КРАТКИЙ ОБЗОР РЕШЕНИЯ

Netskope for Microsoft Office 365

Microsoft Office 365 берут на вооружение организации самого разного размера. Netskope for Office 365 – единственный брокер безопасного доступа в облако (CASB) со статусом Microsoft Gold Cloud Productivity Partner – дает пользователям весь необходимый инструментарий для эффективной работы, обеспечивая контроль и визуализацию для защиты конфиденциальных данных, предотвращения утечек и выполнения требований регуляторов.

ОСНОВНЫЕ ВАРИАНТЫ ИСПОЛЬЗОВАНИЯ

- **Применяйте детализированные политики защиты от утечки данных во всех приложениях Office 365:** предотвращайте загрузку/выгрузку конфиденциальных данных из/во все приложения Office 365.
- **Формируйте средства управления совместным доступом и совместной работой:** ограничьте доступ к конфиденциальным данным или данным под грифом секретности в Office 365 для посторонних лиц.
- **Управляйте загрузкой и синхронизацией данных на неуправляемых устройствах:** применяйте детализированные политики доступа к неуправляемым устройствам посредством контекстно-зависимых пользовательских политик.
- **Проводите расследования, используя подробные журналы аудита:** изучайте полный журнал аудита всех действий пользователей и приложений.
- **Обнаруживайте угрозы со стороны сотрудников и вредоносные программы и принимайте меры:** обнаруживайте инсайдерские угрозы, скомпрометированные учетные записи, облачные угрозы, вредоносное ПО и аномальное поведение пользователей.

ПРОБЛЕМА

Совместная работа и коммуникация – залог высокой производительности в современных организациях. Microsoft Office 365 обеспечивает необходимую среду для облегчения совместной работы и коммуникации и по сути повышает производительность многих организаций, независимо от их размера. Пакет Office 365 создан с нуля прямо в облаке и призван помогать мобильным сотрудникам выполнять свою работу в любом месте и в любое время. Однако эта же гибкость может облегчить задачу хакерам и тем самым свести на нет огромный рост производительности, достигнутый организацией. Хотя в Microsoft Office 365 и есть собственные средства защиты, организациям часто нужен более комплексный подход к безопасности, который бы учитывал использование корпоративных приложений и мобильность сотрудников.

NETSKOPE FOR OFFICE 365

Netskope for Office 365 – надежный инструмент, который помогает ИБ-специалистам понимать и контролировать рискованные действия в приложениях Office 365, защищать конфиденциальные данные и блокировать облачные угрозы. Netskope дает более подробную картину действий и использования на уровне данных как во всех приложениях Office 365, так и в любых других управляемых или неуправляемых облачных приложениях, используемых вашей организацией. Буквально по каждому приложению ИБ-специалисты могут отследить нарушения в работе с корпоративными данными и потенциальные киберугрозы, которые могут нести опасность для вашей организации и помешать ей соответствовать требованиям регуляторов.

ВОЗМОЖНОСТИ

ПОЛНЫЙ ОБЗОР OFFICE 365 И ВСЕХ ПРИЛОЖЕНИЙ

Netskope обеспечивает детальную визуализацию по вашему пакету Office 365 и всем приложениям, используемым в вашей организации. ИБ-специалисты могут как анализировать каждое приложение Office 365 отдельно, так и получать сводное представление об использовании. В таких приложениях Office 365, как Exchange, SharePoint и OneDrive, могут проявляться ранее неизвестные – критичные для безопасности – действия и использование данных, о которых ИБ-специалисты до этого просто не догадывались. Netskope даст вам детальное представление о действиях в Office 365 и распространении конфиденциальных данных внутри вашей организации и за ее пределами. Однако для надежной защиты нужны еще средства гранулярного контроля доступа как для управляемых, так и для неуправляемых облачных приложений. Самая большая проблема для ИБ-специалистов – это неофициальное использование неуправляемых приложений, которые можно в изобилии найти в любой организации. Даже самую надежную защиту Office 365 можно обойти, используя теневые ИТ или пользовательские приложения, которые могут создать шлюз для извлечения конфиденциальных данных.

Netskope даст вам детальное представление о действиях в Office 365 и распространении конфиденциальных данных внутри вашей организации и за ее пределами.

