CYBERARK CONJUR® SECRETS MANAGER ENTERPRISE

ПРОБЛЕМАТИКА

По мере того как предприятия внедряют DevOps и автоматизируют свою ИТ-инфраструктуру, у них возникает необходимость обеспечивать безопасность своих динамично меняющихся задач, облачных и автоматизированных ИТ-сред без ущерба для скорости разработки - любое решение безопасности должно удовлетворять потребности как группы безопасности, так и разработчиков.

Приложения используют секреты для безопасного доступа к конфиденциальным ресурсам. Из-за удобства учётные данные часто сохраняются в исходном коде, однако подобная практика представляет собой огромный риск, потому что такие секреты нельзя ротировать или менять, ими трудно управлять и сложно проверять. Также они случайно могут быть опубликованы в репозиториях кода.

Кроме того, инструменты управления конфигурацией и инструментами CI/CD используют секреты для взаимодействия с другими инструментами и доступа к другим ресурсам. Этот доступ должны контролировать администраторы DevOps, разработчики и другие специалисты, которые их администрируют. Эти инструменты стали привлекательными для злоумышленников, поэтому необходимо защищать не только секреты, используемые приложениями, но и учётные данные, используемые самими инструментами и управляющими ими специалистами.

РЕШЕНИЕ

Conjur Enterprise - это решение для управления секретами в соответствии с уникальными требованиями инфраструктуры облачных сред, контейнеров и сред DevOps. Решение помогает разработчикам и подразделениям безопасности защищать, изменять, проверять и управлять секретами и другими учётными данными, которые используют приложения, инструменты автоматизации и другие сервисы.

Conjur Enterprise специально разработан для контейнерных сред и может легко масштабироваться. Решение интегрируется с широко используемыми инструментами и платформами DevOps, и существующими системами, помогая организациям улучшить существующие модели и методы обеспечения безопасности. Решение позволяет организациям, независимо от того, на каком этапе цифровой трансформации они находятся, защищать приложения и автоматизированные процессы, а также интегрировать передовые методы управления секретами в рабочие процессы разработчиков.

Conjur Enterprise - это полнофункциональное решение корпоративного класса, поддерживаемое компанией CyberArk. Возможности решения включают доступ к графическому интерфейсу, ротацию, аудит и отчетность, а также функции HA/DR. Дополнительные ресурсы по защите сред DevOps можно найти на сайте www.cyberark.com/devops, а версия с открытым исходным кодом, Conjur Open Source, и сообщество разработчиков доступны по адресу www.conjur.org/blog.

ПРЕИМУЩЕСТВА

Снижение рисков в динамических облачных средах и средах DevOps без ущерба для безопасности, гибкости или скорости бизнеса.

Для групп ИБ

Обеспечивает защиту от атак и взломов цепочки разработки программного обеспечения за счёт последовательного управления и мониторинга учётных данных, секретов и привилегий приложений в средах автоматизации и DevOps с применением корпоративных политик и стандартов безопасности.

Платформа CyberArk Identity Security Platform предоставляет безопасный доступ администраторам DevOps, назначающим привилегии.

Для рабочих процессов

Снижение нагрузки на ИТ благодаря массовому масштабированию и гибкости развёртывания в облачных, мультиоблачных или гибридных средах. Улучшение защиты бизнеса.

Для разработчиков

Простой и безопасный доступ приложений к ресурсам с помощью встроенной интеграции с инструментом CI/CD, контейнерными платформами и Secretless Broker.

Ускоренный доступ разработчиков с помощью решений с открытым исходным кодом.

Кроме того, Conjur Enterprise является частью платформы CyberArk Identity Security Platform, которая помогает организациям защищать доступ к критически важным бизнес-данным и инфраструктуре, а также ускорять бизнес в облаке. Элементы платформы могут быть объединены в единое комплексное решение, которое будет обеспечивать безопасность привилегированного доступа корпоративного класса в гибридных, мультиоблачных и контейнерных средах. Интегрированное решение помогает организациям уменьшить поверхность атаки за счёт применения единых политик как к пользователям, так и к другим объектам.

КЛЮЧЕВЫЕ ХАРАКТЕРИСТИКИ

- **Комплексное управление секретами** для привилегированных учётных данных, таких как ключи API, сертификаты, пароли, ключи SSH и токены. Секреты надежно управляются и автоматически меняются в соответствии с политикой.
- **Интеграция с набором инструментов DevOps** использует встроенные средства защиты и управления секретами, инструменты CI/CD (Ansible, Jenkins и Azure DevOps), а также программное обеспечение для оркестрации контейнеров (Kubernetes).
- **Интеграция с платформами DevOps** Интеграция с платформами DevOps обеспечивает защиту и управление секретами и учётными данными, используемыми средами PaaS, включая Kubernetes, Red Hat OpenShift, VMware Tanzu и Cloud Foundry.
- **Контроль доступа на основе ролей (RBAC)** позволяет легко назначать отдельные привилегии разным группам сервисных учётных записей с разными правами. Администраторы могут определять различные роли (например, разработку, тестирование, эксплуатацию, администрирование) и предоставлять каждой роли уникальные привилегии для определенных ресурсов (например, пароль базы данных, точка доступа к веб-сервису).
- **Единые записи аудита** для всех событий авторизации и операций с секретами.
- **Удобный графический интерфейс** обеспечивает общий визуальный контроль пользователей, машин и секретов.
- **Инновационная функция Secretless Broker** упрощает безопасное подключение приложений к базам данных, SSH и HTTPS без извлечения секретов и управления ими. Это повышает безопасность, изолируя приложения от раскрытия секретов.
- **Масштабируемость, производительность и доступность облака.** Использует распределенную архитектуру высокой доступности с компонентами Leader и Follower. Leaders и Followers могут быть распределены по зонам, регионам и мультиоблачным средам для минимизации задержки, поддержки масштабируемости и устойчивости, а также разделения данных между средами (например, prod, dev, GCP, AWS).
- **Интеграция с CyberArk Identity Security Platform** позволяет организациям использовать централизованный подход на основе политик для последовательного управления учётными данными как сотрудников, так сервисных учётных записей. Например, интеграции позволяют управлять, синхронизировать и отслеживать учётные данные в средах DevOps, изолировать мониторинг и контроль привилегированного доступа пользователей-людей, включая администраторов DevOps, управляющих цепочкой инструментов.
- **Поддержка интеграции** с существующими системами безопасности, включая SIEM.

ОБЗОР

Варианты развёртывания:

Docker Image
Amazon Machine Image (AMI)

SDK и библиотеки разработки:

Go, Java, Ruby, .NET
REST API, CLI

Интеграция с Cloud Native и DevOps:

Tools/Toolchains: Ansible, Jenkins, Puppet, Terraform

Public Clouds: AWS, Azure, GCP

PaaS/Container Orchestration: Kubernetes, Red Hat OpenShift, VMware Tanzu, Cloud Foundry

Container Security: Aqua

Community Integrations (e.g., Azure DevOps, Concourse, TeamCity)

Интеграция с CyberArk Vault:

CyberArk Privilege Access Manager (Privilege On-Premises) CyberArk Privilege Cloud®

Другие встроенные интеграции и инструменты

Secretless Broker: Red Hat OpenShift, Kubernetes
Summon

Решения безопасности:

HSM integration
SIEM tools

Собственные аутентификаторы:

Kubernetes
Red Hat OpenShift AWS IAM
Azure
Google Cloud Platform
OpenID Connect (OIDC)