CYBERARK®

WHITE PAPER

SECURING HYBRID CLOUD ENVIRONMENTS AND WORKLOADS ON AMAZON WEB SERVICES (AWS)

CyberArk.com

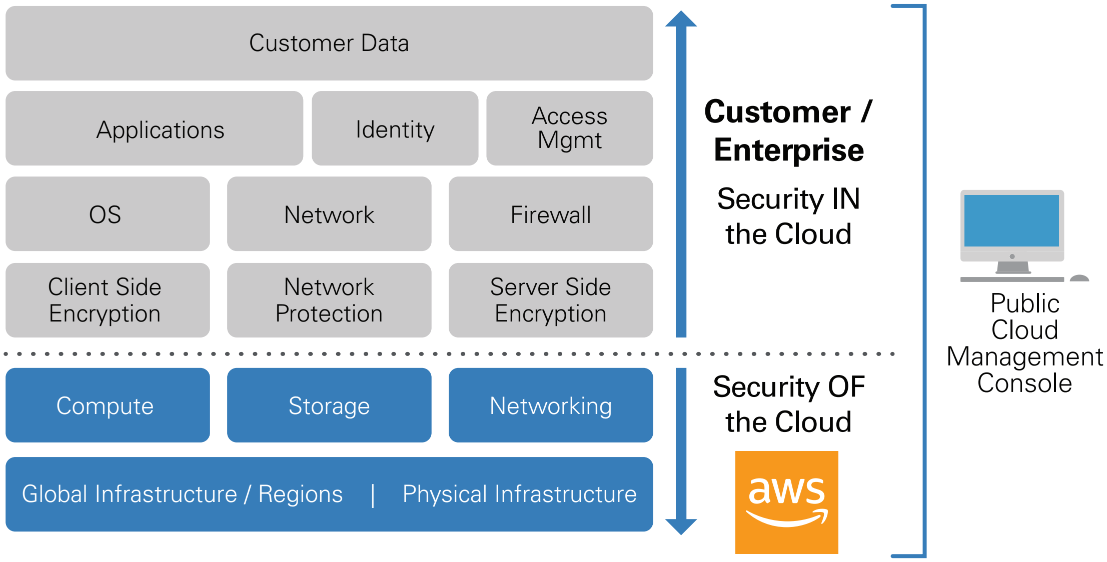
Table of Contents

Introduction: Securing Hybrid Workloads

Organizations embark on a cloud journey for a variety of reasons. Some are native cloud, or "all-in" cloud from the start, and they don't need to make the journey from on-premises to cloud. More typically, organizations migrate segments of their business over time from on-premises to the cloud – even as part of a "Cloud-First" strategy. Thus, they operate in hybrid environments, with both on-premises and cloud environments to secure.

Hybrid environments impact established IT security systems and practices. They expand attack surfaces, introduce new types of threats, and alter security management roles and responsibilities. Organizations increasingly recognize that they must adopt new security tools and methodologies to efficiently monitor, control and protect hybrid environments.

Robust security is a critical requirement for organizations. In a traditional on-premises implementation, corporate security teams are responsible for safeguarding the underlying IT infrastructure (compute, storage and network platforms) as well all the applications and content running and residing in the data center. For cloud, it is important for organizations to recognize that security in the cloud is a shared responsibility between the public cloud vendor and the organization. AWS goes to great efforts to ensure the security OF the cloud infrastructure, including the compute, storage and networking resources as well as the physical infrastructure. However, each of the public cloud vendors are very clear that security in the cloud is a shared responsibility, and that the organization, as the application owner, is responsible for protecting their applications, data, the OS and other enterprise infrastructure, as well as other workloads running IN the cloud. Essentially, the organization is responsible for securing everything above the hypervisor or equivalent layer.



Regardless of where organizations are in their cloud journey, CyberArk's goal is to enable them to protect their cloud workloads by providing powerful solutions for securing privileged accounts and credentials at each stage of the journey. CyberArk offers cloud automation tools and integrations to simplify and accelerate the deployment of CyberArk solutions in AWS.

Securing Hybrid Cloud Environments

Hybrid clouds introduce a myriad of challenges for IT security organizations. They expand attack surfaces, introduce new types of threats, and can challenge security management roles and responsibilities.

