CYBERARK®

DATA SHEET

CyberArk® Secrets Manager

Enables organizations to centrally secure credentials used by almost all application types across cloud-native and hybrid environments

The Challenge

Enterprises are increasingly adopting DevOps methodologies and automation to improve business agility while also leveraging commercial and internally developed applications. However, each application and other non-human identity relies on credentials to access sensitive resources. While application and IT environments can vary significantly — from highly dynamic, cloud native to largely static and even mainframe based — these credentials need to be secured regardless of the application type and compute environment. Securing these credentials poses challenges for IT security, operations, and compliance teams:

- **Application and other non-human credentials are widespread –** they include embedded hard-coded credentials in business-critical applications including internally developed and commercial off-the-shelf solutions (COTS), security software such as vulnerability scanners, application servers, IT management software, Robotic Process Automation (RPA) platforms, and the CI/CD tool chain.
- **Application and other non-human credentials need to be managed –** in addition to eliminating hard-coded credentials, recommended approaches and techniques include strong authentication, least privilege, role-based access controls, rotation, and audit.
- **Automated processes are incredibly powerful –** they can access protected data, scale at unparalleled rates, leverage cloud resources, and rapidly execute business processes to drive tremendous value. However, as security and software supply chain breaches demonstrate, automated processes are susceptible to sophisticated cyberattacks, which can occur suddenly and spread rapidly.

It is critical that both human and non-human access is consistently managed and secured across the enterprise, from admin consoles, to databases, applications, and other sensitive assets.

KEY BENEFITS

For Security Teams

- Protect against breaches by centrally managing credentials used by most application types and non-human identities.
- Reduce vault sprawl by centrally managing secrets across multiple project teams and environments.
- Prevent inadvertent exposure of credentials by eliminating hard-coded credentials.
- Simplify securing identities as part of the most complete and extensible Identity Security Platform

For Operations

- Reduce complexity and burden on IT by automating the management and rotation of application credentials.
- Secure mission critical applications running at scale.

For Developers

- Simplify how applications securely access sensitive resources with the most of out-of-the-box integrations and flexible APIs.
- Use AWS Secrets Manager with no change in experience.
- Avoid impacting velocity.

For Compliance and Audit

- Leverage a unified security solution to ease the burden of meeting extensive compliance and regulatory requirements.

The Solution

CyberArk Secrets Manager is designed to secure secrets and credentials used by the broadest range of application types in hybrid, cloud-native and containerized environments. Additionally, Secrets Manager is designed to offers customers the flexibility to select the solutions which best meets their unique use cases and approaches, including, for example, SaaS solutions which simplify deployment and operations, self-hosted solutions and solutions for customers that are committed to a specific provider or vendor. The platform enables secrets for all the various use cases, application types and approaches to be centrally managed to help apply consistent policies, simplify audit and reduce vault sprawl.

- **For cloud-native applications built using DevOps methodologies –** Several solutions are offered, each of which solve a unique set of uses cases.
    - **For multi-cloud and DevOps environments –** Conjur Secrets Manager Enterprise and the SaaS version Conjur Cloud* provide secrets management solutions designed for the unique requirements of multi-cloud and multi-vendor DevOps environments. Conjur offers REST APIs and integrates with a wide range of DevOps tools, container platforms, and supports hybrid and multi-cloud environments. Developer resources and Conjur Open Source are also available at www.conjur.org.
    - **For teams that have embraced AWS Secrets Manager –** Secrets Hub* enables security teams to centrally manage and rotate secrets in AWS Secrets Manager, while giving developers the same native experience. The SaaS offering helps reduce vault sprawl across multiple AWS project teams and simplify securing hybrid environments.

