Рабочее место будущего: подготовка

Руководство по объединению, упрощению и обеспечению безопасности облачных сервисов

Содержание

Адаптация к рабочим процессам будущего

Рабочие места будущего для сотрудников больше не будут привязаны к столам, офисам и даже устройствам. Вместо этого будут использоваться все облачные и физические ресурсы, необходимые сотрудникам для выполнения работы, причем более безопасным и контекстуальным образом, чем в наши дни.

Раньше вы начинали день с включения физического устройства, предназначенного только для вас. Ваши данные, приложения и учетные данные для входа находились в одном месте. Теперь работа перемещается с устройства в облако. Действительно, сегодня многие часто используемые приложения (и даже инструменты для повышения производительности) являются облачными приложениями в виде программного обеспечения как услуги (SaaS). Однако в связи с тем, что с помощью приложений SaaS можно быстро удовлетворять эти новые потребности, сотрудникам приходится запоминать многочисленные учетные данные для входа, использовать различные источники данных, а также учитывать различные риски безопасности, число которых угрожающе быстро растет. В результате корпоративные ИТ-отделы еще больше обеспокоены уменьшением контроля, понимания и возможности управления приложениями SaaS, которые используют сотрудники, состоянием конфиденциальных данных в этих приложениях, а также способом интеграции этих приложений SaaS в ИТ-инфраструктуру компании.

Чем больше облачных сервисов используется сотрудниками, тем больше ИТ-отделу необходима **платформа безопасного цифрового рабочего места**. Благодаря ей ИТ-администраторы смогут управлять вопросами обеспечения безопасности и предоставлением пользователям приложений SaaS, веб-приложений и даже локальных приложений, а сотрудники будут начинать день по-новому, осуществляя индивидуальный безопасный доступ к этим приложениям.

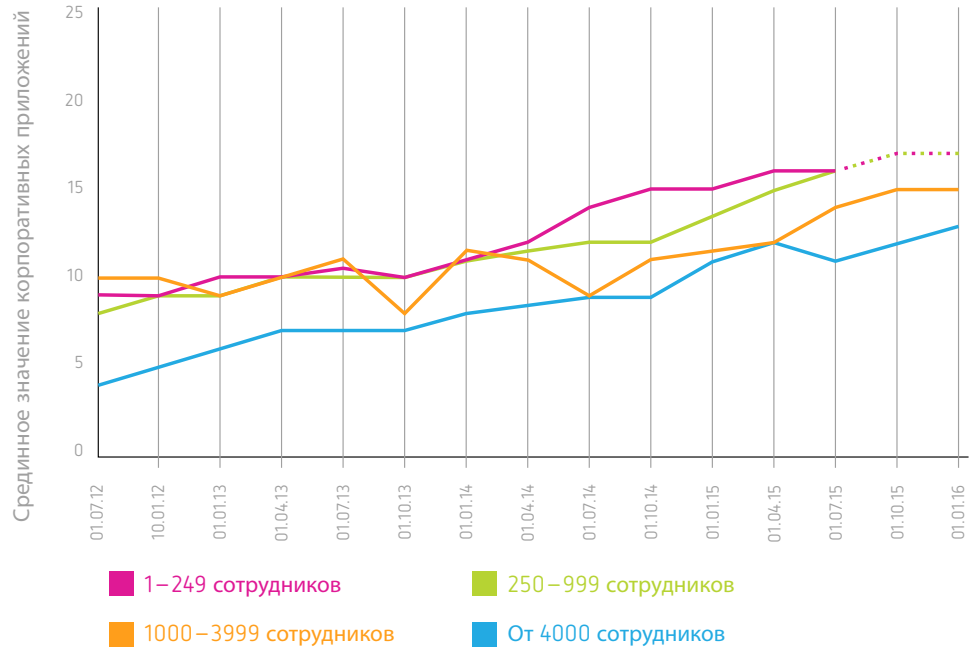
Эволюция рабочего места

Чтобы реально понимать те проблемы, с которыми организации сталкиваются при внедрении новой рабочей среды, нам необходимо разобраться, как создалась такая ситуация.

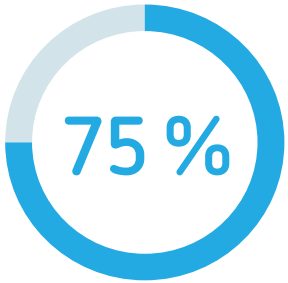
Традиционно сотрудник начинал рабочий день за своим столом, перед стационарным компьютером. Вход в систему давал ему доступ ко всему необходимому для выполнения работы: программам, корпоративному серверу, важным документам и т. д. Безопасность сети зачастую ограничивалась территорией организации и собственной сетью, а ИТ-отдел мог с легкостью управлять ею.

