citrix

Приложение о безопасности служб Citrix

Версия 2.0
Дата вступления в силу: 20 апреля 2020 г.

Оглавление

Это Приложение о безопасности служб Citrix (далее — «Приложение») описывает элементы управления безопасностью, реализованные в рамках работы служб Citrix Cloud, служб технической поддержки или консультационных служб (далее — «Службы»), предоставляемых клиентам по соответствующей лицензии Citrix и/или соглашению об использовании служб и применимому заказу на Службы (все вместе — «Соглашение»). Бета-версии и предварительные версии лабораторных/технических служб (в том числе Citrix Cloud Labs) и внутренние ИТ-системы Citrix, не используемые в предоставлении Служб, не входят в область действия этого Приложения.

Термины, написанные с заглавной буквы, имеют значение, указанное в Соглашении или определенное в настоящем документе. «Клиентское содержимое» означает любые данные, отправленные в учетную запись Клиента для хранения, или данные в вычислительной среде Клиента, к которой компании Citrix может быть предоставлен доступ с целью обеспечения работы Служб. «Журналы» означает записи о Службах, в частности данные и сведения о работе, стабильности, использовании, безопасности, поддержке, а также технические сведения об устройствах, системах, соответствующем программном обеспечении, службах или периферийных устройствах, относящиеся к использованию Клиентом Служб.

1. Область действия

В настоящем Приложении описываются административные, физические и технические элементы управления безопасностью, которые компания Citrix использует для обеспечения конфиденциальности, целостности и доступности Служб. Эти элементы управления относятся к операционным средам, а также системам и средам Служб Citrix. Citrix использует стандарт ISO/IEC 27002 в качестве базового уровня для своей программы обеспечения безопасности Служб.

Компания Citrix пытается постоянно дорабатывать и улучшать свои методы обеспечения безопасности, поэтому оставляет за собой право изменять элементы управления, описанные в настоящем документе. Независимо от изменений уровень безопасности не будет уменьшен в течение соответствующего срока действия Служб.

2. Инфраструктура программы и политики обеспечения безопасности

В Citrix есть инфраструктура программы и политики обеспечения безопасности, установленная и одобренная руководителями подразделений Citrix, относящихся к различным сферам деятельности.

2.1 Курирование угроз безопасности

Комитет по курированию угроз кибербезопасности Citrix (CROC) управляет действиями по контролю угроз безопасности. Комитет CROC состоит из руководителей различных подразделений. Руководство высшего звена ежегодно проверяет состав комитета и следит за тем, чтобы различные бизнес-сферы и операционных сферы были представлены в равной степени.

Комитет CROC собирается не реже чем раз в квартал и предоставляет аналитические данные, указания и инструкции в отношении идентификации, оценки и устранения угроз безопасности в корпоративной деятельности и в инфраструктуре предоставления служб.

2.2 Контроль угроз безопасности

Citrix использует программу контроля угроз безопасности (SRM), которая определяет потенциальные угрозы продуктам и службам Citrix, а также инфраструктуре Citrix, оценивает значимость рисков, связанных с этими угрозами, разрабатывает стратегии снижения рисков и помогает отделам разработки продуктов и проектирования реализовать эти стратегии.

В программе SRM применяются общепризнанные отраслевые стандарты, например ISO/IEC 31000 и ISO/IEC 27005.

2.3 Информационная безопасность

Компания Citrix назначила Руководителя по информационной безопасности (CISO), который несет ответственность за курирование безопасности, стратегию политики безопасности, обеспечение соответствия требованиям и контроль за исполнением. Директор по мониторингу безопасности и реагированию руководит процессами реагирования на инциденты, в том числе изучением, сдерживанием и устранением.

2.4 Физическая и экологическая безопасность

Отдел безопасности Citrix совместно с отделом административно-хозяйственного управления контролирует физический доступ на объекты Citrix.

3. Управление доступом

Citrix требует использовать меры по контролю доступа, предполагающие предоставление и сохранение необходимых прав для доступа к системам, ресурсам, данным и объектам компании с целью защиты от потенциального повреждения, раскрытия или потери. Citrix использует принцип минимальных прав (безопасность на основе ролей), предоставляя пользователям доступ только к тому содержимому, которое им необходимо для выполнения должностных функций или ролей.

Менеджеры разрабатывают роли для обеспечения надлежащего разделения обязанностей, распределяя задачи и права между несколькими людьми с целью обеспечения защиты от мошеннических действий и ошибок.

