eBook

Secure Identity. Secure everything.

The three principles of a modern Identity strategy

okta

What does your organization think about when it thinks about Identity?

More than likely, the first thing that comes to mind is security — and for good reason. In a threat landscape dominated by credential theft and phishing attacks, it's clear that Identity is the central factor in bad actors' strategies for breaching critical networks and accessing sensitive information. That's why Identity must be the center of every future-ready organization's approach to modern, end-to-end security.

And yet, too many organizations are playing catch up. They're stuck on the now-obsolete paradigm of the secure perimeter, increasingly recognizing that conventional network- and device-focused security tools offer little protection from sophisticated Identity-based attacks and struggling to gain visibility to understand and effectively remediate risk.

Defining a modern Identity strategy

A modern Identity strategy provides a path toward gaining essential visibility across your Identity landscape, identifying vulnerabilities to strengthen security posture, and enabling fast, successful response to potential attacks. Just as critically, a modern Identity strategy can deliver this strong protection — while enabling the seamless connectivity and frictionless experiences that are essential to business success today.

This resource highlights why Identity must be the foundation of enterprise security and technology, and includes information on:

- How Identity-related threats have accelerated
- How traditional approaches to Identity leave organizations vulnerable
- Three principles to guide the adoption of modern Identity

okta

The fragmentation of the enterprise security stack

The past decade witnessed a stark transformation in the enterprise tech stack. The rapid adoption of cloud services, SaaS applications, and remote work has fundamentally changed the way we collaborate and connect. In a business environment that demands tech-enabled differentiation, the notion of maintaining technological unity under an enterprise license agreement (ELA) with one company is out of date. Instead, competitive businesses know they need to build agility and high levels of performance into their workforce and customer technologies and product offerings using a patchwork of best-in-breed solutions.

Modern tech stacks are supremely advanced — and extremely complicated. Ever-expanding networks of point solutions make up fragmented IT environments that scatter business resources (and the Identities contained within them) across a tangled-yet-disconnected web of systems, apps, and infrastructure.

Siloed tech creates security blind spots

This fragmentation creates major security liabilities. It expands the attack surface for would-be attackers by siloing Identities in different places, increasing the likelihood of unnoticed credential theft and exploitation. And it makes it next-to-impossible for security teams to get the broad and deep visibility to access that's needed to remediate vulnerabilities and identify risk.

Bad actors know that Identity represents an expanding blind spot in most enterprises, which is why Identity has become their number one attack vector. According to the 2024 Verizon Data Breach Report, in which Okta participated, 80% of breaches involve some form of compromised Identity. Even more disconcerting is how many organizations are fundamentally unprepared for this new reality: In 2024, the average number of days it took to recognize and contain a data breach was a whopping 290.

