IBM Trusteer Pinpoint Detect

В настоящем Описании Услуги описывается Облачная Услуга. В соответствующих документах заказа указываются цены и дополнительные сведения о заказе Клиента.

1. Облачная Услуга

IBM Trusteer Pinpoint - это облачная услуга, призванная обеспечить другой уровень защиты и нацеленная на обнаружение и минимизацию потерь от вредоносного ПО, фишинга и атак с использованием учётной записи в мошеннических целях. Trusteer Pinpoint можно интегрировать в принадлежащие Клиенту Приложения для Бизнеса и/или для Розничной торговли, для работы с которыми Клиент приобрёл подписку на Облачные Услуги, и в процессы предотвращения мошенничества.

В данную Облачную Услугу входят:

a. Trusteer Management Application (TMA) и Trustboard:

TMA — традиционное управляющее приложение Trusteer, позволяющее Клиенту просматривать и классифицировать предупреждения. Trustboard — более новое управляющее приложение, служащее в основном для исследований. Единовременно Клиенты могут выбрать только одно приложение: либо TMA, либо Trustboard. И TMA, и Trustboard предоставляются в облачной среде IBM Trusteer, в которой Клиент (и неограниченное число его авторизованных сотрудников) может: (i) просматривать и загружать определённые отчёты о событиях и оценки рисков, а также (ii) просматривать, подписываться и настраивать доставку каналов получения данных об угрозах, создаваемых с помощью приложений Pinpoint. IBM Trusteer Pinpoint Detect и IBM Trusteer Pinpoint Verify используются в качестве компонентов входа в систему TMA и Trustboard.

b. Веб-сценарий и/или API-интерфейсы:

Используются для внедрения на веб-сайте с целью тестирования или использования Облачной Услуги.

«Сеанс» — это взаимодействие между приложением Клиента (браузерным или мобильным) и Облачной Услугой, в которой создаётся одна или несколько оценок риска в реальном времени. Время Сеанса измеряется от момента начала взаимодействия до момента его окончания. Взаимодействие заканчивается, когда происходит одно из следующих событий:

- Выполняется обычный сброс взаимодействия или выход из приложения.
- Закрывается браузер, приложение или вкладка.
- Удаляются файлы cookie.
- Происходит тайм-аут.

Сеанс может включать произвольное количество операций: вход в систему, просмотр, оформление заказа, настройка способа оплаты и других, как указано в Приложении Клиента. Уточнение: для целей настоящей Облачной Услуги одно Соединение (как будет определено далее) приравнивается к одному Сеансу.

1.1 Предложения

Клиент может выбрать из следующих доступных предложений.

1.1.1 IBM Trusteer Pinpoint Detect Standard for Retail и/или IBM Trusteer Pinpoint Detect Standard for Business

Настоящая Облачная Услуга сочетает в себе Облачные Услуги IBM Trusteer Pinpoint Criminal Detection и IBM Trusteer Pinpoint Malware Detection, в результате чего получается единое комплексное решение.

Решение помогает без участия клиента обнаруживать вредоносное ПО и/или подозрительные действия по использованию учётной записи в мошеннических целях в браузерах, подключающихся к Приложению для Розничной торговли или Бизнеса, с использованием ID устройства, обнаруживать фишинг и кражу идентификационных данных с помощью вредоносного кода.

Предложения IBM Trusteer Pinpoint обеспечивают иной уровень защиты и нацелены на обнаружение попыток использования учётной записи в мошеннических целях и предоставление непосредственно Клиенту данных оценки рисков для браузеров или мобильных устройств (с использованием исходных браузеров или мобильных приложений Клиента), осуществляющих доступ к Приложениям для Розничной торговли или Бизнеса. Данная Услуга также может использоваться для доступа удалённых сотрудников с целью оценки риска от управляемых и неуправляемых устройств.

В эту Облачную Услугу включена поддержка уровня Premium (в соответствии с определением, приведённым ниже в разделе Техническая поддержка).

Данную услугу можно приобретать пакетами по 100 Соответствующих критериям Участников или по 100 Соединений.

1.1.2 IBM Trusteer Pinpoint Detect Premium for Retail и/или IBM Trusteer Pinpoint Detect Premium for Business

Настоящая Облачная Услуга сочетает в себе Облачные Услуги IBM Trusteer Pinpoint Criminal Detection и IBM Trusteer Pinpoint Malware Detection, в результате чего получается единое, комплексное, легко интегрируемое решение.

Решение помогает без участия клиента обнаруживать вредоносное ПО и/или подозрительные действия по использованию учётной записи в мошеннических целях в браузерах, подключающихся к Приложению для Розничной торговли или Бизнеса, с использованием ID устройства, обнаруживать фишинг и кражу идентификационных данных с помощью вредоносного кода. Предложения IBM Trusteer Pinpoint обеспечивают иной уровень защиты и нацелены на обнаружение попыток использования учётной записи в мошеннических целях и предоставление непосредственно Клиенту данных оценки рисков для браузеров или мобильных устройств (с использованием исходных браузеров или мобильных приложений Клиента), осуществляющих доступ к Приложениям для Бизнеса или Розничной торговли.

В состав данной услуги входят расширенные функции и услуги, включая следующее: расширенные услуги по развёртыванию и настройке, индивидуальные услуги в сфере безопасности, услуги по расследованию и т. д. Услуга включает в себя до 200 часов консультаций экспертов по вопросам развёртывания приложений и 200 часов консультаций экспертов по вопросам анализа безопасности после установки приложений. В состав текущих услуг входят по 20 часов обслуживания в год на каждое развёрнутое приложение и по 100 часов анализа безопасности в год на каждое приложение. Все дополнительные услуги предоставляются за дополнительную плату.

