# The Necessary Tools for Enabling End Point Security

Sophisticated security threats require modern methods in building cyber-resilient systems.

Andrey Pozhogin, Sr. Product Marketing Manager, Endpoint Privilege Security @ CyberArk, and an IT Security Expert

### What is the importance of endpoint security when protecting against ransomware attacks?

**Pozhogin** Endpoint security is the organization's last chance to block ransomware before it deals damage. If you are at the point where your endpoint security is making the decision to block or allow a ransomware sample, quite a few of your defense layers have already fallen. They have already successfully touched the endpoint — they are in.

It means your organization has been targeted, it has been identified within vectors of attacks, and the attacker has made it all the way through email security, network security, sandboxes and so on.

The decisions your endpoint security team makes in the next moments is the difference between "just another day" and "the systems are down, do we have any backups?" Thus, a multi-layered identity-based endpoint security is an absolutely critical component of a defense-in-depth (DiD) approach.

**“Adaptive and scalable security controls continuously fine tune the balance between convenience and security to ensure the user is not overly burdened with security processes while assessed risk remains at acceptable levels.”**

**— Andrey Pozhogin, Sr. Product Marketing Manager, Endpoint Privilege Security, CyberArk**

## How can Endpoint Privilege Management (EPM) lower ransomware risk while improving user experience and smoothing local IT operations?

**Pozhogin** With CyberArk’s Endpoint Privilege Manager, an organization from day one can confidently defend against attacks by removing local admin rights, enforcing least privilege, and protecting the entire endpoint security stack from tampering. This will defuse most TTPs and prevent things like tampering with backup and logging agents, disabling shadow copies, wiping master boot record (MBR), exploiting a significant number of vulnerabilities and living-off-the-land (LotL) attacks.

Credential theft protection prevents attackers from compromising more credentials, elevating their privileges and moving laterally.

The Endpoint Privilege Manager also adds an additional layer of defense around sensitive data. Only designated content handlers are then allowed to even touch the data, so any high-risk or newly introduced software wouldn’t even be able to read the data.

The beauty of least privilege projects leveraging the right tools such as Endpoint Privilege Manager is that most operations involving elevation are completely automated and are transparent to the user. This helps significantly relieve the amount of user requests sent to the service desk. In addition, those operations are logged and provide a full audit trail for privileged actions.

## How does Privileged Access Management (PAM) dovetail with zero trust principles, such as identity, credential and access management (ICAM), to boost cyber resilience to ransomware?

**Pozhogin** Federal officials have said ransomware is here to stay. With the pandemic leading to boosts in remote work, accessing data from mobile devices and widespread workforce changes, identity has quickly become the

new perimeter. Privileged access is a necessity. Under certain conditions, every identity has (some) privilege associated with it — an IT admin who needs to work on a server, a human resources official who has access to salaries, a financial analyst looking at the business.

Bad actors are thrilled with the attack surface expansion due to the explosion of identities with privileged access, so Privileged Access Management (PAM) is a necessity in defending against ransomware. A PAM strategy enforces the principle of least privilege to restrict account permissions to a minimum level. With CISA's recommended zero trust maturity model, determining advanced access requires least privilege controls to consider identity. Therefore, PAM enables zero trust by reducing the expanded attack surface of identity, through credentials control and access to sensitive information, ultimately preventing the spread of ransomware and boosting cyber resilience.

## Can organizations maintain a strong cyber posture and limit ransomware exposure under a bring-your-own-device (BYOD) policy? If so, how?

**Pozhogin** Ransomware is a top-of-mind concern for most organizations. Ransomware is no different than any other malware that exploits poor foundational security.

Over 51% of respondents in CyberArk's Threat Landscape Report indicated that unmanaged identities represent the biggest security risk in today's hybrid/remote work environment. About 61% of respondents have identity-security controls in place for employer-assigned user devices, compared to 40% for employee-sourced or "bring-your-own-devices" user devices.

As ransomware evolves, new variants not only encrypt data and damage business continuity, but also lead to public data leaks of confidential information. CyberArk can secure both the endpoint where attacks often start, as well as the

Photo Credit: XXXXXXXXXXX

privileged credentials attackers leverage to move horizontally and vertically.

Using controls like multi-factor authentication, privileged credential rotation and session isolation, and removing local admin rights from endpoints, CyberArk is a trusted partner that helps any organization reduce the risks associated with ransomware attacks while protecting the user experience.

## What is the role of adaptable and scalable security controls, such as adaptable multi-factor authentication (MFA), in a cyber strategy to protect against ransomware?

**Pozhogin** Adaptive and scalable security controls continuously fine tune the balance between convenience and security to ensure the user is not overly burdened with security processes while assessed risk remains at acceptable levels. Continuous and adaptive multi-factor authentication, while not sufficient for ensuring trust on the endpoints on its own, together with endpoint privilege security controls creates a formidable barrier in the path of ransomware. As an example — ransomware operators often rely on legitimate tools to establish foothold on the endpoint, set the stage for the attack, exfiltrate data and launch the payload (so-called “LOL” or “LOtL” attacks — live-off-the-land).

With identity-driven endpoint security, such as CyberArk Endpoint Privilege Manager and CyberArk Identity, we can selectively challenge the user based on the assessed risk of their action to MFA themselves. Let’s say the user is attempting to launch PowerShell with administrative privileges — this operation will allow the user to do pretty much anything on the endpoint, including disabling shadow copies, tempering with backup agents and altering logs. In this case, it is smart to ensure this is indeed your system administrator who’s launching the elevated PowerShell console and challenge them to MFA. Such MFA interventions, called “step-up” authentications, allow to significantly raise the security and defend against ransomware — all while maintaining system usability and user convenience.”

# SECURE PRIVILEGE. STOP ATTACKS.

ACROSS THE ENTERPRISE
IN THE CLOUD
ON ENDPOINTS

Unsecured privileged accounts add risk to your business anywhere they exist— 100% of advanced cyber attacks involve them. Seamlessly protect privileged accounts across the enterprise— on premises, in the cloud and on your endpoints with CyberArk.

Federal Certifications and Compliances Include:

- DoD UC APL
- Common Criteria Certified
- NIST SP 800-53 / -171 / -82 / -63
- NERC-CIP
- DHS CDM Phase II Privilege Management Solution
- Army Certificate of Networthiness (CoN)
- Available on DoD Cyber Range
- HSPD-12
- In Evaluation for NIAP

**CyberArk.com**

©2022 CyberArk Software Ltd. All rights reserved.

CYBERARK®