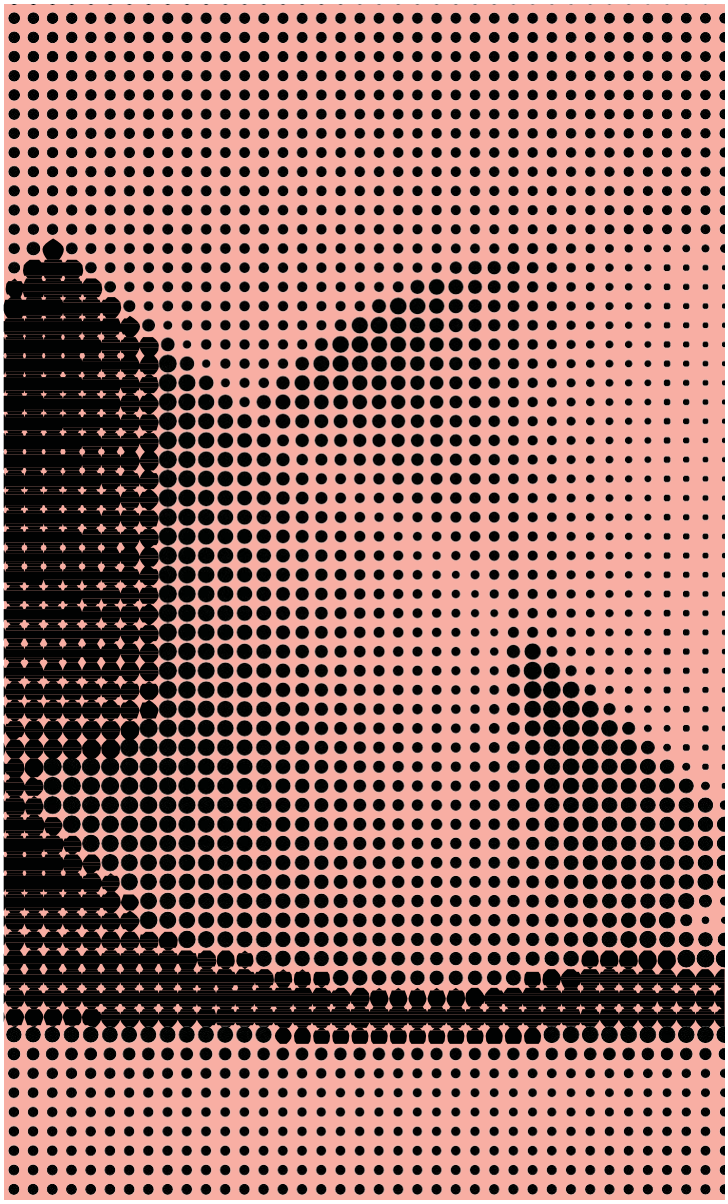
Datasheet
April 2022

okta | proofpoint

Protect against advanced attacks that target high-risk users

Combine email and identity security to prevent cloud account takeovers and credential phishing

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. The greatest challenge is mitigating risk - defending people's identities and securing their access to apps. This includes preventing attacks before they reach people, protecting users and access to resources by securing identity, and enabling visibility and rapid response when threats are detected. Okta and Proofpoint recognize that people are key targets in a Zero Trust world, and together provide the holistic approach businesses need.



Key Solution Benefits

- Adopt a **people-centric approach** to security that protects against credential theft and phishing
- Gain visibility into your most targeted users and **apply granular security policies** to all your users
- **Orchestrate remediation actions** on potentially compromised users, like quarantining emails, prompting for MFA, and other adaptive controls
- Achieve **greater efficiency** and **respond faster** through more automated security

