CITRIX®

Решения нового поколения для доставки цифровых рабочих мест

Содержание

Современные меры безопасности для цифрового рабочего места 3

Трудности ИТ-отделов, связанные с обеспечением безопасности 5

Использование решений для удаленного доступа с целью повышения безопасности
и комфортности работы пользователей 7

Устранение сложности — 4 критерия, которым должна отвечать современная система безопасности 9

Обеспечение баланса между рисками для безопасности и бизнес-приоритетами 10

Современные меры безопасности для цифрового рабочего места

Цифровая трансформация помогает компаниям повысить производительность труда, привлечь потребителей и предоставить своим сотрудникам новые возможности. Она подталкивает к пересмотру способов выполнения работы благодаря созданию цифровых рабочих мест, предназначенных для повышения гибкости и уровня обслуживания и снижения количества времени, необходимого для достижения успеха. Сотрудники, больше не привязанные к рабочим столам и офисам, работают как виртуальные команды, общаясь и сотрудничая в любое время, где угодно, используя необходимые им приложения и устройства.

43 % сотрудников по крайней мере часть времени работают удаленно[1]. В связи с увеличившейся мобильностью сотрудников и переходом на приложения SaaS организации требуют от своих ИТ-отделов обеспечить для сотрудников возможность оставаться на связи практически в любое время и в любом месте. Однако новая инфраструктура приложений для SaaS, BYO и сред, предоставляемых по требованию для работы из любого места, также создает новые трудности в рабочих процессах и риски для безопасности. Во многих случаях ИТ-отделам не хватает сквозной видимости и контроля, и они с трудом обеспечивают оптимальную комфортность работы своим сотрудникам и клиентам.

Назад к содержанию

К 2021 году 25 % корпоративного трафика данных будет обходить периметр безопасности (сегодня этот показатель составляет 10 %) и направляться с мобильных и портативных устройств напрямую в облако[2]

Организации торопятся осуществить масштабирование, в связи с чем ИТ-отделам приходится приобретать комплекс разнообразных продуктов для разных типов приложений и устройств. Кроме того, разные подразделения компаний подписываются на собственные приложения SaaS для совместной работы или выполнения задач. В результате сотрудникам приходится проходить несколько шлюзов или точек доступа, чтобы пользоваться разными типами приложений, из-за чего комфортность работы снижается. Такое отсутствие целостной стратегии приводит к еще большему усложнению ИТ-инфраструктуры и, возможно, перерасходу бюджета. На уже перегруженные ИТ-отделы ложится еще больше обязанностей, поскольку они вынуждены управлять несколькими решениями и реагировать на обращения в службу поддержки, число которых неуклонно возрастает. В итоге применение нескольких решений и связанные с этим сложности задерживают внедрение важных политик контроля доступа.

Но есть более лучший подход.

Решения для предоставления доступа нового поколения от Citrix могут применяться в самых разных сферах за рамками традиционной технологии VPN. Такие решения защищают корпоративные приложения, базовую инфраструктуру и данные в них. Они позволяют применять единообразные и детальные политики безопасности, упростить администрирование для ИТ-отдела и повысить комфортность работы пользователей. Решения для предоставления доступа нового поколения также обеспечивают контроль и видимость во все более сложных гибридных облачных средах.

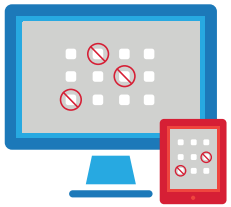
↑ Назад к содержанию

Трудности ИТ-отделов, связанные с обеспечением безопасности

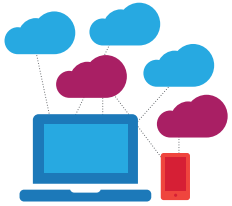
Gartner прогнозирует, что к 2020 году 90 % организаций будут применять бизнес-процессы на базе мобильных устройств[3]. Gartner также полагает, что программное обеспечение как услуга (Software-as-a-Service, SaaS) остается крупнейшим сегментом рынка облачных технологий, а соответствующая прибыль, как ожидается, увеличится на 22,2 % и достигнет 73,6 млрд долларов США в 2018 году[4]. Международная исследовательская фирма ожидает, что к 2021 году затраты на SaaS достигнут 45 % от общей суммы расходов на прикладное программное обеспечение[4]

Хотя применение мобильных и SaaS-приложений предназначено для того, чтобы производительность труда повышалась, а организации опережали конкурентов в плане инноваций, оно также может привести к проблемам для ИТ-отдела, связанным с обеспечением безопасности, включая следующие.

Средства обеспечения безопасности для SaaS-приложений
Традиционные поставщики технологии единого входа (SSO) не предоставляют ИТ-отделам средств контроля за действиями пользователей в приложениях SaaS. В результате пользователи могут делиться в них информацией с кем угодно.



