ЭВРИТЕГ Платформа безопасности данных

Предотвращение массовых утечек чувствительных данных из информационных систем

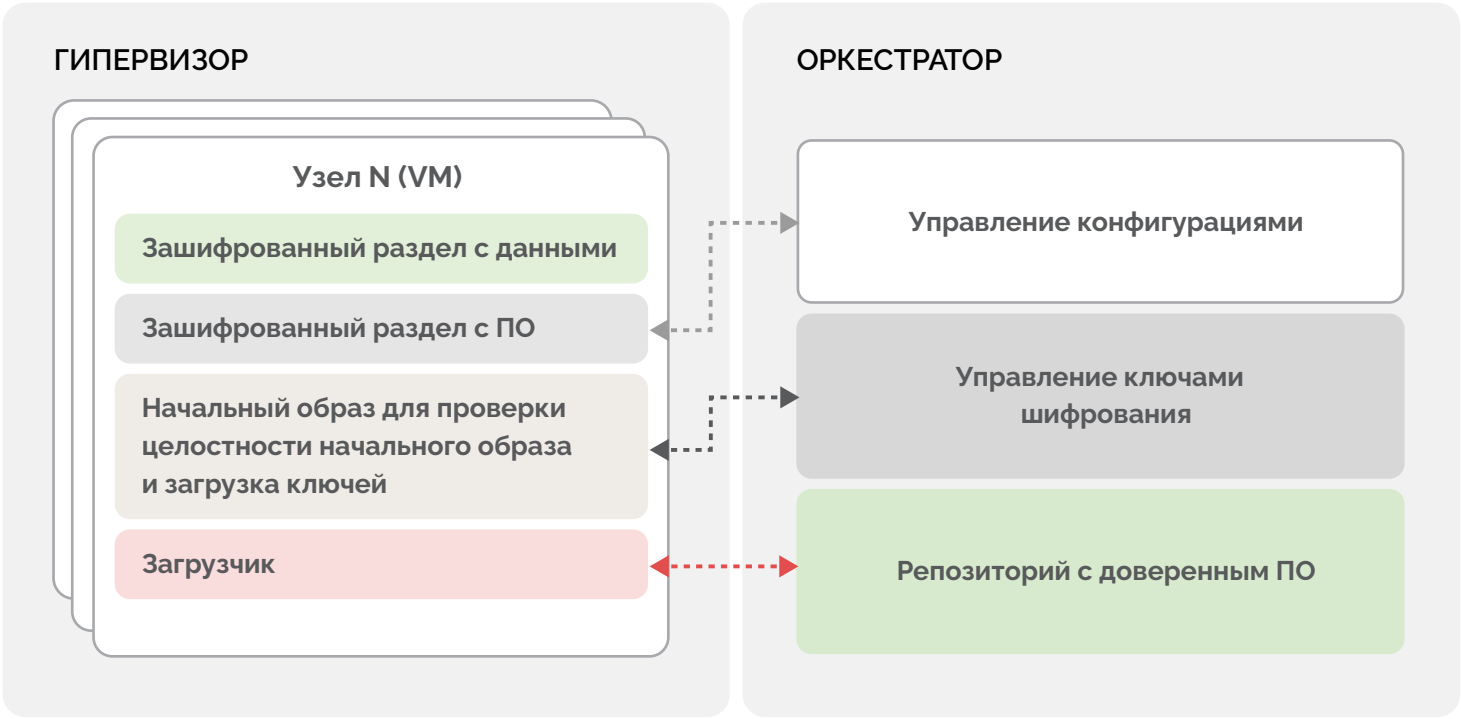
ЭВРИТЕГ

Новый продукт от компании ЭВРИТЕГ помогает компаниям, которые хранят чувствительные данные в различных базах данных (таких как Postgres, MongoDB, ClickHouse), не допустить их потерю или утечку из-за действий злоумышленников.

Реализованный комплексный подход к обеспечению защиты данных гарантировано не имеет возможности их обойти, даже привилегированным пользователям

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ ПРОДУКТА

- Развертывание баз данных в безопасной оболочке для предотвращения несанкционированного доступа
- Преднастроенные политики безопасности, которые можно удобно настраивать под конкретную специфику бизнеса
- Единый оркестратор для управления всеми базами данных компании
- Поддержка вертикальной и горизонтальной масштабируемости
- Удобные инструменты эксплуатации и миграции данных
- Решение соответствует требованиям регуляторов РФ (скоро)



ОТ ЧЕГО ЗАЩИЩАЕМ

- От выгрузки данных за счет автоматизации запросов (получение всех данных БД через единичные запросы) в следствии умышленных действий пользователя или взлома клиентской машины
- От скачивания дампа базы или файлов данных при доступе к серверной инфраструктуре, в следствии умышленных действий администраторов или нарушения регламентов эксплуатации
- От взлома и хищения данных со стороны хакеров, получивших доступ к инфраструктуре в следствии эксплуатации уязвимостей, компрометации учетных данных пользователей

В реализации продукта заложены концепции модели Zero Trust (концепция Нулевого Доверия):

Безопасный доступ ко всем ресурсам независимо от их местоположения

Основная задача средств защиты на уровне клиента и бизнес-приложения, усложнить возможность «автоматизированного» сбора данных в случае утраты контроля над рабочим местом пользователя, а также исключить возможность доступа к сервису вне рабочего места пользователя.

Для этого применяются следующие подходы:

- Механизмы контроля серверного и клиентского сертификатов
- Механизмы аутентификации клиента (совместно с аутентификацией пользователей на уровне бизнес-приложения)
- Механизмы использования различных клиентов (и секретов) для работы с различными сущностями
- Механизмы передачи данных конечного пользователя при обращении к БД

Проверка и регистрация всего трафика

Основной уровень защиты данных при утрате контроля над рабочим местом пользователя или злоупотреблении со стороны легитимного пользователя.

Основные механизмы защиты:

- Проверка адресов (белые/черные списки)
- Аутентификация и идентификация пользователей и клиентов
- Частотная фильтрация запросов на основании статистической модели
- Фильтрация ответов (маскирование, ограничение)

Стратегия минимальных привилегий и инверсивных механик управления

На данном уровне, все механизмы защиты нацелены на предотвращение доступа к данным со стороны привилегированных пользователей (в том числе администраторов средств виртуализации) в случае утраты контроля над рабочими местами, компрометации учетных данных или умышленного злоупотребления.

Механизмы защиты базируются на нескольких принципах:

- Инверсия управления
- Доверенное ПО
- Проверка целостности образа виртуальной машины
- Отсутствие прямого доступа
- Контролируемый запуск

ЭВРИТЕГ

Устойчивость к кибератакам, что обеспечивает непрерывность бизнес-процессов и минимизирует финансовые потери от простоя

Повышение доверия клиентов и укрепление репутации как надежного партнера и поставщика услуг за счет демонстрации высокого уровня информационной безопасности

Минимизация последствий, связанных с нарушением конфиденциальности персональных данных или в следствии возможных судебных исков

Повышение эффективности работы внутренних служб, таких как ИТ, ИБ и SOC за счет автоматизации процессов аудита и контроля доступа к данным

Снижение зависимости от дорогостоящих кадров для эксплуатации платформы и сложного внедрения в клиентский ИТ ландшафт

DSP.EVERYTAG.RU

EVERYTAG.RU +7 (495) 141 44 45 HELLO@EVERYTAG.RU