Однако по мере расширения интернет-услуг распространенность браузерных приложений SaaS резко возросла. Организации убедились в способности поставщиков предоставлять лучшие в своем роде безопасные решения, которые одной компании необходимы для расчета заработной платы, другой для управления проектами, а третьей для продаж. Чем больше организации применяют эту стратегию, тем больше увеличивается число разнородных поставщиков облачных сервисов.

Срединное значение готовых облачных приложений в зависимости от размера компании с течением времени[1]



С расширением использования облачных сервисов сотрудники все чаще получают доступ к необходимым для работы ресурсам не с помощью десктопов, а через интернет-браузер.

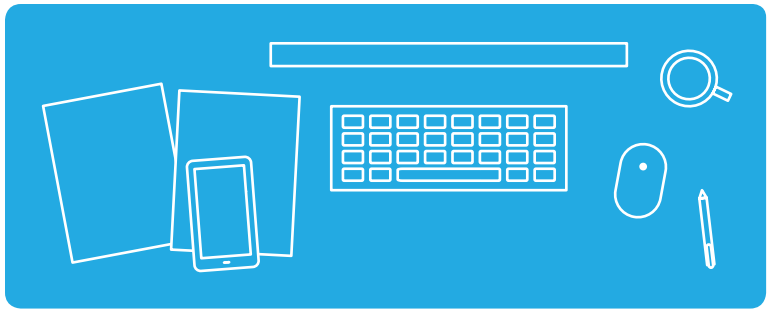


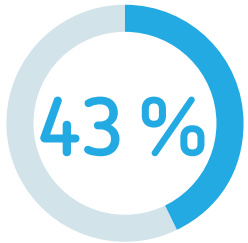
корпоративных рабочих нагрузок в настоящее время находятся в облаке.[2]

Благодаря приложениям SaaS возникла современная культура работы в любом месте, дающая сотрудникам возможность осуществлять доступ к своему рабочему месту практически с любого устройства. Из-за того, что сотрудники меньше привязаны к физическому месту, они могут:

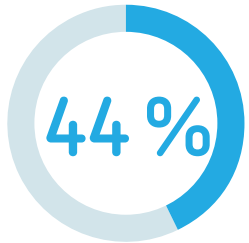
- продуктивно работать в любом месте, где есть интернет-соединение;
- использовать свои устройства, будь то стационарный компьютер, ноутбук, планшет или смартфон;
- использовать необходимые документы на важных встречах независимо от места хранения документов.

Рост потребности в мобильном доступе на рабочем месте[3]





опрошенных специалистов считают использование мобильных устройств необходимым для своей работы.



проверяют или используют мобильное устройство для работы более 20 раз в сутки.

Однако новые способы, с помощью которых сотрудники осуществляют доступ к рабочему месту, также создают множество проблем пользователям, руководителям и ИТ-отделам.

Проблемы современного рабочего места

Хотя такой способ работы и приносит пользу, у него также имеется ряд нежелательных последствий. В связи с таким большим количеством санкционированных (и несанкционированных) приложений SaaS неизбежно повышение сложности сети и рисков безопасности.

Множество учетных данных для входа, фрагментированный доступ

Сотрудники не могут просто начать новый день. Большое число приложений влечет за собой множество учетных данных для входа, нарушение рабочих процессов и снижение продуктивности. В связи с большим количеством различных имен пользователей и паролей сотрудники пренебрегают грамотным использованием паролей, например используют одинаковые учетные данные для нескольких учетных записей или записывают их. А наличие множества учетных данных для входа означает, что ИТ-отдел не может просто создать или убрать глобальный доступ.

Неконтекстуальный доступ

Отсутствие контроля за приложениями не дает ИТ-отделу возможности ограничивать или открывать доступ к конфиденциальным данным в небезопасных устройствах, местах или сетях.

Отсутствие интегрированных рабочих процессов

Так как сотрудники выполняют несколько процессов в разных приложениях, рабочие процессы становятся фрагментированными и зачастую дублируются. Например, финансовый отдел использует одно приложение для учета расходов, а другое для учета выплаты компенсаций, однако процесс синхронизации этих приложений отсутствует.

Непоследовательное обеспечение безопасности

Отдельные приложения SaaS часто имеют собственные политики безопасности и соответствия стандартам, управления данными и доступом. В результате возникает несколько периметров и типов обеспечения безопасности, полностью контролировать которые ИТ-отделу сложно, а порой и невозможно.

