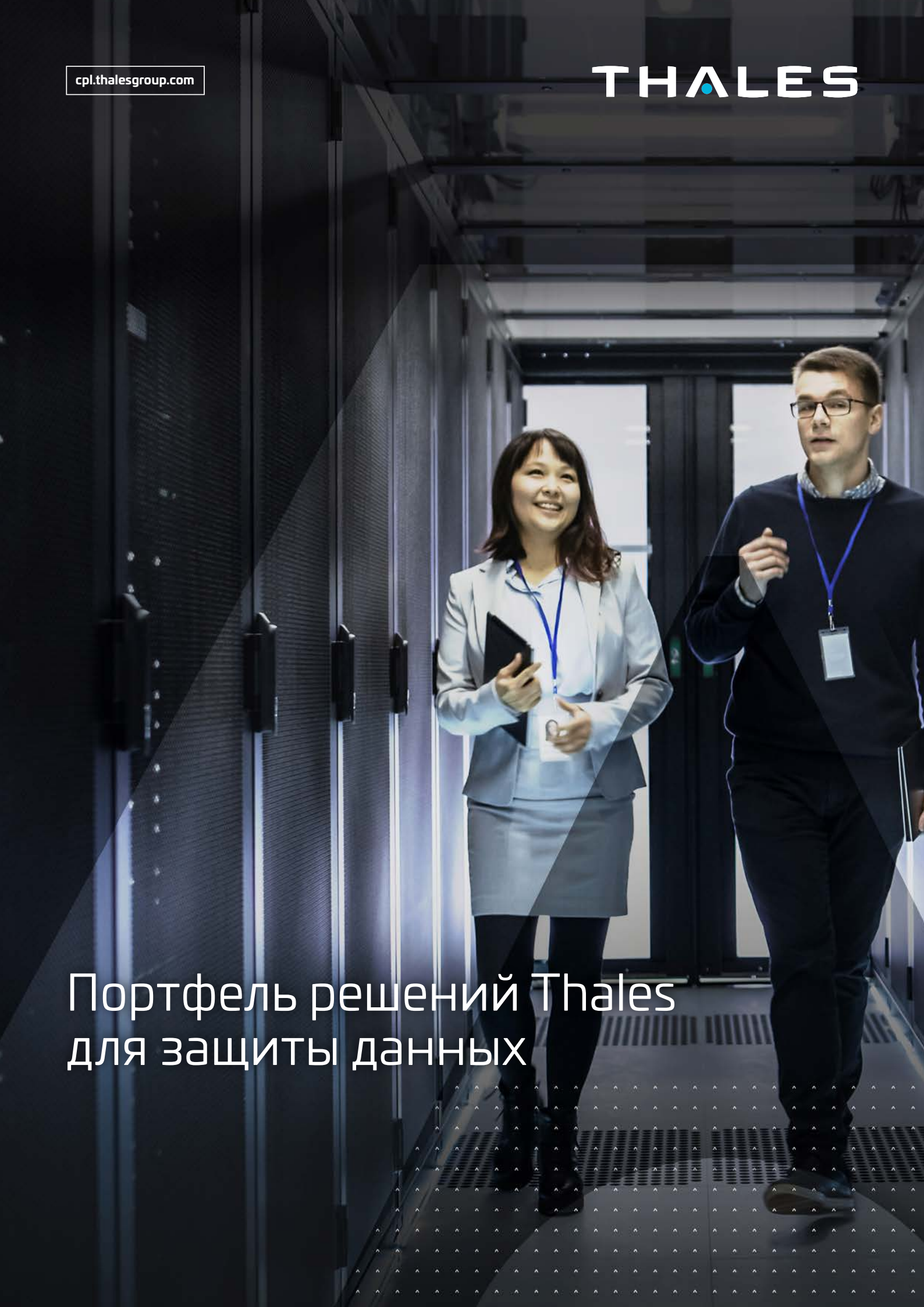
cpl.thalesgroup.com

THALES



Портфель решений Thales для защиты данных

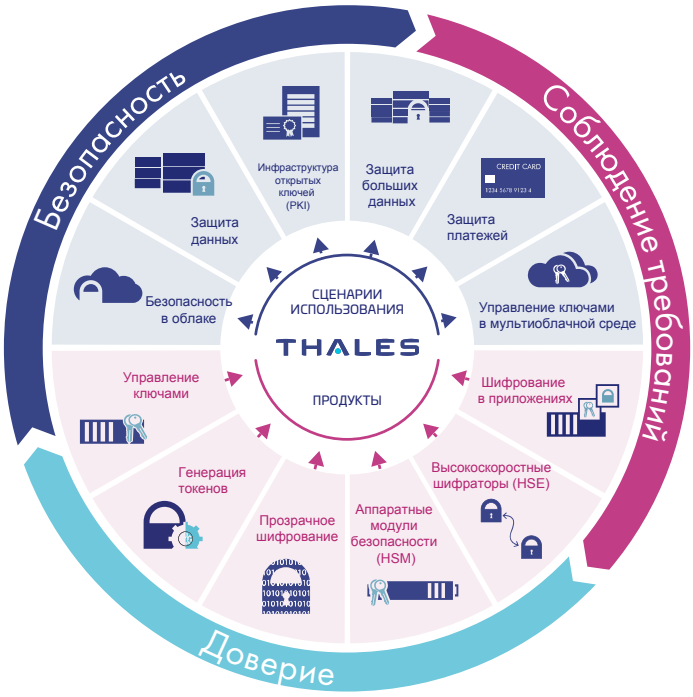
Портфель решений Thales для защиты данных

Нарушения безопасности возникают с пугающей регулярностью, а нормативные требования к защите данных ужесточаются — компаниям нужны эффективные инструменты для обнаружения и защиты конфиденциальных данных в локальных, гибридных и мультиоблачных средах.

Thales предлагает портфель передовых продуктов, которые помогают организациям защитить данные при хранении и передаче в масштабах всей ИТ-экосистемы и обеспечить полную безопасность и контроль ключей шифрования. Эти решения упрощают процессы защиты данных, повышают эффективность работы компаний и помогают быстро адаптироваться к нормативным требованиям. Независимо от того, где размещены ваши данные, они всегда будут в безопасности. Надежные и эффективные продукты и решения Thales могут разворачивать в своих средах центры обработки данных, поставщики облачных служб (CSP) и поставщики управляемых сервисов (MSP). Их также можно использовать как облачную службу, находящуюся под управлением Thales.

Возможности, которые предоставляют продукты Thales для защиты данных:

- **Защита данных при хранении** с помощью платформы CipherTrust Data Security Platform. Обнаружение, защита и контроль конфиденциальных данных организации в любой среде с помощью унифицированных инструментов нового поколения.
