proofpoint.

INTEGRATION BRIEF

Proofpoint and CyberArk Partnership

Protect privileged users with a people-centric approach

Products

- Proofpoint Targeted Attack Protection
- Proofpoint Identity Threat Defense platform
- CyberArk Privileged Access Management Solutions

Key Benefits

- Detect and stop email threats targeting your people
- Identify your organization's Very Attacked People (VAPs)
- Discover and remediate currently vulnerable identities
- Detect active threats attempting malicious use of privileged identities
- Apply adaptive controls to high-risk privileged users for enhanced protection

Advanced targeted threats are a continuing problem. These threats are direct attacks aimed at an organization's people, many of whom have privileged access to IT systems. To secure your organization against them, you must know who your targeted privileged users are. And you need to understand them. Proofpoint and CyberArk have partnered to provide our joint customers with a people-centric approach that protects your privileged users. Together, we defend against threats to your Very Attacked People™ (VAPs) and their privileged access.

More than 90% of today's cyberthreats start with email, the No. 1 threat vector. Proofpoint Targeted Attack Protection (TAP) helps you stay ahead of attackers. It detects, analyzes and blocks ransomware and other advanced email threats that are delivered through malicious attachments, URLs or deceptive text-based messages. It also provides detailed visibility into your most attacked users.

TAP features the Proofpoint Attack Index, which aggregates the following factors to help you identify and better understand your VAPs:

- **Attacker sophistication.** This shows, for example, whether an attacker is a nation-state or an unknown actor.
- **Targeting type.** This shows, for example, whether an attack is highly targeted or a broad-based campaign.
- **Attack type.** This indicates if the attack is credential phishing, backdoor malware or something else.
- **Attack volume.** This indicates how much this person is being attacked.

Proofpoint Targeted Attack Protection can identify a malicious link when a user clicks on it inside an email. It then shares this information with CyberArk, which delivers real-time remediation by automatically disabling certain features, disabling the user completely or forcing a real-time change of password.

Proofpoint also offers the Proofpoint Identity Threat Defense platform, which detects and remediates identity-centric vulnerabilities and active threats within your organization. The platform takes a preventive approach. It stops attackers' lateral movement and privilege escalations before they can reach your most critical assets.

CyberArk is the leading provider of privileged access management (PAM). It helps organizations secure access to critical business data and infrastructure. It also protects a distributed workforce and accelerates business in the cloud. CyberArk was built on a foundation of intelligent privilege controls. It has since evolved to protect against the leading causes of breaches: compromised human and machine identities and credentials.

How the Integration Works

Protect VAPs with privileged access management

Proofpoint TAP identifies your VAPs and shares that information with CyberArk. CyberArk can then manage the privileged access of these VAPs, who have a high level of potential impact to the business.

Proofpoint Identity Threat Defense provides continuous discovery of vulnerable privileged accounts, including shadow admins. It uses auto lookup in CyberArk to indicate the accounts that are configured in the Vault and those that are not.

Revoke privileged access for potentially compromised users

Today's threat actors are more sophisticated than ever, often using advanced techniques such as time-delayed attacks. TAP rewrites every URL and provides click-time sandboxing for each of your users. TAP can identify a malicious link when a user clicks on it inside an email. It then shares this with CyberArk. With this information CyberArk delivers real-time remediation by automatically disabling certain features, disabling the user completely or forcing a real-time change of password.

Discover cached credentials

Identity Threat Defense continuously discovers cached credentials and automatically remediates them. As such, the attacker cannot freely move laterally toward your organization's crown jewels, or most critical assets. By integrating with CyberArk, our platform discovers and flags users and service accounts that do not have their credentials managed in the CyberArk Vault.

Contain and remediate attacks targeted at privileged users and high-risk assets

Proofpoint Threat Response helps you resolve threats faster and more efficiently. It enhances your security alerts with internal and external context and intelligence. And once evidence of a breach is detected (for example, if malware is installed on a privileged user's machine), Threat Response creates an alert on your dashboard. What's more, it lets you drill down to view detailed incident-related information.

Identity Threat Defense deploys deceptive privileged accounts and other deceptions across an IT environment. This sets up tripwires that prompt the security teams to detect threats and respond to them with precision. The platform uses CyberArk Secrets Manager to manage admin and host credentials as well as automated password rotation for the systems with which it communicates.

Benefits of Proofpoint and CyberArk

Proofpoint and CyberArk enhance security with layered defenses for users with privileged access. Proofpoint prevents attackers from gaining access to your users. It also helps identify the accounts that may be most at risk. CyberArk takes this insight and applies adaptive controls and policies to these high-risk privileged users. This ensures that they are accessing what they need—and nothing more.

This integration helps you:

- Stop targeted threats before they reach your people.
- Identify your VAPs and the systems they have access to.
- Keep your VAPs safe with adaptive controls.
- Decrease the risk of unwanted access to your most sensitive data and accounts.
- Streamline the response process for privileged users when a compromise is detected.

Summary

Using both Proofpoint and CyberArk solutions in tandem enhances your organization's defense against the No. 1 threat vector, privileged identities. This integrated approach streamlines your efforts and prioritizes defenses to safeguard your most critical assets.

LEARN MORE

For more information, visit proofpoint.com.