

Deckhouse
Stronghold

Deckhouse Stronghold.
Обзорная презентация

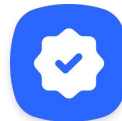
Что такое секреты и почему их важно защищать



Что можно считать секретами?



Пароли



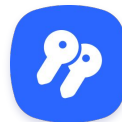
Сертификаты



Токены

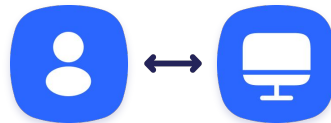


Ключи API

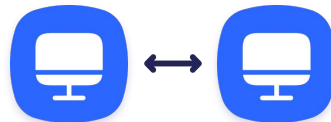


SSH-ключи

Секреты могут быть:



Пользовательскими
(человек ↔ приложение)



Инфраструктурными
(приложение ↔ приложение)



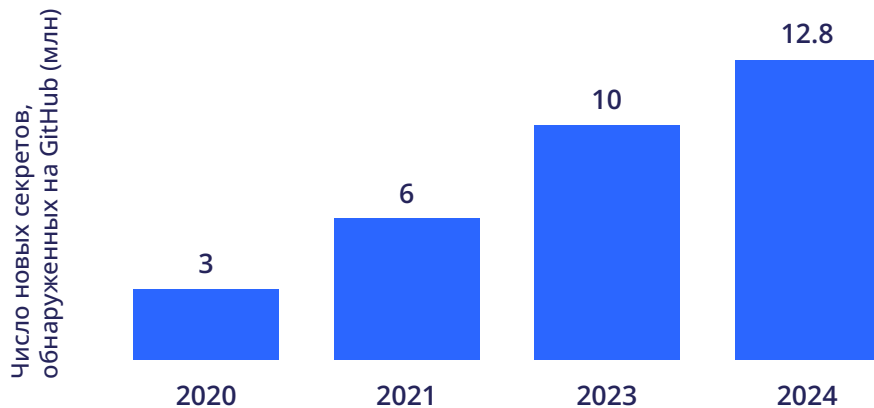
Deckhouse
Stronghold

Количество секретов непрерывно растёт

С ростом сложности цифровых цепочек поставок **разрастание секретов становится «Ахиллесовой пятой»** для организаций любого размера и уровня безопасности*

**По данным отчёта [«The State Of Secrets Sprawl 2024»](#) компании GitGuardian*

Секреты, найденные на GitHub (млн)



Не все компании хранят секреты безопасно*

Интересный факт

Более 90% скомпрометированных секретов остаются валидными в течение 5 дней**

**По данным отчёта [«Secrets Management: The Next Big Security Threat For Businesses»](#) компании 1Password*

***По данным отчёта [«The State Of Secrets Sprawl 2024»](#) компании GitGuardian*

80% ИТ/DevOps-команд не обеспечивают безопасного хранения секретов



65% уверены, что в их инфраструктуре более 500 секретов



60% сталкивались с утечками секретов



25% хранят секреты более чем на 10 ресурсах и обмениваются ими



Ручное управление секретами — дорого и долго



- Из-за утечки секретов компании несут не только репутационные, но и финансовые потери — средний ущерб от одной утечки оценивается в 11,5 млн руб.*
- 61% DevOps-команд признались, что разработка продуктов ведётся с задержкой в связи с низким качеством процессов управления секретами**
- 80% отметили, что слишком заняты, чтобы уделять должное внимание секретам**
- 25 минут в день тратит один сотрудник ИТ-и DevOps-команд на ручное управление секретами, что приводит к большим годовым издержкам*

**По данным отчёта [«Оценка ущерба от утечек информации и затрат на ликвидацию последствий»](#) группы ЦИРКОН и ГК Infowatch*

***По данным отчёта [«Secrets Management: The Next Big Security Threat For Businesses»](#) компании 1Password*

Ручное управление секретами — дорого и долго



Количество секретов	1-100	100-500	500 и более
Количество сотрудников	1	2	4
Общие трудозатраты в день, ч.	0,25	2	8
Общие трудозатраты в год, ч.	62	496	1 984
Издержки в год, руб.	124 000	992 000	3 968 000