Securing the operations of both the cloud and on-premises environments is one of the unique challenges of hybrid environments. This can be even more challenging when organizations use multiple cloud vendors and operate multiple on-premises environments. To consistently enforce security and access policies across hybrid environments, it is important to establish a single control point for the on-premises and cloud environments. Typically this is achieved by using the same privileged account security solution, so that enterprises can consistently enforce security policies regardless of the different compute environments and development pipelines.

CyberArk Privileged Account Security Solution

The CyberArk Privileged Account Security Solution is designed from the ground up to provide robust privileged account access control for on-premises, cloud and hybrid cloud environments. The solution protects, manages and audits user and application credentials, provides least-privileged access, controls applications, and secures, monitors, and analyzes all privileged activity—actively alerting on anomalous behavior. An isolated vault server, unified policy engine, comprehensive discovery engine and multiple layers of security provide unmatched protection for privileged accounts, while ensuring high scalability and reliability.

In an AWS hybrid cloud implementation, the CyberArk solution helps enterprise IT security teams:

- Centrally manage privileged account access controls for on-premises infrastructure and AWS-based resources
- Easily revoke privileges or update security credentials in response to threats or attacks.

The CyberArk Privileged Account Security Solution helps organizations mitigate risks and simplify operations by eliminating administrative silos, increasing automation and implementing consistent security practices and policies across on-premises and AWS-based workloads. For customers implementing multi-cloud architectures, the solution can be extended across different cloud providers.

Deploying the CyberArk Privileged Account Security Solution on AWS

The CyberArk Privileged Account Security Solution is comprised of a collection of tightly integrated functional components that can be deployed in various configurations for ultimate flexibility, scalability and resiliency. Architectural components can be installed on-premises and/or in the cloud to satisfy diverse customer environments and business requirements.

The core elements of the CyberArk Privileged Account Security Solution include:

- CyberArk Enterprise Password Vault – used to discover, secure, rotate and control access to privileged account passwords
- CyberArk Privileged Session Manager – used to isolate, monitor, record and control privileged sessions
- CyberArk SSH Key Manager – used to secure, rotate, monitor and control access to SSH keys associated with privileged account.

The additional components enable CyberArk to be configured to support a variety of use cases. (See sidebar for details on additional components)

Architecting CyberArk in Hybrid AWS Environments

From an architectural and performance perspective, the typical best practice (and preferred approach) is to deploy the CyberArk components; Password Vault Web Access, Central Password Manager, CyberArk Privileged Session Manager and CyberArk Privileged Session Manager SSH Proxy in the same computing environment. For optimal performance, the components must be close, from a network perspective, to the managed devices. CyberArk supports a distributed architecture which is designed to allow multiple instances of the components to be deployed – so components can be located on both the on-premises and AWS environments.

There are various architectural approaches for deploying the CyberArk Privileged Account Security Solution in a hybrid environment. The key decisions to make are where to deploy the primary and DR vaults, and then determine how to deploy the components to efficiently support privilege requests in the on-premises, AWS and any other computing and development environments. In organizations with hybrid environments that are already using a privileged account security solution, the solution will have already been deployed by the organization to help secure the on-premises environment. In this case, the primary and DR vaults will run in the on-premises data center and instances of the components will need to run in both the on-premises and hybrid environments.

CyberArk offers cloud automation capabilities to help customers establish a complete CyberArk Privileged Account Security environment on AWS. CyberArk's AMI and CloudFormation Templates enable a complete CyberArk environment (including the primary and DR (Disaster Recovery) vaults, all the components and session monitoring) to be conveniently built and deployed in as little as 15 minutes in a native AWS environment. However, while this is very powerful for customers with "all in," or native-cloud environments, unless organizations have fully adopted the cloud, most organizations will have some form of a hybrid environment. The CyberArk's AMI and CloudFormation Templates can be configured to support hybrid environments. However, by necessity, there are more manual steps required when the on-premises environment is already established (e.g., to establish secure communication paths between the cloud and on-premises environments with a VPN).

CyberArk Privileged Account Security Solution Architectural Components

CyberArk Privileged Account Security Solution architectural components include:

Password Vault – provides secure storage and sharing of privileged account credentials, audit data, and sessions, using multiple layers of encryption and security. Includes a discovery engine that automatically detects new devices and changes to privileged account credentials.

Password Vault Web Access (PVWA) – a fully-featured web interface that provides a unified console for requesting, accessing and managing privileged account credentials.

