Deckhouse Stronghold

Deckhouse Stronghold

Безопасное управление жизненным циклом секретов

Хранение секретов — уязвимое место в инфраструктуре организаций

Инфраструктурные секреты — ключевые компоненты безопасности информационных систем и приложений. Это пароли, ключи API, SSH-ключи, токены и другие конфиденциальные данные — они позволяют приложениям и сервисам взаимодействовать друг с другом и функционировать безопасно.

Неправильное управление этими данными может привести к серьёзным последствиям — от утечек и взломов до полной компрометации бизнес-процессов, вследствие чего компании терпят ощутимый финансовый и репутационный ущерб.

Эффективный подход к управлению секретами

Чтобы снизить подобные риски, необходимы комплексный подход и внедрение передовых технологий и методов защиты. В частности, могут помочь специальные инструменты — так называемые хранилища секретов.

Deckhouse Stronghold — решение, предназначенное для централизованного управления секретами, их хранения и контролируемого распространения в безопасной и управляемой среде.

Решение обеспечивает защиту конфиденциальных данных при взаимодействии пользователей и приложений, что, в свою очередь, позволяет повысить уровень безопасности существующих бизнес-процессов организации, а также выполнить требования законодательства и различных стандартов по защите конфиденциальной информации (КИ).

Кроме того, Deckhouse Stronghold повышает уровень автоматизации процессов управления секретами, что помогает оптимизировать трудозатраты персонала и сократить издержки, вызванные большим количеством ручных операций с секретами.

Основные возможности

- Централизованное управление жизненным циклом секретов
- Автоматизация процессов хранения секретов и аудит доступа к ним
- Замена HashiCorp Vault и других зарубежных аналогов
- Выполнение требований законодательства по защите КИ
- Снижение трудозатрат персонала на управление секретами на ~40 %
- Изменение структуры расходов на управление секретами (↓OPEX)

Что такое секреты?

- Пароли
- Сертификаты
- Токены
- Ключи API
- SSH-ключи

Типы секретов

Пользовательские
(человек — приложение)

Инфраструктурные
(приложение — приложение)

80 %

ИТ-и DevOps-команд хранят секреты небезопасно[1]

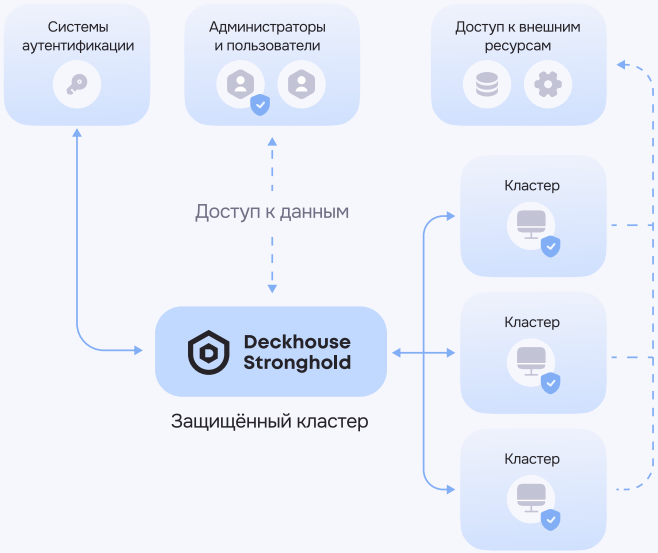
25 минут

ежедневно тратит один сотрудник на ручное управление секретами[1], что может привести к большим годовым издержкам (~4 млн руб.)

1 По данным отчёта Secrets management: the next big security threat for businesses компании 1Password.

Принцип работы

- Клиент (приложение, сервис, пользователь) проходит процедуру аутентификации в Stronghold и запрашивает доступ к необходимому секрету
- Stronghold анализирует запрос, а затем подтверждает либо отклоняет его
- Если доступ есть, операция по чтению секрета разрешается. Если доступа нет — операция отклоняется
- Используя полученный секрет, клиент получает доступ к внешним ресурсам



Преимущества

Пространства имён (namespaces), максимально совместимые с HashiCorp Vault Enterprise по возможностям и методам API. Функция позволяет создавать дочерние рабочие пространства, выдавать права на управление ими, а также поддерживать вложенность и создавать иерархии.

Автоматические бэкапы. Резервные копии создаются автоматически по настроенному расписанию и могут сохраняться как в файлы, так и в S3-совместимое объектное хранилище.

Репликация данных. Возможность реплицировать хранилища секретов типа KV1/KV2. Построена на архитектуре master-slave с применением pull-модели получения данных: подчинённые slave-узлы сами опрашивают master-узел.

Поддержка аппаратных модулей безопасности (HSM). С помощью внешних HSM можно шифровать и расшифровывать root-ключ, которым Deckhouse Stronghold шифрует данные, используя алгоритм AES 256, а также обеспечить двойное шифрование особенно чувствительных данных, применяя комбинации нескольких алгоритмов (AES + RSA, AES + AES, AES + ГОСТ).

Несколько безопасных способов автоматизированной доставки секретов в приложения. За них отвечает модуль secrets-store-integration. Автоматическая доставка секретов упрощает процесс интеграции и минимизирует ручной труд, а также уменьшает вероятность утечек данных.

Сокращение количества возможных векторов атаки. В основе хранилища только один бинарный файл, что уменьшает количество потенциальных точек входа для атак и повышает общую безопасность системы.

Простота использования. Удобный веб-интерфейс делает процесс управления секретами понятным и доступным для пользователей различного уровня.

Управление через единый API, совместимый с API HashiCorp Vault. Полная совместимость с API HashiCorp Vault позволяет легко интегрировать Deckhouse Stronghold в существующие системы и использовать уже имеющиеся инструменты и скрипты.

Возможность автоматического распечатывания (auto unseal). Позволяет автоматически разблокировать хранилище после перезапуска или перезагрузки узлов, устраняя необходимость ручного вмешательства и снижая риск ошибки.

Безопасность соединений. Все сетевые соединения в Deckhouse Stronghold проходят через протокол TLS с проверкой сертификатов удостоверяющего центра (Certificate Authority), что обеспечивает высокий уровень защиты данных при передаче.

Deckhouse Stronghold | Перейти в Telegram | Смотреть RuTube | Открыть блог