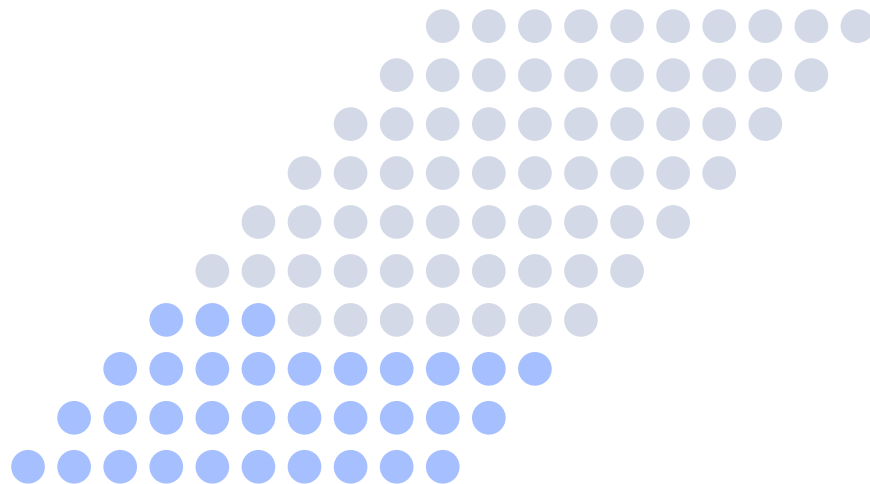
Защита секретов входит в топ-5 направлений развития ИБ

Какие направления наиболее
приоритетны для вашей
стратегии кибербезопасности?

**По данным отчёта [«The State of Secrets Management 2024»](#) компании Akeyless*



Защита секретов входит в **топ-5** направлений развития ИБ



33%* считают безопасность секретов
одним из важнейших приоритетов

**По данным отчёта «The State of Secrets Management 2024»
компании Akeyless*

Недавние кейсы



Код и пароли Binance были доступны на GitHub в течение нескольких месяцев

Источник: securitylab.ru



Mercedes-Benz

Исходные коды Mercedes-Benz утекли из-за случайно раскрытого токена GitHub

Источник: xakep.ru



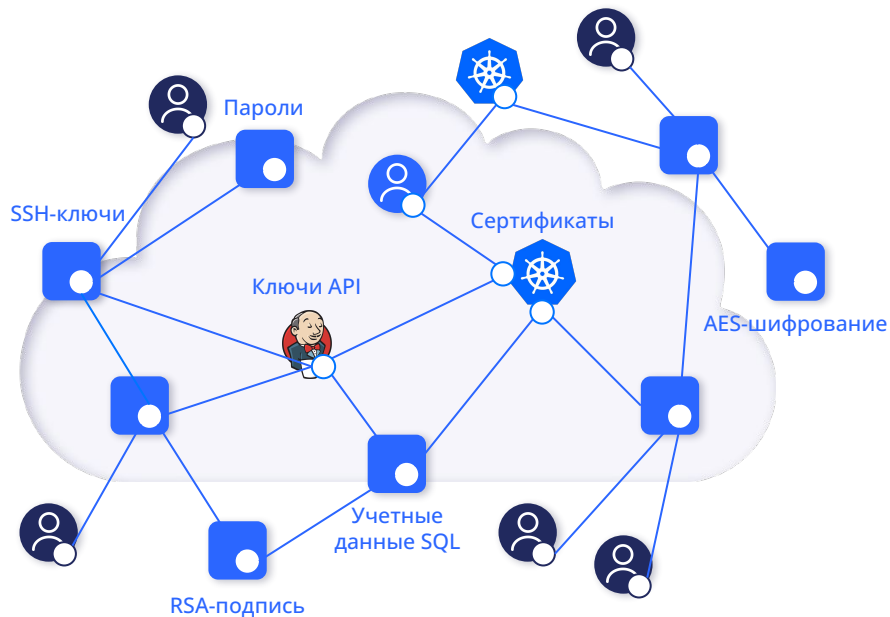
DeerSeek допустил утечку данных более чем на миллион записей

