Reducing the risk and impact of ransomware

The massive shift to remote working has increased vulnerabilities and risk as people, processes, and technology controls are targeted by cyber attackers. This new way of working has created even more opportunities for attackers to exploit common control gaps and move laterally through an environment to deploy ransomware. Targeting critical infrastructure, operations, and sensitive data is not only potentially devastating for companies but also lucrative for malicious actors, as the average amount paid out by ransomware victims continues to increase.

The rise in ransomware

When ransomware attacks are successful, the combined costs of lawsuits and fines can be significant. In addition to the tangible costs, which include lost revenue while systems are down, the cost of remediation, and customer compensation or litigation, there are intangible costs as well. The damage to brand and company reputation, as well as diminished long-term customer trust, can linger long after an attack is over. And, even if companies choose to pay the ransom, attackers still may not release data or systems.

41 percent of organizations have reported experiencing increased incidents while employees are working from home.

Source: Harvey Nash/KPMG CIO Survey, 2020.

Ransomware will cost its victims around $265 billion (USD) annually by 2031, with a new attack every two seconds.

Source: Cybersecurity Ventures

Prepare and respond: Reducing the risk and impact of ransomware attacks

In today's complex environment, attackers have ample opportunities to exploit security vulnerabilities, including:

- Overprivileged human and nonhuman identities (apps, service accounts, bots)
- Weak authentication
- Risky remote access by your workforce and third-party vendors
- Failure to routinely audit accounts and privileges
- Unknown attacks (zero-day) that use software application weaknesses.

Attackers seek the path of least resistance, which is why they thrive in an environment that lacks basic controls and defenses where there are existing issues or gaps in information technology (IT) systems that could be proactively addressed by a known fix. In fact, 85 percent to 90 percent of ransomware campaigns work by targeting known vulnerabilities to gain initial access.[1]

A combination of preventative and detective controls should be employed in order to prevent an attack from occurring while also able to detect or identify possible attacks quickly in order to resolve the incident and greatly reduce the overall organizational impact.

Source:

[1] 2020 Verizon Data Breach Investigations Report

A defense-in-depth approach to ransomware

By taking a defense-in-depth approach to ransomware—instituting a wide range of endpoint security controls—you can strengthen your security posture and reduce exposure. Privileged management is a critical, and often overlooked, component of an effective endpoint security strategy.

A defense-in-depth approach to ransomware security, where endpoint management (see page 3) works alongside endpoint security tools, such as EDR and NGAV, can provide holistic protection against ransomware with privilege at its core. Attackers often try to gain unauthorized access to privileged accounts via malware or phishing attacks at the endpoint. Once they gain a foothold, they can traverse the network looking for high-value targets and use elevated privileges to steal confidential information or launch ransomware to disrupt critical applications. Forrester estimates that at least 80 percent of data breaches have a connection to compromised privileged credentials.[2]

59 percent of IT decision makers included ransomware on their list of greatest security risks.

Source: CyberArk Global Advanced Threat Landscape Report

Keys to managing endpoints, reducing the attack surface, and securing the enterprise against attack

- **Remove local administrator rights** from standard user accounts to reduce the attack surface.
- **Automatically elevate account privileges** for specific authorized tasks to keep users productive without providing unnecessary privileges.
- **Restrict applications on user endpoints** to prevent unknown applications from accessing the internet and gaining the read, write, and modify permissions needed to encrypt files.
- **Use antivirus and EDR tools** to detect and protect against malware executing and moving throughout the environment.
- **Frequently and automatically back up and test data** from endpoints and servers to allow for effective disaster recovery.