- **Защита данных при передаче** с помощью специализированных высокоскоростных аппаратных и виртуальных сетевых шифраторов. Высокоскоростные шифраторы позволяют защитить конфиденциальные данные (включая данные видео- и голосовой связи) при их передаче между ЦОД, из точки в точку, в узлы для резервного копирования и аварийного восстановления, а также в облачные хранилища.
- Безопасное **управление ключами шифрования** с распределением обязанностей на всем протяжении жизненного цикла. Для этого можно воспользоваться платформой CipherTrust Data Security Platform либо службами CipherTrust Key Broker, доступными в рамках платформы Data Protection on Demand (DPoD).
- **Контроль криптографических функций**. Безопасное управление, обработка и хранение ключей и функций шифрования с помощью надежных и устойчивых к взлому модулей Luna Network Hardware Security Modules (HSM) и облачных модулей Luna Cloud HSM, соответствующих стандарту FIPS 140-2. Аппаратные модули можно использовать в локальной среде предприятия, а облачные — на платформе DPoD как службу. Кроме того, можно развернуть гибридное решение, поддерживающее и локальную, и облачную среду.
- **Эффективная защита транзакций** в средах обработки розничных платежей, в платежных приложениях и при обработке платежей с PIN-кодом с помощью модулей payShield HSM.
- **Безопасный обмен файлами** между внутренними и внешними пользователями и возможность хранить, публиковать и синхронизировать файлы в локальной и облачной среде с помощью корпоративного приложения SureDrop, обеспечивающего защиту данных на уровне оборонных стандартов.