okta

It's time to change Identity

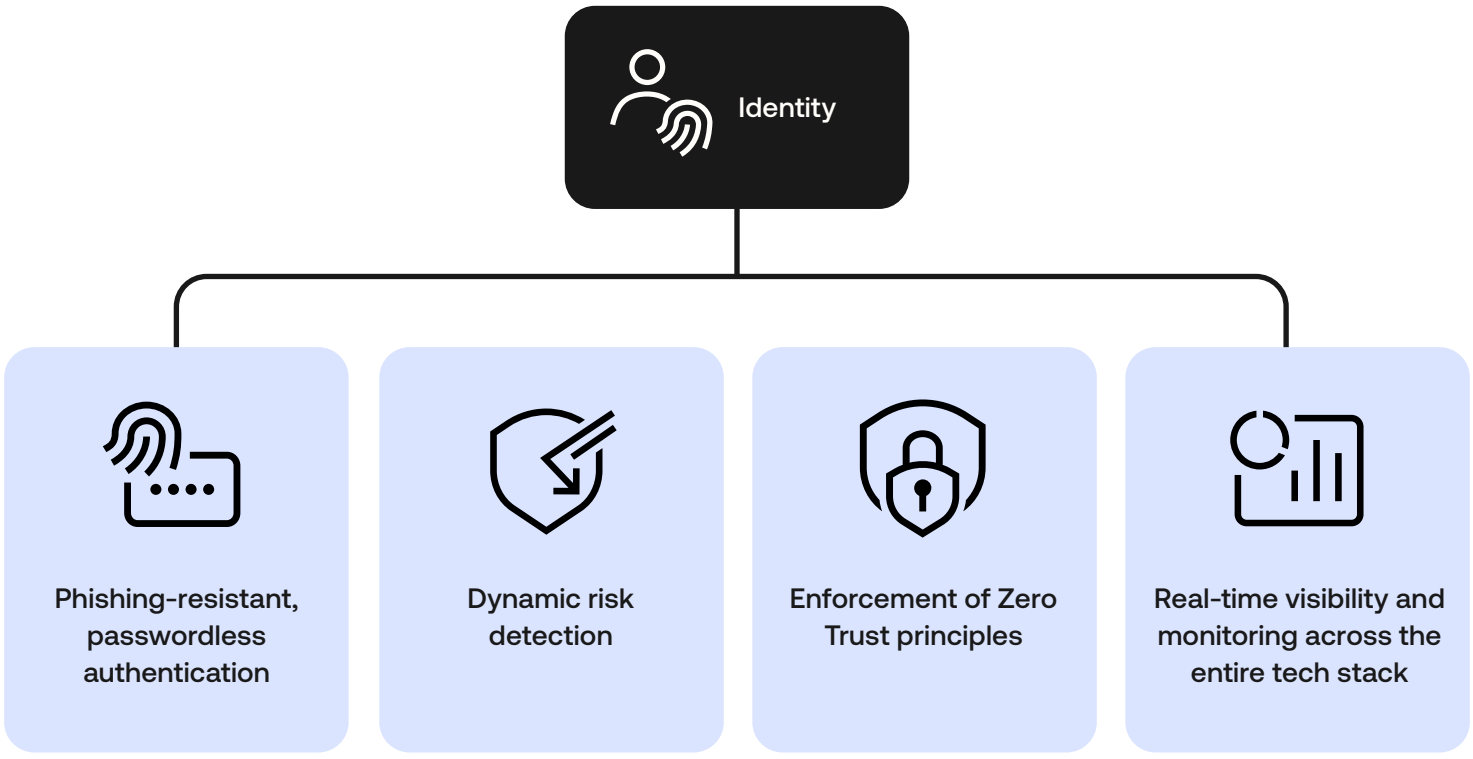
Every organization understands that Identity plays an important role in security. But traditionally, that role is that of a gatekeeper. Few organizations are making use of Identity in an equally critical role: as the essential fabric for enterprise-wide security visibility and intelligence.

For example, most businesses rely on Identity to enable seamless access with secure authentication. But by integrating that Identity functionality more fully into their technology and security ecosystems, organizations can enable dynamic risk detection in real time or support automatic remediation strategies after a bad actor has authenticated using stolen credentials. These are just a few of the ways that Identity can empower security teams to take a more confident and proactive approach to strengthening their security posture.

Centralizing Identity in your security ecosystem

To ignore this potential is to disregard what we already know: that Identity has become the battleground of enterprise cybersecurity. It's how most attackers get in, and it's how the most successful security teams keep attackers out. A modern Identity strategy has the potential to act as a connective thread that enhances every component part of your security environment through a stronger, more unified, and more immediate posture in the face of increasingly sophisticated threats.

To meet the moment, organizations must take a much more expansive (and strategic) view of what Identity is and what it can do.



A closer look at the threat

Bad actors are counting on outdated approaches to Identity. Fragmented IT and security environments scatter core resources, apps, and Identities across different systems and infrastructure, leaving them vulnerable to unnoticed and unaddressed Identity-related attacks. The results can range from inconvenient to disastrous.

