Whitepaper

Anatomy of identity based attacks

How to protect against threats related to your users

Contents

2 Identity's role in security

3 Phishing

6 End-user device compromise

7 Insider threats

9 Post-authentication threats

11 Brute force attacks

13 Summary

Identity's role in security

Traditionally, Identity's job as part of an organizational security strategy was limited to verifying valid users at the point of authentication and granting appropriate access. However, as attackers increasingly targeted users and their credentials, Identity and Access Management (IAM) systems expanded their security capabilities to help protect against these threats. Identity has also come to the forefront for security leaders undertaking a Zero Trust strategy to fortify their defenses.

Now, Identity is becoming a key element in an organization's cybersecurity strategy. With remote work, unmanaged devices, and cloud and SaaS environments, Identity is the only common thread that connects people to the devices, apps, and resources needed to do their jobs. Identity providers are leveraging those connections.

As the only technology universally integrated across IT, Identity is uniquely positioned to foster a more collaborative approach to IT security. Okta Workforce Identity Cloud is leveraging its security controls and those of other systems to help you assess risk, repel threats, and improve cybersecurity posture. This Identity-powered approach to security:

- Unifies and strengthens Identity policy, visibility, and control with a converged IAM, Identity Governance and Administration (IGA) and Privileged Access Management (PAM) platform
- Helps detect risks that may threaten the organization, either on its own or working with your existing security products
- Continuously assesses risk before, during, and after user authentication
- Adaptively responds to threats based on real-time information

This paper will look at the following growing threats impacting organizations today, and how Okta can play a role in threat protection, detection, and response, before, during, and after the point of authentication.

- Phishing
- End-user device compromise
- Insider threats
- Post-authentication threats
- Brute force attacks

Identity and security statistics

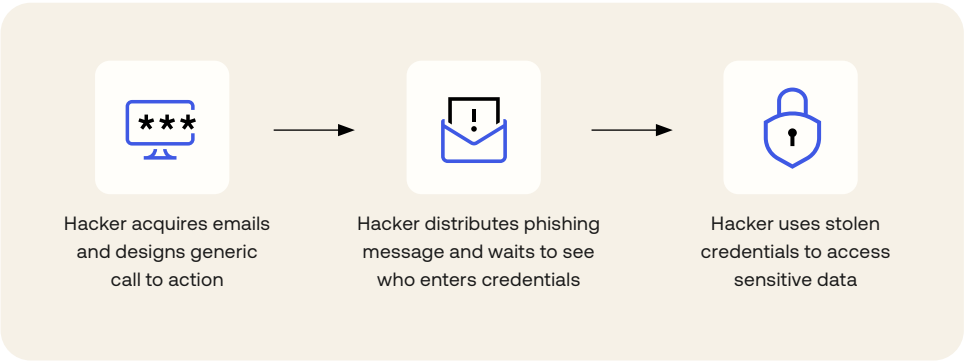
- Attackers used stolen credentials in **45%** of data breaches in **2022**, up from **42%** the previous year[1]
- **74%** of all breaches include the human element, via error, privilege misuse, use of stolen credentials, or social engineering[1]
- **86%** of web application breaches involve stolen credentials[1]

[1] 2023 Verizon Data Breach Investigations Report

Phishing

Phishing schemes are the number one internet crime reported in the US and cause the highest financial loss to victims[2]. Attackers conduct phishing attacks at scale with AI and automation, which makes them increasingly difficult to detect and catch. Most phishing attacks start with emails that attempt to trick users into entering their credentials into a fake website. These emails and websites can look convincing, with suitable branding and language, and using source email addresses very close to the target address. Once an attacker has access to a user's credentials, they use them to log in and gain a foothold as part of a larger attack, for example

- Installing ransomware on organizational systems to elicit a payout
- Performing business email compromise (BEC) in an attempt to redirect funds to a bank account they control, such as changing the account numbers for payroll deposits or invoices
- Mining applications for sensitive data to sell on the dark web



Organizations are investing in spam filters, email security software, antivirus, web filters, and user education programs to protect against the over 156 million phishing emails sent worldwide every day. However, as attacks grow more sophisticated, these traditional defenses are increasingly being circumvented. Similarly, multi-factor authentication (MFA) has been the gold standard for preventing credential theft, including phishing. But recent high-profile attacks have shown that MFA is no longer enough to prevent all data breaches. MFA can be vulnerable to adversary-in-the-middle (AitM) attacks, SIM-swapping attacks, pass-the-cookie attacks, MFA Fatigue, or MFA bombing attacks (in which attackers repeatedly send MFA push notifications). MFA only makes sense if it is resilient against bypassing and hacking.