3.1 Новые учетные записи, роли и запросы на доступ

Citrix требует формальный запрос для доступа к системам или данным компании. Для каждого запроса на доступ требуется минимальное утверждение менеджера пользователя, гарантирующее, что доступ предусмотрен ролью пользователя. Администраторы доступа подтверждают получение необходимых утверждений, прежде чем предоставить доступ к системам или данным.

3.2 Проверка учетных записей

Citrix ведет и обновляет записи о правах безопасности для сотрудников и подрядчиков, которым разрешено получать доступ к системам Citrix с Клиентским содержимым. Применяется принцип минимальных прав.

Citrix выполняет проверку учетных записей и предоставленных прав в отношении основных систем не реже двух раз в год. Любые изменения, которые необходимо внести в результате проверки, проходят формальный процесс запроса на доступ для подтверждения того, что пользователю и его роли требуется доступ к соответствующим системам.

3.3 Прекращение действия учетной записи, роли и доступа

Citrix требует, чтобы доступ учетной записи пользователя был отключен, отозван или отменен сразу после уведомления об изменении (если применимо) или аннулировании роли пользователя, завершения взаимодействия с пользователем или его ухода из компании.

Запросы на отмену доступа документируются и отслеживаются.

3.4 Учетные данные

Citrix требует наличия многофакторной проверки подлинности для удаленного доступа сотрудников к системам Citrix и в обязательном порядке требует применения следующих способов работы с паролями и управления ими.

- Пароли регулярно обновляются согласно системным требованиям, установленным Citrix
- Пароли должны соответствовать требованиям к длине и сложности, в том числе длина не должна быть меньше 10 символов и паролями не могут быть обычные или словарные слова
- Деактивированные или недействительные идентификаторы пользователей не назначаются другим лицам
- Citrix следит за порядком деактивации паролей, которые были непреднамеренно раскрыты
- Citrix отслеживает повторные попытки получить доступ к Службам с помощью недействительного пароля и применяет автоматические действия для блокировки таких попыток

Citrix предпринимает специальные меры для сохранения конфиденциальности и целостности паролей во время их назначения, распределения и хранения, например:

- Citrix требует хеширования паролей в течение всего срока их действия,
- Citrix запрещает раскрытие паролей.

4. Разработка и обслуживание систем

Citrix применяет процесс безопасного проектирования, который включает в себя стандарты и процедуры изменения элементов управления, позволяющие обеспечить соответствие требованиям к безопасности информационных систем, проверку и тестирование кода, а также безопасность в отношении использования данных тестирования. Управляет этим процессом и отслеживает его специальный отдел безопасности, который также несет ответственность за проверку разработки, моделирование угроз, ручную проверку кода, выборочные проверки и тестирование на проникновение.

4.1 Принципы безопасного проектирования

Citrix внедрила формальную методику жизненного цикла разработки систем (SDLC), которая управляет требованиями в отношении разработки, комплектования, реализации и обслуживания компьютеризированных информационных систем и соответствующих технологий.

Citrix использует программную систему для управления проверкой и утверждением открытых источников информации, в том числе для осуществления периодической проверки и аудита собственных программных продуктов. В Citrix есть задокументированные политики, доступные всем сотрудникам, в отношении использования открытых источников информации, а также обучения разработчиков и использования ими рекомендаций по работе с открытыми источниками.

4.2 Управление изменениями

Процесс управления изменениями в инфраструктуре и программном обеспечении Citrix определяет требования к безопасности и требует, чтобы изменения программного обеспечения и инфраструктуры были авторизованны, формально задокументированы, протестированы (если применимо), проверены и утверждены перед переносом в производственную среду. Отслеживание изменений программного обеспечения и инфраструктуры и управление ими осуществляется с помощью систем управления работой.

Процесс управления изменениями надлежащим образом разделен, и доступ к переносу изменений в производственную среду имеет только авторизованный персонал.

5. Управление активами

5.1 Управление физическими и виртуальными активами

Citrix ведет динамический учет управляемых Citrix физических и виртуальных систем, используемых для предоставления Служб (далее — «Активы служб»). Владельцы систем несут ответственность за обслуживание и обновление своих Активов служб в соответствии со стандартами безопасности Citrix.

Разработаны формальные процедуры уничтожения, содержащие инструкции о безопасном уничтожении данных Citrix и Клиентов. Компания Citrix уничтожает все данные, которые больше не требуются, с учетом классификации и процедур удаления, предотвращающих воссоздание и чтение данных.

