Datasheet February 2024

Identity Security Checklist

40 questions to help protect your organization from Identity-based cyberattacks

Security breaches over the last year have clearly shown that Identity is a significant attack vector for cybercriminals 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.

The data supporting this is irrefutable. Credential reuse has become a rampant problem, with 86% of web application breaches stemming from compromised credentials.[1] According to our 2023 State of Secure Identity Report, we found that over half of our Customer Identity Cloud customer applications have experienced at least one attack using breached or leaked credentials.[2] Furthermore, bypassing MFA continues to be a focus of threat actors, as the cost of executing social engineering continues to drop. 12.7% of MFA attempts on our platform met the criteria of an MFA bypass attempt.[2]

All this data makes one thing evident – 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 adopt the strongest possible Identity security posture. Please note that this is general advice; your organization will know best.

[1] *Verizon 2023 Data Breach Investigations Report*

[2] *Okta State of Secure Identity Report 2023*

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 ***regularly reviewing and updating admin roles?***
4. Do you implement ***least-privilege access*** within your Identity Security solution to minimize potential attack surfaces? In particular, do you remove admin rights wherever possible?

Advanced

1. Is there a robust strategy to ***continuously monitor and assess user and device behavior*** to detect anomalous or suspicious activities that may indicate a threat?
2. Do you ***constrain the permissions of IT support staff*** in ways that prevent them from performing operations on highly privileged users? For example, do you create and assign custom administrator roles for these users?
3. Do you have measures in place to ***continuously verify*** the Identity of users throughout their interactions within your most critical resources?
4. Do you require ***zero trust security from your sub-processors?*** 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

1. Have you implemented Multi-Factor Authentication (MFA) for all and ***phishing-resistant MFA for privileged accounts***?
2. Do you require ***step-up authentication*** for protected actions?
3. Do you ***extend phishing resistance across the complete employee lifecycle*** from enrollment/onboarding through to recovery?
4. Do you automatically ***alert users when all MFA factors are reset*** for an account?
5. Do you have an ***Identity governance strategy***, and how does it align with industry standards and best practices?
6. Is there ***automation in Identity lifecycle management***, including onboarding, offboarding, and access reviews, to ensure accuracy and efficiency?
7. What criteria ***define an Identity account as dormant*** in your organization? How frequently do you conduct dormant account reviews?
8. Are you ***actively rotating passwords*** for all service accounts?

Advanced

1. Does your Identity governance solution enforce the ***segregation of duties*** to prevent conflicts that could lead to security vulnerabilities?
2. Do you have mechanisms in place for ***periodic attestation and certification of user access*** rights?
3. Are privileged accounts fortified with robust ***multi-factor phishing-resistant authentication*** measures to ensure an elevated level of security?
4. Has a comprehensive ***Privileged Access Management (PAM)*** solution been deployed to exercise precise control and continuous monitoring over access to vital systems and data?
5. Do you ***require that support contractors authenticate via IAM solutions*** for all workplace applications, and not only those applications used directly for the provision of customer support?
6. 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?

Strategies for Remediation and Mitigation

Foundational

1. What existing methods and tools do you have to help ***increase the monitoring of privileged accounts***?
2. How is ***User Behavior Analytics*** integrated into the overall Identity security strategy for detection and response capabilities?
3. Do you have ***automatic alerts*** when changes are made to your on-premise AD agents?
4. Do you use ***API tokens when making API calls*** with automation tools, or with Infrastructure as Code tools such as Terraform?
5. Do you ***prevent account lockout for legitimate users***, by blocking suspicious sign-in attempts from unknown devices so that legitimate users are not locked out if an unknown causes a lockout?
6. 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

1. Do you ***enforce a list of allowed network zones for APIs*** to restrict attackers and malware from stealing SSWS tokens, and from replaying them outside of the specified IP range in order to gain unauthorized access?
2. 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?
3. 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?
4. Do you ***leverage enhanced bot detection*** and protection using third-party scores and edge-based component signals?
5. Do you ***extend session management*** control and enhance token security? In particular, do you provide customers with full programmatic control of sessions so they can build their own session control dashboards and tailor their users' experience?

Employee Training and Awareness

Foundational

1. 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?
2. Are employees informed and educated about the implementation and benefits of strong password policies and ***passwordless authentication*** options?
3. 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?
4. Is there a ***mechanism for employees to report security concerns*** or seek clarification on security-related matters?
5. Are employees informed about the threat of having personal email accounts as part of a ***password recovery flow***? Do they know that threat actors view personal email accounts as the weakest link in your authentication?

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.