Источник: wiz.io

Использование секретов становится более массовым

Основные тренды, влияющие на рост количества секретов:

- 1 Контейнеризация
- 2 Гибридные и мультиоблака
- 3 DevOps, CI/CD и автоматизация
- 4 Технологии Zero Trust



Как **правильно** хранить секреты



В репозитории с секретами
или репозитории приложений



В системе управления
конфигурациями



В системе деплоя
(Jenkins, Teamcity)



Только на серверах, на которых
работает ваш сервис



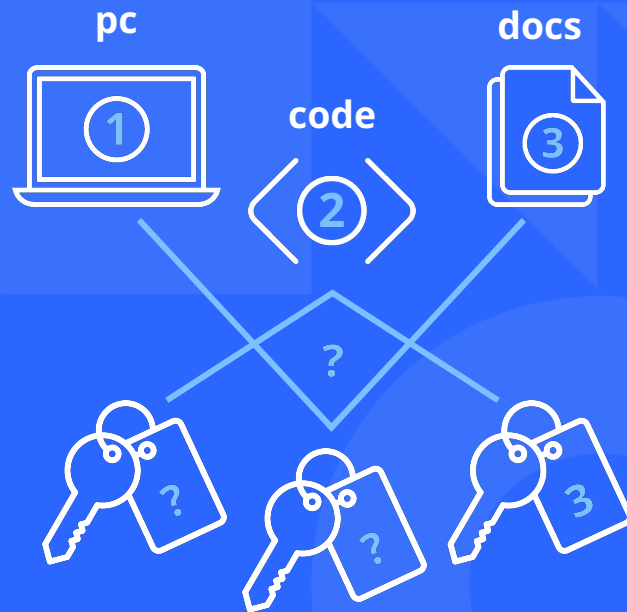
Только на личном компьютере



В отдельном хранилище секретов

Ручное управление секретами

- Секреты организации хранятся **хаотично** и в **небезопасных** местах
- IT-отделы и DevOps-команды **не могут их контролировать**
- Появляются **уязвимости**, возрастает риск компрометации и **утечки секретов**



Хранение секретов с помощью Deckhouse Stronghold

- **Централизованное решение** для безопасного хранения секретов
- **Легкое управление** жизненным циклом секретов и ролями доступа к ним
- Полное **шифрование данных** — даже если кто-то украдёт физический сервер, он не сможет получить доступ к секретам



DECKHOUSE

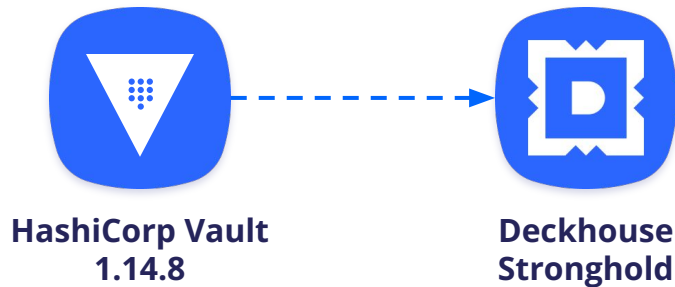
Stronghold



Что такое Deckhouse Stronghold

Решение для централизованного управления жизненным циклом секретов.

Защищает пароли, ключи API, сертификаты, SSH-ключи, токены и другие конфиденциальные данные от утечек, а также обеспечивает безопасную доставку секретов в приложения.



