merlin cyber | CYBERARK®

SOLUTION BRIEF

# Closing the Endpoint Security Gap with **CyberArk Endpoint Privilege Manager (EPM)**

## Extending Privileged Access Management to the endpoint to stop attacks at the source.

As cyber adversaries increasingly target endpoints through orphaned accounts, unmanaged administrative privileges, and other identity-related vulnerabilities, identity controls are emerging as the new security perimeter. Federal agencies protecting distributed workforces and mission-critical systems can no longer rely on detective security controls alone. Extending Privileged Access Management (PAM) capabilities to the endpoint with CyberArk EPM prevents identity based attacks at the source, stopping ransomware execution, privilege abuse, and Endpoint Detection & Response (EDR) bypass before compromise occurs. Integrating preventative controls like EPM with detective controls such as EDR delivers comprehensive cybersecurity protection, reducing attacker dwell time, accelerating mean time to remediation (MTTR), and transforming identity security from reactive to proactive.

With CyberArk EPM, agencies can achieve a holistic endpoint protection and prevention strategy. By preventing unauthorized privilege escalation, lateral movement, and enforcing least privilege without disrupting productivity, EPM also enables agencies to safeguard existing EDR investments by preventing attackers' tampering and evasion tactics that degrade EDR efficacy.

## **The Challenge:** Endpoints as the Identity Attack Surface

1. Endpoints are the most common entry point for attack vectors like phishing, credential theft, and abuse of unmanaged local admin rights, with 68% of organizations experiencing one or more endpoint attacks that successfully compromised data and/or their IT infrastructure (Ponemon Institute)

2. Sophisticated adversaries increasingly evade or delay EDR using fileless techniques, code injection attacks, DLL side loading, indirect system calls, and living off the land binaries (LOLBins).

3. EDR frequently alerts after suspicious activity starts. Without EPM's preventative identity security controls on endpoints, agencies are reacting to incidents rather than proactively preventing them.

To meet Zero Trust objectives, **"never trust, always verify,"** agencies must enforce least privilege and pre execution controls on the endpoint.

## Policy & Industry Context:

### Why Prevention is Paramount at the Endpoint

**CISA-FOCUSED COMMENTARY**

CISA-focused commentary calls for a shift toward holistic endpoint protection and prevention that begins with EPM—because ransomware and stealthy, EDR evasion techniques continue to afflict the public sector. Industry commentary also highlights that privileges left unmanaged on endpoints become prime vectors for bypass and lateral movement.

**STRATEGIC ALIGNMENT**

Prevention at the endpoint complements CISA's broader push to reduce attacker dwell time across the federal enterprise and strengthens Zero Trust outcomes.

Extending PAM to endpoints with EPM operationalizes prevention where it matters most and improves the fidelity and efficacy of detective tooling.

## The Solution: Extend PAM to Endpoints with CyberArk EPM

CyberArk EPM brings PAM's proven governance and least privilege enforcement to endpoints, closing a critical gap while protecting and strengthening EDR:

- Remove local admin rights without breaking user productivity through contextual, policy based elevation and allow lists.
- Enforce least privilege across all identities and endpoints, with granular, just in time (JIT) elevation when needed.
- Control application and script execution with policy, blocking ransomware and unknown threats pre execution.
- Block common EDR evasion vectors (fileless malware, DLL side loading, indirect system calls, LOLBins).
- Automate policy creation and management to allow, restrict, or elevate with auditability.

With EPM in place, federal agencies can close the identity–endpoint gap by preventing abuse of local privileges that enables lateral movement, preserve and enhance EDR efficacy by blocking bypass tactics before they trigger alerts or cause damage, and advance Zero Trust by operationalizing least privilege where users actually work—the endpoint.

## Protect Your EDR Investment with EPM

EPM hardens and reduces risk for your EDR deployment by preventing the very actions attackers use to bypass it:

**TAMPER-RESISTANT BY POLICY**
Block or require approved elevation for attempts to uninstall, disable, or stop EDR agents, services, or drivers.

**SCRIPT AND TOOL CONTROL**
Deny untrusted scripts and LOLBins used to kill processes, modify registry/driver settings, or alter telemetry.

