CYBERARK®

SOLUTION BRIEF

CyberArk Endpoint Privilege Manager Jump Start

ACCELERATE YOUR ENDPOINT PRIVILEGE MANAGER ROLLOUT

In today's hyper-connected world, desktops and servers are vulnerable to a variety of increasingly sophisticated and dangerous cyberattacks that disrupt businesses, damage companies' reputations and lead to steep regulatory fines and costly lawsuits.

As an integral component of the CyberArk Identity Security Platform, CyberArk Endpoint Privilege Manager is designed to remove local admin rights, enforce least-privilege security, defend against ransomware and cached credential compromise, and enable application control at the endpoint -- thus helping to contain attackers at the point of entry, before they can traverse your network and inflict serious damage.

CYBERARK JUMP START PACKAGES

Quick security posture improvements:

- Streamline EPM deployment
- Accelerate time-to-value (TTV)
- Accelerate return on investment (ROI)
- Free up IT ops and security staff

CyberArk Endpoint Privilege Manager is a highly advanced, versatile, and configurable tool that allows any level of customization. While this is one of the reasons EPM appeals to large enterprises, it may pose challenges for inexperienced users and could decrease time-to-value (TTV) – an important metric that impacts operational efficiency and ROI. Another important consideration is that misconfigurations routinely top the list of reasons for cyber incidents, and security tools are not an exception. Ranging from increased resource use (e.g., CPU utilization or increased network traffic) to impacted business continuity through a misguided policy configuration, the consequences of configuration mistakes can be costly.

Through the extensive CyberArk Partner Network, many channel partner representatives have achieved CyberArk Certified Delivery Engineer (CDE) certification and can deploy this solution. Either CyberArk Security Services or certified Channel Partners, can help you accelerate the rollout of Endpoint Privilege Manager and make the most of your CyberArk investments with expert advice from seasoned endpoint security specialists. CyberArk's professional services organization has deep knowledge and vast experience in successfully implementing the solution in thousands of businesses across the globe.

With the CyberArk Endpoint Privilege Manager Jump Start Package, a knowledgeable CyberArk Security Services professional will guide you through every phase of your EPM journey, from planning to pilot to production. The Jump Start Package can help streamline your rollout, improve your security posture, and accelerate time-to-value, while freeing up valuable IT operations and security personnel to focus on core business activities. The solution

also provides enablement for your IT personnel who will manage EPM going forward. Combined with the hands-on training and knowledge transfer during the rollout phase, you'll end up with fully deployed product and trained personnel to administer it.

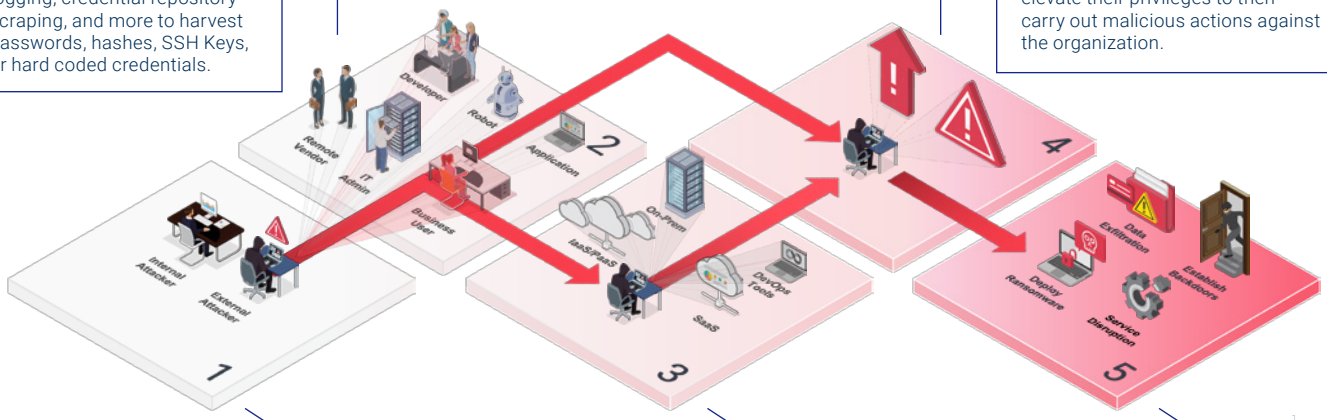
GAIN EXPERT GUIDANCE AT EVERY STEP OF THE JOURNEY

The CyberArk Endpoint Privilege Manager Jump Start service follows the key principles of the **CyberArk Blueprint for Identity Security Success** – a field-proven, prescriptive security framework reflecting the combined knowledge and experience of CyberArk's global Security Services, Threat Research and Innovations Labs, Customer Success and Sales Engineering organizations. The CyberArk Blueprint prescribes a pragmatic, staged implementation approach that addresses the most high-risk vulnerabilities as quickly as possible.

UNDERSTANDING THE ATTACK CHAIN

CREDENTIAL THEFT
Actors use techniques such as social engineering, keystroke logging, credential repository scraping, and more to harvest passwords, hashes, SSH Keys, or hard coded credentials.

PRIVILEGE ESCALATION & ABUSE
Once a bad actor has discovered the access they desire, they will elevate their privileges to then carry out malicious actions against the organization.



MALICIOUS ACTORS
Bad actors can exist either internally or externally to the organization. External actors use a wide variety of techniques to gain entry, while internal actors tend to leverage existing knowledge and access.

