okta

Unify Identity to get foundational security right.

Waiting for the moment of the attack is too late.

The vast majority of breaches stem from some form of credential abuse, making the task of reliably authenticating Identity a core concern for security leaders in every industry. The stakes of this responsibility are widely understood. The average cost of a data breach in 2023 was a staggering $4.45 million[1] and the fear of this type of outcome is palpable in boardrooms around the world.

But too often, security and IT leaders limit their focus exclusively to the act of authentication. This constrains their window of opportunity for thwarting would-be attackers to the enforcement of authentication policies *at the moment of the attack*. And while enforcement is obviously a central part of any robust security strategy, security leaders must take action *before* and *after* authentication to mitigate damage, prevent breaches, and blunt their impact.

To provide their organizations with the strongest possible defense against sophisticated threats, security leaders need to adopt a more holistic approach to Identity-powered security—one that mitigates threats before, during, and after authentication.

Pre-Authentication

Strengthening your security posture begins with minimizing vulnerabilities and reducing the attack surface.

Discover **Determine**

Authentication

Authentication policy is only as powerful as your methods for enforcing that policy at the moment of attack.

Enforce

Post-Authentication

When a potential breach becomes a concrete threat, the speed and efficacy of your response matters.

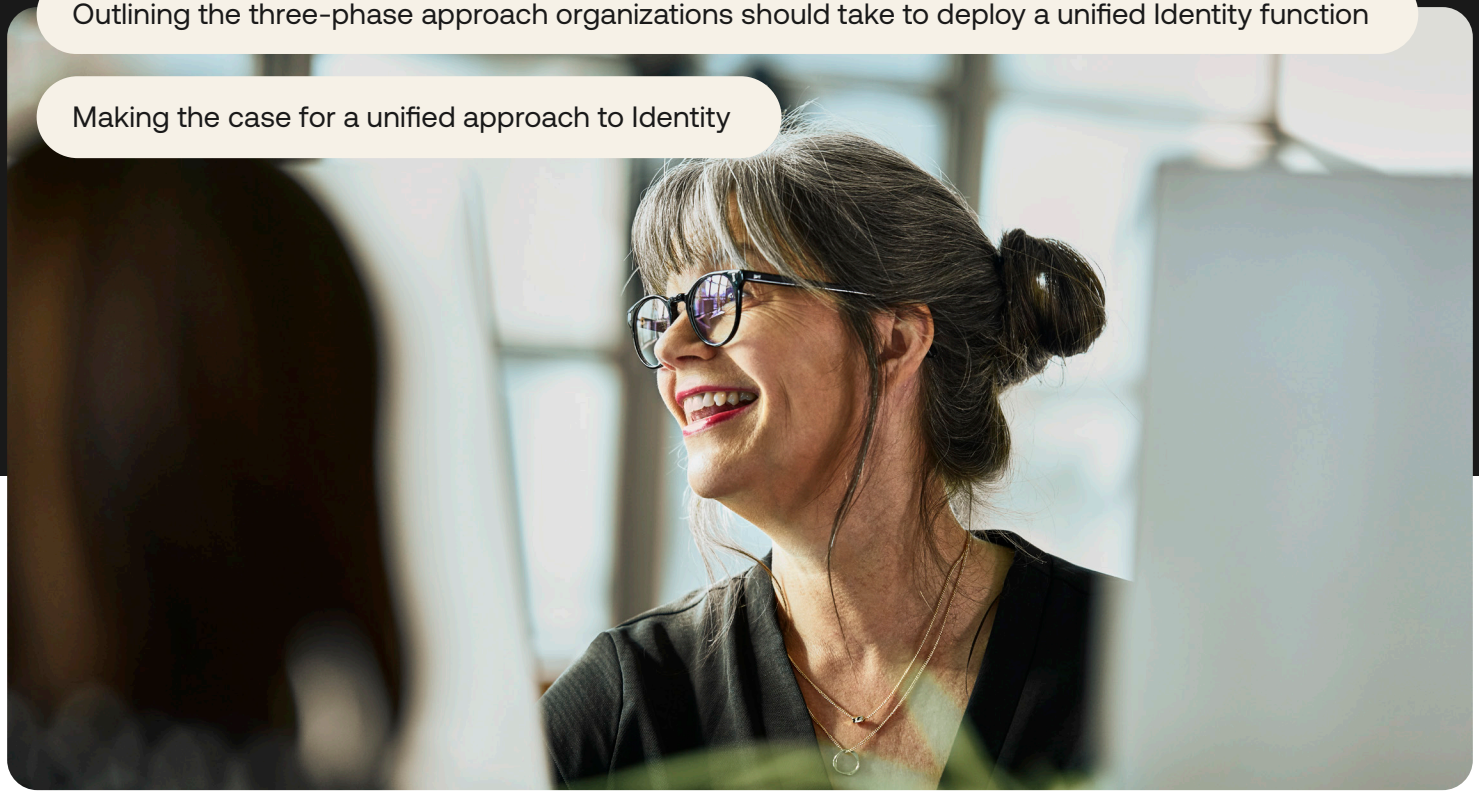
Detect **Respond**

[1] IBM: Cost of a Data Breach Report 2024

okta

This resource charts a path forward by:

- Showing how modern, cloud-based IAM software can support unified Identity
- Outlining the three-phase approach organizations should take to deploy a unified Identity function
- Making the case for a unified approach to Identity



Why Change: The need for a unified solution.

