okta + proofpoint.

Deliver Comprehensive People-Centric Security Against Credential-Based Attacks

Higher education institutions are made up of many types of users—students, faculty, staff and others—who connect to campus resources from a variety of locations, including on campus, at home, from another campus's network, or from the local coffee shop. The traditional security perimeter no longer holds up in today's cloud and mobile-first world. Now people are the perimeter, which is why phishing and stolen credentials remain the two leading threat vectors in successful attacks. Higher education institutions need a comprehensive people-centric strategy to protect all users and campus resources. Okta + Proofpoint work together to get the job done.

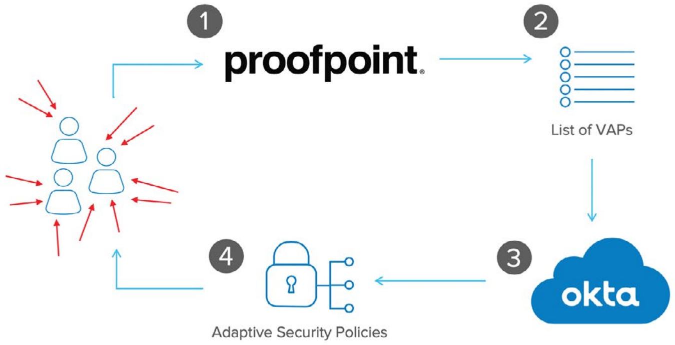
Provide people-centric security

Okta, the leader in identity and access management, and Proofpoint, the leading email security solution provider, work together to safeguard higher education institutions with people-centric security tools purpose-built to counteract threats today and as they evolve. 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's Targeted Attack Protection (TAP) offers advanced email security providing total visibility into and protection from today's most sophisticated email 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 Office 365, G Suite, and the entire IT environment.

Together, Okta + Proofpoint let you:

- 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

Protect Very Attacked Persons



Proactive security with Proofpoint and Okta

1. Proofpoint identifies Very Attacked Persons (VAPs)
2. VAP list is exported from Proofpoint to a group in Okta
3. Adaptive security policies are configured for VAP group in Okta
4. Adaptive security policies are applied to VAPs

Protect your most targeted users with proactive, adaptive security

Campus resources often contain sensitive data that attackers try to steal—research, PHI, PII, and more. Increasingly, attackers are using phishing and other credential-based attack campaigns to gain unauthorized access and exploit this sensitive data. Okta and Proofpoint provide unparalleled visibility and adaptive controls on a higher education institution's most targeted users. Proofpoint identifies those at-risk users, or Very Attacked Persons (VAPs), based on threat type, target, and sophistication. Through an API integration, Proofpoint then pushes this list of users to a group in Okta to enforce stronger security controls. Then, based on easily configurable authentication policies within Okta, users within this group must adhere to adaptive security controls, like stronger sign-on policies, factor enrollment requirements, shorter session times, or more stringent password requirements. Together, Okta and Proofpoint work to provide better visibility and more granular security policies for those users who need it most.

Examples of Okta's adaptive authentication policies for at-risk or potentially compromised users:

- Apply dynamic MFA policies, such as require the enrollment of a stronger factor (e.g. U2F or Okta Verify), shorten factor session length to prompt re-authentication sooner, and apply app-level MFA requirements to sign in to sensitive applications
- Restrict access to sensitive resources, like HR or clinical apps, or assign access to applications, such as a security awareness training
- Adjust password policies, such as minimum length, complexity requirements, expiration, reuse, and lockout

Neutralize incoming attacks with orchestrated security response

With Okta and Proofpoint, higher education institutions can leverage integrated tools to automate their first line of defense and reduce attack response time. If a user clicks on a malicious link in an email, an institution can take automated response actions to remediate the threat, thanks to Proofpoint's Threat Response Auto-Pull (TRAP) integrated with the Okta Identity Cloud. These automated API actions can include quarantining the email from affected users' inboxes and applying stronger authentication policies, like requiring Okta MFA.

With Okta + Proofpoint, higher education institutions can...

- Safeguard against phishing and credential-based attacks with advanced threat detection and automated remediation
- Take an adaptive, risk-based approach to help protect your most at-risk users and help prevent successful credential-phishing attacks
- Orchestrate remediation actions across email security and identity platforms to mitigate exposure to threats

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 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 6,000 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 6,100 organizations, including the University of Notre Dame, San Jose State University, St. Edward's University, Ursinus College, Oklahoma Wesleyan University, and Maryville University, trust Okta to help protect the identities of their workforces and customers.

For more information, go to okta.com