IBM Trusteer Fraud Protection

Uraian Layanan ini menguraikan Layanan Cloud yang disediakan oleh IBM untuk Klien. Klien adalah pihak yang melakukan perjanjian serta pengguna dan penerimanya yang sah atas Layanan Cloud. Penawaran dan Bukti Kepemilikan (*Proof of Entitlement* - "PoE") yang berlaku diberikan sebagai Dokumen Transaksi yang terpisah.

1. Layanan Cloud

Layanan Cloud berikut dicakup dalam Uraian Layanan ini:

Layanan Cloud Rapport:

- IBM Trusteer Rapport for Business
- IBM Trusteer Rapport for Business Premium Support
- IBM Trusteer Rapport for Retail
- 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

Layanan Pinpoint Cloud:

- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition Premium Support
- IBM Trusteer Pinpoint Criminal Detection for Business
- IBM Trusteer Pinpoint Criminal Detection for Business Premium Support
- IBM Trusteer Pinpoint Criminal Detection for Retail
- IBM Trusteer Pinpoint Criminal Detection for Retail Premium Support
- IBM Trusteer Pinpoint Carbon Copy for Business
- IBM Trusteer Pinpoint Carbon Copy for Business Premium Support

- IBM Trusteer Pinpoint Carbon Copy for Retail
- IBM Trusteer Pinpoint Carbon Copy for Retail Premium Support
- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Rapport Remediation for Retail Premium Support
- IBM Trusteer Pinpoint Criminal Detection II for Business
- IBM Trusteer Pinpoint Criminal Detection II for Retail
- IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Advanced Edition
- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Rapport Remediation for Business Premium Support
- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail
- IBM Trusteer Pinpoint Criminal Detection Additional Applications 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 Criminal Detection Redeployment
- 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 Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- 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 with access management integration for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Business
- IBM Trusteer Pinpoint Detect Premium with access management integration for Retail
- IBM Trusteer Pinpoint Detect Premium with access management integration for Business
- IBM Trusteer Pinpoint Detect Standard Redeployment
- IBM Trusteer Pinpoint Detect Premium Redeployment
- IBM Trusteer Pinpoint Detect Standard For Retail Premium Support
- IBM Trusteer Pinpoint Detect Standard For Business Premium Support

Layanan Cloud Mobile:

- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile SDK for Retail
- IBM Trusteer Mobile Browser for Business
- IBM Trusteer Mobile Browser for Business Premium Support
- IBM Trusteer Mobile Browser for Retail

- IBM Trusteer Mobile Browser for Retail Premium Support

1.1 Layanan Cloud Bisnis dan Ritel

Layanan Cloud IBM Trusteer diberikan untuk penggunaan dengan jenis Aplikasi tertentu. Aplikasi ditentukan sebagai salah satu jenis berikut: Ritel atau Bisnis. Tawaran terpisah tersedia untuk Aplikasi Ritel dan Aplikasi Bisnis.

a. Aplikasi Ritel didefinisikan sebagai suatu aplikasi perbankan online, aplikasi mobile atau aplikasi *e-commerce* yang dirancang untuk melayani konsumen. Kebijakan Klien dapat mengklasifikasikan usaha kecil tertentu memenuhi syarat untuk akses ritel.

b. Aplikasi Bisnis didefinisikan sebagai sebuah aplikasi perbankan online, aplikasi mobile atau aplikasi *e-commerce* yang dirancang untuk melayani perusahaan, institusi, atau entitas yang setara, atau aplikasi apa pun yang tidak dikategorikan sebagai Ritel.

1.1.1 Layanan Cloud Bisnis

- IBM Trusteer Rapport for Business
- IBM Trusteer Rapport II for Business
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition
- IBM Trusteer Pinpoint Criminal Detection II for Business
- IBM Trusteer Pinpoint Criminal Detection for Business
- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile Browser for Business
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Pinpoint Detect Standard with access management integration for Business
- IBM Trusteer Pinpoint Detect Premium with access management integration for Business

1.1.2 Layanan Cloud Ritel

- IBM Trusteer Rapport for Retail
- IBM Trusteer Rapport II for Retail
- IBM Trusteer Pinpoint Criminal Detection for Retail
- IBM Trusteer Pinpoint Criminal Detection II for Retail
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Standard Edition
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Retail
- IBM Trusteer Pinpoint Detect Premium with access management integration for Retail
- IBM Trusteer Mobile SDK for Retail
- IBM Trusteer Mobile Browser for Retail

Untuk masing-masing Layanan Cloud Bisnis dan Ritel, tersedia produk Dukungan Premium terkait dengan biaya tambahan, dengan pengecualian Layanan Cloud IBM Trusteer Mobile SDK.

1.1.3 Layanan Cloud tambahan untuk IBM Trusteer Rapport

a. Layanan Cloud tambahan tersedia untuk IBM Trusteer Rapport 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. Layanan Cloud tambahan tersedia untuk IBM Trusteer Rapport 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

Untuk masing-masing *add-on* Bisnis dan Ritel pada Layanan Cloud IBM Trusteer Rapport, kecuali untuk *add-on* IBM Trusteer Rapport Mandatory Service, tersedia produk Dukungan Premium terkait dengan biaya tambahan.

Langganan ke IBM Trusteer Rapport for Business atau IBM Trusteer Rapport for Retail merupakan prasyarat untuk Layanan Cloud tambahan terkait yang tercantum dalam pasal ini.

1.1.4 Layanan Cloud tambahan untuk IBM Trusteer Pinpoint Malware Detection dan/atau IBM Trusteer Pinpoint Malware Detection II

a. Layanan Cloud tambahan tersedia untuk IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition atau IBM Trusteer Pinpoint Malware Detection for Business Standard Edition atau untuk IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business atau IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business:
   - IBM Trusteer Pinpoint Carbon Copy for Business
   - IBM Trusteer Rapport Remediation for Business
   - IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

b. Layanan Cloud tambahan tersedia untuk IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition atau IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition atau untuk IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition atau IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition:
   - IBM Trusteer Pinpoint Carbon Copy for Retail
   - IBM Trusteer Rapport Remediation for Retail
   - IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail

Dukungan premium tersedia untuk tawaran spesifik sebagaimana yang ditetapkan dalam dokumen ini. Langganan IBM Trusteer Pinpoint Malware Detection for Business atau IBM Trusteer Pinpoint Malware Detection for Retail atau IBM Trusteer Pinpoint Malware Detection II for Business atau IBM Trusteer Pinpoint Malware Detection II for Retail merupakan prasyarat untuk Layanan Cloud tambahan terkait yang tercantum dalam pasal ini.

