CYBERARK®

EBOOK

The Buyer's Guide to Managing Endpoint Privileges

Defending Against Ransomware and Other Pervasive Threats

Table of Contents

Introduction

Organizations need a way to empower their users and admins to go about their duties without compromising security and opening gaps for cyber criminals. Endpoint privilege managers can help.

Why manage privileges on the endpoints?

Privileged endpoint accounts like Microsoft Windows, MacOS and Linux administrator accounts are a common target for threat actors. Once adversaries gain access to privileged accounts they can traverse a network, taking over workstations, servers and other critical parts of the infrastructure. Attackers and cybercriminals often exploit privileged endpoint accounts to:

- Alter configurations
- Completely disable threat detection and antivirus programs, or disaster recovery tools
- Launch ransomware and other malware
- Steal confidential data

Cyber attacks can lead to business disruptions, revenue loss and regulatory fines. The average total cost of a data breach is $4.24 million.[1] And most cyber attacks begin at the endpoint.

Nearly 70% of organizations experience one or more endpoint breaches a year.[2] Endpoint privilege managers help mitigate cyber risk by providing foundational endpoint security controls, locking down endpoint privileges and improving application governance.

The average total cost of a data breach is $4.24 million.[1]

[1] IBM Security Cost of a Data Breach Report 2021
[2] The Third Annual Study on the State of Endpoint Security Risk, Ponemon Institute, January 2020

Choosing the Right Endpoint Privilege Manager

Endpoint privilege managers (EPMs) are the cornerstones of an endpoint security stack. They improve security and reduce risk by removing local admin rights from endpoints, enforcing least privileges, preventing credential theft and privilege abuse, and containing cyber attacks. Endpoint privilege managers reduce vulnerabilities by granting the right people and applications the right level of access to the right resources at the right time. And they simplify compliance by making it easy to enforce and audit endpoint privilege policies.

When it comes to endpoint privilege managers, not all products are the same. A complete solution:

- **Helps remove local admin rights** without impacting user experience and creating operational bottlenecks.
- **Enforces the principle of least privilege** to reduce endpoint vulnerabilities and shrink attack surfaces.
- **Supports smart (conditional) rules-based application control** to defend against unknown malware variants without impairing legitimate applications.
- **Includes comprehensive administrative reports and dashboards** to improve oversight, increase visibility, and streamline compliance audits and forensics investigations.
- **Offers additional capabilities like** credential theft protection, privilege deception and threat analysis functionality to further reduce risk and exposure.

This buyer's guide reviews the key capabilities of an endpoint privilege manager and provides tips for evaluating products and selecting the right tool for your business.

Evaluation Criteria

1 Removing local admin rights

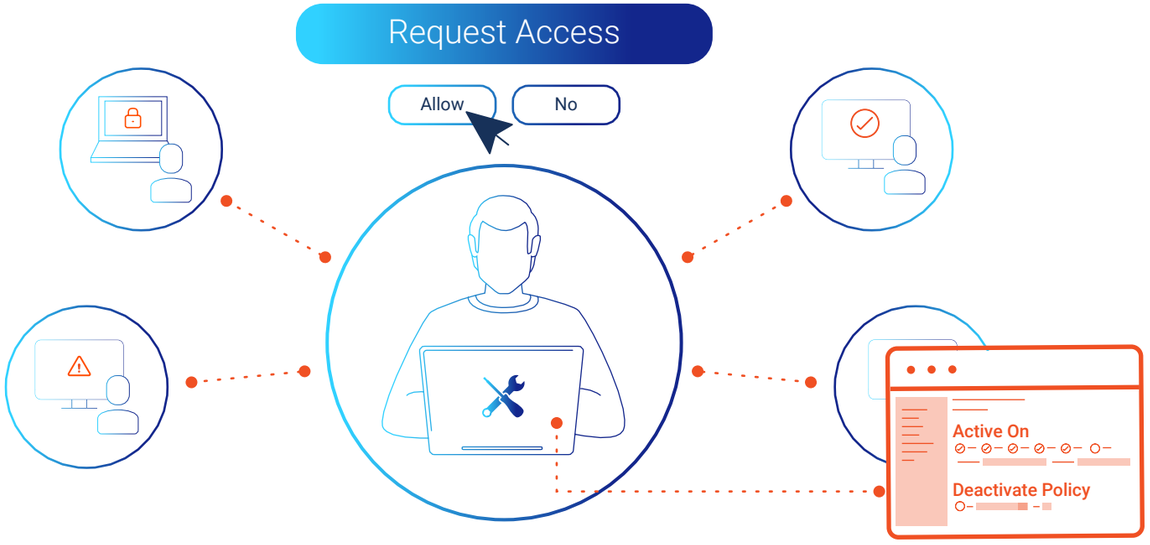
Removing local admin rights as a security measure is not going to be a revelation to anybody even remotely associated with IT. Restricting users to work under standard user accounts has a profound positive impact on security. But without the right tools and planning, removing local admin rights can profoundly impair the user experience. Far too many IT departments hastily remove local admin rights only to face an immediate backlash from angry users — stories range from comic to catastrophic. Once bitten and twice shy, some IT folks even go as far as to say that removing local admin rights hurts an organization more than it helps it. And those who are not that radical probably had some different experiences based on their setup — maybe they just spend their day remoting into user machines to install a font or a printer, update a program or change the time zone. Or maybe they tried to force their way onto the users and eventually had to budge and give the local admin rights back.

