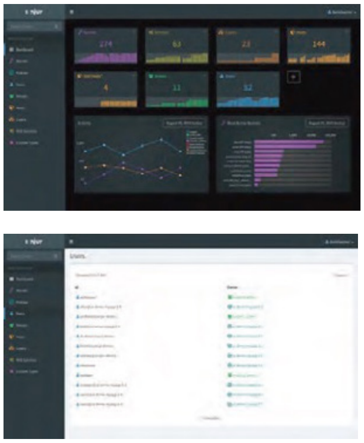
Conjur Enterprise

Secure Secrets Used by Machines and Users Throughout the DevOps Pipeline



Conjur centralizes and streamlines secret protection, management and auditing

The Challenge

Enterprises are automating IT infrastructure and instituting DevOps methodologies to accelerate the pace of innovation. Traditional identity and access management solutions are not designed to natively support the unique security needs of DevOps workflows. Enterprises must introduce new systems and practices to support dynamic workloads, microservices and automated IT without compromising security or service velocity.

Since DevOps pipelines are fully automated and contain many different tools, platforms and resources, there are many secrets hidden in various locations throughout the pipeline. Attackers know where to look for these systems and how to exploit them. This is a huge threat surface with many potential open-doors for attackers.

Secrets embedded in app code pose an enormous risk. Secrets can be easily exposed, since there is no audit or control over who's accessing them. Additional risks lie within the configuration management and other tools used in the DevOps pipeline. As high consumers of secrets, these tools have become the new targets for attackers.

In addition, it's critical to secure the underlying infrastructure of the pipeline. Finally, there is always a group of DevOps personas that need to interactively access the different tools, to administer, maintain or even make changes in break-glass scenarios. Controlling and monitoring the interactive access of these privileged users has also become a critical means to protect the DevOps pipeline.

The Solution

CyberArk Conjur is a secrets management solution tailored specifically to the unique infrastructure requirements of native cloud and DevOps environments. The solution helps IT and information security organizations secure and manage secrets used by machines identities (applications, microservices, applications, CI/CD tools, APIs, etc.) and users throughout the DevOps pipeline.

Conjur helps organizations improve their security posture, mitigate risks and meet stringent compliance requirements without slowing down CI/CD workflows. With Conjur, secrets, keys, certificates, and authentication data are all stored securely—out of repositories, out of source code, and off of hard drives—for ultimate protection, control and manageability.

Conjur is the only platform independent secrets management solution specifically architected for containerized environments and can be deployed on premises or to any cloud at massive scale. The solution integrates seamlessly with a variety of CI/CD tools such as configuration management tools and CI servers. It also integrates with existing Active Directory, LDAP, and SIEM systems helping organizations protect and extend previous investments, and preserve established security models and practices.

Conjur is available as free and open source software at conjur.org and github.com/cyberark. Conjur enables organizations, regardless of where they are in their DevOps journey, to integrate secrets management best practices into their workflow and evolve their DevOps projects with Conjur.

Conjur Enterprise is a fully featured, enterprise-class solution fully backed by CyberArk's world-class support and service organization. Key Conjur Enterprise features include: GUI access, audit and reporting, HA/DR functionality, and integrations with the CyberArk Privileged Account Security Solution, AD/LDAP and SIEM systems. With Conjur Enterprise, organizations can extend their current Privileged Account Security Solution from CyberArk to enable comprehensive control and consistent governance across the enterprise, into the cloud and throughout the DevOps pipeline. More details on Conjur Enterprise can be found at cyberark.com.

Key Features

Key features and functions include:

- Comprehensive secrets management for sensitive data such as API keys, certificates, passwords, SSH keys and tokens. Secrets are securely stored and managed in an encrypted and access-controlled container on the Conjur server and can be automatically rotated based on policy. Conjur also ensures that applications deployed in auto scaling environments such as AWS can dynamically and securely access secrets.
- Role-based access controls (RBAC) makes it easy to assign distinct privileges to different groups of users or machines with different responsibilities. Administrators can define various roles (e.g. development, test, operations, administration) and grant each role unique privileges (e.g. read, write, delete) for specific resources (e.g. database password, VM or server, web service endpoint.)
- Centralized, tamper-proof audit records for all authorization events and secrets operations, with an intuitive interface to generate and review compliance reports.
- Integration with DevOps toolchain secures and manages secrets used by CI/CD tools such as Ansible, Chef, Jenkins and Puppet and container orchestration software such as Docker and Kubernetes.
- Easy to use GUI provides an overall view of users, machines, and secrets managed by Conjur and a comprehensive view of audit data. The GUI can also be used to configure policies and policy-based workflows.
- CyberArk Privileged Account Security Solution, AD/LDAP and SIEM support for integration with existing security systems and practices.
- Cloud scalability, performance and availability. Conjur is based on a distributed, high-availability architecture with distinct Master and Follower components. Masters and Followers can be distributed across zones, regions and clouds to minimize latency and enable high scalability and resiliency. The solution leverages capabilities such as Amazon Auto Scaling Groups to enable elastic, horizontal scaling at massive loads with no degradation of system performance.

Specifications

- Deployment Options:
  - Docker Image
  - Amazon AMI
  - RPM
- Supported Client Development Libraries:
  - Go
  - Java
  - .NET
  - Node.js
  - Ruby
  - Python
- DevOps Toolchain:
  - Ansible
  - Chef
  - Jenkins
  - Puppet
- Containers/Container Orchestration:
  - Docker
  - Kubernetes
- Other Integrations:
  - CyberArk Privileged Account Security Solution
  - Active Directory and LDAP
  - HSM integration
  - SIEM tools

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.