensures the integrity and availability of critical enterprise directory services at every step in the cyber kill chain and cuts recovery time by 90%. Purpose-built for securing hybrid Active Directory environments, Semperis' patented technology protects over 50 million identities from cyberattacks, data breaches, and operational errors. The world's leading organizations trust Semperis to spot directory vulnerabilities, intercept cyberattacks in progress, and quickly recover from ransomware and other data integrity emergencies. Semperis is headquartered in Hoboken, New Jersey, and operates internationally, with its research and development team distributed throughout the United States, Canada, and Israel.

Semperis hosts the award-winning Hybrid Identity Protection conference and podcast series (www.hipconf.com) and built the free Active Directory security assessment tool, Purple Knight (www.purple-knight.com). The company has received the highest level of industry accolades, recently named to Inc. Magazine's list of best workplaces for 2022 and ranked the fastest-growing cybersecurity company in America by the Financial Times. Semperis is a Microsoft Enterprise Cloud Alliance and Co-Sell partner.

+1-703-908-4884
info@semperis.com
www.semperis.com

221 River Street
9th Floor
Hoboken, NJ 07030