proofpoint.

SOLUTION BRIEF

Proofpoint and Okta Partnership

okta

Gain adaptive controls for high-risk users and protection against credential phishing and cloud account takeovers

Products

- Proofpoint Targeted Attack Protection
- Proofpoint Threat Response Auto-Pull
- Proofpoint Cloud App Security Broker
- Okta Identity Cloud
- Okta Workflows

Key Benefits

- Visibility into the most at-risk users
- Protection from malicious URLs and messages in real time
- Protection from account takeovers in more than 7000 Okta-federated cloud apps
- Adaptive, risk-based access control
- Higher efficiency through more automated security

Today's cyber attacks target people. To stop them, you need a people-centric understanding of how attackers work, who they target and what they might be after.

At Proofpoint, we give you visibility into your Very Attacked People™ (VAPs). This concept is our way of identifying and protecting the users most at risk in your organization. We start by quantifying the severity of each attack based on criteria such as:

- **Attacker type.** The attacker's level of sophistication and, in turn, risk to the organization.
- **Targeting type.** How narrowly or broadly targeted the attack is.
- **Threat type.** Reflects the type of malware, tools or techniques involved in the attack.

Then we look at the overall volume of attacks targeting that user. Together, these factors help reveal the VAPs within your organization.

In addition to VAP visibility, we can also alert you on cloud accounts with suspicious logins that used Okta credentials. The advanced suspicious login detection is based on criteria such as:

- Email and cloud threat intelligence
- Cloud user behavior analytics

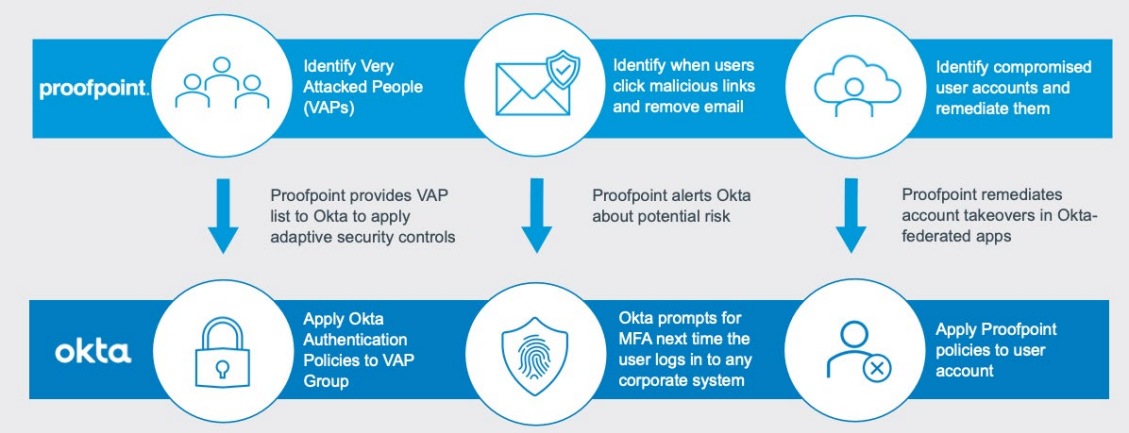

Figure 1. Together, Proofpoint and Okta protect against advanced attacks that target people.

But visibility is just one piece of the puzzle—what you do with that insight is just as important. That's where adaptive controls come in. By applying extra layers of protection to users who are targeted with the most threats, you can protect them and mitigate any damage that can come from these threats.

Proofpoint solutions offer several built-in adaptive controls. But you can extend them even further through Okta's cloud-based identity management features. Okta Identity Cloud helps you control access and apply extra layers of authentication to your VAPs. It's simple to deploy and easy use.

Together, Proofpoint and Okta provide you with the enhanced, flexible security you need for today's people-focused threats.

How the Integration Works

Apply adaptive security controls to VAPs

Proofpoint Targeted Attack Protection (TAP) identifies VAPs and shares that intelligence with Okta Identity Cloud and Workflows to apply adaptive controls and secure their identity.

The adaptive controls that can be applied are any authentication policies such as:

- Password policy
- Authentication policy
- Factor enrollment
- Application access
- Application sign-on
- User roles/entitlements

Close the security loop

Email

When Proofpoint TAP detects that a user has clicked a phishing link in an email, it will notify Proofpoint Threat Response Auto-Pull (TRAP) to remove the email from the user's inbox. From there, TRAP will alert Okta, and Okta will add affected users to a group subject to stricter MFA policies.

Cloud

Proofpoint detects and remediates suspicious logins to cloud applications via TAP, Cloud App Security Broker (CASB) behavior analytics and Proofpoint and third-party threat intelligence. Based on customer policy, CASB instructs Okta on the appropriate remediation action.

Common Use Cases

Here are a few common use cases for the Proofpoint-Okta integration:

- Assign or restrict access to unsafe apps based on user risk or suspicious logins.
- Create dynamic multifactor authentication (MFA) policies based on user risk. These might include MFA session and factor length; which MFA factors users are required, allowed or disallowed from enrolling; and app-level MFA requirements.
- Adjust a user's roles or entitlements for authorization in downstream apps when deemed a high-risk user.
- Automatically adjust password policy for your most highly attacked users. These might include complexity, history, expiration and reuse.
- Leverage Okta Workflows to perform a set of actions inside many different business applications for additional security.
- Remediate suspicious logins based on your corporate security policies. Remediation can include revoking the user session, resetting the MFA factors or suspending the user and forcing a password change.

By using these best-of-breed solutions together, you can identify and protect your most at-risk users and respond to credential phishing attacks and account takeover attempts more quickly and accurately. That means less time resolving and recovering from incidents.

Advantages of the Proofpoint-Okta Integration

Every second matters in an incident response. Confirming whether a user has clicked on a credential phishing URL or whether a suspicious login attempt is legitimate takes time. So does verifying whether the user has been compromised. And the clock is still ticking when you reset their password or step up authentication.

With Proofpoint and Okta, you reduce the chances that your users are compromised. And just as important, you respond faster when something goes wrong.

That means your team is freed up to focus on other cybersecurity challenges and stay ahead of the next attack. It's simply a better experience for incident responders, security analysts and system administrators.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.