Pinpoint Detect может использовать транзакции из каналов Mobile и Web. Если включены транзакции Mobile, действует правило Pinpoint by Connection. В эту Облачную Услугу включена защита одного Приложения. Для каждого дополнительного Приложения Клиент должен приобрести разрешение на IBM Trusteer Pinpoint Detect Premium Additional Applications.

В эту Облачную Услугу включена поддержка уровня Premium.

Услуги IBM Trusteer Pinpoint Detect Premium for Retail and Business можно приобретать пакетами по 100 Соответствующих критериям Участников, а услуги IBM Trusteer Pinpoint Detect Premium — пакетами по 100 Соединений. Если Клиент будет приобретать Соединения, то начиная с первого приложения взимается плата за Дополнительные Приложения.

Pinpoint Detect Policy Manager:

Policy Manager входит в состав услуги Pinpoint Detect Premium и предоставляется в облачной среде IBM Trusteer, в которой Клиент (и неограниченное число авторизованных сотрудников) может: (i) разрабатывать, тестировать и развёртывать в производственной среде правила обнаружения мошеннической деятельности, (ii) разрабатывать отчёты и панели мониторинга и (iii) просматривать, настраивать и устанавливать политики безопасности и политики обнаружения подозрительной деятельности в Приложении заказчика.

Для активации компонента Policy Manager и получения услуг глубокой поддержки требуются консультационные услуги. Сведения о консультационных услугах указываются отдельно в рабочем задании.

При активации Policy Manager компания IBM оставляет за собой право получать доступ к среде Клиента в целях предоставления поддержки для настройки политик Клиента с целью предотвращения серьёзных проблем, связанных с изменениями политик.

Клиент обязуется защищать все данные, доступные через Policy Manager, от несанкционированного использования.

При активации компонента Policy Manager Клиент обязуется следовать указаниям IBM по настройке правил, как указано в документации. Клиент признаёт, что IBM не несёт ответственности за последствия несоблюдения Клиентом настоящих рекомендаций.

Проблемы со стабильностью и снижением качества услуг, связанные с неправильной настройкой компонента Policy Manager Клиентом, не будут рассматриваться в качестве Времени простоя при расчёте показателей SLA.

1.1.3 IBM Trusteer Pinpoint Detect for Connections

Данная Облачная Услуга обеспечивает защиту и нацелена на обнаружение попыток использования учётной записи в мошеннических целях и предоставление данных оценки рисков / доверия для браузеров и мобильных устройств (с использованием исходных браузеров или мобильных приложений Клиента), осуществляющих доступ к приложениям для Бизнеса или Розничной торговли. В данном решении используются разные индикаторы риска, обеспечивающие анализ устройства конечного пользователя, соединения и поведения, а также сравнение полученных данных с историей пользователя для выявления подозрительного использования.

Данная Облачная Услуга может использовать соединения из каналов Mobile и Web. IBM Trusteer Pinpoint Detect включает в себя разрешение на IBM Trusteer Mobile SDK, если это необходимо.

Данную Облачную Услугу можно приобретать пакетами по 100 Соединений в год.

1.2 Дополнительные Услуги

Для Облачных Услуг, описываемых в этом разделе, необходимо предварительно иметь разрешение на IBM Trusteer Pinpoint Detect Premium, IBM Trusteer Pinpoint Detect Standard или IBM Trusteer Pinpoint for Connections.

1.2.1 IBM Trusteer Pinpoint Detect Standard Application

Приложение Клиента — это Веб-приложение или Мобильное приложение. Веб-приложение охватывает все функции, предлагаемые Соответствующим требованиям Участникам Клиента через несколько веб-страниц, начиная со страницы входа в систему или идентификации. Его мониторинг осуществляется в форме одного Приложения в консоли Trusteer. Мобильное приложение охватывает все функции, предлагаемые Соответствующим требованиям Участникам Клиента через одну программу, которую можно загрузить из магазина приложений (магазина), начиная со страницы входа в систему или идентификации. Её мониторинг осуществляется в форме одного Приложения в консоли Trusteer.

Для интеграции IBM Trusteer Pinpoint требуется разрешение на IBM Trusteer Pinpoint Application для каждого Приложения.

- Для развёртывания IBM Trusteer Pinpoint Detect Standard требуется разрешение на IBM Trusteer Pinpoint Detect Standard Application для каждого Приложения.

1.2.2 IBM Trusteer Pinpoint Detect Premium Application

Приложение Клиента — это Веб-приложение или Мобильное приложение. Веб-приложение охватывает все функции, предлагаемые Соответствующим требованиям Участникам Клиента через несколько веб-страниц, начиная со страницы входа в систему или идентификации. Его мониторинг осуществляется в форме одного Приложения в консоли Trusteer. Мобильное приложение охватывает все функции, предлагаемые Соответствующим требованиям Участникам Клиента через одну программу, которую можно загрузить из магазина приложений (магазина), начиная со страницы входа в систему или идентификации. Её мониторинг осуществляется в форме одного Приложения в консоли Trusteer.

Услуга включает в себя до 200 часов консультаций экспертов по вопросам развёртывания приложений и 200 часов консультаций экспертов по вопросам анализа безопасности после установки приложений. В состав текущих услуг входят по 20 часов обслуживания в год на каждое развёрнутое приложение и по 100 часов анализа безопасности в год на каждое приложение.

