eBook

Unlock the power and potential of unified Identity

Five key outcomes for your organization

okta

The critical role of Identity

Identity is key to modern security. In today's cloud-based world, where systems and applications are deeply connected, Identity determines whether an organization's sensitive data stays safe or becomes vulnerable.

Bad actors already recognize Identity as a key target, but businesses across industries are too frequently caught unprepared. Identity-related attacks are rising at a rate of 180% year-over-year (YoY), and yet the average number of days it takes for an organization to contain a breach is 290 (Verizon 2024 Data Breach Report).

The core issue is Identity fragmentation across tech and security systems. Without a unified approach to Identity security, organizations weaken their risk mitigation efforts and overwhelm IT and security teams with inefficient tools that can't keep up with today's complex threats.

To get back on track, organizations must develop an integrated, Identity-focused security strategy. This strategy should detect risks across IT and security systems, respond with real-time remediation and prevent future attacks through centralized Identity governance and security orchestration.

A guide to future-ready Identity

This resource illustrates how organizations can build a unified Identity focused security strategy, including:

- How fragmented Identity makes risk hard to resolve
- Why the modern enterprise requires an Identity-first approach to security
- The five key outcomes of a unified security strategy

Getting security right starts with putting Identity first

The way businesses operate today looks dramatically different than five years ago. Hybrid workforces mean productivity now hinges on seamlessly connecting a decentralized network of full-time employees, contract workers, customers, and third-party partners accessing key resources and networks from around the world. Accelerated adoption of cloud services and SaaS applications facilitates these connections, making it easier to connect, collaborate, and deliver secured customer experiences in increasingly flexible ways.

But this broad shift in how we work fundamentally changes how we secure our businesses and customers. Legacy security paradigms — which tend to revolve around network perimeters and on-premise deployments — are simply not built for the era of cloud-native applications and remote collaboration. As security experts have been proclaiming for years now, the traditional concept of a security perimeter is no longer relevant.

Getting Identity right — with high visibility into who is accessing what, from where and under what conditions — is critical to ensuring both security and seamless experiences. The modern understanding of Zero Trust dictates that the concepts of trusted devices and trusted networks no longer apply. Organizations need to enable their decentralized, hybrid workforces to connect from any device, any network, anywhere, while also ensuring customers can securely access services with seamless, frictionless interactions.

Bad actors know that Identity is the new battleground in cybersecurity. Identity-related attacks are now the primary method of gaining unauthorized access to sensitive information. In 2024, an overwhelming 80% of data breaches began with stolen credentials and/or phishing attacks (Verizon 2024 Data Breach Report).

This makes Identity the core of modern security. Organizations can only achieve Zero Trust levels of threat protection — and enable seamless collaboration, secured customer experiences, and productivity — by going all-in on a full, integrated approach to Identity security.

Turning Identity into a competitive advantage

While Identity is your organization's biggest security risk, it's also your greatest opportunity. By recognizing its central role and modernizing Identity-powered functions, including Customer Identity, you can mitigate risk, outpace bad actors, and unlock key advantages. A strong Identity strategy enables faster connectivity, more agile collaboration, seamless compliance, and stronger security outcomes.