Основные преимущества

- **Усиленная безопасность и соблюдение нормативных требований**
  Продукты и решения Thales для защиты данных соответствуют ряду требований к безопасности и конфиденциальности данных, в том числе Регламенту ЕС об электронной идентификации и удостоверительных сервисах для электронных транзакций (eIDAS), Стандарту безопасности данных индустрии платежных карт (PCI DSS), Общему регламенту ЕС по защите данных (GDPR), Закону США об охране и ответственности за информацию, полученную в результате медицинского страхования (HIPAA), Федеральному закону США об управлении информационной безопасностью (FISMA) и региональным законам о защите и конфиденциальности данных.
- **Повышение эффективности работы сотрудников и использования ресурсов**
  Продукты и решения Thales подходят для различных сценариев применения. Этому способствуют возможность интеграции, единый канал глобальной поддержки, успешный опыт защиты от новых и развивающихся угроз, а также крупнейшая в отрасли партнерская экосистема в области защиты данных. Мы уделяем огромное внимание удобству использования и предоставляем API для автоматизации и гибкого управления процессами, с которыми ИТ-администраторы могут быстро развернуть защиту и контролировать безопасность данных. Thales и партнеры предлагают ряд услуг по проектированию, внедрению решений и обучению работе с ними, чтобы вы могли быстро развернуть нужную защиту, не отрывая своих сотрудников от основной работы.
- **Сниженная совокупная стоимость владения**
  Thales предлагает комплекс решений и продуктов для защиты данных, доказавших свою эффективность в новых и традиционных системах. Наши решения легко масштабируются и адаптируются к новым сценариям использования. С Thales вы окупите свои вложения и сократите операционные и капитальные затраты.

Защита данных при хранении

Платформа защиты данных CipherTrust Data Security Platform объединяет функции обнаружения, классификации и защиты данных с инструментами детального контроля доступа и централизованного управления ключами. Это позволяет направлять меньше ресурсов на защиту данных, полностью контролировать соблюдение нормативных требований и снизить риски для бизнеса. Платформа состоит из перечисленных ниже компонентов.

CipherTrust Manager
CipherTrust Manager — центр управления безопасностью. Это передовое корпоративное решение для централизованного управления ключами, детального контроля доступа и настройки политик безопасности. CipherTrust Manager управляет жизненным циклом ключей шифрования: генерацией, ротацией, разрушением, импортом и экспортом, — а также контролирует доступ к ключам и политикам на основе ролей, поддерживает возможности проведения аудита и составления отчетов и содержит API REST для разработчиков. CipherTrust Manager обеспечивает централизованное управление ключами шифрования и политиками для соединителей, описанных ниже. Решение доступно в аппаратном или виртуальном варианте, оно соответствует требованиям FIPS 140-2 к безопасности (уровень 3) и использует самый защищенный корень доверия для хранения ключей.

CipherTrust Data Discovery and Classification
Решение CipherTrust Data Discovery and Classification обнаруживает структурированные и неструктурированные конфиденциальные данные, регулируемые нормативными требованиями, в облачных средах, массивах больших данных и традиционных хранилищах. Единая панель мониторинга позволяет отслеживать конфиденциальные данные и связанные с ними риски, принимать эффективные решения об устранении брешей в системе защиты, приоритизировать меры по устранению проблем и защищать данные во время миграции в облако и обмена с третьими сторонами. Решение оптимизирует процессы защиты данных, начиная с настройки политик, обнаружения и классификации данных и заканчивая анализом рисков и составлением отчетов. Таким образом, оно помогает устранить слепые зоны в системе безопасности и излишние сложности.

CipherTrust Transparent Encryption
Решение CipherTrust Transparent Encryption выполняет шифрование данных при хранении, контролирует доступ привилегированных пользователей и генерирует подробные журналы событий доступа к данным. Соединители защищают данные в файлах, томах дисков и базах данных в ОС Windows, AIX и Linux на физических и виртуальных серверах, в облаке и в средах больших данных. Расширение Live Data Transformation для CipherTrust Transparent Encryption обеспечивает непрерывное шифрование данных и смену ключей. Журналы и отчеты с аналитическими данными о безопасности помогают отчитываться о соблюдении нормативных требований и ускоряют обнаружение угроз с помощью передовых систем управления данными и событиями безопасности (SIEM).