Privileged Session Manager – secures, controls and monitors access to privileged accounts across the hybrid environment. Decouples end-users from targets, enabling secure connections to privileged devices without divulging passwords.

Privileged Session Manager SSH Proxy – similar to the Privileged Session Manager, but acts as a proxy for SSH-enabled devices. Controls access to privileged sessions and initiates SSH connections to remote devices on behalf of the user without disclosing SSH credentials.

Central Password Manager (CPM) – automatically enforces corporate security policies across the hybrid environment. Capable of generating new random passwords, replacing existing passwords on remote machines and saving the new passwords in the vault without human interaction.

All architectural components can be installed in a redundant fashion for high availability.

In hybrid environments the CyberArk CloudFormation Templates (CFT) can be used to build a complete CyberArk environment in AWS or simply to build the components in AWS which then to link with the vaults installed in the on-premises environment. Once built, the components will need to be linked to the vaults using a secure communications path.

For hybrid environments the CyberArk AMI and CyberArk CloudFormation Templates (CFTs) should be used as a reference architecture and configured by the enterprise to meet the requirements of their unique environment. There are, of course, many different hybrid environments and potential deployment configurations (contact your CyberArk sales representative for additional information).

Typical Hybrid Configurations

Two typical hybrid configurations are shown in the diagrams below. Note, the diagrams have been simplified to show a single AWS cloud environment and a basic DR vault configuration. Of course, the CyberArk architecture is very flexible and has been configured to support complex and demanding environments at some of the largest enterprises.

The first diagram, of an extended configuration, shows the Vault (Primary and DR) running on-premises and managing infrastructure and workloads in the on-premises environment and extended out to manage infrastructure and workloads running on the AWS cloud. Here, the CyberArk components running on AWS have been built leveraging CyberArk's CFT and AMI automation capabilities.

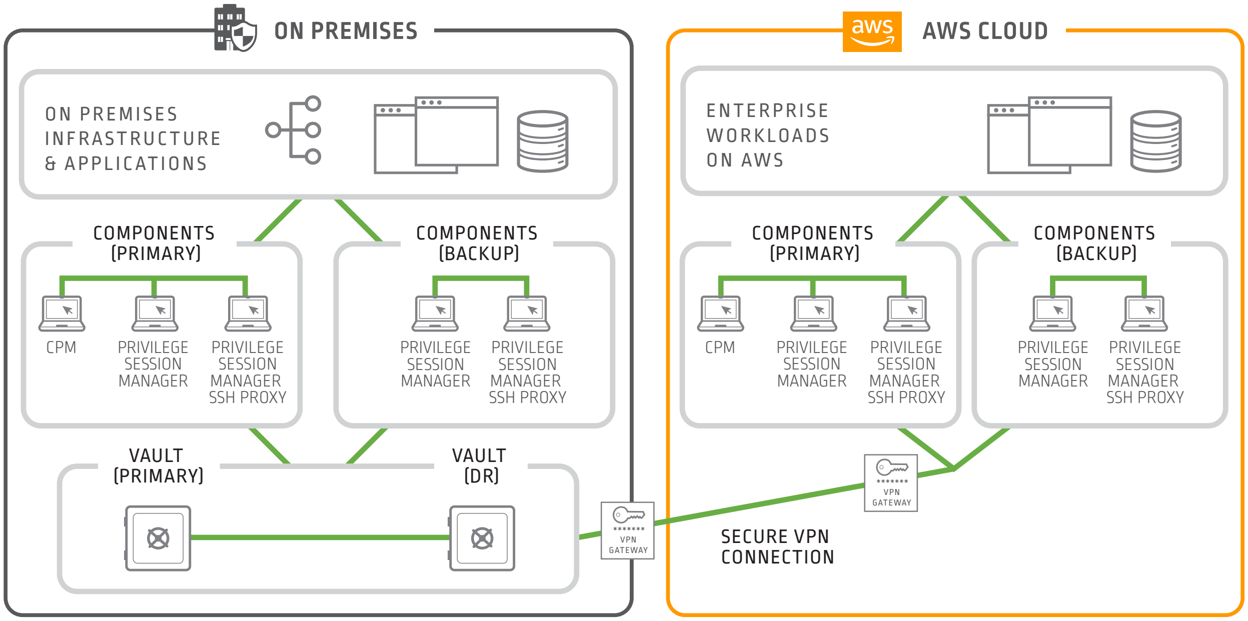
Configuration Example 1 – Existing On-Premises CyberArk Customer Introducing AWS-Based Workloads as Part of a Hybrid Cloud Initiative

The first configuration represents an existing CyberArk customer introducing AWS, for example, to run new applications on AWS or as part of a phased workload migration program to AWS. In this example, the customer is currently using the CyberArk Privileged Account Security Solution to secure its on-premises infrastructure and is extending the solution to secure new AWS workloads.