Технологические активы Citrix очищаются и удаляются, когда больше не требуются в соответствующей области. Технологические активы включают, в частности, отдельные вычислительные устройства, многофункциональные вычислительные устройства, устройства обработки изображений и сетевые устройства. Уничтожение координируется глобальными службами управления угрозами безопасности и системой информационной безопасности.

5.2 Управление приложениями и системами

Владельцы приложений и систем несут ответственность за проверку и классификацию данных, которые они хранят, уничтожают, передают или к которым они получают доступ. Помимо других элементов управления сотрудники и подрядчики обязаны выполнять следующее.

- Отнесение Клиентского содержимого к одной из двух наивысших категорий конфиденциальной информации Citrix и применение надлежащих ограничений доступа
- Ограничение печати Клиентского содержимого и уничтожение печатных материалов в безопасных контейнерах
- Отказ от хранения корпоративной или Конфиденциальной информации на любом оборудовании или устройстве, которое не соответствует требованиям политик и стандартов безопасности Citrix
- Защита компьютеров и данных, оставленных без присмотра

5.3 Хранение данных

Клиентское содержимое, хранящееся в службах Citrix Cloud, доступно Клиенту в течение ограниченного периода времени после окончания предоставления Служб, а затем удаляется (за исключением резервных копий) после отправки подтверждения Клиенту об удалении. Дополнительные сведения см. в документации конкретных служб. Клиентское содержимое также может храниться после окончания предоставления служб, если это требуется по закону. Компания Citrix будет соблюдать требования настоящего Приложения, пока такое Клиентское содержимое не будет навсегда удалено.

6. Безопасность управления персоналом

Обеспечение безопасности Клиентского содержимого является одним из основных требований для всех сотрудников и подрядчиков Citrix. Кодекс делового поведения Citrix требует, чтобы все сотрудники и подрядчики придерживались политик и стандартов безопасности Citrix, и отдельно рассматривает вопрос защиты конфиденциальной информации, а также личной информации Клиентов, партнеров, поставщиков и сотрудников Citri.

Все сотрудники и подрядчики Citrix должны соблюдать соглашения о конфиденциальности, распространяющиеся на такую информацию Клиентов. Служба безопасности Citrix также регулярно передает сотрудникам сведения о темах, связанных с информационной и физической безопасностью, чтобы обеспечивать актуальность знаний по конкретным темам.

6.1 Проверка данных

Citrix в настоящее время пользуется услугами поставщиков проверки данных для всех новых сотрудников и требует того же для персонала сторонних поставщиков, кроме тех случаев, когда это запрещено местным законом или трудовым законодательством.

6.2 Обучение

Все сотрудники должны пройти обучение по защите данных и политикам компании, разработанным для защиты Конфиденциальной информации Citrix, которая включает в себя Конфиденциальную информацию Клиентов, партнеров, поставщиков и сотрудников. В обучении рассматриваются методики и принципы обеспечения конфиденциальности, которые применяются к обработке персональных данных сотрудниками, в том числе необходимость ограничений использования, хранения персональных данных, доступа и предоставления доступа к ним. Сотрудники инженерных подразделений проходят специальное обучение, в котором рассматриваются вопросы безопасной разработки, построения архитектуры и написания кода.

6.3 Обеспечение принудительного исполнения

Все сотрудники должны соблюдать политики и стандарты безопасности и конфиденциальности Citrix. Их несоблюдение повлечет применение мер дисциплинарного воздействия вплоть до увольнения.

7. Оперативная безопасность

7.1 Безопасность сети и системы

У Citrix есть задокументированные стандарты усиления защиты сети и системы, созданные для обеспечения безопасной конфигурации сетей и систем. В частности, в соответствии с этими стандартами обязательными являются следующие процедуры.

- Изменение или отключение настроек и/или учетных записей по умолчанию
- Применение баннеров для входа
- Контролируемое использование административного доступа
- Использование служебных учетных записей только в целях, для которых они созданы
- Настройка параметров входа и оповещения, подходящих для аудита

Citrix требует реализации антивредоносного программного обеспечения на серверах и рабочих станциях и проверок сети на вредоносное программное обеспечение.

Элементы управления сети контролируют доступ к Клиентскому содержимому. К ним относятся, если применимо: настройка промежуточной недоверенной зоны между Интернетом и внутренней сетью, которая включает защитный механизм для ограничения доступа и несанкционированного трафика; сегментация сети для предотвращения несанкционированного доступа к Клиентскому содержимому; отделение веб-серверов и серверов приложений от соответствующих серверов баз данных в многоуровневой структуре, ограничивающей трафик между уровнями.

