IBM Trusteer Fraud Protection

Essa Descrição de Serviço descreve o Serviço em Nuvem que a IBM fornece ao Cliente. Cliente significa a parte contratante, bem como seus usuários autorizados e destinatários do Serviço em Nuvem. A Cotação e o Certificado de Titularidade (PoE - Proof of Entitlement) aplicáveis são fornecidos como Documentos de Transação.

1. Serviço em Nuvem

Os Serviços em Nuvem a seguir são cobertos por esta Descrição de Serviço:

Serviços em Nuvem Pinpoint Assure:

- IBM Trusteer Pinpoint Assure
- IBM Trusteer Pinpoint Assure Application
- IBM Trusteer Mobile Carrier Intelligence

Serviços em Nuvem Rapport:

- IBM Trusteer Rapport for Business Premium Support
- IBM Trusteer Rapport for Retail Premium Support
- IBM Trusteer Rapport II for Business
- IBM Trusteer Rapport II for Retail
- IBM Trusteer Rapport Fraud Feeds for Business
- IBM Trusteer Rapport Fraud Feeds for Business Premium Support
- IBM Trusteer Rapport Fraud Feeds for Retail
- IBM Trusteer Rapport Fraud Feeds for Retail Premium Support
- IBM Trusteer Rapport Phishing Protection for Business
- IBM Trusteer Rapport Phishing Protection for Business Premium Support
- IBM Trusteer Rapport Phishing Protection for Retail
- IBM Trusteer Rapport Phishing Protection for Retail Premium Support
- IBM Trusteer Rapport Mandatory Service for Business
- IBM Trusteer Rapport Mandatory Service for Retail
- IBM Trusteer Rapport Additional Applications for Retail
- IBM Trusteer Rapport Additional Applications for Business
- IBM Trusteer Rapport Large Redeployment
- IBM Trusteer Rapport Small Redeployment

Serviços em Nuvem Pinpoint:

- IBM Trusteer Pinpoint Malware Detection Standard Edition for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail Premium Support
- IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail Premium Support
- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Rapport Remediation for Retail Premium Support
- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Rapport Remediation for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business

- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Business
- IBM Trusteer Pinpoint Malware Detection Redeployment
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business
- IBM Trusteer Rapport for Mitigation for Retail
- IBM Trusteer Rapport for Mitigation for Retail Premium Support
- IBM Trusteer Rapport for Mitigation for Business
- IBM Trusteer Rapport for Mitigation for Business Premium Support
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Standard Redeployment
- IBM Trusteer Pinpoint Detect Premium Redeployment
- IBM Trusteer Pinpoint Detect Standard for Retail Premium Support
- IBM Trusteer Digital Content Pack for Retail
- IBM Trusteer Digital Content Pack for Business
- IBM Trusteer New Account Fraud for Business
- IBM Trusteer New Account Fraud for Retail
- IBM Trusteer Project Management and Consultancy Services
- IBM Trusteer Security Research Consultancy Services
- IBM Trusteer Training Services
- IBM Trusteer Pinpoint Detect Standard Application
- IBM Trusteer Pinpoint Detect Premium Application
- IBM Trusteer Pinpoint Detect Standard
- IBM Trusteer Pinpoint Detect Premium
- IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect
- IBM Trusteer Pinpoint Verify

Serviços em Nuvem para Dispositivo Móvel:

- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile SDK for Retail

1.1 Serviços em Nuvem de Business e de Retail

Os Serviços em Nuvem IBM Trusteer são concedidos para uso com tipos específicos de Aplicativos. Um Aplicativo é definido como um dos tipos a seguir: Retail ou Business. Ofertas distintas estão disponíveis para Aplicativos de Retail e Aplicativos de Business.

a. Um Aplicativo de Retail é definido como um aplicativo bancário on-line, aplicativo de dispositivo móvel ou aplicativo de comércio eletrônico (e-commerce) projetado para atender consumidores. A política do Cliente pode classificar determinadas empresas de pequeno porte como elegíveis para acesso de retail.

b. Um Aplicativo de Business é definido como um aplicativo bancário on-line, aplicativo de dispositivo móvel ou aplicativo de comércio eletrônico (e-commerce) projetado para atender entidades corporativas, institucionais ou equivalentes, ou qualquer aplicativo que não seja categorizado como de Retail.

1.1.1 Serviços em Nuvem de Business

- IBM Trusteer Rapport II for Business
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Digital Content Pack for Business
- IBM Trusteer New Account Fraud for Business
- IBM Trusteer Mobile SDK for Business

1.1.2 Serviços em Nuvem de Retail

- IBM Trusteer Rapport II for Retail
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Digital Content Pack for Retail
- IBM Trusteer New Account Fraud for Retail
- IBM Trusteer Mobile SDK for Retail

Para cada um dos Serviços em Nuvem de Business e de Retail, há um produto de Suporte Premium associado disponível mediante o pagamento de um encargo adicional, com a exceção dos Serviços em Nuvem do IBM Trusteer Mobile SDK.

1.1.3 Serviços adicionais para o IBM Trusteer Rapport II

a. Serviços em Nuvem adicionais disponíveis para o IBM Trusteer Rapport II for Business:
   - IBM Trusteer Rapport Fraud Feeds for Business
   - IBM Trusteer Rapport Phishing Protection for Business
   - IBM Trusteer Rapport Mandatory Service for Business
   - IBM Trusteer Rapport Additional Applications for Business

b. Serviços em Nuvem adicionais disponíveis para o IBM Trusteer Rapport II for Retail:
   - IBM Trusteer Rapport Fraud Feeds for Retail
   - IBM Trusteer Rapport Phishing Protection for Retail
   - IBM Trusteer Rapport Mandatory Service for Retail
   - IBM Trusteer Rapport Additional Applications For Retail

Para cada um dos complementos de Business e Retail para Serviços em Nuvem IBM Trusteer Rapport, exceto para os complementos do IBM Trusteer Rapport Mandatory Service, há um produto de Suporte Premium associado disponível mediante o pagamento de um encargo adicional.

A subscrição do IBM Trusteer Rapport II for Business ou do IBM Trusteer Rapport II for Retail é um pré-requisito dos Serviços em Nuvem associados adicionais listados nesta seção.

1.1.4 Serviços em Nuvem adicionais para o IBM Trusteer Pinpoint Malware Detection II

a. Serviços em Nuvem adicionais disponíveis para o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business ou IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business:
   - IBM Trusteer Rapport Remediation for Business

- IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

b. Serviços em Nuvem adicionais disponíveis para o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail ou IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail:

- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail

O Suporte Premium está disponível para ofertas específicas conforme especificado neste documento. A subscrição do IBM Trusteer Pinpoint Malware Detection II for Business ou do IBM Trusteer Pinpoint Malware Detection II for Retail é um pré-requisito dos Serviços em Nuvem associados adicionais listados nesta seção.

1.1.5 Serviços em Nuvem adicionais disponíveis para o IBM Trusteer Pinpoint Detect Standard e/ou IBM Trusteer Pinpoint Detect Premium e/ou IBM Trusteer Pinpoint Detect Standard for Retail e/ou IBM Trusteer Pinpoint Detect Premium for Retail e/ou IBM Trusteer Pinpoint Detect Standard for Business e/ou IBM Trusteer Pinpoint Detect Premium for Business

a. Serviços em Nuvem adicionais disponíveis para o IBM Trusteer Detect Standard for Business e/ou IBM Trusteer Pinpoint Detect Premium for Business:

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business
- IBM Trusteer Digital Content Pack for Business
- IBM Trusteer New Account Fraud for Business

b. Serviços em Nuvem adicionais disponíveis para o IBM Trusteer Detect Standard for Retail e/ou IBM Trusteer Pinpoint Detect Premium for Retail:

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail
- IBM Trusteer Digital Content Pack for Retail
- IBM Trusteer New Account Fraud for Retail

c. Serviços disponíveis para o IBM Trusteer Pinpoint Detect Standard e/ou IBM Trusteer Pinpoint Premium:

- IBM Trusteer Pinpoint Detect Standard Application
- IBM Trusteer Pinpoint Detect Premium Application

d. Serviços em Nuvem adicionais disponíveis para o IBM Trusteer Pinpoint Detect Premium

- IBM Trusteer Pinpoint Verify

A subscrição para o IBM Trusteer Pinpoint Detect Standard ou IBM Trusteer Pinpoint Detect Premium ou IBM Trusteer Pinpoint Detect Standard for Retail ou IBM Trusteer Pinpoint Detect Premium for Retail ou IBM Trusteer Pinpoint Detect Standard for Business ou IBM Trusteer Pinpoint Detect Premium for Business é um pré-requisito para os Serviços em Nuvem adicionais associados listados nesta seção.

1.1.6 Outros Serviços em Nuvem adicionais

Qualquer subscrição adicional de Serviços em Nuvem para as subscrições básicas acima que não esteja listada no presente documento, nem esteja atualmente disponível ou em desenvolvimento, não é considerada uma atualização e deve ser concedida separadamente.

1.2 Definições

Titular da Conta – significa o usuário final do Cliente, que instalou o software de ativação do cliente, aceitou o contrato de licença de usuário final (EULA - End User License Agreement) e autenticou pelo menos uma vez com o Aplicativo de Retail ou de Business do Cliente para o qual o Cliente subscreveu a cobertura de Serviços em Nuvem.

Software Cliente do Titular da Conta – refere-se ao software de ativação do cliente IBM Trusteer Rapport ou a qualquer outro software de ativação do cliente que seja fornecido com alguns Serviços em Nuvem para a instalação no dispositivo do usuário final.

Trusteer Splash – refere-se ao splash que é fornecido para o Cliente com base nos modelos de splash disponíveis.

Página de Entrada – refere-se à página hospedada pela IBM que é fornecida para o Cliente com o splash do Cliente e o Software Cliente do Titular da Conta transferível por download.