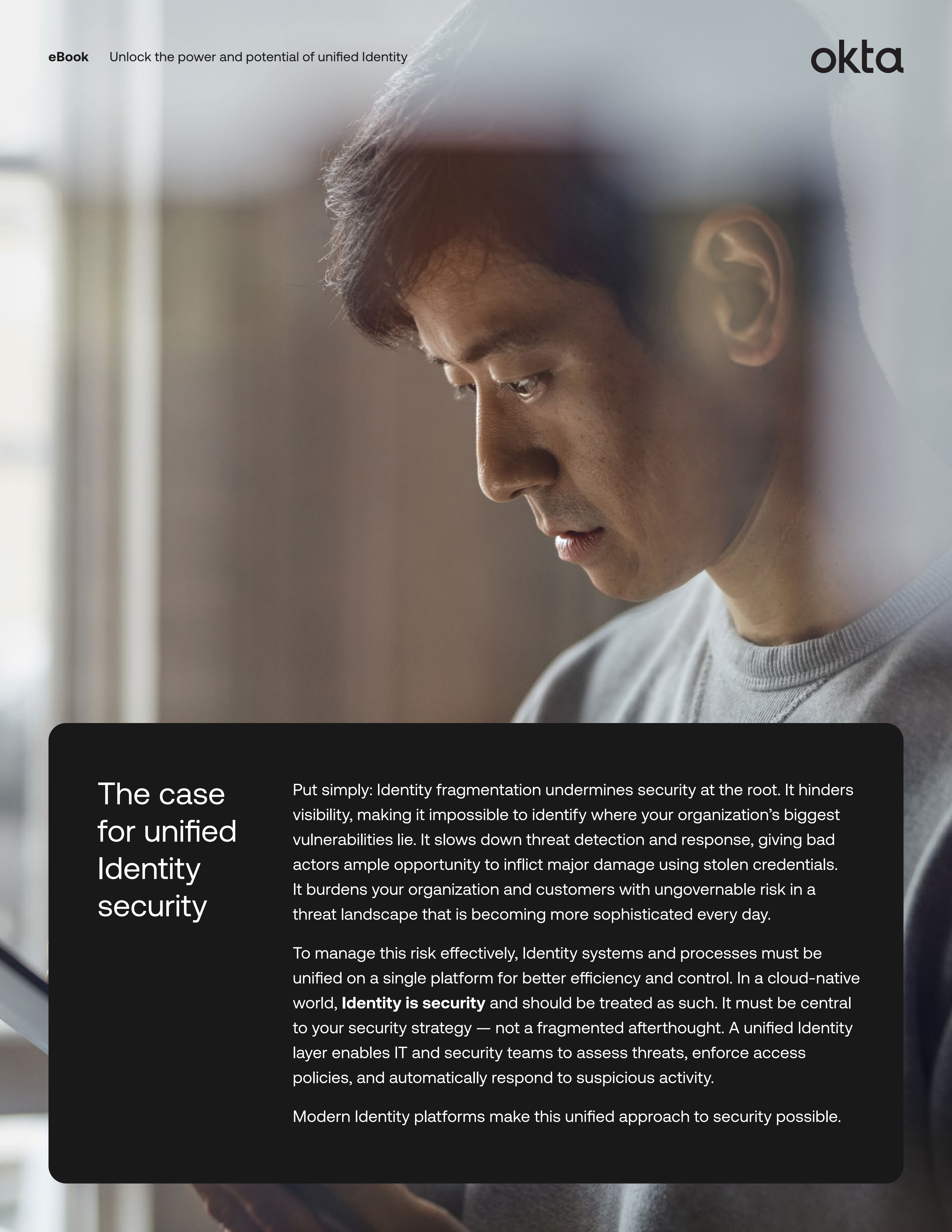
Fragmented Identity creates dangerous blind spots

The broad shift in how we work — moving toward more distributed productivity and collaboration that prioritizes speed and agility above all — has also fundamentally changed the composition and structure of security and tech stacks across virtually every industry. Gone are the days of purchasing your entire stack through one company under an enterprise license agreement (ELA). Successful organizations now depend on an ecosystem of best-of-breed solutions that support their targeted business, security, and customer experience needs. Their ability to drive growth, protect their company, and deliver seamless and secure interactions for customers depends, therefore, on their ability to *connect* those solutions and *maximize their value.*

But this best-of-breed approach creates ever-expanding tech stacks that leave IT and security teams struggling to adjust and keep up. Too often, this results in fragmented IT environments that leave core resources and Identities scattered across different systems and infrastructure.

Outcomes of fragmented Identity

- Poor visibility into the organization’s real-time security posture and individual permissions across different systems and applications
- Delayed response times that allow bad actors to turn Identity-related vulnerabilities into costly, debilitating breaches
- Cumbersome, time-consuming user permissioning practices that leave important access determinations vulnerable to human error



The case for unified Identity security

Put simply: Identity fragmentation undermines security at the root. It hinders visibility, making it impossible to identify where your organization's biggest vulnerabilities lie. It slows down threat detection and response, giving bad actors ample opportunity to inflict major damage using stolen credentials. It burdens your organization and customers with ungovernable risk in a threat landscape that is becoming more sophisticated every day.