7.2 Ведение журналов

Citrix собирает Журналы для подтверждения правильного функционирования Служб, чтобы помочь в устранении системных проблем и защитить сети и Клиентское содержимое. Журналы могут содержать идентификатор доступа, время, предоставленную или отклоненную авторизацию, диагностические данные, например файлы трассировки и сбоев, и другие важные сведения.

Журналы могут использоваться в идентифицируемой форме (i) для предоставления, улучшения Служб, обеспечения их защиты, управления ими и определения их параметров, а также для получения соответствующей аналитики, (ii) по запросу Клиента или его конечных пользователей, (iii) для соответствия требованиям политик Citrix, применимого законодательства, нормативов или запроса государственных служб. Для этого может выполняться мониторинг работы, стабильности, использования и безопасности Служб и соответствующих компонентов. Клиенты не могут блокировать такой мониторинг или вмешиваться в него.

Дополнительные сведения о Клиентских данных и работе с Журналами см. в разделе Конфиденциальность и соответствие требованиям центра управления безопасностью Citrix, где содержатся несколько официальных документов в отношении ведения журналов Citrix.

7.3 Защита данных во время передачи

Компания Citrix развернула протоколы безопасной передачи данных в отношении передачи информации в общедоступных сетях, которые являются частью Служб. Службы защищены шифрованием, а доступ через Интернет защищен с помощью TLS-соединений.

8. Физическая безопасность

8.1 Объекты Citrix

Компания Citrix использует следующие элементы управления, разработанные для предотвращения несанкционированного доступа на объекты.

- Доступ на объекты могут получить только авторизованные лица
- Посетителям необходимо зарегистрироваться в цифровом журнале посетителей, их будут сопровождать и за ними будут наблюдать в течение всего визита
- Сотрудники, подрядчики и гости должны носить значки с идентификаторами, которые должны быть видны в течение всего времени пребывания на объекте
- Отдел безопасности контролирует доступ на объекты в нерабочее время
- Охранники, система обнаружения проникновения и/или камеры видеонаблюдения следят за пунктами входа в здания, платформами отгрузки и разгрузки и зонами общего доступа (механизмы отслеживания доступа могут различаться в зависимости от объекта и его расположения)

Кроме того, на объектах Citrix предусмотрено следующее.

- Системы и устройства подавления и обнаружения огня
- Системы и устройства управления климатом (температурой, влажностью и т. д.)
- Доступные главные запорные или отсечные водяные клапаны
- Альтернативные источники питания (генератор, система аварийного энергоснабжения и т. д.)
- Аварийные выходы и пути эвакуации

Защита коммуникационных шкафов, расположенных в офисах, осуществляется посредством доступа по значкам и мониторинга.

8.2 Центры обработки данных

Кроме элементов управления объектами Citrix, описанных выше, для объектов, которыми управляет и владеет Citrix, в центрах обработки данных, используемых для предоставления Служб, реализованы дополнительные элементы управления.

Компания Citrix использует системы, созданные для защиты от потери данных из-за прекращения подачи питания или сетевых помех, в том числе глобальную избыточную инфраструктуру служб с настроенными узлами аварийного восстановления. Центры обработки данных и поставщики услуг Интернета оцениваются с целью оптимизации пропускной способности, задержек и аварийного восстановления.

Центры обработки данных располагаются в объектах, не связанных с поставщиками услуг Интернета. В них обеспечена физическая защита, резервный источник питания, избыточность инфраструктуры и уровень непрерывной работы в рамках соглашений с ключевыми поставщиками.

Если компания Citrix использует сторонние центры обработки данных или облачные службы для предоставления Служб, она заключает договоры с поставщиками, которые соответствуют минимальным требованиям к физической и экологической безопасности объектов Citrix.

9. Непрерывность бизнес-процессов и аварийное восстановление

9.1 Непрерывность бизнес-процессов

Citrix стратегически планирует непрерывность бизнес-операций во время неблагоприятных или аварийных ситуаций, и разрабатывает системы для обеспечения работы служб при возникновении таких событий.

Citrix выполняет анализ последствий для деятельности на уровне подразделений не менее одного раза в два года и осуществляет ежегодные проверки. Результаты такого анализа используются для создания плана непрерывности деятельности для каждого подразделения, в котором определены и задокументированы требования к ресурсам, параметры и методы восстановления, потребности перемещения и меры безопасности, необходимые на каждом этапе процесса, чтобы избежать сбоев и простоев. Руководящий состав каждого подразделения проверяет и утверждает план непрерывности деятельности каждый год или в случае серьезных организационных изменений.