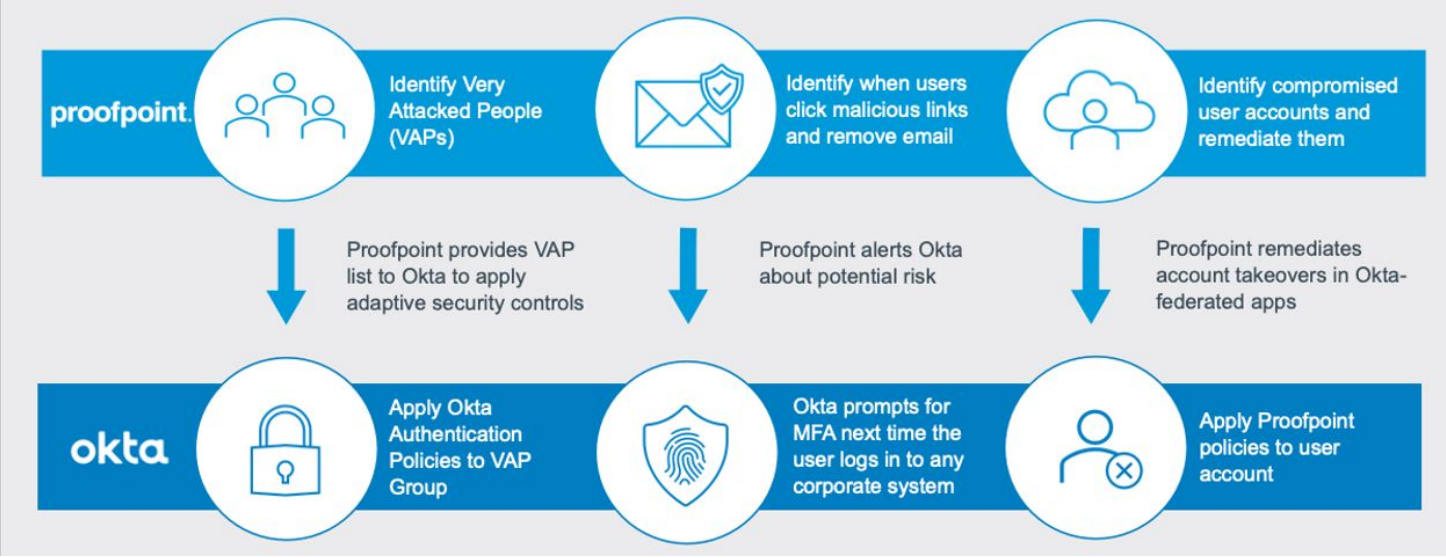
Extend people-centric security through automated adaptive controls

The Okta Identity Cloud protects your users and their access to resources through centralized access policies across cloud and on-prem apps and services, with Single Sign-On (SSO) and Multi-Factor Authentication (MFA) as critical security controls. Proofpoint identifies at-risk users, or Very Attacked Persons (VAPs), based on threat type, target, and sophistication to offer advanced cloud and email security to protect against attacks. With advanced tools for applying fine-grained adaptive security measures and containing and remediating attack campaigns, the integration offers a comprehensive solution to help secure access to cloud apps, Office 365, G Suite, and the entire IT environment.

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 identities. 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



Okta and Proofpoint protect against advanced attacks that target people

Integration Use Cases

- Assign or restrict access to unsafe apps based on **user risk or suspicious logins**
- Create **dynamic MFA policies based on user risk**: which MFA factors users are required, allowed, or disallowed from enrolling, along with 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, including **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, such as revoking the user session, resetting MFA factors, or suspending the user and forcing a password change

Close the security loop with cloud and email integrations

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.

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 that's subject to stricter MFA policies.

By using Okta and Proofpoint, 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, freeing up time to focus on other cybersecurity challenges and stay ahead of the next attack.

For more information on this integration, go to **okta.com/partners/proofpoint**

If you have more questions, please contact our sales team at **okta.com/contact-sales**

About Okta

Okta is the leading independent identity provider. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With more than 7,000 pre-built integrations to applications and infrastructure providers, Okta provides simple and secure access to people and organizations everywhere, giving them the confidence to reach their full potential. More than 14,000 organizations, including JetBlue, Nordstrom, Siemens, Slack, Takeda, Teach for America, and Twilio, trust Okta to help protect the identities of their workforces and customers. For more information, go to **okta.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 **proofpoint.com**.