To manage this risk effectively, Identity systems and processes must be unified on a single platform for better efficiency and control. In a cloud-native world, **Identity is security** and should be treated as such. It must be central to your security strategy — not a fragmented afterthought. A unified Identity layer enables IT and security teams to assess threats, enforce access policies, and automatically respond to suspicious activity.

Modern Identity platforms make this unified approach to security possible.

Outcomes of a unified, Identity-first security strategy

Few will argue with the need to unify and consolidate Identity systems and processes. The challenge for most organizations will be translating that from conceptual philosophy into actionable strategy.

A unified, Identity-first security strategy comprises a set of material outcomes that, together, drive measurable impact in how your organization protects critical assets, secures customer interactions, streamlines everyday workflows, and drives higher performance across all business operations.

Outcome 1: Broad visibility into Identity threats and real-time remediation

Outcome 2: Comprehensive and reliable zero-standing/least-standing privilege

Outcome 3: Proven Zero Trust

Outcome 4: Better control of non-human and machine Identities

Outcome 5: Maximize value realization throughout technology and security investments

Enabling critical outcomes with Okta

The Okta Platform enables a robust and vastly simplified approach to Identity-first security. Through a diverse suite of products and features, Okta provides end-to-end protection from sophisticated threats without burdening your workflows or customer experiences with excessive friction. And by unifying Identity orchestration, Okta enables new levels of visibility into signals and policies across your IT, security, and customer environments, arming your teams with powerful options for thwarting potential risks in real time.

Outcome 1

Broad visibility into Identity threats and real-time remediation

Fragmented technology and security stacks generate a mountain of data on risks and potential threats. This setup leaves your team sifting through logs and piecing together an understanding of what really demands attention — making real-time remediation all but impossible.

Driving faster and more effective risk remediation demands starting with a centralized, comprehensive view into your Identity risk profile — one that can synthesize and prioritize all the signals generated across your security tools into real-time, actionable insights. For organizations managing customer identities, this means detecting and addressing account takeovers, fraudulent activities, and compromised credentials in real time to safeguard both customer trust and sensitive data.

Furthermore, remediating risk cannot rely on slow, manual actions. Your Identity solution must tie real-time insights into automated remediation workflows that can be tailored to suit the specific needs of your business.

Unifying Identity security makes this possible. By unifying your security stack with a modern Identity solution, you can integrate your phishing resistance measures with a centralized, Identity-first risk engine for a comprehensive view into Identity threats as they emerge and evolve in real time. Whether protecting your workforce or customers, this level of visibility is what the current landscape demands, and is what unified Identity delivers.

Okta makes it possible

Identity Threat Protection with Okta AI

- Gain real-time visibility into threats across systems, devices, and user types, ensuring a proactive security posture
- Leverage third-party signals alongside first-party data from Okta for deeper insights and faster threat detection
- Quickly mitigate threats with customizable automated actions, such as triggering MFA or logging out compromised users

Okta FastPass

- Enable passwordless, phishing-resistant authentication for a seamless and secure user experience
- Verify device security posture during authentication to prevent unauthorized access
- Improve login security to quickly identify and respond to unusual activity
- Block untrustworthy apps before they can exploit authentication processes

Outcome 2

Comprehensive and reliable zero-standing/least-standing privilege

Establishing and enforcing least-privilege access across your organization can feel like a neverending, insurmountable challenge, especially in a fragmented Identity stack that leans heavily on manual integrations.

Modern Identity solutions equip you with the tools and capabilities to make just-in-time access into an enforceable reality. By unifying Identity Governance and Privileged Access Management, organizations can centralize visibility into who can access what and have highly granular controls over that access.

