Simplify cluster security at scale

Centralized secrets management across hybrid, multicloud environments

Table of contents

Executive summary

Managing secrets across Kubernetes clusters in hybrid and 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, whether public or private, without impeding DevOps velocity.

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 because they are the keys to the kingdom in many ways. Secrets, such as passwords, tokens, and Secure Shell (SSH) keys, are used by applications and other nonhuman identities, in addition to 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 known as islands of security (Figure 1).

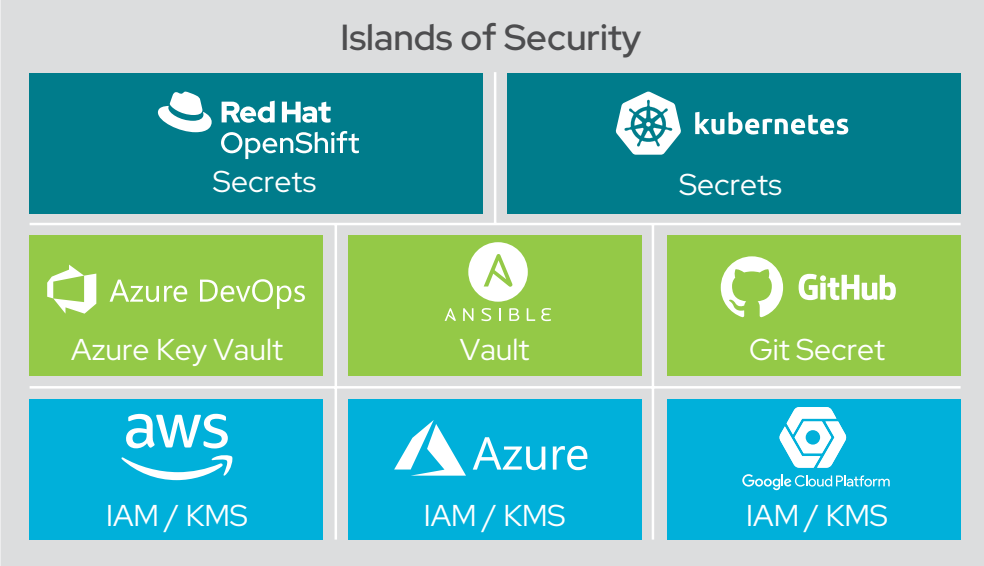

Figure 1. Islands of Security

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 public and private clouds, 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.

A better way to secure secrets—especially when scaling out hybrid, multicloud environments—is to centralize and automate secrets management, establishing a single point of control. Taking this approach allows organizations to 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 helps to increase security, mitigate risk, and improve compliance throughout the application life cycle.

Secrets are safer with Red Hat and CyberArk

Centralization and automation are the keys to prioritizing the security of 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 help organizations achieve strong, straightforward security for Kubernetes clusters in multiple public and private clouds.

The combined capabilities provided by both companies equip solution architects to design Kubernetes clusters, with an emphasis on security, that deliver value to all core stakeholders:

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

Each company's offering—Red Hat® OpenShift® Container Platform and CyberArk Secrets Manager—plays a key role in designing a multicloud solution with security in mind.

Container security is built into Red Hat OpenShift

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® and Red Hat Enterprise Linux CoreOS. These added services provide strong security for the container platform with features that include:

- Host and runtime security.
- Role-based access controls (RBAC).
- Project namespaces.
- Integrated software-defined networking (SDN) with default network policies.
- Logging, monitoring, and metrics.

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

Red Hat Enterprise Linux and Red Hat Enterprise Linux CoreOS provide a security-hardened foundation for a hybrid, multicloud solution. However, for secrets management, Red Hat best practices recommend using an external secrets vault. That is where CyberArk Application Access Manager comes in.

Key characteristics that make Red Hat OpenShift deployments security-focused

1. Security-Enhanced 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 containers.
4. Network segmentation is built-in through advanced policies or service mesh, or both.
5. Secrets management is extended and enhanced with an external vault.

Secrets management automated by CyberArk Secrets Manager

Secrets Manager provides comprehensive privileged access, credential, and secrets management for widely used application types and nonhuman identities. A component of Secrets Manager allows for centralized identity and secrets management that controls and audits access to Kubernetes clusters in multiple clouds. Moreover, it includes integrations with Red Hat OpenShift, making it less complex for solution architects to design a complete solution for hardening and managing hybrid, multicloud environments.