У Citrix есть аварийные планы и планы экстренных мероприятий для всех объектов Citrix. Если объекты недоступны, сотрудники могут работать удаленно на других объектах Citrix или в месте по своему выбору. Дополнительные стратегии восстановления задокументированы в планах непрерывности деятельности, если применимо.

9.2 Аварийное восстановление

Компания Citrix стремится свести к минимуму влияние от прерывания обслуживания или выполнения операций, реализуя процессы и элементы управления, созданные для обеспечения стабильного и организованного восстановления бизнес-систем и данных Citrix. Citrix реализует избыточность для всех критически важных систем, данных и инфраструктуры. В плане аварийного восстановления используется оценка, выполненная в рамках анализа последствий для деятельности (см. выше), для определения и документации параметров времени восстановления, методов, приоритетов и мер безопасности, необходимых на каждом этапе процесса, чтобы избежать сбоев и простоев.

В плане указывается общая структура и подход к восстановлению критически важных систем и данных, в том числе следующее.

- Роли и обязанности сотрудников и отделов
- Контактные данные важного персонала и сторонних компаний
- Требования к обучению и планы для важного персонала
- Цели и приоритеты восстановления, показатели успеха
- Схема полного восстановления

Руководящий состав проверяет и утверждает план аварийного восстановления каждый год или в случае серьезных организационных изменений.

10. Реагирование на инциденты

Компания Citrix имеет план реагирования на инциденты кибербезопасности, где подробно описаны процессы обнаружения, идентификации, анализа Инцидентов безопасности, влияющих на управляемые Citrix сети и/или системы или Клиентское содержимое, сообщения о них и реагирования на них. Обучение реагированию на Инциденты безопасности и соответствующие проверки проводятся не реже раза в год.

«Инцидент безопасности» означает несанкционированный доступ к Клиентскому содержимому, ставший причиной нарушения конфиденциальности, целостности или доступности. Если компания Citrix определяет, что Клиентское содержимое, которое находится под ее управлением, подверглось воздействию в результате Инцидента безопасности, Клиент будет уведомлен об этом в срок, требуемый по закону. В уведомлении Citrix опишет, если известно, характер инцидента, период времени и возможные последствия для Клиента.

Citrix ведет записи обо всех Инцидентах безопасности.

11. Управление поставщиками

Для предоставления Служб Citrix может пользоваться услугами субподрядчиков и агентов. Всем субподрядчикам и агентам доступ к Клиентскому содержимому должен предоставляться, только если это необходимо для предоставления Служб. Субподрядчики и агенты должны заключать письменные соглашения, по которым от них требуется обеспечение уровня защиты данных не меньше установленного в настоящем Приложении, если применимо. Компания Citrix постоянно несет ответственность за соответствие своих субподрядчиков и агентов условиям Соглашения, если применимо. Список субподрядчиков Citrix, у которых может быть доступ к Клиентскому содержимому, доступен в центре управления безопасностью Citrix.

11.1 Подключение

В программе контроля угроз сторонних организаций Citrix предоставлен системный подход к управлению угрозами безопасности, которые возникают при работе со сторонними поставщиками. Citrix работает над определением, анализом и сведением к минимуму угроз безопасности, прежде чем приступить к закупкам у таких сторонних компаний.

Citrix заключает соглашения с поставщиками для документации надлежащих мер безопасности и обязательств, соответствующих тем, что указаны в настоящем Приложении.

11.2 Непрерывная оценка

Citrix периодически осуществляет оценку угроз безопасности, чтобы меры безопасности постоянно применялись в ходе взаимодействия с поставщиками. В случае изменения предоставляемых услуг или существующих договоров требуется провести оценку угроз безопасности, чтобы убедиться, что изменения не несут дополнительные или чрезмерные угрозы.

11.3 Отключение

Citrix уведомляет организацию, занимающуюся материально-техническим обеспечением, за 90 дней до планируемой даты завершения сотрудничества или завершения срока действия договора с поставщиком. Организация, занимающаяся материально-техническим обеспечением, координирует окончание сотрудничества, чтобы убедиться, что корпоративные данные и активы Citrix в безопасности и обрабатываются надлежащим образом.

