

How to Protect Your Organization from Identity-Based Attacks

Identity-based Attacks

Many organizations understand that there's a link between identity and security, but few fully grasp how foundational identity is to a modern security strategy. Organizations with gaps in their identity security are significantly more at risk of experiencing a compromise or breach.



Source: <https://www.verizon.com/business/resources/reports/dbir/>

If attackers get control of the right identity, they can break into a network, move laterally once inside, facilitate fraud, and extract sensitive data. Not to mention they can compromise a brand's reputation and customer loyalty overnight.

Types of identity-based attacks

- Password spray
- Man-in-the middle (MITM)
- Account takeover (ATO)
- Business email compromise (BEC)
- Phishing
- Spear phishing
- Credential stuffing
- Brute force

A strong identity security strategy is needed to fortify your security posture. The right identity solution provides protection, detection, and response for today's identity-based threats.



Protection

The best offense is a good defense

Actions to take

Deploy multi-factor authentication (MFA)

Enable passwordless authentication

Automate identity lifecycle

Enforce access policies

Benefits

- 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
- Eliminate a significant threat vector for your organization (passwords!)
- Strengthen security posture with higher assurance factors such as push tokens and biometric-based logins
- Reduce additional strain placed on your security team caused by password resets and other workflows
- Ensure the right person has the right level of access at the right time with automatic provisioning and deprovisioning
- Reduce your attack surface and mitigate lateral movement within your environment in the event that a bad actor or malicious internal user gains access to your systems
- Enable IT and security teams to oversee and unify access policies across all resources (applications, APIs, servers, and more)
- Centralize access management for all users (employees, partners, and contractors)



Detection

You can't stop what you can't see

Actions to take

Deploy risk-based access management

Ensure identity visibility across the technology ecosystem

Leverage identity-based detections for use by your security operations team

Benefits

- Take immediate action to stop threats in their tracks by automatically detecting suspicious behavior patterns
- 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
- Proactively detect potential identity-based threats across your environment





Response

Quickly mitigate and strengthen your security posture

Actions to take

Identify identity-specific triggers for response

Automate remediation actions

Analyze security logs

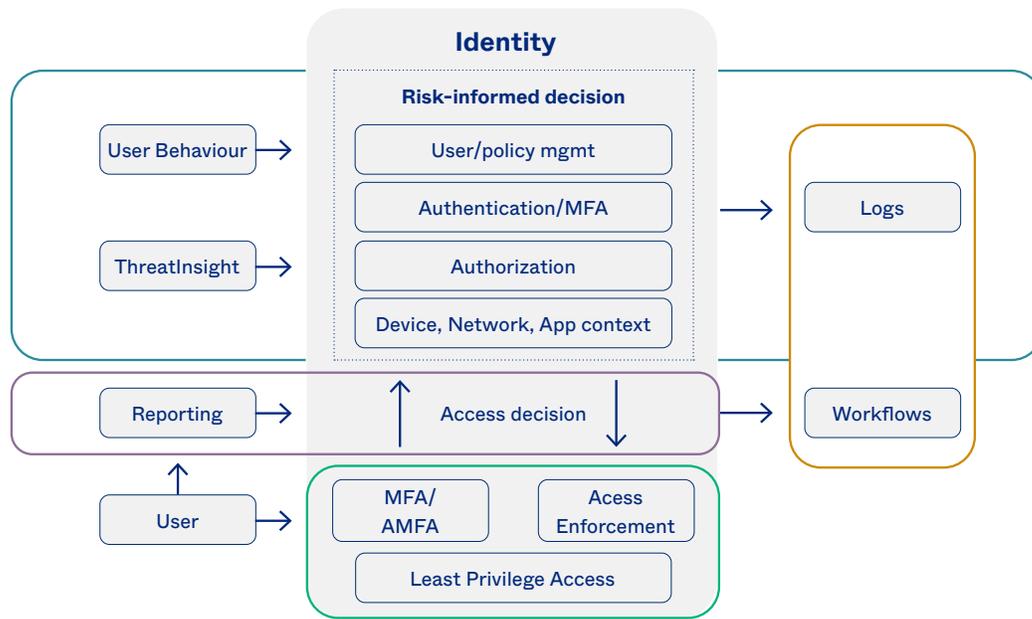
Benefits

- Stop bad actors in their tracks by quickly suspending compromised accounts
- Mitigate additional risk by blocking any malicious activity
- Automate the response against common identity-based scenarios and attacks to enable your team to be more efficient
- Strengthen your security posture across your entire security stack by leveraging 3rd-party integrations and data feeds
- 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.



Detection Protection Mitigation Response

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>