CYBERARK®

Secrets Management for Clouds, Containers and DevOps

Key Benefits

- Security-first, scalable, enterprise-ready solution
- Centralized secret protection, management and auditing
- Granular least privilege access control
- Controlled and monitored user access to sensitive DevOps resources

Today's software delivery pipeline centers on delivering high-quality products and services to market faster and more efficiently than ever before. This is made possible through the use of DevOps methodologies. DevOps focuses on rapid, continuous development, integration, delivery and deployment; it was not fundamentally designed with security in mind. Yet, nearly every component of the highly interconnected and rapidly changing DevOps ecosystem utilizes secrets.

Secrets are used by:

- **Infrastructure:** Hosts, machines and systems that are created and used in almost every environment (development, testing, staging and production)
- **Continuous Integration and Continuous Delivery (CI/CD) tools**
- **Applications and micro-services:** The final outputs of the delivery pipeline

Additionally, developers, IT operations staff and administrators require quick, easy workflow to do their jobs effectively, and as such, cannot be constrained by restrictive policies that impede the velocity of the delivery pipeline.

Secrets represent one of the largest security vulnerabilities an organization faces today. In the hands of an external attacker or malicious insider, secrets allow attackers to take full control of an organization's IT infrastructure, disable security controls, steal confidential information, commit financial fraud and disrupt operations.

Built for Security. Designed for Agility.

Designed for deployment across any environment, the CyberArk solution is all about the automation, agility and control needed to secure cloud and DevOps environments.

The CyberArk Privileged Account Security Solution delivers key capabilities across all virtualized and cloud environments, including:

- Secure and manage secrets (e.g. passwords, encryption keys, SSH keys and tokens) used by machines (e.g. applications, containers, micro-services and EC2 instances) and users throughout the DevOps pipeline. Secrets are automatically stored and rotated based on the organization's security policy.
- Secure secrets retrieval by machines based on strong application authentication. The solution provides modern APIs, such as C#, C++, Python, Java, .Net, Go, Ruby and Node.Js for extended platform support.

- Provide various integrations with CI/CD tools to deliver off-the-shelf, automated secrets management. Secrets used by multiple CI/CD tools (e.g. Puppet, Chef and Ansible) and cloud platforms (AWS, MS Azure and Google Cloud) are automatically secured and managed.
- Control and monitor privileged user access to CI/CD tool as well as cloud platform consoles.
- Enforce the least privilege principle by limiting privileged user access to sensitive resources, such as hosts (in 'break glass' scenarios) and centrally manage privilege escalation. User privileges can automatically be elevated in an on-demand, one-time basis in accordance with established access policies.
- Provide centralized audit and reporting capabilities to address IT audit requirements with automated enforcement of privileged account policies (e.g. frequency of secrets rotation and password complexity). All audit records are stored in tamper-proof storage to prevent unauthorized access, modification or deletion of logs.
- Cloud-native, scalable solution built to support massive concurrent usage as well as performance spikes. Leveraging capabilities such as Amazon Auto Scaling Groups (ASG), the solution has demonstrated elastic, horizontal scaling at massive loads.
- High Availability architecture delivered as clustered software to ensure the highest degree of uptime and availability for cloud and DevOps environments.
- Enterprise grade Active Directory/LDAP and AWS Identity and Access Management integrations enabling organizations to leverage trusted business systems for centralized user management.

Key Benefits:

- **Security-first, scalable, enterprise-ready solution** to address all privileged account security and secrets management needs across any environment.
- **Centralized secrets protection, management and auditing.** Automatically secures and manages secrets (e.g. passwords, SSH keys and API keys) of users and machines from the instant they are created. All secrets-related events are automatically and immutably logged for audit purposes.
- **Granular least privilege access control.** Implements least privilege policies by controlling which DevOps resources privileged users can access and limits what they are authorized to do with those resources based on their roles and tasks.
- **Controlled and monitored user access to sensitive DevOps resources.** Centralizes access to DevOps resources to maximize control and visibility

Platform Support

CyberArk-Conjur Server

- Amazon EC2
- Amazon VPC
- Microsoft Azure
- VMware vSphere
- Physical servers
- Linux platforms via a Docker container

Client development libraries

- Ruby
- Node.js
- Java
- Python

Command-line and web GUI for management

DevOps Toolchain Integrations

- Jenkins
- Puppet
- Chef
- Docker
- VMware
- Amazon Web Services
- Cloud Foundary
- OpenStack
- Splunk

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.