Мы **не копируем**
HashiCorp Vault,
мы **переосмысливаем**
хранилище секретов

Какие задачи мы помогаем решать



Выполнить требования НПА
(ФЗ-152, ФЗ-149, ФЗ-187*)



Реализовать переход
на отечественное ПО



Исключить небезопасное
и хаотичное хранение секретов



Сформировать единый подход
к управлению секретами



Изменить структуру расходов
на управление секретами (↓OPEX)



Компенсировать нехватку
экспертизы и ресурсов персонала

**По завершении процедуры сертификации ФСТЭК России*

Выполнение требований законодательства по защите конфиденциальной информации



Ситуация

Законодательство по защите КИ непрерывно развивается, появляются новые требования



Проблемы

Как разобраться в законах и выполнить необходимые требования?



Решение

Deckhouse Stronghold соответствует всем необходимым требованиям законодательства (ФЗ-152, ФЗ-149, ФЗ-187*)



**По завершении процедуры сертификации ФСТЭК России*

Переход на российское ПО



Ситуация

Западные вендоры ушли,
оставив без поддержки



Проблемы

Какое ПО выбрать на замену?
Какому вендору довериться?



Решение

Deckhouse Stronghold находится в реестре
отечественного ПО (№22339 от 24.04.2024),
полностью соответствует требованиям
Минцифры и имеет надёжную техническую
поддержку от вендора



Отсутствие контроля и единого подхода



Ситуация

Бизнес развивается, вместе с тем растёт и количество секретов



Проблемы

Где хранятся секреты? Надёжно ли они защищены? Не случится ли утечка?



Решение

Deckhouse Stronghold хранит все секреты в едином месте в зашифрованном виде, благодаря чему даже физическое хищение серверов не позволит злоумышленникам получить к ним доступ



Оптимизация трудозатрат персонала



Ситуация

Сотрудники тратят слишком много рабочего времени на ручное управление секретами



Проблемы

Как оптимизировать ресурсы и сфокусироваться на более профильных задачах?



Решение

Deckhouse Stronghold автоматизирует процессы хранения секретов и управления ими — это экономит в среднем 105 рабочих дней персонала в год



Deckhouse Stronghold **помогает**

- Исключить риски утечек конфиденциальной информации
- Оптимизировать трудозатраты персонала (команды DevOps и DevSecOps, сотрудники ИБ, разработчики)
- Сократить time-to-market и время интеграции при разработке собственных продуктов и сервисов
- Снизить издержки, возникающие вследствие ручного управления секретами

Вы получаете

- ✓ Защиту бизнеса от финансовых и репутационных потерь
- ✓ Возможность фокусироваться на более профильных задачах
- ✓ Своевременный запуск продуктов, соответствующих требованиям ИБ
- ✓ Уменьшение операционных расходов (OPEX) на ИБ

Основные возможности продукта



Хранение секретов как key-value



Отказоустойчивость «из коробки»