When integrated with Red Hat OpenShift, Secrets Manager extends and enhances the security of OpenShift to enterprise scale. It lets teams consistently secure, rotate, and protect secrets and credentials used by applications, scripts, machines, and humans. Importantly, Secrets Manager is designed to remove the security burden from developers. By centralizing secrets management, Secrets Manager protects DevOps consoles, continuous integration and continuous delivery (CI/CD) pipelines, and production Kubernetes clusters regardless of the cloud provider—private enterprise, Amazon Web Services (AWS), Microsoft Azure, or Google Cloud—and 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 system security or compliance.

Secrets management using Red Hat OpenShift and Secrets Manager

Secrets Manager extends the CyberArk Identity Security Platform, which provides a single, centralized control point for risk-based credential security and session management, establishing consistent enforcement of policies across on-premise infrastructures and cloud environments. In many ways, Red Hat OpenShift is the ideal platform to host Secrets Manager because it supports a distributed architecture that allows secrets to be distributed from a central vault across geographies for local consumption with minimal latency (Figure 2).

Safeguard application secrets across the enterprise

CyberArk Secrets Manager minimizes the impact on development and IT operations teams by integrating secrets management natively into 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.

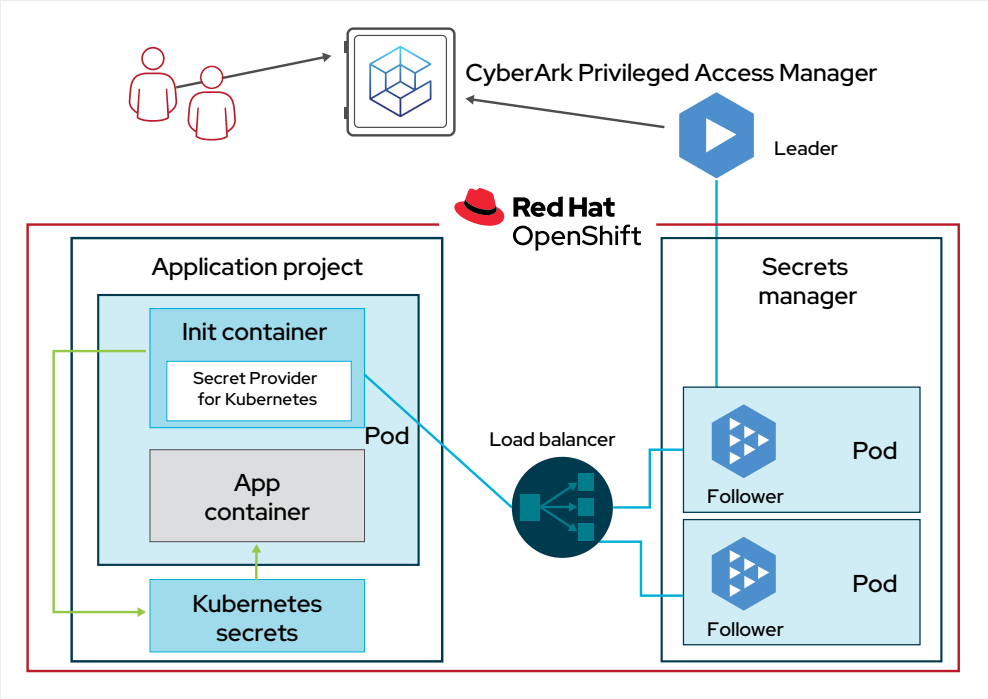

Figure 2. Leader/follower architecture

Secrets Manager follows security best practices

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

Within the Red Hat OpenShift cluster, Secrets Manager runs 1 or more pods—called Followers—which are 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, implementing affinity rules, and scheduling.

Secrets Manager orchestrates authentication automatically, removing that burden from developers. Within Red Hat OpenShift, a small container authenticates Kubernetes pods in lieu of developers needing to write authentication code. Application pods are assigned unique identities using a combination of Kubernetes cluster ID, namespace (project), and service account values within Red Hat OpenShift. Each identity is granted explicit permissions to control what it can and cannot access using declarative 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.

Eliminating the “secret zero” problem

Using Secrets Manager to manage secrets eliminates the classic “secret zero” problem. Having a secret zero to your most privileged assets is an open invitation to attackers. The challenge underlying most methods of safeguarding secrets is how to protect the secret zero, which is the initial credential (password, token, certificate, etc.) used to grant access to all other secrets.

With Secrets Manager, there is no need for a secret zero. Instead, Secrets Manager defines identities in terms of attributes that can be verified with the native characteristics of the platforms or tools being used. It uses the underlying container orchestration services to validate the identity of an application rather than trusting a credential that could be compromised and used in unauthorized ways.

Support for multiple secrets retrieval options

Secrets Manager supports a variety of methods for retrieving secrets. It can dynamically retrieve and provide them as Kubernetes secrets, accessible via the application’s file system. Applications can also retrieve secrets directly from Secrets Manager using representational state transfer (REST) application programming interface (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 (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.

