Simplify cluster security at scale

Centralized secrets management across hybrid, multicloud environments

Abstract

Managing secrets across Kubernetes clusters in hybrid and/or multicloud environments using traditional approaches can create a multitude of security risks. CyberArk and Red Hat have an approach that centralizes and automates secrets management, mitigating those risks. This paper explains how solution architects can use our integrated technologies to help organizations strengthen security in Kubernetes clusters across production and development environments in multiple clouds, public and private, without impeding DevOps velocity.

Table of Contents

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

Red Hat

Key characteristics that make Red Hat OpenShift deployments secure

1. Security-Enanced Linux (SELinux), Namespaces, CGroups, and Secure Computing Mode are employed
2. Red Hat Enterprise Linux CoreOS is deployed as an immutable container with automated updates
3. Application security is integrated into DevOps from code through container
4. Network segmentation is built in through advanced policies and/or a service mesh
5. Secrets management is extended and enhanced with an external vault

The challenge of secrets management in hybrid, multicloud environments

Digital authentication credentials—commonly referred to as secrets—are a highly desirable target for cyber attackers. That's because, in many ways, they are the keys to the kingdom. Secrets, such as passwords, tokens, and SSH keys, are used by applications and other non-human identities, as well as human identities, to unlock access to privileged accounts, services, and resources in both production and development environments. In the wrong hands, these secrets could be used to breach applications, databases, domain controllers, and other critical infrastructure to maliciously disrupt operations or steal private information and intellectual property.

Developers can use a variety of methods for managing secrets. Fortunately, developers increasingly understand how reckless it is to hard-code secrets directly into application code and scripts, and many avoid this dangerous practice. While a better option is to use the services native to cloud platforms, such as Microsoft Azure Key Vault, this choice often results in something we call islands of security. (Figure 1)

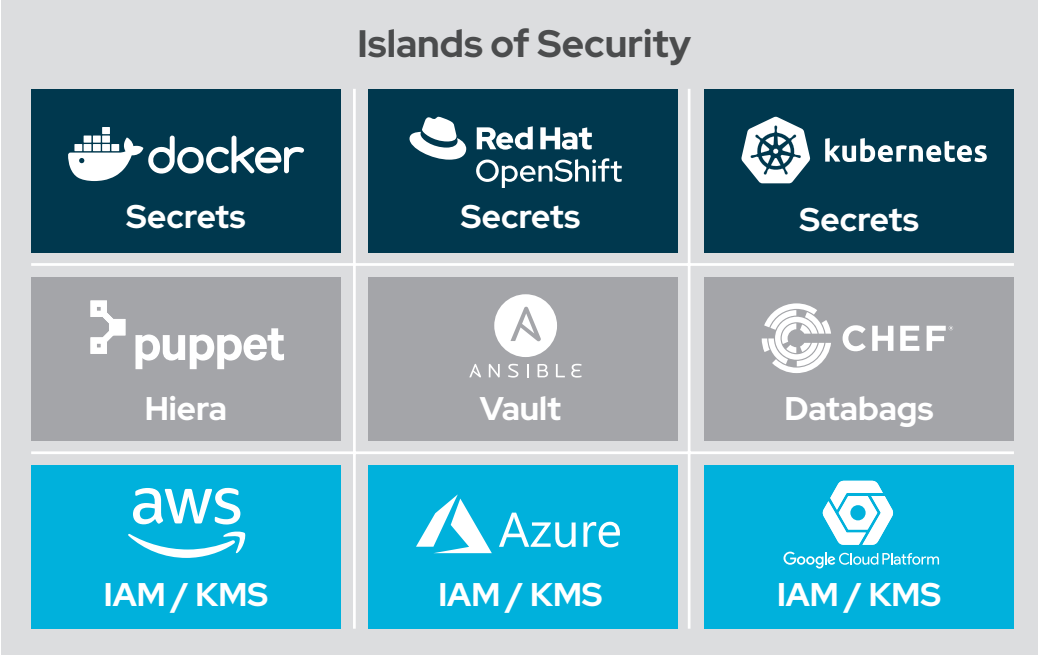

Figure 1. Islands of Security

By relying on individual native tools, secrets cannot be securely shared across clusters and clouds. Moreover, these native tools each have varying degrees of security, and spreading secrets across multiple tools exposes additional points of risk. In cloud environments with multiple Kubernetes clusters, secrets can proliferate very rapidly, creating a large attack surface for bad actors to exploit. Introduce multiple clouds, public and private, and secrets management quickly becomes untenable.

