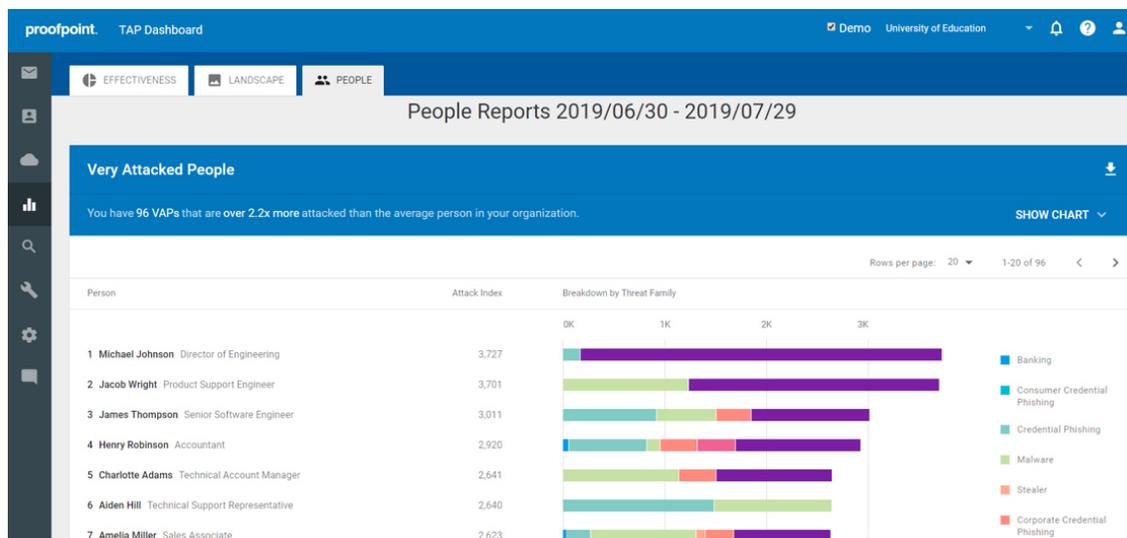


# PROOFPOINT AND OKTA PARTNERSHIP

## GAIN ADAPTIVE CONTROLS FOR HIGH-RISK USERS AND CREDENTIAL PHISH PROTECTION

Organizations continue to struggle with advanced attacks that are focused on targeting their individual users. At Proofpoint, we take a people-centric approach to looking at how threat actors carry out their attacks. This allows us to provide you with visibility into the most attacked users within your organization. Based on various attack criteria—such as attack targeting, type of attack, and threat actor sophistication—we can generate the threat severity for each attack. Going further, we look at the overall volume of attacks impacting an individual user. And combining these provides you with visibility into the Very Attacked People (VAPs) within your organization.

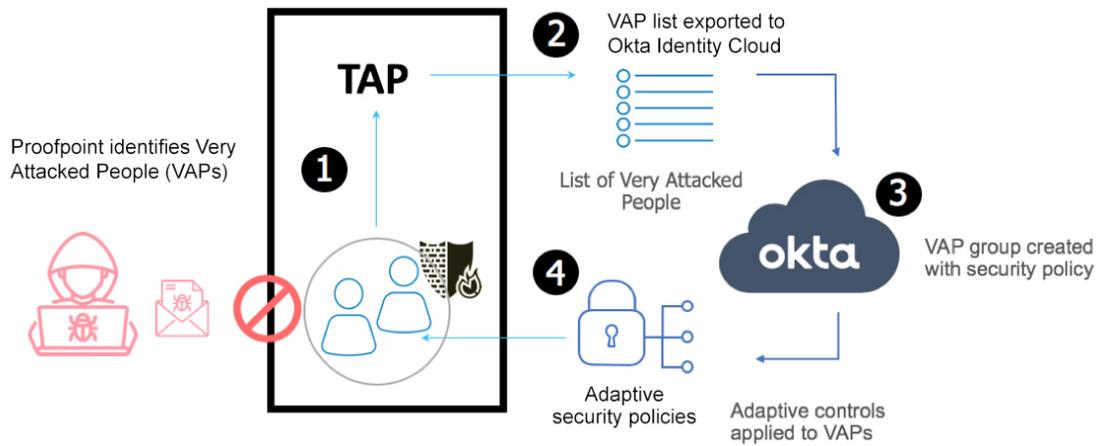


Providing this level of visibility is just one piece of the puzzle when it comes to helping your organization solve for these threats. Adaptive controls are an important part of mitigating damage that can come from these threats. While we have several adaptive controls built into our solutions, we also have a partnership with Okta. This lets us extend these adaptive controls to Identity Management. With Okta, you get a cloud-based approach to Identity Management, with simplicity of setup and ease of use for end users. And together, we can understand your organization's most risky users with Proofpoint tools, and we can manage the user's identity with Okta Identity Cloud. This provides you with the enhanced security you need when your organization—and your people—come under attack from sophisticated threats.

This integration provides you with several impactful use cases to protect your organization and your most attacked people. As a joint customer, you can:

- Assign access to applications or restrict access to risky applications based on the riskiness of your users.
- Create dynamic MFA policies based on user risk. This includes MFA session and factor length, which MFA factors users are required/allowed/disallowed from enrolling, and app-level MFA requirements.
- Adjust a user's roles or entitlements for authorization in downstream apps if they are deemed high risk.
- Automatically adjust password policy such as complexity, history, expiration and reuse for your most highly attacked users.

<sup>1</sup> Verizon. "2019 Data Breach Investigations Report." July 2019.



This integration of these best-of-breed solutions also reduces the time needed to clean up credential phishing attacks with accurate, timely response. The solutions are:

- **Proofpoint Threat Response Auto-Pull (TRAP)**, which enables you to move detected malicious or unwanted messages to quarantine after delivery. It also tracks forwarded mail and distribution lists and creates an auditable activity trail. This minimizes your threat exposure and eliminates the possibility of reinfection. TRAP is part of the Proofpoint Threat Response security orchestration platform. This means all Threat Response users can achieve the same benefits as TRAP.
- **Okta Identity Cloud**, which implements numerous factors for authentication across knowledge, possession, biometric, and contextual factors, to strengthen security and confirm user identities.

## HOW THE INTEGRATION WORKS

You can now link Proofpoint TRAP with Okta Identity Cloud. And once we detect that a user has clicked on a malicious URL and has accessed the web page, your administrators can automatically enable step-up authentication for all systems secured with Okta. This forces the user to reauthenticate to confirm his or her identity—using multiple factors and according to policy—before accessing any corporate system.

As a joint customer, it's easy to benefit from this integration. You can configure TRAP to consume alerts from Proofpoint products. And you can configure the response actions to allow API calls into Okta to add the affected user to a group. That user group will be subject to MFA policies.

## KEY BENEFITS

Response time adds up. Especially when you're confirming if a user has clicked on a malicious credential phishing URL, determining if they have been compromised, and resetting their password or stepping up authentication.

Now with the Proofpoint and Okta integration, precautionary measures are in place. These help you reduce the likelihood of account compromise. We also provide you with a superior user experience for your incident responders, security analysts and system administrators. Now they can easily verify the action taken and free their time to focus on other cybersecurity challenges. This helps to keep you ahead of the next attack.

### ABOUT PROOFPOINT, INC.

Proofpoint, Inc. (PFPT) is a leading cybersecurity 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 to mitigate their most critical security and compliance risks across email, the cloud, social media, and the web. More information is available at [www.proofpoint.com](http://www.proofpoint.com).

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.