Manual processes

Cumbersome, time-consuming permissioning practices that leave important access determinations vulnerable to human error

Blind spots

Poor visibility into the organization's real-time security posture and individual permissions across different systems and applications

Slow response

Delayed response times that allow bad actors to turn Identity-related vulnerabilities into costly, debilitating breaches

This problem is not going away — it's accelerating. AI-powered applications, services, and users are poised to make Identity-related risks even more difficult to detect and thwart. To make it worse, Identity-related attacks don't just look like stolen credentials anymore. Post-authentication threats like stolen session cookies add a new dimension to the already complicated task of monitoring log information for suspicious activity. Add onto this the ever-present risks of well-funded nation-state attacks and hard-to-detect insider threats and you're left with a dire portrait of where risk lies — and where it's going.

80%

Over 80% of all data breaches stem from Identity-related attacks

(Verizon)

180%

Identity-related attacks are increasing at a rate of 180% YoY

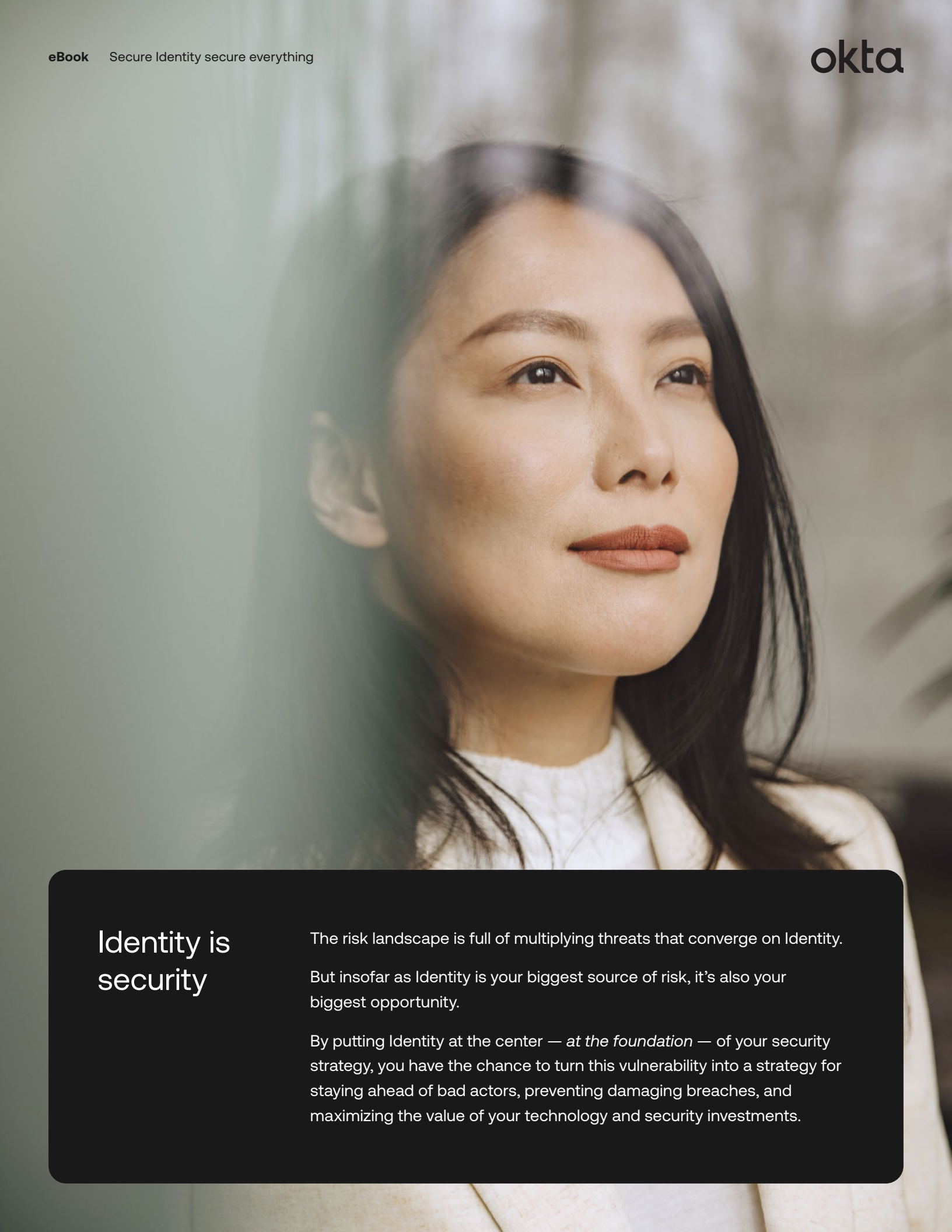
(Verizon)