1.1.5 Layanan Cloud tambahan untuk IBM Trusteer Pinpoint Criminal Detection dan/atau IBM Trusteer Pinpoint Criminal Detection II

a. Layanan Cloud tambahan tersedia untuk IBM Trusteer Pinpoint Criminal Detection for Business atau IBM Trusteer Pinpoint Criminal Detection II:
   - IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business

b. Layanan Cloud tambahan tersedia untuk IBM Trusteer Pinpoint Criminal Detection for Retail dan/atau IBM Trusteer Pinpoint Criminal Detection II for Retail:
   - IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

Dukungan premium tersedia untuk tawaran spesifik sebagaimana yang ditetapkan dalam dokumen ini.

Langganan IBM Trusteer Pinpoint Criminal Detection for Business atau IBM Trusteer Pinpoint Criminal Detection for Retail atau IBM Trusteer Pinpoint Criminal Detection II for Business atau IBM Trusteer

Pinpoint Criminal Detection II for Retail merupakan prasyarat untuk Layanan Cloud tambahan terkait yang tercantum dalam pasal ini.

1.1.6 Layanan Cloud tambahan untuk IBM Trusteer Pinpoint Detect Standard dan/atau IBM Trusteer Pinpoint Detect Premium dan/atau IBM Security Pinpoint Detect Standard with access management integration dan/atau IBM Security Detect Premium with access management integration

a. Layanan Cloud tambahan tersedia untuk IBM Trusteer Detect Standard for Business dan/atau IBM Trusteer Pinpoint Detect Premium for Business dan/atau IBM Security Pinpoint Detect Standard with access management integration for Business dan/atau IBM Security Detect Premium with access management integration for Business:

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

b. Layanan Cloud tambahan tersedia untuk IBM Trusteer Detect Standard for Retail dan/atau IBM Trusteer Pinpoint Detect Premium for Retail dan/atau IBM Security Pinpoint Detect Standard with access management integration for Retail dan/atau IBM Security Detect Premium with access management integration for Retail:

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail

Langganan ke IBM Trusteer Detect Standard atau IBM Trusteer Pinpoint Detect Premium atau IBM Security Pinpoint Detect Standard with access management integration atau IBM Security Detect Premium with access management integration merupakan prasyarat untuk Layanan Cloud tambahan terkait yang tercantum dalam pasal ini.

1.1.7 Layanan Cloud Tambahan Lainnya

Setiap langganan Layanan Cloud tambahan untuk langganan dasar di atas yang tidak tercantum dalam dokumen ini, baik tersedia saat ini atau dalam pengembangan, tidak dianggap sebagai pembaruan dan harus diberikan secara terpisah.

1.2 Definisi

Pemegang Akun – adalah pengguna dari Klien, yang telah memasang perangkat lunak klien yang diaktifkan, yang menerima perjanjian lisensi pengguna akhir (*end user license agreement* - "EULA"), dan mengotentikasi setidaknya satu kali dengan Aplikasi Ritel atau Bisnis Klien yang untuknya Klien telah berlangganan cakupan Layanan Cloud.

Perangkat Lunak Klien Pemegang Akun – adalah perangkat lunak klien yang diaktifkan IBM Trusteer Rapport atau perangkat lunak klien yang diaktifkan IBM Trusteer Mobile Browser atau perangkat lunak klien yang diaktifkan apa pun lainnya yang disediakan dengan beberapa Layanan Cloud untuk dipasang pada perangkat pengguna akhir.

Trusteer Splash – mengacu pada splash yang diberikan kepada Klien berdasarkan templat splash yang tersedia.

Halaman Awal – mengacu pada halaman yang diselenggarakan (*hosted*) oleh IBM yang diberikan kepada Klien dengan splash Klien dan Perangkat Lunak Klien Pemegang Akun yang dapat diunduh.

2. Layanan Cloud IBM Trusteer Rapport

2.1 IBM Trusteer Rapport for Retail dan/atau IBM Trusteer Rapport for Business ("Trusteer Rapport")

Trusteer Rapport memberikan lapisan perlindungan terhadap *phishing* dan serangan *malware* Man-in-the-Browser (MiTB). Menggunakan jaringan puluhan juta titik akhir di seluruh dunia, IBM Trusteer Rapport mengumpulkan keterangan-keterangan mengenai *phishing* dan serangan malware aktif terhadap organisasi di seluruh dunia. IBM Trusteer Rapport menggunakan algoritma perilaku yang bertujuan untuk memblokir serangan *phishing* dan untuk mencegah pemasangan dan pengoperasian *strain malware* MiTB.

Layanan Cloud ini memiliki metrik biaya Peserta yang Memenuhi Syarat. Tawaran Bisnis dijual dalam paket berisi 10 Peserta yang Memenuhi Syarat. Tawaran Ritel dijual dalam paket berisi 100 Peserta yang Memenuhi Syarat.

Tawaran Layanan Cloud ini mencakup:

a. Aplikasi Trusteer Management (Trusteer Management Application - "TMA"):

   TMA tersedia pada lingkungan yang diselenggarakan (*hosted*) oleh cloud IBM Trusteer, yang melaluinya Klien (dan personelnya yang sah dalam jumlah tidak terbatas) dapat: (i) menampilkan dan mengunduh pelaporan data peristiwa dan penilaian risiko tertentu, dan (ii) menampilkan konfigurasi perangkat lunak klien yang diaktifkan yang dilisensikan untuk Peserta yang Memenuhi Syarat Klien berdasarkan perjanjian lisensi pengguna akhir ("EULA") tanpa biaya dan tersedia untuk diunduh ke perangkat (PC/MAC) atau *desktop* Peserta yang Memenuhi Syarat, juga dikenal sebagai rangkaian perangkat lunak Trusteer Rapport ("Perangkat Lunak Klien Pemegang Akun"). Klien hanya dapat memasarkan Perangkat Lunak Klien Pemegang Akun yang menggunakan Trusteer Splash atau Rapport API dan Klien tidak dapat menggunakan Perangkat Lunak Klien Pemegang Akun untuk operasi bisnis internal atau penggunaan oleh karyawannya (selain penggunaan pribadi oleh karyawan).

b. Skrip Web:

   Untuk akses pada situs web dengan tujuan mengakses atau menggunakan Layanan Cloud.

c. Data peristiwa:

