CYBERARK®

WHITEPAPER

Five Ways to Improve Privileged Access Management with AWS Managed Services and CyberArk

aws

Table of Contents

Introduction

Privileged access management is cited as a major concern for enterprises as they move their workloads to Amazon Web Services (AWS) cloud environments. Managing accounts with elevated permissions allows organizations to control risk by reducing their attack surface and mitigating the impact of privilege misuse. AWS Managed Services (AMS) helps customers to manage their AWS infrastructure more efficiently and securely. AMS provides access management controls by scoping down AWS IAM using least privilege principles and scanning for common IAM misconfigurations.

Securing and monitoring privileged access remains one of the largest security concerns in the enterprise cloud journey. For customers that have implemented CyberArk or plan to implement CyberArk in the future, strategic placement and configuration of your CyberArk **Privileged Access Management Solution in an AMS** implementation enriches the cloud security posture by adding additional configuration options for protecting, controlling, and monitoring privileged access across on-premises, cloud, and hybrid infrastructure.

Enterprises want to adopt AWS at scale but often the skills that have served them well in traditional IT do not always translate to success in the cloud. Organizations must transform with new skills, tools and processes, while maintaining compliance and accelerating innovation to drive their businesses. AWS Managed Services (AMS) is designed to solve these use cases for enterprises, enabling them to migrate to AWS at scale more quickly, reduce their operating costs, improve security and compliance and focus on their differentiating business priorities.

CyberArk can assist AMS customer success in the cloud by helping you:

- **Reduce security risk** by strengthening privileged AMS account access controls and safeguarding privileged account credentials.
- **Improve oversight and compliance** by proactively monitoring and controlling privileged AMS account sessions and intelligently identifying suspicious activity.
- **Enhance access controls and streamline internal access** by utilizing the CyberArk Privileged Session Manager as a bastion host to monitor and isolate sessions, manage access to applications and commands directly from a user's local workstation.
- **Optimize investments** by enriching established privileged access management solutions and practices to AMS.

If your company plans to deploy to AMS, this white paper explains five ways CyberArk and AMS can help reduce privileged access risk, improve visibility and control, and simplify operations.

You will learn how CyberArk Privileged Access Management solutions can help your organization:

1. Isolate, monitor, and control AWS Management Console sessions to strengthen security.
2. Provide an isolated and monitored RDP session directly to an internal instance from your local workstation.
3. Secure and manage ServiceNow IT Service Management account credentials to reduce risk.
4. Isolate, monitor, and control AWS Systems Manager Session Manager sessions to bolster security.
5. Integrate with AWS Security Hub to centralize and unify security monitoring and forensics.

CYBERARK PRIVILEGED ACCESS MANAGEMENT COMPONENTS

- **Enterprise Password Vault** – a hardened and secured digital repository used to store privileged AMS account information.
- **Password Vault Web Access** – a fully featured web interface that provides a single console for requesting, accessing, and managing privileged AMS account credentials.
- **Central Policy Manager** – a single authority that enforces enterprise security policies by automatically changing passwords and rotating SSH keys on remote machines and storing new passwords or keys in the vault—all without human interaction.
- **Privileged Session Manager** – a central access control point used to isolate, monitor and control all privileged sessions. Acting as a secure proxy server, the PSM separates endpoints from AMS target systems and isolates privileged user sessions.
- **Privileged Threat Analytics** – an advanced analytics engine that continuously monitors the use of privileged AMS accounts, identifies suspicious actions, and detects in-progress attacks.

USE CASE #1

Use CyberArk to Isolate, Monitor, and Control AWS Management Console Sessions

You can use CyberArk Privil to secure and monitor interactive access to the AWS Management Console, leveraging AWS Identity and Access Management (IAM) roles.

