Решения для защиты данных

Самые современные алгоритмы шифрования с сохранением исходного формата, stateless-токенизация и управление ключами, реализованные компанией Micro Focus в решениях для защиты данных, позволяют защищать корпоративные приложения, инфраструктуру обработки данных, гибридные и облачные ИТ-среды, платежные экосистемы, критически важные системы, хранилища, а также платформы Больших данных и Интернета вещей.

Основные решения:

+ Масштабируемая защита Больших данных
+ Снижение затрат на соблюдение нормативных требований
+ Безопасный обмен данными в корпоративной среде

Наши возможности:

+ Шифрование с сохранением исходного формата
+ Защищенная stateless-токенизация
+ Создание криптографических ключей по требованию

Наши преимущества:

+ Нейтрализация последствий компрометации инфраструктуры благодаря деидентификации данных
+ Доступность защищенных данных для приложений и анализа
+ Сплошная защита данных — от унаследованных до гибридных ИТ-систем

Решения Micro Focus Data Security обеспечивают переход на инновационные, дата-центричные механизмы безопасности, оснащенные возможностями шифрования и токенизацией. С их помощью ведущие компании мира защищают корпоративные данные и тем самым нейтрализуют негативные последствия возможныз взломов или утечек данных при хранении, перемещении и обработке. Data Security решает самую острую проблему ИБ, упрощая защиту данных в сложных многокомпонентных средах, содержащих как унаследованные, так и новые системы.

Решения

Масштабируемая защита Больших данных

Технология Hyper FPE эффективно, с высокой производительностью защищает потоки данных, поступающие в озера данных, позволяя аналиировать продуктивные данные и уменьшая вероятность их ненадлежащего использования или утечки. Надежно защищенная информация, очищенная от идентифицирующих сведений, становится доступной более широкому кругу руководителей различных подразделений компании и определенным группам бизнес-пользователей, что способствует созданию новых источников доходов и оптимизации ИТ без возрастания риска потери данных по мере увеличения их объемов.

Снижение затрат на соблюдение нормативных требований

Данные очищаются от идентифицирующих сведений с помощью проверенных, основанных на стандартах методов, которые соответствуют требованиям псевдонимизации и анонимизации, предусмотренным европейской директивой GDPR и аналогичными законами. Шифрование и хеширование с сохранением формата препятствуют возникновению сбоев в работе приложений и процессов и поддерживаются как для традиционных, так и для гибридных ИТ-сред. Сократить масштаб аудиторских проверок помогает stateless-токенизация (без смены состояния), проверенная на соответствие требованиям стандарта PCI DSS, который используется ведущими банками, сетями розничной торговли и платежными системами.

Защищенные облачные рабочие нагрузки

Облачные механизмы защиты данных Micro Focus SecureData поддерживают как гибридные, так и традиционные ИТ-системы, предоставляя единую панель управления.

В SecureData реализован не зависящий от конкретных платформ подход к развертыванию, позволяющий преодолевать границы между ИТ-системами. Это достигается благодаря stateless-архитектуре (без отслеживания состояния) и шлюзам, использующим технологию SecureData Sentry.

Аппаратные средства, гарантирующие надежную защиту

Atalla HSM и Enterprise Secure Key Manager (ESKM) являются основой комплексов обеспечения усиленной безопасности, сертифицированных на соответствие стандарту NIST FIPS 140-2 и предназначенных для криптографической защиты данных в рамках процессов, требующих повышенной надежности, в том числе в платежных приложениях, а также в системах управления ключами для хранилищ и серверных данных. Atalla HSM интегрируется с программными

комплексами Micro Focus SecureData, предоставляя аппаратную базу для защиты криптографических секретов.

Защищенный обмен сообщениями в корпоративной среде

Система сквозного шифрования электронной почты для настольных компьютеров, облаков и мобильных устройств масштабируется до миллионов пользователей и обеспечивает защиту конфиденциальных сведений, в том числе составляющих врачебную тайну. Помимо соблюдения нормативных требований к конфиденциальности, уменьшается вероятность ненадлежащего использования данных и уязвимостей, которые приводят к потерям данных, штрафам и восстановительным работам.

Продукты

Voltage SecureData Enterprise

Сквозная защита при помощи Hyper FPE и токенизации гарантирует обеспечение безопасности данных на протяжении всего жизненного цикла информации — от ее создания до использования, перемещения и хранения.

- Обеспечивает высокий уровень масштабирования при защите решений по приему, обработке, хранению и иным операциям с данными.
- Помогает соблюдать нормативные требования, ограничивая область их действия, снижая затраты на внедрение и управление.
- Поддерживает как унаследованные, так и современные гибридные ИТ-системы, позволяя без каких-либо затруднений внедрять новые приложения.