Доступ к хранилищу через API и UI



Совместимость с API HC Vault



Хранение данных в зашифрованном виде



Полная наблюдаемость жизненного цикла секретов



Разграничение доступа с помощью гибкого набора политик



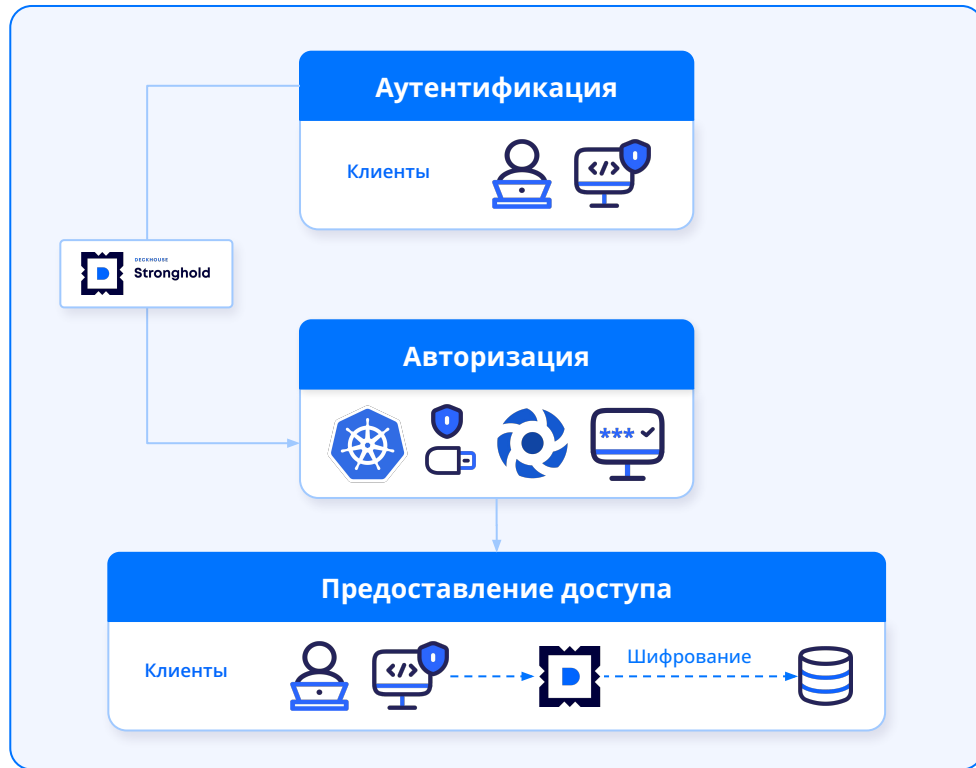
Интеграция с внутренними и внешними сервисами

Как устроен Stronghold

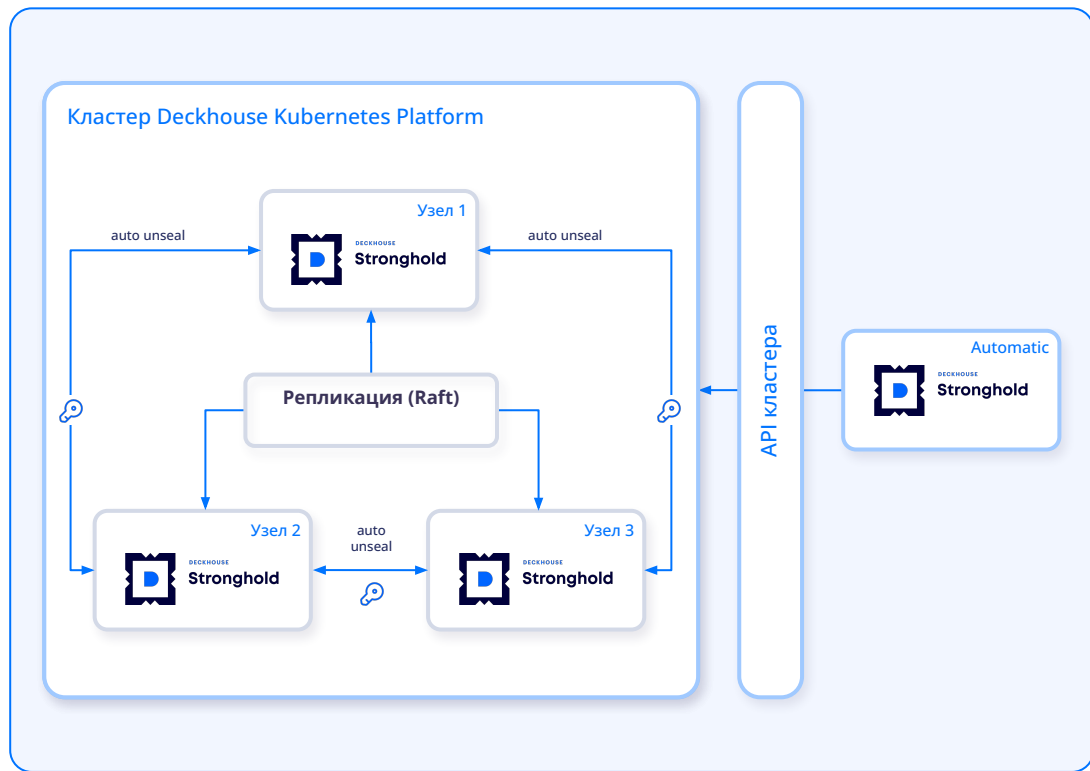


Как работает Stronghold

- Клиент через Stronghold или внешнюю систему подтверждает, что обращается именно он
- Stronghold анализирует, можно ли предоставить доступ к запрошенному секрету
- Если доступ есть, то операция по чтению или записи секрета разрешается