[2] Federal Bureau of Investigation Internet Crime Report 2022

Mitigation strategies

1. **User tools and training.** Since phishing attacks target users, it's critical to provide them with tools for prevention.
    a. Stage phishing simulation campaigns with Okta Workflows by sending fake MFA prompts to educate users on MFA Fatigue.
    b. Make it easy to inform end users of authentication changes in their accounts with Okta HealthInsight. This capability also makes it easy for users to report suspicious authentication events.
2. **Least privilege access**. Okta Identity Governance (OIG) enables access controls that limit user access only to the resources they need for their role or a project on a time-bound basis, reducing the risk of lateral movement if a phishing or other social engineering attempt is successful. Similarly, OIG automates and manages the joiner, mover, and leaver processes across cloud and on-prem resources and certifies access on a recurring basis. This automation reduces the risk of threat actors using dormant accounts to launch phishing attacks or gain access.
3. **Step up authentication**. Okta Adaptive MFA behavior detection analyzes user behavior patterns and creates profiles of typical patterns based on previous activity. You can configure policy rules that respond automatically to changes in user behavior, for example, requiring an additional factor if a user attempts to sign in from a different country or IP address.
4. **Phishing-resistant authentication.** Phishing-resistant authentication is designed to prevent attackers from bypassing MFA by eliminating shared secrets such as security questions. It also prevents users from entering credentials into fake domains set up by attackers. Okta supports
    a. All major phishing-resistant authentication methods, including any FIDO2 WebAuthn option and PIV/CAC smart cards
    b. Okta FastPass, a phishing-resistant, passwordless, Zero Trust authenticator suitable for managed and unmanaged devices

5. **Threat detection**. Security teams can take advantage of Okta integrations with leading email providers and set up adaptive authentication policies based on risk. For example, Okta policies could step up authentication or lock user accounts in response to threats detected at the email layer. Okta Identity Threat Protection with Okta AI leverages security signals from various security solutions, including email security vendors. If these vendors detect incoming phishing emails or malicious links, they can alert Okta to elevate the user's risk level and trigger appropriate inline responses.

6. **Threat response**. Beyond detection, Identity Threat Protection orchestrates tailored responses based on policy configuration and the assessed user risk levels. For example, a medium risk level may prompt Identity Threat Protection to send notifications to the SIEM or incident response team, while a high risk may trigger user re-authentication, kill a user session, or even log users out of supported applications with the capability enabled.

End-user device compromise

Work-from-anywhere and BYOD has opened the door to more threats against user phones, laptops, and other devices. As phishing-resistant adoption increases, threat actors may also turn to compromising devices as a way into your organization.

Cyberattacks often start with compromising an end-user device, for example, tricking an end user to install malware. This malware can then steal credentials and, as with phishing, allow the threat actor to move laterally in the organization to spread ransomware, exfiltrate sensitive data, or execute BEC. Identity can play a role in preventing and detecting some endpoint attacks by adding extra security to devices and verifying devices during and after authentication.

Mitigation strategies

1. **Device trust.** Device trust ensures only users with trusted, managed devices can access your environment. Okta strengthens device trust by ensuring each managed device has a suitable security posture before a user is allowed to log in. The Okta Verify app integrates with mobile device management (MDM) and endpoint detection and response (EDR) tools and captures device signals during sign-in. Based on these signals and the policies you define, Okta makes an access decision.
2. **Device assurance.** For unmanaged devices or managed devices without MDM or EDR support, Okta Verify can perform device health checks and make an access decision based on your policies. For example, you can require disk encryption and up-to-date OS versions and disallow jailbroken devices. After authentication, FastPass can continue to perform device checks in the background every time a user opens a new app. Depending on what information the device returns, FastPass may request re-authentication or reject the request to access the app.
3. **Device access protection**. Okta Device Access extends the same secure MFA experiences to how users sign in to their desktops, extending an extra level of protection to their devices. Device Access can confirm a user's identity and grant access even without an internet connection.

4. **Trusted application filters.** Administrators can create an allowlist of apps to help ensure that malicious or unverified applications on user devices cannot exploit FastPass to gain unauthorized access.
5. **Threat detection and response.** Identity Threat Protection integrates with leading EDR vendors for device malware scanning and response. Automated responses include actions like re-authentication requirements or logging users out of compromised devices based on the real-time risk assessment by Identity Threat Protection.

