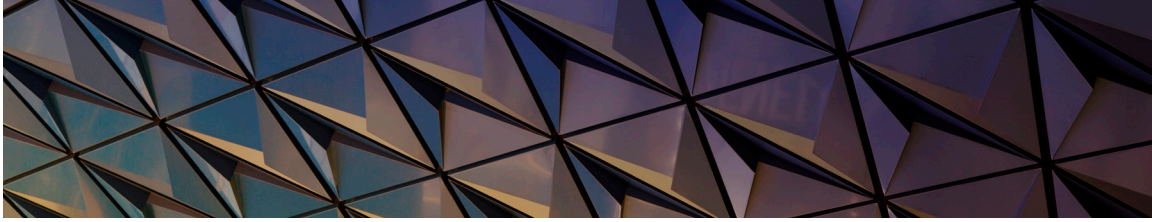
451 Research
by S&P Global



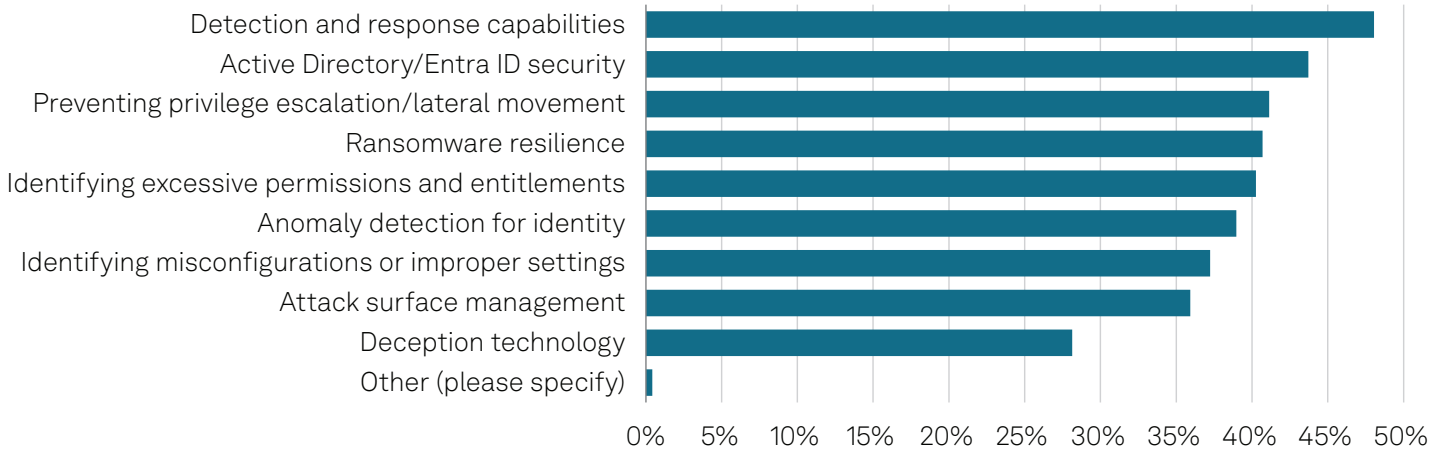
Beyond ITDR: Identity resilience needs detection, protection and recovery

The Take

"Attackers don't break in, they log in." While this phrase has become a cliché, most attackers target identity and access management (IAM) systems directly, typically by leveraging stolen credentials to compromise the identity infrastructure itself, escalate privileges and otherwise enable a successful breach. This phenomenon provided the foundation for an entirely new sector of the cybersecurity market: identity threat detection and response (ITDR). ITDR emerged specifically to help thwart identity-based attacks by applying a variety of methods to detect anomalies such as privilege escalation and lateral movement, secure directory services and provide remediation options such as removing excessive privileges. However, a truly comprehensive approach to securing identities and identity infrastructure requires more than just detection and response. It should also include capabilities for protection and recovery to keep an organization's identity estate running smoothly.

Survey data from 451 Research's Voice of the Enterprise (VotE) service shows that the most important features of ITDR offerings are detection and response (48% versus 39% in 2024's survey), security for Microsoft Active Directory (AD) and Entra ID (44% versus 39% in 2024), and preventing privilege escalation/lateral movement (41% versus 38% in 2024).