Без ведома ИБ-отдела сотрудник мог совершенно спокойно загрузить конфиденциальные данные из управляемого экземпляра Office 365, а потом их же выгрузить в свой личный экземпляр Office 365. Netskope предоставляет надежную платформу облачной безопасности, которая обнаруживает все приложения – как управляемые, так и неуправляемые. Используя Cloud XD, Netskope четко различает корпоративные и личные экземпляры любых облачных приложений, помогая заблокировать все потенциальные пути утечки конфиденциальных данных за пределы организации.

Благодаря Cloud XD платформа безопасности Netskope обеспечивает глубокий гранулярный контекстно-зависимый контроль в ваших политиках безопасности.

ПОЛИТИКИ ГРАНУЛЯРНОГО КОНТРОЛЯ ДОСТУПА

Сегодняшние сотрудники требуют свободы и хотят активно использовать собственные персональные устройства в рабочем пространстве, обращаясь при этом к конфиденциальным корпоративным ресурсам, размещенным в облаке. Однако легкость доступа может привести к загрузке конфиденциальных данных на персональные устройства и, значит, повысить риск для организации, поскольку сотрудник может потом выгрузить эти же данные в свое личное облачное приложение – и всё это прямо под носом у ИБ-специалистов. Netskope может применять детализированные политики безопасности к приложениям Office 365, устройствам сотрудников и конфиденциальным данным, запрещая движение данных по маршрутам, по которым они не должны двигаться. Благодаря Cloud XD платформа безопасности Netskope обеспечивает глубокий гранулярный контекстно-зависимый контроль в ваших политиках безопасности. Cloud XD в реальном времени выполняет глубокую проверку пакетов в трафике облачных приложений и обнаруживает контекстную информацию, на основании которой ИБ-специалисты могут устанавливать особо жесткие меры безопасности специально для каждого активно используемого облачного приложения – будь то управляемого или нет.

С новыми мощными средствами контроля ИБ-специалисты могут отказаться от грубой и примитивной политики "разрешить/запретить", которая часто не может различить корпоративный и личный экземпляр одного и того же облачного приложения. Так, контроль за облачными приложениями и блокировка нежелательных маршрутов движения данных гарантируют, что пользователи и отделы смогут и дальше использовать облачные приложения, не ставя безопасность организации под угрозу.