1.3 Serviços em Nuvem do IBM Trusteer Rapport

1.3.1 IBM Trusteer Rapport II for Retail e/ou IBM Trusteer Rapport II for Business ("Trusteer Rapport II")

O Serviço em Nuvem do Trusteer Rapport II é uma nova construção do IBM Trusteer Rapport para ajudar a padronizar encargos relacionados à proteção de diversos Aplicativos e substitui encargos únicos ao incluir Aplicativos.

O Trusteer Rapport II fornece uma camada de proteção contra ataques de phishing e de malware Man-in-the-Browser (MitB). Usando uma rede de dezenas de milhões de terminais em todo o mundo, o IBM Trusteer Rapport coleta inteligência sobre ataques ativos de phishing e malware contra organizações no mundo inteiro. O IBM Trusteer Rapport aplica algoritmos comportamentais destinados a bloquear ataques de phishing e evitar a instalação e a operação de variantes de malware MitB.

Esse Serviço em Nuvem está autorizado sob a métrica de encargo de Participante Elegível ou sob a métrica de encargo de Dispositivo Cliente. A oferta para Business é vendida em pacotes de 10 Participantes Elegíveis ou 10 Dispositivos Cliente. A oferta para Retail é vendida em pacotes de 100 Participantes Elegíveis ou 100 Dispositivos Cliente.

Essa oferta de Serviço em Nuvem inclui:

a. Trusteer Management Application ("TMA"):

   O TMA é disponibilizado no ambiente hospedado na nuvem do IBM Trusteer por meio do qual o Cliente (e um número ilimitado de sua equipe autorizada) pode: (i) visualizar e fazer download de relatórios de dados de avaliações de risco de determinados eventos e (ii) visualizar a configuração do software de ativação do cliente licenciado para Participantes Elegíveis do Cliente sob um contrato de licença de usuário final ("EULA") sem encargos e disponibilizado para download nos desktops ou nos dispositivos (PC/MACs) dos Participantes Elegíveis, também conhecido como o suite de software Trusteer Rapport ("Software Cliente do Titular da Conta"). O Cliente pode disponibilizar o Software Cliente do Titular da Conta apenas usando o Trusteer Splash ou Rapport API e o Cliente não pode usar o Software Cliente do Titular da Conta para suas operações internas de Business ou para uso de seus funcionários (exceto para uso pessoal dos funcionários).

b. Script da Web:

   Para acesso em um website para o propósito de acessar ou usar o Serviço em Nuvem.

c. Dados de eventos:

   O Cliente (e um número ilimitado de sua equipe autorizada) pode usar o TMA para receber os dados de eventos gerados a partir do Software Cliente do Titular da Conta resultantes das interações on-line dos Titulares da Conta com seu Aplicativo de Business ou de Retail para o qual o Cliente subscreveu a cobertura de Serviços em Nuvem. Dados de eventos serão recebidos a partir do Account Holder Client Software dos Participantes Elegíveis que está em execução em seus dispositivos, que aceitaram o EULA, e autenticaram com o Aplicativo de Business ou de Retail do Cliente pelo menos uma vez, e a configuração do Cliente deve incluir a coleta de IDs do usuário.

d. Trusteer Splash:

   A plataforma de marketing Trusteer Splash identifica e oferece o Software Cliente do Titular da Conta a Participantes Elegíveis que estiverem acessando Aplicativos de Business e/ou Retail do Cliente para os quais o Cliente subscreveu a cobertura de Serviços em Nuvem. O Cliente pode selecionar dentre os Modelos Splash disponíveis. Splashs customizados podem ser contratados sob um contrato ou descrição de trabalho separado.

O Cliente pode concordar em fornecer suas marcas comerciais, logotipos ou ícones para uso em conexão com o TMA e apenas para utilização com o Trusteer Splash e para exibição no Software Cliente do Titular da Conta ou nas páginas de entrada hospedadas pela IBM e no website do IBM Trusteer. Qualquer uso de suas marcas comerciais, logotipos ou ícones fornecidos estará de acordo com políticas razoáveis da IBM com relação à publicidade e ao uso da marca comercial.

O Cliente deve subscrever o Serviço em Nuvem do IBM Trusteer Rapport Mandatory Service se desejar empregar qualquer tipo de implementação obrigatória no Software Cliente do Titular da Conta.

A implementação obrigatória do Software Cliente do Titular da Conta inclui, mas não está limitada a qualquer tipo de implementação obrigatória por qualquer mecanismo ou meio que obrigue, direta ou indiretamente, um Participante Elegível a fazer download do Software Cliente do Titular da Conta, ou qualquer outro método, ferramenta, procedimento, acordo ou mecanismo, não criado por ou aprovado pela IBM, criado para efetuar um bypass dos requisitos de licenciamento desta implementação obrigatória do Software Cliente do Titular da Conta.

O Trusteer Rapport II for Business e/ou o Trusteer Rapport II for Retail incluem proteção para um Aplicativo. Para cada Aplicativo adicional, o Cliente deve obter a autorização do IBM Trusteer Rapport Additional Applications.

1.3.2 Serviços em Nuvem Adicionais Opcionais para o IBM Trusteer Rapport II for Business e/ou IBM Trusteer Rapport II for Retail

A subscrição do IBM Trusteer Rapport II Cloud Services é um pré-requisito para a subscrição de qualquer um dos seguintes Serviços em Nuvem. Se o Serviço em Nuvem for designado como "for Business", então, os Serviços em Nuvem adicionais adquiridos também devem ser designados como "for Business". O Cliente receberá dados de evento dos Participantes Elegíveis ou Dispositivos Cliente que executam o Software Cliente do Titular da Conta e que aceitaram o EULA e se autenticaram com os Aplicativos de Business e/ou Retail do Cliente pelo menos uma vez e, nesse caso, a configuração do Cliente deve incluir a coleta de IDs de Usuário. O Cliente receberá dados de evento dos Participantes Elegíveis ou Dispositivos do Cliente que executam o Software Cliente do Titular da Conta e que aceitaram o EULA e se autenticaram com os Aplicativos de Negócios e/ou de Varejo do Cliente pelo menos uma vez e, nesse caso, a configuração do Cliente deve incluir a coleta de IDs de Usuário.

1.3.3 IBM Trusteer Rapport Fraud Feeds for Business e/ou IBM Trusteer Rapport Fraud Feeds for Retail

Ao subscrever esse Serviço em Nuvem complementar, o Cliente (e um número ilimitado de membros da sua equipe autorizada) pode usar o TMA para visualizar, subscrever e configurar a entrega de feeds de ameaça gerados a partir do Serviço em Nuvem do Trusteer Rapport. Feeds podem ser enviados por e-mail a endereços de e-mail designados ou por SFTP como arquivos de texto.

Essa oferta é aplicável somente sob a métrica de encargo de Participante Elegível.

1.3.4 IBM Trusteer Rapport Phishing Protection for Business e/ou IBM Trusteer Rapport Phishing Protection for Retail

O Cliente (e um número ilimitado de sua equipe autorizada) pode usar o TMA para receber notificações de dados de eventos relacionados ao envio das credenciais de login do Titular da Conta para um site suspeito de prática de phishing ou potencialmente fraudulento. Aplicativos on-line legítimos (URLs) podem ser erroneamente sinalizados como sites de phishing e o Serviço em Nuvem pode alertar os Titulares de Conta que um site legítimo é um site de phishing. Nesse caso, o Cliente deverá notificar a IBM sobre tal erro, e a IBM deve corrigir o erro. Essa deverá ser a única solução do Cliente para tal erro.

Esse Serviço em Nuvem está autorizado sob a métrica de encargo de Participante Elegível ou sob a métrica de encargo de Dispositivo Cliente. A oferta de Business é vendida em pacotes de 10 Participantes Elegíveis ou 10 Dispositivos Cliente. A oferta de Retail é vendida em pacotes de 100 Participantes Elegíveis ou 100 Dispositivos Cliente.

O suporte premium pode ser obtido para esses serviços em nuvem, sob a métrica de encargo de Participante Elegível ou sob a métrica de encargo de Dispositivo Cliente. A oferta de negócios é vendida em pacotes de 10 Participantes Elegíveis ou 10 Dispositivos Cliente. A oferta de varejo é vendida em pacotes de 100 Participantes Elegíveis ou 100 Dispositivos Cliente.

1.3.5 IBM Trusteer Rapport Mandatory Service for Business e/ou IBM Trusteer Rapport Mandatory Service for Retail

O Cliente pode usar uma instância da plataforma de marketing Trusteer Splash para impor o download do Software Cliente do Titular da Conta aos Participantes Elegíveis acessando Aplicativos de Business e/ou Retail do Cliente para os quais o Cliente subscreveu cobertura de Serviços em Nuvem.

O IBM Trusteer Rapport Premium Support for Business é um pré-requisito para o IBM Security Rapport Mandatory Service for Business.

O IBM Trusteer Rapport Premium Support for Retail é um pré-requisito para o IBM Security Rapport Mandatory Service for Retail.

O Cliente pode implementar a funcionalidade adicional do IBM Trusteer Rapport Mandatory Service somente se ela foi solicitada e configurada para uso com o Aplicativo de Retail ou de Business do Cliente para o qual o Cliente subscreveu a cobertura de Serviços em Nuvem.

Esse Serviço em Nuvem está autorizado sob a métrica de encargo de Participante Elegível. A oferta para Business é vendida em pacotes de 10 Participantes Elegíveis. A oferta para Retail é vendida em pacotes de 100 Participantes Elegíveis.

1.3.6 IBM Trusteer Rapport Large Redeployment e/ou IBM Trusteer Rapport Small Redeployment

Os Clientes, que estiverem reimplementando seus Aplicativos bancários on-line durante o período de vigência do serviço e, consequentemente, precisarem de mudanças em sua implementação do IBM Trusteer Rapport II, deverão comprar o Serviço em Nuvem do IBM Trusteer Rapport Redeployment.