      Conjur and Secrets Hub integrate with the CyberArk Identity Security Platform to provide a single enterprise-wide platform for securing privileged credentials.
- **For securing commercial off-the-shelf solutions –** Credential Providers can rotate and manage the credentials that third-party tools and solutions such as security tools, RPA, automation tools, IT management, etc. need to complete their jobs. For example, a vulnerability scanner typically needs high levels of privilege to scan systems across the enterprise's infrastructure. Now instead of storing privilege credentials in COTS solutions, they are managed by CyberArk. And to simplify how enterprises allow third party solutions to access privileged credentials, CyberArk offers the most validated COTS integrations for solving identity security challenges.
- **For internally-developed traditional applications –** Credential Providers can protect business-system data and simplify operations by eliminating hard-coded credentials from internally developed applications. The solution provides a comprehensive set of features for managing application passwords and SSH keys, and supports a broad range of application environments, including application servers, Java, .Net, and scripting running on a variety of platforms and operating systems including Unix/Linux, Windows and zOS.

Secrets Manager provides robust enterprise-grade capabilities and integrates with existing systems to help organizations protect and extend established security models and practices.

*Note, Conjur Cloud and Secrets Hub are currently offered as Early Availability - contact sales@cyberark.com for additional information.

Capabilities

Secrets Manager solutions are designed to help organizations:

- **Establish strong authentication –** by leveraging the native attributes of applications, containers, and other non-human identities to eliminate the "secret zero bootstrapping" challenge and potential vulnerability.
- **Manage and rotate secrets –** by leveraging dual accounts and other techniques.
- **Simplify integrations –** by supporting validated integrations with CI/CD toolsets, and container platforms, and a wide range of commercial software platforms, applications and tools, such as business applications, security tools and RPA.
- **Accelerate deployment and usage –** by providing developers with easy to-use solutions to secure secrets in application and DevOps environments.
- **Ensure a comprehensive audit –** by tracking access and providing tamper-resistant audit.
- **Consistently apply access policies –** by applying role-based access controls on non-human identities, leveraging integrations with other CyberArk and partner solutions to centralize policy management across the enterprise.
- **Ensure business continuity and other enterprise requirements –** including scalability, availability, redundancy and resiliency.
- **Simplify deployment –** With both SaaS and self-hosted versions of Secrets Manager and support for SaaS and Self-Hosted versions of the CyberArk Vault.

CyberArk Identity Security Platform

Secrets Manager is part of the CyberArk Identity Security Platform which helps organizations secure access to critical business data and infrastructure, protect a distributed workforce, and accelerate business in the cloud. The integrated solution helps organizations reduce the attack surface by applying consistent policies to human and non-human identities across the enterprise.

OVERVIEW

Cloud Native and DevOps Integrations:

- Tools/Toolchains: Ansible, Jenkins, Puppet, Terraform
- Public Clouds: AWS, Azure, GCP
- PaaS/Container Orchestration: Kubernetes, Red Hat OpenShift, Rancher, VMware Tanzu
- Secretless Broker: OpenShift, Kubernetes
- Container Security: Aqua, Twistlock

Native Authenticators:

- Kubernetes
- Red Hat OpenShift
- AWS Secrets Manager
- AWS IAM
- Azure
- Google Cloud Platform
- JSON Web Token (JWT)
- OpenID Connect (OIDC)

COTS Application Integrations:

- Security Software: Vulnerability Management, Discovery Solutions, etc.
- IT Management Software
- Robot Process Automation and other Automation Solutions

Application Server Integrations:

- JBoss, Oracle WebLogic Server, Tomcat, IBM WebSphere Application Server, WebSphere Liberty

Enterprise Grade:

- HSM integration, SIEM Tools
- AES-256, RSA-2048, SHA2

SDK and Development Libraries:

- DevOps: Go, Java, Ruby, .NET
- Application SDK: C/C++, CLI, Java, .NET, .NET Core, / .NET Standard, Web Service/REST

CyberArk Vault Integrations:

- CyberArk Privilege Access Manager (Self-hosted)
- CyberArk Privilege Cloud®

CYBERARK®