Features considered most important for ITDR by IT decision-maker respondents



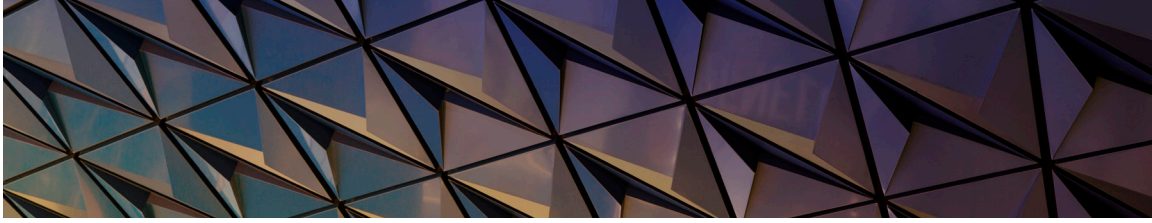
Q. What are the most important features for identity threat detection and response (ITDR)? Please select all that apply.
Base: All respondents, abbreviated fielding (n=231).
Source: 451 Research's Voice of the Enterprise: Information Security, Identity Management 2025.

Business impact

ITDR is a key component of identity resilience, but it is not enough. ITDR helps teams detect and respond to a wide range of identity-based threats, including ransomware and attacks on AD. But as identity environments become more complex and the associated risks grow, identity resilience is becoming an imperative as identity-based attacks become more destructive and persistent.

Copyright © 2026 S&P Global. The content of this artifact is for educational purposes only. S&P Global does not endorse any companies, technologies, products, services, or solutions. Permission to reprint or distribute any content from this artifact requires the prior written approval of S&P Global.Content may be created with the assistance of an AI tool in accordance with our Terms of Use.

451 Research
by S&P Global



Organizations need to protect more than just the identities in AD and Entra ID. While AD and Entra ID remain the foundation of many enterprises' IT estates, many firms' identity assets are distributed across a growing range of directories, apps, devices and workloads. Organizations need to protect their entire hybrid identity estate so access can be protected and cleanly restored after a cyber incident.

Identity systems need more than just detection and response. To strengthen identity resilience, organizations should look for misconfigurations, improper settings, and unnecessary or excessive access rights, entitlements or permissions. Comprehensive protection should also include backup and recovery features for AD and Entra ID, AD forests and other identity providers such as Okta.

Basic backup and recovery is inadequate to deliver true identity resilience. Identities are not just another workload; they are high-value targets for attackers because they enable access to critical information and resources. Traditional backup and recovery approaches based on VMs and databases retrofitted for identity environments are insufficient and fail to account for the nuances required to detect, withstand and recover from identity attacks.

Looking ahead

Identity systems underpin access and provide critical support across the business, so identity attacks can disrupt operations well beyond the identity environment itself — a reality that corporate management teams often are not fully aware of. Further, the exponential rise of non-human identities — particularly agents — introduces new complexities and risks, as non-human identities can be used to target human identities in an attack. Thus, as identity environments become more complex and the associated risks grow, identity resilience is becoming an imperative — foundational to both cyber resilience and overall enterprise security.

Identity resilience as a whole is emerging as a necessary response to modern identity challenges, but it is not yet a distinct category. Its emergence speaks to the challenges organizations face and the requirement for an end-to-end approach to quickly and cleanly detect and recover from identity-based attacks.

What specific capabilities are truly needed for identity resilience? At a high level, identity resilience should combine detection, protection and recovery in a holistic, unified offering that goes beyond reactive techniques focused on a narrow set of identity resources.

Specific technical requirements include the ability to keep an organization's identity providers continually online and functioning to avoid downtime and service disruption for customers. Most IAM tools assume an identity provider is always available, so identity recovery and response are important, as are automated AD forest recovery and automated remediation. Another critical feature is the ability to restore to the last known trusted state; as 451 survey data shows, ransomware remains a major threat, and it is critical not to restore poisoned data or reinstate attacker access. Additional key capabilities include continuous monitoring for directory changes, misconfigurations and permissions; decoupling recovery from the original OS; recovering to different infrastructure; and post-breach forensics.

COHESITY

As organizations look to strengthen identity resilience, they should understand that identity is uniquely at risk and challenging to protect. Organizations need to answer which identities were compromised and how to restore trusted access. Cohesity Identity Resilience is designed to help security and IT teams face those challenges to protect identity systems before, during, and after an attack. It aligns to the real sequence of identity compromise so you can proactively harden, surgically remove attacker persistence, and bring back identity systems cleanly and quickly.

To learn more, visit: cohesity.com/identity-resilience.