

A unified identity security program

One program to define, enforce and correct access for every identity (human, machine and AI agent), operating as the identity control plane among the tools you already own.

Identity is the leading initial attack vector, and the fastest-growing share of the risk isn't your human workforce. It's the service accounts, embedded credentials and AI agents operating alongside it, most of which no one formally owns. The tools defending identity remain fragmented across three consoles; attackers treat identity as one attack surface.

One Identity closes that gap with a unified program: Identity Manager (IGA), Safeguard (PAM) and Active Roles (Simple Governance for Microsoft Environments), engineered as one closed loop that defines what every identity should have, enforces it and corrects divergence automatically. **It operates as the identity control plane among your existing tools, not a replacement for them**, producing a risk posture your team can operate, your auditors can verify and your CFO can defend.

The challenge, quantified

- Credential abuse is the No. 1 initial attack vector, present at the start of 22% of breaches and involved in 88% of basic web-application attacks. Third-party breach involvement doubled year-over-year to 30%. (Verizon 2025 DBIR)
- The average breach now costs \$4.44M globally and \$10.22M in the US. Among organizations that suffered an AI-related security incident, 97% lacked proper AI access controls. (IBM Cost of a Data Breach 2025)

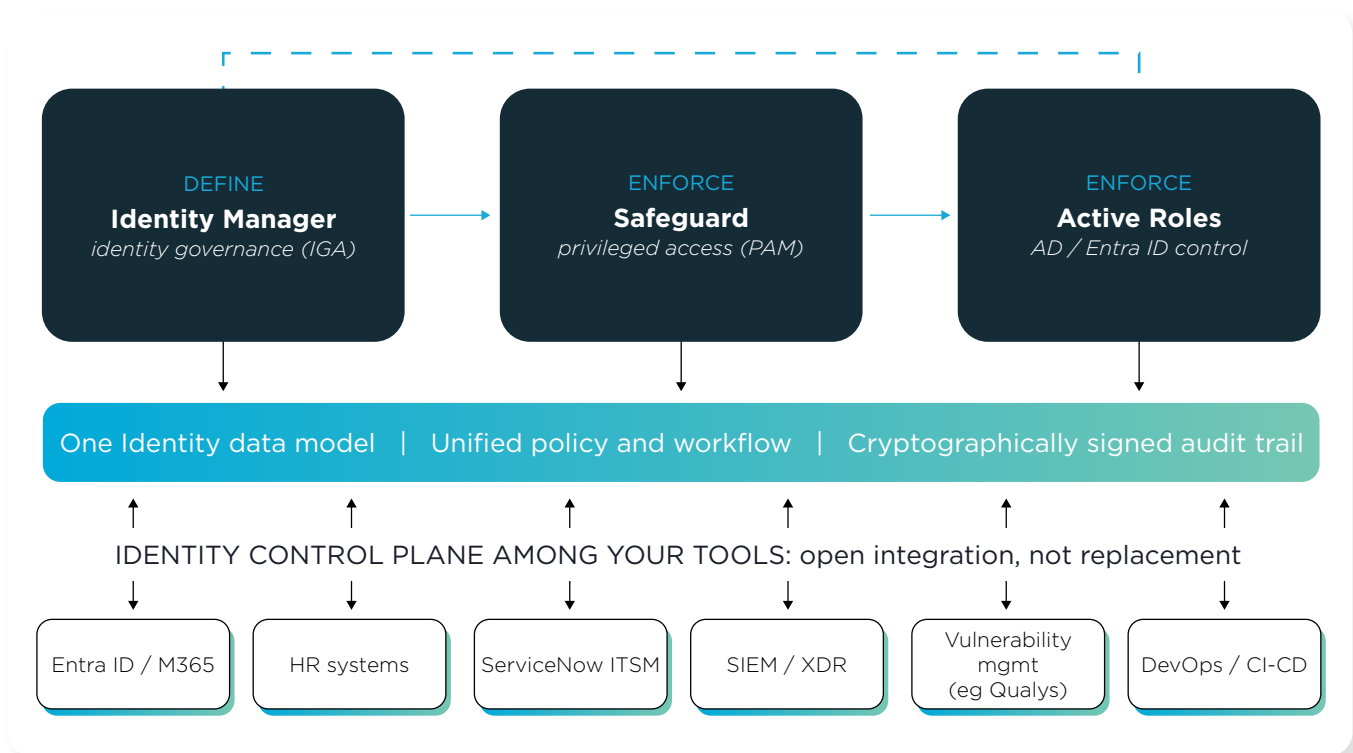
Behind the numbers, one structural gap: access certified in the IGA tool isn't what's enforced in the directory; non-human identities outnumber people

yet were never enrolled in lifecycle governance; and AI agents are arriving faster than ownership models. The status-quo cost is operational: audit prep in weeks, revocation in days, and three stacks to integrate and pay for.