All of this can really be solved by a well-rounded endpoint privilege manager, which can remove local admin rights and then, based on policies, elevate certain programs or tasks in a transparent manner so a user would never see a prompt or need to ask IT for assistance. And if they have some special case, they can request elevation, which can be approved without ever remoting to the machine. On the backend, a good endpoint privilege manager would even integrate with an IT ticketing system for smooth workflows and fast elevations.

2 Least privilege enforcement

Endpoint privilege managers grant end users the minimum set of privileges they need to perform a task — a concept known as the principle of least privilege. By removing local admin rights from standard user accounts and elevating user privileges only when absolutely required, endpoint privilege managers help reduce endpoint security vulnerabilities and prevent ransomware and other threats.

Most endpoint privilege managers support Just-in-Time (JIT) privilege elevation, escalating privileges for a prescribed length of time to allow end users to install applications or reconfigure endpoint settings. Best-of-breed solutions support automated workflows that enable on-demand privilege elevation without impairing the user experience or burdening support teams. Leading solutions also provide APIs to integrate permission request and approval processes into help desk workflows or other IT operations systems.



EPM solutions are the cornerstone of an endpoint security stack.

Managing endpoint privileges is foundational

Endpoint security should begin with privilege management. Most adversaries exploit privileged accounts to orchestrate attacks. An endpoint privilege manager is central to the endpoint security stack and underpins other endpoint threat detection and mitigation tools.

Endpoint detection and response (EDR) solutions and other endpoint security products identify and block malware and other threats. They aren't designed to prevent privilege abuse. Endpoint privilege managers are specifically designed to lock down privileged accounts and tightly control the applications privileged accounts can run and the resources they can access. Endpoint privilege managers serve as the first and most important line of endpoint defense, stopping attackers at their point of entry, working in concert with other endpoint security products to block, contain and remediate threats.