12. Соответствие требованиям

12.1 Обработка персональных данных

Персональные данные — это информация, относящаяся к идентифицированному или идентифицируемому лицу. Клиент определяет персональные данные, которые входят в Клиентское содержимое. Во время предоставления Служб компания Citrix выступает в качестве обработчика данных, а Клиент остается контролером всех персональных данных, входящих в Клиентское содержимое. Citrix будет действовать в соответствии с инструкциями Клиента в отношении обработки таких персональных данных, как указано в Соглашении.

Дальнейшие сведения об обработке персональных данных в соответствии с Общим регламентом по защите данных (GDPR), в том числе о механизмах, используемых для международной передачи таких данных, представлены в Соглашении об обработке данных Citrix.

12.2 Расположение служб

Клиенты служб Citrix Cloud могут выбирать географическое расположение среды Облачных служб (*см. также статью Географические аспекты Citrix Cloud*). В ходе действия подписки на Облачные службы компания Citrix не будет менять географическое расположение среды, выбранное Клиентом, без согласия Клиента. Обратите внимание, что в рамках предоставления Служб Клиентское содержимое может быть передано в США и другие страны, где работает компания Citrix и/или ее поставщики услуг, если это необходимо для предоставления Служб.

12.3 Раскрытие Клиентского содержимого

Компания Citrix может раскрывать Клиентское содержимое в объеме, предусмотренным законом, в том числе в ответ на судебный запрос, судебное решение, административное постановление или иной нормативный акт, имеющий обязательную силу (далее каждый из вариантов — «Требование»). За исключением случаев, когда это запрещено законом, компания Citrix незамедлительно уведомит Клиента о Требовании и предоставит Клиенту помощь, обоснованно необходимую для своевременного ответа на Требование .

12.4 Безопасность Клиента и нормативные требования

Службы предназначены для использования в более крупной ИТ-среде Клиента, поэтому Клиенты несут полную ответственность за все аспекты безопасности, которые не контролируются компанией Citrix явным образом, в частности элементы управления доступом, брандмауэры, приложения и сети, которые Клиент может использовать в отношении Служб.

Клиенты обязаны определить, распространяются ли на использование ими Служб, в том числе на предоставление компании Citrix доступа к Клиентскому содержимому в рамках служб, какие-либо нормативные требования или требования к безопасности помимо тех, что указаны в Соглашении, в том числе в настоящем Приложении. В связи с этим Клиенты не должны отправлять или хранить какое-либо Клиентское содержимое, подпадающее под действие законов, которые предусматривают конкретные элементы управления, не указанные в настоящем Приложении (к таким законам могут относиться, например, Международные правила торговли оружием США или аналогичные нормативные требования любой страны, которая запрещает импорт или экспорт предметов военного снабжения или услуг в сфере обороны), защищенную медицинскую информацию, информацию о платежных картах или данные с контролируемым распространением в соответствии с постановлениями правительства, если иное не указано в Соглашении и применимом Описании служб и стороны заранее не заключили дополнительные соглашения (например, Соглашение с деловым партнером HIPAA), дающие право компании Citrix обрабатывать такие данные.

13. Аудит и запросы Клиентов

Citrix будет не чаще одного раза в год отвечать на запросы аудита. Таким ответом будет считаться ответ на оценки угроз Клиента. Клиенты также могут в любое время получить доступ к пакету комплексной проверки Citrix для ознакомления с актуальным пакетом безопасности и анкетой. Пакет комплексной проверки безопасности Citrix создан для запросов клиентов в отношении безопасности и предоставляет доступную информацию о безопасности. Пакет комплексной проверки Citrix содержит три документа для каждого продукта: заполненную упрощенную анкету с общей стандартной информацией об оценках (более 300 вопросов), обзор средств безопасности и элементов управления Citrix и пакет свидетельств в отношении отобранных политик и элементов управления. Анкета со стандартной информацией является наиболее часто применяемой анкетой среди наших Клиентов, которая используется во всех отраслевых секторах. Пакет комплексной проверки можно загрузить в центре управления безопасностью Citrix.

14. Контактные данные Citrix

Функция	Контактные данные
Служба поддержки	https://www.citrix.com/contact/technical-support.html
Сообщение об Инциденте безопасности	secure@citrix.com
Потенциальные уязвимости в продуктах Citrix	https://www.citrix.com/about/trust-center/security.html#lightbox-38764 (Нажмите кнопку «Сообщить об угрозе безопасности».)

Отдел корпоративных продаж
Северная Америка | 800-424-8749 Международный | +1 408-790-8000

Местонахождение
Главный офис компании | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, США