okta

Identity Driven Security

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

info@okta.com
1-888-722-7871

Identity Driven Security

Introduction

In today's business environment, almost every organization has experienced a serious security breach, will soon be breached, or has been breached and does not yet know it. Most IT and security professionals agree that if a persistent attacker wants to gain access to an organization's network or sensitive information, they usually can. To prevent security breaches companies often employ a variety of solutions including firewalls, antivirus (AV), web application firewalls (WAF), security information and event management (SIEM), endpoint monitoring, malware sandboxing, cloud application security, and so on. These point solutions are designed to protect against infrastructure tampering while monitoring data flow.

Infrastructure security technologies offer adequate defensive controls but don't typically address one of the most strategic concerns: Identity and Access Management (IAM). Most IT and security professionals understand that IAM is a critical component and central pillar to maintaining adequate security but often struggle with ensuring the right balance between protection and usability. Users need adequate and secure on-demand access to appropriate systems and information while the organization needs to implement and maintain proper security controls to prevent attackers from also gaining access. The desired goal is to validate that only authorized users have access to sensitive data. This can ensure that infrastructure compromises such as machine infections are rendered ineffective.

61%
of users are more likely to share a work password than a personal password[1]

The Growing Threat of Credential Theft

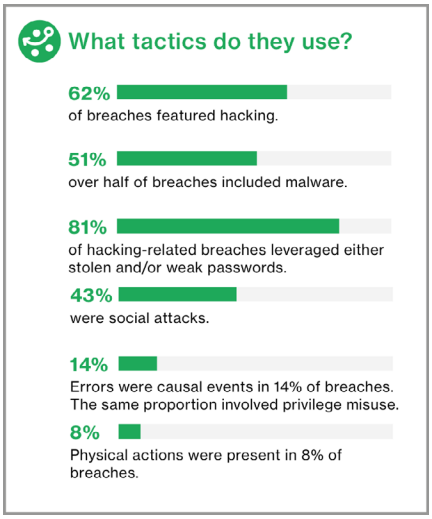
User credential theft is by far one of the most challenging security issues faced by most organizations. The 2017 Verizon Data Breach Investigation Report validates that almost 81% of data breaches involve stolen or weak identity credentials, up from 63% in 2016. The Verizon report also indicates that user credentials are targeted in over 90% of phishing attacks. These attacks frequently use sophisticated phishing and spear phishing under the heading of "social engineering." Even though many organizations are trying to better educate their users about these threats, credential phishing is still rampant. Hackers are using fake emails, text messages, websites and other clever techniques to steal user credentials. Most experts now agree that credential harvesting has become one of the most effective tactics used by threat actors to gain access to a firm's crown jewels.

[1] Source: LastPass, "Keep Your Friends Close and Your Passwords Closer," February 2016

Simple password protections are no longer adequate to thwart these attacks. In most organizations, users duplicate 73% of their passwords, and an average of 40 services are often registered to one email account. The average user only has five passwords, and those passwords they believe are complex and secure may actually be easier for hackers to crack. According to former National Institute of Standards and Technology (NIST) manager, Bill Burr, the password tricks and tips suggested by experts over the years might make us more vulnerable to hacking. Burr admitted that his previous advice might have steered users toward easily predictable schemes.

Once a hacker discovers a single password, such as one used for a personal banking account, they can exploit this knowledge to gain access to a variety of business systems and applications that contain sensitive information. This vulnerability exposes firms to serious consequences including ransom demands, brand damage, regulatory fines, and costly lawsuits.

81% of breaches were caused due to stolen and/or weak passwords.



Screenshot from the Executive summary in Verizon Data Breach Report 2017

Security Landscape Gaps

A variety of security solutions are effective at mitigating most outward facing attacks. They help prevent machine modification via anti-malware for endpoints and networks. They can detect malicious behavior (SIEM, DLP), protect applications (WAF), shield the network and endpoint (firewalls, IDS/IPS, endpoint protection solutions), and guard valuable information (Encryption, DRM, DAM solutions). Unfortunately, many of these solutions can be difficult to implement and manage. Also, they often create a mountain of data, reports, and identified incidents or threats that are overrunning available resources. What's worse, even with these fortifications in place, IT and security teams are still powerless against newer and more sophisticated attacks on end-user credentials.

Most of these security solutions focus on infrastructure protection, but once an attacker successfully steals the identity of a legitimate user, all bets are off. Granted an open door, attackers can start wreaking havoc from the inside. To avoid this serious possibility, IT and security professionals need to implement a holistic identity solution that offers strong user authentication as a single platform.

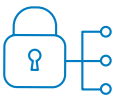
Identity is the Missing Ingredient

Mobile workforces are changing how information is accessed and used, and attackers are targeting remote users with increasing frequency and efficiency. This dynamic creates a two-edged sword. On one edge, productivity, morale, and employee retainment improve. On the other, a more open posture creates a security nightmare for organizations. The proliferation of mobile, cloud, VPNs, and other remote technologies opens the door wider to potential attacks. IT teams now have far less visibility and control over employee "worst practices." A potential disaster is in the making every time a user connects to an unsecured WiFi network at a local coffee shop. Managing identities while ensuring seamless and uncomplicated access can lead to higher support costs and increased employee frustration. Users may complain about password management while demanding ease of access to applications and information regardless of location. They expect the tools they're given to improve, not hinder, their productivity.