CyberArk Components Utilized

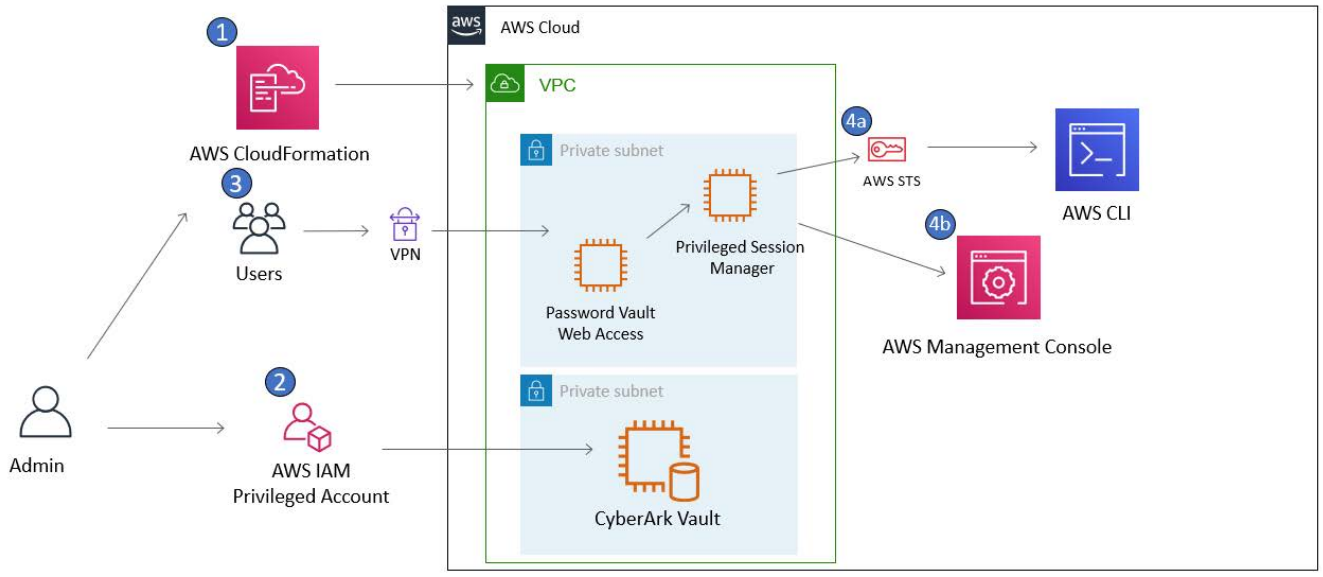
- Enterprise Password Vault
- Password Vault Web Access
- Privileged Session Manager

How it Works

1. The CyberArk solution is deployed in your Amazon Virtual Private Cloud (Amazon VPC) by AMS.
2. AWS Management Console accounts (IAM privileged account identities) are onboarded to the CyberArk Enterprise Password Vault.
3. Privileged users authenticate to the Password Vault Web Access portal.

4a. CyberArk Privileged Session Manager leverages the role associated to the vaulted AWS IAM credential to generate an AWS Security Token Service (STS) token and launch a monitored CLI session
or

4b. Privileged Session Manager leverages Vaulted AWS IAM credentials to establish a secure session to the AWS Management Console.



Benefits

- Improves security by isolating and controlling privileged sessions.
- Reduces exposure by ensuring AWS Management Console credentials are not disclosed to users.
- Improves compliance and forensics by monitoring and recording privileged sessions.
- Simplifies adoption by leveraging standard AWS identity management systems and practices for role-based access control.

USE CASE #2

Use CyberArk PSM to access AWS instances directly from a local workstation

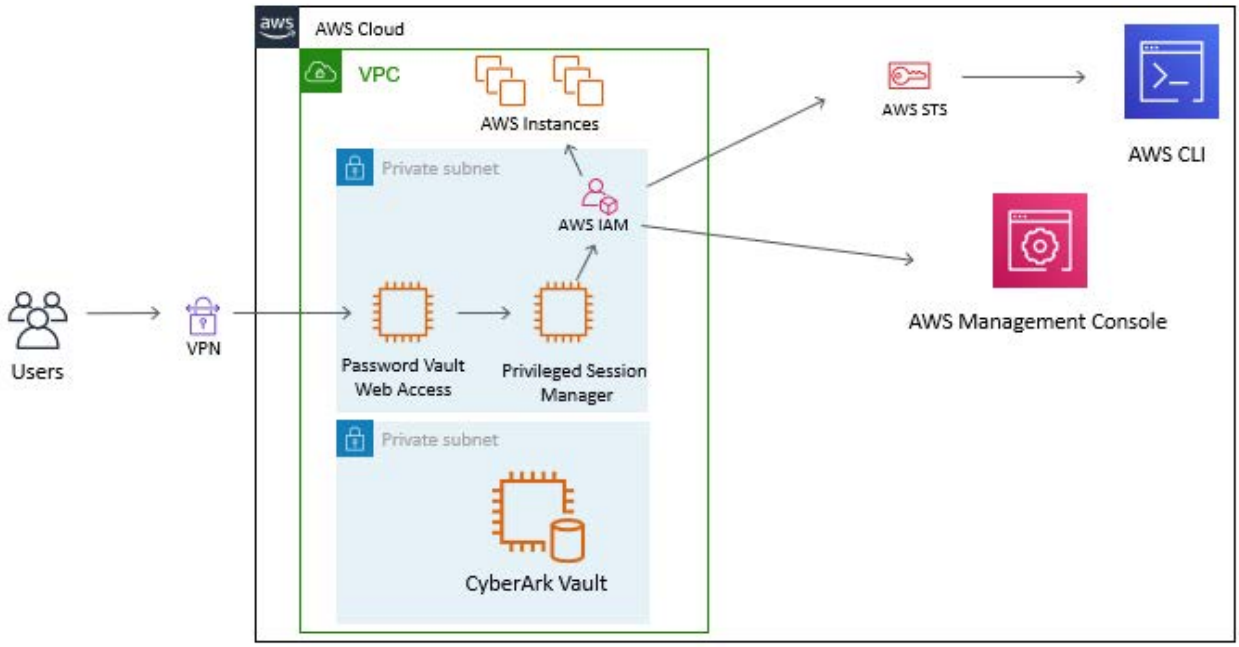
The CyberArk solution can be used as an additional security layer by allowing administrators to granularly control access to applications or administrative commands from a monitored session that can be launched directly from user's local workstation.

