netskope

Памятка для партнеров

Почему Netskope?

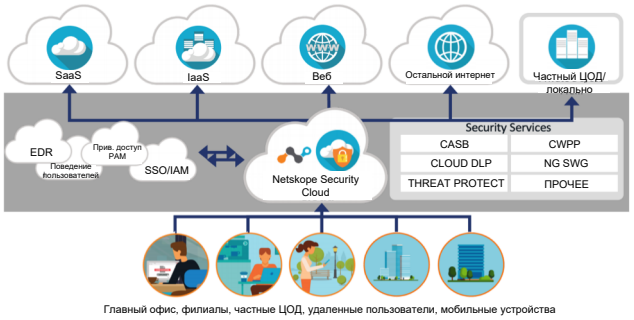
Сегодня большинство людей, устройств, приложений и данных находятся вне корпоративного периметра. А значит, с традиционными технологиями и приемами защиты мы слепы перед львиной долей угроз и рисков утечки данных. Пришло время перемен. Нужно по-новому взглянуть на периметр нашей сети.

SWG+CASB+DLP = Защищенный веб-шлюз нового поколения

Netskope Security Cloud обеспечивает непревзойденную прозрачность, защиту данных и противодействие угрозам в режиме реального времени, когда вы заходите в облачные сервисы, на веб-сайты и в частные приложения из любой точки мира и с любого устройства.

Что такое Netskope Security Cloud?

Решение Netskope Security Cloud позволяет компаниям применять политики безопасности к пользователям и данным, где бы они ни находились, включая управляемые и неуправляемые облачные приложения, публичные облачные среды, веб-сайты и частные корпоративные приложения, размещенные либо в собственных ЦОДах, либо в публичных облаках.



Типичные варианты использования

- Защита облачных приложений
- Обнаружение теневых ИТ
- Архитектура прямого подключения к сети
- Обнаружение облачных и веб-угроз
- Управление и защита публичных облаков
- Предотвращение утечек данных

Уточняющие вопросы

- Предстоит ли вам обновление защищенного веб-шлюза (SWG) Blue Coat / Forcepoint / Zscaler?
- Знаете ли вы, что 85% трафика через веб-шлюзы – это трафик облачных приложений?
- Может ли ваш текущий SWG расшифровывать и проверять SSL-трафик?
- Может ли ваш SWG различать личные и корпоративные экземпляры облачных приложений?
- Ваш текущий SWG размещен в вашем ЦОДе? В таком случае удаленные офисы и пользователей вы подключаете через него?
- Беспокоитесь ли вы об утечках данных через неуправляемые облачные приложения («теневые ИТ»)?
- Нужно ли вам хранить конфиденциальные данные (персональные, медицинские, реквизиты банковских карт) только в санкционированных облачных сервисах?
- Нужно ли вам идентифицировать небезопасные облачные приложения и отслеживать небезопасное поведение пользователей?
- Беспокоит ли вас, что системы ваших пользователей облачных сервисов AWS, Azure или GCP могут быть неправильно сконфигурированы, из-за чего данные оказываются под угрозой?
- Нужно ли вам предотвращать утечки данных из публичных облачных сред?

Продукты Netskope

Защищенный веб-шлюз нового поколения – это веб-шлюз в облаке, который не только фильтрует использование веб-ресурсов, но и понимает природу облачных приложений. Веб-шлюз Netskope NG SWG защищает пользователей в сети, обнаруживая вредоносное ПО, фишинговые веб-сайты и эксплойты типа "drive-by" (со скрытой загрузкой). Netskope также защищает данные организации от утечки или компрометации из-за рискованных действий пользователей в облачных приложениях или выгрузки конфиденциальных данных в теневые ИТ. Веб-шлюз Netskope NG SWG отвечает потребностям крупнейших организаций, предоставляя сервис с низкой задержкой и полной проверкой SSL-трафика.

Лучший на рынке брокер безопасного доступа в облако (CASB) быстро обнаруживает факт использования облачных приложений и защищает данные в управляемых или неуправляемых облачных приложениях. В результате брокер не позволяет нерадивым пользователям выгрузить конфиденциальные данные в теневые ИТ или получить из сети доступ к информации в корпоративном облачном хранилище. Брокер Netskope CASB защищает Office 365, G Suite, Salesforce и многие другие корпоративные приложения.

Cloud DLP — самая передовая в отрасли облачная система для защиты конфиденциальных данных компании от утечки и компрометации. Среди ее возможностей: более 3 000 идентификаторов данных, поддержка более 1 000 типов файлов, пользовательские регулярные выражения, анализ близости, международная поддержка с использованием двухбайтных символов, цифровые отпечатки, оптическое распознавание текста и точное сопоставление данных.

Netskope Private Access обеспечивает безопасный доступ к приложению из любой точки мира. Netskope Private Access предоставляет пользователям безопасный удаленный доступ к приложениям как в публичном облаке, так и в частных ЦОДах. В результате удаленным пользователям не нужно создавать VPN для получения доступа к частным приложениям из корпоративной сети, а компании не нужно устанавливать личность пользователя и подтверждать безопасность устройств, прежде чем разрешить им такой доступ.