### Техническое описание

Netskope API Protection

### Основные моменты

* Поиск и защита конфиденциального контента, который хранится в ваших облачных сервисах
* Инвентаризация контента и пользователей
* Выполнение различных действий, таких как аннулирование прав доступа, отправка в карантин и шифрование
* Простое и легкое внеполосное развертывание

## Для многих зарекомендовавших себя облачных сервисов корпоративного класса API-интерфейсы опубликованы, что позволяет обеспечить сторонний контроль. Netskope API Protection использует эти API-интерфейсы (предлагаемые такими вендорами как Box, G Suite, Office 365 и Slack), чтобы получить представление об использовании сервисов и о данных, которые в них присутствуют. Благодаря этому Netskope может применять мощные политики для контроля доступа и защиты данных.

### ОБЗОР ПРОДУКТА

Netskope API Protection проверяет контент, который уже присутствует в облачных сервисах, независимо от того, когда он был выгружен и где он был создан. Решение инвентаризирует и классифицирует контент, его владельцев и тех, кто с ним взаимодействует, а также сообщает статус совместного доступа к контенту. Кроме того, оно позволяет загружать файлы для изучения и выполнять разные действия, например, ограничить доступ, аннулировать общий доступ, зашифровать контент, отправить его в карантин и сохранить для судебных целей.

### ЛЕГКОЕ РАЗВЕРТЫВАНИЕ

Netskope API Protection настраивается просто и без усилий. После получения доступа к вашему частному облачному арендатору Netskope оптимизированная конфигурация использует API-интерфейс, разрешенный транзакцией по протоколу OAuth, для создания защищенного подключения к облачному сервису. И через несколько минут вы увидите, какие конфиденциальные данные есть в вашем облачном сервисе.

### ОПРЕДЕЛЕНИЕ СТЕПЕНИ ОТКРЫТОСТИ ДАННЫХ

Netskope API Protection дает подробную картину данных, хранящихся в ваших санкционированных облачных сервисах. Ваши файлы классифицируются и отображаются по следующим категориям: Частные (нет совместного доступа), Доступные внутри сети (для людей, находящихся в домене организации), Доступные вне сети (для людей вне домена организации) и Общедоступные (как правило, доступные для всех по ссылке). Кроме того, они классифицируются и отображаются по типам файлов: Google Doc, MS PowerPoint, PDF, CSV, XML, Box Note и т.д.

### NETSKOPE API PROTECTION + САМАЯ ПЕРЕДОВАЯ В ОТРАСЛИ СИСТЕМА DLP

В сочетании с Netskope DLP функция Introspection позволяет находить и защищать контент, отвечающий DLP-профилю. Используйте самую передовую в отрасли систему DLP с набором предустановленных профилей DLP, таких как «персональные данные» (PII), «конфиденциальные медицинские сведения» (PHI), «исходный код» и т.д., либо создайте собственные профили. Кроме того, интеграция Netskope с локальными системами DLP позволяет выполнить первый проход в облаке, а затем передать сведения о предполагаемых нарушениях в локальную систему DLP по защищенному протоколу ICAP.

### ДЕЙСТВУЙТЕ

Используйте мощный механизм управления политиками Netskope для блокирования, ограничения или аннулирования доступа, отправки в карантин или сохранения для судебных целей. Одним щелчком мыши ограничивайте доступ для владельцев файлов, внутренних пользователей, пользователей из одного или нескольких доменов, внесенных в белый или черный список, либо удаляйте любые найденные общедоступные ссылки. Кроме того, Netskope API Protection позволяет вам создавать политики и гарантировать их хирургически точную настройку.

Вы можете выбирать конкретный экземпляр санкционированного сервиса; работать с папками, принадлежащими всем пользователям или конкретной группе пользователей; указывать в фильтре, должна ли политика применяться к файлам, исходя из статуса общего доступа; ограничивать доступ на основании домена; выбирать типы файлов для сканирования; указывать, применять ли сканирование к файлам, двигаясь вперед и/или назад во времени; выбирать DLP-профиль, который следует применить; и назначать соответствующее действие, например, уведомить пользователя, зашифровать контент, поместить его в карантин или сохранить для судебных целей. Кроме того, вы можете настраивать отправку уведомлений, исходя из всего вышеперечисленного.