- Для развёртывания IBM Trusteer Pinpoint Premium требуется разрешение на IBM Trusteer Pinpoint Detect Premium Application для каждого Приложения.

1.2.3 IBM Trusteer New Account Fraud for Retail и/или IBM Trusteer New Account Fraud for Business

Данная услуга доступна подписчикам Pinpoint и нацелена на обнаружение аномалий, выявление подозрительных действий и выдачу предупреждений на ранних этапах процесса создания учётных записей. В рамках услуги осуществляется мониторинг новых учётных записей для выявления действий, характерных для случаев мошенничества, а также профилирование новых учётных записей для получения ранних предупреждений о том, что новые учётные записи могут быть подставными или использоваться для осуществления мошенничества, в форме отчётов об использовании в TMA.

IBM Trusteer New Account Fraud for Retail и IBM Trusteer New Account Fraud for Business предоставляются пакетами по 10 Вызовов API.

1.2.4 IBM Trusteer Digital Content Pack for Retail и/или IBM Trusteer Digital Content Pack for Business

IBM Trusteer Digital Content Pack даёт аналитикам безопасности возможность интегрировать новые модели мошенничества параллельно с полной поддержкой создания и изменения специальных моделей для реагирования на появляющиеся угрозы. Данное решение содержит обширный набор правил, информации и политик, которые можно приобрести в качестве дополнительной интегральной части решения. Предложение Digital Content Pack помогает усилить интеграцию инструментов предотвращения цифрового мошенничества Trusteer с каналами безналичной оплаты IBM Safer Payments. Опираясь на встроенные правила и определённую бизнес-логику, Digital Content Pack позволяет банкам и другим финансовым учреждениям расширить свои возможности в сфере обнаружения и предотвращения мошенничества.

Предложение IBM Trusteer Digital Content Pack for Retail продаётся пакетами на 100 Соответствующих критериям Участников. Предложение IBM Trusteer Digital Content Pack for Business продаётся пакетами на 10 Соответствующих критериям Участников.

Для интеграции Digital Content Pack с Pinpoint Detect и IBM Safer Payments, а также для предоставления поддержки, требующей значительного объёма работы, необходимо приобрести консультационные услуги. Консультационные услуги приобретаются отдельно по отдельному рабочему заданию.

1.2.5 IBM Trusteer Pinpoint Malware Detection

В случае обнаружения вредоносного ПО в Облачных Услугах IBM Trusteer Pinpoint Malware Detection II Клиент должен следовать рекомендациям из Руководства по лучшим методам работы с Pinpoint. Не следует использовать Облачные Услуги IBM Trusteer Pinpoint Malware Detection II каким-либо способом, который повлияет на работу Соответствующего критериям Участника сразу после обнаружения вредоносного ПО или мошеннического использования учётной записи, таким образом чтобы другие пользователи могли связать действия Клиента с использованием Облачных Услуг IBM Trusteer Pinpoint (например, уведомления, сообщения, блокирование устройств или блокирование доступа к Приложению для Бизнеса и/или для Розничной торговли сразу же после обнаружения вредоносного ПО или мошеннического использования учётной записи).

1.2.6 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business и/или IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail и/или IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business и/или IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

IBM Security Pinpoint Malware Detection II — это новый вариант IBM Trusteer Pinpoint Malware Detection, помогающий систематизировать оплату защиты нескольких Приложений и заменить разовые платежи при добавлении Приложений.

Обнаружение заражений финансовым вредоносным ПО типа "Человек в браузере" (MitB) в браузерах, подключающихся к Приложениям для Бизнеса и/или Розничной торговли. Облачные Услуги IBM Trusteer Pinpoint Malware Detection обеспечивают иной уровень защиты и призваны помочь организациям сконцентрироваться на процессах предотвращения мошенничества на основании риска заражения вредоносным кодом; это обеспечивается благодаря предоставлению Клиенту оценок и предупреждений о наличии финансового вредоносного ПО типа MitB.

a. Данные о событиях:

   Клиент (и неограниченное число его авторизованных сотрудников) может использовать TMA для получения данных о событиях, генерируемых в результате онлайн-взаимодействий

Соответствующих критериям Участников с принадлежащими Клиенту Приложениями для Бизнеса и/или Приложениями для Розничной торговли.

b. Версия Advanced Edition:

Версии Advanced Edition для Бизнеса и/или для Розничной торговли предлагают дополнительные возможности обнаружения и защиты, которые настраиваются в соответствии со структурой и потоком принадлежащих Клиенту Приложений для Бизнеса и/или для Розничной торговли; они могут приспосабливаться к особенностям угроз, нацеленных на Клиента. Они могут встраиваться в принадлежащие Клиенту Приложения для Бизнеса и/или Розничной торговли на различных площадках.

Версия Advanced Edition предлагается Клиенту в минимальных объёмах 100 тыс. Соответствующих критериям Участников для Розничной торговли или 10 тыс. Соответствующих критериям Участников для Бизнеса, с 1000 пакетов по 100 Соответствующих критериям Участников для Розничной торговли или 1000 пакетов по 10 Соответствующих критериям Участников для Бизнеса.

c. Версия Standard Edition:

Версии Standard Edition for Business и Retail представляют собой быстрые в развёртывании решения, обеспечивающие основные функции данной Облачной Услуги в соответствии с описанием в данном документе.