A 3rd option is to dynamically update Kubernetes secrets with values retrieved from Secrets Manager. Many applications are already written to use Kubernetes secrets, which are inherently insecure because they are not encrypted—just Base64 encoded. The manifests that define Kubernetes secrets can easily find their way into source code repositories, where they can be exploited by attackers. For applications that already use Kubernetes secrets, dynamically updating those 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).

More than 50% of Fortune 500 enterprises use and trust CyberArk with their privileged account credentials.[1]

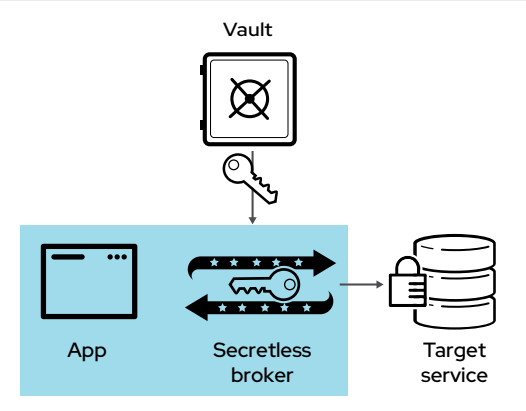

Figure 3. Secretless broker architecture

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

Conclusion

Using traditional approaches to manage secrets across Kubernetes clusters in hybrid, multicloud environments can be challenging and risky, quickly leading to secrets sprawl and a greatly expanded attack surface for bad actors to exploit. Red Hat and CyberArk have collaborated to defend against attacks while improving operational efficiency by 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. The integration between Secrets Manager and Red Hat OpenShift provides solution architects with a ready-made security platform for Kubernetes they can design into a hybrid, multicloud solution and bring to their customers.

This joint solution for developers and operations staff is:

- **Security-focused.** It centrally manages and safeguards secrets according to policy across multiple clusters and clouds, eliminating secrets sprawl and shrinking the attack vector.
- **Simple.** It allows developers to reinforce their security posture, manage, and rotate secrets and credentials with no need to write code or make script changes.

1 *CyberArk. www.cyberark.com/company. accessed August 2023.*

- **Holistic.** It consistently safeguards secrets and credentials used by containerized applications, automation scripts, and the people accessing platforms and management consoles.

Together, Red Hat and CyberArk offer a better way to manage secrets—one that is simple to implement, more focused on security, and scalable across hybrid, multicloud environments.

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 let those implementations 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 life cycle: 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 security-focused Linux OS in all clouds.

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 multicluster management (Figure 4).

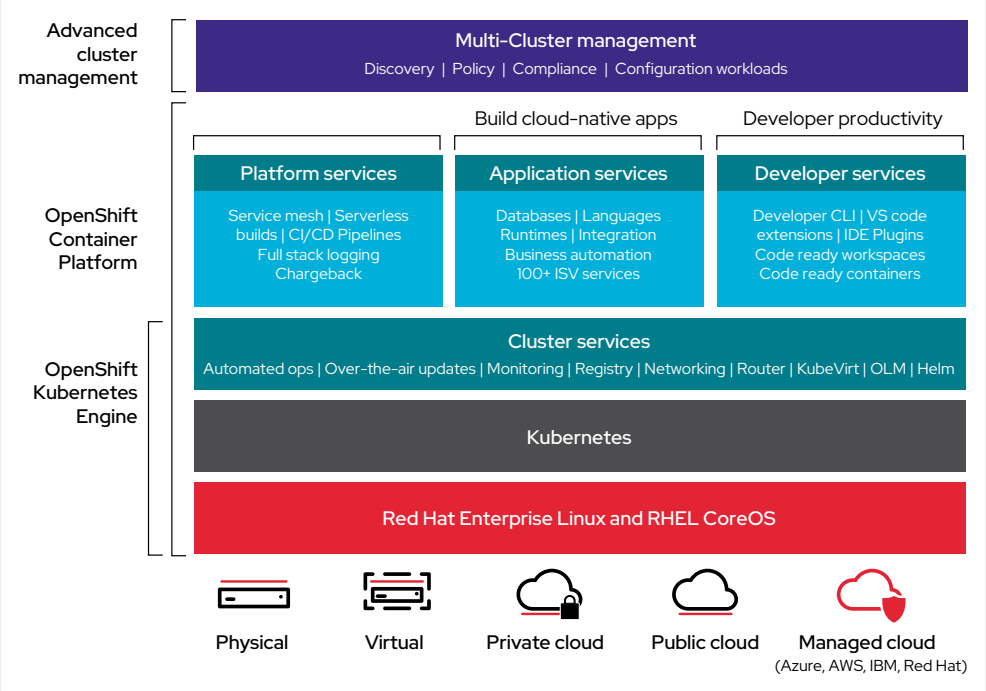

Figure 4. Red Hat Platform

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. Red Hat Enterprise Linux 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 OS, Red Hat Enterprise Linux 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. Red Hat Enterprise Linux CoreOS is an immutable OS that is tested and shipped in conjunction with Red Hat OpenShift. 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.

