



Identity security posture: The must-have checklist for attack readiness

14 questions to help protect your organization
from identity-based cyber attacks

The adversary doesn't care about your firewall; they care about your credentials. Attackers are exploiting session tokens, bypassing weak MFA via AiTM proxies, and weaponizing Non-Human Identities (NHIs) like dormant service accounts to pivot undetected.

Use this checklist to audit your defense capabilities against the modern threat landscape.

Please note that this checklist is intended only as a component of your overall security program.



Pre-attack: Proactive posture management

This section focuses on eliminating misconfigurations and reducing the identity attack surface before an attack occurs.

1. Do you continuously validate the identity security posture for both human and non-human identities (e.g., service accounts, API keys)?
2. Can you automatically enforce least privilege and validate that there are no MFA bypasses?
3. Do you have a process to identify stale or partially off-boarded accounts that still have active access?
4. Is there a system to prioritize and remediate identity misconfigurations and excessive permissions to minimize the potential blast radius of a breach?
5. Do you use an "identity lens" to get a holistic view of who has access to what resources and how they authenticate, covering gaps left by CSPM and SSPM tools?

Identity Security Posture Management

Continuously discover and remediate identity risks and misconfigurations.



During attack: Continuous threat detection and response

This section covers the capabilities needed to detect and respond to threats in real-time as they happen.

6. Have you implemented phishing-resistant authentication (e.g., Okta FastPass) to protect users against phishing attacks?
7. Do you continuously monitor session activity and user behavior after initial authentication to detect anomalies and potential lateral movement?
8. Can you automate inline responses to contain incidents, such as performing a universal logout across apps and devices, enforcing step-up MFA, or triggering custom workflows?
9. Do you have AI-driven bot protection that can detect and mitigate automated attacks without requiring user input like traditional CAPTCHA?
10. Does your system continuously assess risk levels and user and device context to dynamically evaluate and enforce security policies throughout a session?

Identity Threat Protection

Automatically detect and respond to identity-based threats in real time.

Okta Device Access

Secure device login that hardens protection and simplifies resource access.

Okta FastPass

Gain Zero Trust security with phishing-resistant, passwordless authentication.



Post-attack: Strengthen identity resilience

This section focuses on improving security posture and response after an incident has occurred.

11. Do you have tools for incident observability and forensics that can uncover the complete identity attack path?
12. Is there a system to improve incident handling by using identity event correlation and shared intelligence across security tools?
13. Can you provide compliance assurance by mapping identity controls to common frameworks (e.g., NIST)?
14. Do you have a continuous feedback loop to analyze security events and fine-tune responses over time?

Okta Recognized as an Overall Leader in the 2025 KuppingerCole Leadership Compass for ITDR.

[Read more here](#)

Okta makes it possible

Regardless of where you sit on the spectrum of attack readiness, Okta provides the end-to-end visibility and real-time response capabilities necessary to secure your organization before, during, and after an incident.

With visibility into 10 billion global logins and 2 billion blocked threats monthly, Okta sees the TTPs (Tactics, Techniques, and Procedures) others miss. By unifying signals across your entire ecosystem, Okta enables you to move from reactive defense to proactive resilience—eliminating misconfigurations, stopping phishing in its tracks, and automating inline responses to contain threats instantly.

Take the next step: Turn your identity layer into your strongest security asset.

About Okta

Okta, Inc. is The World's Identity Company™. We secure Identity, so everyone is free to safely use any technology. Our customer and workforce solutions empower businesses and developers to use the power of Identity to drive security, efficiencies, and success — all while protecting their users, employees, and partners. Learn why the world's leading brands trust Okta for authentication, authorization, and more at okta.com.