Отказоустойчивость Stronghold



- Любой активный узел Stronghold в кластере обнаруживает и автоматически распечатывает остальные узлы при условии, что у них валидный сертификат (ключ хранится только в памяти Stronghold)
- Для репликации данных и отказоустойчивой работы Stronghold используется алгоритм Raft
- Компонент **Stronghold Automatic** отвечает за настройку аутентификации, создание групп и ролей администраторов

Безопасность Stronghold

В рамках сертификации ФСТЭК России по 4-му уровню доверия Stronghold проходит **комплексную проверку** защищённости различными методами тестирования:



Статический анализ
исходных текстов



Тестирование на проникновение



Динамический анализ
исходных текстов



Фаззинг-тестирование

АО «Флант» выстраивает процессы безопасной разработки ПО
согласно ГОСТ Р 56939-2024

Преимущества Stronghold

Механизм namespaces для создания пространств имён и делегирования прав на управление ими

Единое хранилище секретов с возможностью автоматического распечатывания (auto unseal)

Поддержка различных методов аутентификации и гибкая настройка авторизации и политик доступа к хранилищу и секретам

Удобный и русифицированный веб-интерфейс

Управление через единый API, совместимый с API Hashicorp Vault

Репликация KV1/KV2 на архитектуре master-slave с применением pull-модели

В реестре отечественного ПО
(реестровая запись №22339 от 24.04.2024)

Модуль secrets-store-integration (несколько безопасных способов автоматизированной доставки секретов в приложение)

Только один бинарный файл — минимум векторов атаки

Все соединения только через TLS с проверкой CA

Возможные сценарии использования

Для кого полезно:



Команды DevOps и DevSecOps



Сотрудники подразделений ИБ



Разработчики

Хранение секретов

- Доступ к секретам в зашифрованном хранилище через API
- Модуль доставки помогает безопасно подкладывать секреты в качестве переменных окружения или файлов в приложения

Секреты для CI/CD

- Интеграция с системами CI/CD (Jenkins, GitLab CI, CircleCI и др.) позволяет автоматически обновлять секреты в процессе развертывания

Управление инфраструктурой частных ключей (PKI)

- Хранение и управление жизненным циклом сертификатов и ключей, включая списки отзыва

Аутентификация и авторизация

- Интеграция с существующими системами аутентификации и авторизации (LDAP, Active Directory, Blitz, Keycloak и Kubernetes)
- Подпись SSH-ключей для безопасного доступа к серверам

Управление динамическими секретами

- Создание временных учётных данных для доступа разработчиков и приложений к базам данных PostgreSQL, MySQL и MongoDB

**Мы умеем хранить
секреты!**



**Deckhouse
Stronghold**



[Заявка на демо](#)

Проведём демонстрацию продукта
и ответим на все вопросы

ОТКАЗ ОТ ОТВЕТСТВЕННОСТИ

Информация, изложенная в настоящем материале/презентации, представлена в ознакомительных целях, и не является ни основанием для принятия коммерчески значимых решений, ни персональным либо публичным предложением к заключению каких-либо соглашений или договоров.

В связи с тем, что планы и решения касаются возможностей осуществления процесса разработки и релиза указанных программных продуктов и/или их отдельных модулей остаются на усмотрение АО «Флант», настоящим мы не предоставляем каких-либо явных и/или подразумеваемых заверений об обстоятельствах либо гарантий касаются, в том числе, но не ограничиваясь, функциональных характеристик, описания, коммерческих условий и возможности разработки, релиза и распространения программных продуктов.