Voltage SecureData Payments

Шифрование по принципу «точка-точка» согласно требованиям стандарта PCI и обеспечение безопасности платежей на всем пути их проведения — от регистрации в POS-терминале до выполнения конкретных операций в процессинговом центре.

- Осуществляет сквозную защиту данных банковских карт в рамках экосистемы цифровых платежей, в том числе при хранении и перемещении денежных средств.
- Ограничивает область применения PCI без изменения критически важных рабочих и бизнес-процессов.
- Обеспечивает комплексное шифрование «точка-точка» (P2PE) и токенизацию для розничных платежей.

Voltage SecureData for Hadoop and IoT

Безопасность конфиденциальных данных, используемых в Hadoop и системах Интернета вещей, включая Kylo и Apache NiFi.

- Защищает данные на границе сред для безопасной крупномасштабной загрузки в озера и хранилища данных.
- Очищает данные от идентифицирующих сведений с сохранением возможности их использования в приложениях, предназначенных для обработки и анализа Больших данных.
- Ограничивает доступ на уровне индивидуальных полей данных, приложений и пользователей, уменьшая риски.

Voltage SecureData Cloud

Облачная система защиты данных, обрабатываемых приложениями, применяемая как для традиционных ИТ-сред, так и при переходе к гибридным.

- Позволяет выполнять анализ данных в гибридных облаках или межоблачных средах, реализуя не зависящий от платформ контроль над ключами без привязки к местонахождению данных.
- Обслуживает гибридные ИТ-среды с помощью прозрачных шлюзов, предоставляя единую панель управления.

Voltage SecureData Sentry

Сквозное шифрование с использованием современного метода брокеров безопасного доступа в облако (CASB), упрощающего внедрение средств безопасности и ускоряющего их окупаемость.

- Минимизирует вмешательство в работу систем и снижает уровень риска для унаследованных сред.
- Позволяет начать защищать приложения быстрее, чем с помощью API, упрощая разработку самых разных приложений.
- Обеспечивает поддержку CASB для SaaS, облаков, корпоративных систем, коммерческих программных продуктов, унаследованных приложений и др.

Защита периферии с SecureData

Voltage SecureData Mobile защищает данные, полученные на оконечных устройствах, а Voltage SecureData Web — конфиденциальные сведения от доступа через веб-браузеры, для чего использует инструмент Voltage Page Integrated Encryption (PIE).

- Обеспечивает защиту омниканальных решений и комплексную безопасность электронной коммерции при работе с цифровыми платежными системами.
- Помогает продавцам ограничить область применения PCI DSS для транзакций, выполняемых через мобильные устройства и веб-интерфейсы.
- Ускоряет разработку приложений с помощью простых нативных библиотек для iOS и Android.

Voltage SecureMail

Глобальное шифрование корпоративной электронной почты поддерживается для офисных сотрудников, мобильных пользователей, а также для клиентов и партнеров.

- Обеспечивает единые принципы защиты электронной почты и вложений для настольных компьютеров, облачных сервисов и мобильных устройств.
- Масштабируется за счет использования stateless-управления ключами (без отслеживания состояния) с применением основанной на стандартах технологии Identity-Based Encryption (IBE).
- Гибкое SaaS-решение поддерживает гибридные, локальные и облачные ИТ-среды.

Atalla HSM

Аппаратный модуль безопасности, сертифицированный на соответствие FIPS 140-2 Level 3, защищает зашифрованные материалы и обеспечивает аутентификацию по карте.

- Отвечает высочайшим государственным стандартам и требованиям финансовой отрасли к обеспечению гарантированной надежности.
- Обеспечивает защищенную высокопроизводительную масштабируемую обработку финансовых транзакций.
- Устанавливает новые стандарты удаленного управления и защиты ключей.

Enterprise Secure Key Manager (ESKM)

Управление криптографическими ключами для защиты инфраструктуры хранения и серверных данных с поддержкой стандарта OASIS KMIP.

- Взаимодействует с решениями, реализующими стандарт KMIP, в составе комплекса обеспечения усиленной безопасности, сертифицированного на соответствие FIPS 140-2 Level 2.
- Защищает данные на дисковых массивах, в ленточных библиотеках и связанных с ними ИТ-системах, сохраняя высокую доступность информации.
- Реализует универсальные принципы управления ключами предприятия, защищая ключи приложений, работающих в глобально распределенной среде.

Более подробная информация представлена здесь:

https://software.microfocus.com/software/data-security-encryption