CYBERARK

SOLUTION BRIEF

BETTER TOGETHER: CYBERARK ENDPOINT PRIVILEGE MANAGER + EDR/NGAV SOLUTIONS

HIGHLIGHTS

Deploy CyberArk Endpoint Privilege Manager in combination with Endpoint Detection & Response and Next-Generation Antivirus solutions as part of a defense-in-depth security strategy.

- Adopt an assume-breach mentality
- Lock-down privileges
- Defend against ransomware and zero-day exploits
- Identify anomalous activity
- Prevent lateral movement
- Mitigate risk and exposure

THE CHALLENGE

In today's digital world, PCs, Macs, and servers are all vulnerable to a variety of sophisticated cyberattacks. Inadequately protected endpoints provide an entry point for threat actors to penetrate your network, steal data, and take down critical applications and infrastructure. Endpoint-originated attacks and malware can disrupt your business, damage your company's reputation and lead to steep regulatory fines and costly lawsuits. In today's world it is not so much a question of if a breach will happen, but when. Yet many IT planners underestimate endpoint security risks, leaving the door open for attackers.

THE SOLUTION

Forward-looking organizations are taking a defense-in-depth approach to endpoint security, implementing a combination of proactive and reactive endpoint security controls to defend against advanced threats and contain adversaries when they do penetrate defenses. CyberArk Endpoint Privilege Manager is speci ically designed to help you reduce endpoint vulnerabilities, isolate threats, and mitigate risk as part of a defense-in-depth strategy.

Conceived with an assume-breach mindset, CyberArk Endpoint Privilege Manager enforces least privilege security and application controls at the endpoint, helping contain attackers at the point of entry, before they can traverse your network and inflict serious damage. You can use the CyberArk solution in conjunction with Endpoint Detection and Response (EDR) solutions and Next-Generation Antivirus (NGAV) solutions to defend against ransomware and other forms of malware, mitigate advanced persistent threats, and stop adversaries before they can move laterally and wreak havoc.

CyberArk Endpoint Privilege Manager Overview

CyberArk Endpoint Privilege Manager helps strengthen endpoint security without complicating IT operations or hindering end-users. The solution reduces privileged access security risks by removing local admin rights from endpoints, and temporarily elevating end-user privileges on-demand, in real-time, with minimal help desk involvement. CyberArk Endpoint Privilege Manager also protects against ransomware and other types of malware by intelligently blocking or restricting suspicious or untrusted applications. And it defends against credential theft by safeguarding passwords and other secrets

cached by Windows, web browsers, and other programs. The solution protects Windows Server, Windows Desktop, and MacOS computers, and is delivered as Software-as-a-Service (SaaS) solution for ultimate simplicity and agility.

Endpoint Detection and Response Solution Overview

Endpoint detection and response solutions let you intelligently identify and mitigate suspicious activity on endpoints. Most EDR solutions continuously monitor, record, and analyze endpoint activities, helping you efficiently detect and mitigate advanced threats. Many EDR solutions use artificial intelligence (AI) and machine learning (ML) to identify patterns symptomatic of malicious activity. EDR tools provide visibility into suspicious endpoint behavior in real-time so you can respond to advanced threats before they can take root and spread across the enterprise.

Next-Generation Antivirus Solution Overview

Antivirus programs help detect and remove harmful software from endpoints. Next-generation antivirus protection solutions use advanced analytics to defend against zero-day exploits and other advanced forms of malware that can evade conventional signature-based antivirus programs. Unlike traditional antivirus solutions that scan files looking for known patterns, NGAV solutions take a holistic approach, examining every process running on an endpoint, using AI and ML to intelligently detect and proactively block previously unknown forms of malware as well as fileless (malware-free) exploits.

WHY CYBERARK

CyberArk 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.

The table below compares the key functions of CyberArk Endpoint Privilege Manager and typical EDR and NGAV solutions. You can use all three solutions as part of a defense-in-depth strategy to maximize your endpoint security posture and minimize risk and uncertainty.

	Endpoint Privilege Manager	EDR	NGAV
Enforce least privilege (remove local admin rights)	Y		
Just -in-time-privilege escalation	Y		
Application control (restrict application usage)	Y		
Command control (restrict command execution rights)	Y		
Credential management and theft protection	Y		
Privilege Deception capabilities	Y		
Ransomware/malware protection	Y	Y	Y
Monitor and analyze endpoint behavior in near-real-time using AI and ML		Y	
Intelligently identify anomalous and suspicious behavior		Y	
Provide remediation guidance		Y	
Identify and block advanced threats, including fileless attacks and zero-day exploits	Y		Y
Combine AI and ML to increase the security posture	Y		Y