### ЗАЩИТИТЕ КОНФИДЕНЦИАЛЬНЫЙ КОНТЕНТ СИЛЬНЫМ ШИФРОВАНИЕМ

Защитите свои конфиденциальные данные сильным 256-битным шифрованием Netskope с поддержкой облачного отказоустойчивого управления ключами по стандарту FIPS 140-2 Level 3 с помощью дополнительного аппаратного модуля безопасности или интеграции с локальной KMIP-совместимой системой управления ключами.

### ЗАЩИТИТЕСЬ ОТ НАИБОЛЕЕ ОПАСНЫХ ОБЛАЧНЫХ УГРОЗ

Сочетая системы безопасности с решением Netskope Threat Protection, вы получаете защиту от различных штаммов вредоносных программ (например, программ-вымогателей), которые могут скрываться и распространяться в облачных сервисах. Вредоносные программы помещаются в карантин и заменяются файлом-заглушкой, который сообщает пользователю о принятых мерах.

### NETSKOPE API PROTECTION + ВАРИАНТЫ РАЗВЕРТЫВАНИЯ В РЕАЛЬНОМ ВРЕМЕНИ ДЛЯ ВСЕСТОРОННЕЙ ЗАЩИТЫ

API Introspection защищает контент, который хранится в облачных приложениях. Развертывание в разрыв помогает защитить и контролировать действия (например, загрузку и выгрузку) в реальном времени. Сочетание API Introspection и развертывания в разрыв позволяет защитить как хранящийся контент, так и действия в реальном времени, гарантируя безопасность ваших данных при любых условиях.

### С ПРИЦЕЛОМ НА МАСШТАБ

Некоторые крупнейшие мировые компании развернули защиту API в самых требовательных средах, причем в отдельных случаях число файлов исчисляется миллионами, а число пользователей превышает 300 тысяч. Для надежной проверки данных, независимо от количества файлов, папок или пользователей, Netskope API Protection использует заявленную на патент технологию.

# Облачные сервисы с поддержкой Netskope API Protection

Особенности решения Netskope API Protection

|  |  |
| --- | --- |
| **КАРТИНА ОБЛАЧНЫХ СЕРВИСОВ** | |
| Облачный сервис | Имя и владелец экземпляра (корпоративный, личный, иное) |
| Действия | История действий |
| Файлы | Имя файла  Владелец  Размер  Тип  Путь к файлу  Триггеры политики DLP  Статус шифрования  Открытость для внешних доменов  Истечение срока действия ссылки для общего доступа  История версий |
| Пользователи | Поименованные пользователи учетной записи с подробными сведениями о доступе  Внешние пользователи с подробными сведениями о доступе |
| **ДОСТУПНЫЕ ДЕЙСТВИЯ – ЗАВИСЯТ ОТ ОБЛАЧНЫХ СЕРВИСОВ ИЗ-ЗА БОЛЬШОГО РАЗНООБРАЗИЯ ОПУБЛИКОВАННЫХ API-ИНТЕРФЕЙСОВ** | |
| Доступ | Изменить доступ или владение  Ограничить доступ  Аннулировать доступ |
| Защита данных | Политики DLP  Предотвратить загрузку  Зашифровать/расшифровать данные |
| **Расширенная защита от угроз** | Проверка сервисов на вредоносное ПО |
| Рабочие процессы | Карантин  Сохранение для судебных целей  Уведомить изначальных/конечных пользователей о действии |

Netskope – лидер в обеспечении облачной безопасности. Мы помогаем крупнейшим организациям в мире пользоваться преимуществами облачных и веб-сервисов и при этом не жертвовать собственной безопасностью. Наша запатентованная технология Cloud XD отслеживает и контролирует действия на всех облачных сервисах или веб-сайтах, а заказчики получают всестороннюю защиту данных, которая работает абсолютно везде. Мы называем это умной облачной безопасностью.

©2019 Netskope, Inc. Все права защищены. Netskope – зарегистрированный товарный знак, а Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index и SkopeSights – товарные знаки Netskope, Inc. Все другие товарные знаки являются товарными знаками соответствующих владельцев. 07/19 DS-78-6