proofpoint | CYBERARK



SOLUTION BRIEF

Proofpoint + CyberArk

Protecting privileged access from the inbox to the vault.

Protect Privileged Access from the Inbox to the Vault

More than 90% of cyberthreats start with email. Many of the people being attacked hold privileged access to critical systems, and attackers who compromise a user don't stop at the inbox. They look for privileged accounts, cached credentials, and unmanaged local admins to move laterally and escalate. Security teams that treat email security and privileged access management as separate disciplines can't connect a phishing click to an exposed privileged account, and that gives attackers the time they need.

Since 2020, Proofpoint and CyberArk have connected the two sides of that path. Proofpoint's human-centric threat detection and identity threat defense share who is being attacked and which accounts are exposed. CyberArk's privileged access management restricts, disables, or rotates in response. Together, they protect privilege before it is exploited.

Know Who Attackers Target, Then Tighten Their Access

Very Attacked People (VAPs) are the individuals attackers target hardest, and many hold privileged access. Proofpoint Core Email Protection (TAP) identifies them with the Proofpoint Attack Index, which aggregates attacker sophistication, targeting type, attack type, and attack volume, then shares that risk with CyberArk.

Key Benefits

- Know which privileged users attackers are targeting and tighten their access
- Respond on a privileged account the moment its user clicks a malicious link
- Find the privileged accounts your Vault doesn't yet manage
- Run deception without exposing administrator credentials to Proofpoint

VAP Identification	Malicious-Click Response
Core Email Protection (TAP) + CyberArk Privileged Access Management Proofpoint identifies your Very Attacked People and shares the list with CyberArk through a CyberArk-built plugin. CyberArk applies adaptive controls and policies to these users, so they can access what they need and nothing more.	**Core Email Protection (TAP) → CyberArk** When TAP detects that a user clicked a malicious link, it shares the click with CyberArk, which can disable certain features, disable the user, or force a password change in real time. Proofpoint shares the signal; CyberArk performs the response.

©Proofpoint, Inc. 2026

Find the Privileged Accounts Your Vault Doesn't Manage

Privileged accounts that were never onboarded to the Vault are the ones attackers can use without resistance, so Proofpoint Identity Threat Defense continuously looks for them and checks what it finds against CyberArk.

Vault Coverage Discovery	Cached Credential Detection
Identity Threat Defense + CyberArk Vault Spotlight discovers local administrator accounts and domain user credentials across endpoints and checks each against CyberArk's list of managed accounts. Each is marked managed by CyberArk, managed by another tool such as LAPS, or unknown, and accounts managed on only some machines are flagged as partially managed.	**Identity Threat Defense + CyberArk Vault** Identity Threat Defense continuously discovers cached credentials that could let attackers move laterally toward critical assets. It checks them against the CyberArk Vault and flags users and service accounts whose credentials aren't managed there, so you can close the gap before attackers use it.

Run Deception Without Exposing Admin Credentials

Deception and forensics need administrator access to endpoints, and Proofpoint Shadow gets it from CyberArk on demand rather than asking you to hand those credentials to another security tool.

On-Demand Credential Retrieval	Nothing to Store, Nothing to Break
Proofpoint Shadow + CyberArk Secrets Manager To deploy deceptions or collect forensics on an endpoint, Shadow requests that host's administrator credentials from Secrets Manager. This works for on-premises deployments through the CyberArk Credential Provider and for SaaS deployments through the Central Credential Provider.	**Credentials Retrieved, Not Held** Customers don't expose administrator credentials to Proofpoint, and retrieved credentials aren't stored in the Proofpoint database. Operation continues when passwords rotate, and deceptions raise a high-confidence alert when an attacker engages with them.

Protect Privilege Before It Is Exploited

Each integration builds on products you already run: Proofpoint threat protection and identity threat defense on one side, CyberArk privileged access management on the other. A risk detected in the inbox or your environment triggers the right control on privilege, and Vault gaps are found before attackers find them. Together, Proofpoint and CyberArk help you protect your most attacked people, close privileged identity gaps, and connect your email, identity, and privileged access teams around the same attack.

Learn More

For more information, visit **proofpoint.com/us/partners/cyberark**

CyberArk is now part of Palo Alto Networks, and its portfolio is branded Idira.
Product names in this brief reflect the CyberArk products these integrations were built with.

proofpoint.

About Proofpoint, Inc. Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises, and millions of smaller organizations in stopping threats, preventing data loss, and building resilience across people and AI workflows. Proofpoint's collaboration and data security platform helps organizations of all sizes protect and empower their people while embracing AI securely and confidently. Learn more at **www.proofpoint.com**

Connect with Proofpoint: **LinkedIn**

Proofpoint is a registered trademark or tradename of Proofpoint, Inc. in the U.S. and/or other countries. All other trademarks contained herein are the property of their respective owners.