LATERAL & VERTICAL MOVEMENT
Actors will leverage that access to navigate across an organization's resources, whether it be laterally from within a risk tier (e.g. workstation to workstation) or crossing vertically into another risk tier or environment (e.g. workstation to cloud or workstation to DevOps tool).

ACTIONS ON OBJECTIVES
Those malicious actions are typically predefined objectives such as data theft, ransomware distribution, service disruption, supply chain spread, brand damage and more.

The CyberArk Jump Start packages follow a three-phase, repeatable approach: planning, deploying and expanding rollout of Endpoint Privilege Manager implementation, tailored to your specific business requirements. Jump Start services also include CyberArk training credits to help users get up to speed on administering and monitoring the EPM solution.

LEARNING

To streamline the learning process, customers with Jump Start services are eligible to take the Endpoint Privilege Manager Administration instructor-led live training or related self-paced training from CyberArk University. Integrated knowledge transfer is also conducted throughout the Jump Start service. In addition, short tutorials are available at no charge to supplement courses and provide quick references.

DISCOVERY AND PLANNING

During the Discovery and Planning phase, a CyberArk Security Services professional will work with your team to gain an understanding of your business requirements, operating environment, and network architecture.

During the EPM discovery and planning session, we will review your company's required business goals and recommend the best approach for achieving them. We will work with your team to develop a detailed, risk-aligned deployment strategy to defend against the most critical endpoint security threats in the short term (vertical movement, credential theft, privilege creep, ransomware, etc.) and to address lower-risk vulnerabilities over time.

The strategy includes a prioritized roadmap for implementing Endpoint Privilege Manager agents, onboarding user groups, and defining policies tailored to your unique business requirements, endpoint applications, organizational structure, and functional roles and responsibilities. We will exit this phase with a clearly defined set of business requirements, an implementation strategy, and a recommendation for the ongoing rollout.

DEPLOYMENT

In the Deployment phase, you will begin implementing Endpoint Privilege Manager, targeting the threats that pose the greatest potential risk in accordance with the CyberArk Blueprint.

This phase begins with a small-scale pilot program to evaluate the effectiveness of the plan, test out the methods and procedures, and identify corrections and adjustments required for full-scale production.

We will work with your team to verify the EPM implementation strategy will achieve the desired business goals without impacting applications, impairing user productivity, or disrupting operations. Customers will end up with a predictable and repeatable process that can efficiently scale across the organization.

Security measures implemented in the Deployment phase include removing local admin rights, enforcing least privilege, and denying the listing of known threats. At the conclusion of this phase, EPM is deployed in production, local admin rights are removed from endpoints, and least-privilege access controls are established. By mitigating the most critical threats, customers can improve their security posture and reduce security risk rapidly.

EXPAND AND SECURE

Following the recommendations of the CyberArk Blueprint, the Expand and Secure phase extends the scope of the Endpoint Privilege Manager implementation to address lower-risk vulnerabilities.

A CyberArk Security Services professional will work with your team to broaden the scope of the deployment, introduce advanced EPM functionality and improve your overall security posture. During this phase, you might institute fine-grained application controls to limit access to endpoint memory, disk or networking resources and protect against more sophisticated attacks. Additional controls are implemented, such as restrictions against internet-downloaded applications and enablement of ransomware defenses. We will exit this phase with a comprehensive endpoint security implementation that takes full advantage of CyberArk Endpoint Privilege Manager's features and capabilities, and fully addresses the business requirements identified in the Discovery and Planning phase.

JUMP START BENEFITS

By leveraging CyberArk's Endpoint Privilege Manager Jump Start services, you get:

- Predictable rollout schedule with defined by over 1,500 deployments
- Access to CyberArk's experienced engineers and customer success organization
- Accelerated time-to-value
- Specialized hands-on training and knowledge transfer

OUTCOME DETAILS

EPM Jump Start Phases	Phase Outcomes	Outcome Description
Discovery and Planning Phase	• EPM deployment methodology • Prerequisite's checklist • Roles and responsibilities	• Define agent deployment methodology and future agent deployment process • Review enterprise integration • Draft prerequisites checklist for deployment planning • Define project timelines with roles and responsibilities
Deployment Phase	• EPM agents installed in pilot deployment • Active events monitoring • Just-in-time (JIT) user elevation and application deny listing management • Administration best practices	• Deploy EPM agents with initial policies enabled and events monitoring active. • Enable just-in-time user elevation and application elevation management policy features. • Define repeatable process for agents' deployment. • Remove local administrator rights on endpoints. • Deploy ransomware protection policies. • Configure application controls and internet-downloaded application restrictions. • Define best practices related to ongoing events and applications management.
Expand and Secure Phase	• Eight (8) meetings up to sixteen (16) hours	• Expand deployment of agents and configured features from Deployment phase. • Activate local credentials theft protection. • Provide guidance to administrators for ongoing expansions, operations, and administration.
Training Services	• Four (4) training credits	• Complete the recommended EPM Administration instructor-led training or EPM (SaaS) Administration self-paced trainings.
Add-On to Jump Start	• Additional outcomes for use cases, components, and integrations	• Extend the Jump Start service to provide additional outcomes for strategic guidance, discovery, design, deployment, expansion, and program delivery management.

NEXT STEPS

Contact your designated sales account executive to learn more about the CyberArk Endpoint Privileged Manager Jump Start or submit our **contact form**.

About CyberArk

CyberArk is the global leader in Identity Security. Centered on privileged access management, 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®