A reimplementação pode ser devido à mudança do domínio ou da URL do host do Aplicativo, à aplicação de mudanças à configuração de splash ou à mudança para uma nova plataforma bancária on-line pelo Cliente.

Pelo período de transição da reimplementação de seis meses, o Cliente tem autorização para Aplicativos adicionais na base de um para um em execução além dos Aplicativos já subscritos.

O IBM Trusteer Rapport Large Redeployment se aplica a ambientes com mais de 20.000 usuários e o IBM Trusteer Rapport Small Redeployment se aplica a ambientes com 20.000 usuários ou menos.

1.3.7 IBM Trusteer Rapport Additional Applications for Business e/ou IBM Trusteer Rapport Additional Applications for Retail

Para o IBM Trusteer Rapport II for Business, a implementação em qualquer Aplicativo de Business adicional além do primeiro Aplicativo requer a autorização do Serviço em Nuvem do IBM Trusteer Rapport Additional Applications for Business. Para o IBM Trusteer Rapport II for Retail, a implementação em qualquer Aplicativo de retail adicional além do primeiro Aplicativo requer a autorização do Serviço em Nuvem do IBM Trusteer Rapport Additional Applications for Retail.

1.4 Serviços em Nuvem do IBM Trusteer Pinpoint

O IBM Trusteer Pinpoint é um serviço baseado em nuvem que é projetado para fornecer outra camada de proteção e destina-se a detectar e mitigar ataques de malware, phishing e controle de conta (account take over). O Trusteer Pinpoint pode ser integrado a Aplicativos de Business e/ou Retail do Cliente para os quais o Cliente subscreveu a cobertura de Serviços em Nuvem e processos de prevenção de fraude.

Esse Serviço em Nuvem inclui:

a. TMA:

   O TMA é disponibilizado no ambiente hospedado na nuvem do IBM Trusteer por meio do qual o Cliente (e um número ilimitado de sua equipe autorizada) pode: (i) visualizar e fazer download de relatórios de dados de avaliações de risco de determinados eventos e (ii) visualizar, subscrever e configurar a entrega de feeds de ameaça gerados a partir das ofertas Pinpoint.

b. Script da Web e/ou APIs:

   Para implementação em um website para os propósitos de acesso ou uso do Serviço em Nuvem.

1.4.1 IBM Trusteer Pinpoint Malware Detection

No caso de detecção de malware nos Serviços em Nuvem do IBM Trusteer Pinpoint Malware Detection II, o Cliente deve seguir o Guia de Melhores Práticas do Pinpoint. O Cliente não deve usar os Serviços em Nuvem do IBM Trusteer Pinpoint Malware Detection II de qualquer maneira que afete a experiência do Participante Elegível imediatamente após uma detecção de malware ou de controle de conta (account take over), de forma que permita que outros vinculem ações do Cliente ao uso de Serviços em Nuvem do IBM Trusteer Pinpoint (por exemplo, notificações, mensagens, bloqueio de dispositivos ou bloqueio de acesso ao Aplicativo de Business e/ou Retail imediatamente após uma detecção de malware ou de controle de conta).

1.4.2 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business e/ou o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail e/ou o IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business e/ou o IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

O IBM Security Pinpoint Malware Detection II é uma reformulação do IBM Trusteer Pinpoint Malware Detection para ajudar a padronizar encargos relacionados à proteção de diversos Aplicativos e substitui os encargos únicos ao adicionar Aplicativos.

Detecção sem ação do Cliente (Clientless) nos navegadores infectados por malware financeiro Man in the Browser (MitB) se conectando a um Aplicativo de Business e/ou Retail. Os Serviços em Nuvem IBM Trusteer Pinpoint Malware Detection fornecem outra camada de proteção e destinam-se a permitir que as organizações se concentrem nos processos de prevenção de fraude com base no risco de malware, através do fornecimento ao Cliente de avaliações e alertas de presença do malware financeiro MitB.

a. Dados de eventos:

   O Cliente (e um número ilimitado de sua equipe autorizada) pode usar o TMA para receber dados de eventos gerados como um resultado das interações online dos Participantes Elegíveis com o(s) Aplicativo(s) de Business e/ou Retail do Cliente.

b. Advanced Edition:

   As ofertas Advanced Editions para Business e/ou Retail oferecem uma camada adicional de detecção e proteção que é ajustada e customizada para a estrutura e o fluxo dos Aplicativos de Business e/ou Retail do Cliente, e podem ser customizadas para o cenário de ameaça específico visando o Cliente. Elas podem ser incorporadas em diversos locais nos Aplicativos de Business e/ou Retail do Cliente.

   A Advanced Edition é oferecida ao Cliente em quantidades mínimas de pelo menos 100 mil Participantes Elegíveis de Retail ou 10 mil Participantes Elegíveis de Business, com 1000 pacotes de 100 Participantes Elegíveis para Retail ou 1000 pacotes de 10 Participantes Elegíveis para Business.

c. Standard Edition:

   As Standard Editions para Business e/ou para Retail são soluções de rápida implementação que fornecem a principal funcionalidade desse Serviço em Nuvem, conforme descrito no presente documento.

Esse Serviço em Nuvem inclui proteção de um Aplicativo. Para cada Aplicativo adicional, o Cliente deve obter a autorização do IBM Trusteer Pinpoint Malware Detection Additional Applications.

1.4.3 Serviços em Nuvem Adicionais Opcionais para o IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail e/ou IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail e/ou IBM Pinpoint Trusteer Pinpoint Malware Detection Standard Edition II for Business e/ou IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business

- Para o Serviço em Nuvem IBM Trusteer Rapport Remediation for Retail, existe um pré-requisito do IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail ou IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.
- Para o Serviço em Nuvem IBM Trusteer Rapport Remediation for Business, existe um pré-requisito do IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business ou IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.

1.4.4 IBM Trusteer Rapport Remediation for Retail e/ou IBM Trusteer Rapport Remediation for Business

O IBM Trusteer Rapport Remediation Retail e o IBM Trusteer Rapport Remediation for Business têm como foco investigar, corrigir, bloquear e remover infecções de malware man-in-the-browser (MitB) de dispositivos (PC/MACs) infectados de Participantes Elegíveis do Cliente que acessam o Aplicativo do Cliente de forma ad hoc em que infecções de malware MitB foram detectadas por dados de eventos do IBM Trusteer Pinpoint Malware Detection. O Cliente deve ter uma subscrição vigente para o IBM Trusteer Pinpoint Malware Detection II efetivamente em execução no Aplicativo do Cliente. O Cliente pode usar essa oferta de Serviço em Nuvem apenas em conexão com os Participantes Elegíveis que acessam o Aplicativo do Cliente e exclusivamente como uma ferramenta que tem como objetivo investigar e corrigir um dispositivo (PC/MAC) específico infectado de forma ad hoc. O IBM Trusteer Rapport Remediation deve ser executado efetivamente nesse dispositivo (PC/MAC) do Participante Elegível afetado e esse

Participante Elegível afetado precisa aceitar o EULA, autenticar com os Aplicativos do Cliente pelo menos uma vez, e a configuração do Cliente deve incluir a coleta de IDs de Usuários. Para evitar dúvidas, esta oferta de Serviço em Nuvem não inclui o direito de usar o Trusteer Splash e/ou promover o Software Cliente do Titular da Conta de qualquer outra forma ao público em geral de Participantes Elegíveis do Cliente.

1.4.5 IBM Trusteer Pinpoint Malware Detection Redeployment

Os Clientes que estiverem reimplementando seus Aplicativos bancários on-line durante o período de vigência do serviço e, consequentemente, precisarem de mudanças em sua implementação do Serviço em Nuvem do IBM Trusteer Pinpoint Malware Detection II deverão comprar o IBM Trusteer Pinpoint Malware Detection Redeployment.

A reimplementação pode ser devido à mudança do domínio ou da URL do host do Aplicativo, à conversão do Aplicativo on-line para uma nova tecnologia, à mudança para uma nova plataforma financeira on-line ou à inclusão de um novo fluxo de login em um Aplicativo existente pelo Cliente.

Pelo período de transição da reimplementação de seis meses, o Cliente tem autorização para Aplicativos adicionais na base de um para um em execução além dos Aplicativos já subscritos.

Para o IBM Trusteer Pinpoint Malware Detection Additional Applications ou IBM Trusteer Pinpoint Malware Detection II Standard Edition ou IBM Trusteer Pinpoint Malware Detection II Advanced Edition, a implementação em qualquer Aplicativo adicional além do primeiro Aplicativo requer a autorização do IBM Trusteer Pinpoint Malware Detection Additional Applications.

1.4.6 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail e/ou IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

- Para o IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail ou IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail, a implementação de qualquer Aplicativo de Retail além do primeiro Aplicativo requer autorização do IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail.
- Para IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business ou IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business, a implementação de qualquer Aplicativo de Business além do primeiro Aplicativo requer a autorização do IBM Trusteer Pinpoint Malware Detection Additional Applications for Business.

1.5 IBM Trusteer Fraud Protection Suite

O IBM Trusteer Fraud Protection Suite ("Suite") é uma coleção de serviços baseados em nuvem projetada para fornecer uma camada de proteção contra fraude e que pode ser integrada a produtos IBM adicionais para fornecer uma solução de gerenciamento de ciclo de vida. O Suite inclui os seguintes serviços baseados em nuvem:

- IBM Trusteer Pinpoint Detect, que visa detectar e mitigar ataques de malware, phishing e controle de conta. O Trusteer Pinpoint Detect pode ser integrado a Aplicativos de Business e/ou de Retail do Cliente para os quais o Cliente subscreveu a cobertura do Serviço em Nuvem e processos de prevenção de fraude.
- IBM Trusteer Rapport for Mitigation, que visa corrigir e proteger terminais infectados.