В эту Облачную Услугу включена защита одного Приложения. Для каждого дополнительного Приложения Клиент должен приобрести разрешение на IBM Trusteer Pinpoint Malware Detection Additional Applications.

1.2.7 Необязательные дополнительные Облачные Услуги для IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail и/или IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail и/или IBM Pinpoint Trusteer Pinpoint Malware Detection Standard Edition II for Business и/или IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business

- Для Облачной Услуги IBM Trusteer Rapport Remediation for Retail предварительным условием является наличие IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail или IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.
- Для Облачной Услуги IBM Trusteer Rapport Remediation for Business предварительным условием является наличие IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business или IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.

1.2.8 IBM Trusteer Pinpoint Criminal Detection for Business и/или IBM Trusteer Pinpoint Criminal Detection for Retail

Обнаружение без участия клиента подозрительных действий по использованию учётной записи в мошеннических целях в браузерах, подключающихся к Приложению для бизнеса или Приложению для розничной торговли, с использованием ID устройства, обнаружение фишинга и кражи идентификационных данных с помощью вредоносного кода. Облачные Услуги IBM Trusteer Pinpoint Criminal Detection обеспечивают иной уровень защиты и нацелены на обнаружение попыток использования учётной записи в мошеннических целях и предоставление непосредственно Клиенту данных оценки рисков для браузеров или мобильных устройств (с использованием исходных браузеров или мобильных приложений Клиента), осуществляющих доступ к Приложениям для Бизнеса или Розничной торговли.

a. Данные о событиях:

Единовременно Клиенты могут выбрать только одно приложение: либо TMA, либо Trustboard. Клиент (и неограниченное число его авторизованных сотрудников) может использовать TMA или Trustboard для получения данных о событиях, генерируемых в результате онлайн-взаимодействий Соответствующих критериям Участников с принадлежащими Клиенту Приложениями для Бизнеса и/или Приложениями для Розничной торговли, для работы с которыми Клиент приобрел подписку на Облачные Услуги; или Клиент может получать данные о событиях в фоновом режиме с помощью API-интерфейса.

1.2.9 IBM Trusteer Pinpoint Criminal Detection II for Business и/или IBM Trusteer Pinpoint Criminal Detection II for Retail

IBM Security Pinpoint Criminal Detection II — это новый вариант IBM Trusteer Pinpoint Criminal Detection, помогающий систематизировать оплату защиты нескольких Приложений и заменить разовые платежи при добавлении Приложений.

Обнаружение без участия клиента подозрительных действий по использованию учётной записи в мошеннических целях в браузерах, подключающихся к Приложению для бизнеса или Приложению для розничной торговли, с использованием ID устройства, обнаружение фишинга и кражи идентификационных данных с помощью вредоносного кода. Облачные Услуги IBM Trusteer Pinpoint Criminal Detection II обеспечивают иной уровень защиты и нацелены на обнаружение попыток использования учётной записи в мошеннических целях и предоставление непосредственно Клиенту данных оценки рисков для браузеров или мобильных устройств (с использованием исходных браузеров или мобильных приложений Клиента), осуществляющих доступ к Приложениям для Бизнеса или Розничной торговли.

a. Данные о событиях:

   Единовременно Клиенты могут выбрать только одно приложение: либо TMA, либо Trustboard. Клиент (и неограниченное число его авторизованных сотрудников) может использовать TMA или Trustboard для получения данных о событиях, генерируемых в результате онлайн-взаимодействий Соответствующих критериям Участников с принадлежащими Клиенту Приложениями для Бизнеса и/или Приложениями для Розничной торговли, для работы с которыми Клиент приобрел подписку на Облачные Услуги; или Клиент может получать данные о событиях в фоновом режиме с помощью API-интерфейса.

В эту Облачную Услугу включена защита одного Приложения. Для каждого дополнительного Приложения Клиент должен приобрести разрешение на IBM Trusteer Pinpoint Criminal Detection Additional Applications.

1.2.10 IBM Trusteer Rapport Remediation for Retail и/или IBM Trusteer Rapport Remediation for Business

Предложения IBM Trusteer Rapport Remediation for Retail и IBM Trusteer Rapport Remediation for Business призваны исследовать, минимизировать отрицательные последствия, блокировать и удалять вредоносное ПО типа MitB с заражённых устройств (ПК/MAC) Соответствующих критериям Участников Клиента, которые на разовой основе осуществляют доступ к Приложению Клиента, где было обнаружено вредоносное ПО MitB, согласно данным о событиях, сгенерированным IBM Trusteer Pinpoint Malware Detection. У Клиента должна быть действующая подписка на предложение IBM Trusteer Pinpoint Malware Detection II, которое выполняется на Приложении Клиента. Клиент может использовать эту Облачную Услугу только в связи в Соответствующими критериям Участниками, которые осуществляют доступ к Приложению Клиента, и только в качестве средства, которое призвано проанализировать и устранить заражение конкретного устройства (ПК/MAC) на разовой основе. Предложение IBM Trusteer Rapport Remediation должно выполняться на таком заражённом устройстве Соответствующего критериям Участника (ПК/MAC), и такой Соответствующий критериям Участник должен принять условия EULA, как минимум один раз пройти идентификацию в Приложении(-ях) Клиента; конфигурация Клиента должна включать собрание ID Пользователей. Во избежание сомнений, настоящее предложение Облачной Услуги не включает право на использование Trusteer Splash и/или распространение Клиентского ПО Владельца Учётной записи любым иным способом всем группам Соответствующих критериям Участников Клиента. В контексте настоящего Описания Услуги: Владелец Учётной записи - это конечный пользователь Клиента, который установил клиентскую часть ПО, принял лицензионное соглашение с конечными пользователями ("EULA") и как минимум один раз прошёл идентификацию в Приложении Клиента для Розничной торговли или для Бизнеса, для работы с которыми Клиент приобрёл подписку на Облачную Услугу. Клиентское ПО Владельца Учётной записи - это клиентская часть ПО IBM Trusteer Rapport или клиентская часть любого другого ПО, которые предоставляются вместе с некоторыми Облачными Услугами для установки на устройствах конечных пользователей.

