okta

How to protect your organization from Identity-based attacks

Identity-based attacks

Identity is foundational to a modern security strategy. Organizations with gaps in their Identity security are significantly more at risk of experiencing a compromise or breach.

86%	Of web app breaches involve the use of stolen credentials [1]
74%	Of breaches involved the human element, which includes errors or misuse [1]
+150%	Annual growth of phishing attacks since 2019 [2]

If attackers get control of a worker's Identity, they can break into a network, move laterally, facilitate fraud, and extract sensitive data. These actions can compromise a brand's reputation and customer loyalty overnight.

Examples of Identity-based attacks include

- Password spray
- Credential stuffing
- Adversary-in-the middle (AiTM)
- Account takeover (ATO)
- Business email compromise (BEC)
- Phishing
- Spear phishing
- Push notification abuse

A strong Identity security strategy fortifies your security posture and should provide not only protection, but also detection and response, for today's Identity-based threats.

[1] 2023 Verizon Data Breach Investigations Report
[2] APWG Phishing Trends Activity Report, Q4 2022

okta

Protection

The best offense is a good defense

Actions to take	Benefits
Deploy phishing-resistant multi-factor authentication (MFA)	• Prevent access to valuable resources even when a bad actor has a username or password • Automatically prompt for an additional factor — that the bad actor does not have access to — when necessary
Enable passwordless authentication	• Eliminate a significant threat vector for your organization • Strengthen your security posture with higher assurance factors with no shared secrets • Reduce the strain on security teams caused by password resets and other workflows
Automate Identity lifecycle	• Ensure the right person has the right level of access at the right time with automatic provisioning and deprovisioning • Reduce the attack surface and mitigate lateral movement within your environment in the event that a bad actor or malicious internal user gains access to systems
Enforce access policies	• Unify access policies across all resources (e.g., applications, APIs, servers, and more) • Centralize access management for all users (e.g., employees, partners, and contractors)

okta

Detection

You can't stop what you can't see — or predict

Actions to take	Benefits
Deploy risk-based access management	• Stop threats in their tracks by automatically detecting suspicious behavior patterns
Ensure Identity visibility across the technology ecosystem	• Understand which users have access to which resources at any given time – even as the number of apps and services continues to rise and user ecosystems constantly fluctuate
Notify users about unusual security events	• Turn users into your most powerful asset by empowering them to flag strange behavior / logins
Leverage Identity-based detections for use by your security operations team	• Quickly alert the SOC to compromised user accounts or credential misuse. Having identity-specific detection rules enables SOC to get ahead of threats that leverage stolen credentials or account takeover for faster containment • Enable faster correlation of identity events with other security alerts to identify broader attack narratives. Identity threats rarely happen in isolation - they are part of larger campaigns

okta

Response

Quickly mitigate and strengthen your security posture

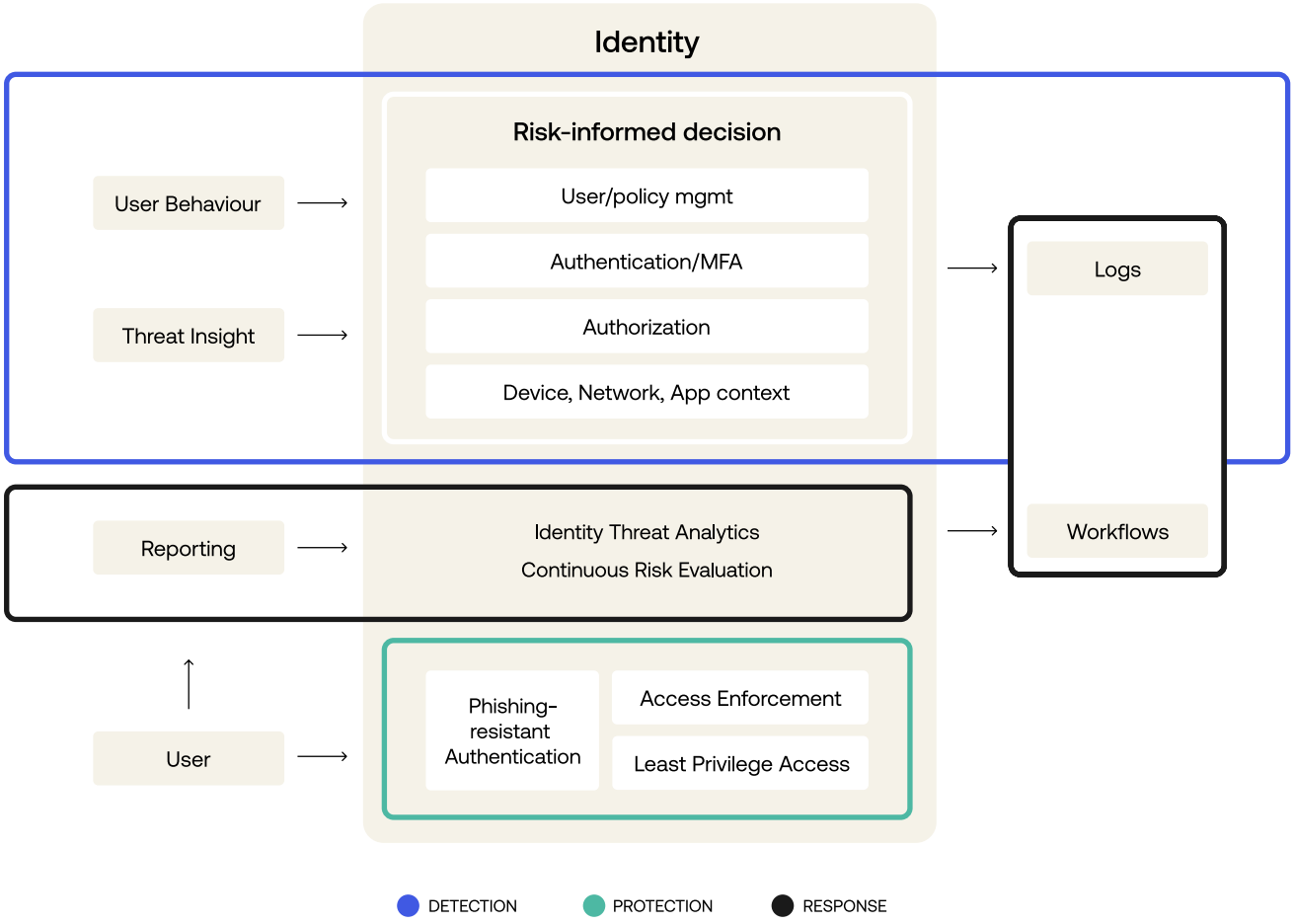
Actions to take	Benefits
Identify Identity-specific triggers for response	• Stop bad actors in their tracks by quickly suspending compromised accounts • Mitigate additional risk by blocking malicious activity
Automate remediation actions	• Automate response to common Identity-based scenarios and attacks, improving team efficiency • Strengthen security posture across your entire security stack by leveraging third-party integrations and data feeds
Analyze security logs	• Understand incidents and inform future security decisions with end-to-end visibility of the authentication journey

How Okta can help

A comprehensive Identity solution is the cornerstone of a modern security strategy. Okta can help safeguard your organization with protection, detection, and response for today's Identity-based threats.

Our vision is to deliver a secure, scalable, and compliance-based access experience that fully supports your business goals today, and into the future.

Engage with our Identity Assessment Tool to see what steps you can take immediately to strengthen your Identity security: https://www.okta.com/zero-trust-assessment/#homepage



About Okta

Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology—anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com.