Теневые ИТ-технологии
Сотрудники часто используют приложения или облачные решения по собственной инициативе, не спрашивая разрешения у ИТ-отдела, в нарушение корпоративных политик в отношении безопасности и соответствия стандартам.



Разрастание облака
Организации используют сервисы на основе нескольких облачных инфраструктур, а также многочисленные приложения SaaS, из-за чего среда, которую необходимо защищать, расширяется.

Неправильное пользование паролями
ИТ-отделы регулярно напоминают о важности введения и применения надежных политик в отношении паролей. Однако, согласно результатам опроса, проведенного LogMeIn, 62 % респондентов используют для рабочей учетной записи тот же пароль, что и для личной[5]

Соответствие международным стандартам
Новые сложные требования в отношении безопасности, например требования Общего регламента ЕС по защите данных (GDPR), заставляют ИТ-отделы спешно внедрять соответствующую инфраструктуру обеспечения безопасности. Более половины респондентов в глобальном исследовании, проведенном Citrix и Ponemon Institute, были обеспокоены тем, как их организации будут справляться с рисками, связанными с введением новых международных правил конфиденциальности и безопасности и требований в отношении кибербезопасности[6]

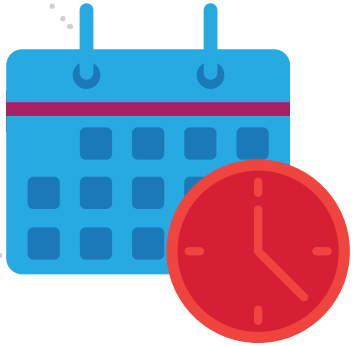
Назад к содержанию

Для защиты расширяющегося сетевого периметра многие ИТ-отделы поддерживают широкий спектр специализированных решений для обеспечения безопасности, в каждом из которых применяются собственные консоли управления и политики. Неудивительно, что 83 % респондентов опроса, проведенного Ponemon, сообщили, что сложность бизнес- и ИТ-операций делает их уязвимыми[7]

Переход к цифровому бизнесу заставляет ИТ-отделы пересмотреть способы обеспечения безопасности инфраструктуры, устройств и данных. Безопасный цифровой периметр дает возможность применить современный, ориентированный на пользователей подход к обеспечению надежности, производительности и безопасности приложений, развертываемых в центре обработки данных, облаке или доставляемых в виде SaaS. Это позволяет ИТ-отделу:

- свести к минимуму и скрыть потенциальные уязвимости;
- получить полную видимость в приложениях SaaS, а также гибридных и многооблачных средах;
- автоматизировать контекстные действия и политики на основе триггеров;
- делиться информацией об угрозах в сервисах для предотвращения вредоносных действий.

7,35 млн долл. США общие организационные убытки от утечек данных в 2017 г. по сравнению с 7,05 млн в 2016 г.[7]



68 % утечек обнаруживается лишь через несколько месяцев или позже[8]

79 % глобальных сетей пострадали как минимум от одной успешной кибератаки[9]

Назад к содержанию

Использование решений для удаленного доступа с целью повышения безопасности и комфортности работы пользователей

Для современных цифровых рабочих мест требуются решения, защищающие их от известных угроз и в то же время прогнозирующие новые и потенциальные угрозы для конфиденциальных бизнес-данных и личной информации, но при этом не снижающие продуктивность и не препятствующие разрешенному доступу. Решения для безопасного удаленного доступа нового поколения помогают ИТ-отделам создавать стратегии обеспечения безопасности, консолидирующие ресурсы, обеспечивающие экономию, повышающие комфортность работы пользователей и гарантирующие эффективность бизнес-стратегий соответствия стандартам. При оценке таких решений необходимо учитывать следующие факторы.

Повышение комфортности работы конечного пользователя
Решение для удаленного доступа нового поколения дает пользователям единую точку доступа и систему единого входа (SSO) в бизнес-приложения, развернутые в центре обработки данных или облаке, а также доставляемые в виде приложений SaaS, на целом ряде устройств, включая ноутбуки, настольные ПК, тонкие клиенты, планшеты и смартфоны. Пользователи должны иметь возможность переключаться между сетями и выходить из корпоративной сети без прерывания VPN-сеансов с SSL-шифрованием и без необходимости запускать VPN вручную.

Назад к содержанию

Политика контроля контекстного доступа

В связи с постоянной угрозой внутренних и внешних атак управление доступом является важнейшей задачей. Поэтому необходима многофакторная аутентификация, которая запрашивает у пользователей дополнительные учетные данные на основе их личности, местоположения и состояния устройства. У ИТ-администратора должна быть возможность создавать, изменять и применять политики безопасного доступа к данным в среде приложения. Эти политики могут применяться для VDI-, веб-, мобильных, корпоративных и SaaS-приложений.