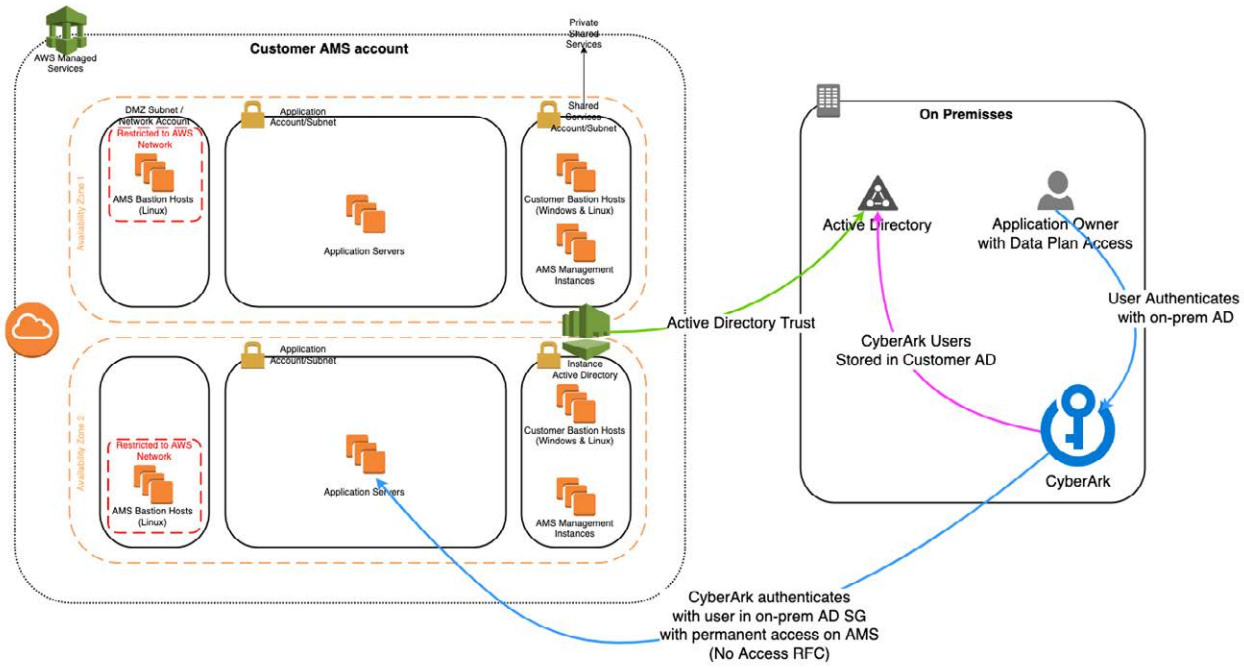
CyberArk Components Utilized

- Enterprise Password Vault
- Password Vault Web Access
- Privileged Session Manager

How it Works

- The CyberArk solution is deployed in your Amazon VPC by AMS and acts as a proxy server (bastion host) for the AMS environment. (The Password Vault Web Access component is deployed in a private subnet).
- Privileged users authenticate to the Password Vault Web Access portal over a secure VPN connection or AWS PrivateLink. (AWS supports a variety of VPN connection methods)
- Privileged Session Manager isolates privileged users, establishing distinct sessions with target systems without exposing private addresses to the outside world.