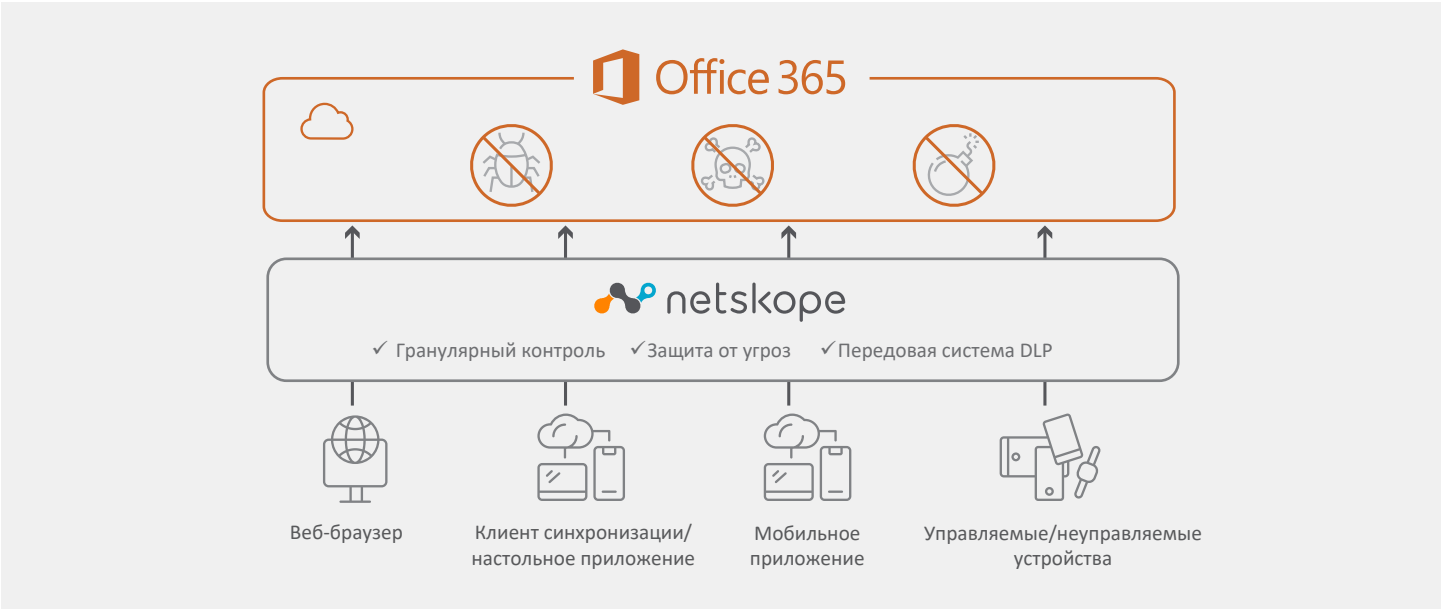

Рис. 1. Netskope for Office 365

РАСШИРЕННАЯ ЗАЩИТА ОТ УТЕЧКИ ДАННЫХ

Данные оказываются под угрозой, поскольку периметр корпоративной сети размывается, а корпоративные приложения и пользователи работают вне зоны действия традиционных линий защиты. Появившееся сразу в облаке, решение Netskope обеспечивает заточенную под облако защиту данных от утечки при их передаче в любое приложение SaaS, IaaS или веб-сервис. Созданное с нуля, оно имеет самые передовые в отрасли возможности DLP, призванные обеспечить высокую точность и низкий уровень ложных срабатываний. Netskope – это свыше 3 000 идентификаторов данных, поддержка более 1 000 типов файлов, пользовательские регулярные выражения, анализ близости, цифровые отпечатки, точное сопоставление данных и оптическое распознавание символов (OCR). Netskope помогает автоматизировать сложную ручную настройку политик, предлагая более 40 готовых шаблонов политик (PCI, HIPAA, GDPR и т.д.), что позволяет заказчикам ускорить внедрение благодаря быстрой адаптации шаблонов под их уникальные требования. Netskope for Office 365 позволяет администраторам ИБ задавать детализированные правила DLP, которые гарантируют, что при совместной работе сотрудники не будут случайно передавать конфиденциальные данные в нарушение корпоративной политики безопасности. Так, Netskope защищает вашу организацию и гарантирует сотрудникам максимальную производительность.

ЗАЩИТА ОТ ОБЛАЧНЫХ УГРОЗ И ВРЕДОНОСНОГО ПО

Поскольку сейчас организации развертывают свои приложения и данные в облаке, киберпреступники также меняют векторы своих атак и пытаются найти слабые места в облачной защите. Традиционные локально развертываемые ИБ-решения часто вообще не анализируют облачный трафик, и это в то время, когда в современных компаниях мобильные пользователи напрямую обращаются к облачным приложениям с оконечных устройств.

Созданное в облаке, решение Netskope защищает Office 365, непосредственно анализируя облачный трафик и выявляя облачные угрозы, которые часто ускользают от традиционных систем безопасности. При поддержке группы Netskope Threat Labs, специализирующейся на обнаружении и анализе новых облачных угроз, Netskope создает эшелонированную оборону для облачных сервисов, включая всесторонний охват всех облачных ресурсов, предотвращение угроз на самых разных уровнях и гибкость при выборе мер защиты. Netskope дает углубленное представление об облачном трафике, на что другие решения просто не способны, и противодействует новым облачным угрозам, которые слишком часто ускользают от существующих систем безопасности.

Netskope собирает данные о событиях из Office 365. Используя передовые алгоритмы машинного обучения, Netskope может отмечать аномальные действия под учетными записями пользователей, которые могут сигнализировать о том, что киберпреступники обошли вашу систему защиты и пытаются украсть данные.

