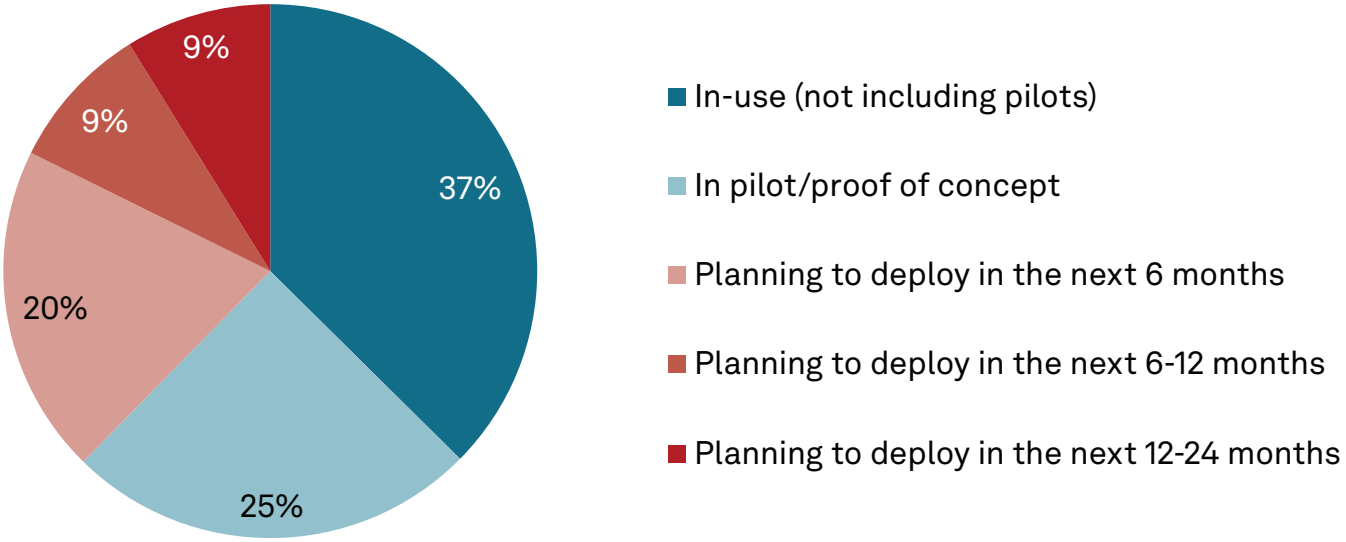
451 Research
S&P Global
Market Intelligence
Business Impact Brief

Identity and Access Threat Mitigation:
A Convergence of Priorities for Enterprise Defense

The 451 Take

In our surveys of enterprise security practitioners, threat detection and response emerges as a top priority. More than 90% of respondents to 451 Research's Voice of the Enterprise: Information Security, Technology Roadmap 2022 study indicated that extended detection and response (XDR) – a concept that embraces a range of new approaches to a variety of threats and their mitigation – was either already in use or planned for deployment within the next 24 months. Meanwhile, the percentage of respondents reporting that these technologies are already in use at their organization rose to 34% from 20% in the prior survey.

XDR Implementation Status



Q. What is your organization's status of implementation for the following information security technologies? -Extended detection and response (XDR)

Base: All respondents (n=133)

Source: 451 Research's Voice of the Enterprise: Information Security, Technology Roadmap 2022

Among the range of threats that organizations are looking to address, those that target identity and access controls are some of the most significant. These controls are among the first lines of defense any organization can have against unauthorized access and exploitation of sensitive digital resources. This, in turn, has made them a target – and one that is more assiduously targeted by adversaries, as evident in a range of successful attacks. Just as important is the need for effective response to identity and access threats, in order to reduce the exploitable attack surface and mitigate the impact of an attack.

Business Impact

For the adversary, defeating IAM offers high return on effort. Simple economics support a straightforward fact: attackers can get a lot of bang out of compromising IAM. Exploiting access gives them the same degree of privilege in interacting with digital assets as the genuine user or account holder – and if they're discreet, they may throw off few signals that would attract unwelcome attention. This has played a key role in the success of attacks such as those involving ransomware.

Targeting IAM exploits the human factor in technology defense. When technology control depends on people to recognize and defeat a threat, attackers can exploit human behavior and induce individuals to give up sensitive access or information – and people can be exploited in ways technology can't.

IAM systems harbor a wealth of information for attackers. Directory systems often serve as an encyclopedic catalog not only of access accounts, privileges and groups, but of policy as well as assets and their attributes. This is intentional, in that a directory can be a convenient way of enabling users to find digital assets throughout the organization. When attackers compromise legitimate access, they may also gain access to this comprehensive inventory.

Increased targeting of IAM controls means organizations must harden this primary line of defense. The attributes of IAM systems have made them a particularly attractive target for attackers. The success of tactics from Mimikatz to Bloodhound to phishing and malware illustrates the rewards of exploiting IAM assets for the attacker. Widely adopted IAM systems won't be going away anytime soon – and they often incorporate a substantial legacy of issues that must be protected to assure their resilience.

Proactive IAM must be matched with appropriate IAM threat detection and response. These factors have introduced the need to focus the growing sophistication of threat detection and response on threats to identity and access controls. If attackers are able to compromise and use legitimate access without arousing a response, threat detection must be sharpened accordingly, across a range of techniques. Furthermore, organizations must take an equally comprehensive approach to their response to such attacks. If they don't, attackers may achieve the undetected persistence they crave in order to maintain a foothold that can be leveraged for maximum sustained impact.

Looking Ahead

The current threat environment has not only heightened the need to better defend IAM resources; it has given rise to identity and access threat mitigation as an emerging trend in its own right. An emphasis on a wide range of techniques to detect and defeat attacks against IAM and to harden IAM against such threats is already assuming a growing significance. We expect this significance to be called out by name in features specific to mitigating IAM threats across a range of products and services in the cybersecurity market. It will be an increasingly defined attribute of defenses that complement both proactive and reactive cyber resilience.