CYBERARK®

SOLUTION BRIEF

CyberArk Endpoint Privilege Manager Out-of-the-Box Configurations Speed Time to Value

Ride the fast lane to least privilege and close the security gap

CyberArk Endpoint Privilege Manager offers several ready-to-go policies out of the box to instantly close most crucial security gaps, improve compliance and audit readiness and lay a thorough foundation for organizations' policy set development and evolution.

With straightforward local admin removal workflow and background elevation mechanics, QuickStart's predefined set of policies, credential theft protection and anti-ransomware policy, organizations can hit the ground running, shortening Time to Value to days or even hours and significantly boost security while improving user experience and reducing load on the IT service desk.

PROBLEM

Configurability distinguishes an enterprise-grade solution from the ones targeting small and mid-market businesses. These solutions provide an abundant number of features and options that serve many needs, including diverse IT infrastructures, specialist team approaches to IT operations and security, and supporting a wide geographic presence. This can overwhelm and steer IT security admins with the unlimited configuration options, requiring significant time and resources dedicated to designing their own path to and maintaining least privilege.

SOLUTION

CyberArk Endpoint Privilege Manager offers several post-deployment configuration options available immediately upon a new set creation. Most of the configurations can be enabled with the push of a single button, while some require minimal configuration with step-by-step instructions.

Remove Local Administrators

Remove specified users or user groups from local administrator groups throughout Windows and Mac deployments. A policy allows users to justify and request elevation for unhandled applications, creating an audit trail and providing Endpoint Privilege Manager administrators with visibility into what applications users require. Those applications that are used often can be added to a policy, so they are automatically elevated for the user. This helps ensure the user experience is not impacted.

CYBERARK ENDPOINT PRIVILEGE MANAGER DEFAULT POLICIES

Remove Local Administrators

- Removes local administrators
- Provides audited elevation for unhandled applications
- Collects justifications for application use

QuickStart Policy

- Blocks known common attack vectors
- Defuse common exploitation techniques
- Elevates both UAC-aware and old non-UAC applications that require administrative privileges
- Provides discovery mechanism

Credential Theft Protection

- Protect against credential theft on the endpoint
- Places credential lures for early attack alert

Protection Against Ransomware

- Protects against data loss resulting from a ransomware attack

Restrict Unhandled Applications Access to Resources

- Defends against exploits
- Stops abuse of legitimate applications
- Breaks communication with the attacker and command-and-control servers
- Prevents network-based data encryption

QuickStart Policies

QuickStart policies help organizations extract immediate benefits from the Endpoint Privilege Manager deployment. Upon activating the QuickStart, organizations achieve immediate risk reduction by getting a head start with a least privilege management framework and establishing a foundation, streamlining IT operations and improving users' experience — all while creating an audit trail.

Credential Theft Protection

Defend credentials and credential stores and detect attacks early with credential lures placed in attackers' pathways, disarming high-impact techniques such as Golden Ticket and Golden SAML. CyberArk Endpoint Privilege Manager provides protection of credentials stored in browsers, administration tools, operating systems and others with several dozen credential defense rules that allow for more granular control when needed. Optional credential lures act as trip wires to alert administrators of an ongoing attack.

Protection Against Ransomware

CyberArk Endpoint Privilege Manager adds an additional layer of defense around sensitive data with an access control policy. Only designated content handlers are allowed access to data. The policy can work alongside other endpoint security tools but does not rely on detection and requires almost no extra resources to provide reliable and robust protection from newly surfacing strains of ransomware, blocking both data loss and extortion.

Restrict Unhandled Applications Access to Resources

This policy allows with a single push of a button to drastically reduce the area of attack and prevent many exploits and attacks by controlling access to Intranet, the Internet, network shares and other processes' memory. This effectively blocks exploitation attempts, abuse of legitimate applications, communications with the attacker and command-and-control (C&C) servers, network-based data encryption and data exfiltration.

Learn more at www.cyberark.com/epm

CYBERARK®