Os Serviços em Nuvem incluem:

a. TMA:

   O TMA é disponibilizado no ambiente hospedado em nuvem do IBM Trusteer, através do qual o Cliente (e um número ilimitado de membros de sua equipe autorizada) pode: (i) receber relatórios de dados de eventos e avaliações de risco e (ii) visualizar, configurar e definir políticas de segurança e políticas relacionadas ao relatório de dados de eventos.

b. Dados de eventos:

   O Cliente (e um número ilimitado de membros de sua equipe autorizada) pode usar o TMA para receber dados de eventos gerados como um resultado das interações on-line dos Participantes Elegíveis com o(s) Aplicativo(s) do Cliente para o(s) qual(is) o Cliente subscreveu a cobertura do Serviço em Nuvem, ou o Cliente pode receber os dados dos eventos por meio de um modo de entrega de API de backend.

c. Script da Web e/ou APIs:

Para implementação em um website para os propósitos de acesso ou uso do Serviço em Nuvem.

Melhores Práticas do Pinpoint

Em caso de detecção de malware ou detecção de tomada de controle de conta (account takeover), o Cliente deve seguir o Guia de Melhores Práticas do Pinpoint. O Cliente não deve usar os Serviços em Nuvem do IBM Security Trusteer Pinpoint Detect de qualquer forma que possa afetar a experiência do Participante Elegível imediatamente após uma detecção de malware ou de controle de conta, de maneira que permita que outros vinculem as ações do Cliente ao uso de ofertas IBM Trusteer Pinpoint Detect (por exemplo, notificações, mensagens, bloqueio de dispositivos ou bloqueio de acesso ao Aplicativo de Business e/ou Retail imediatamente após uma detecção de malware ou de controle de conta (account take over)).

1.5.1 IBM Trusteer Pinpoint Detect Standard for Retail e/ou IBM Trusteer Pinpoint Detect Standard for Business

Esse Serviço em Nuvem combina os Serviços em Nuvem IBM Trusteer Pinpoint Criminal Detection e IBM Trusteer Pinpoint Malware Detection para oferecer uma única solução unificada.

A solução ajuda na detecção de malware sem ação do Cliente (clientless) e/ou suspeita de atividade de controle de conta em navegadores se conectando a um Aplicativo de Negócio ou de Retail, usando ID de dispositivo, detecção de phishing e detecção de furto de credencial acionada por malware. As ofertas IBM Trusteer Pinpoint oferecem outra camada de proteção e visam detectar tentativas de controle de conta e fornecer diretamente para o Cliente indicadores de avaliação de risco de navegadores ou dispositivos móveis (por meio de navegador nativo ou aplicativo móvel do Cliente) acessando um Aplicativo de Negócio ou de Retail.

O suporte Padrão (conforme definido na seção Suporte Técnico abaixo) está incluído neste Serviço em Nuvem. Para o suporte Premium, o Cliente deve adquirir o Pinpoint Standard Premium Support.

Esse Serviço em Nuvem inclui proteção de um Aplicativo. Para cada Aplicativo adicional, o Cliente deve obter uma autorização para IBM Trusteer Pinpoint Detect Standard Additional Applications.

O serviço está disponível para compra em pacotes de 100 Participantes Elegíveis ou 100 Conexões. Caso o Cliente escolha adquirir o serviço por Conexões, os encargos do Additional Application serão aplicáveis a partir do primeiro aplicativo.

1.5.2 IBM Trusteer Pinpoint Detect Premium for Retail e/ou IBM Trusteer Pinpoint Detect Premium for Business

Esse Serviço em Nuvem combina o IBM Trusteer Pinpoint Criminal Detection e o IBM Trusteer Pinpoint Malware Detection para oferecer uma solução unificada exclusiva e de fácil integração.

A solução ajuda na detecção de malware sem ação do Cliente e/ou atividade suspeita de controle de conta em navegadores se conectando a um Aplicativo de Negócio ou de Retail, usando ID de dispositivo, detecção de phishing e detecção de furto de credencial acionada por malware. As ofertas IBM Trusteer Pinpoint fornecem outra camada de proteção e visam detectar tentativas de controle de conta e fornecer diretamente para o Cliente indicadores de avaliação de risco de navegadores ou dispositivos móveis (por meio de um navegador nativo ou aplicativo de dispositivo móvel do Cliente) acessando um Aplicativo de Negócio ou Retail.

O serviço inclui funcionalidades e serviços aprimorados, sendo eles: implementação estendida e serviços de configuração, políticas de segurança customizadas, serviços de investigação, etc. O serviço inclui até 200 horas de recursos compartilhados para serviços de implementação por aplicativo e 200 horas de recursos compartilhados para análise de segurança por aplicativo após a configuração. Os serviços contínuos incluem 20 horas da manutenção de implementação por ano por aplicativo e 100 horas de pesquisas de segurança por aplicativo por ano. Qualquer esforço adicional estará sujeito a encargos adicionais.

O Pinpoint Detect pode consumir transações dos canais Mobile e Web. Caso transações do Mobile sejam incluídas, o Pinpoint por Conexão se aplicará. Esse Serviço em Nuvem inclui proteção de um Aplicativo. Para cada Aplicativo adicional, o Cliente deve obter autorização para o IBM Trusteer Pinpoint Detect Premium Additional Applications.

O suporte Premium está incluído nesse Serviço em Nuvem.

Os serviços IBM Trusteer Pinpoint Detect Premium for Retail e Business estão disponíveis para compra em pacotes de 100 Participantes Elegíveis ou o IBM Trusteer Pinpoint Detect Premium por pacotes de 100 Conexões. Caso o Cliente escolha adquirir o serviço por Conexões, os encargos de Aplicação Adicionais serão aplicáveis a partir do primeiro aplicativo.

Pinpoint Detect Policy Manager:

O Policy Manager está incluído no serviço Pinpoint Detect Premium e está disponível no ambiente hospedado na nuvem do IBM Trusteer, através do qual o Cliente (e um número ilimitado de pessoas autorizadas) pode: (i) projetar, testar e implementar na lógica do ambiente de produção para detectar atividade fraudulenta, (ii) desenvolver relatórios e painéis e (iii) visualizar, configurar e definir políticas de segurança e políticas para detectar atividades suspeitas no Aplicativo do cliente.

Os serviços de consultoria são necessários para a ativação do recurso Policy Manager e para o suporte de detalhamento adicional necessário. Os detalhes dos serviços de consultoria serão descritos separadamente em uma descrição de trabalho.

Quando o Policy Manager estiver ativado, a IBM reserva-se o direito de acessar o ambiente do Cliente para fins de suporte, para ajustar as políticas do Cliente a fim de corrigir os principais problemas derivados de mudanças na política.

O Cliente compromete-se a proteger os dados expostos através do Policy Manager contra uso indevido.

Quando o recurso Policy Manager estiver ativado, o Cliente deve seguir as diretrizes da IBM para a configuração das regras, conforme descrito na documentação. O Cliente reconhece que a IBM não é responsável por qualquer situação que possa decorrer do não seguimento dessas recomendações por parte do Cliente.

Qualquer problema de degradação de estabilidade e/ou de serviço que possa surgir devido à configuração incorreta do recurso Policy Manager pelo Cliente não será considerado como Tempo de Inatividade para o cálculo do SLA.

1.5.3 Serviços opcionais para o IBM Trusteer Pinpoint Detect Standard e/ou IBM Trusteer Pinpoint Detect Premium

Para os Serviços em Nuvem nesta seção, há um pré-requisito de autorização para o IBM Trusteer Pinpoint Detect Premium ou IBM Trusteer Pinpoint Detect Standard.

1.5.4 IBM Trusteer Rapport for Mitigation for Retail e/ou IBM Trusteer Rapport for Mitigation for Business

- O IBM Trusteer Rapport for Mitigation for Retail tem como foco investigar, corrigir, bloquear e remover infeções de malware de dispositivos (PC/MACs) infectados de Participantes Elegíveis do Cliente que acessam o Aplicativo de Retail do Cliente de forma ad hoc, em que infecções de malware foram detectadas por dados de eventos do IBM Trusteer Pinpoint Detect Premium ou do IBM Trusteer Pinpoint Detect Standard. O Cliente deve ter uma subscrição vigente para o IBM Trusteer Pinpoint Detect Premium ou IBM Trusteer Pinpoint Detect Standard efetivamente em execução no Aplicativo de Retail do Cliente. O Cliente pode usar esse Serviço em Nuvem apenas em conexão com os Participantes Elegíveis que acessam o Aplicativo de Retail do Cliente e exclusivamente como uma ferramenta que tem como objetivo investigar e corrigir um dispositivo particular infectado (PC/MAC) de forma ad hoc. De fato, o IBM Trusteer Rapport for Mitigation for Retail deve ser executado no dispositivo do Participante Elegível afetado (PC/MAC), e esse Participante Elegível afetado deve aceitar o EULA, se autenticar com os Aplicativos de Retail do Cliente pelo menos uma vez e a configuração do Cliente deve incluir a coleta de IDs do usuário. Para evitar dúvidas, esse Serviço em Nuvem não inclui o direito de usar o Trusteer Splash e/ou promover o Software Cliente do Titular da Conta de qualquer outra forma na população de Participantes Elegíveis gerais do Cliente.
- O IBM Trusteer Rapport for Mitigation for Business tem como foco investigar, corrigir, bloquear e remover infeções de malware de dispositivos (PC/MACs) infectados de Participantes Elegíveis do Cliente que acessam o Aplicativo de Negócio do Cliente de forma ad hoc, em que infecções de malware foram detectadas por dados de eventos do IBM Trusteer Pinpoint Detect Premium ou do IBM Trusteer Pinpoint Detect Standard. O Cliente deve ter uma subscrição vigente para o IBM Trusteer Pinpoint Detect Premium ou IBM Trusteer Pinpoint Detect Standard efetivamente em execução no Aplicativo de Negócio do Cliente. O Cliente pode usar esse Serviço em Nuvem apenas em conexão com os Participantes Elegíveis que acessam o Aplicativo de Negócio do

Cliente e exclusivamente como uma ferramenta que tem como objetivo investigar e corrigir um dispositivo particular infectado (PC/MAC) de forma ad hoc. De fato, o IBM Trusteer Rapport for Mitigation for Business deve ser executado no dispositivo do Participante Elegível afetado (PC/MAC), e esse Participante Elegível afetado deve aceitar o EULA, se autenticar com os Aplicativos de Negócio do Cliente pelo menos uma vez e a configuração do Cliente deve incluir a coleta de IDs do usuário. Para evitar dúvidas, esse Serviço em Nuvem não inclui o direito de usar o Trusteer Splash e/ou promover o Software Cliente do Titular da Conta de qualquer outra forma na população de Participantes Elegíveis gerais do Cliente.

