okta

The Strategic Value of Identity for CISOs

The vanishing network perimeter has made identity the critical cybersecurity control plane, dramatically changing security operations. This brief provides a summary of the research* into these changes by the Enterprise Strategy Group, conducted in partnership with Okta, which revealed five key insights on how identity security has become a foundational focus for CISOs:

1. The CISO has moved from defense to offense.
2. CISO responsibilities have shifted toward strategic business enablement.
3. CISOs recognize identity as their organization's biggest vulnerability.
4. CISOs see no easy fixes for identity security.
5. Tech bloat exacerbates identity security problems.

KEY INSIGHT #1:

The CISO has moved from defense to offense

Conventional perimeter-based enterprise security strategies have an inherently defensive nature, but that defensive stance cannot keep up with modern work. The ESG research showed that CISOs' top "jobs to be done" all center on proactive strategies — risk quantification/ reporting, control rationalization, and data privacy:

KEY INSIGHT #2:

CISO responsibilities have shifted toward strategic business enablement

Based on the ESG research, the way CISOs think about their responsibilities is becoming more strategic in nature — and shifting toward more business-critical outcomes.

CISOs' most important responsibilities.

Maturing/evolving policies related to data security and privacy (e.g., Zero Trust)

CISOs are redefining success metrics and moving beyond incident rates and response times to emphasize the business impact of security, such as how downtime frequency or duration connects to security events.

Quantifying/demonstrating how security enables business growth/objectives

A job that used to focus heavily on compliance metrics is now thinking more strategically about business productivity and other "people metrics."

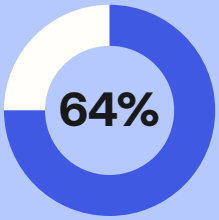
Ensuring strong & seamless authentication across workforce and customers

Identity governance also jumped up the priority list, with CISOs in the research cohort thinking of responsibilities like credential management and access reviews in terms of supporting frictionless access for employees and customers.

KEY INSIGHT #3:

CISOs recognize identity as their organization's biggest vulnerability

Despite the shift from reactive to proactive strategies, roughly 2 in 3 CISOs in the study say it's challenging for them to protect against cyberattacks. More to the point, CISOs recognize identity security as their biggest vulnerability, reporting a wide range of identity challenges that weaken their overall security posture. This should come as no surprise, as widely reported research shows identity is now the top vector for data breach.



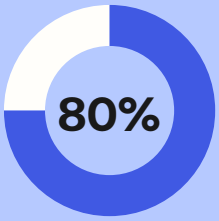
of CISOs say it's **challenging** to stop cybersecurity attacks

2 in 3

of CISOs say the **majority** of **security incidents** are caused by identity

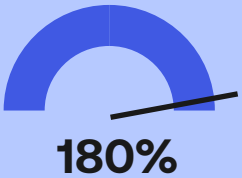
Top identity challenges hindering cyber defenses, as reported by surveyed CISOs

1. Inability to accurately identify and prevent fraudulent account creation and sign-in attempts at scale
2. Inconsistent identity governance practices
3. Lack of support for stronger authentication/ heavy reliance on passwords
4. Manual/ fragmented identity operations
5. Insufficient MFA



of data breaches start with **compromised identites**

Verizon 2024 Data Breach Report



YOY increase in identity-related attacks

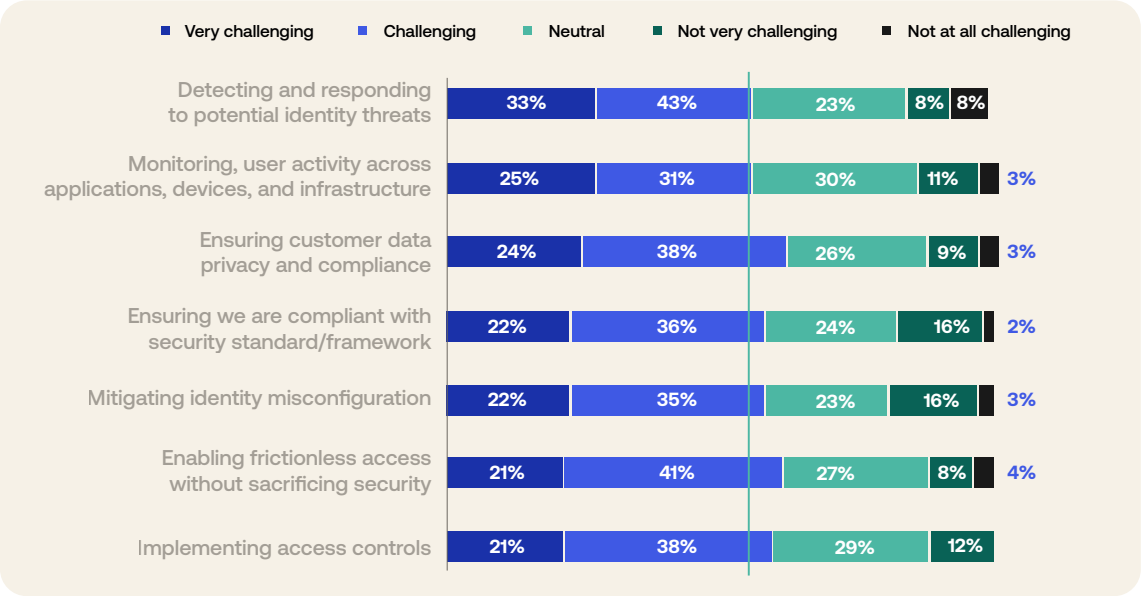
Verizon 2024 Data Breach Report

KEY INSIGHT #4:

CISOs see no easy fixes for identity security

Given its role in the majority of breaches, it's not surprising that a vast majority of CISOs in the research (76%) recognize strengthening identity security as a top priority. So, why haven't they "fixed" it?

Because it's not a single issue to address — they're fighting the identity security battle on multiple fronts, and most CISOs say that ***every element*** of identity security is challenging.



KEY INSIGHT #5:

Tech bloat exacerbates identity security problems

One consistent theme uniting both the business enablement and business protection challenges that CISOs face: tech bloat is making everything worse. Decentralized tech deployment and SaaS sprawl are epidemic problems in the typical enterprise, but those issues now extend to security stacks. The research shows most organizations are working with more than 50 different cybersecurity vendors. Security teams are spending too much time manually orchestrating processes and data flows across solutions — and CISOs are busy trying to create better integrations and eliminate redundancies.

The research also found the following:

Biggest identity security risks

1. Visibility gaps across security tooling
2. Misconfigured/ overprovisioned accounts

Top barriers to enabling frictionless access

1. Managing audit trails across solutions
2. Complexities of managing multiple identity solutions

The typical organization has 60 Different Cybersecurity Vendors

okta

Okta: Powering an Identity-First Security Strategy

The ESG research clearly demonstrates that identity is no longer just an IT function; it is foundational to modern enterprise security. Okta's identity platform is purpose-built to deliver the comprehensive security and agility required for CISOs who want to lead with a proactive, identity-first approach. Okta empowers CISOs to shift from defense to offense by providing the foundational identity security necessary to reduce risk, simplify complexity, and confidently navigate the evolving threat landscape.

* The research/survey was conducted by Enterprise Strategy Group, in partnership with Okta, on or around 01/2025 to 02/2025 and included interviews with over 150 CIOs in North America, EMEA, and APJ.

Ready to learn more about the platform?

We'd love to hear about the challenges you're facing and share how Okta can help.

Learn more