CipherTrust Application Data Protection
CipherTrust Application Data Protection предоставляет через API криптографические функции для служб управления ключами, подписывания, хеширования и шифрования. Благодаря этому решению разработчики могут без труда защитить данные на сервере приложений или в узле больших данных. В комплект поставки решения входит совместимый пример кода. CipherTrust Application Data Protection ускоряет разработку настраиваемых решений для защиты данных и упрощает управление ключами для разработчиков. Кроме того, оно позволяет строго распределять обязанности по управлению ключами посредством политик, которые может контролировать только отдел ИТ-безопасности.

CipherTrust Tokenization
Решение CipherTrust Tokenization доступно в вариантах с хранилищем и без хранилища. Оно помогает сократить стоимость и сложность соблюдения таких стандартов безопасности данных, как PCI-DSS. Вариант без хранилища поддерживает функции динамической маскировки данных на основе политик, а вариант с хранилищем содержит дополнительные API для различных сред. Оба варианта позволяют с легкостью добавить функцию генерации токенов в приложения через API RESTful.

CipherTrust Database Protection
Решения CipherTrust Database Protection позволяют встраивать в базы данных функции шифрования данных, хранящихся в конфиденциальных полях, с обеспечением надежного централизованного управления ключами и без необходимости модифицировать приложения баз данных. Решения CipherTrust Database Protection совместимы с базами данных Oracle, Microsoft SQL Server, IBM DB2 и Teradata.

CipherTrust Enterprise Key Management
CipherTrust Key Management — надежные решения на основе стандартов для управления ключами шифрования в масштабе всего предприятия. Они упрощают административные задачи управления ключами шифрования, гарантируют надежность ключей и доступ к ним только авторизованных служб шифрования. Решения CipherTrust Key Management подходят для различных сценариев использования:

- решение **CipherTrust Cloud Key Manager** оптимизирует управление собственными ключами шифрования (BYOK) на платформах Amazon Web Services, Microsoft Azure, Salesforce и IBM Cloud. Это решение обеспечивает комплексный контроль и автоматизацию жизненного цикла ключей в облаке, повышая эффективность работы отдела ИТ-безопасности и упрощая управление ключами в облаке;
- решение **CipherTrust TDE Key Management** совместимо с такими базами данных, как Oracle, Microsoft SQL и Microsoft Always Encrypted;
- решение **CipherTrust KMIP Server** централизует управление клиентами KMIP и поддерживает полное шифрование диска, работу с большими данными, базами данных IBM DB2, архивами на магнитных лентах, VMware vSphere, шифрование vSAN и т. д.

Защита данных при передаче

Thales предлагает высокоскоростные шифраторы (HSE) для шифрования данных при передаче независимо от сети (на уровнях 2, 3 и 4). Они гарантируют безопасность данных при передаче из одной точки в другую или из локальной среды в облачную и наоборот. Решения HSE позволяют нашим клиентам лучше защищать конфиденциальные данные, данные видео- и голосовой связи и метаданные от прослушивания, наблюдения и явного или скрытого перехвата — по разумной цене и без ущерба производительности. Шифраторы HSE от Thales доступны в аппаратном и виртуальном вариантах, с одним или несколькими портами, и поддерживают широкий диапазон скоростей сети, от 10 Мбит/с до 100 Гбит/с.

- **Аппаратные шифраторы серии CN** — сетевые устройства для независимого от сети шифрования данных при передаче (на уровнях 2, 3 и 4). Они сертифицированы в соответствии с FIPS 140-2, уровень 3, а также Common Criteria EAL 2 и 4+.
- **Виртуальные шифраторы серии CV** — решения повышенной надежности, которые обеспечивают стойкое шифрование данных при передаче по высокоскоростным каналам WAN и SD-WAN с помощью виртуализации сетевых функций (NFV).