   Klien (dan personelnya yang sah dalam jumlah tidak terbatas) dapat menggunakan TMA untuk menerima data peristiwa yang dihasilkan dari Perangkat Lunak Klien Pemegang Akun sebagai hasil dari interaksi online Pemegang Akun dengan Aplikasi Bisnis atau Ritel-nya yang untuknya Klien telah berlangganan cakupan Layanan Cloud. Data peristiwa akan diterima dari Perangkat Lunak Klien Pemegang Akun Peserta yang Memenuhi Syarat yang berjalan pada perangkat mereka, yang telah menerima EULA, diotentikasi dengan Aplikasi Bisnis atau Ritel Klien setidaknya sekali dan konfigurasi Klien harus mencakup kumpulan ID Pengguna.

d. Trusteer Splash:

   Platform pemasaran Trusteer Splash mengidentifikasi dan memasarkan Perangkat Lunak Klien Pemegang Akun kepada Peserta yang Memenuhi Syarat yang mengakses Aplikasi Bisnis dan/atau Ritel Klien yang untuknya Klien telah berlangganan cakupan Layanan Cloud. Klien dapat memilih dari Templat Splash yang tersedia. Splash yang disesuaikan dapat dikontrak berdasarkan perjanjian atau pernyataan kerja yang terpisah.

Klien dapat setuju untuk memberikan merek dagang, logo, atau lambangnya untuk digunakan sehubungan dengan TMA dan hanya untuk dimanfaatkan dengan Trusteer Splash dan untuk ditampilkan di Perangkat Lunak Klien Pemegang Akun atau pada halaman awal yang diselenggarakan (*hosted*) oleh IBM dan pada situs web IBM Trusteer. Setiap penggunaan merek dagang, logo, atau lambang yang diberikan akan sesuai dengan kebijakan IBM yang wajar mengenai iklan dan penggunaan merek dagang.

Klien harus berlangganan Layanan Cloud IBM Trusteer Rapport Mandatory Service jika Klien ingin menggunakan jenis apa pun dari penyebaran wajib Perangkat Lunak Klien Pemegang Akun.

Penyebaran wajib Perangkat Lunak Klien Pemegang Akun termasuk namun tidak terbatas pada setiap jenis penyebaran wajib oleh mekanisme atau alat apa pun yang secara langsung atau tidak langsung mengharuskan Peserta yang Memenuhi Syarat untuk mengunduh Perangkat Lunak Klien Pemegang Akun, atau metode, alat, prosedur, perjanjian, atau mekanisme apa pun, yang tidak dibuat atau disetujui oleh IBM, yang dibuat untuk mengabaikan persyaratan pemberian lisensi penyebaran wajib Perangkat Lunak Klien Pemegang Akun ini.

2.2 IBM Trusteer Rapport II for Retail dan/atau IBM Trusteer Rapport II for Business ("Trusteer Rapport II")

Layanan Cloud Trusteer Rapport II merupakan konstruksi baru atas IBM Trusteer Rapport untuk membantu melakukan standardisasi biaya yang berkaitan dengan perlindungan beberapa Aplikasi dan mengganti biaya satu kali saat menambahkan Aplikasi.

Trusteer Rapport II memberikan lapisan perlindungan terhadap *phishing* dan serangan *malware* Man-in-the-Browser (MitB). Menggunakan jaringan puluhan juta titik akhir di seluruh dunia, IBM Trusteer Rapport mengumpulkan keterangan-keterangan mengenai *phishing* dan serangan *malware* aktif terhadap organisasi di seluruh dunia. IBM Trusteer Rapport menggunakan algoritma perilaku yang bertujuan untuk memblokir serangan *phishing* dan untuk mencegah pemasangan dan pengoperasian *strain malware* MiTB.

Layanan Cloud ini dimiliki sesuai dengan metrik biaya Peserta yang Memenuhi Syarat. Tawaran Bisnis dijual dalam paket berisi 10 Peserta yang Memenuhi Syarat. Tawaran Ritel dijual dalam paket berisi 100 Peserta yang Memenuhi Syarat.

Tawaran Layanan Cloud ini mencakup:

a. Aplikasi Trusteer Management (Trusteer Management Application - "TMA"):

   TMA tersedia pada lingkungan yang diselenggarakan (*hosted*) oleh cloud IBM Trusteer, yang melaluinya Klien (dan personelnya yang sah dalam jumlah tidak terbatas) dapat: (i) menampilkan dan mengunduh pelaporan data peristiwa dan penilaian risiko tertentu, dan (ii) menampilkan konfigurasi perangkat lunak klien yang diaktifkan yang dilisensikan untuk Peserta yang Memenuhi Syarat Klien berdasarkan perjanjian lisensi pengguna akhir ("EULA") tanpa biaya dan tersedia untuk diunduh ke perangkat (PC/MAC) atau *desktop* Peserta yang Memenuhi Syarat, juga dikenal sebagai rangkaian perangkat lunak Trusteer Rapport ("Perangkat Lunak Klien Pemegang Akun"). Klien hanya dapat memasarkan Perangkat Lunak Klien Pemegang Akun yang menggunakan Trusteer Splash atau Rapport API dan Klien tidak dapat menggunakan Perangkat Lunak Klien Pemegang Akun untuk operasi bisnis internal atau penggunaan oleh karyawannya (selain penggunaan pribadi oleh karyawan).

b. Skrip Web:

   Untuk akses pada situs web dengan tujuan mengakses atau menggunakan Layanan Cloud.

c. Data peristiwa:

   Klien (dan personelnya yang sah dalam jumlah tidak terbatas) dapat menggunakan TMA untuk menerima data peristiwa yang dihasilkan dari Perangkat Lunak Klien Pemegang Akun sebagai hasil dari interaksi online Pemegang Akun dengan Aplikasi Bisnis atau Ritel-nya yang untuknya Klien telah berlangganan cakupan Layanan Cloud. Data peristiwa akan diterima dari Perangkat Lunak Klien Pemegang Akun Peserta yang Memenuhi Syarat yang berjalan pada perangkat mereka, yang telah menerima EULA, diotentikasi dengan Aplikasi Bisnis atau Ritel Klien setidaknya sekali dan konfigurasi Klien harus mencakup kumpulan ID Pengguna.

d. Trusteer Splash:

   Platform pemasaran Trusteer Splash mengidentifikasi dan memasarkan Perangkat Lunak Klien Pemegang Akun kepada Peserta yang Memenuhi Syarat yang mengakses Aplikasi Bisnis dan/atau Ritel Klien yang untuknya Klien telah berlangganan cakupan Layanan Cloud. Klien dapat memilih dari Templat Splash yang tersedia. Splash yang disesuaikan dapat dikontrak berdasarkan perjanjian atau pernyataan kerja yang terpisah.