1.5.5 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail e/ou IBM Trusteer Pinpoint Detect Standard Additional Applications for Business e/ou IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail e/ou IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

O serviço inclui até 200 horas de recursos compartilhados para serviços de implementação por aplicativo e 200 horas de recursos compartilhados para análise de segurança por aplicativo após a configuração. Os serviços contínuos incluem 20 horas de manutenção da implementação por ano por aplicativo e 100 horas de pesquisas de segurança por aplicativo por ano.

- Para o IBM Trusteer Pinpoint Detect Standard for Retail, a implantação em qualquer Aplicativo de Retail adicional além do primeiro Aplicativo requer a autorização do IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail.
- Para o IBM Trusteer Pinpoint Detect Standard for Business, a implementação em qualquer Aplicativo de Negócio adicional além do primeiro Aplicativo requer autorização do IBM Trusteer Pinpoint Detect Standard Additional Applications for Business.
- Para o IBM Trusteer Pinpoint Premium for Retail, a implantação de qualquer Aplicativo de Retail adicional além do primeiro Aplicativo requer a autorização do IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail.
- Para o IBM Trusteer Pinpoint Premium for Business, a implantação de qualquer Aplicativo de Negócio adicional além do primeiro Aplicativo requer a autorização do IBM Trusteer Pinpoint Detect Premium Additional Applications for Business.

1.5.6 IBM Trusteer Pinpoint Detect Standard Application e/ou IBM Trusteer Pinpoint Detect Premium Application

Esse serviço é aplicável para os canais Web e Mobile.

O serviço inclui até 200 horas de recursos compartilhados para serviços de implementação por aplicativo e 200 horas de recursos compartilhados para análise de segurança por aplicativo após a configuração. Os serviços contínuos incluem 20 horas da manutenção de implementação por ano por aplicativo e 100 horas de pesquisas de segurança por aplicativo por ano

- A implementação do IBM Trusteer Pinpoint Detect Standard requer a autorização do IBM Trusteer Pinpoint Detect Standard Application para cada Aplicativo.
- A implementação do IBM Trusteer Pinpoint Premium requer autorização do IBM Trusteer Pinpoint Detect Premium Application para cada Aplicativo.

1.5.7 IBM Trusteer Pinpoint Detect Standard Redeployment e/ou IBM Trusteer Pinpoint Detect Premium Redeployment

Os Clientes, que estiverem reimplementando seus Aplicativos bancários on-line durante o período de vigência do serviço e, consequentemente, precisarem de mudanças em sua implementação do IBM Trusteer Pinpoint Detect, deverão comprar o IBM Trusteer Pinpoint Detect Redeployment.

A reimplementação pode ser devido à mudança do domínio ou da URL do host do Aplicativo, à conversão do Aplicativo on-line para uma nova tecnologia, à mudança para uma nova plataforma financeira on-line ou à inclusão de um novo fluxo de login em um Aplicativo existente pelo Cliente.

Pelo período de transição da reimplementação de seis meses, o Cliente tem autorização para Aplicativos adicionais na base de um para um em execução além dos Aplicativos já subscritos.

1.5.8 IBM Trusteer Pinpoint Detect Standard for Retail Premium Support e/ou IBM Trusteer Pinpoint Detect Standard for Business Premium Support

Os Clientes que adquirirem o Serviço em Nuvem Pinpoint Detect Standard poderão adquirir o serviço Premium Support. O escopo dos serviços Premium Support está listado na seção 4 abaixo.

1.5.9 IBM Trusteer Digital Content Pack for Retail e/ou IBM Trusteer Digital Content Pack for Business

O IBM Trusteer Digital Content Pack permite que os analistas de segurança integrem novos modelos de fraude enquanto suportam totalmente a criação e modificação de modelos sob demanda para reagir a ameaças em constante evolução. Consiste em um amplo conjunto de regras, insights e políticas que podem ser adquiridos como parte adicional e integral da solução. O Digital Content Pack ajuda a estreitar ainda mais a integração entre os recursos de prevenção de fraudes digitais do Trusteer e os canais de pagamento eletrônico do IBM Safer Payments. Ao utilizar suas regras integradas e sua lógica de Business específica, o Digital Content Pack permite que bancos e outras instituições financeiras aprimorem ainda mais os recursos existentes de detecção e prevenção de fraudes.

O IBM Trusteer Digital Content Pack for Retail está disponível em pacotes de 100 Participantes Elegíveis. O IBM Trusteer Digital Content Pack for Business está disponível em pacotes de 10 Participantes Elegíveis.

Os serviços de consultoria são necessários para a integração do Digital Content Pack com o Pinpoint Detect e o IBM Safer Payments, assim como para serviços de suporte que requeiram atenção significativa. Os serviços de consultoria são adquiridos separadamente de acordo com uma descrição de trabalho separada.

1.5.10 IBM Trusteer New Account Fraud for Retail e/ou IBM Trusteer New Account Fraud for Business

Esse serviço, disponível para os subscritores do Pinpoint, foi desenvolvido para detectar anomalias, sinalizar atividades suspeitas e gerar alertas já no processo de criação da nova conta. O serviço monitora novas contas para identificar novas atividades associadas à fraude pós-conta e a perfis recentes de contas para fornecer um sinal de alerta antecipado, através de relatórios de uso disponíveis no TMA, de que a nova conta pode ser uma conta ilegal ou pode ser usada para conduzir fraudes.

O IBM Trusteer New Account Fraud for Retail e o IBM Trusteer New Account Fraud for Business estão disponíveis em pacotes de 10 Chamadas API.

1.5.11 IBM Trusteer Pinpoint Verify

O Cliente deve ter uma subscrição vigente do IBM Trusteer Pinpoint Detect Premium antes de se subscrever esse Serviço em Nuvem.

Esse Serviço em Nuvem oferece recursos para que os usuários passem por um segundo fator de autenticação a fim de verificar suas identidades ao acessarem um serviço digital. Ele está disponível para o Pinpoint Detect Premium com a finalidade de fornecer um segundo fator de autenticação para aplicativos protegidos. A decisão sobre quando convidar os usuários para um segundo fator de autenticação é derivada do aplicativo protegido e pode ser baseada nas recomendações retornadas pela plataforma Pinpoint Detect Premium ou em outras políticas definidas pelo aplicativo protegido.

1.6 IBM Trusteer Pinpoint Assure

Esse serviço sinaliza atividades suspeitas e gera alertas no processo de criação/registro de conta nova. O serviço monitora o processo de registro de conta para identificar a atividade associada à fraude a fim de fornecer um sinal de alerta antecipado de que a nova conta pode ser uma conta ilegal ou utilizada para realizar fraudes por meio dos relatórios de uso disponíveis no TMA.

O IBM Trusteer Pinpoint Assure está disponível em pacotes de 100 Conexões.

1.6.1 Serviços opcionais do IBM Trusteer Pinpoint Assure

1.6.2 IBM Trusteer Pinpoint Assure Application

Para a implementação do IBM Trusteer Pinpoint Assureem qualquer Aplicativo é necessária a autorização do IBM Trusteer Pinpoint Assure Application.

O IBM Trusteer Pinpoint Assure está disponível para compra por aplicativo.

1.6.3 IBM Trusteer Mobile Carrier Intelligence e/ou IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

O Cliente deve ter uma subscrição vigente para o IBM Trusteer Pinpoint Assure ou para o IBM Trusteer Pinpoint Detect antes de subscrever esse Serviço em Nuvem.

Esse Serviço em Nuvem aprimora o IBM Trusteer Pinpoint Assure e/ou IBM Trusteer Pinpoint Detect, fornecendo informações e contexto adicionais sobre os números de dispositivo móvel fornecidos para qualquer um dos Serviços em Nuvem, ajudando a determinar o risco de fraude em uma determinada sessão. O Cliente pode consultar o Serviço em Nuvem para conhecer as características do número de um determinado dispositivo móvel, tais como as informações da operadora associadas a esse número.

Os dados fornecidos por esse Serviço em Nuvem referentes aos números de dispositivo móvel ("Inteligência de Dispositivo Móvel") podem ser utilizados apenas para propósitos internos do Cliente e só podem ser retidos por um período de trinta (30) dias. O Cliente deve consultar novamente o Serviço em Nuvem referente ao mesmo número de dispositivo móvel após tal período para obter a Inteligência de Dispositivo Móvel referente a esse número, e não simplesmente reutilizar a Inteligência de Dispositivo recebida em uma consulta anterior. O Cliente não pode armazenar em cache, exceto conforme permitido acima, reutilizar ou utilizar em conjunto, total ou parcialmente, com qualquer extração de dados ou para arquivar a Inteligência de Dispositivo.

1.7 IBM Trusteer Remotely Delivered Services

O IBM Trusteer Remotely Delivered Services está disponível como um complemento opcional para o Pinpoint Detect Premium e o Pinpoint Assure Cloud Services.

1.7.1 IBM Trusteer Project Management and Consultancy Services

Esse serviço fornece até 200 horas de serviços de consultoria durante os quais a IBM realizará alguns ou todos os itens a seguir:

a. Serviços de configuração inicial: reuniões periódicas frequentes, serviços de gerenciamento de projeto

b. Policy Manager: suporte contínuo

A oferta está disponível para ser adquirida por Compromisso.