**RING FENCING SECURITY TOOLS**
Permit only approved parent child process chains and network access for EDR processes to prevent hijack or abuse.

**JIT FOR ADMINS, NOT ADVERSARIES**
Grant time bound, task specific elevation for legitimate EDR maintenance while keeping endpoints free of standing admin rights.

**TELEMETRY INTEGRITY**
Reduce false negatives (when attackers silence sensors) and false positives (by blocking noisy, risky execution paths) to improve SOC signal to noise and MTTR.

## **Prevention + Detection:** A Two Pillar Defense

A modern, comprehensive endpoint protection strategy pairs preventative identity security delivered by CyberArk EPM with detective EDR. EPM stops privilege escalation, risky scripts, and untrusted binaries before they run. It also constrains identities to least privilege and provides just in time (JIT) elevation for approved tasks. In parallel, EDR continuously monitors, detects, and drives targeted response to indicators of compromise (IoCs). Together, these complementary pillars create a defense in depth posture that reduces noise, shortens attacker dwell time, and accelerates response, as fewer high risk actions execute in the first place.

## Make ITDR Actionable with Automation

EPM's policy-driven automation enables Identity Threat Detection & Response (ITDR) to be actionable and automatable:

**DEFENSIVE DECEPTION AT THE IDENTITY LAYER**
Plant decoy credentials to lure attackers and trigger high fidelity alerts when engaged by an adversary.

**AUTOMATED CONTAINMENT**
Revoke access or isolate endpoints upon anomaly detection to break kill chains early.

**GRANULAR JIT ELEVATION**
Automatically elevate only what is needed when it is needed.

**INTEGRATED WORKFLOWS**
Standardize and automate remediation through integrations with ticketing, SOAR, and security operations.

## Resulting operational benefits:

- Measurably reduced attacker dwell time
- Improved MTTR and through fewer false positives and noisy alerts
- Shift from reactive triage to proactive prevention and rapid remediation

## Reference Architecture

### IDENTITY PERIMETER ENFORCEMENT (ENDPOINTS)

CyberArk EPM enforces least privilege, application control, and pre execution blocking directly on workstations, laptops, mobile devices, and servers.

### PRIVILEGED ACCESS MANAGEMENT

Centralized PAM governs privileged accounts and JIT elevation policies; EPM extends these to endpoint users, devices, and processes.

### EDR TELEMETRY & RESPONSE

EDR monitors runtime behaviors; EPM reduces malicious execution paths, improving EDR signal to noise ratios.

### ITDR & AUTOMATION

Decoy credentials + policy signals feed automated isolation/revocation and standardized remediation workflows.

Through continuous verification and applying least privilege across users, endpoints, applications, and workloads, federal agencies can ensure Zero Trust alignment.

## Priority Use Cases for Federal Agencies

### RANSOMWARE PREVENTION AT THE SOURCE:

Block untrusted binaries and script abuse pre execution; deny lateral movement via least privilege.

### BLOCK LATERAL MOVEMENT AND UNAUTHORIZED PRIVILEGE ESCALATION:

Remove standing privileges and block unauthorized applications to reduce the risk of lateral movement and contain the spread of a potential breach.

### INSIDER THREAT DETECTION:

Continuously monitor user behavior and enforce least privilege access to detect anomalies and prevent insider threats.

### EDR BYPASS PREVENTION:

Stop fileless and LOLBin techniques before they run, preserve telemetry integrity and visibility.

### LOCAL ADMIN RIGHTS REVOCATION AT SCALE:

Replace standing admin rights with JIT elevation and policy based approvals across all users and endpoints.