In this scenario, the primary and DR vaults, and other architectural components are already installed in the customer's on-premises data center. The primary and DR vaults will remain on premises, acting as a central control point for managing privileged credentials across the hybrid environment. Additional solution components can be installed on AWS using the CyberArk CFT and AMI automation capabilities. The integrated solution protects, manages and audits credentials across the on-premises and cloud infrastructure in a unified fashion.

Later in the organization's cloud journey, when for example the on-premises data center running CyberArk is closed, the primary and DR vaults can be moved to run on AWS.

EXTEND PRIVILEGED ACCOUNT SECURITY FROM ON-PREMISE TO THE AWS CLOUD


ON PREMISES
ON PREMISES INFRASTRUCTURE & APPLICATIONS
COMPONENTS (PRIMARY)
CPM
PRIVILEGE SESSION MANAGER
PRIVILEGE SESSION MANAGER SSH PROXY
COMPONENTS (BACKUP)
PRIVILEGE SESSION MANAGER
PRIVILEGE SESSION MANAGER SSH PROXY
VAULT (PRIMARY)
VAULT (DR)
VPN GATEWAY
aws
AWS CLOUD
ENTERPRISE WORKLOADS ON AWS
COMPONENTS (PRIMARY)
CPM
PRIVILEGE SESSION MANAGER
PRIVILEGE SESSION MANAGER SSH PROXY
COMPONENTS (BACKUP)
PRIVILEGE SESSION MANAGER
PRIVILEGE SESSION MANAGER SSH PROXY
VPN GATEWAY
SECURE VPN CONNECTION

Components Built and Deployed with CyberArk CloudFormation Templates (CFT) for AWS

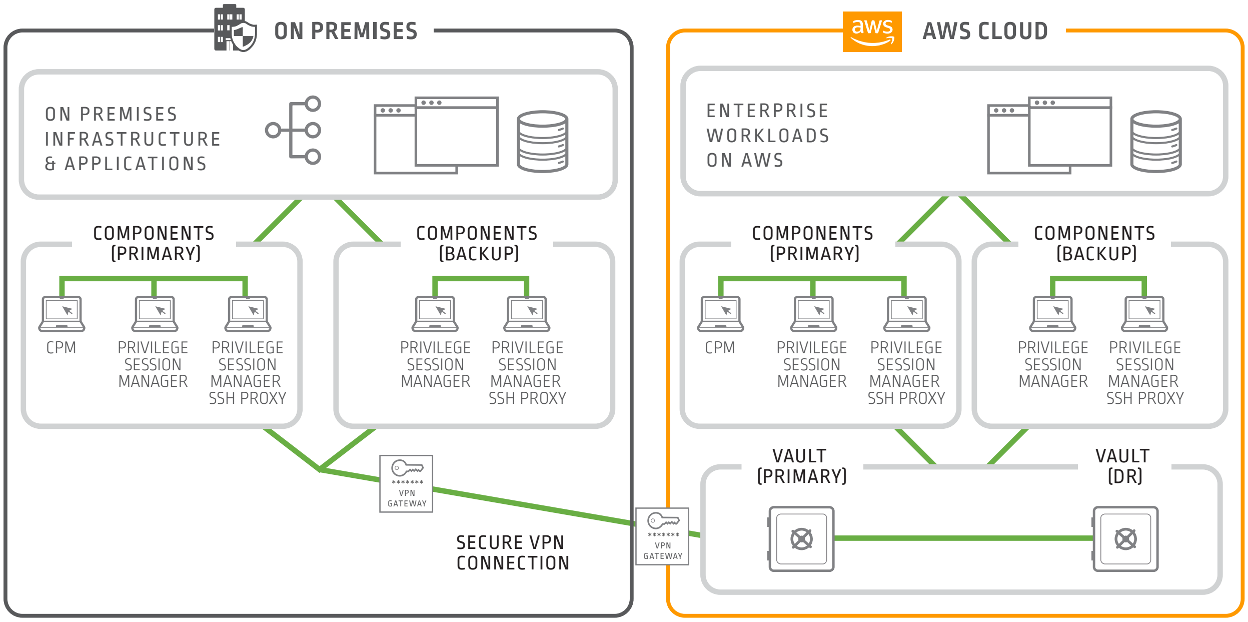
Configuration Example 2 – CyberArk Running on AWS and Managing On-Premises Workloads and Infrastructure

The second configuration represents an enterprise that has already deployed CyberArk in their AWS environment, including the Vaults, and plans to run CyberArk on the cloud to secure on-premises infrastructure.

