



SOLUTION BRIEF

CyberArk Privileged User SaaS Jump Start

THE CYBERARK JUMP START

CyberArk's Privileged User Software as a Service (SaaS) Jump Start helps ensure the customer is successful in starting their identity security and privileged access management (PAM) journey. Leaning on a wide range of experiences working with companies, big and small, to implement PAM programs, Jump Start is tailored to meet the most critical needs of each organization that chooses to implement CyberArk® Privilege Cloud.

The program follows a three-phase approach: Discovery and Planning, Deployment, and Expand and Secure. Outlined in more detail below, each phase can be scaled and repeatedly applied, helping customers achieve a rapid time-to-value on their newly purchased solution. Through the extensive CyberArk Partner Network, many channel partner representatives have achieved CyberArk Certified Delivery Engineer (CDE) certification and can deploy this solution. If your partner has completed the CyberArk Certified Delivery Engineer for Privilege Cloud (CDE-CPC) certification program, we recommend the CyberArk Privileged User SaaS Setup – Partner Plus package.

BENEFITS

- Ensures successful deployment as the customer begins their identity security journey
- Streamlines program launch to ensure long-term readiness and rapid return on investment
- Provides strategic advisement for securing critical assets by leveraging CyberArk's field-proven experience

LEARNING

Customers with the Jump Start service are eligible to take the CyberArk PAM Administration trainings from [CyberArk University](#), available in instructor-led or self-paced formats. Integrated knowledge transfer is also conducted, and free tutorials are available to supplement courses and provide quick references.

DISCOVERY AND PLANNING

The first phase starts by conducting two workshops: a PAM workshop and an Architecture workshop. This includes several key components to help determine the organization's overall privileged landscape. Alongside a CyberArk expert, the organization reviews its requirements and drivers to identify its objectives and use cases.

The PAM workshop reviews the enterprise integrations, dependencies for executing 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. During the Architecture workshop, the organization reviews system and project requirements and prerequisites. Recommendations are provided for the PAM SaaS architecture design, integrations, and deployment sequence, as well as tools to ensure customer readiness.

Upon completion of this phase, the customer is ready to implement and integrate CyberArk Privilege Cloud into the environment, along with several scheduled recurring meetings for priority use case workshops.

DEPLOYMENT

Next, the deployment of the solution commences. The Privilege Cloud Connector, run on a Windows server (physical or virtual), is deployed alongside the customer’s environment. The Connector acts as the broker between the customer’s internal resources and CyberArk’s Privilege Cloud to facilitate session isolation and password management.

This enables the CyberArk expert and the customer to walk through common workflows and use cases before integrating them into production. In this phase, we also perform all critical integrations and configurations, such as implementing secure MFA via CyberArk Identity or other IDP services, user provisioning, audit services via SIEM, etc.

After completing this phase, the customer is ready to successfully secure privileged accounts and access in the organization by executing the plan discussed during Discovery and Planning.

EXPAND AND SECURE

The third phase of Jump Start focuses on expanding and securing the Privilege Cloud deployment to achieve time-to-value. This starts with deploying the use cases defined in the Deployment stage, with an iterative process to progress toward the strategic goals. The iterative process includes four recurring fundamental actions, including onboarding privileged credentials, securing onboarded credentials, eliminating excess privileged accounts and collecting feedback from the organization’s end users. During this process, Jump Start establishes a series of recurring weekly touch points, aligning with the organization’s risk profile and corresponding critical resources, building safes, defining user access groups, and securing additional privileged credentials. CyberArk experts provide strategic advice and best practices to secure the most critical privileged credentials in the short term and to address lower-risk vulnerabilities over time.

At the end of this phase, Privilege SaaS is now implemented with supported processes and the most critical use cases to help ensure the future proofing and expansion of the system, and the customer is ready to expand on their program.

OUTCOME DETAILS

Privilege User SaaS Jump Start	Phase Outcomes	Outcome Description
Discovery and Planning Phase	<ul style="list-style-type: none"> • Solution architecture design • Solution design document • Prerequisite’s checklist • Use case prioritization • Identification of roles and responsibilities 	<ul style="list-style-type: none"> • Define agreed-upon solution architecture for the Deployment phase. • Prioritize use cases for the Expand and Secure phase. • Draft the solution design document, incorporating the outputs from the workshops. Outputs include architecture, deployment strategy, safe design, use case planning and use case prioritization. • Define project timelines, along with roles and responsibilities. • Identify relevant critical organizational process, such as a “break glass” strategy.

Privilege User SaaS Jump Start	Phase Outcomes	Outcome Description
Deployment Phase	<ul style="list-style-type: none"> • Deployment of connectors • Protection and integration of solution according to organizational requirements • Configuration of audit mechanisms • Deployment of additional components in scope, such as Remote Access 	<ul style="list-style-type: none"> • Solution is deployed and installation is complete. Connectors are set up according to organizational requirements, with availability, security and minimizing operational impact in mind. • The solution is protected by MFA and integrated with the organization's supported system for user provisioning. • Audit is set up to support compliance and audit requirements, as well as any additional components in scope based on use cases and organizational requirements. This can include Remote Access to support VPN-less connection to systems for internal and external teams, loosely connected devices to support password management in workstations that are not always connected to the network, etc.
Expand and Secure Phase	<ul style="list-style-type: none"> • Definition of use cases and supporting use case workshops 	<ul style="list-style-type: none"> • Use case covers planning of onboarding and testing of a platform based on technology, as planned during the Discovery and Planning stage. • This includes retrospective and building of a repeated process for onboarding and change management around privileged assets, which CyberArk will manage. • The customer is prepared to onboard accounts, manage secrets and secure privileged accounts with CyberArk through multiple technologies and components.
Training Credits	<ul style="list-style-type: none"> • Training credits as defined in scope (based on tier) 	<ul style="list-style-type: none"> • Recommendations are made for the CyberArk Privilege Cloud Administration training, either instructor-led or self-paced
Add-On to Jump Start	<ul style="list-style-type: none"> • Additional outcomes for use cases, connectors, components and integrations 	<ul style="list-style-type: none"> • Add-on services are available to expand and scale additional use cases, connectors deployment, components and integrations.

NEXT STEPS

Contact your designated sales account executive to learn more about the CyberArk Privileged User SaaS 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.



©Copyright 2022 CyberArk Software. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners. U.S., 07.22. Doc. TSK-1874

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.