CYBERARK

DATA SHEET

ENDPOINT PRIVILEGE MANAGER

Enforce privilege security on desktops, laptops and servers without the negative impact of removing local administrator rights that flood the IT helpdesk.

View all privilege policies, applications and application reputations in a single location.

Platforms & Deployment

Windows Desktop:

- MS Windows XP 32 bit Service Pack 3
- MS Vista 32/64 bit Service Pack 1
- MS Windows 7 32/64 bit
- MS Windows 8 and 8.1 32/64 bit
- MS Windows 10

Windows Server:

- MS Windows Server 2003 32/64 bit
- MS Windows Server 2008 32/64 bit
- MS Windows Server 2008 R2
- MS Windows Server 2012
- MS Windows Server 2012 R2
- MS Windows Server 2016
- MS Windows Server 2019

Mac

- High Sierra 10.13
- Mojave 10.14
- Catalina 10.15

Deployment Options

- On-premises server
- Software-as-a-Service

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 to elevate privileges and move laterally through your network to find valuable information. Enforcing privilege security on the endpoint reduces your attack surface, is a fundamental part of your security program and hardens desktops, laptops and servers resulting in lower risk of a breach and potential damage to the business. However, the downside is a potential impact on user productivity and an increased burden and associated costs for the desktop support team.

To effectively reduce the attack surface and mitigate the risk of a serious data breach without impacting productivity, organizations should implement tools that enforce privilege security on the endpoint to block and contain attacks. They should enforce flexible least privilege policies for business and administrative users, control what applications are allowed to run and ensure that they can detect and block attacks on what is often the first target – credentials. Without such tools in place, organizations will face 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.'** When organizations remove all privileges from business users, the IT team will occasionally need to re-grant privileges for specific tasks. However, once privileges are re-granted, they are rarely revoked which reopens the security loophole associated with excessive administrative rights.
- **Increased risk of successful malware-based attacks.** Organizations that minimize user privileges on Windows and macOS devices can still be vulnerable to malware that does not need privileges to run. Without complementary tools in place to control which applications are permitted to run and protect the attackers main goal, credentials, attackers can successfully use malware-based attacks to gain a foothold into the organization.

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 privilege management, targeted Privilege Threat protection and application control stops and contains damaging attacks at the endpoint of entry. Unknown applications run in a restricted mode to contain threats and Privilege Threat protection blocks credential theft attempts. These critical protection technologies are deployed as a single agent to strengthen and harden all desktops, laptops and servers.

CyberArk Endpoint Privilege Manager also enables security teams to enforce granular least privilege policies for IT administrators, helping organizations effectively segregate duties on Windows servers. Complementing these privilege controls, the solution also delivers application controls designed to manage and control which applications are permitted to run on endpoints and servers.

With CyberArk Endpoint Privilege Manager, organizations are able to:

- **Automatically create policies based on business requirements.** Create application control and privilege elevation policies based on Trusted Sources such as SCCM, software distributors, updaters, URL and more. Policy Templates enable quick implementation for specific server types such as Microsoft SQL Server saving time and closing gaps in privilege security policies for all user roles.

Specifications

Comprehensive Application Support:

- PKG
- DMG
- REST API's support
- Executable
- MSI, MSU
- Administrative Tasks
- Management console snap-ins
- Scripts
- Registry settings
- ActiveX controls
- COM objects
- Web Applications

Flexible and Secure Application Rules:

- File path matching
- Command line matching
- File hashing (SHA-1)
- Product and file information
- Trusted publisher
- Trusted Source SCCM
- Trusted Software Distribution system
- Trusted Updater
- Trusted Network
- Trusted AD group
- Trusted product
- Trusted URL

Credential Protection for:

- Git, Opera Browser and DbVisualizer
- Pass The Hash Attack
- Kerberos Ticket Hash Harvesting
- PuTTy
- Okta AD Agent
- Windows Credential Manager
- Local Security Authority (LSA)
- Local Security Authority Subsystem Service (LSASS)
- Security Account Manager (SAM)
- Domain Credentials Cache (msvcachedv2)
- AD Directory Data Store (NTDS.dit)
- Virtual Secure Module (including in Safe Mode)
- Crypto RSA Machine Keys
- AWS Keys
- Internet Explorer
- Microsoft Edge
- Chrome
- Firefox
- SQL Server Management Studio (SSMS)
- Quest Toad
- Remote Desktop Connection Manager
- FileZilla
- MRemoteNG

Note: some functionality may not be available with all deployment and OS options

- **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.
- **Enforce granular least privilege policies for Windows administrators.** Security teams granularly control which commands and tasks each IT administrator is permitted to execute on Windows Servers based on role.
- **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.
- **Out of the box Ransomware Protection.** OOTB policy definition for protection against ransomware including comprehensive least privilege controls readily tested on hundreds of thousands of malware samples.
- **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.

Benefits

- Provide a critical layer of protection when an attack evades traditional perimeter and endpoint security controls
- A unique combination of technologies, to protect against, block and contain attacks on the endpoint, reducing potential damage to the business
- Strengthen the protection and detection capabilities of your existing endpoint security
- Enables the desktop team to easily implement security policy, with minimal impact on the business
- Prevents users installing unsanctioned applications and causing workstation instability, resulting helpdesk calls and increased support costs
- Enables removal of business users with local administrator rights without reduced user productivity and increased helpdesk calls
- Secure and rotate local administrator password regardless of endpoint location
- Easy deployment with automated policy creation, and OOTB policy templates eases the burden on the desktop IT team and standalone agent enables support on airgap networks
- Helps the desktop team to meet the requirements of the security / risk management team while reducing their workload
- Contains the spread of malware across the network, reducing remediation time and effort

A Comprehensive Solution

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