Having secrets scattered across numerous containers, clusters, and clouds makes it difficult to effectively track, rotate, and monitor their usage. The complexity in verifying components, configurations, and policies to ensure compliance simply becomes overwhelming. Consequently, vulnerabilities could easily be missed, and breaches go undetected, allowing attackers to exfiltrate data—possibly for months—until the vulnerability is remediated.

There is a better way to secure secrets, especially when scaling out hybrid, multicloud environments. By centralizing and automating secrets management, and establishing a single point of control,

Open source secrets management using CyberArk Conjur

Conjur provides a seamless open source interface to securely authenticate, control, and audit non-human access across tools, applications, containers, and clouds via robust secrets management.

organizations can reduce the number of security vulnerabilities and minimize attack surfaces—without slowing DevOps velocity. In the following pages, we explain how, using Red Hat and CyberArk technologies to streamline secrets management across clusters and clouds at scale, thus increasing security, mitigating risk, and improving compliance throughout the application lifecycle.

Your secrets are safe with Red Hat and CyberArk

Centralization and automation are the keys to securing hybrid, multicloud deployments of Kubernetes clusters without imposing a drag on productivity. Red Hat and CyberArk each bring unique technical capabilities to achieve this objective.

First, Red Hat provides a Kubernetes container platform with built-in features that strengthen security. CyberArk then adds centralized secrets management that dynamically and automatically assigns and rotates secrets for applications, scripts, machine identities, and humans. Together, Red Hat and CyberArk provide stronger, easier-to-manage security for Kubernetes clusters in multiple clouds, public and private.

The combined capabilities provided by both companies enable solution architects to design secure Kubernetes clusters that deliver value to all core stakeholders:

- **Developers**–Integrates stronger application security into the development cycle without impeding velocity
- **Operations**–Automates secrets management and rotation, allowing operations staff to focus on higher-level tasks and responsibilities
- **Security**–Centralizes secrets management, eliminating islands of security to shrink the attack surface and mitigate risk

Each company's offerings play a key role in designing a secure multicloud solution. The components are Red Hat® OpenShift® Container Platform and CyberArk Application Access Manager.

Shift left with seamless integration of security into the DevOps lifecycle

Application Access Manager minimizes the impact on development and IT operations teams by integrating secrets management natively into the Red Hat OpenShift container platform. As a result, DevOps teams can improve their security posture and reduce risks without disrupting operations or impeding service velocity.

Container security is built into the Red Hat OpenShift Container Platform

Red Hat OpenShift is an enterprise-ready Kubernetes container platform with full-stack automated operations to manage hybrid cloud and multicloud deployments. The platform is optimized to improve developer productivity and promote innovation. It is important to note that Red Hat OpenShift includes additional enterprise services built on Red Hat Enterprise Linux® (RHEL) and RHEL CoreOS. These added services provide strong security for the container platform with features that include:

- Host and runtime security
- Role-based access controls
- Project namespaces
- Integrated SDN with default network policies
- Logging, monitoring, and metrics

Moreover, RHEL CoreOS further enhances security as an optimized host operating system that is minimal, immutable, and always up to date. RHEL CoreOS provides only the services needed to run containers and delivers image-based, read-only deployments with OS updates that are automated and transparent.

RHEL and RHEL CoreOS provide a secure foundation for a hybrid, multicloud solution. However, for secrets management, Red Hat best practices recommend using an external secrets vault. That's where CyberArk Application Access Manager comes in.

