

# PROOFPOINT THREAT RESPONSE INTEGRATES WITH CYBERARK PRIVILEGED ACCOUNT SECURITY



## HIGHLIGHTS

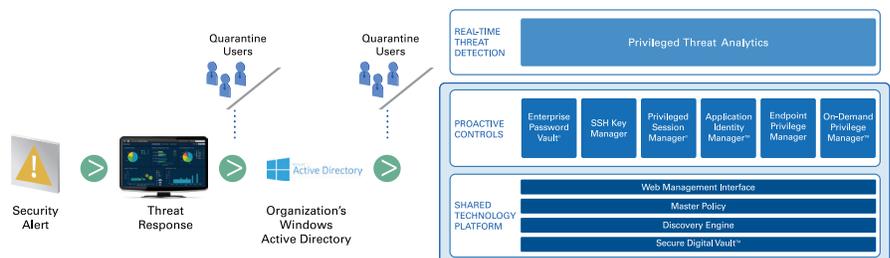
- Quickly investigate and respond to critical threats using automated controls
- Reduce the attack surface by limiting access privileges and deactivating compromised privileged accounts
- Isolate, monitor and control privileged sessions to further shrink the threat surface

Proofpoint and CyberArk are teaming up to help you quickly contain and remediate attacks that target privileged users and high-risk assets. By integrating Proofpoint Threat Response with CyberArk's Privileged Account Security Solution, you can disrupt today's most critical attacks before they cause lasting harm.

Not all security compromises are created equal. Privileged accounts have access to your most valuable resources—and may be pervasive in your IT environment. It's no wonder these valuable accounts have become a prime target in today's most harmful cyber attacks.

You can't prevent every threat. But you can stop them from growing into full-blown security breaches. Effective security means quickly prioritizing alerts for privileged accounts, investigating these critical threats, and resolving them.

Proofpoint Threat Response works with The CyberArk Privileged Account Security Solution to provide the information, insight, and tools you need to investigate, contain, and remediate threats. By combining Proofpoint threat forensics and intelligence with CyberArk's predefined response policies and controls, you can better protect your most valuable accounts and resources.



## REAL-TIME RESPONSE TO SUSPICIOUS PRIVILEGED USER ACTIVITY

Proofpoint Threat Response helps you resolve threats faster and more efficiently by enhancing security alerts with internal and external context and intelligence. It gives you the attack path and history of every alert. Every IP, domain and URL used in an attack are verified against multiple built-in premium intelligence and reputation services.

The CyberArk Privileged Account Security Solution is a unified, enterprise-class solution that helps you manage and secure privileged accounts. It helps you secure credentials, including passwords and SSH keys. It helps you control access to these accounts. And it isolates and records privileged sessions to be used for forensic analysis purposes. Built on a single platform, the solution centralizes all privileged activity for monitoring, protection and control.

Once evidence of a breach is detected (for example, if malware is installed on a privileged user's machine), Threat Response visualizes an alert on your dashboard and gives you the ability to drill down to view detailed incident-related information. Behind the scenes, Threat Response surfaces the true targets of the attack, identified by IP or email addresses, by automatically resolving their full identities. This critical step lets you act based on user identity or group membership within your Windows Active Directory.

The Proofpoint-CyberArk solution lets you decide whether to quarantine targeted accounts. It works by letting you add affected accounts to an "infected users" list. This list is synchronized with the relevant security group within Active Directory, an action you can set for specific intervals. That gives you ample time to further investigate the alert while securing access to sensitive assets. Once privileged users are quarantined, they are added to Active Directory groups with reduced or disabled permissions.

By deploying the CyberArk solution, you can provision access policies for quarantined privileged users. For example, you can block a user from accessing specific databases containing sensitive cardholder data but give them access to less sensitive databases. Based on the user group affiliation that CyberArk automatically retrieves from the Active Directory, user access to privileged credentials is allowed or denied according to your security policies.

You can implement other policies using CyberArk Privileged Session Manager, a component of the CyberArk Privileged Account Security Solution. The CyberArk Privileged Session Manager is a secure central access control point into critical systems. It serves as a secure proxy server, separating endpoints from target systems and isolating privileged sessions to help prevent the spread of malware from vulnerable quarantined users' devices to critical target systems. When privileged users are quarantined for any reason, it provides a secure path for access. It allows these users to still connect to an organization's assets, but only through CyberArk's Privileged Session Manager. All other access options are blocked. Security analysts can monitor all privileged session activity in real time and terminate the session if needed. The CyberArk solution can also capture and store privileged sessions for future auditing or analysis.

By requiring quarantined users to access critical assets through Privileged Session Manager, the CyberArk solution helps you isolate, monitor and control all privileged activity.

## SUMMARY

Integrating Proofpoint Threat Response and CyberArk Privileged Account Security Solution helps you to focus your efforts and resources on your highest-priority targets and biggest risks. The joint solution provides real-time operational insights and policy-based response capabilities for rapid risk mitigation and remediation.

## JOINT CYBERARK-PROOFPOINT SOLUTION

- Gain real-time threat insights using rich evidence collection for quick and effective investigation.
- Preconfigure policies and controls to reduce risks related to privileged users/sensitive assets.
- Isolate critical systems and quarantined user sessions to help prevent the spread of malware from vulnerable end-user devices.

### ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

### ABOUT CYBERARK

CyberArk is the only security company that proactively stops the most advanced cyber threats – those that exploit insider privileges to attack the heart of the enterprise. The company has pioneered a new category of targeted security solutions to protect against cyber threats before attacks can escalate and do irreparable business damage.

©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.