CYBERARK® SECRETS MANAGER

ПРОБЛЕМАТИКА

Методология DevOps и автоматизация применяются для повышения гибкости бизнеса, а также для работы с коммерческими приложениями и приложениями собственной разработки. Однако каждое приложение, инструмент автоматизации и другая идентификационная информация, не относящаяся к человеку, полагается на ту или иную форму привилегированных учётных данных для доступа к конфиденциальным ресурсам. Приложения и ИТ-среды могут значительно различаться в пределах одной организации - от высоко динамичных, облачных, в основном статических и даже мэйнфреймовых. Учётные данные приложений должны быть защищены независимо от типа приложения и вычислительной среды. Их защита создает проблемы для групп ИТ-безопасности, эксплуатации и соблюдения нормативных требований:

- **Приложения и другие учётные данные, не связанные с человеком, используются широко –** они включают встроенные жестко закодированные учётные данные в критически важных бизнес-приложениях, включая разработанные внутри компании и коммерческие готовые решения (COTS), программное обеспечение безопасности, такое как сканеры уязвимостей, серверы приложений, ПО по управлению ИТ, платформы Robotic Process Automation (RPA) и цепочку инструментов CI/CD.
- Приложения и другие учётные данные, не относящимися к человеку, необходимо строго контролировать. Помимо замены жёстко запрограммированных учётных данных в коде и сценариях, рекомендуется использовать строгую аутентификацию, минимальные привилегии, управление доступом на основе ролей, ротацию учётных данных и аудит.
- **Автоматизированные процессы невероятно мощны.** Они могут получать доступ к защищённым данным, масштабироваться с беспрецедентной скоростью, использовать облачные ресурсы и быстро выполнять бизнес-процессы, принося огромную прибыль. Однако, как показывает практика, автоматизированные процессы подвержены угрозам кибератак, которые могут происходить внезапно и быстро распространяться.

Для защиты от атак компании необходимо защищать привилегированные учётные данные не относящихся к человеку идентичностей. Кроме того, эти учётные данные обычно назначаются и управляются такими людьми, как ИТ-администраторы, разработчики и администраторы DevOps. Поэтому очень важно, чтобы доступ человека к консолям администратора также был под постоянным контролем в масштабах всего предприятия.

ПРЕИМУЩЕСТВА

Для ИБ-команд

- Защита от взломов, последовательное управление и отслеживание учётных данных, используемых почти всеми типами приложений и идентичностями, не принадлежащими человеку.
- Предотвращение непреднамеренного раскрытия учётных данных и удаление жёстко заданных учетных данных.
- Часть наиболее полной и расширяемой платформы Identity Security Platform

Для текущих операций

- Снижение сложности и нагрузки на ИТ-отделы за счёт автоматизации управления и ротации учётных данных приложений.
- Безопасная работа критически важных приложений в большом масштабе.

Для разработчиков

- Простой и безопасный доступ приложений к конфиденциальным ресурсам с помощью большинства готовых интеграций и гибких API.
- Защита от скорости поражения.

Для нормативного регулирования и аудита

- Единое решение безопасностфи для соблюдения большого количества нормативных требований.

РЕШЕНИЕ

CyberArk Secrets Manager разработан для защиты секретов и учётных данных многочисленных приложений в гибридных, облачных и контейнерных средах. Secrets Manager включает Conjur® Secrets Manager Enterprise (с открытым исходным кодом) и поставщиков учётных данных (Credential Providers).

