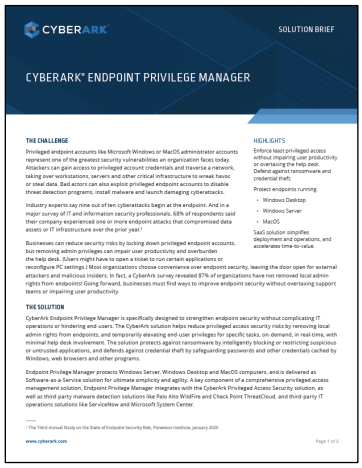
CYBERARK®

SOLUTION BRIEF

CYBERARK® ENDPOINT PRIVILEGE MANAGER

THE CHALLENGE

Privileged endpoint accounts like Microsoft Windows or MacOS administrator accounts represent one of the greatest security vulnerabilities an organization faces today. Attackers can gain access to privileged account credentials and traverse a network, taking over workstations, servers and other critical infrastructure to wreak havoc or steal data. Bad actors can also exploit privileged endpoint accounts to disable threat detection programs, install malware and launch damaging cyberattacks.

Industry experts say nine out of ten cyberattacks begin at the endpoint. And in a major survey of IT and information security professionals, 68% of respondents said their company experienced one or more endpoint attacks that compromised data assets or IT infrastructure over the prior year.[1]

Businesses can reduce security risks by locking down privileged endpoint accounts, but removing admin privileges can impair user productivity and overburden the help desk. (Users might have to open a ticket to run certain applications or reconfigure PC settings.) Most organizations choose convenience over endpoint security, leaving the door open for external attackers and malicious insiders. In fact, a CyberArk survey revealed 87% of organizations have not removed local admin rights from endpoints! Going forward, businesses must find ways to improve endpoint security without overtaxing support teams or impairing user productivity.

THE SOLUTION

CyberArk Endpoint Privilege Manager is specifically designed to strengthen endpoint security without complicating IT operations or hindering end-users. The CyberArk solution helps reduce privileged access security risks by removing local admin rights from endpoints, and temporarily elevating end-user privileges for specific tasks, on demand, in real-time, with minimal help desk involvement. The solution protects against ransomware by intelligently blocking or restricting suspicious or untrusted applications, and defends against credential theft by safeguarding passwords and other credentials cached by Windows, web browsers and other programs.

Endpoint Privilege Manager protects Windows Server, Windows Desktop and MacOS computers, and is delivered as Software-as-a-Service solution for ultimate simplicity and agility. A key component of a comprehensive privileged access management solution, Endpoint Privilege Manager integrates with the CyberArk Privileged Access Security solution, as well as third-party malware detection solutions like Palo Alto WildFire and Check Point ThreatCloud, and third-party IT operations solutions like ServiceNow and Microsoft System Center.

[1] The Third Annual Study on the State of Endpoint Security Risk, Ponemon Institute, January 2020

www.cyberark.com

Page 1 of 2

HIGHLIGHTS

Enforce least privileged access without impairing user productivity or overtaxing the help desk. Defend against ransomware and credential theft.

Protect endpoints running:

- Windows Desktop
- Windows Server
- MacOS

SaaS solution simplifies deployment and operations, and accelerates time-to-value.

CyberArk Endpoint Privilege Manager

Thank you for downloading this CyberArk Solution Brief. Carahsoft is the distributor for CyberArk cybersecurity solutions available via GSA, CMAS, MHEC, and other contract vehicles.

To learn how to take the next step toward acquiring CyberArk's solutions, please check out the following resources and information:

For additional resources:
carah.io/CyberArkResources

For upcoming events:
carah.io/CyberArkEvents

For additional CyberArk solutions:
carah.io/CyberArkSolutions

For additional cybersecurity solutions:
carah.io/cybersolutions

To set up a meeting:
Cyber-Ark@carahsoft.com
703-871-8548

To purchase, check out the contract vehicles available for procurement:
carah.io/CyberArkContracts

For more information, contact Carahsoft or our reseller partners:
Cyber-Ark@carahsoft.com | 703-871-8548

SOLUTION BRIEF

CYBERARK® ENDPOINT PRIVILEGE MANAGER

THE CHALLENGE

Privileged endpoint accounts like Microsoft Windows or MacOS administrator accounts represent one of the greatest security vulnerabilities an organization faces today. Attackers can gain access to privileged account credentials and traverse a network, taking over workstations, servers and other critical infrastructure to wreak havoc or steal data. Bad actors can also exploit privileged endpoint accounts to disable threat detection programs, install malware and launch damaging cyberattacks.