1.2.11 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail и/или IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

- Для IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail и IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail развёртывание дополнительных Приложений для Розничной торговли сверх первого Приложения требует наличия разрешения на IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail.
- Для IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business и IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business развёртывание дополнительных Приложений для Бизнеса сверх первого Приложения требует наличия разрешения на IBM Trusteer Pinpoint Malware Detection Additional Applications for Business.

1.2.12 IBM Trusteer Rapport for Mitigation for Retail и/или IBM Trusteer Rapport for Mitigation for Business

- Предложение IBM Trusteer Rapport for Mitigation for Retail призвано исследовать, минимизировать отрицательные последствия, блокировать и удалять вредоносное ПО с заражённых устройств (ПК/MAC) Соответствующих критериям Участников Клиента, которые на разовой основе осуществляют доступ к принадлежащему Клиенту Приложению для Розничной торговли, где было обнаружено вредоносное ПО, согласно данным о событиях, сгенерированным IBM Trusteer Pinpoint Detect Premium или IBM Trusteer Pinpoint Detect Standard. У Клиента должна быть действующая подписка на предложение IBM Trusteer Pinpoint Detect Premium или IBM Trusteer Pinpoint Detect Standard, которое выполняется на Приложении Клиента для Розничной торговли. Клиент может использовать эту Облачную Услугу только в связи в Соответствующими критериям Участниками, которые осуществляют доступ к Приложению Клиента для Розничной торговли, и только в качестве средства, которое призвано проанализировать и устранить заражение конкретного устройства (ПК/MAC) на разовой основе. Предложение IBM Trusteer Rapport for Mitigation for Retail должно выполняться на таком заражённом устройстве Соответствующего критериям Участника (ПК/MAC), и такой Соответствующий критериям Участник должен принять условия EULA, как минимум один раз пройти идентификацию в Приложении(-ях) Клиента для Розничной торговли; конфигурация Клиента должна включать собрание ID Пользователей. Во избежание сомнений, настоящая Облачная Услуга не включает право на использование Trusteer Splash и/или распространение Клиентского ПО Владельца Учётной записи любым иным способом всем группам Соответствующих критериям Участников Клиента.
- Предложение IBM Trusteer Rapport for Mitigation for Business призвано исследовать, минимизировать отрицательные последствия, блокировать и удалять вредоносное ПО с заражённых устройств (ПК/MAC) Соответствующих критериям Участников Клиента, которые на разовой основе осуществляют доступ к принадлежащему Клиенту Приложению для Бизнеса, где было обнаружено вредоносное ПО, согласно данным о событиях, сгенерированным IBM Trusteer Pinpoint Detect Premium или IBM Trusteer Pinpoint Detect Standard. У Клиента должна быть действующая подписка на предложение IBM Trusteer Pinpoint Detect Premium или IBM Trusteer Pinpoint Detect Standard, которое выполняется на Приложении Клиента для Бизнеса. Клиент может использовать эту Облачную Услугу только в связи с Соответствующими критериям Участниками, которые осуществляют доступ к Приложению Клиента для Бизнеса, и только в качестве средства, которое призвано проанализировать и устранить заражение конкретного устройства (ПК/MAC) на разовой основе. Предложение IBM Trusteer Rapport for Mitigation for Business должно выполняться на таком заражённом устройстве Соответствующего критериям Участника (ПК/MAC), и такой Соответствующий критериям Участник должен принять условия EULA, как минимум один раз пройти идентификацию в Приложении(-ях) Клиента для Бизнеса; конфигурация Клиента должна включать собрание ID Пользователей. Во избежание сомнений, настоящая Облачная Услуга не включает право на использование Trusteer Splash и/или распространение Клиентского ПО Владельца Учётной записи любым иным способом всем группам Соответствующих критериям Участников Клиента.

1.2.13 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail и/или IBM Trusteer Pinpoint Detect Standard Additional Applications for Business

- Для развёртывания IBM Trusteer Pinpoint Detect Standard for Retail и дополнительных Приложений для Розничной торговли сверх первого Приложения требуется разрешение на IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail.
- Для развёртывания IBM Trusteer Pinpoint Detect Standard for Business и дополнительных Приложений для Бизнеса сверх первого Приложения требуется разрешение на IBM Trusteer Pinpoint Detect Standard Additional Applications for Business.

1.2.14 IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail и/или IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

Услуга включает в себя до 200 часов консультаций экспертов по вопросам развёртывания приложений и 200 часов консультаций экспертов по вопросам анализа безопасности после установки приложений. В состав текущих услуг входят по 20 часов обслуживания в год на каждое развёрнутое приложение и по 100 часов анализа безопасности в год на каждое приложение.

- Для развёртывания IBM Trusteer Pinpoint Premium for Retail и дополнительных Приложений для Розничной торговли сверх первого Приложения требуется разрешение на IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail.
- Для развёртывания IBM Trusteer Pinpoint Premium for Business и дополнительных Приложений для Бизнеса сверх первого Приложения требуется разрешение на IBM Trusteer Pinpoint Detect Premium Additional Applications for Business.