1.7.2 IBM Trusteer Security Research Consultancy Services

Esse serviço de consultoria inclui até 200 horas de recursos compartilhados para análise de segurança para oferecer serviços adicionais além da solução definida e o Premium Support (quando aplicável), além de incluir:

a. Pesquisa de fraude estendida: reuniões semanais e treinamento.

b. Suporte de alta prioridade ao lançamento do Cliente

c. Suporte e investigação contínua de regras personalizadas

A oferta está disponível para ser adquirida por Compromisso.

1.7.3 IBM Trusteer Training Services

Esse serviço de consultoria foi projetado para oferecer serviços adicionais além da solução definida e o Premium Support (quando aplicável), além de incluir serviços de treinamento sobre o portfólio do Trusteer para funcionários do Cliente.

A oferta está disponível para ser adquirida por Compromisso.

1.8 Serviços em Nuvem do IBM Trusteer Mobile

1.8.1 IBM Trusteer Mobile SDK for Business e/ou IBM Trusteer Mobile SDK for Retail

Os Serviços em Nuvem do IBM Trusteer Mobile SDK são projetados para incluir outra camada de proteção para fornecer acesso à web seguro em Aplicativos de Business e/ou Retail do Cliente para os quais o Cliente subscreveu a cobertura de Serviços em Nuvem, avaliação de risco de dispositivos e proteção contra pharming. A detecção de Wi-Fi seguro está disponível apenas para plataformas Android.

Os Serviços em Nuvem do IBM Trusteer Mobile SDK incluem um kit de desenvolvimento de software ("SDK") para dispositivo móvel proprietário, um pacote de software que contém documentação, bibliotecas de software proprietário para programação e outros arquivos e itens relacionados, conhecidas

como biblioteca móvel do IBM Trusteer assim como o "Componente de Tempo de Execução" ou "Redistribuível", um código proprietário gerado pelo IBM Trusteer Mobile SDK que pode ser incorporado e integrado aos aplicativos móveis iOS ou Android independentes e protegidos do Cliente para os quais o Cliente subscreveu a cobertura de Serviços em Nuvem. ("Aplicativo de Dispositivo Móvel Integrado do Cliente").

IBM Trusteer Mobile SDK for Retail está disponível em pacotes de 100 Participantes Elegíveis ou pacotes de 100 Dispositivos de Cliente, e o IBM Trusteer Mobile SDK for Business está disponível em pacotes de 10 Participantes Elegíveis ou pacotes de 10 Dispositivos de Cliente.

Através do TMA, o Cliente (e número ilimitado de membros da sua equipe autorizada) pode receber relatórios de dados do evento e avaliações de tendências de risco. Através do Aplicativo de Dispositivo Móvel Integrado do Cliente, o Cliente pode receber informações sobre análise de risco e dispositivos móveis com relação aos dispositivos móveis dos Participantes Elegíveis que fizeram download do Aplicativo de Dispositivo Móvel Integrado do Cliente, permitindo que o Cliente formule uma política de prevenção de fraude ao tornar mandatórias ações de mitigação em relação a estes riscos. Para o propósito desta oferta, "dispositivos móveis" incluem apenas telefones celulares e tablets suportados e não incluem PCs ou MACs.

O Cliente pode:

a. usar internamente o IBM Trusteer Mobile SDK com o propósito exclusivo de desenvolver o Aplicativo de Dispositivo Móvel Integrado do Cliente;

b. integrar o Redistribuível (somente no formato de código objeto) de modo integral não separável no Aplicativo de Dispositivo Móvel Integrado do Cliente. Qualquer parte modificada ou integrada do Redistributível em conformidade com esta concessão de licença deve estar sujeita aos termos da Descrição de Serviço; e

c. comercializar e distribuir o Redistribuível para download para dispositivos móveis dos Participantes Elegíveis ou no portador do Dispositivo Cliente, desde que:

   - Exceto conforme expressamente permitido neste Contrato, o Cliente (1) não pode usar, copiar, modificar ou distribuir o SDK; (2) não pode reverter a montagem, reverter a compilação ou de qualquer outra forma, converter ou reverter a engenharia do SDK, exceto conforme expressamente permitido por lei, sem a possibilidade de renúncia contratual; (3) não pode sublicenciar, alugar ou arrendar o SDK; (4) não pode remover quaisquer arquivos de direitos autorais ou aviso contidos no Redistribuível; (5) não pode usar o mesmo nome de caminho que os arquivos/módulos do Redistribuível originais; e (6) não pode usar nomes ou marcas comerciais da IBM, de seus licenciadores ou distribuidores em conexão com a comercialização do Aplicativo de Dispositivo Móvel Integrado do Cliente sem o consentimento prévio e por escrito da IBM, do licenciador ou do distribuidor.
   - O Redistribuível deve permanecer integrado de uma forma não separável dentro do Aplicativo de Dispositivo Móvel Integrado do Cliente. O Redistribuível deve estar apenas no formato de código de objeto e deve estar em conformidade com todas as orientações, instruções e especificações no SDK e na sua documentação. O contrato de licença do usuário final para o Aplicativo de Dispositivo Móvel Integrado do Cliente deve notificar o usuário final que o Redistribuível não pode ser i) usado para qualquer outro propósito além de ativar o Aplicativo de Dispositivo Móvel Integrado do Cliente, ii) copiado (exceto para propósitos de backup), iii) adicionalmente distribuído ou transferido, iv) ter sua montagem revertida, compilação revertida ou de outra qualquer outra forma, convertido, exceto conforme especificamente permitido por lei e sem a possibilidade de uma renúncia contratual. O contrato de licença do Cliente deve ser pelo menos tão protetor da IBM quanto os termos deste Contrato
   - O SDK pode ser implantado apenas como parte do desenvolvimento e testes de unidade internos do Cliente em dispositivos de teste móveis especificados do Cliente. O Cliente não está autorizado a usar o SDK para o processamento de cargas de trabalho de produção, simulação de cargas de trabalho de produção ou escalabilidade de testes de qualquer código, aplicativo ou sistema. O Cliente não está autorizado a usar qualquer parte do SDK para quaisquer outros propósitos.

O Cliente é o único responsável pelo desenvolvimento, teste e suporte do Aplicativo de Dispositivo Móvel Integrado do Cliente. O Cliente é responsável por toda a assistência técnica para o Aplicativo de Dispositivo Móvel Integrado do Cliente e por quaisquer modificações nos Redistribuíveis feitas pelo Cliente, conforme permitido neste documento.

O Cliente está autorizado a instalar e usar os Redistribuíveis e o IBM Security Mobile SDK apenas para suportar o uso dos Serviços em Nuvem pelo Cliente.

A IBM não garante que qualquer aplicativo ou resultado obtidos pelo uso de ferramentas móveis incluídas no IBM Security Mobile SDK irá funcionar, interoperar ou ser compatível com qualquer dispositivo móvel ou plataforma de sistema operacional móvel específico.

Componentes de Origem e Materiais de Amostra - O IBM Trusteer Mobile SDK pode incluir alguns componentes no formato de código-fonte ("Componentes de Origem") e outros materiais identificados como Materiais de Amostra. O Cliente pode copiar e modificar Componentes de Origem e Materiais de Amostra somente para uso interno, desde que esse uso esteja dentro dos limites dos direitos da licença sob este Contrato e que o Cliente não altere ou exclua quaisquer informações ou avisos sobre direitos autorais contidos nos Componentes de Origem ou nos Materiais de Amostra. A IBM fornece os Componentes Fonte e Materiais de Amostra sem obrigação de suporte e "NO ESTADO". O Cliente deve observar que os Componentes de Origem ou os Materiais de Amostra são fornecidos exclusivamente como exemplo de como implementar o Embeddable no CIMA, os Componentes de Origem ou os Materiais de Amostra podem não ser compatíveis com o ambiente de desenvolvimento do Cliente e o Cliente é o único responsável pelos testes e implementação do Embeddable em seu CIMA.

2. Proteção de Dados e Conteúdo

A Planilha de Processamento e Proteção de Dados (Planilha de Dados) fornece informações específicas sobre o Serviço em Nuvem no que se refere ao tipo de Conteúdo habilitado para processamento, às atividades de processamento envolvidas, aos recursos de proteção de dados e aos detalhes específicos sobre a retenção e a devolução de Conteúdo. Todos os detalhes ou esclarecimentos e termos, incluindo as responsabilidades do Cliente, em torno do uso do Serviço em Nuvem e dos recursos de proteção de dados, se houver, são definidos nesta seção. Pode haver mais de uma planilha de dados aplicável ao uso do Serviço em Nuvem pelo Cliente, com base nas opções selecionadas pelo Cliente. A Planilha de Dados pode estar disponível somente em inglês e não no idioma local. Inobstante qualquer prática legal ou consuetudinária local, as partes concordam que entendem inglês e que o mesmo é um idioma apropriado à aquisição e uso dos Serviços em Nuvem. A(s) seguinte(s) Planilha(s) de Dados aplica(m)-se ao Serviço em Nuvem e suas opções disponíveis. O Cliente está ciente que i) a IBM pode modificar a(s) Planilha(s) de Dados, de tempos em tempos, a critério exclusivo da IBM e ii) tais modificações substituirão versões anteriores. A intenção de qualquer modificação na(s) Planilha(s) de Dados será para i) melhorar ou esclarecer compromissos existentes, ii) manter o alinhamento com as normas atualmente adotadas e as leis aplicáveis ou iii) fornecer compromissos adicionais. Nenhuma modificação na(s) Planilha(s) de Dados degradará materialmente a proteção de dados de um Serviço em Nuvem.