Insider threats

Insider threats are on the rise and can be malicious, like a deliberate attempt to steal information or cause harm. However, 55% of insider incidents involve employee negligence, like failing to secure devices, install security updates, or follow company security policies. Other insider threats include legitimate mistakes or users fooled by a new type of attack. Last year, it took an average of 86 days to contain an insider incident, and the average cost per organization for insider risk increased to $16.2M.[3]

Identity plays a role in an organization's insider risk management program. For example, 56%3 of organizations report deploying privileged access management (PAM) solutions to reduce the risk of insiders mistakenly or maliciously accessing privileged credentials and accounts. Similarly, IGA systems can minimize the impact of insider threats on an organization.

[3] Cost of Insider Risks Global Report, 2023

Mitigation strategies

1. **Device access protection.** Suppose an insider loses a laptop or leaves it in an unsecured location. Device Access provides an additional layer of security that can help prevent unverified users from gaining access to data stored on the device, even if the device isn't connected to the internet.

2. **Least privilege access.** Okta Identity Governance helps organizations create processes that limit insiders to only the apps and resources required for their role and project, minimizing the risk of users gaining inappropriate access to valuable information. Administrators can set access to expire after a certain time or run access certification campaigns to verify appropriate access.

3. **Privileged account access.** Reduce the risk of insiders accessing sensitive resources inappropriately. Okta Privileged Access protects critical resources by eliminating standing access, securing shared accounts, and providing individual accountability for usage. Okta unites critical PAM capabilities with IAM and Identity Governance in a single platform, increasing visibility and simplifying policy enforcement for privileged accounts and resources. This unification eliminates the need for siloed IAM, IGA, and PAM tools and improves security. Behaviors or signals that elevate user risk levels in IAM are automatically transmitted to Privileged Access for action, reducing the risk of malicious or careless insiders leveraging privileged credentials.

4. **Threat detection**. Sometimes, valid users may misuse organizational resources. Identity Threat Protection with Okta AI works with other security tools such as EDR solutions, cloud access security brokers (CASB), and SIEMs. These security tools identify suspicious behaviors, such as a user downloading a large number of files from a directory, and notify Okta of elevated user risk.

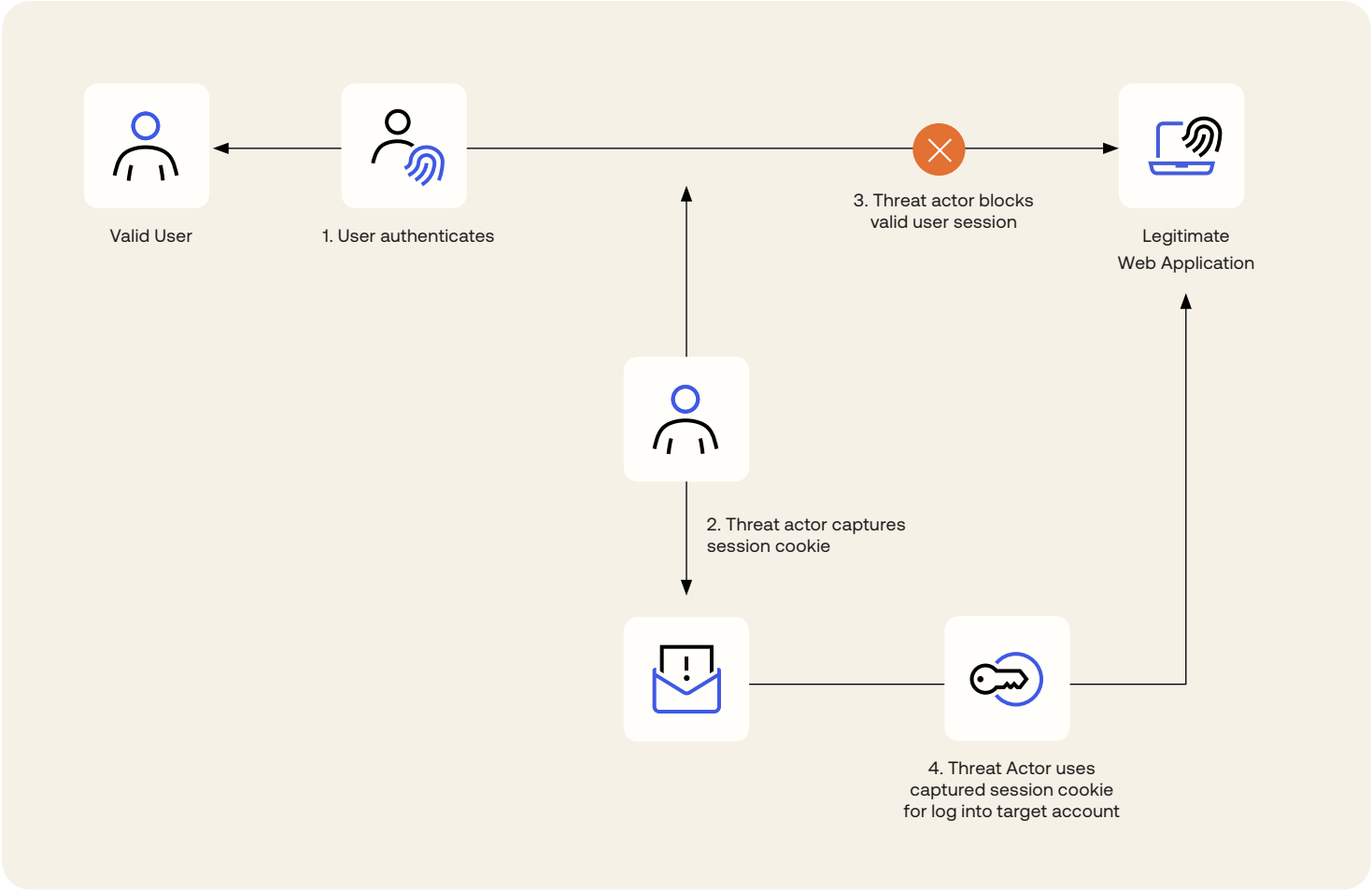
5. **Threat response**. As with other attacks, Okta can automatically and appropriately respond to elevated user risk profiles by requiring re-authentication, limiting access, or logging users out of supported applications.