ПРЕИМУЩЕСТВА	ОПИСАНИЕ
ДЕТАЛЬНЫЙ КОНТРОЛЬ И ВИЗУАЛИЗАЦИЯ ДЛЯ OFFICE 365 И ОБЛАЧНЫХ ПРИЛОЖЕНИЙ	УЗНАЙТЕ ОБО ВСЕМ, ЧТО ПРОИСХОДИТ В OFFICE 365 И ВСЕХ ОБЛАЧНЫХ ПРИЛОЖЕНИЯХ: • Обнаруживайте все управляемые и неуправляемые облачные приложения («теневые ИТ») • Предотвращайте утечку данных из корпоративного экземпляра Office 365 из-за использования личных экземпляров Office 365 • Предотвращайте утечку данных из корпоративного экземпляра Office 365 из-за использования неуправляемых облачных приложений • Предотвращайте передачу конфиденциальных данных третьим лицам • Предотвращайте хранение в облаке ценных данных с грифом секретности • Блокируйте загрузку данных из Office 365 на персональные устройства • Обнаруживайте скомпрометированные учетные записи и инсайдерские угрозы / угрозы от привилегированных пользователей • Ведите журнал аудита всех действий для последующих расследований
ПОЛИТИКИ ГРАНУЛЯРНОГО КОНТРОЛЯ ДОСТУПА	ЛЕГКО СОЗДАВАЙТЕ ДЕТАЛИЗИРОВАННЫЕ КОНТЕКСТНО-ЗАВИСИМЫЕ ПОЛИТИКИ ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА: Установите гранулярный контроль доступа к Office 365 по: • типу устройств (управляемые, неуправляемые) • типу действий (загрузка, выгрузка) • конкретному пользователю (Джон Смит) • атрибутам пользователя (роль, департамент) • диапазону IP-адресов (например, сеть, прокси) • географическому местоположению (например, Россия) Применяйте политики гранулярного контроля доступа, такие как: • разрешить/запретить доступ к конкретным приложениям Office 365 • разрешить/запретить пользователям конкретные действия в каждом приложении Office 365 • сделайте обязательной усиленную аутентификацию
РАСШИРЕННАЯ ЗАЩИТА ОТ УТЕЧКИ ДАННЫХ	РАЗРАБОТАЙТЕ ДЕТАЛИЗИРОВАННЫЕ ПОЛИТИКИ DLP С ПОМОЩЬЮ ЛЕГКИХ В ИСПОЛЬЗОВАНИИ ШАБЛОНОВ. • Задавайте ключевые слова и фразы для обнаружения конфиденциальных данных или данных под грифом секретности • Задавайте буквенно-цифровые шаблоны с помощью пользовательских регулярных выражений • Метаданные файла (имя, размер и тип файла) • Цифровой отпечаток неструктурированных файлов • Цифровой отпечаток структурированных файлов с точным или частичным совпадением • Отраслевые словари ключевых слов Варианты действий системы DLP: • Уведомить конечного пользователя • Уведомить администратора • Отправить файл в карантин • Удалить файл
ЗАЩИТА ОТ ОБЛАЧНЫХ УГРОЗ И ВРЕДОНОСНОГО ПО	ПОЛУЧИТЕ ВСЕСТОРОННИЙ ОХВАТ ВСЕХ ОБЛАЧНЫХ УГРОЗ: • Инсайдерские угрозы: обнаруживайте поведенческие аномалии по необычным объемам данных, загружаемых или выгружаемых пользователем, изменениям поведения и частоте входов в облачный сервис • Скомпрометированные учетные записи: анализируйте попытки доступа, выявляя случаи входа в систему из подозрительных мест, атаки методом перебора и вход по нестандартному сценарию • Угрозы от привилегированных пользователей: выявляйте внезапные повышения прав, неактивные учетные записи и доступ к системе в необычное время • Вредоносное ПО: блокируйте известные вредоносные программы, обнаруживайте неизвестные файлы, а также выявляйте команды и управленческие действия, которые могут сигнализировать о краже данных

ЗАПРОСИТЕ ДЕМОНСТРАЦИЮ ОНЛАЙН ИЛИ БЕСПЛАТНЫЙ АУДИТ:

https://www.netskope.com/request-demo

netskope

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. Netskope разбирается в облаках как никто другой и ставит данные во главу угла, помогая ИБ-командам найти правильный баланс между защитой и скоростью, которые нужны им для дальнейшего движения по пути цифровой трансформации. Взгляните на свой периметр по-новому вместе с компанией Netskope.