Benefits

- Improves ease of access to internal instances by leveraging PSM to function as a bastion host.
- Strengthens security by isolating privileged users and minimizing attack surfaces.
- Improves compliance and forensics by monitoring and recording privileged sessions.
- Simplifies adoption by supporting a variety of AWS-sanctioned VPN connectivity methods.

USE CASE #3

Use CyberArk to Secure and Manage ServiceNow ITSM Account Credentials

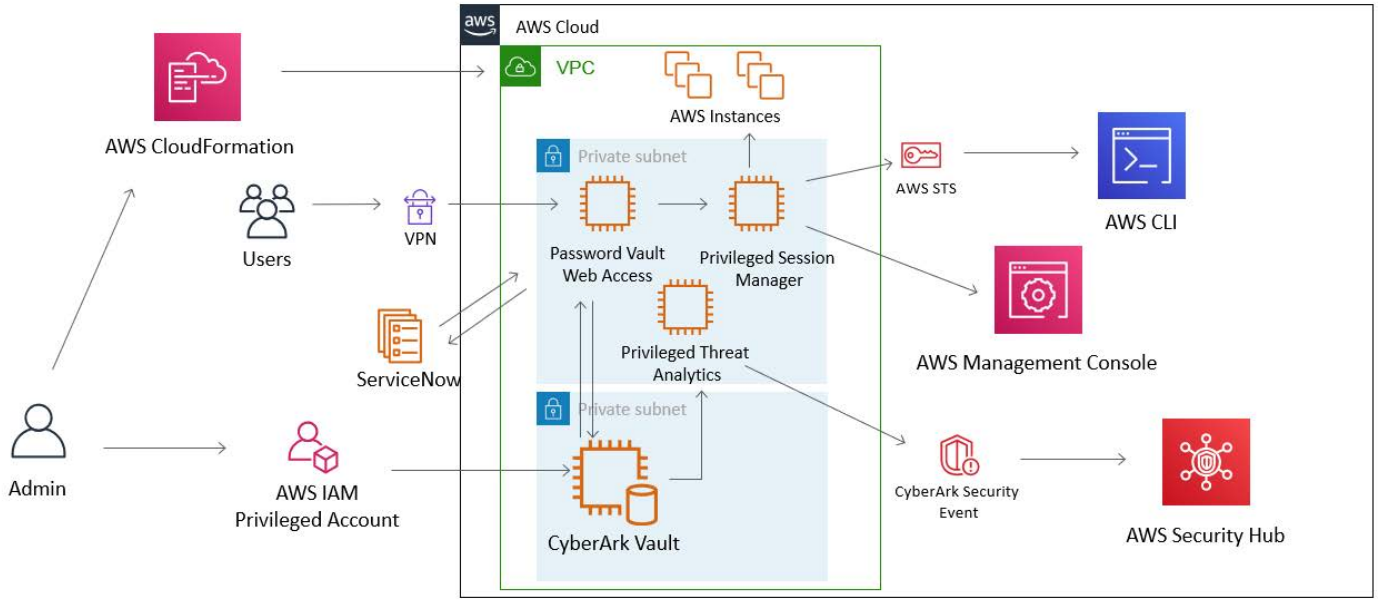
Many AMS customers use ServiceNow IT Service Management (ITSM) for incident tracking and change management. You can use the CyberArk Solution to secure and monitor privileged ServiceNow interactions, leveraging AWS IAM roles.

CyberArk Components Utilized

- Enterprise Password Vault
- Privileged Session Manager
- Central Policy Manager

How it Works

- The CyberArk solution is deployed by AMS in your Amazon VPC.
- ServiceNow accounts (IAM privileged account identities) are onboarded to the CyberArk Enterprise Password Vault.
- Upon session establishment, the ServiceNow connector retrieves privileged account credentials from the CyberArk vault to input ITSM entries into the ServiceNow system.
- Privileged Session Manager establishes a connection to a target host.
- Central Policy Manager automatically rotates credentials based on business rules.



Benefits

- Improves security by isolating and controlling privileged ServiceNow connections.
- Unifies privileged access management for AWS infrastructure and all ServiceNow functions: ticketing, discovery, orchestration, etc.
- Simplifies adoption by leveraging standard AWS identity management systems and practices for role-based access control.
- Improves visibility by monitoring and recording privileged sessions.