1.2.15 IBM Trusteer Pinpoint Detect Standard for Retail Premium Support и/или IBM Trusteer Pinpoint Detect Standard for Business Premium Support

Клиенты, купившие Облачную Услугу Pinpoint Detect Standard, могут приобрести услугу Premium Support. Объём услуг Premium Support перечислен в разделе 4 ниже.

1.2.16 IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

У Клиента должна быть действующая подписка на предложение IBM Trusteer Pinpoint Detect до подписки на данную Облачную Услугу.

Данная Облачная Услуга расширяет возможности IBM Trusteer Pinpoint Detect за счёт предоставления дополнительной информации и контекста о номерах мобильных телефонов, предоставляемых любой из этих Облачных Услуг, с целью определения риска мошенничества в рамках отдельно взятого сеанса. Клиент может направить запрос в Облачную Услугу для определения характеристик мобильного номера, например для получения информации об операторе.

Данные, предоставленные данной Облачной Услугой о номерах мобильных телефонов («Информация о мобильных номерах»), должны использоваться только во внутренних целях Клиента и могут храниться не более тридцати (30) дней. По истечении данного периода Клиент обязан повторно направить запрос в Облачную Услугу, если ему вновь потребуется Информация о мобильном номере в отношении соответствующего номера. Повторное использование Информации о мобильном номере, полученной по предыдущему обращению, не допускается. Клиенту запрещается кэшировать, за исключением указанных выше разрешённых случаев, повторно использовать и использовать, как полностью, так и частично, в любых приложениях по глубокому анализу или архивированию данных любую полученную Информацию о мобильных номерах.

1.3 Услуги по ускорению внедрения (Acceleration Services)

1.3.1 IBM Trusteer Pinpoint Detect Standard Redeployment и/или IBM Trusteer Pinpoint Detect Premium Redeployment

Клиенты, повторно развёртывающие свои Приложения для онлайн-банкинга в течение срока оказания услуги и, как следствие, нуждающиеся в изменении параметров развёртывания IBM Trusteer Pinpoint Detect, должны приобрести услугу IBM Trusteer Pinpoint Detect Redeployment.

Повторное развёртывание может потребоваться в случае изменения клиентом URL хоста или домена Приложения, перевода Приложения на новую технологию, перехода на новую платформу онлайн-банкинга или добавления нового процесса входа в систему для имеющегося Приложения.

В течение переходного периода повторного развёртывания продолжительностью в 6 месяцев Клиент имеет право развёртывать дополнительные Приложения по схеме «один к одному» на базе Приложений, на которые уже приобретена подписка.

1.3.2 IBM Trusteer Pinpoint Malware Detection Redeployment

Клиенты, повторно развёртывающие свои Приложения для онлайн-банкинга в течение срока оказания услуги и, как следствие, нуждающиеся в изменении параметров развёртывания IBM Trusteer Pinpoint Malware Detection II, должны приобрести услугу IBM Trusteer Pinpoint Malware Detection Redeployment.

Повторное развёртывание может потребоваться в случае изменения Клиентом URL хоста или домена Приложения, перевода Приложения на новую технологию, перехода на новую платформу онлайн-банкинга или добавления нового процесса входа в систему для имеющегося Приложения.

В течение переходного периода повторного развёртывания продолжительностью в 6 месяцев Клиент имеет право развёртывать дополнительные Приложения по схеме «один к одному» на базе Приложений, на которые уже приобретена подписка.

В отношении IBM Trusteer Pinpoint Malware Detection Additional Applications для IBM Trusteer Pinpoint Malware Detection II Standard Edition или IBM Trusteer Pinpoint Malware Detection II Advanced Edition развёртывание дополнительных Приложений сверх первого Приложения требует наличия разрешения на IBM Trusteer Pinpoint Malware Detection Additional Applications.

1.3.3 IBM Trusteer Pinpoint Criminal Detection Redeployment

Клиенты, повторно развёртывающие свои Приложения для онлайн-банкинга в течение срока оказания услуги и, как следствие, нуждающиеся в изменении параметров развёртывания Облачной Услуги IBM Trusteer Pinpoint Criminal Detection, должны приобрести услугу IBM Trusteer Pinpoint Criminal Detection Redeployment.

Повторное развёртывание может потребоваться в случае изменения Клиентом URL хоста или домена Приложения, перевода Приложения на новую технологию, перехода на новую платформу онлайн-банкинга или добавления нового процесса входа в систему для имеющегося Приложения.

В течение переходного периода повторного развёртывания продолжительностью в 6 месяцев Клиент имеет право развёртывать дополнительные Приложения по схеме «один к одному» на базе Приложений, на которые уже приобретена подписка.

2. Обработка и защита Данных – Спецификации

Дополнение IBM об Обработке Данных (DPA), приведённое на веб-странице http://ibm.com/dpa, и Спецификации обработки и защиты данных (именуемые спецификациями или Приложениями к DPA), ссылки на которые приводятся ниже, содержат дополнительную информацию о защите данных в Облачных Услугах и её вариантах в зависимости от типа Содержимого, подлежащего обработке, применяемых операциях обработки, функциях защиты данных и особенностях сохранения и возврата Содержимого. DPA применяется к персональным данным, входящим в Содержимое, в том случае, если, и в той мере, в какой применяются i) Общеевропейский регламент о защите персональных данных (GDPR) (EU/2016/679); или ii) другие законы о защите данных, указанные на веб-странице http://ibm.com/dpa/dpl.