The program: three pillars, one closed loop

- **Define | Identity Manager (IGA):** automated lifecycle and provisioning across on-prem, hybrid and cloud; continuous certification and attestation; ITDR playbooks that act on identity threats automatically.
- **Enforce | Safeguard (PAM):** discovers and vaults privileged and machine credentials; Zero Standing Privilege via just-in-time access; session recording with behavioral analytics; signed audit trails on demand.
- **Enforce | Active Roles:** policy enforced at the moment of change across AD, Entra ID and M365; permanent rights eliminated; one governed console for the hybrid Microsoft estate.
- **Deliberate scope:** this program covers the governance-and-privilege control plane, where audit findings originate and consolidation pays back fastest. Workforce authentication/SSO is intentionally out of scope; One Identity serves it with OneLogin, and the program integrates with whichever access-management platform you run, including Entra ID.

Architecture at a glance



The loop in an incident: Safeguard flags a service account acting outside its pattern and an ITDR playbook in Identity Manager disables it and triggers owner attestation. Active Roles enforces the change across AD/Entra. One event, one signed audit record, minutes end to end, versus three tickets over three days across point tools.

Business outcomes and how they're measured

- **Reduce business risk:** standing privilege replaced with just-in-time access; unowned accounts eliminated; automated response cuts detect-to-contain time, the single largest driver of breach cost in IBM's 2025 analysis. Measured via expected-loss modeling against published benchmarks.

- **Lower the cost to operate:** three point products, contracts and custom IGA-PAM-directory integrations collapse into one pre-integrated program. Measured in license delta, integration engineering hours and audit-prep hours, with evidence on demand for SOX ITGC, DORA, NIS2, PCI DSS 4.0 (Req. 7/8/10) and HIPAA §164.312.
- **Help the business move faster:** day-one access for joiners, same-day revocation for leavers and a governed on-ramp for AI initiatives. Measured in time-to-access, time-to-revoke and ticket volume; a value model is quantified for your environment in the assessment below.

One discipline, every identity type

The same discipline of named ownership, vaulted and rotated credentials, scoped access, monitored activity and an accountable audit trail extends from employees to service accounts to AI agents, each registered with an identity record and owner before deployment. **Plainly:** agent governance today means proven NHI controls extended to agents; purpose-built controls for fully autonomous, ephemeral agents are roadmap and we will tell you which is which.

Why One Identity

- Built together, not bought together. The three products share one identity data model, one policy engine and one signed audit trail, engineered as one program for years rather than assembled by acquisition. The closed loop ships; it isn't a services project.
- Control plane, not lock-in: the honest tradeoff. Open, bi-directional integrations with Entra, SIEM/XDR, ServiceNow, vulnerability management, HR and DevOps toolchains. A best-of-breed stack can win any single category feature-by-feature; what it can't do is close the loop between categories without integration you build, maintain and audit yourself. The loop, not the feature list, is where identity risk lives.
- Proven at scale. 500M+ identities for 11,000+ organizations, including 80% of the Fortune 100. Visionary, 2025 Gartner® Magic Quadrant™ for PAM; recognized in the 2025 Gartner® Market Guide for IGA. Deployed self-managed to fully managed, no rip-and-replace: the program coexists with incumbent IGA/PAM during phased migration.

Learn more about:

- [Active Roles](#)
- [Identity Manager](#)
- [Safeguard](#)



About One Identity

One Identity delivers trusted identity security for enterprises worldwide to protect every identity, human and non-human. With flexible deployment options and subscription terms, from self-managed to fully managed, our solutions plug directly into an organization's identity fabric to strengthen the identity perimeter, reduce breach risk and keep governance and compliance aligned at scale. Headquartered in Cork, Ireland, and trusted by 80 of the Fortune 100, One Identity is a leading provider of integrated identity governance and administration (IGA) and privileged access management (PAM) for identity security without compromise. Learn more at [oneidentity.com](#).