

# Три признака того, что пора переходить на цифровое рабочее место

Как подход, выходящий за рамки только десктопов, позволит повысить продуктивность пользователей, предоставить дополнительные возможности ИТ-отделу и обеспечить безопасность данных

---

Еще совсем недавно для быстрого введения сотрудников в курс дела было достаточно корпоративного или виртуального десктопа. Со временем ситуация изменилась. Три намечающиеся тенденции показывают, что, если вы хотите соответствовать растущим потребностям своей организации в отношении производительности, вам пора переходить на безопасное цифровое рабочее место.

- 1. Растущее число мобильных сотрудников**
- 2. Модернизация приложений**
- 3. Исчезающий периметр безопасности**

---

Узнайте, как подход, выходящий за рамки только десктопов, позволит повысить продуктивность, предоставить вашему ИТ-отделу возможность проявлять больше гибкости и надежнее защитить данные вашей компании.



Знаете ли вы?



Более 1/3

сотрудников сменили бы работу, чтобы иметь более гибкий график<sup>1</sup>.



Всего 57%

сотрудников постоянно работают в том же месте, что и их коллеги<sup>1</sup>.

### 1. Растущее число мобильных сотрудников

Сотрудники хотят выбирать, где и как работать. В действительности, согласно результатам исследования Gallup, 37% сотрудников сменили бы работу, чтобы иметь возможность хотя бы часть времени работать там, где им удобно. Исследование также показало, что всего 57% сотрудников в течение 100% времени работают в том же месте, что и их коллеги<sup>1</sup>. Сегодня компании признают потенциал удаленной работы в плане повышения продуктивности, гибкости и комфортности работы сотрудников независимо от их местонахождения, будь то дом, объект клиента, отель или кафе. Это подталкивает ИТ-отделы развиваться соответствующим образом. Несмотря на то что доставлять виртуальные приложения мобильным сотрудникам возможно, существуют другие факторы, затрудняющие виртуализацию, в частности современные приложения.

### 2. Модернизация приложений

Приложения все чаще разрабатываются для работы на любой платформе. Microsoft Office — хороший пример современных приложений, так как составляющие этого пакета могут работать на нескольких разных платформах, включая Windows 10, iOS, Android и Macintosh. Кроме того, Microsoft Office можно доставлять в виде нативных приложений или даже сервиса SaaS. К тому же современные приложения создают новые проблемы. Как обеспечить безопасность современных приложений и управление ими? Например, такой традиционный инструмент управления клиентами, как SCCM, дает возможность осуществлять доставку и управление

устаревшими приложениями для десктопов Windows на ноутбуке с Windows 7, но не позволяет управлять современными приложениями Windows 10 на смартфоне BYOD и отделять личные данные сотрудника от корпоративных данных. В результате традиционные инструменты управления клиентами приходится дополнять решениями для управления мобильностью предприятия. Такое сочетание управления клиентами и управления мобильностью предприятия называется унифицированным управлением конечными устройствами (UEM).

### 3. Исчезающий периметр цифровой безопасности

Чем мобильнее сотрудники, тем сложнее удерживать корпоративные данные в центрах обработки данных. Вашим пользователям необходим доступ к их файлам независимо от того, находятся ли эти файлы на серверах за файрволом, на сервере надежного провайдера или на десктопе пользователя в офисе. Некоторые ваши пользователи, возможно, стали использовать нативные клиенты мобильной электронной почты вместо виртуальной почты, сохраняя файловые вложения из сообщений электронной почты на своем личном смартфоне в незашифрованном виде. При этом такой сотрудник, возможно, пользуется подключением через VPN, которое хакер может использовать для получения доступа к вашим ресурсам за файрволом, взломав загруженное сотрудником мобильное приложение.

## Выйдите за рамки виртуализации и внедрите цифровое рабочее место с помощью Citrix

Полное и интегрированное цифровое рабочее место предоставит пользователям безопасный доступ к их приложениям, десктопам и данным откуда угодно. Citrix Workspace сочетает технологию виртуализации Citrix с другими возможностями, включая унифицированное управление конечными устройствами (UEM), синхронизацию и обмен корпоративными файлами (EFSS), шлюз безопасного доступа к сети и аналитику для обеспечения безопасности и мониторинга эффективности работы приложений.

### Унифицированное управление конечными устройствами (UEM)

Решение UEM компании Citrix упрощает для ИТ-организаций управление растущим числом мобильных сотрудников. Это решение обеспечивает централизованное управление целым рядом различных платформ и устройств, в том числе десктопами, ноутбуками, смартфонами, планшетами, устройствами Интернета вещей и другими тонкими клиентами, например устройствами Google Chromebook. Кроме того, Citrix позволяет вам управлять не просто мобильными, а современными приложениями. Решение UEM компании Citrix также предоставляет уникальные возможности, дополняющие Microsoft EMS/Intune, в том числе микро-VPN для O365. Вы сможете хранить данные на мобильных устройствах в зашифрованном виде, что уменьшит проблему исчезающего периметра цифровой безопасности.