USE CASE #4

Use CyberArk to Isolate, Monitor, and Control AWS Systems Manager Session Manager Connections

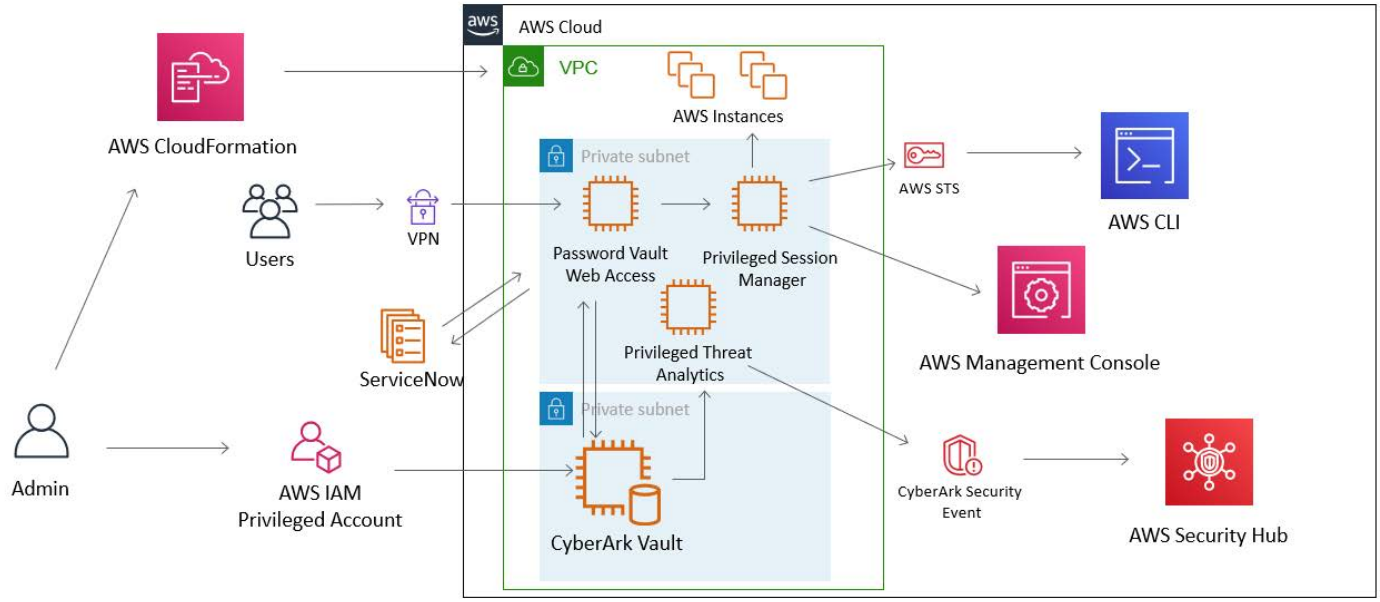
AWS Systems Manager Session Manager lets you manage Amazon EC2 instances through a browser-based shell or through the AWS CLI. You can use the CyberArk Solution to further secure, isolate and monitor Session Manager sessions between the AWS management console and an Amazon EC2 instance.

CyberArk Components Utilized

- Enterprise Password Vault
- Central Policy Manager

How it Works

- The CyberArk solution is deployed by AMS in your Amazon VPC with the AmazonSSMManagedInstanceCore default policy assigned using CyberArk provided AWS Cloud Formation templates.
- AWS IAM privileged account identities are onboarded to the CyberArk Enterprise Password Vault.
- User launches the AWS Systems Manager console from AWS Management Console.
- User navigates to the AWS SSM Session Manager page, selects an Amazon EC2 instance to launch a Session Manager CLI connection based on the policy assigned to the AWS IAM user logged into the AWS Management Console.
- Central Policy Manager automatically rotates credentials based on business rules.



Benefits

- Provides secure and auditable instance management without the need to open inbound ports, maintain bastion hosts, or manage SSH keys.
- Improves compliance and forensics by monitoring and recording privileged sessions.
- Simplifies adoption by leveraging standard AWS identity management systems and practices for role-based access control.