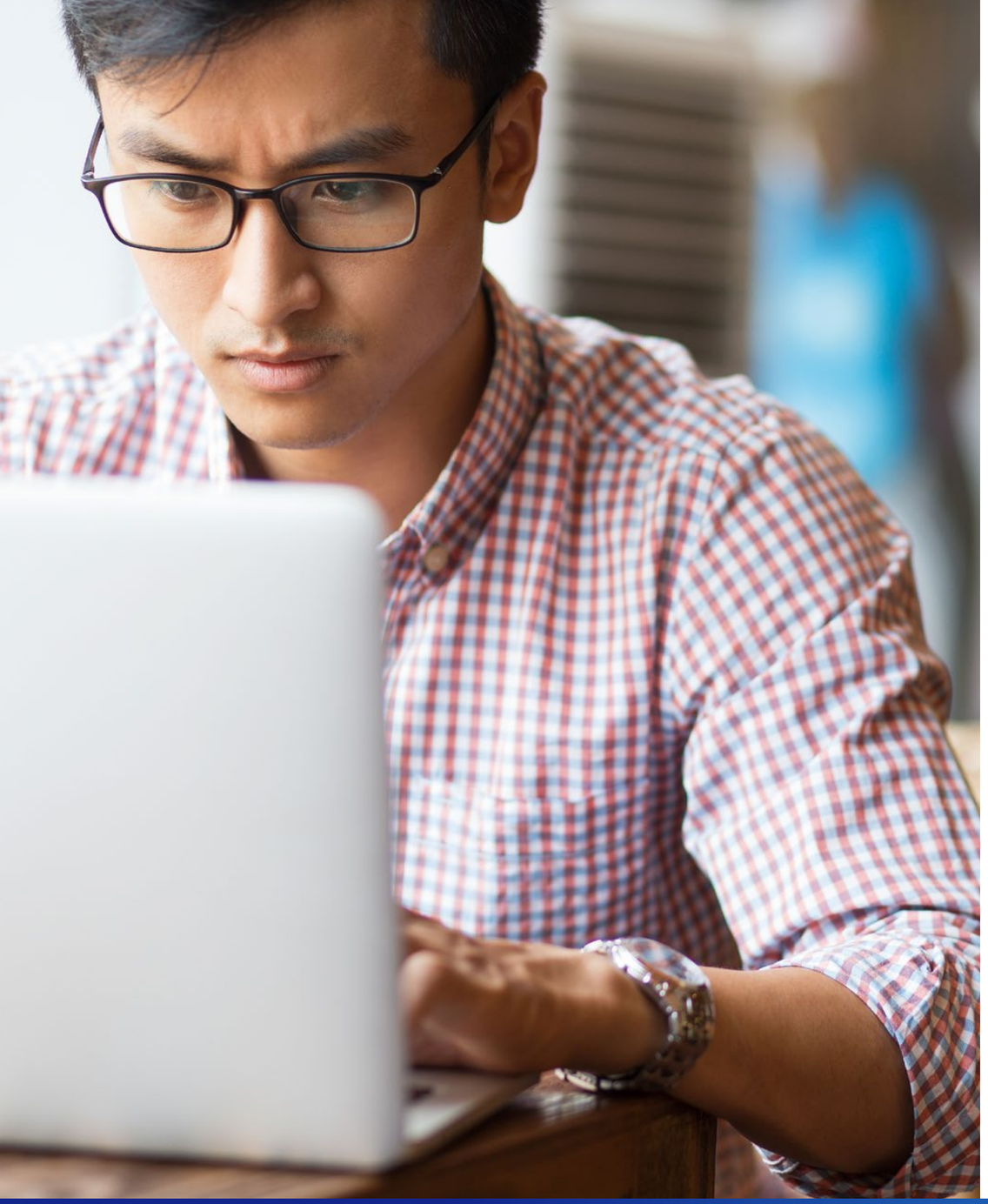
3 Conditional application control

Most endpoint privilege managers let you denylist applications to prevent known malware from running (or allowlist applications to allow only trusted applications to run). Denylisting is helpful for detecting and blocking previously identified malware samples, but it is not all that effective at defending against modern and constantly evolving threats like ransomware. (Every day, cyber criminals introduce thousands of new ransomware variants into the wild. Left alone, each individual threat can be packaged and repackaged to avoid list-based detections).

Allowlisting and denylisting can also be quite challenging to implement and maintain because business software constantly evolves. Leading endpoint privileged managers let you keep pace with change by controlling execution permissions based on a variety of parameters, such as file attributes, digital signature, location, source, update server or reference image. For example, only allow an application delivered by designated “trusted updater” programs.

Best-in-class endpoint privilege managers let you implement conditional policies to block attacks involving trusted applications. For example, you could create a rule that would allow users to launch PowerShell with certain parameters. But then create another rule that would prevent other apps from launching PowerShell as a child process, thus eliminating chained exploit techniques.

Leading endpoint privilege managers support application greylisting to help you defend against unknown malware variants without impeding the operation of unknown applications that pose no known security risks. Greylist policies apply to applications that aren’t explicitly allowlisted nor denylisted. Leading solutions include pre-built policies that provide out-of-the-gate protection against ransomware and other advanced threats.



4 Administrative reports and dashboards

Most endpoint privilege managers provide monitoring and reporting capabilities to help administrators improve visibility, track user and application behavior, and support compliance audits and forensics investigations. Most solutions offer administrators canned reports indicating which endpoints and applications are protected and the specific policies and business rules enforced. Some also offer historical reports to help administrators track the status of endpoint privilege management deployments and coverage and demonstrate progress to executives and compliance auditors.

Many solutions also include privileged management, application activity and threat intelligence reports to help information security team keep taps on suspicious behavior and streamline compliance and forensics activities. Leading endpoint privilege managers generate detailed event messages whenever a policy is invoked and include dashboards and tools for observing and exploring policy-use events and statistics (aka policy audit).

151%

Ransomware attacks increase in the first half of 2021.[3]

$4.62 million

Average total cost of a ransomware breach.[4]

Endpoint privilege managers reduce ransomware-related risks

Ransomware is arguably today's most pervasive and destructive cyber threat. Ransomware attacks can damage your company's reputation and paralyze your business. It can take weeks or even months to recover from a ransomware attack, even if you decide to pay the ransom.

Ransomware attacks typically begin by targeting endpoints like Windows PCs and Macs, using phishing schemes, malware downloaders, stolen credentials or known vulnerabilities to penetrate systems. Once an attacker gains access to an endpoint, they can traverse the network, using elevated privileges to spread malware and encrypt files on high-value targets like Windows servers and Linux servers.