- **Conjur Secrets Manager Enterprise - это решение по управлению секретами, которое было специально адаптировано для уникальных требований облачных сред и сред DevOps.** Решение интегрируется с широким спектром инструментов DevOps, платформами оркестровки PaaS/контейнеров и поддерживает гибридные и мультиоблачные среды. Решение интегрируется с CyberArk Identity Security Platform, обеспечивая единую корпоративную платформу для защиты привилегированных учётных данных. Ресурсы для разработчиков и Conjur Open Source доступны на сайте www.conjur.org. -

- **Защита готовых коммерческих решений.** Поставщики учётных данных могут менять учётные данные, которые необходимы сторонним продуктам и решениям, таким как инструменты безопасности, RPA, инструменты автоматизации, управление ИТ и т. д. Например, сканеру уязвимостей обычно требуются высокие уровни привилегий для сканирования систем в инфраструктуре предприятия. Вместо хранения учётных данных привилегий в решениях COTS они управляются CyberArk. Чтобы упростить доступ сторонних решений к привилегированным учётным данным, CyberArk предлагает наиболее проверенные интеграции COTS для решения проблем безопасности идентификации.
- **Стандартные приложения внутренней разработки.** Поставщики учётных данных могут защитить данные бизнес-систем и упростить операции, удалив жёстко заданные учётные данные из приложений, разработанных внутри компании. Решение предоставляет полный набор функций для управления паролями приложений и SSH-ключами, а также поддерживает широкий спектр сред приложений, включая серверы приложений, Java, .Net и сценарии, выполняемые на различных платформах и операционных системах, включая Unix / Linux, Windows и zOS.

Secrets Manager предоставляет надёжные возможности корпоративного уровня и интегрируется с существующими системами, помогая организациям защищать и расширять установленные модели и методы обеспечения безопасности.

ВОЗМОЖНОСТИ

Решения Secrets Manager призваны помочь организациям:

- **Обеспечить строгую аутентификацию** с использованием собственных атрибутов приложений, контейнеров и других идентификаторов, отличных от человека, для устранения проблемы «секретной нулевой начальной загрузки» и потенциальной уязвимости.
- **Управлять и менять секреты,** используя двойные учётные записи и другие методы.
- **Упростить интеграцию** за счёт поддержки проверенных интеграций с наборами инструментов CI/CD и контейнерными платформами, а также с широким спектром коммерческих программных платформ, приложений и инструментов, таких как бизнес-приложения, инструменты безопасности и RPA.
- **Ускорить развёртывание,** предоставив разработчикам простые в использовании решения для защиты секретов в средах приложений и DevOps.
- **Обеспечить всесторонний аудит любого доступа,** отслеживая весь доступ и обеспечивая устойчивый аудит.
- **Последовательно применять политику доступа,** используя средства управления доступом на основе ролей для лиц, не являющихся людьми, а также интеграцию с другими решениями CyberArk и партнёров для централизации управления политиками в масштабах всего предприятия.
- **Обеспечить непрерывность бизнеса и другие требования предприятия,** включая масштабируемость, доступность, избыточность и отказоустойчивость.
- **Гибкие варианты развертывания.** Secrets Manager поддерживает как SaaS, так и локальные версии CyberArk Vault, что упрощает развертывание и повышает гибкость, а также гарантирует безопасность за счёт централизованного управления учётными данными и секретами в масштабах всего предприятия.

ОБЗОР

Интеграция приложений OTS

- Security Software: Vulnerability Management, Discovery Solutions, etc.
- IT Management Software
- Robot Process Automation и другие автоматизированные решения

Интеграция с серверами приложений:

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

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
- Secretless Broker: OpenShift, Kubernetes
- Container Security: Aqua, Twistlock

Корпоративный урвоень:

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

SDK библиотеки разработчиков:

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

Собственные аутентификаторы:

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

Интеграция с CyberArk Vault:

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

ПЛАТФОРМА БЕЗОПАСНОЙ ИДЕНТИФИКАЦИИ CYBERARK

Secrets Manager является частью платформы CyberArk Identity Security Platform, которая помогает защитить доступ к критически важным бизнес-данным и инфраструктуре, распределенную рабочую силу и ускорить бизнес в облаке. Интегрированное решение помогает уменьшить поверхность атаки за счёт применения согласованных политик к личным и нечеловеческим идентификаторам на предприятии.