SOLUTION BRIEF

CYBERARK PRIVILEGED ACCESS MANAGER ON-PREMISES JUMP START

WORK WITH THE MARKET LEADER TO PLAN, DEPLOY AND SCALE CYBERARK PRIVILEGE ON-PREMISES

SYSTEMS AND TARGETS PRIVILEGE ON-PREMISES SECURES INCLUDES:

- Windows Domain
- Unix Local Accounts
- Windows Local Accounts
- MS SQL
- Cisco Network Devices
- ServiceNow ITSM Systems
- Microsoft Azure Active Directory
- AWS IAM Credentials
- AWS Access Keys

For a full list please visit the CyberArk Marketplace

About CyberArk

CyberArk (NASDAQ: CYBR) is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security solutions for any identity – human or machine – across business applications, distributed workforces, hybrid cloud workloads, and throughout DevOps pipelines. The world's leading organizations trust Cyberark to help secure their most critical assets. To learn more about CyberArk, visit www.cyberark.com.

TOOLS WITH NO PLANS

Often, organizations purchase new security tools and find themselves left to their own devices to plan, integrate and deploy their new technology. Not surprisingly, this leads to security tools either being misconfigured or sitting on the shelf undeployed, which in turn brings customer frustration, anger and attrition. However, the more pressing issue is that these tools leave organizations with a false sense of security when, in reality, a misconfigured or unconfigured security solution isn't doing anyone any favors.

On the other hand, if vendors do offer hands-on onboarding and training, it often comes with an exorbitant (sometimes hidden) price tag, long and drawn-out timelines as well as a finite finish line. This creates stress for customer organizations as well as a ticking clock as soon as an engagement starts, since the organization knows they need to get every thing done by the end of the engagement.

THE CYBERARK JUMP START

Leaning on a wide range of experiences working with companies big and small to implement successful Identity Security programs, CyberArk created the Jump Start to help organizations reduce risk and stay secure. The Jump Start is designed to deliver positive business outcomes, maximize customer's return on investment in the CyberArk® Privilege On-Premises™ solution, the industry's leading Privileged Access Management (PAM) solution and drive a successful adoption. It follows a three-phase approach that can be scaled and repeatedly applied – helping customers achieve a rapid time-to-value on their newly purchased solution.

Discovery and Planning

The first phase helps determine the objectives, use cases, and priorities and starts by conducting Privileged Access Management and Architecture Design workshops. This includes several key components to help determine the overall privileged landscape of an organization. Together, with a CyberArk expert, organizations review their requirements and drivers to determine the objectives and use cases that need to be tackled. This includes a discovery session that is run based on a predefined set of questions informed by lessons learned through CyberArk deployments with over 6000 customers. The discovery session is designed to draw out information on the key factors in an organization's environment.

In this session, there is an in-depth review of critical risks, controls and roadmap using the CyberArk Blueprint recommendations and identification of the roles and responsibilities for the project team to deploy PAM and ultimately scale their program to secure additional use cases.

Second, an Architecture Workshop session is conducted to review the enterprise integrations, dependencies for executing the use cases on schedule, operational considerations, and technical status of the server builds; including directory services, authentication methods, monitoring strategies and integrations with other security tools. Then, together with the CyberArk expert, the organization reviews systems requirements and prerequisites for deployment readiness, such as: server deployment location(s), load balancing, change management and the change approval process. Finally, an offline review is performed to provide recommendations on Privilege On-Premises architecture design, integrations, deployment sequence and PAM program roadmap.

The Privilege On-Premises Pre-Implementation Checklist is used alongside the Privileged Access Management and Architecture Design workshops. The checklist must be completed to ensure that each party is ready for installation. This leads naturally into a planning session with a CyberArk expert to map out how to properly onboard accounts to Privilege On-Premises. In this planning session, the primary goal is to prioritize the use cases that are most important to the customer as well as reviewing the enterprise integrations and setting goals for how and when to achieve them. Additional consultation on where in the network CyberArk components should be deployed also delivers value and sets expectations early, facilitating a smooth implementation. This in turn informs the remainder of the Jump Start, which is created and delivered to the customer by a CyberArk expert. This is also the stage where the necessary personnel and access control processes are mapped out and identified for implementation.

The end result of this phase leaves the customer ready to implement and integrate CyberArk Privilege On-Premises into the environment.

Deployment

This deployment phase is when the action starts. Key Privilege On-Premises infrastructure is deployed, integrated and configured for the customer's environment. This phase also incorporates key organizational requirements and use cases identified in the Discovery portion and starts the onboarding of critical assets into the CyberArk Vault, including getting the User Portal set up for up to two administrators, and configuring the CyberArk Identity Cloud Connectors to enable secure MFA and SSO for Privilege On-Premises users. Tasks for this phase include setting up the basic workflow process templates for things like Dual Control Access/Permissions creation, establishing the onboarding process for accounts and other steps for organizational autonomy. This risk-based approach starts by onboarding the most critical and sensitive internal resources first and then continuing to onboard resources in order of most to least sensitive until all organizational objectives are met.

The end result of this phase is that the customer is now ready to successfully secure privileged accounts and access in the organization.

Expand and Secure

The third phase of the Jump Start focuses on expanding and securing the Privilege On-Premises deployment and sets finite and recurring goals for what comes next. Typically, there are three recurring fundamental actions that should be scaled and understood, including account onboarding, eliminating excess privileged accounts and collecting feedback from the organization's end users. To ensure alignment with customer priorities, the Jump Start establishes tailored best practices recommendations based on an organization's risk tolerance and the available resources who previously implemented use cases, building safes/groups and securing additional assets. CyberArk experts provide strategic advice for securing critical assets, including security best practices specific to each organization's environment.

The end result of this phase is that Privilege On-Premises is now fully implemented with supported processes that help to ensure the future proofing of the system. As the solution is being rolled out and deployed, the Jump Start also includes an option for Basic Administration self-paced training course which provides necessary knowledge for customers to administer and monitor the solution. The training is composed of several e-learning modules and the covered topics include architecture, access control, onboarding, master policy, platforms, and many more.

Three Phases of the Privileged Access Manager On-Premises Jump Start

PHASE 1
DISCOVERY AND PLANNING

- Team Introduction and role definitions
- Use case analysis
- Architecture considerations
- Authentication methods
- Goal setting for deployment phase

PHASE 2
DEPLOYMENT

- Deployment of Privilege On-Premises Components
- Common workflow demonstrations and core use case testing
- Assist with configuration of key CyberArk components
- Assist with baseline Access control model

PHASE 3
EXPAND & SECURE

- Provide strategic advisement for securing critical assets
- Develop recommendations and security best practices specific to the customer's environment
- Define an approach that helps you reach your overall PAM goals

CyberArk Privilege On-Premises

CyberArk® Privilege On-Premises solution is a part of the CyberArk Identity Security Platform, providing foundational controls for protecting, controlling, and monitoring privileged access across on-premises, cloud, and hybrid infrastructure. The solution helps organizations efficiently manage privileged credentials with strong authentication methods, proactively monitor and control privileged account activity, intelligently identify suspicious activity and quickly respond to threats.

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.