#### Основные возможности решения UEM компании Citrix:

- управление мобильными устройствами (MDM) на популярных платформах (включая Windows 10, iOS, Android, MacOS и Интернет вещей);
- гибкое управление мобильными приложениями (MAM) с поддержкой платформенного MAM (например, управляемое приложение iOS, а также Samsung KNOX, AppConfig Community, Windows Information Protection); Citrix MAM с технологией MDX, обеспечивающее второй уровень шифрования на уровне приложений без регистрации устройства; и поддержка Intune MAM для защиты O365;
- безопасные приложения корпоративного класса для повышения продуктивности, в том числе Secure Mail и Secure Web;
- управление мобильным контентом (MCM), включая технологию Citrix для

синхронизации и обмена файлами, которое интегрируется с Secure Mail, благодаря чему ваши сотрудники получают доступ к рабочим файлам где угодно одним нажатием на ссылку в электронном сообщении, причем пользователям не нужно отправлять вложения по электронной почте;

- управление идентификацией (IDM) с поддержкой двухфакторной аутентификации и технологии единого входа (SSO) для любого приложения (мобильного, виртуального, SaaS-, веб-), доставляемого через настраиваемый магазин приложений;
- безопасность доступа через сетевой шлюз благодаря уникальному подключению микро-VPN для конкретных приложений, что снижает риск несанкционированного доступа к вашей сети.

### Синхронизация и обмен корпоративными файлами (EFSS)

Несмотря на то что виртуализация приложений и десктопов не позволяет пользователям осуществлять доступ к файлам из виртуальных приложений, как было отмечено ранее, все больше пользователей переходят на современные приложения, поэтому им необходимо комплексное и безопасное решение для доступа к файлам независимо от типа приложения и места его хранения. Решение EFSS компании Citrix дополняет виртуализацию приложений и десктопов в рамках полноценного цифрового рабочего места.

#### Решение EFSS компании Citrix обеспечивает:

- доступ к данным из любого места и с любого устройства с помощью инструментов и приложений для синхронизации данных;
- безопасный доступ к данным внутри сети, включая SharePoint и сетевые диски;
- бесперебойность и комфортность работы пользователя в Microsoft Outlook® Plug-In, интеграцию в Windows Explorer и Mac Finder; поддержку больших файлов — до 100 ГБ; встроенный редактор мобильного контента;
- контроль местонахождения данных посредством StorageZones и StorageZone Connectors для SharePoint и сетевых дисков, что предоставляет ИТ-отделу гибкость и средства управления для выбора места хранения данных, которое соответствовало бы стандартам и требованиям регулирующих органов, ИТ-стратегии и инфраструктуре;

- централизованное управление и безопасность, включая мощные функции отчетности и уведомления, а также интеграцию DLP;
- нативные политики безопасности устройств для усиления безопасности на конечных устройствах;
- синхронизацию виртуальных десктопов по требованию.

### Citrix Unified Gateway

Ввиду растущего числа типов используемых устройств и приложений удаленный доступ легко может стать большой проблемой для ИТ-отдела из-за огромного количества специализированных продуктов для различных устройств, моделей принадлежности данных, сетей и приложений. ИТ-отделу необходимо консолидировать и упростить инфраструктуру удаленного доступа, в то же время предоставив пользователям простой способ доступа к их приложениям с любого устройства.

Citrix Unified Gateway обеспечивает удаленный доступ к виртуальным средам с устройства любого типа, удаленный доступ к корпоративным, веб- и SaaS-приложениям на базе виртуальной частной сети с SSL-шифрованием, а также интеграцию с решением Citrix для унифицированного управления конечными устройствами (UEM) с целью безопасного доступа к мобильным устройствам.

#### Кроме того, Citrix Unified Gateway обеспечивает:

- единый URL-адрес для доступа к любому приложению на устройстве любого типа с предоставлением унифицированного и безопасного доступа;
- возможности микро-VPN благодаря решению UEM компании Citrix для безопасного доступа к мобильным устройствам;
- бесперебойную высокоэффективную работу с приложениями в любой сети;
- технологию единого входа (SSO) в виртуальные, мобильные, веб- и SaaS-приложения;
- многофакторную аутентификацию, сквозной мониторинг трафика всех приложений и контекстуальный контроль доступа.