Application Access Manager follows security best practices

Application Access Manager supports a default-deny, zero-trust model. Only authenticated identities can request secrets to which they have been granted access. In addition, Application Access Manager's granular role-based access control (RBAC) supports segregating duties across applications and personnel (e.g., cluster administrators vs. developers).

Secrets management automated by CyberArk Application Access Manager

Application Access Manager provides comprehensive privileged access, credential, and secrets management for widely used application types and non-human identities. A component of Application Access Manager enables centralized identity and secrets management that controls and audits access to Kubernetes clusters in multiple clouds, both public and private. Moreover, it includes integrations with Red Hat OpenShift Container Platform, making it easy for solution architects to design a complete solution for securing and managing hybrid, multicloud environments.

When integrated with Red Hat OpenShift, Application Access Manager extends and enhances the security of OpenShift to enterprise scale. It enables teams to consistently secure, rotate, and protect secrets and credentials used by applications, scripts, machines. and humans. Importantly, Application Access Manager is designed to remove the security burden from developers. By centralizing secrets management, Application Access Manager protects DevOps consoles, CI/CD pipelines, and production Kubernetes clusters regardless of the cloud provider—private enterprise, AWS, Microsoft Azure, or Google Cloud—with minimal human effort required. As a result, development teams can continuously deliver new applications and enhanced functionality using their chosen DevOps techniques and tools without compromising the security or compliance of the systems.

Secrets management using OpenShift and Application Access Manager

Application Access Manager extends the core CyberArk Privileged Access Security (PAS) portfolio, which provides a single, centralized control point for risk-based credential security and session management, enabling policies to be consistently enforced across on-premises infrastructures and cloud environments. In many ways, OpenShift is the ideal platform to host Application Access Manager, supporting a distributed architecture that allows secrets to be distributed from a central vault across geographies for local consumption with minimal latency. (Figure 2)

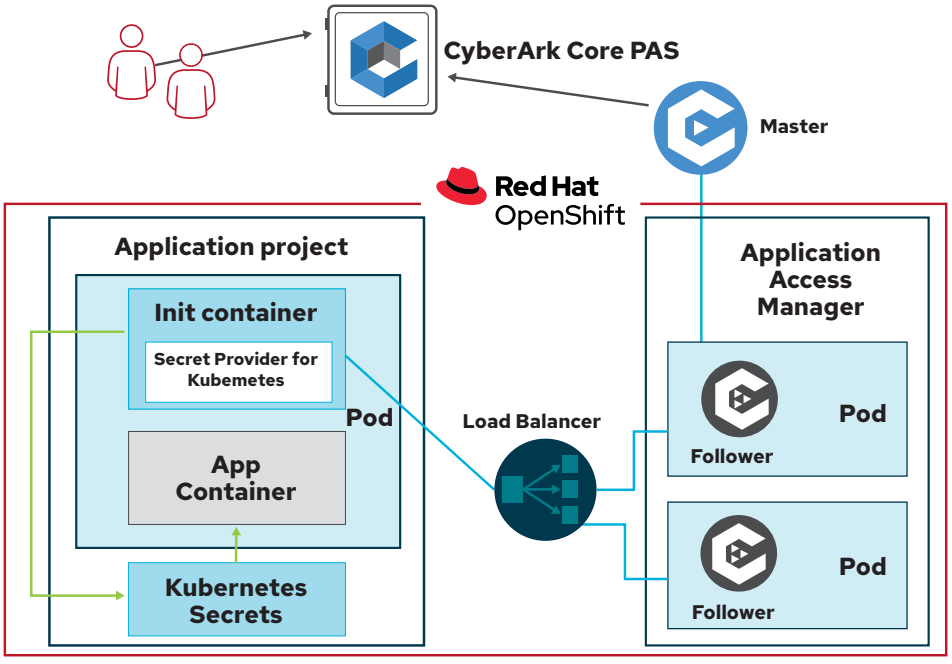

Figure 2. Master/Follower Architecture

Within the Red Hat OpenShift cluster, Application Access Manager runs one or more pods, called Followers, deployed as a service. Applications authenticate to the Follower service to retrieve credentials and access endpoint systems (databases, web services, SSH servers, etc.). Followers can

run inside or outside of the cluster; however, CyberArk best practices recommend running Followers in the cluster to take advantage of capabilities such as autoscaling, rolling upgrades, affinity rules, and scheduling.