1.9B

1.9 billion session cookies were stolen from Fortune 1000 employees in 2023

(Fortune)

okta



Identity is security

The risk landscape is full of multiplying threats that converge on Identity.

But insofar as Identity is your biggest source of risk, it's also your biggest opportunity.

By putting Identity at the center — *at the foundation* — of your security strategy, you have the chance to turn this vulnerability into a strategy for staying ahead of bad actors, preventing damaging breaches, and maximizing the value of your technology and security investments.

okta

The three principles of a modern Identity strategy

Now that we've covered the stakes of taking an Identity-first approach to security, let's dive into something more practical: how to take your organization's Identity from where it is to where it needs to be.

Modern, cloud-native Identity solutions give you a fast track to remediate fragmentation issues. This solution provides centralized controls and unified, real-time visibility across all systems and applications — and enables IT and security teams to eliminate blind spots, surface risks and speed response.

This enormous value is divided into three categories:

Comprehensive visibility

to ensure that no vulnerabilities are slipping through the gaps or going unaddressed

Powerful orchestration

to enforce real-time remediation in the event of a potential breach

Broad & deep integrations

to unlock the value of full connectivity throughout your security and tech stacks

In surveying the marketplace for a modern Identity solution, organizations must look for a platform that can deliver on all three of these fronts.

okta

Principle #1

Comprehensive visibility

Individually managing access permissions across different applications and systems leads to easily exploitable security gaps and access policies that are constantly being undermined by human error.

A modern Identity solution must equip your teams with tools that centralize and simplify the provisioning and deprovisioning of access. It must also provide a comprehensive, real-time view of your organization's full spectrum of Identity threats — both in administrative time and run time, ensuring secure, seamless experiences across employees, partners, and customers.

Admin time

- Governance tools that offer a comprehensive look at access across all systems and applications, complete with granular and automation-enabled provisioning and deprovisioning features
- Posture management tools that simplify the analysis and monitoring of security vulnerabilities and customer Identities across the organization

Run time

- Privileged access management tools that offer specialized protections for highly privileged information without creating excessive friction for IT teams or end users
- Real-time threat response features that leverage automation and organization-wide risk monitoring to quickly and effectively remediate potential threats

Checklist: Can your Identity solution...

- ☐ Give you visibility into all threats across all systems, devices, and types, and customer accounts?
- ☐ Incorporate third-party signals from across your tech stack (in addition to first-party signals from your Identity provider) for comprehensive, real-time threat visibility?
- ☐ Run automated scans of all your tools and evaluate your setup against an aggregated set of Zero Trust frameworks?
- ☐ Proactively identify vulnerabilities and security gaps before they can be exploited?
- ☐ Continuously uncover critical misconfigurations and gaps, such as inconsistent MFA enforcement, account sprawl, and weak customer authentication policies?
- ☐ Automate provisioning and deprovisioning when someone moves within the org or when a customer's risk profile changes?
- ☐ Offer secure access for highly privileged information that can be customized based on the user and use case?
- ☐ Discover non-human Identities and set granular permissions for them to reduce your company's attack surface?
- ☐ Integrate with human resources software and directories for consolidated management of employee information and permissions?
- ☐ Connect with customer Identities to manage and secure customer accounts at scale?