Industry experts say nine out of ten cyberattacks begin at the endpoint. And in a major survey of IT and information security professionals, 68% of respondents said their company experienced one or more endpoint attacks that compromised data assets or IT infrastructure over the prior year.[1]

Businesses can reduce security risks by locking down privileged endpoint accounts, but removing admin privileges can impair user productivity and overburden the help desk. (Users might have to open a ticket to run certain applications or reconfigure PC settings.) Most organizations choose convenience over endpoint security, leaving the door open for external attackers and malicious insiders. In fact, a CyberArk survey revealed 87% of organizations have not removed local admin rights from endpoints! Going forward, businesses must find ways to improve endpoint security without overtaxing support teams or impairing user productivity.

HIGHLIGHTS

Enforce least privileged access without impairing user productivity or overtaxing the help desk. Defend against ransomware and credential theft.

Protect endpoints running:

- Windows Desktop
- Windows Server
- MacOS

SaaS solution simplifies deployment and operations, and accelerates time-to-value.

THE SOLUTION

CyberArk Endpoint Privilege Manager is specifically designed to strengthen endpoint security without complicating IT operations or hindering end-users. The CyberArk solution helps reduce privileged access security risks by removing local admin rights from endpoints, and temporarily elevating end-user privileges for specific tasks, on-demand, in real-time, with minimal help desk involvement. The solution protects against ransomware by intelligently blocking or restricting suspicious or untrusted applications, and defends against credential theft by safeguarding passwords and other credentials cached by Windows, web browsers and other programs.

Endpoint Privilege Manager protects Windows Server, Windows Desktop and MacOS computers, and is delivered as Software-as-a-Service solution for ultimate simplicity and agility. A key component of a comprehensive privileged access management solution, Endpoint Privilege Manager integrates with the CyberArk Privileged Access Security solution, as well as third-party malware detection solutions like Palo Alto WildFire and Check Point ThreatCloud, and third-party IT operations solutions like ServiceNow and Microsoft System Center.

[1] The Third Annual Study on the State of Endpoint Security Risk, Ponemon Institute, January 2020

WHY CYBERARK

CyberArk (NASDAQ: CYBR) is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security solutions for any identity – human or machine – across business applications, distributed workforces, hybrid cloud workloads, and throughout DevOps pipelines. The world's leading organizations trust Cyberark to help secure their most critical assets. To learn more about CyberArk, visit www.cyberark.com.

HOW IT WORKS

CyberArk Endpoint Privilege Manager includes an agent component that runs on protected endpoints, and a centralized administrative console that authorized IT and security operations professionals use to oversee the Endpoint Privilege Manager implementation, configure privileged access security settings and policies, monitor endpoint security events and statistics, and terminate suspicious applications and processes.

Just-in-Time Privilege Elevation

With Endpoint Privilege Manager, IT organizations can remove local admin rights from endpoints and dynamically escalate privileges for a predefined period of time to allow end-users to install or run applications or reconfigure endpoint settings. End-users can request elevated privileges on-demand, directly from the Endpoint Privilege Manager agent. Requests are approved interactively by authorized administrators or automatically based on policy.) REST APIs make it easy to automate workflows and integrate seamlessly with helpdesk systems or other IT operations solutions.

Ransomware Protection and Application Control

Endpoint Privilege Manager protects against ransomware by tightly controlling how applications run—allowing trusted applications to run normally, blocking malicious software, and forcing unknown applications to run in a restricted mode with no access to the enterprise network. The solution integrates with the complimentary CyberArk Application Risk Analysis Service as well as a variety of third-party threat analysis solutions to intelligently identify malicious applications.

Credential Theft Protection and Privilege Deception

Endpoint Privilege Manager automatically detects and blocks attempts to steal credentials cached by Windows, web browsers, password managers, single sign-on solutions and other programs, preventing attackers from gaining a foothold for lateral movement. The CyberArk solution also creates deceptive privileged accounts (i.e. honeypots) to lure and contain attackers at the point of entry, before they can do harm.

BENEFITS

- **Strengthen security and reduce vulnerabilities** by granting the right people the right access privileges to the right resources at the right time, helping enforce the principle of least privilege.
- **Streamline IT and security operations and free up staff** by automating manually intensive, time-consuming administrative tasks.
- **Optimize user productivity and satisfaction** by allowing end-users to request privileges—quickly and easily—without engaging the help desk.
- **Improve security posture and mitigate risk** by defending against ransomware.
- **Protect and extend investments** by leveraging CyberArk Privilege Access Security and third-party security and IT operations solutions integrations.