Application Access Manager orchestrates authentication automatically, removing that burden from developers. Authentication is performed in OpenShift by a small container that authenticates Kubernetes pods—there is no need to write authentication code. Application pods are assigned unique identities using a combination of Kubernetes cluster ID, namespace (project), and service account values within OpenShift. Each identity is granted explicit permissions to control what it can and cannot access using declarative role-based access control (RBAC) policies.

Another important consideration is the flexibility to scale and adapt to individual application requirements. Developers can configure the level of granularity for identities. For example, all pods in a namespace (project) can share the same identity, or a pod may run as a specific Kubernetes service account.

Eliminates the "secret zero" problem

Using Application Access Manager to manage secrets eliminates the classic secret zero problem. Having a secret zero—or "master key"—to your most privileged assets is an open invitation to attackers. The challenge with traditional methods of securing secrets is how to secure that master key, the initial credential (password, token, certificate, etc.) required to authenticate the identity of an application and its access to other secrets.

With Application Access Manager, there is no need for a secret zero. Instead, Application Access Manager defines identities in terms of attributes that can be verified with the native characteristics of the platforms or tools being used. It trusts the platform to validate the authenticity of an identity rather than trusting a credential that could easily be copied and used in unauthorized ways.

Supports multiple options for retrieving secrets

Application Access Manager supports a variety of methods for retrieving secrets. It can dynamically retrieve secrets and provide them as Kubernetes secrets, accessible as files in the application's file system. Applications can also retrieve secrets directly from Application Access Manager using REST API calls or the Go, Java, .Net, and Ruby libraries.

A less intrusive option is secrets injection, which provides secrets as dynamically created environment variables rather than requiring the application to retrieve its own secrets. CyberArk provides an open source solution called Summon (https://cyberark.github.io/summon/), which runs in an application image and retrieves secrets for the application. It calls the application with those secret values bound to environment variables. The application only needs to read the environment variables, and once the application exits, the secrets disappear with it.

A third option is to dynamically update Kubernetes secrets with values retrieved from Application Access Manager. Many applications are already written to use Kubernetes secrets, which are inherently insecure since they are not encrypted, just Base64 encoded. The manifests that define Kubernetes secrets can easily find their way into source code repositories, where they are easily exploited by attackers. For applications that already use Kubernetes secrets, dynamically updating Kubernetes secrets provides greater security without rewriting a single line of application code.

The most secure approach for handling secrets is with Secretless. This innovative solution uses a "secretless broker" container to authenticate the pod, retrieve credentials, and establish connections to databases, web services, or SSH servers without the application ever having access to credentials. (Figure 3)

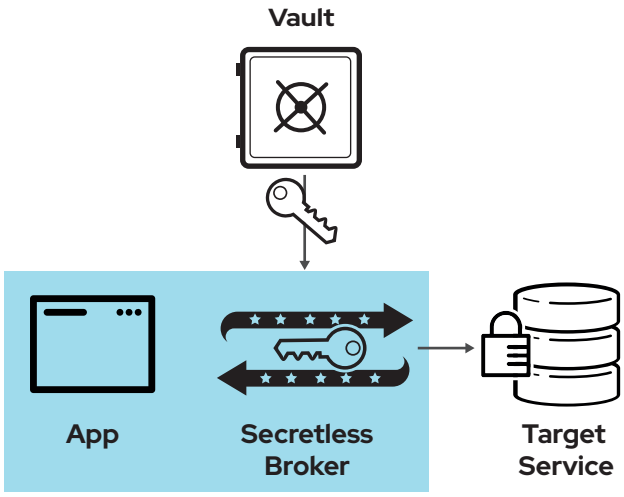

Figure 3. Secretless Broker Architecture

Secretless further strengthens security, reducing the attack surface because secrets and credentials are not exposed to application code or developers. It also simplifies life for developers and operations staff. There is no longer a need for developers to directly interact with a secrets management solution or learn how to code to its APIs. Moreover, operations can provision and remove access more easily because there is no need for each application to interact with the secrets-management solution. Additional information is available at https://secretless.io.