Проблемы современного рабочего места (продолжение)

Разные пользовательские интерфейсы
Облачные приложения часто оптимизированы для разных браузеров, устройств или операционных систем и имеют разные пользовательские интерфейсы. А из-за практического отсутствия контроля ИТ-отдел не может решить многие проблемы. Ввиду этого число устройств, которые сотрудники могут использовать для уникальных или специальных приложений, зачастую ограничено.

Отсутствие управления основными данными
Из-за большого числа облачных приложений у ИТ-отдела нет возможности знать и проверять, где хранятся данные и как ими управляют.

Отсутствие комплексного понимания и аналитики
Отключенная (или отсутствующая) аналитика отдельных приложений не дает ИТ-администраторам полного представления об использовании приложений, соответствии стандартам и состоянии безопасности. ИТ-отдел лишается возможности сбора применимых на практике данных для управления или контроля пользовательской среды.

Нарушение управления для ИТ-отдела
Не имея единого места для конфигурирования и мониторинга приложений SaaS, ИТ-отдел не может надлежащим образом управлять данными в организации, что лишает его возможности улучшить или автоматизировать процесс в приложениях.

Одним из решений проблемы сложности и рисков для ИТ-руководства является запрет на использование приложений SaaS. Однако такой предсказуемый ответ со стороны ИТ-отдела создаст противоречие с теми сферами деятельности организации, где эти приложения необходимы, что вынудит пользователей «уйти в тень», а у ИТ-администраторов будет еще меньше контроля за используемыми приложениями SaaS.

Примеры: Проблема с...

использованием несанкционированных приложений
Сотрудники используют популярное приложение для обмена мгновенными сообщениями. Несмотря на то, что приложение санкционировано ИТ-отделом, технология единого входа и контроля управления отсутствует. Из-за этого в системе безопасности возникают лазейки, (a) когда сотрудники добавляют к приложению «плагины» и (b) когда сотрудники уходят из компании, забирая с собой свои учетные записи (и все размещенные конфиденциальные данные).

отсутствием контекстуального доступа
Сотрудники используют популярное приложение, предоставляемое ИТ-отделом. Однако устройство одного из сотрудников взломано хакером. Из-за отсутствия контекстуальной безопасности система не замечает, что доступ с одного устройства сотрудника связан с безопасной сетью на стороне потребителя, в то время как другое устройство одновременно осуществляет доступ к приложению из внешней сети, расположенной в нескольких тысячах километров.

Снижение продуктивности, отсутствие контроля и риски безопасности в конечном итоге сказываются на финансовых показателях вашей компании. Однако есть способ упростить администрирование, в то же время используя лучшие в своем роде приложения SaaS, необходимые вашей организации.

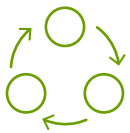
Решение:

безопасное цифровое рабочее место

Из-за того, что эти трудности кажутся непреодолимыми, ИТ-руководство может начать вводить запреты. Вместо того, чтобы блокировать пользователей, приложения и сети, существует альтернативный подход — полностью перейти в облакоцентричный и SaaS-центричный мир. Безопасное цифровое рабочее место позволяет решать эти проблемы, используя при этом все преимущества внешних облачных приложений и приложений SaaS.

Технология единого входа

Технология единого входа дает пользователям возможность однократного входа в систему с получением доступа ко всем своим облачным приложениям. Она также позволяет ИТ-отделу предоставлять сотрудникам глобальный доступ при приеме на работу и аннулировать его при увольнении.



Интегрированный рабочий процесс

Обеспечивает логичную интеграцию между приложениями, а также рабочую среду приложений с сохранением данных о поступающих запросах.

Стабильная комфортность работы пользователей

Гарантирует стабильную комфортность работы независимо от того, какое приложение сочетается с каким устройством, почти такую же производительность, как при работе на «родном» устройстве, а также автоматическую адаптацию функционала приложения к особенностям устройства.

Контекстуальный контроль безопасности

При адаптационном подходе к созданию «программно определяемого периметра» безопасность и права применяются контекстуально на основе устройств, сетей, мест и поведения пользователей.

Контекстуальный доступ

Благодаря более детальному пониманию устройств, сетей, потребностей приложений и политики обеспечения безопасности, ИТ-отдел может предоставить пользователям полный или частичный доступ к разрешенным устройствам и местам. В результате ИТ-отдел будет уверен в безопасности доступа, а пользователи смогут пользоваться наиболее оптимальным и эффективным способом доступа к рабочему месту.

