okta

Identity Security Checklist

40 questions to help protect your organization from Identity-based cyber attacks

Security breaches over the last year have clearly shown that Identity is a significant attack vector for cyber criminals and nation-state threat actors. More than being a simple login box, Identity is the first and last line of defense for companies' most sensitive data and infrastructure. Identity is security.

Okta is at the forefront of helping our customers and the industry in the fight against Identity-based attacks.

We support over 10 billion logins globally and protect 18,000+ customers against more than 2 billion malicious requests in a month. As an industry leader, we are committed to sharing best practices like this checklist to help our customers assess and adopt the strongest possible Identity security posture. Please note that this checklist is intended only as a component of your overall security program.

okta

Unified Identity Security and Zero Trust

Foundational

1. Does your Identity Security solution contribute to a ***holistic cybersecurity strategy*** encompassing Identity and Access Management, incident response, risk management, and continuous improvement initiatives?
2. Do you have measures in place to ***authenticate and authorize users, devices, and applications*** dynamically based on the context of the access request?
3. Are there established processes for ***approving, reviewing and updating privileged access***?
4. Do you implement ***least-privilege access*** within your Identity Security solution to minimize potential attack surfaces? In particular, do you minimize or remove admin rights wherever possible?

Advanced

5. Is there a robust strategy to ***continuously monitor and assess user and device behavior*** to detect anomalous or suspicious activities?
6. Do you ***constrain the permissions of IT support staff*** in ways that prevent them from performing operations on highly privileged accounts? For example, do you create and assign custom administrator roles for these users?
7. Do you have mechanisms in place for ***strong help desk Identity verification for privileged users***, such as using visual verification?
8. Do you have measures in place to ***continuously verify*** the Identity of users throughout their interactions within your most critical resources?
9. Do you require ***zero trust security from your third parties who access your IT environment***? In particular, do you verify and audit the posture of these third parties, as opposed to implicitly trusting their ability to maintain their network perimeter?

Identity and Access Management

Foundational

10. Have you implemented ***phishing-resistant Multi Factor Authentication*** for access to all sensitive resources?
11. Do you ***extend phishing resistance across the complete employee lifecycle*** from enrollment/onboarding through to recovery?
12. Do you require ***step-up authentication*** when administrators perform sensitive actions?
13. Do you automatically ***alert users on high risk events - such as when all MFA factors are reset*** for an account or when an account is accessed using a new device?
14. Is there ***automation in Identity lifecycle management***, including onboarding, offboarding, and access reviews, to ensure accuracy and efficiency?
15. What criteria ***define an Identity account as dormant*** in your organization? How frequently do you conduct dormant account reviews?
16. Do you have a strategy for service account credentials - such as ***periodically rotating passwords or rotating passwords after every interactive access***?
17. Do you have an ***Identity governance strategy***, and how does it align with industry standards and best practices?
18. Do you have mechanisms in place for ***periodic attestation and certification of user access*** rights?
19. Do you have mechanisms in place to ensure secure and seamless access to resources for remote users on both ***corporate and personal devices*** (both laptop and mobile)?

Advanced

20. Does your Identity governance solution enforce ***segregation of duties*** to prevent toxic combinations of access?
21. Are privileged accounts fortified with robust ***multi-factor phishing-resistant authentication*** measures to ensure an elevated level of security?
22. Has a ***comprehensive Privileged Access Management*** (PAM) solution been deployed to discover, secure, record and monitor privileged accounts?
23. Do you require that ***third parties who access your IT environment authenticate via IAM*** solutions for all workplace applications?
24. Do you ***apply IP binding to authenticate users to critical resources***? Are administrators able to automatically revoke an administrative session if the IP address observed during an API or web request differs from the IP address recorded when the session was established?
25. Do you ***block requests to your Identity solution by network type*** (e.g. anonymizing proxies)?

okta

Strategies for Remediation and Mitigation

Foundational

26. What existing methods and tools do you have to help ***increase the monitoring of privileged accounts***?
27. How is ***User Behavior Analytics*** integrated into the overall Identity security strategy for detection and response capabilities?
28. Do you have ***automatic alerts*** when changes are made to your on-premise AD agents?
29. Does your Identity platform support an "***infrastructure-as-code***" approach to building and maintaining systems?
30. Can your Identity solution recognize requests from known devices, to ***prevent account lockouts*** during brute force attacks?

Advanced

31. Can you ***enforce location-based restrictions*** for both user and machine-to-machine access?
32. Do you ***allow admins to detect and block requests from an anonymizer*** based on an evaluation of whether an IP address is associated with an anonymizer's address?
33. Do you ***enforce token binding for machine-to-machine (M2M) integrations*** using proof of possession to ensure that only authenticated applications can use tokens to access APIs?
34. Do you ***leverage enhanced bot detection and protection*** using third-party scores and edge-based component signals?
35. When building applications, do you ***implement session management control and enhanced token security***? In particular, do you build your own session control dashboards to tailor the user experience?

Employee Training and Awareness

Foundational

36. Do you frequently conduct ***regular phishing-awareness training***, and general cybersecurity training sessions for employees to educate them on the latest security threats and best practices?
37. Are employees informed and educated about the implementation and benefits of strong password policies and ***passwordless authentication*** options?
38. Do you conduct ***simulated phishing exercises*** to test employees' resilience to phishing attempts and provide targeted training for those who may be victims of such attacks?
39. Is there a ***mechanism for employees to report security concerns*** or seek clarification on security-related matters?
40. Have employees been educated on the ***importance of keeping software and devices up to date*** with the latest security patches?