Conclusion

As presented in this paper, managing secrets across Kubernetes clusters in hybrid, multicloud environments can be challenging—and risky—using traditional approaches. They quickly lead to secrets sprawl and a greatly expanded attack surface for bad actors to exploit. However, Red Hat and CyberArk have collaborated to shrink the attack surface while simplifying secrets management for clusters across multiple clouds, both public and private.

Building on the security features baked into Red Hat OpenShift, CyberArk centralizes secrets management in a secure vault, automatically issuing and rotating secrets across containers and clusters in any type of cloud, public or private. Because Application Access Manager seamlessly integrates with OpenShift, solution architects can bring their customers a ready-made security platform for Kubernetes, which can be designed into a hybrid, multicloud solution quickly and easily.

The value of this joint solution for developers and operations staff can be summed up with three key points:

- **Secure**–Centrally manages and secures secrets according to policy across multiple clusters and clouds, eliminating secrets sprawl and shrinking the attack vector
- **Simple**–Enables developers to secure, manage and rotate secrets and credentials with no need to write code or make script changes
- **Holistic**–Consistently secures secrets and credentials used by containerized applications and automation scripts, as well as the people accessing platforms and management consoles

Together, Red Hat and CyberArk simply offer a better way to manage secrets—one that's easy to implement, more secure, and scalable across hybrid, multicloud environments.

Red Hat Open Hybrid Cloud

Open Hybrid Cloud is the Red Hat strategy for helping organizations move their IT architectures into the future—starting with open source. Initiated in 2012, our Open Hybrid Cloud strategy provides unparalleled flexibility, control, and choice. For example, with Open Hybrid Cloud, an application built to run in a private data center today can easily be run in a private or public cloud in the future. There is no need to rebuild the application, retrain people, maintain different environments, or compromise security. That's the power of open source.

Next steps

To learn more about how Red Hat and CyberArk integrate their respective technologies, visit www.cyberark.com/redhat

To schedule a demo of Application Access Manager running with Red Hat OpenShift, visit www.cyberark.com/request-demo

Appendix: Additional product information

Red Hat and CyberArk offer a suite of products with unique features and capabilities to simplify cluster management and security in hybrid multicloud deployments. This appendix highlights the key distinctions of those products for solution architects to consider when designing customer solutions.

How Red Hat stands out when it comes to containers

Containers deliver consistency for hybrid and multicloud implementations, and Red Hat products enable those implementations to run at full scale with no compromises. Moreover, Red Hat infrastructure products for containers are certified on the major cloud providers. With a hybrid, multicloud infrastructure from Red Hat, organizations are assured of:

- A consistent developer experience throughout the development lifecycle—code to build to deploy.
- A consistent operational interface with automated operations.
- A cloud-agnostic application and data infrastructure platform.
- DevOps tooling compatible across clouds.
- A single, more secure Linux operating system in all clouds.

