HealthManagement
Promoting Management and Leadership

Identity Security 2024: Mapping the Threats and Goals

The efficient management of identities and access has become central to digital business. It determines the speed and agility with which an organization is able to operate or pursue new goals; it underpins employee productivity and enables operational efficiencies; and it is key to security, privacy, and compliance. Most organizations have deployed identity and access management (IAM) solutions to handle their operational demands effectively.

However, the identity infrastructure and processes themselves are a frequent target of cyberattackers, driving recognition that identity security measures need to be improved.

What Are the Main Identity Threats?

IDC's *Global Identity Management Assessment Survey 2023* found that in Western Europe, the two categories of identity that are perceived as the biggest threats are **hybrid or remote employees and partners, suppliers, or affiliates** (each category mentioned by 49.6% of respondents). The external nature of these identities — from a location perspective, an employment perspective or both — increases the attack surface of the organization and creates potential vulnerability and exposure of data, systems, and processes.

Nevertheless, those roles also provide access to a broader talent pool and deliver operational efficiencies and economies of scale, allowing organizations to outsource non-core functions. Consequently, organizations are striving to accurately assess and manage the risk.

What Are the Top IAM Investments?

Accordingly, the top two service areas in which Western European organizations are planning to make significant IAM investments to address the security risk **are identity management** for roles and authorizations (56.9%) and **privileged access management** (PAM – 53.3%).

Note that since the onset of the COVID-19 pandemic in 2019, investments in PAM have been growing steadily, as organizations required greater control over remote employees accessing sensitive corporate applications and data.

Which IAM Areas Must Improve

The survey also asked which IAM areas organizations need to improve on significantly in the next 18 months. From a list of options including functional, operational, structural, and organizational aspects, the top responses were squarely in the area of identity security:

- The biggest share of organizations (45.1%) want to improve their ability to detect insider threats.
- A further 44.3% aim to improve identity threat detection and response (ITDR).
- 9% aim to improve integration with other IT security solutions.

The emergence of ITDR in the last couple of years as a key priority for organizations building out their security and identity capabilities has been a key takeaway of multiple IDC surveys now.

The final area to touch on is the “wish list” question, always a good barometer of what respondents really value. In this case, if your organization had the budget and resources to do so, what’s the one identity technology solution you’d add or strengthen in the next three months?

The top response was strong authentication, such as two-factor authentication or multifactor authentication (MFA), cited by 25.6%. This was followed by generative AI (GenAI) for fraud detection and identification of synthetic identities (20.3%) and, again, ITDR (19.5%).

The rapid maturing of deep fake tools and capabilities underlined by real-world examples of successful attacks is already driving demand for security tools to protect against them as the GenAI arms race heats up.

Identity really is at the heart of everything in the digital era: business, security, trust, compliance, risk management, operational efficiency, and more. It is fundamental to enterprise initiatives such as building cyber resilience or adopting zero trust principles.

Many direct references to IAM and identity security controls in the growing landscape of EU legislation further emphasize why identity should be high on every organization’s priority list. This new report maps many of the key trends shaping the **European identity and access landscape in 2024.**

Mark Child

Associate Research Director, European Security

Source & Image Credit: IDC

Published on : Thu, 14 Mar 2024