Stronger security. Better ROI.

How a unified approach to Identity security helps extend the value of your security investments

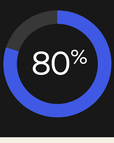
As your organization evolves, you continuously adopt new security and technology solutions to meet growing needs.

However, these additions often fragment your tech stack, making it increasingly difficult to monitor and manage Identity data effectively.

The result? Scattered permissioning, security blindspots, and an overburdened security team.

Identity fragmentation across security tools undermines your ability to aggressively catch and remediate potential breaches in real-time.

Bad actors know this, which is why Identity has become their #1 vector of attack.



80% of data breaches began with stolen credentials and/or phishing attacks.

(Verizon)

Even organizations with advanced security solutions remain vulnerable to threats.

Without seamless integration, these tools can create blind spots, operational silos and delayed threat response — weakening overall security and increasing the risk of breaches.

180%

Identity-related attacks are rising at a rate of 180% year-over-year.

(Okta)

290 days

On average, it takes organizations 290 days to contain a breach.

(Verizon)

$4.8M

The cost of the average data breach in 2024 was $4.88 million.

(IBM)

Question:

How can modern organizations maximize the power of their security investments?

Answer:

A unified approach to Identity-driven security that connects all risk and contextual signals into one centralized platform.

Okta makes it possible.

By unifying Identity orchestration, Okta aggregates insights from across your tech and security stacks, centralizes them within a single platform, and enables real-time threat remediation with automation-driven workflows.

Identity Threat Protection with Okta AI

Continuously assess user risk and context and automatically respond to identity threats across your ecosystem

- Synthesize and prioritize risk signals from across all systems, devices, and user types, to help ensure a proactive security posture
- Leverage both third- and first-party signals to detect and remediate emerging threats in real-time
- Quickly mitigate threats with customizable automated actions, such as triggering MFA or logging out compromised users from all active sessions

Okta Identity Governance

Gain a unified view of access across systems and applications, ensuring better control and oversight

- Streamline permissioning with role-based and group-based access to help ensure the right people have the right access for the right amount of time
- Automate role changes and de-provisioning to maintain security
- Help ensure new hires have the proper access from day one, accelerating their productivity and reducing risk

Okta Identity security posture management

Get fully integrated, real-time confirmation of Zero Trust principles across the entire organization

- Proactively identify vulnerabilities and security gaps before they can be exploited
- Continuously uncover critical misconfigurations and gaps, such as inconsistent MFA enforcement, and account sprawl
- Run automated scans of your tools and evaluate your setup against an aggregated set of Zero Trust frameworks

Ready to learn more about unifying your security strategy with modern Identity solutions?

Reach out to our team and see the Okta platform in action.

Contact us