Klien dapat setuju untuk memberikan merek dagang, logo, atau lambangnya untuk digunakan sehubungan dengan TMA dan hanya untuk dimanfaatkan dengan Trusteer Splash dan untuk ditampilkan di Perangkat Lunak Klien Pemegang Akun atau pada halaman awal yang diselenggarakan (*hosted*) oleh IBM dan pada situs web IBM Trusteer. Setiap penggunaan merek dagang, logo, atau lambang yang diberikan akan sesuai dengan kebijakan IBM yang wajar mengenai iklan dan penggunaan merek dagang.

Klien harus berlangganan Layanan Cloud IBM Trusteer Rapport Mandatory Service jika Klien ingin menggunakan jenis apa pun dari penyebaran wajib Perangkat Lunak Klien Pemegang Akun.

Penyebaran wajib Perangkat Lunak Klien Pemegang Akun termasuk namun tidak terbatas pada setiap jenis penyebaran wajib oleh mekanisme atau alat apa pun yang secara langsung atau tidak langsung mengharuskan Peserta yang Memenuhi Syarat untuk mengunduh Perangkat Lunak Klien Pemegang Akun, atau metode, alat, prosedur, perjanjian, atau mekanisme apa pun, yang tidak dibuat atau disetujui oleh IBM, yang dibuat untuk mengabaikan persyaratan pemberian lisensi penyebaran wajib Perangkat Lunak Klien Pemegang Akun ini.

Setiap Trusteer Rapport II for Business dan/atau Trusteer Rapport II for Retail mencakup perlindungan untuk satu Aplikasi. Untuk setiap Aplikasi tambahan, Klien harus memperoleh kepemilikan atas Aplikasi Tambahan IBM Trusteer Rapport.

2.3 Layanan Cloud Tambahan Opsional untuk IBM Trusteer Rapport for Business dan/atau IBM Trusteer Rapport for Retail dan/atau IBM Trusteer Rapport II for Business dan/atau IBM Trusteer Rapport II for Retail

Langganan Layanan Cloud IBM Trusteer Rapport atau Layanan Cloud IBM Trusteer Rapport II merupakan prasyarat untuk langganan ke setiap Layanan Cloud tambahan berikut ini. Jika Layanan

Cloud ditetapkan sebagai "for Business", maka Layanan Cloud tambahan yang diperoleh juga harus ditetapkan sebagai "for Business". Jika Layanan Cloud ditetapkan sebagai "for Retail", Layanan Cloud tambahan yang diperoleh juga harus ditetapkan sebagai "for Retail". Klien akan menerima data peristiwa dari Peserta yang Memenuhi Syarat yang menjalankan Perangkat Lunak Klien Pemegang Akun yang telah menerima EULA, mengotentikasi dengan Aplikasi(-aplikasi) Bisnis dan/atau Ritel Klien setidaknya sekali, dan konfigurasi Klien harus mencakup kumpulan ID Pengguna.

2.3.1 IBM Trusteer Rapport Fraud Feeds for Business dan/atau IBM Trusteer Rapport Fraud Feeds for Retail

Saat berlangganan Layanan Cloud add-on ini, Klien (dan personelnya yang sah dalam jumlah tidak terbatas) dapat menggunakan TMA untuk melihat, berlangganan, dan mengonfigurasi pengiriman umpan ancaman yang dihasilkan dari Layanan Cloud Trusteer Rapport. Umpan dapat dikirim melalui email ke alamat email yang ditetapkan atau melalui SFTP sebagai file teks.

2.3.2 IBM Trusteer Rapport Phishing Protection for Business dan/atau IBM Trusteer Rapport Phishing Protection for Retail

Klien (dan personelnya yang sah dalam jumlah yang tidak terbatas) dapat menggunakan TMA untuk menerima pemberitahuan data peristiwa yang berkaitan dengan penyerahan kredensial *login* Pemegang Akun ke situs yang diduga *phishing* atau berpotensi penipuan. Aplikasi online yang sah (URL) mungkin keliru ditandai sebagai situs *phishing* dan Layanan Cloud dapat memperingatkan Pemegang Akun bahwa situs yang sah tersebut adalah situs *phishing*. Dalam hal tersebut, Klien harus memberi tahu IBM mengenai kesalahan tersebut dan IBM akan memperbaiki kesalahan tersebut. Ini akan menjadi satu-satunya perbaikan Klien untuk kesalahan tersebut.

2.3.3 IBM Trusteer Rapport Mandatory Service for Business dan/atau IBM Trusteer Rapport Mandatory Service for Retail

Klien dapat menggunakan suatu mesin virtual dari platform pemasaran Trusteer Splash untuk mewajibkan unduhan Perangkat Lunak Klien Pemegang Akun kepada Peserta yang Memenuhi Syarat yang mengakses Aplikasi Bisnis dan/atau Ritel Klien yang untuknya Klien telah berlangganan cakupan Layanan Cloud.

IBM Trusteer Rapport Premium Support for Business merupakan prasyarat untuk IBM Security Rapport Mandatory Service for Business.

IBM Trusteer Rapport Premium Support for Retail merupakan prasyarat untuk IBM Security Rapport Mandatory Service for Retail.

Klien dapat menerapkan fungsionalitas tambahan IBM Trusteer Rapport Mandatory Service hanya jika diperintahkan dan dikonfigurasikan untuk penggunaan dengan Aplikasi Ritel atau Bisnis Klien yang untuknya Klien telah berlangganan cakupan Layanan Cloud.

2.3.4 IBM Trusteer Rapport Large Redeployment dan/atau IBM Trusteer Rapport Small Redeployment

Klien yang menyebarkan ulang Aplikasi perbankan online mereka selama jangka waktu Layanan dan sebagai akibatnya, membutuhkan perubahan pada penyebaran mereka atas IBM Trusteer Rapport atau IBM Trusteer Rapport II harus membeli Layanan Cloud IBM Trusteer Rapport Redeployment.

Penyebaran ulang dapat disebabkan oleh Klien yang mengubah domain atau URL host Aplikasi, menerapkan perubahan pada konfigurasi splash, atau berpindah ke *platform* perbankan online yang baru.

Untuk periode transisi penyebaran ulang 6 bulan, Klien berhak atas Aplikasi tambahan secara satu per satu yang berjalan di atas Aplikasi yang telah dilanggankan.