USE CASE #5

Send Security and Compliance Data to AWS Security Hub for Unified Monitoring and Analysis

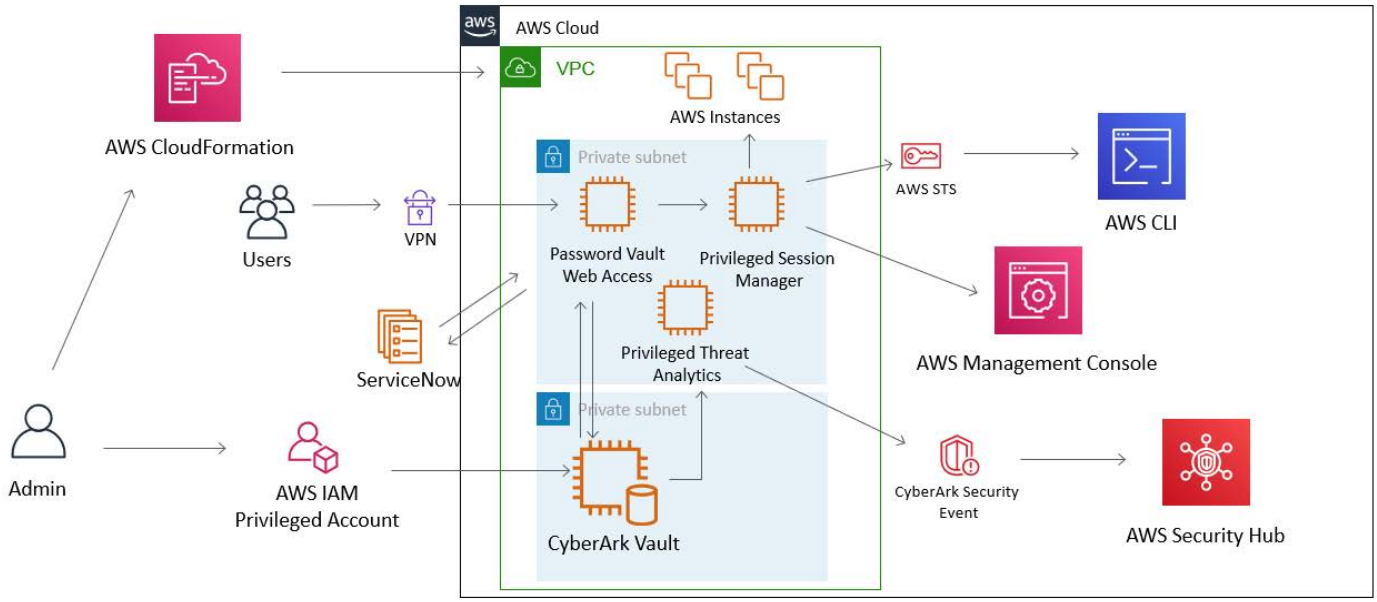
AWS Security Hub gives you a comprehensive view of your security alerts and security posture across your AWS accounts. You can integrate the CyberArk Privileged Access Management Solution with the AWS Security hub to give security and compliance administrators unified visibility into AWS services and partner integrations.

CyberArk Components Utilized

- Privileged Threat Analytics

How it Works

- Privileged Threat Analytics forwards security and compliance data to AWS Security Hub.
- AWS Security Hub collects, aggregates, and correlates data from multiple sources.
- Visual dashboard provides single-pane visibility across entire AWS environment.



Benefits

- Provides centralized, end-to-end visibility into critical security and compliance alarms and insights.
- Uses advanced analytics to rapidly detect complex attacks.
- Leverages machine learning to continuously adapt to evolving user behaviors.
- Detects threats early, helping shorten an attacker's window of opportunity, enabling rapid remediation and mitigation.

Summary

Integrating CyberArk Privileged Access Management with AWS Managed Services access controls helps to solve business challenges related to privileged AMS accounts and and proper configuration of infrastructure for maximum availability and service disruption. Implementation of the outlined use cases helps IT and security professionals efficiently manage AMS privileged account credentials and proactively monitor and control privileged account activity. If your company plans to deploy AWS Managed Services, CyberArk and AMS can help you drive operational efficiencies and make the most of your AMS investment so you can focus on your differentiated workloads.

Learn more about how CyberArk can help you strengthen privileged access management.

LEARN MORE

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.

About AMS
As enterprise customers move towards adopting the cloud at scale, some find their people need help and time to gain AWS skills and experience. AWS Managed Services (AMS) operates AWS on your behalf, providing a secure and compliant AWS Landing Zone, a proven enterprise operating model, on-going cost optimization, and day-to-day infrastructure management. By implementing best practices to maintain your infrastructure, AWS Managed Services helps to reduce your operational overhead and risk. AWS Managed Services automates common activities, such as change requests, monitoring, patch management, security, and backup services, and provides full-lifecycle services to provision, run, and support your infrastructure. AWS Managed Services unburdens you from infrastructure operations so you can direct resources toward differentiating your business.

CYBERARK®