



Identity Security

Closing the Gaps in Enterprise Access Risk

Businesses have expanded access to systems, data, and workflows faster than many identity programs were designed to manage. What once centered largely on employee logins now includes contractors, partners, service accounts, cloud workloads, automation, and AI agents. That broader mix of identities creates a larger and more complex attack surface, especially when credentials and permissions don't have clear ownership.

Identity Has Outgrown Traditional Access Management

Identity is the front door to the enterprise, but the risk doesn't stop at login. A trusted identity can become a path an attacker uses to move through systems, reach sensitive data, or misuse accounts and services. That's why identity security must be treated as a program, not a narrower access management function. Governance, ownership, and process have to hold the program together. Tools support that work, but they can't replace it. Existing identity tools still matter, but organizations also need access management, governance, and privileged access to work together under a single governance model.

Machine Identities Are Expanding the Risk

In many enterprise environments, machine identities, including AI agents, now outnumber human identities by more than 100 to 1. That means many access decisions involve accounts, credentials, services, scripts, and



- Technologies are outpacing the identity governance built to control them.
- Machine identities and AI agents are expanding business-critical risk.
- Clear ownership is essential before access can be governed.
- Organizations can build stronger identity programs now, even as standards continue to form.

automated processes that don't behave like human users and often lack the same ownership, review, and credential discipline. Exposure can also extend outside the organization when partners, vendors, or data subprocessors retain access that isn't limited, reviewed, or revoked when it should be.

Precision Comes Before Tools

A mature identity security program doesn't assume every risk can be eliminated. It uses data to identify gaps, rank exposure, and decide what needs to change first. It also creates accountability by tying identities, access decisions, and activity back to a clear owner. That work has to come before tool decisions. Once organizations understand their identity estate, access patterns, and highest-risk gaps, they can make better decisions about where technology, automation, and process changes will have the greatest impact.

Ownership Before Control

Organizations can't reduce risk if they don't know what identities exist, who owns them, what access they have, or whether that access is still appropriate. Organizations need to identify identities, understand what they are, and assign clear ownership before they can govern access effectively. Partial visibility isn't enough. Leaders need a complete view across every identity type before they can prioritize the risks that matter most, such as standing privilege, orphaned accounts, stale credentials, and unmanaged third-party access.

that can mature as standards and technologies become clearer.

Evolving Solutions helps organizations bring precision to identity security. By assessing the full identity estate, mapping current controls to business and compliance requirements, and identifying the gaps that create the most risk, we lead a prioritized, sequenced roadmap with defined ownership and measurable controls. With the right visibility, ownership, and governance model, organizations can reduce the business impact of compromised or misused identities.

Building Against Forming Standards

That foundation matters because identity security is still evolving. Standards and controls for non-human identities and AI agents are still taking shape, so leaders can't design around a fixed end state. But they don't have to wait. Leaders can start now by building the process, visibility, and governance model



We help organizations build the governance foundation for identity-driven security.

Let's Get to Work!