More than 50% of Fortune 100 enterprises use and trust CyberArk with their privileged account credentials

To deliver on these advantages, Red Hat provides a full stack for building, deploying, and running hybrid, multicloud environments. This stack includes a full-featured Linux distribution and CoreOS, a certified Kubernetes engine, a comprehensive container platform, and multi-cluster management. (Figure 4)

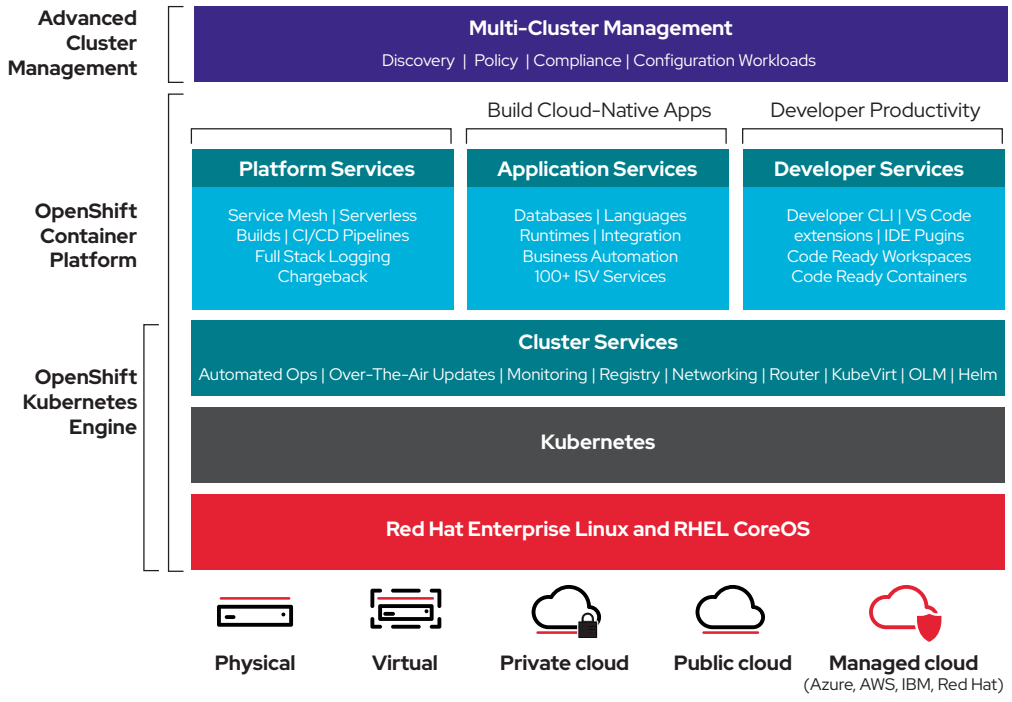

Figure 4. Red Hat Platform

This architecture is designed with the understanding that Linux is foundational to containers. Containers depend on Linux features, Kubernetes uses Linux to manage resources, and applications in containers are running in Linux. RHEL has long been recognized as a leading Linux distribution,

providing a stable and proven foundation for diverse cloud environments and enterprise implementations at global scale.

As the container host operating system, RHEL CoreOS is operated as part of the Kubernetes cluster, with the configuration for components managed by Machine Config Operator, including CRI-O config, Kubelet config, authorized registries, and SSH config. As discussed earlier in this paper, RHEL CoreOS is an immutable operating system, tested, and shipped in conjunction with the OpenShift platform. Red Hat runs thousands of tests against these configurations.

Red Hat OpenShift Container Platform also offers unique capabilities that are ideal for hybrid, multicloud environments. It is an enterprise Kubernetes container platform that provides a full set of tooling for developer productivity and DevOps—proven over 16 years of development and continuous enhancement.

OpenShift is especially well-suited for hybrid and multicloud deployments because of its flexibility. It provides a cloud-like experience everywhere, empowering developers to innovate without constraints. Additionally, by providing a consistent development and operational experience across any combination of clouds (public and private), OpenShift not only stands up to the demands of running applications in multiple clouds but also reduces the amount of operational complexity that comes from a multicloud strategy.

At the top of the stack is Red Hat Advanced Cluster Management for Kubernetes, designed to simplify multi-cluster, multicloud management. Advanced Cluster Management for Kubernetes centrally creates, updates, and deletes Kubernetes clusters across multiple private and public clouds. It also allows users to search, find, and modify any Kubernetes resource across the entire domain, also helpful for quickly troubleshooting and resolving issues.