Следует пояснить, что в Спецификациях, как правило, перечислены все площадки, на которых IBM (включая всех сторонних подрядчиков по обработке) размещает и обрабатывает Персональные Данные — безотносительно центра обработки данных, в котором проводится развёртывание данных услуг. Список площадок, на которых осуществляются размещение и обработка данных для конкретного центра обработки данных, на базе которого развёртываются услуги, приведён в Разделе 5.2 ниже (Дополнительная информация о площадках обработки).

IBM Trusteer Pinpoint Criminal Detect

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402489853624

IBM Trusteer Pinpoint Detect

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=3D3DA0C0E5F711E5A3808DA17FABE9B1

IBM Trusteer Pinpoint Malware Detection

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402489595035

IBM Trusteer Mobile SDK

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492847439

3. Уровни обслуживания и Техническая поддержка

3.1 Соглашение об уровне обслуживания

IBM предоставляет Клиенту следующее соглашение об уровне обслуживания в отношении доступности услуг (SLA). IBM будет применять наивысший применимый размер компенсации на основе совокупных показателей доступности Облачной Услуги в соответствии с нижеприведённой таблицей. Показатель доступности в процентах вычисляется как общее число минут за договорной месяц минус общее число минут Простоя Услуги за договорной месяц, делённое на общее число минут в договорном месяце. Определение Простоя Услуги, процесс подачи претензий и способы информирования IBM о проблемах с доступностью услуги приводятся в справочнике по поддержке Облачных Услуг IBM, который можно найти на веб-странице по адресу: https://www.ibm.com/software/support/saas_support_overview.html.

Доступность	Кредит (% месячной платы за подписку*)
Менее 99,9%	2%
Менее 99,0%	5%
Менее 95,0%	10%

* Плата за подписку - это договорная цена за месяц, являющийся предметом претензии.

3.2 Техническая поддержка

Информацию о Технической поддержке для Облачной Услуги, включая контактные данные службы поддержки, уровни серьёзности, часы работы, время ответа и другие сведения о поддержке и применимых процессах, можно найти, выбрав раздел "Облачная Услуга" в руководстве IBM по поддержке, доступном на веб-странице по адресу https://www.ibm.com/support/home/pages/support-guide/.

Поддержка класса Premium:

Подписка на Поддержку класса Premium доступна для Облачной Услуги за дополнительную плату и включает следующее:

- Круглосуточная поддержка (в режиме 24x7) для проблем всех уровней серьёзности.
- Клиенты могут обращаться в службу поддержки непосредственно по телефону и путём запроса обратного вызова (когда служба поддержки связывается с Клиентом).
- Клиенты и их Соответствующие критериям Участники могут подавать заявки в службу поддержки в электронной форме - подробное описание приводится в Руководстве по поддержке для SaaS.
- Клиенты могут использовать Портал поддержки Клиентов для получения уведомлений, документов, описаний примеров использования, ответов на часто задаваемые вопросы: http://www.ibm.com/software/security/trusteer/support/.

4. Платежи

4.1 Системы расчёта оплаты

Системы расчёта оплаты для Облачной Услуги указываются в Документе по Транзакции.

К данной Облачной Услуге применяются следующие системы расчёта оплаты:

- Поручение – это профессиональные услуги или услуги по обучению, связанные с Облачными Услугами.

- Соответствующий критериям Участник - это физическое или юридическое лицо, имеющее право участвовать в любой программе предоставления услуг, которой управляют или которую отслеживают Облачные Услуги.
- Приложение – это компьютерная программа с уникальным именем, которая разработана с помощью Облачных Услуг, доступ к которой предоставляется через Облачные Услуги или которая используется Облачными Услугами.
- API-вызов - это обращение к Облачным Услугам через программный интерфейс.
- Соединение – это связь с базой данных, приложением, сервером или устройством любого другого типа, которые были или становятся доступными для Облачных Услуг.

4.2 Плата за дистанционные услуги

Срок действия дистанционной услуги истекает через 90 дней с момента приобретения независимо от того, была ли использована дистанционная услуга.

5. Дополнительные положения

К Соглашениям об Облачных Услугах (или эквивалентным базовым соглашениям об облачных инфраструктурах), заключённым до 1 января 2019 года, применяются положения, приведённые на веб-странице https://www.ibm.com/acs.

5.1 EULA и основание для обработки данных Субъектов Персональных Данных

Для Облачных Услуг IBM Trusteer Rapport (включая Rapport Remediation или Rapport for Mitigation при развёртывании в связи с Облачными Услугами Pinpoint): если не согласованы другие условия, и согласно основанию для обработки, самостоятельно установленному Клиентом, Клиент уполномочивает IBM предоставить Лицензионное соглашение с конечными пользователями, доступное на веб-странице https://trusteer.secure.force.com/PKB/articles/en_US/FAQ/RAPPORT-DATA-PRIVACY-NOTICE-AND-END-USER-LICENSE-AGREEMENT-EULA, для получения компанией IBM разрешения на сбор и обработку информации, необходимой для предоставления Облачных Услуг.