Red Hat OpenShift is especially 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, Red Hat OpenShift not only stands up to the demands of running applications in multiple clouds but also reduces the operational complexity associated with a multicloud strategy.

At the top of the stack is Red Hat Advanced Cluster Management for Kubernetes—a tool designed to simplify multicluster, multicloud management. Red Hat Advanced Cluster Management 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 and is helpful for quickly troubleshooting and resolving issues.

With Red Hat Advanced Cluster Management, users can deploy applications from multiple sources at scale and quickly visualize application relationships across clusters. Red Hat Advanced Cluster Management also provides policy-based governance, risk, and compliance, allowing 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, 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 Secrets Manager is part of the CyberArk Identity Security Platform (Figure 5).

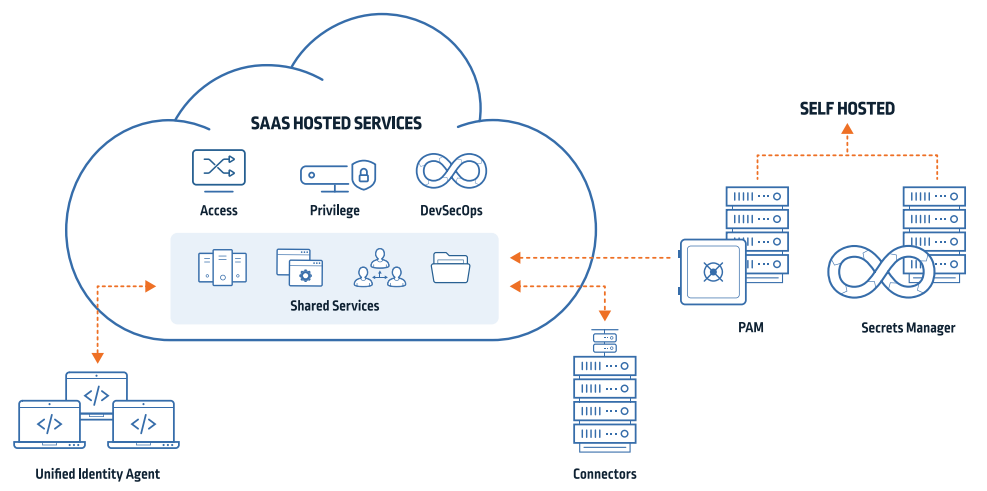

Figure 5. CyberArk Identity Security Platform

A component of Secrets 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, Secrets Manager helps development and IT operations teams improve their security posture and reduce risks with minimal impact on DevOps or CI/CD pipelines and without impeding service velocity.

CyberArk Secrets Manager manages the credentials and secrets used by the widest range of application types and DevOps tools—from cloud-native applications to automation platforms and robotic process automation (RPA) to mainframe and everything in between. The solutions are

designed to improve the organization's overall security posture and operational efficiency by automating and simplifying key security functions. It delivers secrets to Red Hat OpenShift containers with end-to-end encryption and automatically rotates credentials. Secrets Manager also facilitates separation of duties and applies strong RBAC controls with comprehensive audit trails for proof of compliance. Moreover, it supports business continuity with enterprise-class scalability, availability, redundancy, and resilience.

In addition, Secrets Manager extends naturally to CyberArk Privileged Access Manager, which protects, monitors, detects, alerts, and manages privileged accounts and other credentials for both human and nonhuman users and identities. Elements in each product can be deployed independently or combined to form a cohesive, end-to-end identity security solution across hybrid, multicloud, Platform-as-a-Service (PaaS), and DevOps environments.

More detailed information on the Identity Security Platform 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 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 life cycle. The world's leading organizations trust CyberArk to help secure their most critical assets. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blogs, or follow us on Twitter via @CyberArk, LinkedIn, or Facebook.

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 develop cloud-native applications, integrate existing and new IT applications, and automate and manage complex environments. A trusted adviser to the Fortune 500, Red Hat provides award-winning support, training, and consulting services that bring the benefits of open innovation to any industry. Red Hat is a connective hub in a global network of enterprises, partners, and communities, helping organizations grow, transform, and 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
#469184_0823