A unified Identity security solution also streamlines Identity management by consolidating governance, privileged access management, and other Identity-related functions into a single platform. This centralization helps ensure consistent access policies and strengthens the security of your organization's most critical data.

Okta makes it possible

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
- Help ensure new hires have the proper access from day one, accelerating their productivity and reducing risk
- Automate role changes and de-provisioning to maintain security

Okta Privileged Access

- Protect highly privileged information with secure access controls
- Customize access protocols to align with specific users and use cases
- Maintain high visibility into privileged activity, enabling better auditing and risk management
- Simplify access requests with user-friendly integrations that accelerate workflows without compromising security

Okta Integration Network

Okta's library of 7,000+ pre-built integrations helps you get visibility into access to virtually every component of your tech stack through one pane of glass.

Google Workspace slack

salesforce HubSpot zoom

Outcome 3

Proven Zero Trust

While most organizations long ago committed to Zero Trust principles, few are operating within a Zero Trust framework today. That's because, like enforcing least-privileged access, achieving Zero Trust with a fragmented Identity stack requires a nearly impossible tangle of manual monitoring at a pace that humans cannot sustain.

A unified approach to Identity-first security is the key to confirming (with a high level of confidence) that your organization is walking the walk of Zero Trust operations. Unifying your tech stack under a modern Identity platform makes it easy to achieve — and prove — compliance with Zero Trust principles across your technology stack. No more manually checking permissions for every user across every application and system. Unified Identity replaces this tedious (and error-prone) work with automated analysis, providing higher levels of confidence and threat protection with fewer resources.

Okta makes it possible

Identity Security Posture Management

- Run automated scans of 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 and account sprawl
- Get the confidence and confirmation of Zero Trust principles in minutes — not days or weeks

Outcome 4

Better control of non-human and machine Identities

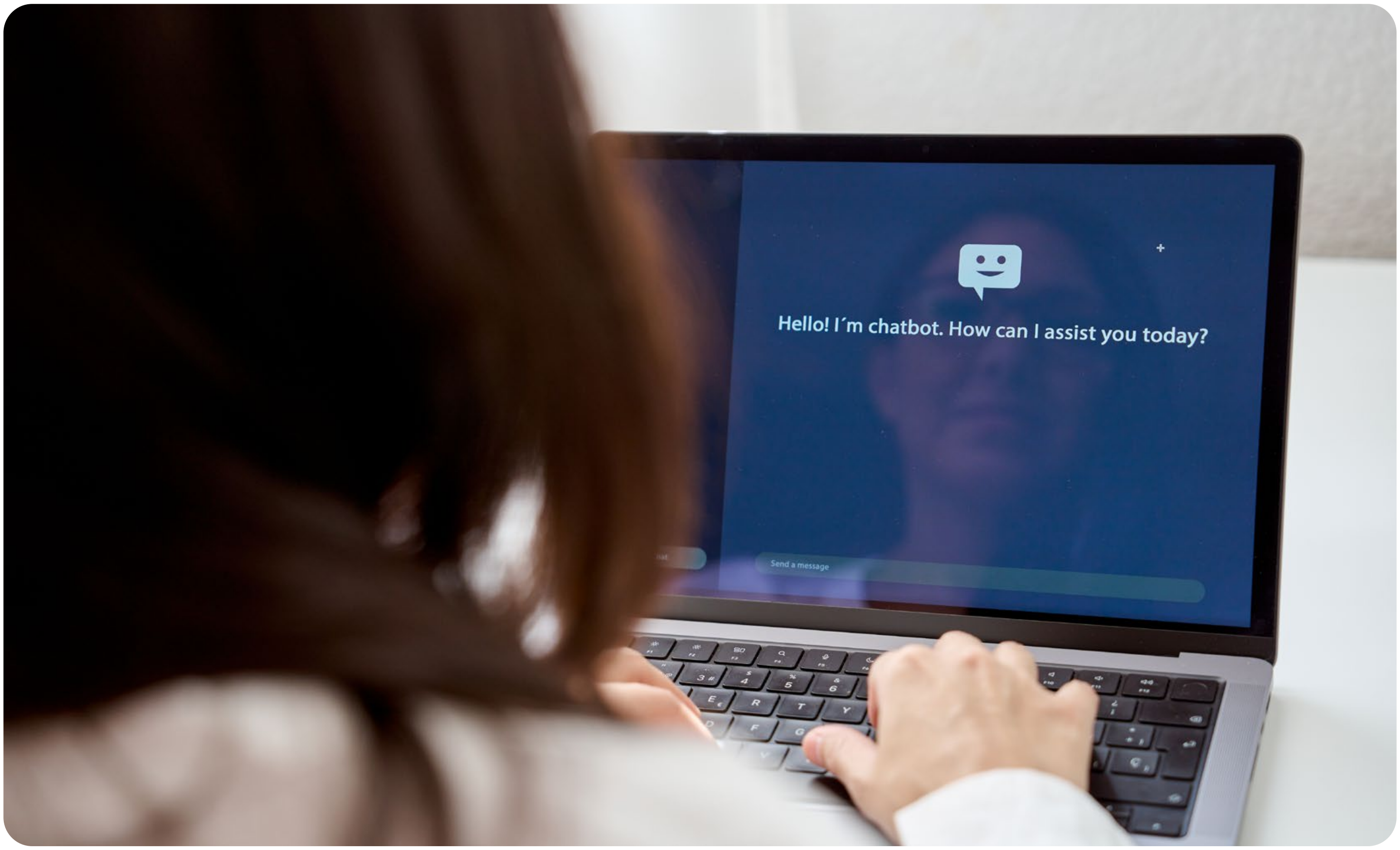
Non-human Identities — like machine-, service-, and AI-agent Identities — accelerate your business' core capacities for collaboration, innovation, and general productivity. But they also present a rapidly growing and largely unmonitored vector for bad actors to initiate a breach.