IBM Trusteer Rapport Large Redeployment berlaku pada lingkungan dengan lebih dari 20.000 pengguna, dan IBM Trusteer Rapport Small Redeployment berlaku pada lingkungan dengan kurang dari atau sebanyak 20.000 pengguna.

2.3.5 IBM Trusteer Rapport Additional Applications for Business dan/atau IBM Trusteer Rapport Additional Applications for Retail

Untuk IBM Trusteer Rapport II for Business, penyebaran pada Aplikasi Bisnis tambahan apa pun di luar Aplikasi pertama memerlukan kepemilikan atas Aplikasi Tambahan Layanan Cloud IBM Trusteer Rapport for Business. Untuk IBM Trusteer Rapport II for Retail, penyebaran pada Aplikasi Ritel tambahan apa pun di luar Aplikasi pertama memerlukan kepemilikan atas Layanan Cloud IBM Trusteer Rapport Additional Applications for Retail.

3. Layanan Cloud IBM Trusteer Pinpoint

IBM Trusteer Pinpoint adalah layanan berbasis cloud yang dirancang untuk memberikan lapisan perlindungan yang lain dan bertujuan untuk mendeteksi serta mengurangi serangan *malware*, *phishing*, dan pengambilalihan akun. Trusteer Pinpoint dapat diintegrasikan ke dalam Aplikasi Bisnis dan/atau Ritel Klien yang untuknya Klien telah berlangganan cakupan Layanan Cloud dan proses pencegahan penipuan.

Layanan Cloud ini mencakup:

a. TMA:

   TMA tersedia pada lingkungan yang diselenggarakan (*hosted*) oleh cloud oleh IBM Trusteer, yang melaluinya Klien (dan personelnya yang sah dalam jumlah tidak terbatas) dapat: (i) menampilkan dan mengunduh pelaporan data peristiwa dan penilaian risiko tertentu, dan (ii) menampilkan, berlangganan, dan mengonfigurasi pengiriman umpan ancaman yang dihasilkan dari tawaran Pinpoint.

b. Skrip Web dan/atau API:

   Untuk penyebaran pada situs web untuk tujuan mengakses atau menggunakan Layanan Cloud.

3.1 IBM Trusteer Pinpoint Malware Detection dan IBM Trusteer Pinpoint Criminal Detection Best Practices

Dalam hal deteksi *malware* pada Layanan Cloud IBM Trusteer Pinpoint Malware Detection atau Layanan Cloud IBM Trusteer Pinpoint Malware Detection II atau deteksi pengambilalihan akun pada Layanan Cloud IBM Trusteer Pinpoint Criminal Detection atau Layanan Cloud IBM Trusteer Pinpoint Criminal Detection II, Klien harus mengikuti Panduan Praktik Terbaik Pinpoint. Jangan menggunakan Layanan Cloud IBM Trusteer Pinpoint Malware Detection atau Layanan Cloud IBM Trusteer Pinpoint Malware Detection II atau Layanan Cloud IBM Trusteer Pinpoint Criminal Detection atau Layanan Cloud IBM Trusteer Pinpoint Criminal Detection II dengan cara apa pun yang akan memengaruhi pengalaman Peserta yang Memenuhi Syarat segera setelah deteksi malware atau pengambilalihan akun, sedemikian rupa sehingga memungkinkan pihak lain mengaitkan tindakan Klien dengan penggunaan Layanan Cloud IBM Trusteer Pinpoint (misalnya, pemberitahuan, pesan, pemblokiran perangkat, atau pemblokiran akses ke Aplikasi Bisnis dan/atau Ritel segera setelah deteksi *malware* atau pengambilalihan akun.

3.2 IBM Trusteer Pinpoint Criminal Detection for Business dan/atau IBM Trusteer Pinpoint Criminal Detection for Retail

Pendeteksian tanpa Klien atas aktivitas pengambilalihan akun yang mencurigakan pada *browser* yang terhubung ke Aplikasi Bisnis atau Ritel yang menggunakan ID perangkat, deteksi *phishing*, dan deteksi pencurian kredensial yang disebabkan oleh *malware*. Layanan Cloud IBM Trusteer Pinpoint Criminal Detection menyediakan lapisan perlindungan lain dan bertujuan untuk mendeteksi upaya pengambilalihan akun dan memberikan skor penilaian risiko *browser* atau perangkat mobile (melalui *browser* asli atau aplikasi mobile Klien) yang mengakses Aplikasi Bisnis atau Aplikasi Ritel secara langsung ke Klien.

a. Data peristiwa:

   Klien (dan personelnya yang sah dalam jumlah tidak terbatas) dapat menggunakan TMA untuk menerima data peristiwa yang dihasilkan dari interaksi online Peserta yang Memenuhi Syarat dengan Aplikasi(-aplikasi) Bisnis dan/atau Ritel Klien yang untuknya Klien telah berlangganan cakupan Layanan Cloud atau Klien dapat menerima data peristiwa melalui mode penyampaian API backend.

3.3 IBM Trusteer Pinpoint Criminal Detection II for Business dan/atau IBM Trusteer Pinpoint Criminal Detection II for Retail

IBM Security Pinpoint Criminal Detection II merupakan konstruksi baru atas IBM Trusteer Pinpoint Criminal Detection untuk membantu melakukan standardisasi biaya terkait dengan perlindungan beberapa Aplikasi dan mengganti biaya satu kali saat menambahkan Aplikasi.

Pendeteksian tanpa Klien atas aktivitas pengambilalihan akun yang mencurigakan pada browser yang terhubung ke Aplikasi Bisnis atau Ritel yang menggunakan ID perangkat, deteksi *phishing*, dan deteksi pencurian kredensial yang disebabkan oleh *malware*. Layanan Cloud IBM Trusteer Pinpoint Criminal Detection II memberikan lapisan perlindungan lain dan bertujuan untuk mendeteksi upaya pengambilalihan akun dan memberikan skor penilaian risiko *browser* atau perangkat mobile (melalui

browser asli atau aplikasi mobile Klien) yang mengakses Aplikasi Bisnis atau Ritel secara langsung kepada Klien.

a. Data peristiwa:

Klien (dan personelnya yang sah dalam jumlah tidak terbatas) dapat menggunakan TMA untuk menerima data peristiwa yang dihasilkan dari interaksi online Peserta yang Memenuhi Syarat dengan Aplikasi(-aplikasi) Bisnis dan/atau Ritel Klien yang untuknya Klien telah berlangganan cakupan Layanan Cloud atau Klien dapat menerima data peristiwa melalui mode penyampaian API backend.