Endpoint privilege managers provide foundational endpoint security controls that are fundamental for preventing ransomware. When deployed as part of a comprehensive endpoint security strategy, the right endpoint privilege manager can help you contain attacks and prevent ransomware from spreading across your business by restricting endpoint privileges on both desktops and servers, defending against credential theft and abuse, and containing vertical and lateral movement. Best-of-breed endpoint privilege managers let you prevent unhandled applications from accessing sensitive data. So even if ransomware slips through your defenses, you can still prevent encryption and limit damage.

[3] Seals, Tara. "Ransomware Volumes Hit Record Highs as 2021 Wears On." www.threatpost.com. August 3, 2021.
[4] IBM, Ponemon Institute. "Cost of a Data Breach Report." 2021

5 Credential theft protection and privilege deception

There are some leading-edge capabilities only provided by the most advanced endpoint privilege managers: credential theft protection and privilege deception.

Credential theft plays a major role in most cyber attacks. Credentials cached by the Windows operating system, web browsers, password managers and single sign-on (SSO) solutions are common targets for threat actors. Adversaries use stolen passwords to gain illicit entry to the network and services, move laterally and perpetrate attacks against high-value targets.

Windows server identity stores are common targets for attackers. For example, an attacker might target the Microsoft Active Directory Data Store (NTDS.dit) to harvest user hashes as the first step in a Golden Ticket attack. Or an adversary might target an identity management solution to harvest RSA private encryption keys as the first step in a Golden SAML attack.

Advanced endpoint privilege managers automatically detect and block the actions threat actors typically take to steal credentials cached by Windows, web browsers, password managers, SSO programs or other applications.

Best-in-class endpoint privilege managers also provide privilege deception capabilities to attract and throw off would-be attackers. They let you create fake “honeypot” accounts with bait usernames, such as admin2, and intentionally weak passwords to lure attackers, track their actions and foil their efforts.

Endpoint Privilege Manager Checklist

Not all endpoint privilege managers are the same. Product features and capabilities vary significantly from vendor to vendor. When evaluating an endpoint privilege manager, look for a solution that

- Removes local admin rights on Windows workstations, Windows servers, Linux servers and Macs to defend against ransomware and vulnerability exploitations in general
- Supports JIT privilege escalation for a prescribed length of time to let users update software, make configuration changes or perform other actions requiring administrative privileges
- Automates privilege escalation requests to improve the user experience and reduce help desk burdens
- Tightly controls application permissions and actions based on context to limit areas of attack and prevent software abuse
- Comes with pre-defined policies to simplify deployment and accelerate time to value
- Includes administrative reports and dashboards to improve visibility and streamline compliance and forensics
- Automatically detects and blocks attempts to steal credentials cached by Windows, browsers, password managers and SSO solutions
- Provides decoy privileged accounts to lure, detect and block attackers at the point of entry before they can do harm

Conclusion

Endpoint privilege managers are the cornerstone of the modern endpoint security stack and are fundamental for protecting against ransomware and other contemporary threats.

Best-of-breed endpoint privilege managers can help you:

- **Remove local admin rights** without impacting user experience and creating operational bottlenecks
- **Defend against attacks** by protecting against threats targeting and originating on endpoints
- **Drive operational efficiencies** by hardening endpoints without impacting workforce productivity
- **Enable the digital business** by allowing more user independence without jeopardizing security
- **Satisfy audit and compliance requirements** by making it easy to enforce and demonstrate policies

Endpoint privilege managers can help you strengthen security, reduce risk and improve user experience by giving the right people and applications the right access to the right resources at the right time.

Next Steps

CyberArk Endpoint Privilege Manager strengthens endpoint security without complicating IT operations or impairing the user experience. The solution reduces endpoint security vulnerabilities by removing local admin rights from endpoints and temporarily elevating end-user privileges on demand, in real time, with little or no help desk involvement.

CyberArk Endpoint Privilege Manager™ blocks ransomware by tightly controlling application permissions based on fine-grained, conditional business rules, offering built-in 100% protection against more than 3 million strains of malware. The solution also defends against credential theft by safeguarding credential stores, helping to contain attackers and reduce blast radius.

CyberArk Endpoint Privilege Manager protects Windows, Windows Server, MacOS and Linux endpoints and is available as Software-as-a-Service (SaaS) solution for ultimate simplicity and agility.

We hope you've found this buyer's guide useful as you evaluate evaluate your organization's needs.

Learn how CyberArk Endpoint Privilege Manager can help your business stop ransomware and other modern threats.

LEARN MORE

CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blogs or follow us on Twitter via @CyberArk, LinkedIn or Facebook.

U.S., 02.22 Doc: TSK-864

CYBERARK®