Повышение безопасности и управляемости приложений SaaS

Решения нового поколения дают ИТ-отделам средства мониторинга и управления действиями пользователей после их входа в приложения SaaS. Усовершенствованные политики безопасности позволяют ИТ-отделам контролировать такие действия пользователей, как копирование, вставка и загрузка. Они также могут контролировать способность пользователей делать снимки экрана с данными, размещенными в приложениях SaaS. Это защищает от риска утечки конфиденциальных корпоративных данных — случайной или преднамеренной — и позволяет организации с уверенностью перейти на SaaS- и облачные приложения.

Консолидация сетевой инфраструктуры

Решения нового поколения обеспечивают один URL-адрес и консолидируют инфраструктуру удаленного доступа, помогая ИТ-отделу снизить затраты и облегчить применение политик безопасности и соответствия стандартам. Консолидация также позволяет уменьшить сложность, повысить эффективность и снизить стоимость владения.

Сквозная видимость

Отсутствие видимости в пределах корпоративной инфраструктуры усложняет ИТ-отделам задачу устранения проблем с производительностью, что вызывает раздражение пользователей и снижает их продуктивность. Решения нового поколения обеспечивают полную видимость трафика во всех приложениях, гарантируя безотказную работу приложений и уменьшая время реагирования службы поддержки на запросы.

Защита пользователей

Контроль доступа пользователей к Интернету защищает их от непреднамеренного перехода по ссылкам на вредоносное ПО на веб-сайтах. Он также помогает соблюдать требования в отношении безопасности, например Закон о защите детей в Интернете (CIPA), запрещая пользователям доступ к недопустимому контенту с корпоративных устройств и из корпоративных сетей.

Лишь 48 % организаций имеют политики безопасности, предоставляющие надлежащий доступ только уполномоченным сотрудникам и третьим лицам к конфиденциальной бизнес-информации[10]

Назад к содержанию

Устранение сложности — 4 критерия, которым должна отвечать современная система безопасности

Руководителям ИТ-отделов известно, что традиционная инфраструктура обеспечения безопасности работала должным образом, когда корпоративными конечными устройствами были настольные ПК, а доступ к ресурсам ограничивался корпоративной сетью. Но для современных работников, использующих цифровые технологии, требуется современный подход к безопасности, включающий следующие основные элементы.

1

Видимость и контроль передачи данных из центра обработки данных в облако, позволяющие ИТ-отделам обеспечивать безопасность гибридных сред, которые включают в себя ресурсы на стороне потребителя, общедоступные и частные облачные среды.

2

Интегрированные решения для обеспечения безопасности, позволяющие организациям защищаться от широкого спектра угроз без необходимости создавать и обслуживать пользовательские интерфейсы и соединения.

3

Централизованное управление, позволяющее немногочисленному персоналу развертывать и поддерживать единый набор политик безопасности, независимо от технологий обеспечения безопасности, вычислительных сред и регионов.

4

Комплексная аналитика системы безопасности, позволяющая ИТ-отделам выявлять сложные, скрытые и многовекторные угрозы безопасности.

Сочетание этих факторов не только упрощает управление и сокращает расходы, но также значительно повышает способность организации с уверенностью развертывать и модифицировать приложения.

Назад к содержанию

Обеспечение баланса между рисками для безопасности и бизнес-приоритетами

Подход Citrix к защите цифровых рабочих мест дает вам возможность уменьшить риски для безопасности, в то же время обеспечивая такие способы работы, которые стимулируют инновации и рост. Решения Citrix включают контекстный безопасный удаленный доступ, обеспечивая централизованное управление и распределенное применение политик в каждой контрольной точке. Ваши сотрудники смогут безопасно подключаться, совместно работать и обмениваться информацией из любого места с помощью любого устройства по своему выбору.

Назад к содержанию

Устраните основные проблемы безопасности с помощью решений Citrix

Контекстный и безопасный доступ
Предоставьте сотрудникам и третьим лицам безопасный контекстный доступ к бизнес-приложениям и данным независимо от устройства и местоположения.

Обеспечение безопасности мобильных приложений и устройств
Управляйте безопасностью мобильных устройств и приложений, предотвращая угрозы и атаки со стороны вредоносного ПО без ущерба для продуктивности.

Безопасная совместная работа и защита интеллектуальной собственности
Защищайте информацию от потери и хищения, предотвращайте несанкционированный доступ и кражу интеллектуальной собственности.

Администрирование, риски и соответствие стандартам
Управляйте рисками, соблюдайте международные стандарты и отраслевые нормы.

Непрерывность бизнеса и безопасность приложений
Обеспечьте непрерывность работы, а также доступность приложений и систем во время перебоев в работе организации и кибератак.

Благодаря Citrix вы сможете защитить приложения, контент и сети, а также проактивно устранять угрозы безопасности в SaaS-, гибридных и многооблачных средах. У вас будет возможность учитывать бизнес-приоритеты и потребности пользователей, внедряя инновации и в то же время обеспечивая безопасность своих данных, приложений и сети.

Назад к содержанию

CITRIX®

Для получения более подробной информации посетите веб-сайт citrix.ru/secure.

Назад к содержанию