Link(s) para a(s) Planilha(s) de Dados aplicável(is):

IBM Trusteer Mobile SDK

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

IBM Trusteer Mobile Secure Browser

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492579396

IBM Trusteer Pinpoint Assure

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=CF0C527046E011E8ADCBA344DE8FB657

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 Rapport

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402483908375

IBM Trusteer Pinpoint Verify

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=735E5650E26711E69CCD7F0385C6524D

(A planilha de dados IBM Cloud Identity Verify reflete o IBM Trusteer Pinpoint Verify)

O Cliente é responsável por tomar as medidas necessárias para pedir, ativar ou usar os recursos de proteção de dados disponíveis para um Serviço em Nuvem, bem como aceita a responsabilidade pelo uso dos Serviços em Nuvem caso o Cliente não consiga tomar essas medidas, incluindo o atendimento aos requisitos de proteção de dados ou a outros requisitos legais em relação ao Conteúdo.

O Adendo de Processamento de Dados (DPA - Data Processing Addendum) da IBM em http://ibm.com/dpa e o(s) Apêndice(s) do DPA aplicam-se e são referenciados como parte do Contrato, se e até o limite em que o Regulamento Geral sobre Proteção de Dados da União Europeia (EU/2016/679) (GDPR - General Data Protection Regulation) aplica-se aos dados pessoais contidos no Conteúdo. A(s) Planilha(s) de Dados aplicável(is) a esse Serviço em Nuvem servirá(ão) como Apêndice(s) do DPA. Se o DPA se aplicar, a obrigação da IBM notificar sobre as mudanças nos Subprocessadores e direito do Cliente se opor à aplicação de tais mudanças se aplicarão, conforme estabelecido no DPA.

2.1 EULA e Base de Processamento de Dados dos Titulares dos Dados

Para os Serviços em Nuvem IBM Trusteer Rapport (incluindo Rapport Remediation ou Rapport for Mitigation quando implementado junto com os Serviços em Nuvem Pinpoint):

A menos que tenha sido acordado de outra forma e de acordo com a base de processamento que o Cliente estabeleceu de forma independente, o Cliente autoriza a IBM a fornecer o Contrato de Licença de Usuário Final (EULA) disponível em https://www.trusteer.com/support/end-user-license-agreement para permitir que a IBM colete e processe as informações necessárias para fornecer os Serviços em Nuvem.

2.2 Uso de Dados

A IBM não usará ou divulgará os resultados decorrentes do uso do Serviço em Nuvem pelo Cliente que são exclusivos de seu Conteúdo (Insights) ou que de outra forma identifiquem o Cliente. A IBM pode, no entanto, usar Conteúdo e outras informações (exceto Insights) que resultem do Conteúdo no curso do fornecimento do citado Serviço em Nuvem, removendo identificadores pessoais; de modo que qualquer dado pessoal não possa mais ser atribuído a um indivíduo específico sem o uso de informações adicionais. A IBM usará tais dados somente para pesquisas, testes e desenvolvimento de ofertas.

2.3 Processamento e Armazenamento de Dados

2.3.1 Informações Adicionais do Local de Processamento

Para os serviços do Trusteer Pinpoint Verify, todos os locais de hospedagem e processamento são especificados na Planilha de Dados pertinente.

Para todos os outros serviços prestados através do Datacenter da Alemanha, a IBM limitará o processamento de Dados Pessoais ao país da entidade contratante da IBM e aos seguintes países: Alemanha, Israel, Irlanda, Holanda e quaisquer outros países adicionais listados na planilha de dados aplicável para Terceiros Subprocessadores da IBM.

Para todos os outros serviços prestados através do Datacenter do Japão, a IBM limitará o processamento de Dados Pessoais ao país da entidade contratante da IBM e aos seguintes países: Japão, Israel, Irlanda e quaisquer outros países adicionais listados na planilha de dados aplicável para Terceiros Subprocessadores da IBM.

Para todos os outros serviços prestados através do Datacenter dos Estados Unidos, a IBM limitará o processamento de Dados Pessoais ao país da entidade contratante da IBM e aos seguintes países: Estados Unidos, Israel, Irlanda, Cingapura, Austrália e quaisquer outros países adicionais listados na planilha de dados aplicável para Terceiros Subprocessadores da IBM.

Os serviços de suporte e de manutenção de conta do IBM Trusteer também podem ser fornecidos conforme a necessidade, com base na disponibilidade da equipe IBM pertinente, no local do Cliente e no Datacenter no qual os dados estão hospedados.

2.3.2 Dados do Titular da Conta

Os dados do Titular da Conta serão processados na região em que o Titular da Conta instalou originalmente o Software Cliente do Titular da Conta. Isso pode significar que o conteúdo do Titular da Conta pode ser processado tanto na região de origem quanto na região acordada com o Cliente.

2.3.3 Soluções Integradas

Para fins de esclarecimento, se o Cliente rescindir um desses Serviços em Nuvem, a IBM pode manter os dados do Cliente com o objetivo de fornecer ao mesmo os Serviços em Nuvem remanescentes, pois, de acordo com essa Descrição de Serviço, o Trusteer Fraud Protection é uma solução integrada.

3. Acordo de Nível de Serviço

A IBM fornece o acordo de nível de serviço (SLA - Service Level Agreement) de disponibilidade a seguir para o Serviço em Nuvem, conforme especificado em um PoE. O SLA não é uma garantia. O SLA está disponível somente para o Cliente e se aplica somente ao uso em ambientes de produção.

3.1 Créditos de Disponibilidade

O Cliente deve registar um chamado de suporte de Gravidade 1 com o help desk de suporte técnico IBM em até 24 horas após tomar conhecimento de que o evento causou impacto na disponibilidade do Serviço em Nuvem. O Cliente deve ajudar a IBM, de forma razoável, com qualquer diagnóstico e resolução de problemas.

Uma reivindicação de chamado de suporte pela falha em atender um SLA deve ser submetida dentro de três dias úteis após o término do mês contratado. A solução para uma reivindicação de SLA válida será um crédito em uma fatura futura para o Serviço em Nuvem com base no período durante o qual o processamento do sistema de produção para o Serviço em Nuvem não está disponível ("Tempo de Inatividade"). O Tempo de Inatividade é medido a partir do momento em que Cliente relata o evento até o momento em que o Serviço em Nuvem é restaurado, e não inclui: o tempo relacionado a uma indisponibilidade de manutenção planejada ou anunciada; causas além do controle da IBM; problemas com o Conteúdo ou com a tecnologia, os designs ou instruções do Cliente ou de terceiros; configurações do sistema e de plataformas não suportadas ou outros erros do Cliente; ou incidente de segurança causado pelo Cliente ou testes de segurança do Cliente. A IBM aplicará o mais alto Crédito de Disponibilidade aplicável com base na disponibilidade cumulativa do Serviço em Nuvem durante cada mês contratado, conforme mostrado na tabela abaixo. O total de Crédito de Disponibilidade com relação a qualquer mês contratado não pode exceder 10 por cento de um doze avos (1/12) do encargo anual para o Serviço em Nuvem.

3.2 Níveis de Serviço

Disponibilidade do Serviço em Nuvem durante um mês contratado

Disponibilidade durante um mês contratado	**Crédito (% do encargo de subscrição mensal* para o mês contratado que é objeto de uma reivindicação)**
<99,9%	2%
< 99,0%	5%
< 95,0%	10%

* Se o Serviço em Nuvem foi adquirido de um Parceiro Comercial IBM, o encargo de subscrição mensal será calculado de acordo com o preço de lista corrente para o Serviço em Nuvem em vigor para o Mês Contratado que é objeto de uma reivindicação, descontado a uma razão de 50%. A IBM disponiblizará um desconto diretamente para o Cliente.

Os Níveis de Serviço e os créditos de remuneração associados são medidos separadamente por Serviço em Nuvem e por Aplicativo Cliente.

Ao calcular créditos de SLA para Serviços em Nuvem com base em autorizações de Aplicativo, a Disponibilidade será calculada com base nas diretrizes a seguir:

- Cada Aplicativo terá uma parcela ponderada designada com base no volume da quantidade de sessões contadas durante o mês contratado.
- O tempo de inatividade de cada Serviço em Nuvem por Aplicativo será acumulado separadamente para o mês contratado.

A seguir está um exemplo de um cálculo por um mês de atividade e a ponderação associada. Apenas para propósitos de ilustração:

Aplicativos de Retail	**Parcela do nº total de sessões em um determinado mês contratado**	**Tempo de inatividade total durante o mês contratado**	**Minutos ponderados de tempo de inatividade**
Aplicativo de Retail A	40%	300 minutos	40% x 300 minutos = 120 minutos
Aplicativo de Retail B	20%	250 minutos	20% x 250 minutos = 50 minutos
Aplicativo de Retail C	40%	150 minutos	40% x 150 minutos = 60
			Tempo de inatividade total em minutos ponderados = 230

A disponibilidade, expressa como uma porcentagem, é calculada como: a quantidade total de minutos em um mês contratado, menos a quantidade total de minutos ponderados de tempo de inatividade no mês contratado, dividida pela quantidade total de minutos no mês contratado. A seguir está um cálculo de amostra baseado no exemplo de ponderação acima:

Total de 43.200 minutos em um mês contratado de 30 dias
- 230 minutos de tempo de inatividade ponderado
= 42.970 minutos

43.200 minutos no total

= 2% de Crédito de Disponibilidade para 99,4% de Disponibilidade durante o mês contratado

4. Suporte Técnico

O Suporte Técnico para os Serviços em Nuvem está disponível para um Cliente e seus Participantes Elegíveis a fim de ajudar em seu uso dos Serviços em Nuvem.

O Suporte Padrão está incluído na subscrição de todas as ofertas. O Trusteer Rapport Mandatory Service, que é um complemento ao Trusteer Rapport, tem um pré-requisito do Suporte Premium para a subscrição do Trusteer Rapport base.