Layanan Cloud ini mencakup perlindungan terhadap satu Aplikasi. Untuk setiap Aplikasi tambahan, Klien harus memperoleh kepemilikan atas Aplikasi Tambahan IBM Trusteer Pinpoint Criminal Detection.

3.4 IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition dan/atau IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition dan/atau IBM Trusteer Pinpoint Malware Detection for Business Standard Edition dan/atau IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition

Pendeteksian tanpa Klien pada browser yang terinfeksi *malware* finansial Man in the Browser (MiTB) yang menghubungkan ke Aplikasi Bisnis dan/atau Aplikasi Ritel. Layanan Cloud IBM Trusteer Pinpoint Malware Detection menyediakan lapisan perlindungan lain dan bertujuan untuk memungkinkan organisasi untuk berfokus pada proses pencegahan penipuan berdasarkan risiko *malware* dengan menyediakan penilaian dan peringatan bagi Klien akan adanya *malware* finansial MiTB.

a. Data peristiwa:

Klien (dan personelnya yang sah dalam jumlah tidak terbatas) dapat menggunakan TMA untuk menerima data peristiwa yang dihasilkan dari interaksi online Peserta yang Memenuhi Syarat dengan Aplikasi(-aplikasi) Bisnis dan/atau Ritel Klien.

b. Edisi Tingkat Lanjut:

Edisi Tingkat Lanjut untuk Bisnis dan/atau Ritel menawarkan lapisan deteksi tambahan serta perlindungan yang disesuaikan dan dikustomisasi dengan struktur dan alur Aplikasi Bisnis dan/atau Ritel Klien dan dapat dikustomisasi dengan lanskap ancaman spesifik yang menarget Klien. Hal ini dapat disertakan di berbagai lokasi pada Aplikasi Bisnis dan/atau Ritel Klien.

Edisi Tingkat Lanjut ditawarkan kepada Klien dalam jumlah minimum setidaknya 100K Peserta yang Memenuhi Syarat Ritel atau 10K Peserta yang Memenuhi Syarat Bisnis, yang berarti 1000 paket berisi 100 Peserta yang Memenuhi Syarat untuk Ritel, atau 1000 paket berisi 10 Peserta yang Memenuhi Syarat untuk Bisnis.

c. Edisi Standar:

Edisi Standar untuk Bisnis atau Ritel adalah solusi cepat untuk menyebarkan yang menyediakan fungsionalitas inti dari Layanan Cloud sebagaimana yang diuraikan dalam dokumen ini.

3.5 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business dan/atau IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail dan/atau IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business dan/atau IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

IBM Security Pinpoint Malware Detection II merupakan konstruksi baru atas IBM Trusteer Pinpoint Malware Detection untuk membantu melakukan standardisasi biaya yang berkaitan dengan perlindungan beberapa Aplikasi dan mengganti biaya satu kali saat menambahkan Aplikasi.

Pendeteksian tanpa Klien pada browser yang terinfeksi *malware* finansial Man in the Browser (MiTB) yang menghubungkan ke Aplikasi Bisnis dan/atau Aplikasi Ritel. Layanan Cloud IBM Trusteer Pinpoint Malware Detection menyediakan lapisan perlindungan lain dan bertujuan untuk memungkinkan organisasi untuk berfokus pada proses pencegahan penipuan berdasarkan risiko *malware* dengan menyediakan penilaian dan peringatan bagi Klien akan adanya *malware* finansial MiTB.

a. Data peristiwa:

Klien (dan personelnya yang sah dalam jumlah tidak terbatas) dapat menggunakan TMA untuk menerima data peristiwa yang dihasilkan dari interaksi online Peserta yang Memenuhi Syarat dengan Aplikasi(-aplikasi) Bisnis dan/atau Ritel Klien.

b. Edisi Tingkat Lanjut:

Edisi Tingkat Lanjut untuk Bisnis dan/atau Ritel menawarkan lapisan deteksi tambahan serta perlindungan yang disesuaikan dan dikustomisasi dengan struktur dan alur Aplikasi Bisnis dan/atau Ritel Klien dan dapat dikustomisasi dengan lanskap ancaman spesifik yang menarget Klien. Hal ini dapat disertakan di berbagai lokasi pada Aplikasi Bisnis dan/atau Ritel Klien.

Edisi Tingkat Lanjut ditawarkan kepada Klien dalam jumlah minimum setidaknya 100K Peserta yang Memenuhi Syarat Ritel atau 10K Peserta yang Memenuhi Syarat Bisnis, yang berarti 1000 paket berisi 100 Peserta yang Memenuhi Syarat untuk Ritel, atau 1000 paket berisi 10 Peserta yang Memenuhi Syarat untuk Bisnis.

c. Edisi Standar:

Edisi Standar untuk Bisnis atau Ritel adalah solusi cepat untuk menyebarkan yang menyediakan fungsionalitas inti dari Layanan Cloud sebagaimana yang diuraikan dalam dokumen ini.

Layanan Cloud ini mencakup perlindungan terhadap satu Aplikasi. Untuk setiap Aplikasi tambahan, Klien harus memperoleh kepemilikan atas Aplikasi Tambahan IBM Trusteer Pinpoint Malware Detection.

3.6 Layanan Cloud Tambahan Opsional untuk IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition dan/atau IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition dan/atau IBM Trusteer Pinpoint Malware Detection for Business Standard Edition dan/atau IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition dan/atau IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail dan/atau IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business dan/atau IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail dan/atau IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business

- Untuk Layanan Cloud IBM Trusteer Rapport Remediation for Retail, terdapat prasyarat atas IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail atau IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail atau IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail atau IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.
- Untuk Layanan Cloud IBM Trusteer Rapport Remediation for Business, terdapat prasyarat atas IBM Trusteer Pinpoint Malware Detection Standard Edition for Business atau IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business atau IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business atau IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.
- Untuk IBM Trusteer Pinpoint Carbon Copy for Retail, terdapat prasyarat atas IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail atau IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail atau IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail atau IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.
- Untuk IBM Trusteer Pinpoint Carbon Copy for Business, terdapat prasyarat atas IBM Trusteer Pinpoint Malware Detection Standard Edition for Business atau IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business atau IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business atau IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.

3.6.1 IBM Trusteer Pinpoint Carbon Copy for Business dan/atau IBM Trusteer Pinpoint Carbon Copy for Retail

Tawaran IBM Trusteer Pinpoint Carbon Copy dirancang untuk memberikan lapisan perlindungan lain dan memantau layanan yang dapat membantu mengidentifikasi jika kredensial Peserta yang Memenuhi Syarat telah terancam oleh serangan Phishing pada Aplikasi Ritel atau Bisnis Klien yang untuknya Klien telah berlangganan cakupan tawaran Layanan Cloud.