Централизованная аналитика

ИТ-отделам не придется пользоваться несколькими приложениями для сбора аналитики и пытаться сравнивать их по разным показателям. Вместо этого они могут использовать единую информацию по приложениям для сбора применимых на практике данных об организации.

Управление в руках ИТ-отдела

Благодаря единой панели управления для всех облачных приложений ИТ-отделы могут легко управлять данными по всей организации.

В будущем новое безопасное цифровое рабочее место будет играть ключевую роль, позволяя организациям максимально использовать преимущества облачных систем и не допуская излишней сложности и небезопасности сети, возникающей из-за их широкого бесконтрольного применения.

«Современные сотрудники стремятся делать такой же выбор, какой они делают в качестве потребителей.
[...] Руководители ИТ-отделов могут дать им возможность выбора, используя цифровое рабочее место: бизнес-стратегию, способствующую гибкости и вовлеченности сотрудников посредством более ориентированной на потребителя рабочей среды».
— Gartner [4]

Начните переход в облако там, где вам удобно

Подход компании Citrix к безопасному цифровому рабочему месту дает организациям и их сотрудникам возможность надежного доступа к приложениям и данным, а также стабильную комфортность работы на всех своих устройствах. Он также дает ИТ-отделу единую панель управления для конфигурирования, мониторинга и управления. Это позволяет снизить сложность и риски, поэтому ИТ-администраторы и организации могут безопасно использовать все преимущества облачных сервисов.

Основные преимущества

Адаптивная работа

Унифицированная облачная платформа предоставляет корпоративному пользователю рабочее место, оптимизирующее продуктивность и повышающее производительность как работников интеллектуального труда, так и работников одной операции. Помимо доставки на корпоративные десктопы, ноутбуки и мобильные устройства приложений для повышения продуктивности, такая платформа повышает комфортность работы пользователей благодаря тесно интегрированным приложениям и гарантирует безопасную работу с документами и Интернетом вещей.

Сбор, анализ и применение интеллектуального контекста с помощью аналитики поведения и безопасности

Благодаря контекстуальной доставке приложений и данных в зависимости от поведения пользователей и организаций, конечного устройства и сетевого окружения, а также постоянному профилактическому контролю данных в процессе их передачи, хранения и использования, платформа гарантирует оптимальную работу приложений и снижает риски угроз для инфраструктуры, данных и приложений.

Унификация гибридной доставки облачных сервисов

Платформа обеспечивает безопасный доступ к данным и приложениям независимо от того, предоставляется она как ИТ-услуга из корпоративного центра обработки данных, из одной или нескольких облачных систем, поставщиками SaaS или в виде сочетания локальных и общедоступных облачных сервисов. Она обеспечивает безопасность любого конечного устройства, будь то корпоративное устройство или неконтролируемое личное устройство сотрудника.

Унификация облачных сервисов с помощью Citrix

Так как мобильность продолжает изменять способы работы, компаниям приходится решать связанные с этим сложности и справляться с рисками. Безопасная унификация облачных сервисов позволит вашим сотрудникам работать в любом месте и обеспечит ИТ-отделу дополнительные возможности контроля и управления, а также душевное спокойствие.

Сотрудничество компаний Citrix и Intel по-прежнему гарантирует, что ваше облачное решение оптимизировано для доставки мощных и эффективных облачных решений, обеспечивающих более качественную виртуализацию, безопасность и аналитику.Независимо от того, где и какие облачные системы вы используете — на стороне потребителя, гибридное или общедоступное облако, — компании Citrix и Intel объединяют свои усилия, чтобы помочь вам. Центры обработки данных ведущих поставщиков облачных сервисов используют архитектуру Intel®.

Обеспечьте переход своего предприятия к рабочим местам будущего уже сегодня. **Посетите страницу** citrix.ru/cloud.

Источники:

1. Business @ Work, 2016 г., Okta
2. «Отчет о ситуации в облачных системах», 2017 г., RightScale
3. «Выпуск: отчет о мобильной продуктивности за 2016 г.», 2016 г., Wrike
4. «Gartner: прогноз на 2017 г. Улучшение результатов деятельности благодаря персональному выбору на цифровом рабочем месте», 14 ноября 2016 г., Пол Миллер, Никос Дракос, Кэрол Розвелл, Мэтью У. Кейн, Джеффри Мэнн, Джим Мерфи, Майк Готта, Адам Присет, Гэвин Тей