CYBERARK®

DATA SHEET

CyberArk® Endpoint Privilege Manager

The Challenge

When an attack evades your perimeter and endpoint security, you are reliant on detection technologies to react quickly to try and prevent it spreading. Attackers steal credentials or exploit vulnerabilities to elevate privileges and move laterally through your network to find valuable information. IT teams chose to give users local admin rights and to either not enforce least privilege whatsoever or maintain very relaxed policies, trying to prevent potential impact on user productivity and increased burden and associated costs for the desktop support team. As a result, organizations face these challenges:

- **Lost business productivity.** When organizations eliminate all privileges from business users, users may no longer be able to carry out certain tasks or use certain applications needed for their day-to-day roles. Inflexible privilege policies can bring the business to a halt.
- **High help desk costs.** When IT policies prevent business users from carrying out necessary, day-to- day tasks, users must call the help desk to restore necessary permissions. This can significantly drive up IT costs and overwhelm the support team.
- **Increased security risks due to 'privilege creep.'** Without the right tools, users tend to wrestle local admin rights back when there's a sporadic urgent need and rarely yield them back.
- **Increased risk of successful malware-based attacks.** Even if malware dos not rely on elevated privileges, without comprehensive application control policies in place attackers still can achieve their goals, compromise credentials and exfiltrate sensitive data.

The Solution

CyberArk Endpoint Privilege Manager helps remove the barriers to enforcing least privilege and allows organizations to block and contain attacks at the endpoint, reducing the risk of information being stolen or encrypted and held for ransom. A combination of Endpoint Privilege Management, Privilege Threat Protection and Application Control stops and contains damaging attacks at the point of entry. These critical protection technologies are deployed as a single agent to strengthen and harden all desktops, laptops and servers running Windows, Windows Server, macOS or Linux.

CyberArk Endpoint Privilege Manager fences off cyberattacks by removing local admin rights, elevating applications Just-In-Time while creating an audit trail and protecting security controls from tampering.

PLATFORMS & DEPLOYMENT

Microsoft Windows

- Windows 7 x32, x64
- Windows 8/8.1 x32, x64
- Windows 10 x32, x64
- Windows 11 x32, x64

Microsoft Windows Server

- Windows Server 2008 x32, x64
- Windows Server 2008 R2 x64
- Windows Server 2012/2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Apple macOS

- macOS Monterey 12

Linux

- Red Hat Enterprise Linux 7.x, 8.x
- SUSE Linux Enterprise 12,15
- Amazon Linux 2
- CentOS 7
- Ubuntu 18.04, 20.04

Deployment Options

- Software-as-a-Service

Benefits

With CyberArk Endpoint Privilege Manager, organizations are able to:

- **Remove local admin rights.** Endpoint Privilege Manager helps remove local admin rights while improving user experience and optimizing IT operations. Flexible policy-based management simplifies privilege orchestration and allows controlled Just-In-Time maintenance sessions.
- **Enforce least privilege.** Comprehensive conditional policy-based application control can help you create scenarios for every user group, from HR to DevOps. Endpoint Privilege Manager considers application context, parameters, and attributes to allow or block certain script, application or operation.
- **Allow quick adoption of least privilege by introducing JIT (Just In Time) elevation and access.** Add users to a local privilege group for a limited time, provide an audit trail on the endpoint throughout the temporary period the user had privilege rights, revoke and terminate access at the end of the session or before if required.
- **Securely manage local admin.** Protected credentials from CyberArk Enterprise Password Vault are managed locally on endpoints, on or off the network.
- **Detect and block credential theft attempts.** Credential theft plays a major part in any attack. Advanced protection helps an organization detect and block attempted theft of Windows credentials and those stored by popular web browsers.
- **Seamlessly elevate business user privileges as needed.** Once local administrator rights are removed from business users, CyberArk Endpoint Privilege Manager elevates privileges, based on policy, as required by trusted applications.
- **Quickly identify and block malicious applications.** Leveraging CyberArk's Application Risk Analysis to quickly determine risk associated with any application streamlines policy definitions and aids in preventing malicious applications from running in the environment.

SPECIFICATIONS

Flexible and Secure Application Rules:

- Executables, Dynamic-Link Libraries (dlls), Windows Applications, Scripts
- Exact, partial, wildcard and regexp matching
- File attributes, such as file name, checksum, owner, location and location type, source etc.
- Program attributes, such as product name, company name etc.
- Application context, such as launch parameters, parent process, etc.
- Granular application and child processes behavior control

Credential Protection against:

- Tampering with Endpoint Privilege Manager agent
- Browser-stored credentials and credential stores compromise
- Credential theft from IT applications
- Credential theft from remote access tools
- Suspicious actions
- Windows Credentials Harvesting

Note: certain functionality is only available for selected platforms

- **Out of the box Ransomware Protection.** OOTB policy for protection against ransomware including comprehensive least privilege controls readily tested on hundreds of thousands of ransomware samples.
- **Linux policy-based sudo management** helps eliminate manually intensive, error-prone sudo administrative processes, allowing endpoint security managers to centrally configure sudo and enforce role-specific least privilege at scale.
- **Enable unknown applications to safely run in a restricted mode.** Unknown applications, which are neither trusted nor known to be malicious, are able to run in 'Restricted Mode' which prevents them from accessing corporate resources, sensitive data or the internet.
- **Leverage integrations with threat detection tools to analyze unknown applications.** CyberArk Endpoint Privilege Manager can send unknown applications to Check Point, FireEye and Palo Alto Networks threat detection solutions for automated file analysis.

A Comprehensive Solution

CyberArk Endpoint Privilege Manager is part of the broader CyberArk Identity Security Platform, a complete solution designed to proactively protect against advanced attacks that exploit administrative privileges to gain access to the enterprise's heart, steal sensitive data, and damage critical systems. The solution helps organizations reduce the attack surface by eliminating unnecessary local administrator privileges and strengthening privileged accounts' security. Products in the solution can be managed independently, or combined for a cohesive and comprehensive privileged account security solution.

CYBERARK®

AICPA SOC

SOC 2 Type 2 compliant