## Техническое описание

Netskope для SaaS, IaaS и веб-сервисов:

защита в режиме реального времени

## Основные моменты

* Все облачные и веб-сервисы как на ладони, независимо от площадки, сети или устройства
* Защита действий в SaaS, IaaS и веб-сервисах в режиме реального времени
* Защита данных и пользователей благодаря средствам контроля доступа, информационной безопасности и политикам для борьбы с утечками данных (DLP)

# Используя запатентованный механизм Netskope Cloud XD, решение Netskope Security Cloud может декодировать трафик всех SaaS, IaaS и веб-сервисов и тем самым обеспечивать гранулярный контроль и визуализацию в режиме реального времени. Это позволяет службам безопасности оперативно применять политики к конкретным действиям в облачных и веб-сервисах, вместо того, чтобы сразу блокировать их, мешая работе сотрудников. Благодаря решению Netskope Real-time Protection организации могут применять детализированные политики, а также средства контроля доступа, защиты от утечек и серьезных угроз, сразу же, как только сотрудники обращаются к облачным и веб-сервисам.

## ОБЗОР ПРОДУКТА

Решение Netskope Real-time Protection развертывается в прокси-архитектуре и в режиме реального времени декодирует действия, выполняемые во всех SaaS, IaaS и веб-сервисах, позволяя службам безопасности применять политики и средства контроля для защиты сотрудников. Так, можно запретить выгрузку конфиденциальных данных в несанкционированные облачные сервисы («теневые ИТ»), заблокировать загрузку файлов, зараженных вредоносным ПО, или даже ограничить доступ к тем или иным облачным сервисам в зависимости от статуса устройства (т.е. от того, управляемое оно или нет). Кроме того, через настраиваемые сообщения можно ознакомить сотрудников с корпоративными правилами поведения, касающимися, например, выгрузки конфиденциальной информации только в санкционированный компанией облачный сервис, отправки файлов в карантин, сохранения файлов для судебных нужд и др.

## ГРАНУЛЯРНЫЙ КОНТРОЛЬ И ВИЗУАЛИЗАЦИЯ

Для применения политик безопасности Netskope может использовать подробную информацию по всем облачным и веб-транзакциям, например, данные о площадке, статусе устройства, облачном сервисе или веб-сайте, выполняемом действии и т.д. Можно применять политики типа "Запретить загрузку персональных данных на личные устройства" или развернуть средства для гранулярного контроля доступа в режиме реального времени.

## ЗАЩИТА ДАННЫХ С ПОМОЩЬЮ DLP И ШИФРОВАНИЯ

Netskope в реальном времени проверяет действия на всех санкционированных и несанкционированных облачных сервисах и веб-сайтах: выгрузки, загрузки, совместное использование и т.д. Для защиты конфиденциального контента система задействует более 3000 идентификаторов данных и поддерживает более 1000 типов файлов, а также пользовательские регулярные выражения, цифровые отпечатки, точное сопоставление данных и многое другое. Можно воспользоваться предустановленными профилями, например, «персональные данные» (PII), «конфиденциальные медицинские сведения» (PHI), «данные индустрии платежных карт» (PCI), «ненормативная лексика» и «исходный код», или создать пользовательский профиль. Среди мер защиты доступно сохранение файлов для судебных нужд, помещение в карантин или даже шифрование файла с помощью AES-256. Сделав первый проход в облаке, можно воспользоваться интеграцией с протоколом ICAP, чтобы спустить предполагаемые нарушения на уровень вашей локальной системы DLP. Администраторы могут управлять всем прямо из консоли управления инцидентами Netskope, которая позволяет отслеживать инциденты в течение всего их жизненного цикла: от возникновения до нейтрализации угрозы.

## РАСШИРЕННАЯ ЗАЩИТА ОТ УГРОЗ

Netskope создает эшелонированную оборону для всех облачных и веб-сервисов в режиме реального времени, обнаруживая и нейтрализуя угрозы на самых разных уровнях, включая расширенную проверку на вредоносное ПО, обнаружение аномалий на основе машинного обучения, эвристический анализ и анализ в "песочнице" с динамическим обновлением информации об угрозах сразу из нескольких источников. Известные угрозы устраняются автоматически. Кроме того, настроены процедуры для дальнейшего анализа и устранения последствий новых атак, которые слишком часто обходят существующие системы безопасности. Есть также автоматический сброс скомпрометированных учетных данных, когда сотрудники входят в такие санкционированные облачные сервисы, как Microsoft Office 365 или Google G Suite.

## КОМПЛЕКСНЫЙ ОХВАТ

Netskope Security Cloud охватывает все варианты развертывания облачных сервисов как в реальном времени, так и внеполосно. Для Netskope Real-time Protection служба безопасности может выбрать любой из комплексных вариантов включения в разрыв по модели с обратным и прямым прокси. Netskope обеспечивает полный охват (независимо от сети, устройства или площадки), включая даже клиенты синхронизации, заточенные под облако и мобильные приложения.

Особенности решения Netskope Real-time Protection

|  |  |
| --- | --- |
| **ОСОБЕННОСТИ** | **ПРЕИМУЩЕСТВА** |
| **Контроль и визуализация в режиме реального времени** | * Работайте только с подозрительными действиями, а не блокируйте (или разрешайте) все и сразу * Оцените риск для организации, сопряженный с использованием облачных и веб-сервисов, чтобы выработать грамотную политику информационной безопасности * Стройте эшелонированную защиту, принимая во внимание различные факторы, такие как неуправляемые устройства, местонахождение, небезопасные сети и т.д. |
| **Защита данных** | * Защищайте конфиденциальные данные во всех SaaS, IaaS и веб-сервисах * Используйте шифрование и DLP для соблюдения требований регуляторов * Остановите выгрузку данных в несанкционированные облачные сервисы |
| **Расширенная защита от угроз** | * Получите всестороннюю защиту от угроз для облачных и веб-сервисов * Обнаруживайте аномальные действия и ненадлежащие учетные записи и принимайте меры * Защитите себя от вредоносного ПО и хакерских действий, таких как программы-вымогатели и угрозы нулевого дня |
| **Комплексные варианты развертывания в режиме реального времени** | * Возьмите под контроль все санкционированные и несанкционированные («теневые ИТ») облачные и веб-сервисы * Выбирайте для облачных сервисов включение в разрыв с обратным прокси или любые теоретически возможные варианты с прямым прокси * Выбирайте управление GRE-трафиком или клиента Netskope для веб-трафика |

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.

©2018 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. 06/18 DS-223-1