Аппаратные модули безопасности

Аппаратные модули безопасности Thales HSM помогают соблюдать требования и масштабировать защиту в процессах высокой производительности. Они обладают гарантированной надежностью, устойчивы к взлому и сертифицированы в соответствии со стандартом FIPS 140-2, уровень 3. Они защищают ключи, используемые для шифрования данных при хранении и передаче, и выступают в роли якорей доверия, обеспечивая безопасность главных ключей шифрования, цифровых удостоверений и транзакций. Thales предлагает следующие специализированные модули HSM:

- **модули HSM Luna общего назначения** — точка отсчета доверия для всей экосистемы организации, включая устройства, удостоверения и транзакции. Модули HSM Luna обеспечивают целостность ключей и функций шифрования и доступны в различных вариантах, в том числе как подключаемые к сети устройства, встраиваемые карты PCIe или портативные USB-устройства. Интеграция и разработка решений для защиты жизненного цикла ключей шифрования и операций шифрования становятся проще благодаря многочисленным API, превосходной производительности и сотням готовых партнерских приложений. Для простого управления криптографическими ресурсами HSM Luna можно использовать Crypto Command Center — централизованную платформу, обеспечивающую мониторинг, составление отчетов и подготовку модулей по требованию, а также мгновенные оповещения;
- **модули HSM для защиты платежей** обеспечивают безопасность платежных функций: обработку транзакций, защиту конфиденциальных данных, выдачу учетных данных для платежей, платежи через карты с привязкой к мобильному телефону, а также генерацию токенов для платежей. HSM-модули payShield от Thales используют эмитенты, поставщики услуг, эквайеры, операторы платежей и платежные сети во всем мире. Последняя модель, payShield 10K, соответствует ряду международных и региональных стандартов безопасности, в том числе PCI HSM v3, FIPS 140-2 (уровень 3) и AusPayNet.

Платформа Data Protection on Demand

Отмеченная наградами облачная платформа Thales Data Protection on Demand (DPoD) открывает доступ к широкому ряду облачных служб Luna Cloud HSM, CipherTrust Cloud Key Management и payShield Cloud Payment через удобный онлайн-магазин. Обеспечивать безопасность данных стало проще, дешевле и удобнее, так как больше не нужно покупать, устанавливать и обслуживать оборудование. Вы можете одним щелчком мыши развернуть нужный уровень защиты, добавить службы и политики безопасности и за несколько минут получить отчет об их использовании. Также платформа DPoD идеально подходит поставщикам управляемых сервисов обеспечения безопасности, которые реализуют модель «защита как услуга» и хотят предоставлять своим клиентам эффективные решения для защиты данных в комплексе с другими облачными службами и услугами по обеспечению безопасности.

Службы Luna Cloud HSM

Платформа DPoD поддерживает ряд облачных служб HSM для защиты данных по требованию, которые позволяют клиентам хранить ключи для шифрования данных в облаке, сохраняя полный контроль над ними. Облачные службы Cloud HSM, предлагаемые через магазин DPoD, подходят для различных сценариев использования и интеграции решений в облачных, гибридных и локальных средах.

Службы CipherTrust Cloud Key Management

Службы Key Broker на платформе DPoD предоставляют функции управления собственными ключами (BYOK) в виде облачного сервиса. DPoD обеспечивает простой и надежный контроль ваших ключей и связанных политик безопасности при шифровании данных в средах IaaS, PaaS и SaaS, управляемых поставщиками облачных служб.

Безопасный обмен файлами

Культура работы независимо от места и физической дистанции между коллегами набирает обороты. Не имеет значения, где или как работают сотрудники организации, — всегда есть потребность обмениваться файлами с внутренними и внешними пользователями и синхронизировать изменения в них. Хотя совместная работа очень важна, на передний план всегда должна выходить безопасность данных. Без этого риск несоблюдения требований и утечки данных значительно повышается. SureDrop — это решение корпоративного класса для облачных и локальных сред, которое обеспечивает безопасный обмен файлами и совместную работу с помощью сквозного шифрования. SureDrop со встроенными функциями защиты помогает организациям соблюдать строгие политики безопасного хранения файлов и обладает всеми преимуществами полнофункционального решения для обмена файлами.

О компании Thales

Люди, на которых вы полагаетесь в защите вашей конфиденциальности, полагаются на Thales в защите своих данных. Когда дело касается безопасности данных, организации вынуждены принимать множество важных решений. Вы можете положиться на Thales в том, что касается безопасной цифровой трансформации, — будь то разработка стратегии шифрования, переход в облако или соблюдение нормативных требований.

Мы предлагаем эффективную поддержку важных решений.

THALES

Обратная связь

Адреса и контактные данные всех офисов можно найти на сайте
cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <