Почему традиционный VPN не подходит для современных сотрудников

Содержание

Количество сотрудников, работающих удаленно, стремительно увеличивается. Это обусловлено как необходимостью, так и желанием самих сотрудников. Компании могут предоставлять удаленным работникам корпоративные устройства. Кроме того, благодаря развитию и доступности потребительских технологий работники часто используют собственные устройства. В любом случае, когда работникам было необходимо получить доступ к корпоративным системам и файлам, для обеспечения безопасности выбирали VPN. Однако у традиционных сетей VPN есть недостатки. Ими сложно управлять, и они медленно меняются. Они также создают угрозы безопасности на уровне сети, не масштабируются, не обеспечивают высокую комфортность работы пользователей и не гарантируют конфиденциальность.

Для соблюдения требований к безопасности, производительности и масштабируемости для удаленных работников Citrix предоставляет облачное решение, не использующее VPN для доступа к корпоративным веб-, SaaS-, мобильным и виртуальным приложениям с помощью управляемых, неуправляемых и собственных устройств сотрудников (BYOD) в любой сети. Устаревшая модель безопасности традиционных сетей VPN типа «замок и ров» заменена строгими принципами схемы нулевого доверия, которая увязывает доступ с контекстом по запросу.

Сетями VPN сложно управлять

В зависимости от роли удаленных работников и ресурсов, к которым осуществляется доступ, зачастую используются совершенно разные методы доступа. Сотрудник, администратор, партнер и поставщик услуг используют разные точки входа в одной и той же сети VPN. Часто требуется несколько сетей VPN, и для доступа к SaaS-приложениям используется другой портал с единым входом. Это отнимает время у системных администраторов и зачастую требует значительного количества ресурсов для управления. Для добавления резервной мощности необходима модернизация аппаратного обеспечения или длительный процесс получения лицензии.

Сети VPN во многих случаях дают лишь два варианта: полный доступ или отсутствие доступа. При их использовании требуется настройка сложных политик для ограничения доступа неуправляемых конечных устройств к сети, ресурсам и данным.

При замене традиционных устройств VPN полностью управляемым облачным сервисом, доступным во всем мире, необходимость в сложных политиках сетевой безопасности пропадает, так как сервис предоставляет защищенный контекстуальный доступ к приложениям и данным.

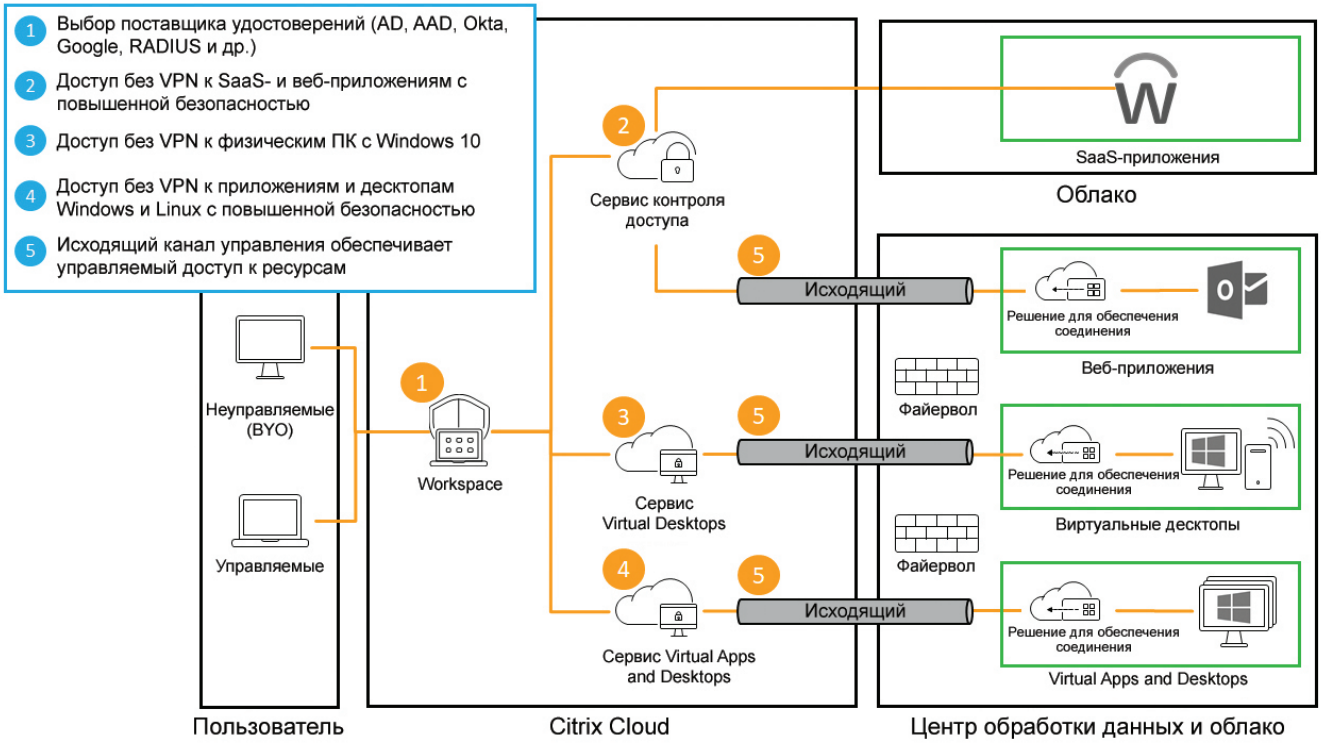
Сети VPN не предназначены для больших объемов данных

Независимо от местонахождения, удаленные работники — как и работодатели — ожидают непрерывного доступа к корпоративной сети. Однако в случае VPN весь пользовательский трафик может идти через корпоративную сеть, увеличивая загруженность и снижая производительность. Кроме того, поскольку VPN обычно развертывают в централизованном хранилище, а пользователи подключаются к внутренним веб-приложениям из разных мест, дополнительные задержки снижают комфортность работы конечных пользователей.

Удаленные работники могут испытывать сложности с доступом к традиционным двухуровневым приложениям, например к тем, которые используются для выставления счетов и управления взаимоотношениями с клиентами. Для этих приложений необходим клиент на устройстве конечного пользователя, а приложения используют нативные протоколы, требующие большой пропускной способности, из-за чего сети VPN и сетевые магистрали быстро перегружаются.

Из-за увеличения загруженности сети и задержек снижается скорость реагирования приложений, что приводит к перебоям, а иногда — к невозможности продолжать работу.

Также необходимо рассмотреть ситуацию с точки зрения работника. Неоптимальное состояние сети на стороне конечного пользователя выводит производительность и комфортность работы пользователей из-под контроля со стороны ИТ-отдела.



Сервис Citrix Access Control, входящий в состав Citrix Workspace, обеспечивает работу без VPN для приложений, доступ к которым можно осуществлять через браузер. К этой категории относятся как веб-приложения, развернутые во внутрикорпоративной сети, например OWA и SharePoint, так и SaaS-приложения, доставляемые из облака, такие как Salesforce и Workday. Таким образом, современные приложения доставляются на любое устройство конечного пользователя при наличии всех средств контекстуального контроля безопасности, и для них не требуется доступ сетевого уровня.

Поскольку решение Citrix Access Control доступно во всем мире, пользователь направляется к ближайшей возможной точке подключения (Point of Presence, POP). Это гарантирует оптимальную производительность и безопасность доступа к SaaS- и веб-приложениям.

Для традиционных двухуровневых приложений, которым требуется большая пропускная способность и производительность которых снижается при доступе из сетей с большими задержками, например при использовании домашнего Wi-Fi, доставка с помощью виртуализированной платформы не только повышает комфортность работы конечных пользователей, но и обеспечивает детальный контроль безопасности на уровне приложения. Решение Citrix Virtual Apps and Desktops, входящее в состав Citrix Workspace, обеспечивает оптимальную безопасность и производительность таких приложений, поскольку оно минимизирует потребность в пропускной способности и динамически регулирует производительность и средства контроля безопасности в таких условиях.

Citrix Virtual Apps and Desktops обеспечивает более высокую комфортность работы удаленных сотрудников по сравнению с нативными приложениями. Приложения, требовательные к ресурсам сети и компьютера, виртуализируются и оптимизируются в центре обработки данных. Клиент приложения также виртуализируется и запускается возле источника данных. Удаленный пользователь использует оптимизированный интернет-протокол, эффективно работающий даже в загруженных сетях.

Системы без VPN не нарушают конфиденциальность сотрудников

Для политик безопасности требуется мониторинг сети. Если в VPN отключено раздельное туннелирование, весь трафик, даже связанный с личными и частными приложениями, пойдет через корпоративную сеть. ИТ-администраторы могут отслеживать не относящийся к работе трафик, что представляет значительную угрозу конфиденциальности для удаленных работников, использующих устройство в свое личное время. Удаленные работники справедливо обеспокоены возможностью перехвата их интернет-соединения, получения доступа к их компьютеру и домашней сети или сбора данных на веб-сайтах, которые они посещают.

С другой стороны, когда доступ заканчивается на уровне приложения, работники чувствуют, что их конфиденциальность обеспечена. Мониторинг конечных пользователей не выполняется, и личный сетевой трафик остается конфиденциальным.

Системы без VPN позволяют применять программы BYOD для повышения продуктивности и удовлетворенности сотрудников

Признавая выгоду использования работниками устройств по своему выбору, многие организации внедрили программы BYOD (использования собственных устройств сотрудников). Однако когда удаленные сотрудники организации подключаются к сети через VPN, установка текущих обновлений безопасности, соблюдение соответствия стандартам и обеспечение совместимости устройств работников может отнимать у ИТ-администраторов много времени. В этой ситуации программа BYOD уже не снижает затраты на конечные устройства и доступ к ним, а создает огромную нагрузку на ИТ-инфраструктуру.

Многие сети VPN не обеспечивают контекстуальные и детальные политики безопасности для программ BYOD и неуправляемых устройств. У удаленных работников должно быть управляемое корпоративное устройство. Помимо программ BYOD, многие компании используют сторонние организации для оказания таких услуг, как расчет заработной платы и пособий и техническая поддержка. Поскольку у устройств независимых сторонних поставщиков услуг имеются собственные настройки, контролировать конечные устройства и обеспечивать их безопасность становится невозможно.

В противоположность этому, Citrix Workspace обеспечивает высокую комфортность работы пользователей практически на любом клиентском устройстве. Если же пользователи не смогут использовать приложение Workspace, комфортность их работы тем не менее останется высокой, включая доступ к веб-, SaaS-приложениям, а также приложениям и десктопам Windows в их веб-браузере.

Удаленным работникам может требоваться доступ к физическим десктопам с личных устройств или устройств BYOD. Citrix Remote PC Access позволяет конечным пользователям входить в систему физического ПК с Windows в офисе удаленно из любого места. А в случае мобильных устройств функция микро-VPN для каждого приложения еще больше уменьшает потребность в VPN для каждого устройства. Комфортность работы пользователей повышается, так как устраняется необходимость в настройке и запуске VPN-клиента, благодаря чему обеспечивается непрерывный доступ к безопасным корпоративным данным.

Сети VPN предоставляют неограниченный доступ к сети

Сети VPN используют устаревшую модель обеспечения безопасности типа «замок и ров», в которой организация должна контролировать всю сеть от начала до конца и полагаться на ее защищенность, включая подключенные к ней устройства. Однако в традиционных сетях VPN механизмы представления данных и контроля для завоевания и проверки доверия недоступны. В сетях VPN используется модель периметра, которая не учитывает

внутренние угрозы и возможность кражи учетных данных, в результате которых злоумышленник получает полный доступ к сети.

Они увеличивают вероятность кибератак на уровне сети, тогда как пользователям нужен только доступ к приложениям. В сети могут присутствовать даже взломанные конечные устройства, что может привести к распространению вредоносного ПО.

Citrix Workspace — это безопасное решение для удаленных работников, не использующее VPN

Citrix предлагает лишенную неудобств среду удаленной работы, которая решает проблемы вашей организации, связанные с безопасностью, управлением и масштабированием. Citrix Workspace объединяет все ресурсы в единый персонализированный пользовательский интерфейс, который можно установить локально на устройстве удаленного работника с помощью приложения Workspace (десктоп и мобильное устройство) или использовать через локальные браузеры для доступа к Workspace посредством Интернета.

Независимо от выбранного подхода и устройства, удаленные работники получают доступ к приложениям, файлам и данным с помощью технологии единого входа, избегая проблем, связанных с моделью типа «замок и ров», используемой в VPN. Безопасность повышается благодаря использованию сервиса Citrix Access Control, который заменяет традиционные устройства VPN полностью управляемым облачным сервисом, доступным во всем мире. Необходимость в сложных политиках сетевой безопасности устраняется благодаря защищенному доступу к приложениям и данным.

