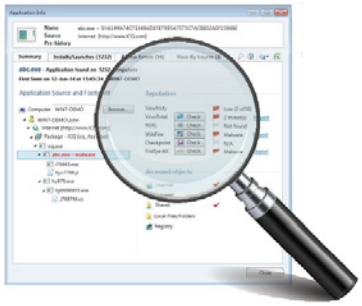
Endpoint Privilege Manager

Enforce privilege security on the endpoint without the negative impact of removing local administrator rights.



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

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, elevate privileges and move laterally through your network to find valuable information. Enforcing privilege security on the endpoint to reduce your attack surface is a fundamental part of your security program. 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 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 security and application control reduces the risk of malware infection. Unknown applications run in a restricted mode to contain threats and behavioral analysis blocks credential theft attempts. These critical protection technologies are deployed as a single agent to strengthen existing endpoint security.

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 and more.
- **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.
- **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.** Automatically compare unknown applications to commercially available blacklist databases, such as VirusTotal and NSRL, to quickly identify known malware and update global policies to prevent these applications from running in the environment.
- **Detect and block credential theft attempts.** Credential theft plays a major part in any attack. Behavioral analysis helps an organization detect and block attempted theft of Windows credentials and those stored by popular web browsers.
- **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.
- **Identify all applications in the environment.** Using an agent on each protected machine, the solution can immediately locate all instances of an application within the environment, and the origin of each.

Benefits

- Provides an additional 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 local administrator rights without reduced user productivity and increased helpdesk calls
- Easy deployment with automated policy creation eases the burden on the desktop team
- ·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 Account 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.

Specifications

Supported Platforms:

Windows Desktop:

- Windows 7 32-bit & 64-bit
- Windows 8 32-bit & 64-bit
- Windows 8.1 32-bit & 64-bit
- Windows 10

Windows Server:

- Windows Server 2008 32-bit & 64-bit
- Windows Server 2008 R2 64-bit
- Windows Server 2012
- Windows Server 2012 R2

Comprehensive Application 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 Computer image
- Trusted AD group
- Trusted product

Deployment Options:

- Microsoft Group Policy (GPO)
- On-premises server
- Software-as-a-Service

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