With Advanced Cluster Management for Kubernetes, users can easily deploy applications from multiple sources at scale, and quickly visualize application relationships across clusters. Advanced Cluster Management for Kubernetes also provides policy-based governance, risk, and compliance, enabling users to centrally set and enforce policies, and quickly conduct detailed auditing. Built-in Center of Internet Security compliance policies and audit checks simplify the process and provide real-time visibility into the organization's compliance posture.

For more details about Red Hat OpenShift Container Platform, visit openshift.com. Additional information about the complete portfolio of open source solutions from Red Hat is available at redhat.com.

Unique secrets management capabilities delivered by CyberArk

CyberArk Application Access Manager is part of the core CyberArk Core Privileged Access Security solution. (Figure 5)

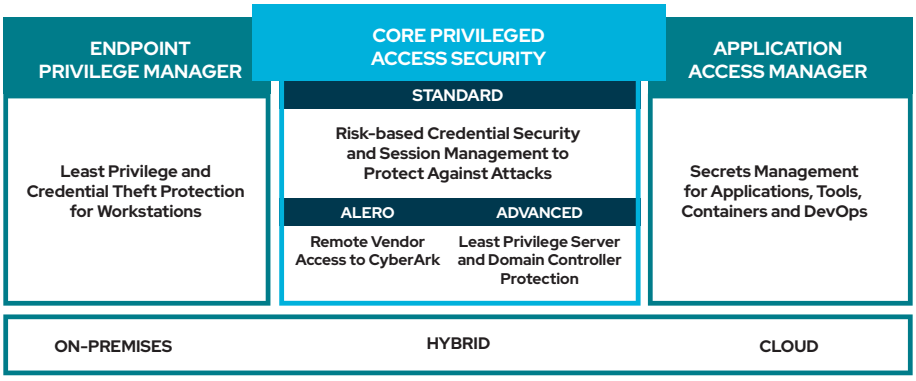

Figure 5. CyberArk Privileged Access Security Portfolio

A component of Application Access Manager is designed specifically to provide a secrets management solution that meets the unique needs of DevOps teams delivering hybrid and multicloud solutions. Because it is integrated natively with Red Hat OpenShift, Application Access Manager enables development and IT operations teams to improve their security posture and reduce risks with minimal impact on DevOps or CI/CD pipelines, and without impeding service velocity.

Application Access Manager delivers strong security features that enable organizations to control, manage, and audit human and non-human privileged access for applications across hybrid, containerized, and multicloud environments. It securely delivers secrets to OpenShift containers with end-to-end encryption and automatically rotates credentials to continually improve the organization's security posture. Application Access Manager also enables separation of duties, and applies strong, role-based access controls with comprehensive audit trails for proof of compliance. Moreover, it supports business continuity with enterprise-class scalability, availability, redundancy, and resilience.

In addition, Application Access Manager extends naturally to the CyberArk Privileged Access Security Solution, which protects, monitors, detects, alerts, and manages privileged accounts and other credentials for both human and non-human users and identities. Elements in each product can be deployed independently or combined to form a cohesive, end-to-end privileged access security solution across hybrid, multicloud, PaaS, and DevOps environments.

More detailed information on the complete privileged access security portfolio from CyberArk is available at cyberark.com/devops. Additional information on Conjur and the CyberArk open source community is available at conjur.org.

About CyberArk

CyberArk, the global leader in privileged access management, offers the industry's most complete solution for securing both the credentials and secrets used by applications, Playbooks, scripts, and other non-human identities, as well as human users. CyberArk solutions are deployed at many of the world's largest enterprises including over half the Fortune 500.

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

NORTH AMERICA
1 888 REDHAT1

EUROPE, MIDDLE EAST, AND AFRICA
00800 7334 2835
europe@redhat.com

ASIA PACIFIC
+65 6490 4200
apac@redhat.com

LATIN AMERICA
+54 11 4329 7300
info-latam@redhat.com

redhat.com
#pccpcj_0620