### Citrix Analytics

Используя широкий набор алгоритмов машинного обучения, решение Citrix Analytics обеспечивает контекстуальную безопасность: оно осуществляет корреляцию и анализ данных разных продуктов для выявления и изоляции рискованных действий пользователей — как собственных сотрудников, так и хакеров, организуемых внешние атаки.

Такие рискованные действия пользователя, собранные воедино, создают обобщенный профиль риска пользователя. После выявления рискованных действий пользователя Citrix Analytics использует различные средства детального управления политиками для уменьшения или полного устранения угрозы: например, многофакторную аутентификацию, запись пользовательских сеансов, установление более строгих требований в отношении доступа к данным, блокирование подозрительных приложений и даже карантин пользователей.

#### Citrix Analytics обеспечивает:

- анализ безопасности на основе поведения пользователей, в котором сочетаются анализ безопасности доступа, анализ безопасности приложений и анализ безопасности данных;
- анализ производительности и операций для отслеживания использования, мониторинга производительности и выявления проблем и их первопричины;
- работу в замкнутом цикле в режиме реального времени путем изменения политик продуктов для уменьшения угроз;
- работу на стороне потребителя, в общедоступном облаке или гибридных средах.

---

## С чего начать

Многие клиенты Citrix совершают переход на цифровые рабочие места путем поэтапного внедрения, ориентируясь на собственных пользователей и примеры использования для своих мобильных сотрудников. Вам также нужно будет определить ключевые сценарии и рабочие процессы. Рассматривайте их с точки зрения пользователей и сотрудников, учитывая их потребности, предпочтения и стиль работы с различными типами устройств, приложений и сетей. Ваша оценка также должна включать корпоративные требования в отношении безопасности и соответствия стандартам. Многие из этих примеров использования могут быть привязаны к таким текущим проектам, как переход на Windows 10 или внедрение O365.

После этого создайте концепцию решения, обозначив в ней предлагаемые рабочие процессы и уровень комфортности работы пользователей. Сначала сосредоточьтесь на легкодостижимой цели, способной быстро принести выгоду, например на внедрении решения UEM компании Citrix для управления устройствами Windows 10 и современными приложениями наряду с управлением другими устройствами и приложениями. Или используйте решение EFSS компании Citrix для поддержки обмена важными файлами с целью уменьшения потери данных.

Проводите проверку вашей концепции решения с участием представителей всех бизнес-подразделений, чтобы гарантировать соответствие всем требованиям. Внедряйте решение на стороне потребителя, в облаке или гибридной среде поэтапно, ориентируясь на своих пользователей и выявленные примеры использования.

## Заключение

Распространение различных стилей мобильной работы и современных приложений, а также исчезающий цифровой периметр создают проблемы, которые невозможно решить с помощью виртуализации или фрагментарного арсенала технологий с привлечением нескольких поставщиков. Только комплексное и унифицированное решение для доставки рабочих мест позволит сотрудникам достичь максимальной продуктивности на любом устройстве с использованием любого приложения, обеспечив комфортность, нужную сотрудникам, и безопасность работы, требуемую ИТ-отделом.

Рабочее место с полной поддержкой мобильности дает ИТ-администраторам возможность оптимизировать и упрощать работу. Работа с единым поставщиком полностью цифровых рабочих мест экономит время, уменьшает потребность в обучении персонала, упрощает предоставление технической поддержки, сокращает общие затраты и предлагает пользователям более комфортные условия работы. Для увеличения вовлеченности и продуктивности сотрудников необходимо предоставить им контекстно-зависимые, надежные и достаточно «умные» цифровые рабочие места, обеспечивающие надлежащий доступ, получение информации и производительность для выполнения работы.

С помощью Citrix Workspace организации могут решить проблемы управления и безопасности, предоставить пользователям богатый набор мобильных приложений корпоративного класса для повышения продуктивности, организовать безопасный обмен файлами с любого устройства и обеспечить пользователям комфортные условия работы за счет единого комплексного решения. Поэтапное внедрение Citrix Workspace, в основе которого лежат наиболее важные для вас сценарии использования этого решения, поможет вам завершить переход к доставке цифровых рабочих мест, сохранив при этом оптимальную эффективность бизнеса.

## Следующие этапы

[Узнайте больше о Citrix Workspace](#)

[Переходите на Citrix Workspace и экономьте](#)

## Источники

<sup>1</sup> Gallup: состояние рабочих мест в США, 2017 г.



## Отдел продаж

Северная Америка | +1 800-424-8749

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

© Citrix Systems, Inc., 2018 г. Все права защищены. Citrix, логотип Citrix и другие знаки, упомянутые в данном документе, являются собственностью компании Citrix Systems, Inc. и/или одного или нескольких ее филиалов и могут быть зарегистрированы в Ведомстве по патентам и товарным знакам США и в других странах. Все остальные знаки являются собственностью соответствующих владельцев.