

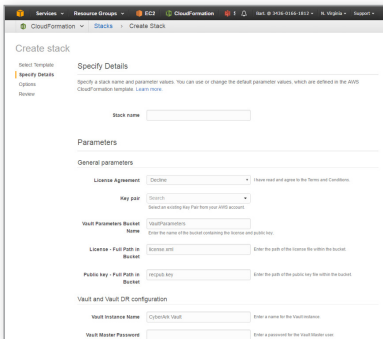


**CYBERARK**<sup>®</sup>

# CyberArk Cloud Automation Capabilities: CyberArk AMIs for AWS

## Key Benefits

- Unparalleled protection of cloud assets with CyberArk Enterprise Password Vault<sup>®</sup>
- Automated deployment in as little as 15 minutes
- Optimized for helping secure AWS assets, and to deploy and run on AWS
- Designed for flexible configuration when required



*User Interface for CyberArk's AWS CloudFormation templates which automate and simplify the set up the CyberArk Privileged Account Security Solution.*

In as little as 15 minutes, administrators can automatically deploy and establish a CyberArk Privileged Account Security environment and begin securing privileged accounts in AWS

## CyberArk AMIs for CyberArk Privileged Account Security Solution, including the CyberArk Enterprise Password Vault<sup>®</sup>

### The Challenge

Enterprises, especially those adopting cloud-first strategies to transform their business, increasingly recognize it is their shared responsibility, not just the cloud vendors', to secure their applications and other assets in the cloud.

IT, security and DevOps leaders want to use automation tools to rapidly and securely deploy and run CyberArk Privileged Account Security solutions, including CyberArk Enterprise Password Vault<sup>®</sup>, CyberArk Privilege Session Manager<sup>®</sup> and CyberArk SSH Key Manager<sup>™</sup>, on AWS (Amazon Web Services) so as to protect the enterprise's cloud assets. Specifically, organizations want to use CyberArk solutions to control, automate, audit and analyze the privileges and credentials associated with their AWS Management Consoles, to configure and manage virtual infrastructure, to enable their applications to connect with data and other sensitive assets, and to dynamically scale elastic production environments – all critical to effective enterprise cloud security strategies.

CyberArk customers migrating to the cloud, and already using CyberArk Privileged Account Security solutions to secure and protect their on-premises environments also want the same level of robust protection and security for the privileged accounts and credentials used in their cloud environments.

### The Solution

Using CyberArk cloud automation capabilities, in as little as 15 minutes, administrators can automatically deploy and establish a complete CyberArk Privileged Account Security environment in their preconfigured AWS environment, so that it is quickly and simply available to start securing the enterprise's cloud assets. The CyberArk environment established by the automation tools can include the CyberArk Enterprise Password Vault, CyberArk Privileged Session Manager, CyberArk SSH Key Manager, and a disaster recovery (DR) vault. The standard deployment architecture leverages AWS privileged account security best practices, including separate AWS Availability Zones for the cloud assets, and the primary and DR vaults, thus ensuring that the vaults are both independent from each other, and the cloud assets being secured. The cloud automation capabilities include CyberArk AMIs (Amazon Machine Images) and AWS CloudFormation templates to automate the deployment of CyberArk solutions. Additional AWS CloudFormation templates from CyberArk automate configuring the AWS VPCs (Virtual Private Clouds), private and public subnets, Security Groups and other elements of the AWS environment to prepare for the automated deployment of CyberArk solutions.

## Key Features and Benefits

**Unparalleled protection of cloud assets** – Provides CyberArk’s highly robust and secure privileged account security solutions to enterprises that have all-in-cloud deployments and other configurations. Complies with CyberArk’s Security Fundamentals for Privileged Account Security and Digital Vault Security Standard that have become the gold standard in privilege account security, trusted by enterprises across the globe to secure the keys to their IT kingdoms.

**Automated deployment in as little as 15 minutes** – With a single click administrators can simply deploy, in as little as 15 minutes, a complete CyberArk Privileged Account Security solution running in their preconfigured AWS environment. The CyberArk solution, established by CyberArk’s cloud automation capabilities, includes separate primary and DR vaults, each in their own independent AWS Availability Zones.

**Optimized to deploy, run and secure AWS** – The design is optimized for AWS and follows AWS privileged account security architecture best practices for deploying and running CyberArk solutions, so that CyberArk solutions can help organizations optimally secure the privileges and credentials associated with the enterprise’s AWS assets. The solution leverages AWS CloudFormation templates for rapid deployment and VPCs for enhanced security and separation of the primary and DR vaults.

**Flexible configuration if required** – While the standard configuration deployed with the automation capabilities enables a single CyberArk solution to support up to potentially thousands of AWS accounts and VPCs, the flexible, modular architecture allows the CyberArk Privileged Account Security solution to be adapted, as necessary, to meet the needs of a broad range of enterprise cloud architectures with varying workflows and cloud footprints. Note, some large enterprises with complex infrastructure environments may choose to build their own AMIs to deploy CyberArk solutions, instead leveraging the CyberArk AMIs and deployment architecture as reference models.

## Why CyberArk?

CyberArk is the only security company focused on eliminating the most advanced cyber threats; those that use insider privileges to attack the heart of the enterprise’s cloud and on-premises environments. Dedicated to stopping attacks before they stop business, CyberArk proactively secures against cyber threats before attacks can escalate and do irreparable damage. CyberArk is trusted by the world’s leading companies to protect their highest value information assets, infrastructure and applications.

CyberArk enables enterprises to protect their cloud assets by providing powerful solutions for securing privileges and credentials at each stage of their cloud journey. With CyberArk enterprises can consistently enforce security policies regardless of their compute environments, development pipelines, DevOps and automation tools. Additionally, CyberArk cloud automation tools simplify and accelerate the deployment of CyberArk in the public cloud.

Other CyberArk cloud security capabilities for AWS, include an integration with Amazon Inspector to simplify discovery and prioritization of privileged account risk, enhanced AWS Access Key protection, and an integration with the AWS Security Token Service to allow secure single sign-on to the AWS Management Console.

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., 05.17. Doc # 161

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.

©CyberArk Software Ltd. | [cyberark.com](http://cyberark.com)

## Additional Information

- Refer to the whitepaper “*Securing the Enterprise’s Cloud Assets on Amazon Web Services (AWS)*” for additional information on using CyberArk solutions to secure assets on AWS.
- Refer to the deployment guide “*Deploying Privileged Account Security on Amazon Web Services*”, for additional information and deployment instructions, including how to set up the AWS environment prior to the automated deployment of the standard CyberArk configuration.
- Contact CyberArk sales or customer support for access to the CyberArk AMIs for AWS and the CyberArk CloudFormation templates.
- Note: valid CyberArk license(s) and a pre-configured AWS environment are required prior to accessing and activating the CyberArk AMIs for AWS and CyberArk CloudFormation templates.
- [cyberark.com/cloud](http://cyberark.com/cloud)