Source:

[2] The Forrester Wave™: Privileged Identity Management, Q4 2018

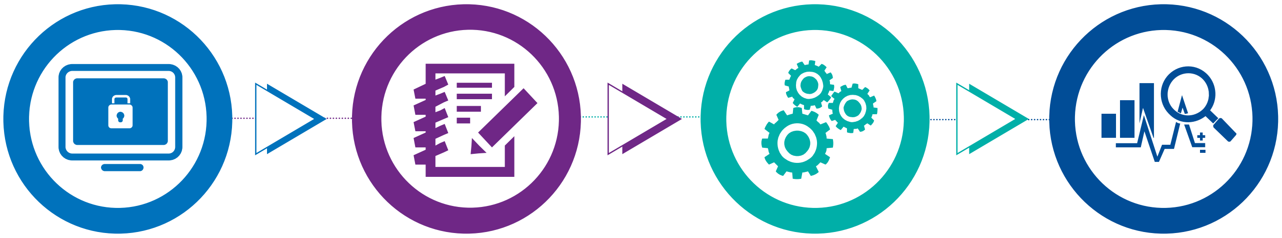
CyberArk’s Endpoint Privilege Manager

Endpoint Privilege Manager (EPM) enforces least privilege on the endpoint to contain attacks early in their lifecycle. It enables revocation of local administrator rights while minimizing impact on user productivity by seamlessly elevating privileges for authorized applications or tasks. Application control, with automatic policy creation, allows organizations to help prevent malicious applications from executing, and runs unknown applications in a restricted mode. This, combined with credential theft protection, helps to prevent malware from gaining a foothold and contains attacks at the endpoint.

> **In CyberArk’s analysis of ransomware samples, the removal of local admin rights, combined with application control, was successful in preventing 3.5 million ransomware attacks.**

The KPMG approach to securing endpoints with CyberArk

Securing endpoints by removing administrative credentials and enforcing a “least privileged” model greatly reduces the impact of a ransomware attack. KPMG can provide the strategy and execution of implementing preventative access management controls using CyberArk’s EPM solution in a holistic manner with minimal impact to the business. Our approach and methodology will enable organizations to quickly implement controls that block common attack vectors through endpoints, while iteratively enhancing policies in the EPM solution through monitoring applications and their respective access level needed to function.



Gain Visibility

Utilize CyberArk’s EPM solution to immediately block known attack vectors and understand application and service level permissions needed on endpoints.

Define Policies

Define policies based on permissions needed for applications and access needed. Policies will be defined to enhance controls across all assets across the enterprise, including remote users. Exception process should be defined in this stage.

Configure and Integrate

Configure policies in EPM and also integrate solution with asset management and other security capabilities. This includes the integration with CMDB/asset management, EDR, and SIEM solution that will enable automation and enhance controls within the environment.

Realize the Benefits

Shortly after enforcement is completed, the monitoring phase begins to assess the results and identify defects, collect end-user feedback, and review exception requests.

Why KPMG?

- **Established track record with CyberArk**—Since 2011, KPMG has been working with CyberArk to secure identity and privileged accounts for organizations across a range of industries.
- **Premier Identity Access Management. (IAM) technology integration partner**—We maintain formal partnerships and alliances with several leading vendors that enable us to have a strong footprint as premier IAM technology integrators. This enables us to bring a holistic approach to your privileged access management (PAM) transformation initiative.
- **Distinct deployment methodology and engagement accelerators**—KPMG has developed a distinct deployment methodology based on a combination of multiple industry frameworks, as well as a wealth of experience deploying PAM solutions in the field.

About CyberArk

CyberArk is the global leader in identity security. Centered on PAM, 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 https://www.cyberark.com.

About KPMG Cyber

KPMG Cyber has an extensive global network that assists organizations in transforming their security, privacy, and continuity controls into business-enabling platforms, all while maintaining the confidentiality, integrity, and availability of critical business functions.

KPMG Cyber's approach—*Prevent, Improve, Detect, Respond*—is designed to be simple and effective, and most importantly, aligned with your business needs.

Contact us

Hemal Shah
Principal
Cyber Security Services
T: 214-601-8198
E: hpshah@kpmg.com

Mike Battillo
Senior Director
Solution Relations
T: 305-358-2300
E: mbattillo@kpmg.com

Debbie Patterson
Senior Director
Alliances
T: 512-423-6150
E: deborahpatterson@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.