Para cada Serviço em Nuvem, uma subscrição do Premium Support está disponível por um encargo adicional, com exceção dos **Serviços em Nuvem IBM Trusteer Mobile SDK**, **Serviços em Nuvem IBM Trusteer Rapport Mandatory Service**, **IBM Trusteer New Account Fraud**, **IBM Trusteer Pinpoint Assure**, **IBM Trusteer Digital Content Pack** e **IBM Trusteer Mobile Carrier Intelligence**. O Cliente deve entrar em contato com seu Representante de Vendas IBM ou Parceiro Comercial IBM.

Suporte Padrão:

- Suporte no horário local - 8h às 17h.
- Os Clientes e seus Participantes Elegíveis podem enviar chamados de suporte eletronicamente, conforme detalhado no guia de suporte do software como um serviço IBM em https://www.ibm.com/software/support/saas_support_guide.html.
- Os Clientes podem acessar o Portal de Suporte ao Cliente para obter notificações, documentos, relatórios de caso e para consultar Perguntas Frequentes em: http://www-01.ibm.com/software/security/trusteer

Suporte Premium:

- Suporte ininterrupto (24x7) para todas as gravidades.
- Os Clientes podem obter suporte diretamente através do telefone e de solicitação de retorno de chamada.
- Os Clientes e seus Participantes Elegíveis podem submeter chamados de suporte eletronicamente, conforme detalhado no Software as a Service [SaaS] Support Handbook.
- Os Clientes podem acessar o Portal de Suporte ao Cliente para obter notificações, documentos, relatórios de caso e para consultar Perguntas Frequentes em: http://www.ibm.com/software/security/trusteer/support/.
- Para obter opções de suporte e detalhes, o Cliente deve acessar o guia de suporte de software como um serviço da IBM disponível em https://www.ibm.com/software/support/saas_support_guide.html.

5. Informações de Autoização e Faturamento

5.1 Métricas de Encargos

O Serviço em Nuvem está disponível sob a métrica de encargos especificada no Documento de Transação:

- Compromisso é uma unidade de medida pela qual os serviços podem ser obtidos. Um Compromisso consiste em serviços profissionais e/ou de treinamento relacionados ao Serviço em Nuvem. Devem ser obtidas autorizações suficientes para cobrir cada Compromisso.
- Participante Elegível é uma unidade de medida pela qual o Serviço em Nuvem pode ser obtido. Cada indivíduo ou entidade elegível a participar de qualquer programa de prestação de serviço gerenciado ou controlado pelo Serviço em Nuvem é um Participante Elegível. Devem ser obtidas autorizações suficientes para cobrir todos os Participantes Elegíveis gerenciados ou controlados pelo Serviço em Nuvem durante o período de medição especificado no Documento de Transação do Cliente.

  Cada programa de prestação de serviço gerenciado pelo Serviço em Nuvem é analisado separadamente e, então, adicionado aos outros. Indivíduos ou entidades elegíveis para diversos programas de prestação de serviço requerem autorizações distintas.

  Para propósitos de autorização destes Serviços em Nuvem, um Participante Elegível é um usuário final de um Cliente, que possui credenciais de login exclusivas para um Aplicativo de Business ou de Retail do Cliente.
- Dispositivo Cliente é uma unidade de medida pela qual o Serviço em Nuvem pode ser obtido. Um Dispositivo Cliente é um único dispositivo de computação do usuário ou um sensor com propósito especial ou dispositivo de telemetria que solicita a execução ou recebe para execução um conjunto de comandos, procedimentos ou aplicativos ou fornece dados para outro sistema de computador que geralmente é referido como um servidor ou de qualquer outra forma gerenciado pelo servidor. Diversos Dispositivos Clientes podem compartilhar acesso a um servidor comum. Um Dispositivo Cliente pode ter alguma capacidade de processamento ou ser programável para permitir que um usuário trabalhe. O Cliente deve obter autorizações para cada Dispositivo Cliente que executa, fornece dados, usa serviços fornecidos ou acessa de outra forma o Serviço em Nuvem durante o período de medição especificado no Documento de Transação do Cliente.
- Aplicativo é uma unidade de medida pela qual o Serviço em Nuvem pode ser obtido. Um Aplicativo é um programa de software com nome exclusivo. Devem ser obtidas autorizações suficientes para cada Aplicativo disponibilizado para acesso e uso durante o período de medição especificado no PoE ou no Documento de Transação do Cliente.

  Para os propósitos deste Serviço em Nuvem, um Aplicativo é um único Aplicativo de Business ou de Retail do Cliente.
- Chamada API é uma unidade de medida pela qual o Serviço em Nuvem pode ser obtido. Uma chamada API é a chamada ao Serviço em Nuvem por meio de uma interface programável. Devem ser obtidas autorizações suficientes para cobrir o número total de Chamadas API, arredondado para cima até a a dezena mais próxima, realizadas durante o período de medição especificado no PoE ou no Documento de Transação do Cliente.

- Conexão é uma unidade de medida pela qual o Serviço em Nuvem pode ser obtido. Uma Conexão é um link ou uma associação de um banco de dados, aplicativo, servidor ou qualquer outro tipo de dispositivo para o Serviço em Nuvem. Devem ser obtidas autorizações suficientes para cobrir o número total de Conexões que foram ou são feitas com o Serviço em Nuvem durante o período de medição especificado no PoE ou no Documento de Transação do Cliente.

  Para os propósitos desse Serviço em Nuvem, uma Conexão é uma sessão ou um fluxo no Aplicativo do Cliente.

5.2 Encargos de Excedentes

Se o uso real do Serviço em Nuvem durante o período de medição exceder a autorização especificada no PoE, será cobrado um encargo de excedente no valor especificado no Documento de Transação no mês posterior a tal uso excedente.

5.3 Frequência de Cobrança

Com base na frequência de cobrança selecionada, a IBM faturará o Cliente os encargos devidos no início do período da frequência de faturamento, exceto pelos encargos excedentes e pelos encargos de tipos de uso, que serão faturados no mês seguinte após a prestação do serviço.

6. Opções de Vigência e Renovação

A vigência do Serviço em Nuvem começa na data em que a IBM notifica o Cliente sobre seu acesso ao Serviço em Nuvem, conforme documentado no PoE. O PoE especificará se o Serviço em Nuvem será renovado automaticamente, continuará em uma base de uso contínuo ou terminará no fim da vigência.

Para renovação automática, a menos que o Cliente forneça uma aviso de rescisão, por escrito, pelo menos 90 dias antes da data de expiração da vigência, o Serviço em Nuvem será renovado automaticamente pela duração especificada no PoE. As renovações estão sujeitas a um aumento de preço anual conforme especificado em uma cotação. No caso de uma renovação automática ocorrer após o recebimento de uma notificação da IBM sobre a retirada de mercado de um Serviço em Nuvem, a vigência da renovação terminará juntamente com o término da vigência da renovação atual ou na data anunciada para a retirada de comercialização do Serviço, o que acontecer primeiro.

No caso de uso contínuo, o Serviço em Nuvem continuará disponível, mês a mês, até que o Cliente forneça um aviso prévio de rescisão, por escrito, 90 dias antes do término. O Serviço em Nuvem permanecerá disponível até o final do mês civil após tal período de 90 dias.

7. Termos Adicionais

7.1 Disposições gerais

O Cliente concorda que a IBM pode referir-se publicamente ao Cliente como um subscritor dos Serviços em Nuvem em comunicações de marketing ou publicidade.

O Cliente não pode usar os Serviços em Nuvem, sozinhos ou em combinação com outros serviços ou produtos, em suporte a qualquer uma das seguintes atividades de alto risco: design, construção, controle ou manutenção de instalações nucleares, sistemas de transporte em massa, sistemas de controle de tráfego aéreo, sistemas de controle automotivo, sistemas de armamento, navegação ou comunicação de aeronaves ou qualquer outra atividade em que falhas no Serviço em Nuvem possam dar origem a uma ameaça material de morte ou de lesões corporais graves.

7.2 Software de Ativação

O Serviço em Nuvem requer o uso do software de ativação que o Cliente transfere por download para os sistemas do Cliente a fim de facilitar o uso do Serviço em Nuvem. O Cliente pode utilizar o software de ativação somente em conexão com o uso do Serviço em Nuvem. O software de ativação é fornecido "NO ESTADO".

7.3 Implementação do IBM Trusteer Fraud Protection

Para cada Aplicativo subscrito pelo Cliente, a subscrição básica do Cliente inclui as atividades de configuração e implementação inicial necessárias na nuvem do IBM Trusteer, incluindo inicialização única, configuração, Modelo Splash, teste e treinamento iniciais.

As atividades de implementação não incluem as atividades de implementação necessárias nos aplicativos ou sistemas do Cliente.

A fase de implementação dos vários Serviços em Nuvem é projetada para ser implementada em prazos conforme detalhado nos guias de implementação pertinentes.

A conclusão dessas fases de implementação dentro do prazo atribuido depende do compromisso e da participação integrais da gerência e da equipe do Cliente. O Cliente deve fornecer as informações necessárias oportunamente. O desempenho da IBM é previsto com base nas informações e decisões oportunas do Cliente e qualquer atraso poderá resultar em custos adicionais e/ou atraso na conclusão desses serviços de implementação.

Para cada Aplicativo subscrito pelo Cliente, a subscrição básica do Cliente inclui as atividades de configuração e implementação inicial necessárias na nuvem do IBM Trusteer, incluindo inicialização única, configuração, Modelo do Splash, teste e treinamento iniciais.

A subscrição do Cliente inclui suporte e teste para as páginas nas quais esse aplicativo do Cliente será identificado como recomendado pela IBM na implementação inicial. A IBM não é responsável por: (i) implementação parcial, (ii) opção do Cliente por não implementar os serviços em nuvem da IBM, conforme recomendado pela IBM ou (iii) a opção do Cliente por conduzir a implementação, configuração e teste por conta própria. (iv) implementação ou proteção parcial resultante de informações inadequadas fornecidas pelo Cliente. Serviços adicionais, incluindo atividades de implementação além da implementação inicial, podem ser contratados mediante o pagamento de um encargo adicional sob um contrato distinto.