CYBERARK®
The Identity Security Company

WHITEPAPER

How Endpoint Privilege Management Fulfills Federal Mandates

Navigate Endpoint Privilege Security in Today's Zero Trust Environments

Table of Contents

Introduction

Cyber adversaries continue to pose an increasing global threat to information systems, particularly those used by the U.S. Federal Government. The extensive government systems, many of them storing and processing high volumes of confidential information, and the vast number of third-party partners and contractors, all increase the attack surface to federal endpoints. The increasing threat levels place more demands on security personnel, yet agencies face workforce shortages and budget pressure challenges. Protecting network and computing infrastructure is critical to preserve the confidentiality, integrity and availability of communication and services across an agency enterprise.

Sixty-three percent of security decision-makers admit that the highest-sensitivity access for employees in their organization, such as IT admins and other privileged user accounts, is not adequately secured today.[1] Even when an attacker does not directly use a privileged account as the initial point of entry, they quickly find ways to enumerate and attack accounts with elevated rights.

Privilege escalation is a key exposure. The MITRE ATT&CK® taxonomy of TTPs — the adversary's tactics, techniques and procedures — includes a whole suite of privilege escalation techniques in the arsenal used for attacking and compromising systems. The ATT&CK® page[2] states that, "Privilege escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations and vulnerabilities."

Agencies have been directed to place increased focus on endpoint detection and response (EDR) and these approaches are vital, but by definition they provide a limited and reactive capability that only applies after an adversary has already enjoyed some level of success. A more proactive strategy is to use endpoint privilege security as a preventive approach. This addresses privilege misuse and enforces role-specific least privilege policies and reduces or removes the ability for the adversary to gain access.

[1] CyberArk, "2023 Identity Security Threat Landscape Report," June 2023
[2] MITRE ATT&CK®

Federal Directives Require Action to Protect Privileged Accounts

Recent administrative directives recognize the importance of enforcing least privilege principles and protecting key accounts from unauthorized access. For example, Executive Order (EO) 14028, Improving the Nation's Cybersecurity, reminds us that the United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector and ultimately the American people's security and privacy. The President states, "It is the policy of my Administration that the prevention, detection, assessment and remediation of cyber incidents is a top priority and essential to national and economic security."

Application of the security measures required by this Presidential order, including mandates to follow privilege access management principles for network-based administration and configuration management of critical software platforms, are greatly improved through the use of automated endpoint privilege security (EPS). EPS is an effective force multiplier, enabling agency success in fulfilling these increasing requirements in the face of workforce and budget challenges. In fact, those applying EPS solutions can often demonstrate a measurable return on the investment, achieved through improved productivity, reduced help-desk inquiries, and, of course, avoiding costly losses and disruptions.

The **White House National Cybersecurity Strategy (NCS)** recognizes the vital role of endpoint privilege security in defending and modernizing the federal infrastructure, strategically employing tools to disrupt adversaries, and, addressing the ransomware threat through a comprehensive Federal approach. In fact, the NCS calls for the development of a digital identity ecosystem. Endpoint privilege security solutions, such as CyberArk Endpoint Privilege Manager (EPM), are front and center in such an ecosystem.

These efforts build on the EO 14028 initiatives, notably through application of a Zero Trust Architecture and major improvements in cyber supply chain risk management. The EO states, "The security and integrity of 'critical software' — software that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources) — is a particular concern." Cybersecurity supply chain security controls, including those for developers and providers of critical software, require protections such as those provided by endpoint privilege security. For example, security measure (SM) 3.3[3] requires the use of "configuration management practices to maintain EO-critical software platforms and all software deployed to those platforms. Practices include [identification of] the proper hardened security configuration for each EO-critical software platform and all software deployed to that platform (hardened security configurations enforce the principles of least privilege, separation of duties, and least functionality)."

[3] National Institute of Standards and Technology (NIST), Executive Order 14028, Improving the Nation's Cybersecurity

Detection and Response are Important, but Foundational Protection is Vital

EO 14028 requires agencies to improve the ability to detect malicious cyber activity on federal networks by enabling EDR solutions. This represents an important step but may not be sufficient to prevent cyber intrusions. Endpoint privilege security serves as the cornerstone of an endpoint privilege management strategy, which can then be bolstered by effective EDR. In fact, CyberArk works in conjunction with EDR solutions to provide a comprehensive approach to preventing, detecting and responding to advanced threats.

Agencies have invested significant resources into EDR solutions and often feel this investment delivers adequate endpoint security. Yet many conventional endpoint threat detection and response tools must reply upon the integrity of the agents and protections on the endpoints — agents that can be manipulated or disabled before the EDR tool can do its work. The cybersecurity landscape is littered with examples of sophisticated attacks that sidestepped EDR solutions. This includes the widely publicized SolarWinds SUNBURST incident, a massive supply chain attack that went undetected for nine months, impacting over 18,000 organizations across the globe including nearly every Fortune 500 company.