For example, the enterprise has adopted a "Cloud-First" approach and leverages AWS as its primary compute platform for new initiatives, but still plans to secure some legacy on-premises applications. In this scenario, the primary and DR vaults, and other solution components are installed on AWS using the CyberArk CFT and AMI automation capabilities. Additional instances of the components are installed in the customer's data center using established CyberArk deployment tools.

Here, CyberArk runs on AWS to serve as a central control point for enforcing and monitoring access privileges across the hybrid environment, enabling CISO and IT leaders to protect, manage and audit credentials across the on-premises and cloud infrastructure in a unified fashion.

USE CLOUD TO SECURE PRIVILEGED ACCOUNTS FOR ON-PREMISE AND CLOUD WORKLOADS


ON PREMISES
ON PREMISES INFRASTRUCTURE & APPLICATIONS
COMPONENTS (PRIMARY)
CPM
PRIVILEGE SESSION MANAGER
PRIVILEGE SESSION MANAGER SSH PROXY
COMPONENTS (BACKUP)
PRIVILEGE SESSION MANAGER
PRIVILEGE SESSION MANAGER SSH PROXY
VPN GATEWAY
SECURE VPN CONNECTION
aws
AWS CLOUD
ENTERPRISE WORKLOADS ON AWS
COMPONENTS (PRIMARY)
CPM
PRIVILEGE SESSION MANAGER
PRIVILEGE SESSION MANAGER SSH PROXY
COMPONENTS (BACKUP)
PRIVILEGE SESSION MANAGER
PRIVILEGE SESSION MANAGER SSH PROXY
VPN GATEWAY
VAULT (PRIMARY)
VAULT (DR)

Complete Privileged Account Security Solution Built and Deployed with CyberArk CloudFormation Templates

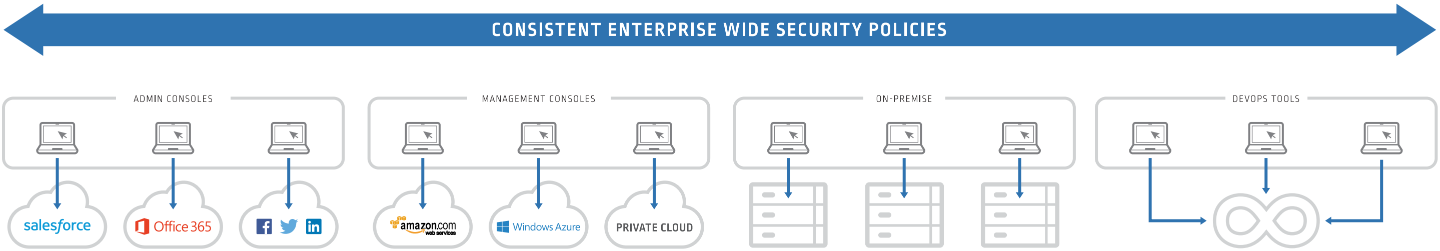
Note, to simplify the diagrams the additional layers of hardening, redundancy and security used in a typical deployment are not shown.

Also note, a separate dedicated network is used to connect the Vault to the CyberArk Privileged Account Security components in each of the computing environments. As part of the hardening process, a secure connection, such as a VPN, should be used and configured, so that the Vault can only be accessed by the CyberArk components.

Summary

CyberArk solutions enable organizations to protect their cloud workloads by providing powerful solutions for securing privileged accounts and credentials at each stage of their cloud journey. CyberArk offers several powerful integrations with AWS, so an organization can increase the security of its cloud workloads. Examples include integration with AWS CloudWatch to support automated on-boarding of SSH keys when new EC2 compute instances are launched by Auto Scaling and other processes. Other integrations include AWS Security Token Service for secure single sign-on to the management console, and AWS Inspector for discovery. CyberArk's cloud automation tools also simplify and accelerate the deployment of CyberArk solutions in the public cloud.