В отношении Облачных Услуг IBM Trusteer Rapport Клиент даёт разрешение IBM как обработчику данных Спонсирующего Предприятия использовать Программу для сбора вредоносного ПО и следов функционирования вредоносного ПО, то есть файлов, связанных со злонамеренной деятельностью, или файлов, связанных с необычным и неправильным функционированием Программы. IBM не будет использовать Программу для воздействия на файлы с персональной информацией конечного пользователя, однако собранные файлы могут содержать персональные данные, которые получены вредоносным ПО без разрешения конечного пользователя. IBM обязуется 1) немедленно удалять любые файлы, не относящиеся к такому анализу, и 2) сохранять имеющие отношение к этому процессу файлы только на период проведения анализа и ни в коем случае не дольше, чем в течение трёх месяцев.

5.2 Дополнительная информация о площадках обработки

Размещение и обработка Персональных Данных, в том числе любыми сторонними подрядчиками обработчика, указанными в Спецификации, будут осуществляться согласно следующему списку:

Для всех услуг, предоставляемых через центр обработки данных в Германии, IBM ограничит размещение и обработку Персональных Данных страной, где находится организация IBM, заключившая договор, и следующими странами: Германия, Израиль, Ирландия и Нидерланды.

Для всех услуг, предоставляемых через центр обработки данных в Японии, IBM ограничит размещение и обработку Персональных Данных страной, где находится организация IBM, заключившая договор, и следующими странами: Япония, Израиль и Ирландия.

Для всех услуг, предоставляемых через центр обработки данных в США, IBM ограничит размещение и обработку Персональных данных страной, где находится организация IBM, заключившая договор, и следующими странами: США, Израиль, Ирландия, Сингапур и Австралия.

В дополнение к вышеуказанным площадкам в отношении всех услуг, предоставляемых через центры обработки данных в Германии, Японии и США, (1) данные поддержки могут размещаться и обрабатываться в Германии и Франции компанией Salesforce.Com как сторонним подрядчиком IBM и (2) для клиентов, давших согласие на отправку данных поставщикам Информации о мобильных номерах, Персональные Данные могут размещаться и обрабатываться в странах соответствующих

сторонних подрядчиков, указанных в Спецификации. Несмотря на любую противоречащую этому информацию в Спецификации, сторонние подрядчики, указанные в положении (2) предыдущего предложения, могут не соответствовать требованиям стандартов ISO 27001 и SOC2.

Услуги поддержки и обслуживания заказчиков IBM Trusteer также могут предоставляться по мере необходимости в случае доступности необходимого персонала IBM, площадки Клиента и центра обработки данных, в котором размещаются данные.

5.3 Данные Владельцев Учётных записей

Во избежание разночтений: если с Клиентским ПО Владельца Учётной записи, принадлежащим конкретному Владельцу Учётной записи, связано несколько заказчиков IBM («Аффилированные Заказчики») и услуги, охватываемые настоящим Описанием Услуги, предоставляются компанией IBM таким Аффилированным Заказчикам через центры обработки данных в разных регионах, то данные Владельца Учётной записи могут обрабатываться на любых и всех площадках, связанных с каждым из таких центров обработки данных, как указано в Разделе 5.2 выше.

5.4 Интегрированные решения

Во избежание разночтений: разнообразные предложения под маркой Trusteer могут образовывать интегрированное решение. Поэтому, если Клиент прекратит пользоваться любыми из этих Облачных Услуг, IBM может сохранить данные Клиента в целях предоставления Клиенту остальных Облачных Услуг, охватываемых данным Описанием Услуги, а также других услуг Trusteer, охватываемых описаниями услуг, применимыми к другим услугам Trusteer.

5.5 Поддерживающее программное обеспечение

В Облачную Услугу входит следующее Поддерживающее Программное обеспечение:

- IBM Rapport Agents

5.6 Лучшие методы работы с Pinpoint

В случае обнаружения вредоносного ПО или мошеннического использования учётной записи Клиент должен следовать рекомендациям из Руководства по лучшим методам работы с Pinpoint. Не следует использовать Облачные Услуги IBM Trusteer Pinpoint Detect каким-либо способом, который повлияет на работу Соответствующего критериям Участника сразу после обнаружения вредоносного ПО или мошеннического использования учётной записи, таким образом чтобы другие пользователи могли связать действия Клиента с использованием предложений IBM Trusteer Pinpoint Detect (например, уведомления, сообщения, блокирование устройств или блокирование доступа к Приложению для Бизнеса и/или для Розничной торговли сразу же после обнаружения вредоносного ПО или мошеннического использования учётной записи).

5.7 Данные, собранные в ходе развёртывания

В ходе развёртывания Облачной Услуги Клиент может предоставлять IBM определённые данные. Такие данные не должны включать информацию, которая может идентифицировать или которая может быть соотнесена с конкретными физическими лицами. Подробные правила, согласно которым компании IBM предоставляются данные в процессе развёртывания, изложены в документе «Рекомендации по развёртыванию Trusteer», который должен быть предоставлен Клиенту.

6. Условия, имеющие преимущественную силу

6.1 Использование данных

Несмотря ни на какие противоречащие положения раздела "Содержимое и защита данных" базовых условий соглашения об Облачной Услуге между сторонами, преимущественную силу имеют следующие положения: IBM не будет использовать и раскрывать результаты использования Облачной Услуги Клиентом, являющиеся уникальными для Содержимого Клиента (Аналитические данные) или иным образом идентифицирующие Клиента. Однако IBM будет использовать Содержимое и другую информацию, полученную из Содержимого (за исключением Аналитических данных) в ходе предоставления Облачной Услуги, для усовершенствования Облачной Услуги. IBM может также распространять информацию об идентификаторах угроз и другие сведения о безопасности, которые есть в Содержимом, в целях обнаружения угроз и защиты от них.