To cover the full breadth of Identity-related security functions their company requires, some organizations employ a network of individual point solutions that each address a different function. For example, they may use one IdP for governance, another for MFA and SSO, and yet another for breach detection.

The problem with this approach is that it adds more complexity and operational friction to the task of keeping data and resources safe. Far from insulating the organization from threat, the distributed authority and information silos inherent to these legacy solutions actually multiply the number of vulnerabilities bad actors can exploit.

A unified approach to Identity minimizes vulnerabilities by delivering a comprehensive, intuitive, and secure means of tackling pre-authentication, authentication, and post-authentication security priorities:

- **Discovering** users, resources, and potential vulnerabilities
- **Determining** secure-by-design access controls and policies
- **Enforcing** least-privileged access
- **Detecting** potential threats quickly
- **Responding** to potential threats immediately

Three phases of stronger Identity security.

When it comes to fortifying your organization's Identity posture, the stakes are simply too high to settle for fragmented Identity solutions that undermine security and leave you open to the worst impacts of cyber-attacks. A unified approach to Identity provides fully integrated insights and automation tools that help proactively mitigate risk, enforce secure-by-design access, and respond to potential threats with speed.

Before Authentication: Discover

Strong risk management begins with a full awareness of where the risk is coming from and what vulnerabilities it might exploit. A unified approach to Identity gives security and IT teams:

- Holistic visibility and control of the organization's Identity posture, which enables a stronger and more timely strategic approach to risk management.
- The ability to incorporate third-party risk signals into continuous monitoring efforts, fueling a more up-to-date set of data concerning potential threat signals.
- Simplified integration with other components of the tech and security stack, including Identity stores, apps resources, etc., which eliminates information silos and exposes misconfigurations that need to be addressed.
- Strengthened security and ease of use.

Before Authentication: Determine

Once vulnerabilities are brought to the surface, the right Identity solution should make the process of determining different levels of access simple. A unified approach to Identity allows security and IT teams to:

- Determine secure-by-design access controls and policies for strong authentication, privileged access, and governance across the entire workforce and tech stack.
- Maintain a least-privilege standard for all users, preventing accidental misconfigurations that grant inappropriate levels of access.
- Configure privileged access from a unified source of truth.
- Eliminate information silos and inappropriate access resulting from reliance on different point solutions that don't integrate (or don't integrate well).

okta

During Authentication: Enforce

Strong enforcement of access policy begins with the right authentication factors and the right governance tools. A unified approach to Identity gives security and IT teams:

- Phishing-resistant authentication factors capable of mitigating the impact of different types of potential breaches (e.g., phishing attacks, session theft, unauthorized local activity) across operating systems and devices. This includes secure options like MFA and SSO and, in especially sensitive cases, biometric options.
- Automated provisioning and deprovisioning features that ensure appropriate changes in access when someone joins, leaves, or moves within the organization.
- The ability to implement time-bound access requests for sensitive permissions and critical infrastructure.
- A robust means of enforcing best security practices for shared privileged accounts with features like password vaulting and transactional phishing-resistant MFA factors.

After Authentication: Detect

Strong threat mitigation begins with a robust means of detecting and evaluating threats across the entirety of the organization's security infrastructure. A unified approach to Identity gives security and IT teams:

- A full toolkit that leverages first- and third-party signals to continuously evaluate risk throughout the organization and flag potential Identity-related threats as they emerge.
- AI-powered risk scores (generated from risk signals across different tools and systems) that determine the Identity health of individual users and the organizational environment at large.
- Real-time analysis of at-risk users, access violations, and potential misconfigurations that could lead to vulnerabilities.

After Authentication: Respond

Once a potential threat has been detected, security leaders need an automation-powered response strategy capable of stopping potential breaches in their tracks. A unified approach to Identity gives security and IT teams:

- Risk-based automation across users, applications, and devices that can make instantaneous, contextual decisions about terminating access.
- The option to universally log out users based on risk signals.
- Step-up MFA options that correlate to elevated risk.
- Streamlined, automated SecOps response measures, including access reviews.

okta

Unifying Identity with Okta

Organizations need a modern Identity solution that delivers a robust defense against phishing attacks while also granting employees secure, privileged access to key information. And in a landscape defined more and more by third-party relationships and part-time, contract, and remote employees, this Identity solution must also include a means of granting targeted, secure temporary access to specific systems and resources.

Okta elevates Identity and Access Management (IAM) across the spectrum of posture, access, governance, and privileged access by centralizing and tightly integrating every aspect of identity. By connecting seamlessly to your existing IdPs and SaaS apps, Okta addresses pre-authentication security concerns through a suite of products that deliver a holistic, intuitive view of your organization's Identity security posture.

Ready to discuss a solution made for your organization's needs?

Start a conversation with us today.

Okta Identity Security Posture Management (ISPM) gathers and analyzes industry threat intelligence in order to provide security leadership with the most comprehensive picture possible of the organization's Identity posture.

Learn more

Okta Single Sign-On and Adaptive Multi-Factor Authentication help security leaders enforce least-privilege access and protect against phishing attacks through an adaptable and powerful suite of features like phishing-resistant login, simplified time-bound access, and risk-based enforcement based on contextual information.

Learn more

Okta Identity Threat Protection (ITP) integrates insights from across your security ecosystem to elevate threat visibility and deepen your understanding of your organization's threat surface, using continuous monitoring, intelligent reporting, and information pulled from an organization's security stack.

Learn more