Unified Identity resolves this blind spot by giving you a comprehensive view into non-human Identities across your tech landscape — showing you where they exist and what they can access. That newfound visibility enables you to monitor their authorizations, manage their access to key resources using highly granular controls, and incorporate these non-human identities into a truly comprehensive Identity security strategy built on the principles of least-privileged access.

Okta makes it possible

Identity Security Posture Management

- Discover non-human Identities and get a centralized view of what they have access to and when
- Set more granular permissions for non-human Identities to reduce your attack surface



Outcome 5

Maximize value realization across technology and security investments

The interconnectivity of your tech stack is the medium through which those tech investments generate business value. Without broad, seamless integration between the myriad parts of your tech stack, you cannot fully realize the value of your technology and security investments.

This is especially true for your security tools: Each solution generates a wealth of data and signals, but if those signals remain siloed, you cannot support the robust and agile threat response and preparedness that today's landscape demands for both protecting sensitive internal systems and delivering secured customer experiences.

A unified, Identity-first security strategy unlocks the full potential of your extended security and tech stacks by connecting these signals to a centralized platform that continuously evaluates your security posture, manages access across applications and systems, safeguards customer identities, and determines automatic remediation strategies.

Success stories

HubSpot

Hubspot

80% of access-request tickets now resolved via automation

Delivery Hero

Delivery Hero

28,800 hours of productivity gained by eliminating outages

TAKEDA ID

TakedaID

5x faster to deploy Identity with Okta than with an in-house solution

Identity-powered solutions for your present needs and your future goals

These five outcomes are more than slick-sounding soundbites for your organization's security handbook. They are key determinants of your organization's security and success. In a risk landscape defined by increasingly sophisticated threats and new, AI-powered methods of attack, the surest approach to a resilient and secure organizational future is a unified, Identity-first approach to security.

Why? Because Identity *is* security. It's the core of any modern strategy for keeping your organization secure. But fulfilling this promise of better security depends on eliminating the Identity fragmentation that allows risk (and business value) to fall through the gaps. In today's landscape, unified, Identity-first security not only helps businesses stay ahead of accelerating threats, it also supports the seamless and frictionless IT environments required to maintain a competitive edge.

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.

okta

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