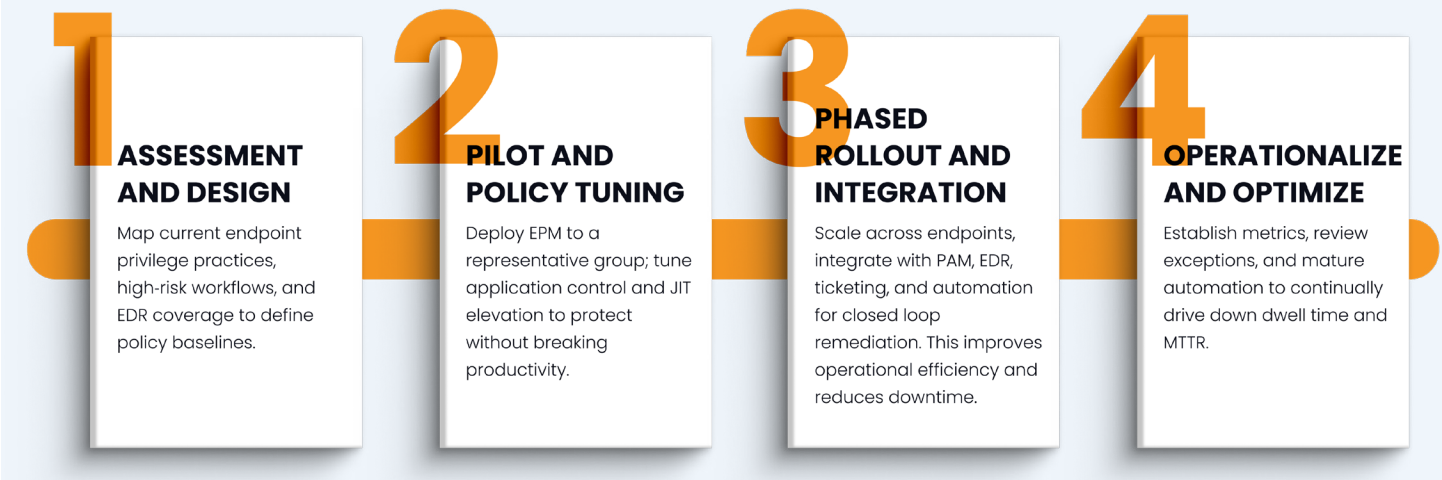
### MISSION CRITICAL WORKSTATION HARDENING:

Enforce trusted application paths for administrators, analysts, and developers.

### CONTRACTOR & FIELD DEVICE CONTROL:

Apply consistent privilege and application controls across all devices and users across on-premises, hybrid, and multi-cloud environments.

## Implementation Approach with Merlin Cyber




## Unlocking Operational Efficiency with Identity Centric Controls

Doing more with less—securely. CyberArk EPM reduces admin overhead, eliminates manual workarounds, and increases IT agility across the complex, hybrid environments common in federal agencies.

From a centralized console, federal teams can define and deploy standardized policies at scale—with inheritance and targeted overrides for specific organizational units, user enclaves, or mission systems. Additionally, OOTB vetted least privilege and application control policy templates accelerate adoption and eliminate risky one off exceptions. By replacing ad hoc local admin workarounds with just in time elevation and approved workflows, ticket volume and break fix cycles decrease. This workflow automation drives consistent control enforcement and reporting to streamline audits and ATO programs by simplifying compliance attestation and POA&M completion. This auditability and a reduction of false positives alerts translate to valuable time and cost savings for federal SOC teams.

CYBERARK®
THE IDENTITY SECURITY COMPANY

merlin® cyber

### Achieve Identity Security Modernization with CyberArk and Merlin Cyber

Ready to modernize identity security and close the endpoint security gap? Merlin Cyber can help your agency plan, pilot, and scale CyberArk EPM to complement your EDR solution, align identity security practices with mission objectives, and protect mission-critical systems from cyber-attacks targeting vulnerable user identities and endpoints.

## About Merlin Cyber

Merlin Cyber is the go-to-market and Zero Trust Modernization affiliate of Merlin Group, a network of companies that invests in, enables, and scales technology companies with disruptive cyber solutions. Through Merlin Cyber, the U.S. Government can access innovative, public sector-ready cybersecurity solutions that are designed to meet government requirements and mission priorities. Merlin does this by selectively partnering with best-in-class cybersecurity brands, investing in visionary emerging technologies, and enabling the U.S. Government to successfully keep ahead of today's critical threats, accelerate Zero Trust modernization initiatives, and defend our nation.

703.752.2928 info@merlincyber.com merlincyber.com

merlin® cyber