3.6.2 IBM Trusteer Rapport Remediation for Retail dan/atau IBM Trusteer Rapport Remediation for Business

IBM Trusteer Rapport Remediation for Retail dan IBM Trusteer Rapport Remediation for Business bertujuan untuk menginvestigasi, memulihkan, memblokir dan menghapus infeksi *malware* man-in-the-browser (MitB) dari perangkat (PC/MAC) Peserta yang Memenuhi Syarat Klien yang terinfeksi yang mengakses Aplikasi Klien secara *ad-hoc*, di mana infeksi malware MitB telah terdeteksi oleh data

peristiwa IBM Trusteer Pinpoint Malware Detection. Klien harus memiliki langganan saat ini untuk IBM Trusteer Pinpoint Malware Detection atau IBM Trusteer Pinpoint Malware Detection II yang benar-benar berjalan pada Aplikasi Klien. Klien dapat menggunakan tawaran Layanan Cloud ini hanya sehubungan dengan Peserta yang Memenuhi Syarat yang mengakses Aplikasi Klien, dan hanya sebagai alat yang bertujuan untuk menginvestigasi serta memulihkan perangkat (PC/MAC) tertentu yang terinfeksi secara ad-hoc. IBM Trusteer Rapport Remediation harus benar-benar berjalan pada perangkat (PC/MAC) Peserta yang Memenuhi Syarat yang terpengaruh tersebut dan Peserta yang Memenuhi Syarat yang terpengaruh tersebut harus menerima EULA, mengotentikasi dengan Aplikasi(-aplikasi) Klien setidaknya sekali, dan konfigurasi Klien harus mencakup kumpulan ID Pengguna. Untuk menghindari keraguan, tawaran Layanan Cloud ini tidak termasuk hak untuk menggunakan Trusteer Splash dan/atau mempromosikan Perangkat Lunak Klien Pemegang Akun dengan cara lain apa pun untuk populasi umum Peserta yang Memenuhi Syarat Klien.

3.6.3 IBM Trusteer Pinpoint Malware Detection Redeployment

Klien yang menyebarkan ulang Aplikasi perbankan online mereka selama jangka waktu layanan dan sebagai akibatnya, membutuhkan perubahan pada penyebaran mereka atas IBM Trusteer Pinpoint Malware Detection dan/atau IBM Trusteer Pinpoint Malware Detection II harus membeli IBM Trusteer Pinpoint Malware Detection Redeployment.

Penyebaran ulang dapat disebabkan oleh Klien yang mengubah domain atau URL host Aplikasi, mengonversikan Aplikasi online ke teknologi baru, berpindah ke *platform* perbankan on-line yang baru atau menambah alur login baru pada Aplikasi yang telah ada.

Untuk periode transisi penyebaran ulang 6 bulan, Klien berhak atas Aplikasi tambahan secara satu per satu yang berjalan di atas Aplikasi yang telah dilanggankan.

3.6.4 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail dan/atau IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

Untuk IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business atau IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business, penyebaran pada Aplikasi Bisnis tambahan apa pun di luar Aplikasi pertama memerlukan kepemilikan atas IBM Trusteer Pinpoint Malware Detection Additional Applications for Business. Untuk IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail atau IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail, penyebaran pada Aplikasi Ritel tambahan apa pun di luar Aplikasi pertama memerlukan kepemilikan atas IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail.

3.7 Layanan Cloud Tambahan Opsional untuk IBM Trusteer Pinpoint Criminal Detection for Business dan/atau IBM Trusteer Pinpoint Criminal Detection for Retail dan/atau untuk IBM Trusteer Pinpoint Criminal Detection II for Business dan/atau IBM Trusteer Pinpoint Criminal Detection II for Retail

3.7.1 IBM Trusteer Pinpoint Criminal Detection Redeployment

Klien yang menyebar ulang Aplikasi perbankan online mereka selama jangka waktu layanan dan sebagai akibatnya, membutuhkan perubahan pada penyebaran mereka atas Layanan Cloud IBM Trusteer Pinpoint Criminal Detection harus membeli IBM Trusteer Pinpoint Criminal Detection Redeployment.

Penyebaran ulang dapat disebabkan oleh Klien yang mengubah *domain* atau URL *host* Aplikasi, mengonversikan Aplikasi online ke teknologi baru, berpindah ke *platform* perbankan on-line yang baru atau menambah alur login baru pada Aplikasi yang telah ada.

Untuk periode transisi penyebaran ulang 6 bulan, Klien berhak atas Aplikasi tambahan secara satu per satu yang berjalan di atas Aplikasi yang telah dilanggankan.

3.7.2 IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business dan/atau IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

Untuk IBM Trusteer Pinpoint Criminal Detection II for Business, penyebaran pada Aplikasi Bisnis tambahan apa pun di luar Aplikasi pertama memerlukan kepemilikan atas IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business. Untuk IBM Trusteer Pinpoint Criminal Detection II for Retail, penyebaran pada Aplikasi Ritel tambahan apa pun di luar Aplikasi pertama memerlukan kepemilikan atas IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail.

4. IBM Trusteer Fraud Protection Suite

IBM Trusteer Fraud Protection Suite ("Suite") merupakan sekumpulan layanan berbasis cloud yang dirancang untuk memberikan lapisan proteksi terhadap penipuan dan dapat terintegrasi dengan produk IBM tambahan untuk memberikan solusi manajemen masa pakai. Suite ini mencakup layanan berbasis cloud berikut:

- IBM Trusteer Pinpoint Detect yang bertujuan untuk mendeteksi dan mengurangi *malware*, *phishing*, dan serangan pengambilalihan akun. Trusteer Pinpoint Detect dapat diintegrasikan ke dalam Aplikasi Bisnis dan/atau Aplikasi Ritel Klien yang untuknya Klien telah berlangganan cakupan Layanan Cloud dan proses pencegahan penipuan.
- IBM Trusteer Rapport for Mitigation yang bertujuan untuk memperbaiki dan melindungi titik akhir yang terinfeksi.