okta

Principle #2

Powerful orchestration

Fragmented security stacks generate mountains of data concerning risks and potential threats. But without a unifying, Identity-powered tool for analyzing and acting on that data, your teams are saddled with the task of sifting through logs and piecing together a time-delayed understanding of which risks demand immediate attention. The result is a slow-moving security function that renders real-time remediation impossible.

A modern Identity solution must equip your teams with tools that prevent, detect, and swiftly remediate potential threats in real time. In addition to the comprehensive visibility described on the previous page, organizations need Identity-powered features that simplify the process of *understanding and acting* on that holistic visibility to thwart would-be attackers before they can inflict real damage.

Checklist: Can your Identity solution...

- ☐ Simplify the task of setting up automated remediation actions?
- ☐ Enable granular customization of remediation actions based on risk factors, policies, and other contextual cues?
- ☐ Trigger robust responses like universal logout to protect against potential breaches?
- ☐ Communicate constantly with your phishing-resistant authentication tools for continuous improvements to remediation strategy?
- ☐ Perform device security checks during an active session?
- ☐ Proactively block malicious IP addresses?
- ☐ Allow employees and customers to set up self-service, phishing resistant factor recovery for secure and simplified ease of use?
- ☐ Continuously detect threats after user-authentication?

okta

Principle #3

Broad & deep integrations

Your tech stack is only as powerful as it is connected. Without seamless integration between the components of your tech stack, it's impossible to fully realize the value of your technology and security investments and achieve full ROI.

A modern Identity solution must connect every component to enable new levels of risk management and efficiency. Vendor-neutral Identity platforms allow for this degree of integration — without burdening your developer and IT teams with the need for custom code.

Checklist: Can your Identity solution...

- ☐ Seamlessly integrate with your key enterprise Saas applications, e.g., your CRM, productivity, collaboration, ERP, and IT ops management apps?
- ☐ Provide deep Identity security capabilities that go beyond simple provisioning and single sign on to provide protection for those apps before, during, and after login?
- ☐ Integrate with core parts of your security stack to enhance risk monitoring, threat detection, and remediation?
- ☐ Offer developer and IT teams no-code options for easily building automation flows that trigger functions across applications?
- ☐ Leverage extensibility features that ensure continuous connectivity with additional applications and systems the organization may bring on in the future?

Outcomes of a unified security strategy

Unified, Identity-first security is more than a concept. In practice, it comprises a set of material outcomes that, together, drive measurable impacts in how your organization protects critical assets, streamlines everyday workflows, and drives higher performance across all business operations.

- Visibility into all Identity threats and real-time remediation
- Complete and reliable zero-standing/least-standing privilege
- Proven zero trust
- Better control of non-human and machine identities
- Fully realized value throughout technology and security investments

Learn more about the five main outcomes of a unified security strategy.