Post-authentication threats

Securing the initial login is no longer enough. As the adoption of multi-factor and phishing-resistant authentication increases, stealing credentials at login will become more difficult for threat actors. This will cause an increase in attacks targeting users and their devices after they've successfully authenticated. Several high-profile breaches have already demonstrated the opportunities for post-authentication attacks.

Session hijacking

After a user successfully authenticates to a particular application server, the server generates a session token or cookie that's stored in a user's browser. Session hijacking can use several methods to steal a session token, including cross-site script (XSS) attacks, malware installation, session sniffing, and more. Once the attacker has a valid session token, they can do anything that a valid user is authorized to do in that application.



Mitigation strategies

1. **Risk mitigation configurations.** Okta enables a number of different configurations to mitigate the risk of stolen sessions:

    b. You can set user sessions to expire after a specific duration or idle time, reducing the length of time that threat actors can steal or use stolen session tokens.

    b. Similarly, Okta Identity Governance can provision fine-grained application entitlements for users based on their roles or projects, mitigating potential risks associated with stolen session cookies by limiting what adversaries can do in a particular application.

    c. You can set an authentication policy rule to require users to re-authenticate every time they attempt to access a new app. Using passwordless authentication via FastPass minimizes the potential inconvenience for users.

2. **Extra VPN security.** Virtual private networks (VPNs) are an excellent way to thwart session sniffing. However, VPNs often only require a username and password, which are vulnerable to attack. Okta integrates with many VPN vendors and adds an extra layer of security with MFA or phishing-resistant MFA, reducing the risk of successful sniffing attacks when users are on public WiFi networks.

3. **Session risk analysis.** Once users are authenticated, Identity Threat Protection continuously monitors user sessions for suspicious or out-of-character behavior. Analytics powers the behavior analysis. Identity Threat Protection also receives security signals from Okta Verify and third-party security tools, forming a real-time view of session risk.

4. **Context re-evaluation**. For organizations that deploy a heterogeneous mix of devices, FastPass silently performs device health checks each time an authenticated user opens a new application. This provides additional assurance that the device and its posture haven't changed before allowing access, mitigating the risk of session hijacking.

5. **Privileged accounts**. Okta Privileged Access reduces the session attack surface by controlling access to privileged accounts to authorized personnel with a legitimate need and limiting the scope of permissions during sessions.

