cpl.thalesgroup.com

THALES

# Расширенная защита данных для Amazon S3 с помощью прозрачного шифрования CipherTrust

## ЗАДАЧА: предотвратить утечки данных, вызванные неверно сконфигурированными настройками безопасности Amazon S3

Amazon Simple Storage Service (S3) - одно из ведущих облачных решений для хранения данных, используемых компаниями по всему миру для поддержки своих ИТ-операций в различных сценариях использования. Сегменты Amazon S3 стали одними из наиболее часто используемых репозиториев облачных хранилищ для самых разнообразных массивов данных — от серверных журналов сервера до персональных данных клиентов. Однако некачественно сконфигурированные сегменты S3 были причиной большого количества утечек данных. Amazon действительно предоставляет ряд услуг и функций безопасности, которые ее клиенты могут использовать для защиты своих активов, но в конечном итоге поставщик облачных услуг возлагает ответственность за защиту конфиденциальности, целостности и доступности данных в облаке, а также за соблюдение определенных бизнес-требований для защита информации на самих клиентов.

# РЕШЕНИЕ: прозрачное шифрование CipherTrust для Amazon S3

В общедоступной облачной среде организации должны защищать конфиденциальные данные и поддерживать полное управление и контроль над своими данными, а также соответствующими ключами и политиками шифрования.

Thales упрощает защиту объектов Amazon S3 и помогает обеспечить соответствие нормам безопасности данных с помощью прозрачного шифрования CipherTrust. Прозрачное шифрование CipherTrust успешно работает с объектами в Amazon S3, обеспечивая прозрачное и автоматическое шифрование конфиденциальных данных, хранящихся в сегментах S3, без каких-либо изменений в приложениях, базах данных, инфраструктуре или бизнес-практике.

Особенности:

- **Прозрачное шифрование данных в облаке.** Обеспечивает прозрачное шифрование конфиденциальных данных, хранящихся в сегментах Amazon S3.
- **Безопасность ключей, принадлежащих клиенту.** Сохраняется контроль и владение ключами шифрования локально или в облаке с помощью решения, совместимого с FIPS 140-2.
- **Быстрое развертывание и внедрение.** Простые в развертывании агенты, работающие на Amazon EC2 и локальных серверах, без необходимости изменять приложения или схему базы данных.
- **Распределение обязанностей.** Добавление детального управления доступом и средств управления доступом привилегированных пользователей, контролируемые группой безопасности.

## Преимущества

**Прозрачное шифрование CipherTrust для Amazon S3.**

Усиливает безопасность данных с помощью средств контроля от несанкционированного доступа на основе детализированных политик доступа, включая, кроме прочего, идентификацию пользователя (например, для главных администраторов с привилегиями) и процессы.

- Новые элементы управления доступом к сегментам S3 для ограничения доступа только авторизованным хостам.
- Злоумышленникам будет отказано в доступе к защищенным сегментам, даже если они неправильно сконфигурированы и широко открыты.
- Ускоряет обнаружение нарушений и отвечает требованиям нормативных требований благодаря подробным журналам доступа к файлам, направляемым в систему управления информацией и событиями безопасности (SIEM).
- Обеспечивает быструю окупаемость инвестиций благодаря простой и гибкой реализации. Агенты шифрования работают на вычислительных виртуальных узлах Amazon EC2 и других серверах, имеющих доступ к сегментам S3, гибкому блочному хранилищу (EBS) и локальному хранилищу.

## Преимущества

- Прозрачное шифрование и контроль доступа к данным, хранящимся в сегментах S3.
- Контроль доступа привилегированных пользователей позволяет привилегированным пользователям выполнять свою работу, не злоупотребляя данными.
- Ведение журнала аудита доступа к данным ускоряет обнаружение угроз и упрощает проведение сетевой криминалистики.
- Использует надежные стандартные протоколы шифрования, такие как Advanced Encryption Standard (AES) для шифрования данных и Elliptic Curve Cryptography (ECC) для обмена ключами.
- Упрощает управление ключами в локальных и мультиоблачных внедрениях за счет централизации управления с помощью менеджера CipherTrust, совместимого с FIPS 140-2.

## Менеджер CipherTrust

Менеджер CipherTrust централизует управление ключами, политиками и журналами для прозрачного шифрования CipherTrust. Он доступен как в виртуальном, так и в физическом форм-факторах для безопасного хранения главных ключей с повышенным уровнем доверия. Эти устройства могут быть развернуты локально, а также в инфраструктурах частного или общедоступного облака. Это позволяет организациям выполнять нормативные правила и требования и соответствовать передовым отраслевым методы обеспечения безопасности данных.

## О компании Thales

Специалисты, которым доверена защита конфиденциальных данных, в решении этих задач полагаются на Thales. Когда дело касается безопасности данных, организации сталкиваются с все большим количеством решающих моментов. Независимо от того, разрабатывается ли стратегия шифрования, осуществляется ли переход в облако или соблюдение нормативных требований, можно с уверенностью положиться на Thales в обеспечении цифровой трансформации.

Решающая техника для решающих моментов.