CyberArk Endpoint Privilege Manager is specifically designed to fill the gaps left by traditional threat detection and mitigation solutions and defend businesses against privileged attackers. Unlike EDR and XDR products, the CyberArk EPM strengthens security and mitigates risk by removing standing admin privileges and enforcing the principle of least privilege. More importantly, CyberArk's endpoint privilege security solution is designed to radically reduces attack surfaces, hardens the operating system, protects credentials, passwords, cookies and other security tokens from compromise and prevents bad actors from tampering with other endpoint security stack components.

SolarWinds SUNBURST incident, a massive supply chain attack that went undetected for nine months, impacted over 18,000 organizations across the globe including nearly every Fortune 500 company.

Since many of today's cyberattacks occur through privilege abuse or escalation at the endpoint, combining effective EDR/XDR with EPM is an excellent way to fulfill federal requirements and reduce the attack area significantly.

Zero Trust Architecture (ZTA), described in NIST Special Publication (SP) 800-207 and associated guidance, is an important engineering model for federal stakeholders, and it's a practical approach for any organization. Despite the name, Zero Trust doesn't mean "don't trust anyone" but rather it draws on the old saying "trust, but verify." The concept means zero assumed trust. For example, just because packets are arriving from an internal server, don't presume that the traffic is safe. And just because a request "says" it is from a known device, service or user, don't presume that they are whom they claim to be.

CISA has announced major ZTA initiatives including a new office that will guide and drive ZTA improvements. CyberArk solutions will help agencies make great progress on these mandatory requirements, of course while also working to defeat adversaries.

CyberArk EPM helps fulfill the requirements of CISA's five ZTA pillars as described in NIST SP 800-207 and in CISA's Zero Trust directives:

CYBERARK ENDPOINT PRIVILEGE MANAGER ENABLES SIGNIFICANT ADVANCEMENT IN ZERO TRUST MATURITY

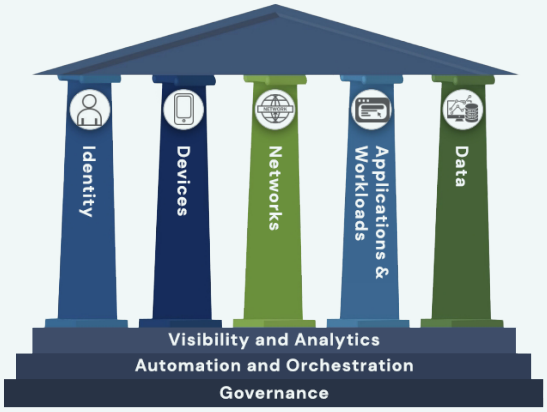

Figure 1. Zero Trust Maturity Model Pillars

Source: CISA Zero Trust Maturity Model Version 2.0, January 2022

1. Identity: Specific to privileged identities or users, access needs to be continuously monitored and validated in terms of user trustworthiness to govern access and privileges. Incorporating identity access with a least privilege approach is foundational to Zero Trust. Privileged identities should only be provided access to the systems when specifically required. Access should be as limited as possible, and access should be immediately revoked when it is no longer required. CyberArk EPM supports this identity management aspect of ZTA effectively for human and non-human identities (e.g., service accounts).

2. Devices: Through robust privilege management and workstations, servers and other endpoint devices, CyberArk EPM improves prevention, detection and response. The CISA Zero Trust Maturity Model (ZTMM) recommends integrated threat protections for your agency devices. Since most breaches involve the compromise of privileged accounts and credentials, CyberArk EPM is a vital part of that protection, and that protection extends to the vital tools for detecting and responding to sophisticated threats.

3. Networks: CyberArk EPM supports the network pillar by limiting untrusted access to internet and intranet systems. ZTMM calls for tailored local controls, dynamic updates and secure external connections based on application and user workflows. The solution helps to prevent malware communication back to command-and-control servers and protects from network-born encryption, such as when files on network shares are encrypted from a compromised machine. In partnership with ZT network security architecture such as network segmentation, traffic management and traffic encryption, CyberArk EPM supports a holistic security model.

4. Applications and Workloads: As part of a comprehensive solution for secure application delivery, CyberArk EPM supports granular execution, elevation and resource access controls and integrated threat protections that can offer enhanced situational awareness and mitigate application-specific threats. The approach includes enforcement of least privilege controls, and also includes very granular application access controls. CyberArk EPM can manage application elevation, allow or deny access to Internet and Intranet services, and can even control and restrict access to memory space of other process. Application security extends to how and when a program can be executed: for example, CyberArk EPM can enable an application to run based on the day of the week or time of the day. It can also restrict what other applications can launch and control depending on the elevation state. These capabilities help to automate application configurations to continuously optimize for security and performance — another ZTMM recommendation.

Notably, while these EPM capabilities already greatly support the applications pillar, integration through extensive partnerships and APIs with the world's most trusted protection, detection and response solutions extend agencies' application and workload security to new heights.

5. Data: ZTMM states that, "Data includes all structured and unstructured files and fragments that reside or have resided in federal systems, devices, networks, applications, databases, infrastructure and backups (including on-premises and virtual environments) as well as the associated metadata." By applying the elements above, CyberArk EPM enables agency practitioners to identify where critically important and sensitive live, enforce least privilege and access to that data, and integrate that solution with effective EDR and monitoring solutions.

Sixty-three percent of security decision-makers

admit that the highest-sensitivity access for employees in their organization, such as IT admins and other privileged user accounts, is not adequately secured today.[4]

[4] CyberArk, "2023 Identity Security Threat Landscape Report," June 2023

CyberArk EPM Reduces Ransomware-related Risks

Among the biggest risks to data today is the threat of a ransomware attack. The likelihood and impact of ransomware can be greatly reduced by the use of 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. Instead of completely removing all privileges from agency users — and potentially hindering their ability to perform their work duties — CyberArk EPM enables automated policy-based and ad hoc workflows that enable on-demand privilege elevation without impairing the end-user experience or burdening support teams.

A glance at the MITRE ATT&CK® TTPs described in an earlier section reminds us that sophisticated attacks, including ransomware attempts, rely on a workflow that includes reconnaissance, initial access, execution and privilege escalation. Effective endpoint privilege security provides multiple methods to thwart these tactics, including through conditional policies to block attacks involving trusted applications. For example, CyberArk EPM could support a rule that would allow users to launch PowerShell with certain parameters while preventing other apps from launching PowerShell as a child process, thus eliminating chained exploit techniques.

While completely blocking endpoint applications can either reduce a user's effectiveness or bury the support team in constant changes, leading endpoint privilege managers support application greylisting to help defend against unknown malware variants without impeding the users' operation of unknown applications that pose no known security risks. Greylist policies apply to applications that aren't explicitly allowlisted nor denylisted. Through automated policies that provide out-of-the-gate protection against ransomware while supporting and reporting access management, EPM is an important element of an agency's comprehensive cybersecurity suite.

CyberArk EPM Enables an Effective Cybersecurity Program for Federal Agencies

While each of these initiatives is important, the key mission for agency security leadership and operations is to establish effective cybersecurity security solutions at the enterprise, mission/business and system levels. CyberArk Endpoint Privilege Manager provides the right solution for many of the security requirements for protecting agency systems.

CyberArk EPM satisfies key requirements in many of the families of security and privacy controls found in the catalog known as **NIST Special Publication 800-53**. Primarily, CyberArk EPM supports the Access Control family. For example, Account Management (AC-2) calls for diligent and secure management of various types of accounts, and for restricted, controlled policies for granting elevated privileges. Control enhancement AC-2 (6) specifically calls out the need for dynamic privilege management as "dynamic access control approaches [that] rely on runtime access control decisions facilitated by dynamic privilege management." CyberArk EPM also supports Access Enforcement (AC-3) and, of course, AC-6 Least Privilege which states, "Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks."

Many of these same needs are reflected in the requirements for Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, NIST SP 800-171 Revision 2. These requirements are an important part of an agency's cybersecurity supply chain risk management (C-SCRM) approach and are often included in agency security reviews (including the emerging Cybersecurity Maturity Model Certification, or CMMC, program). Access Control requirements in this document include:

- **3.1.1** - Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
- **3.1.2** - Limit system access to the types of transactions and functions that authorized users are permitted to execute.
- **3.1.4** - Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
- **3.1.5** - Employ the principle of least privilege, including for specific security functions and privileged accounts.
- **3.1.6** - Use non-privileged accounts or roles when accessing non-security functions.
- **3.1.7** - Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

Through implementation of CyberArk EPM, especially as integrated through APIs to other protection, detection and response tools, agencies are able to effectively plan, achieve, and monitor many of the elements for agency cybersecurity needs. Furthermore, as shown above, CyberArk EPM helps agencies work with contractors and partners to ensure robust cybersecurity in nonfederal systems.

Conclusion

Agencies have a duty to safeguard citizens' information and services using every tool available. Key stakeholders not only expect secure performance but improvement, as demonstrated by increasing programs to drive agency accountability. Federal agencies can make great progress on fulfilling all of these needs by implementing CyberArk EPM to thwart the adversaries, reduce burdens on internal systems (like help desks and administrators), and propel the entity to an advanced Zero Trust and supply chain maturity.

Next Steps

You can schedule a conversation with a CyberArk team member to discuss your security needs.

CONTACT US

About CyberArk

CyberArk is the global leader in identity security. Centered on intelligent privilege controls, 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.

CYBERARK®
The Identity Security Company