Another important consideration, for protecting an enterprise's cloud workloads, is that a significant number of organizations don't use just one cloud provider, but use multiple cloud providers for various reasons – business flexibility, multiple business lines, prior acquisitions, geographic coverage, etc. Additionally, for organizations that have legacy, on-premises or hybrid environments, the same IT administrators may access and manage multiple compute, DevOps tools and automation environments. CISOs and IT leaders typically want, as a best practice, to be able to enforce the same privileged security policies across the entire enterprise regardless of compute environments, delivery pipelines and automation tools.



To implement this best practice, enterprises typically want to manage user credentials and access permissions with a single solution.

Whether your organization has fully embraced cloud or is just starting the journey, it is essential to implement robust privilege management policies to protect cloud and hybrid workloads, and DevOps environments. CyberArk has the solutions, resources and cloud expertise to help your enterprise protect and secure the "keys to your cloud kingdom."

For additional information visit www.cyberark.com/cloud

APPENDIX

Amazon Web Services and CyberArk

Amazon Web Services (AWS) is widely recognized as a leading provider of public cloud services, offering organizations of all sizes a highly reliable, scalable, low-cost infrastructure platform in the cloud. AWS has grown dramatically since its inception just over 11 years ago, and today, AWS serves several hundreds of thousands of businesses in some 190 countries, and operates data centers around the globe.

For customers, the AWS platform offers a broad and ever-increasing array of capabilities and computing resources, including various compute and storage resources as well as many other services. For example, the Amazon EC2 (Elastic Compute Cloud), and S3 (Simple Storage Service), are widely used. Within each service there is a broad range of sub-services available, such as graphics intensive, burstable, high I/O, as well as general purpose compute resources – and similarly for storage. Various databases, networking and some basic security services are also offered as well as tools to build and develop applications.

In addition to internal AWS capabilities, AWS also enables enterprise-focused solutions from third-party vendors like CyberArk.

CyberArk's priority is to help to ensure that organizations including large enterprises can more fully secure and protect their cloud workloads running on AWS. CyberArk has worked closely with AWS at the technical level to ensure that our offerings are optimized for AWS and meet both the AWS architectural requirements, as well as CyberArk's Security Fundamentals for Privileged Account Security.

CyberArk serves a growing group of enterprise customers that are using CyberArk solutions to help protect and secure their cloud workloads running on AWS. The configurations and customer needs can vary significantly depending on the customers' business objectives. For example, in some cases customers run the primary and disaster recovery CyberArk vaults on AWS, while in others a hybrid environment is used. CyberArk continues to expand its AWS focused capabilities, and today, for example, a complete CyberArk environment can be set up on AWS in a matter of minutes using CyberArk cloud automation tools.

Additionally, CyberArk has various integrations with AWS. For example, some customers taking advantage of on-demand computing using AWS Auto Scaling have used CyberArk's Lambda function to help ensure privileged accounts and credentials are immediately secured when new application instances are detected by AWS CloudWatch.

CyberArk's technical teams around the globe have developed deep expertise by working closely with organizations on their AWS cloud journey, as they move from evaluation, to deployment and into production. In some cases customers have shut down their data centers and migrated completely to the cloud, relying on CyberArk solutions to help ensure the security of their on-premises, hybrid, and "all-in" cloud environments.

CyberArk works with, and offers solutions and guidance to, organizations at each stage of their cloud journey – from evaluating security needs during an initial migration to helping ensure the enhanced security of an enterprise embracing a "Cloud-First" strategy.

©Copyright 1999-2017 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., 11.2017. Doc # 175

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.

THIS PUBLICATION IS FOR INFORMATIONAL PURPOSES ONLY AND IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER WHETHER EXPRESSED OR IMPLIED, INCLUDING WARRANTY OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, NON-INFRINGEMENT OR OTHERWISE. IN NO EVENT SHALL CYBERARK BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND IN PARTICULAR CYBERARK SHALL NOT BE LIABLE FOR DIRECT, SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE OR LOSS OF USE, COST OF REPLACEMENT GOODS, LOSS OR DAMAGE TO DATA ARISING FROM USE OF OR IN RELIANCE ON THIS PUBLICATION, EVEN IF CYBERARK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.