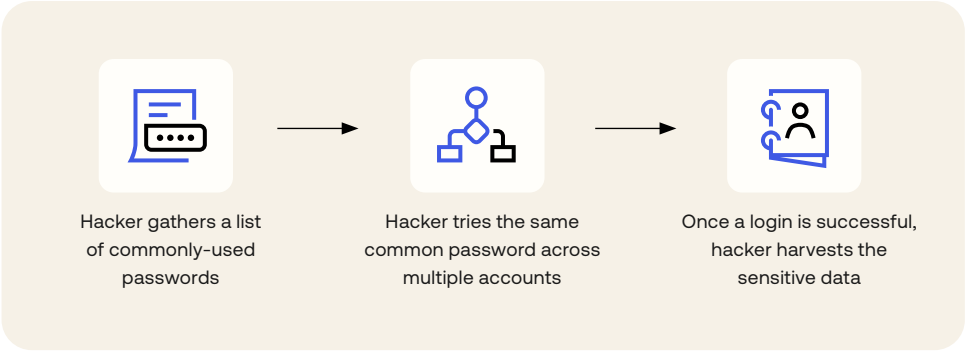
6. **Threat response.** Okta can adaptively respond to risks identified in user sessions by prompting for re-authentication or killing the session entirely. Conversely, Identity Threat Protection can improve the user experience by extending the length of sessions for users with low-risk profiles.

Brute force attacks

Brute force attacks aren't going away as long as people continue to use weak passwords or re-use existing passwords.

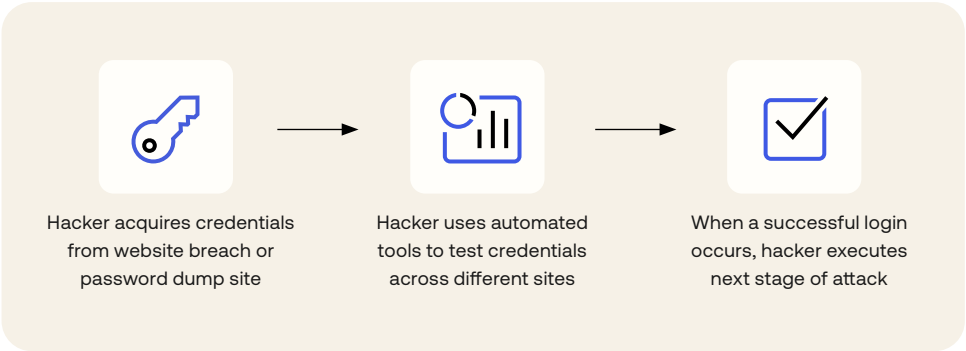
Password spray

A password spray attack relies on volume rather than targeting specific users or accounts. A threat actor uses a few commonly known passwords across multiple accounts in hopes that a user has set that password for their login credential. Often, attackers attempt to stay under account locking thresholds by using a low number of qualified password guesses across many accounts. To increase the likelihood of a correct guess, a threat actor may perform research on targeted organizations to determine if a system requires passwords of a particular length or special characters.



Credential stuffing

In credential stuffing, the threat actor attempts to stuff valid credentials (often harvested from an online data dump) into many different sites, hoping one of them is successful. This attack exploits people's tendency to reuse passwords across multiple sites. The threat actor uses automated tooling to cover a vast number of systems in a short period of time. This attack is often successful, as valid credentials do not trigger password lockout settings.



Mitigation strategies

1. **User tools and training.**
   For organizations still using passwords:

   a. Minimizing password reuse can reduce the likelihood of a credential stuffing attack succeeding. One way to accomplish this is to remove the burden of creating strong passwords for users. Okta's browser plugin can suggest unique passwords and save them automatically when users create new accounts.

   b. Okta can help your organization stay clear of common passwords by enforcing password requirements during the account creation process, reducing the risk of a password spray attack. More information can be found here.

2. **Malicious IP detection.** ThreatInsight aggregates data across the Okta customer base and uses it to detect malicious IP addresses that attempt credential-based attacks. Okta prevents these IP addresses from getting to the authentication stage, reducing the risk of locking valid users out of their accounts.

3. **Secure authentication methods.** Okta offers several authentication choices to thwart brute-force attacks:

   a. FastPass is a Zero Trust authenticator that eliminates the need to use passwords, a significant attack vector. It also evaluates device and browser health and helps ensure only trusted users and their devices can access your environment.

   b. Okta supports a range of other phishing-resistant authentication methods.

   c. Adaptive MFA ensures that threat actors can't complete the authentication flow even if they have a compromised credential. Okta collects user behavior like location, IP address, and other data points to help build a baseline profile and determine the risk level of the login attempt. If MFA is not a control you can enforce for every user and every login, you can layer this control in conjunction with other checks like device fingerprinting. In addition, security admins can set up CAPTCHA in the login flow to augment the security of the authentication request.

Summary

Workforce Identity Cloud offers a range of capabilities that protect users, their devices, and their sessions from threats before, during, and after authentication. Behavior analysis, device checks, and out-of-the-box integrations with other security tools enable Okta to continually assess risk and help your organization to automatically respond to risks related to identity before they have an impact.

Learn more about Workforce Identity Cloud.