Palo Alto Networks and Okta

Preventing Credential Theft and Abuse

Benefits of the Integration

- Detect, block, and prevent phishing attacks.
- Reduce your attack surface by preventing misuse of credentials.
- Ensure only authorized users access your applications.
- Simplify deployment of multi-factor authentication (MFA) across your organization.
- Enforce MFA to critical systems such as SCADA and mainframe servers.
- Meet compliance requirements for strong authentication and access controls.

The Challenge

More than 80% of hacking-related data breaches involve weak or stolen passwords.[1] Ideally, organizations must both stop credentials from being stolen and stop attackers from using stolen credentials to access systems and data. MFA thwarts almost all attempts at credential abuse, such as pass-the-hash and brute force attacks, credential stuffing, and more. Unfortunately, enforcing MFA for all resources—including legacy applications and servers as well as SaaS applications—can be a challenge for IT and DevOps.

Okta

The Okta Identity Cloud makes it easy for organizations to securely connect their users with the resources they need to do their jobs. Okta centralizes access to SaaS apps, web access management (WAM) systems and custom web apps, APIs, and infrastructure. With one set of credentials, users can access all of the resources they need to be productive, wherever and on whatever device they choose. Administrators can assign resources relevant to a user's role as well as set access policies based on role, the resource the user is trying to access, and more. You can prompt for a second factor based on risk signals from the device, network, geography, and more. Finally, Okta can centralize user stores from on-premises systems like Active Directory® or LDAP, as well as HR systems like Workday®, and automate on/offboarding of applications, saving administrators time and reducing the risk of misconfigurations.

Palo Alto Networks ML-Powered NGFW

Palo Alto Networks ML-Powered Next-Generation Firewalls (NGFWs) inspect all traffic at Layer 7 and offer a prevention-focused architecture that is easy to deploy and operate. Automation reduces manual effort so your security teams can replace disconnected tools with tightly integrated innovations, focus on what matters, and enforce consistent protection everywhere.

ML-Powered NGFWs inspect all traffic, including all applications, threats, and content, and tie that traffic to the user, regardless of location or device type. The application, and content—the elements that run your business—become integral components of your enterprise security policy. As a result, you can align security with your business policies as well as write rules that are easy to understand and maintain.

Palo Alto Networks and Okta

Palo Alto Networks and Okta work together to prevent successful phishing attacks and credential abuse as well as simplify MFA deployment and management. Through granular security policies and constantly updated protections that counter the latest threats, Palo Alto Networks NGFWs prevent users from entering corporate credentials into risky or unsanctioned applications in addition to phishing websites that mimic valid ones. By leveraging Okta Adaptive MFA, you can require a second, higher assurance factor such as a security key or WebAuthn before allowing access to corporate resources, mitigating the risk of exposed credentials.

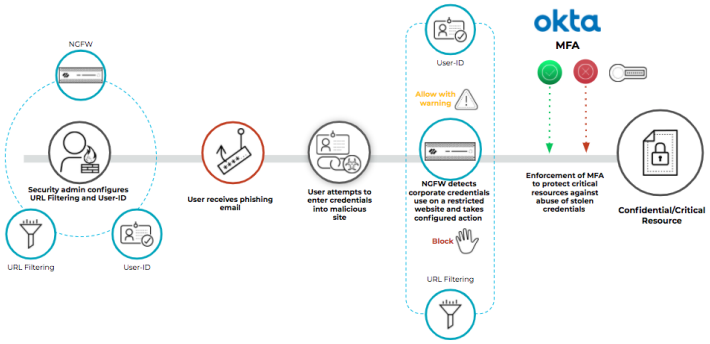

Figure 1: Phishing and credential abuse prevention with Palo Alto Networks and Okta

1. "2019 Data Breach Investigations Report," Verizon, May 2019, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.

Use Case No. 1: Protect Critical Systems from Unauthorized Access

Challenge

Adversaries are increasingly targeting critical systems in many industries, such as SCADA systems. These often run custom and/or legacy applications that do not support MFA. These applications are difficult to modify, and taking them offline to rearchitect their login processes may not be an option. As a result, organizations often leave critical applications exposed to credential abuse.

Solution

Enforce authentication policy, including MFA, without updating your applications and servers or taking critical resources offline. You can configure Palo Alto Networks NGFWs to enforce MFA for web or thick client applications, for some or all users. Configuration of application authentication policies is conveniently centralized using Panorama™ network security management.

Okta Adaptive MFA, part of the Okta Identity Cloud, integrates with Palo Alto Networks NGFWs to verify the identity of a user. Choose from various second-factor options and leverage context-based, granular access policies to balance the needs of users, ease of use, and the sensitivity of the systems being protected. Once users are authenticated, Palo Alto Networks NGFWs can apply further security policies, such as scanning for threats in traffic or denying access to computers without the latest patches installed.

Use Case No. 2: Meet Compliance Requirements

Challenge

Many data protection regulations around the world either require or recommend MFA to safeguard sensitive information. For example, PCI DSS requirement 8.3.1, introduced in PCI DSS 3.2, mandates merchants and payment card processors use MFA to verify all non-console administrative access to the cardholder data environment.

Solution

You can configure Palo Alto Networks NGFWs to enforce MFA for some or all users and/or applications, so you don't have to change existing applications to meet security requirements. Security teams can quickly provision MFA and address compliance without the need to update sensitive resources.

Use Case No. 3: Deploy Seamless Single Sign-On

Challenge

Users have trouble remembering passwords for dozens of apps, which can result in them reusing the same credentials over and over for both personal and corporate access. With one successful phishing attack, these insecure password habits leave your corporate applications and data vulnerable.

Solution

Improve productivity and reduce the risk of users forming bad password habits by easily implementing single sign-on (SSO) and MFA. Palo Alto Networks and Okta customers can deploy SSO to all Security Assertion Markup Language (SAML)-enabled applications, including more than 6,500 applications in the Okta Integration Network, as well as other applications that support federation standards. Palo Alto Networks NGFWs support SAML 2.0 authentication with Captive Portal, GlobalProtect™ network security for endpoints, GlobalProtect Clientless VPN, and administrative UI modules. For more information about secure remote access for your workforce, read the Palo Alto Networks and Okta Secure Remote Access solution brief.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Nearly 8,000 organizations, including Engie, JetBlue, Nordstrom, Takeda Pharmaceutical, Teach for America, T-Mobile and Twilio, trust Okta to help protect the identities of their workforces and customers.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com