Независимо от того, что используют ваши работники — Citrix Virtual Apps and Desktops, веб- или SaaS-приложения, — Citrix Workspace определяет полномочия в зависимости от условной или контекстуальной информации о пользователе и устройстве. Контекстуальные политики безопасности не только позволяют администраторам выполнять идентификацию и аутентификацию пользователей, но и контролировать, какие действия пользователей доступны в определенном приложении, в зависимости от таких параметров, как состояние пользователя и устройства, местоположение и IP-адрес. Workspace также дает организациям возможность устанавливать различный уровень доступа к приложениям и ресурсам. Только доверенным пользователям и устройствам разрешается выполнять определенные функции, например использование буфера обмена, печать и создание локальных копий файлов.

С помощью сервиса Citrix Access Control ИТ-администраторы могут добавить безопасные средства контроля доступа и представление данных в SaaS- и веб-приложениях. Политики защиты приложений защищают от клавиатурных шпионов и ПО для захвата экрана. Нанесение водяных знаков защищает доступ к конфиденциальным приложениям и информации. Вместо того чтобы отказать в доступе удаленному работнику, подключающемуся с недоверенного устройства, ИТ-администраторы могут ограничить функции, к которым он имеет доступ.

Для непрерывного мониторинга и применения политик Citrix Analytics for Security дает администраторам по безопасности возможность постоянной оценки пользовательского риска, в том числе в количественном выражении. После первоначальной проверки учетных данных применяются меры по снижению риска для защиты бизнеса

Заключение

Корпоративные данные могут быть самым ценным активом компании, и организации находят новые способы использовать их. Большинство утечек данных в организациях связаны не со злым умыслом или беспечностью работников, а с неадекватными средствами контроля безопасности, предоставлением лишних привилегий внутренним пользователям и чрезмерной зависимостью от сетевых средств контроля безопасности — «идеальный шторм», который может возникнуть из-за использования традиционного VPN.

Сети VPN являются устаревшими, и им свойственны проблемы, связанные с безопасностью и конфиденциальностью. Поскольку в сетях VPN отсутствуют контекстуальный доступ, постоянный контроль и мониторинг, использование в них модели нулевого доверия невозможно. Их развертывание и управление ими сложны и не обеспечивают высокую комфортность работы пользователей и выбор устройства. У решения Citrix Workspace, включающего Citrix Virtual Apps and Desktops вместе с Citrix Access Control, нет таких ограничений.

Переход ваших работников на Citrix Workspace для обеспечения непрерывности бизнеса осуществляется очень просто. Решение Citrix Virtual Apps and Desktops дает вам возможность быстро осуществлять провижининг сотен рабочих мест с учетом потребностей бизнеса. Провижининг рабочих нагрузок для удовлетворения повышенного спроса может осуществляться на стороне потребителя, в гибридной среде или в любом общедоступном облаке. Организации также могут быстро масштабировать виртуальные приложения и десктопы для временных и удаленных работников.

Каждой организации необходимо знать, что подключение ее удаленных работников настолько же безопасно, как и у работников на стороне потребителя, независимо от их местонахождения и используемого устройства. Citrix Workspace обеспечивает контроль там, где традиционным VPN это не удается. Чтобы узнать больше о функциях и преимуществах Citrix Workspace, свяжитесь со своим представителем по продажам или посетите страницу https://www.citrix.ru/workspace

	Сервис Citrix Access Control, не использующий VPN	Устаревшее устройство VPN
Простота развертывания и настройки	Да	Нет
Простота управления и обслуживания	Да	Нет
Защита базовой сети	Да	Нет
Защита конфиденциальности конечных пользователей	Да	Нет
Использование контекстуального или условного доступа	Да	Нет
Высокая комфортность работы пользователей	Да	Нет
Быстрое масштабирование и провижининг	Да	Нет
Высокая производительность удаленных работников	Да	Нет
Обеспечивает выбор устройства конечного пользователя (BYOD)	Да	Нет
Постоянное обеспечение достоверности и мониторинг	Да	Нет

Отдел продаж
Северная Америка | 800-424-8749
Другие страны | +1 408-790-8000

Офисы
Штаб-квартира | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Кремниевая долина | 4988 Great America Parkway Santa Clara, CA 95054, United States