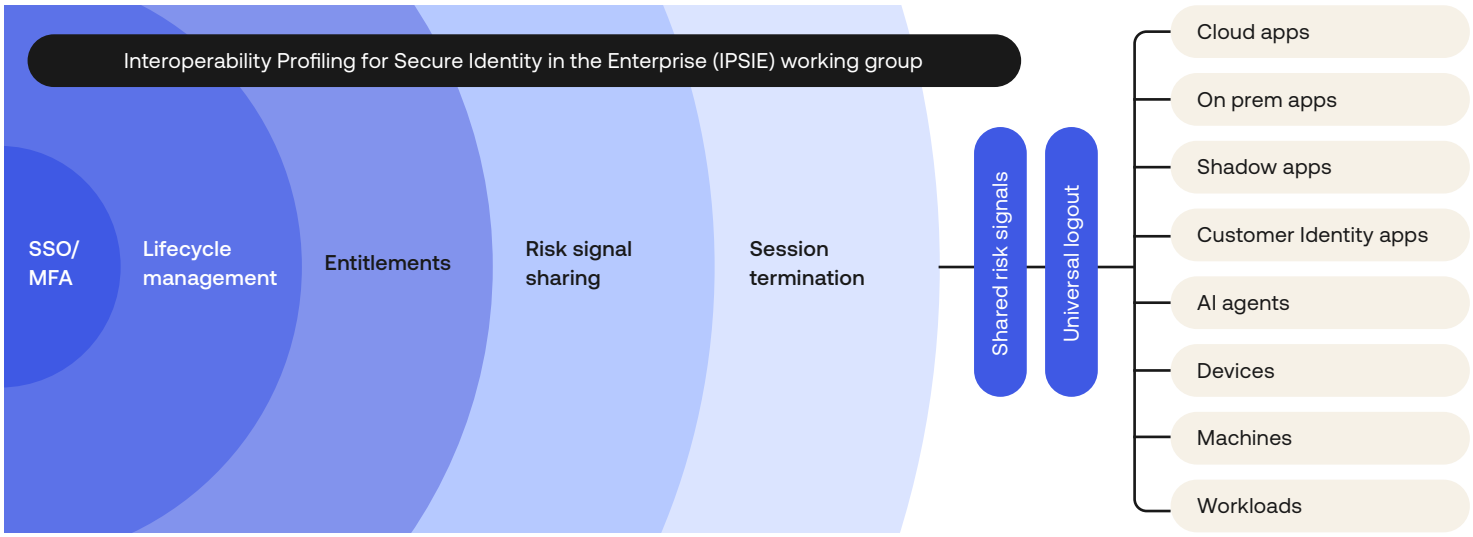
The path to Identity-first security

Fully realized, Identity-first security supports an open ecosystem that makes it easy, efficient, and secure to build and use any app, system, or tool, ensuring that they're secure and manageable by default.

No more Identity siloes. No more costly and time-consuming custom integrations. No more security gaps and blind spots across IT and customer environments. Just one high-performing tech stack that is secure by default and seamless by design.

A modern Identity security standard

The OpenID Foundation's *Interoperability Profile for Secure Identity in the Enterprise* (IPSIE for short) working group is the most recent effort dedicated to making this ideal a reality.



As the first unified Identity Security Standard, IPSIE will provide a path toward a fully integrated ecosystem that conforms to the modern landscape and puts complete control back in your hands.

How to achieve Identity maturity:

The Okta Identity Maturity Model

Modernizing your Identity and unifying your security strategy represent a heavy lift for security and IT teams. Moreover, these are not binary conditions — rather, building a modern Identity strategy must be an ongoing campaign of progressive improvement.

That's why Okta developed the Identity Maturity Model: It provides organizations in every industry a framework, informed by experts and industry benchmarking, that can help you navigate complexity and drive your organization forward with confidence.

Organizations face different challenges depending on where they are in their Identity maturity journey. The Identity Maturity Model takes this into account, providing specific guidance for every stage of the process. It's an invaluable resource when it comes to identifying priorities, measuring progress, and achieving desired business outcomes.

Secure Identity. Secure everything.

It can't be overstated: Identity is Security. To stay ahead of bad actors and set their organizations up for resilient and enduring security, security and IT leaders need to take meaningful steps toward modernizing their Identity solution and unlocking its full potential.

When you secure Identity, you secure your organization's future: You protect against the rising tide of increasingly sophisticated threats and new, AI-powered methods of attack. And you secure the competitive advantage that comes with seamless, automation-enabled security, IT, and customer environments.

To get started on your Identity maturity journey and receive targeted recommendations from Okta experts, learn more or get in touch with our team.

okta

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871