CYBERARK®

SOLUTION BRIEF

Conjur Secrets Manager strengthens CloudBees Jenkins pipeline security

HIGHLIGHTS

The solution enables organizations to:

- Centrally secure and manage secrets and other credentials used across CI/CD pipelines
- Enforce Segregation of Duties (SoD) with Role-Based Access Controls (RBACs)
- Enforce and demonstrate least privilege access policies
- Maintain comprehensive audit trail for proof of compliance
- Minimize impact to operations and development workflows while managing and securing secrets

Application code within the digital supply chain is a common target for today's increasingly sophisticated cyber attackers. CyberArk secrets management solutions help ensure security across the DevOps pipeline, while driving business agility and providing a frictionless experience for developers.

CyberArk Secrets Manager manages secrets for Jenkins pipelines and enables segregation of duties, and authentication and authorization controls for Jenkins executors. Together, CyberArk Secrets Manager and CloudBees CI bring industry best practices to organizations to establish robust, automated, and fully functional secrets management.

The integrated solution is designed to manage and securely store secrets, and inject them into Jenkins processes as needed. As a result, organizations can configure Jenkins to require less privilege, while continuing to ensure artifacts created by Jenkins are verified and reliable. Importantly, secrets can be more-securely shared across CloudBees CI, and other platforms, including other DevOps tools and continuous integration (CI) and continuous delivery (CD) tools integrated with CyberArk.

Mismanaged Jenkins Pipelines Can Expose Security Risks

Jenkins uses secrets to access numerous environments, tools, scripts, applications, and services. But many organizations rely on manual processes to update and rotate these secrets—an inefficient and risky process that does not scale well.

Secrets are a common target for threat actors. Scripts, tools, DevOps admins, internal and external developers, sub-contractors, and IT staff may all have access to secrets used across the CI/CD pipeline. With multiple pipelines in use, organizations may store the same secrets in multiple locations. They may reuse completed pipeline builds, rather than discard them. They may rotate secrets infrequently (or not at all). And even worse, they may hard code secrets into builds and scripts.

CloudBees.

PARTNER PRODUCTS

- CloudBees CI
- Jenkins (Open Source/ Community)

CYBERARK PRODUCTS

- Conjur Secrets Manager Enterprise
- Conjur Secrets Manager Open Source*
- Credential Providers (CCP)**
- CyberArk Privilege Cloud
- CyberArk Privilege On Premises

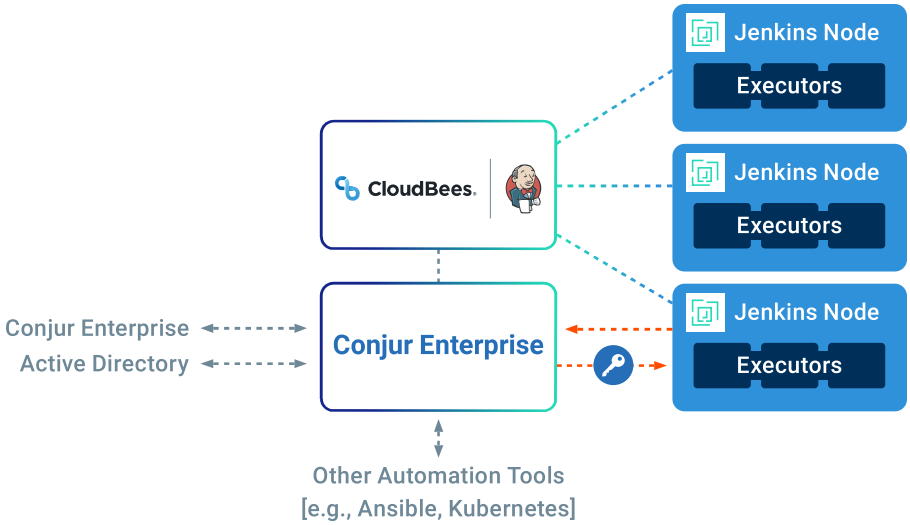
Attackers can exploit weak secrets management practices and CI/CD security vulnerabilities to gain illicit access to CI/CD pipelines and inject malicious code into the build process. High-profile security breaches demonstrate that an attack on the software supply chain can be devastating for the software provider as well as for the potentially thousands of customers that rely on the compromised product release.

While some organizations use secrets plugins available from the Jenkins community, many find this approach becomes increasingly difficult to manage as their operation scales with more jobs and machines. Instead, CyberArk offers plugins (jointly and community developed) as well as Conjur Secrets Manager which is available as enterprise and open source, and the Credential Providers.

Integration Mitigates DevOps Security Risks

The joint Conjur Enterprise and CloudBees solution helps automate nearly all security and management tasks related to secrets used throughout the software development lifecycle, including updating, rotating, encrypting, and controlling access to secrets. Secrets are more secure, when they are rotated automatically and can only be accessed according to policy.

For an additional layer of security, Conjur Enterprise supports strong authentication and authorization controls which organizations can use to govern which identities can update and retrieve secrets (includes native JWT authentication and API Key options). These capabilities help prevent malicious machines from gaining illicit access to DevOps resources and help ensure secrets are governed by the principle of least privilege.



Robust Secrets Management with Conjur Enterprise and CloudBees

* Note, Conjur Open Source may provide more limited support for some CloudBees CI native functionality compared to Conjur Enterprise. Refer to technical documentation https://developer.conjur.net/ for additional information.

** Note, uses CyberArk Plugins to provide secrets to Jenkins/CloudBees CI pipelines.

Solution Secures and Monitors Credentials within CloudBees CI

Conjur Enterprise helps organizations enforce Segregation of Duties (SoD) policies to the applications used in the Jenkins pipeline. This is configured in Conjur Enterprise through group access policies that manage privileged secrets. Conjur Enterprise manages and helps secure access to secrets while helping to enforce SoD policies.

With Conjur Enterprise and CloudBees CI, organizations can:

- Centrally manage secrets across the organization's CI/CD pipelines
- Create collaborative policies to manage secrets, without disrupting the developer environment
- Enable security teams to implement best practices such as encryption, secret rotation, and least privileged access
- Use Machine Identities with RBAC to enable granular authentication control
- Authenticate at the node and process level
- Use common interfaces for injecting secrets
- Work with a dedicated and scalable security platform
- Get on-demand access to reports for audit and compliance needs

Conjur Enterprise is designed as an enterprise-class solution that can manage and secure all secrets (e.g., passwords, SSH keys and API tokens, SSL certificates) used by people or machines (e.g., tools, applications, microservices and infrastructure). The solution is designed to provide Jenkins jobs more secure access to secrets to run tests and build artifacts. In addition, Conjur Enterprise can automatically log secrets-related events for audit and compliance purposes. An open-source version of Conjur Enterprise is available at www.conjur.org.

Integration Avoids Disrupting Developer's Flow

The solution is designed to minimize impact on developers and on pipeline velocity, while providing hassle free security. Developers simply replace how they access a secret with a call to Conjur Enterprise or an environment variable for Conjur Open Source to populate at runtime.

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 lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets. To learn more, visit us at www.cyberark.com.

About CloudBees

CloudBees, the enterprise software delivery company, provides the industry's leading DevOps technology platform. CloudBees enables developers to focus on what they do best: Build stuff that matters, while providing peace of mind to management with powerful risk mitigation, compliance and governance tools. Used by many of the Fortune 100, CloudBees is helping thousands of companies harness the power of continuous everything and gets them on the fastest path from a great idea, to great software, to amazing customer experiences, to being a business that changes lives.

CYBERARK®