Effective IAM allows users convenient access to appropriate organizational information and resources while keeping hackers at bay. When implemented correctly, IAM covers three important bases: identification, authentication, and authorization. Identity solutions offer critical control points that include seamless Single Sign-On (SSO) technology for cloud, mobile, and on-premises applications. They help reduce identity silos across applications and different business units within an organization. They prevent insider threats and misuse of account privileges as an integral component of an overall security posture. Properly integrated IAM and SIEM solutions can strengthen the discovery of malicious attacks and provide security analysts with necessary user information.

Strategic Direction for Identity-Driven Security

The challenges described above highlight the need for a strategic solution to securing identity. Adapting and optimizing IAM across an enterprise should be an integral part of any strategic security plan. When implementing an overall IAM plan, top IT and security professionals usually strive to accomplish the following:



Centralized and unified identity management: Your identity and access control infrastructure should be centralized and include a unified SSO authentication approach. Application sprawl combined with separate user management across disparate departments that use different identity management systems can create security gaps that are easily exploited. Centralized identity management also helps reduce attack surfaces by automating the provisioning and de-provisioning of user accounts. This eliminates orphan accounts that can be used by attackers to gain entry. A single pane of glass for managing users ensures access to appropriate applications and mitigates security weaknesses.

Multi-Factor Authentication (MFA): This technology is now a requirement for several compliance mandates, and it's the best way to shore up security gaps caused by weak and hackable passwords. Even better, Adaptive MFA delivers an optimal user experience and much stronger authentication based on user behavior and context.

Adaptive Multi-Factor Authentication

IT and security teams can usually maintain control over centralized identity management, but ensuring adequate security requires the cooperation of users. They're an integral part of any authentication approach. As we learned earlier, relying solely on passwords is problematic. To address this concern, two-factor authentication (2FA) offers a second form of identity verification, such as one-time passwords, SMS-delivered codes, or user biometrics including fingerprinting.

Adaptive MFA (AMFA) offers the best balance between effective security and user simplicity. This approach allows you to easily adjust the slider bar from left to right to increase or decrease trust levels as desired. Adaptive policies can be based on user behavior and context, such as location, to determine when it's necessary to require a second level of authentication. For example, if a user is working at an office location, based on security policies, AMFA recognizes this as a secure location and sets the appropriate level of authentication. AMFA will also recognize that a user is trying to gain access using a previously authenticated device and adjust accordingly. If a user tries to authenticate from an offsite or unrecognized location, the system will step-up authentication by challenging with a second factor to validate identity.

Protect Against Data Breaches Using Identity Solutions

Mobile and cloud proliferation has exposed organizations to much higher risks for potential hacks and attacks. The traditional perimeter is crumbling under the weight of these threats, making it imperative to re-examine traditional security approaches. IAM must now take center stage to defend against identity-based security breaches.

Okta recommends the following best practices and success factors to dramatically reduce attack surfaces and vectors:

- **Eliminate multiple passwords and replace them with strong, unique password requirements.** SSO is a foundational building block that affords users centralized access to applications and systems from almost any device or location.

- **Protect your crown jewels via secure identity authentication.** MFA—and better yet Adaptive MFA—provides a robust second factor ensuring only legitimate users have access to data. Stolen passwords are no longer a concern as attackers will not gain access when step-up authentication, such as OTP and biometrics, are in place.

- **Implement lifecycle management by using automated provisioning and de-provisioning to reduce the attack surfaces and vectors.** When you add new applications, whether cloud or on-premises, centralized directory services and management of user access to applications ensures consistent visibility and reporting.

- **Monitor and detect user access patterns to key applications and devices.** By aggregating these events in a centralized repository, and sending these events to an incident management product, you gain visibility into user behavior and context to help you identify malicious attacks.

Conclusions

The proliferation of mobile and cloud usage in the workplace increases the risk of credential theft. Traditional endpoint and infrastructure security solutions are ineffective once attackers gain access and appear to be legitimate users. A robust IAM posture designed to prevent these attacks should include Adaptive Multi-Factor Authentication. Implementing AMFA for everything everywhere can eliminate identity sprawl via SSO while moving beyond vulnerable password-only solutions. The best AMFA solutions identify potential account compromises and accelerate attack responses via robust ecosystem integrations. Along with AMFA, sophisticated lifecycle management can ensure orchestration and entitlement management to maintain the optimal level of access to your applications.

With AMFA and lifecycle management, employees can eliminate password frustrations, and IT can reduce management difficulties and expense. A federated architecture that's everywhere your employees are, including cloud, mobile, and on-premises, can reduce attack surfaces and vectors without disrupting user productivity. When attackers try to breach your walls with credential phishing, AMFA defends your castle by offering technical controls at the email gateway and authenticates identities by providing the desired level of assurance and verification. While many solutions deliver a variety of verification capabilities, the best solutions manage identities as a core component of the platform.


okta