Layanan Cloud tersebut mencakup:

a. TMA:

   TMA tersedia pada lingkungan yang di-hosting oleh cloud IBM Trusteer, yang melaluinya Klien (dan personelnya yang sah dalam jumlah tidak terbatas) dapat: (i) menerima pelaporan data peristiwa dan penilaian risiko, dan (ii) melihat, mengonfigurasi, dan mengatur kebijakan keamanan dan kebijakan yang berkaitan dengan pelaporan data peristiwa.

b. Data peristiwa:

   Klien (dan personelnya yang sah dalam jumlah tidak terbatas) dapat menggunakan TMA untuk menerima data peristiwa yang dihasilkan dari interaksi online Peserta yang Memenuhi Syarat dengan Aplikasi(-aplikasi) Bisnis dan/atau Ritel Klien yang untuknya Klien telah berlangganan cakupan Layanan Cloud atau Klien dapat menerima data peristiwa melalui mode penyampaian API backend.

c. Skrip Web dan/atau API:

   Untuk penyebaran pada situs web untuk tujuan mengakses atau menggunakan Layanan Cloud.

Praktik Terbaik Pinpoint

Dalam hal deteksi malware atau deteksi pengambilalihan akun, Klien harus mengikuti Panduan Praktik Terbaik Pinpoint. Jangan menggunakan Layanan Cloud IBM Trusteer Pinpoint Detect dengan cara apa pun yang akan memengaruhi pengalaman Peserta yang Memenuhi Syarat segera setelah deteksi *malware* atau pengambilalihan akun, sedemikian rupa sehingga akan memungkinkan pihak lain untuk menghubungkan tindakan Klien dengan penggunaan tawaran IBM Trusteer Pinpoint Detect (misalnya, pemberitahuan, pesan, pemblokiran perangkat, atau pemblokiran akses ke Aplikasi Bisnis dan/atau Ritel segera setelah deteksi malware atau pengambilalihan akun).

4.1 IBM Trusteer Pinpoint Detect Standard for Business dan/atau IBM Trusteer Pinpoint Detect Standard for Retail

Layanan Cloud ini menggabungkan Layanan Cloud IBM Trusteer Pinpoint Criminal Detection dan IBM Trusteer Pinpoint Malware Detection untuk menawarkan solusi tunggal yang terpadu.

Solusi ini membantu pendeteksian tanpa klien (*clientless detection*) atas *malware* dan/atau aktivitas pengambilalihan akun yang mencurigakan pada *browser* yang menghubungkan ke Aplikasi Bisnis atau Ritel, menggunakan ID perangkat, deteksi *phishing*, dan deteksi pencurian kredensial yang disebabkan oleh *malware*. Tawaran IBM Trusteer Pinpoint menyediakan lapisan perlindungan lain dan bertujuan untuk mendeteksi upaya pengambilalihan akun dan memberikan skor penilaian risiko *browser* atau perangkat mobile (melalui *browser* asli atau aplikasi mobile Klien) yang mengakses Aplikasi Bisnis atau Ritel secara langsung kepada Klien.

Dukungan standar (sebagaimana yang dinyatakan dalam pasal Dukungan Teknis di bawah) tercakup dalam Layanan Cloud ini. Untuk dukungan Premium, Klien harus membeli Detect Premium.

Layanan Cloud ini mencakup perlindungan terhadap satu Aplikasi. Untuk setiap Aplikasi tambahan, Klien harus memperoleh kepemilikan Aplikasi Tambahan IBM Trusteer Pinpoint Detect Standard.

4.2 IBM Trusteer Pinpoint Detect Premium for Business dan/atau IBM Trusteer Pinpoint Detect Premium for Retail

Layanan Cloud ini menggabungkan IBM Trusteer Pinpoint Criminal Detection dan IBM Trusteer Pinpoint Malware Detection untuk menawarkan solusi tunggal terpadu yang mudah diintegrasikan.

Solusi ini membantu pendeteksian tanpa klien (*clientless detection*) atas *malware* dan/atau aktivitas pengambilalihan akun yang mencurigakan pada *browser* yang menghubungkan ke Aplikasi Bisnis atau Ritel, menggunakan ID perangkat, deteksi *phishing*, dan deteksi pencurian kredensial yang disebabkan oleh *malware*. Tawaran IBM Trusteer Pinpoint menyediakan lapisan perlindungan lain dan bertujuan untuk mendeteksi upaya pengambilalihan akun dan memberikan skor penilaian risiko *browser* atau perangkat mobile (melalui *browser* asli atau aplikasi mobile Klien) yang mengakses Aplikasi Bisnis atau Ritel secara langsung kepada Klien.

Layanan tersebut mencakup fungsionalitas dan layanan yang ditingkatkan, termasuk: penyebaran yang diperpanjang dan layanan pengaturan, kebijakan keamanan yang disesuaikan, layanan investigasi, dll.

Layanan Cloud ini mencakup perlindungan terhadap satu Aplikasi. Untuk setiap Aplikasi tambahan, Klien harus memperoleh kepemilikan atas Aplikasi Tambahan IBM Trusteer Pinpoint Detect Premium.

Dukungan premium tercakup dalam Layanan Cloud ini.

Pinpoint Detect Policy Manager:

Policy Manager disertakan dalam layanan Pinpoint Detect Premium dan tersedia di lingkungan yang diselenggarakan oleh cloud IBM Trusteer, yang melaluinya Klien (dan jumlah personelnya yang berwenang yang tidak terbatas jumlahnya) dapat: (i) merancang, menguji dan menyebar ke logika lingkungan produksi untuk mendeteksi aktivitas penipuan, (ii) merancang laporan dan dasbor, dan melihat, mengonfigurasi, serta mengatur kebijakan keamanan dan kebijakan untuk mendeteksi aktivitas yang mencurigakan pada Aplikasi pelanggan.

Layanan konsultasi diperlukan untuk aktivasi fitur Policy Manager dan untuk dukungan penyelidikan mendalam tambahan yang diperlukan. Perincian layanan konsultasi diuraikan secara terpisah dalam pernyataan kerja.

Apabila Policy Manager diaktifkan, IBM berhak untuk mengakses lingkungan Klien untuk tujuan dukungan guna menyesuaikan kebijakan Klien untuk memperbaiki masalah utama yang dihasilkan dari perubahan kebijakan.

Klien berkomitmen untuk melindungi setiap data yang diekspos melalui Policy Manager dari kesalahan penggunaan.

Apabila fitur Policy Manager diaktifkan, Klien harus mematuhi pedoman IBM untuk pengaturan aturan, sebagaimana yang diuraikan dalam dokumentasi. Klien menyatakan bahwa IBM tidak bertanggung jawab atas situasi apa pun yang dihasilkan dari ketidakpatuhan Klien terhadap rekomendasi tersebut.

Setiap masalah penurunan layanan dan/atau stabilitas yang dapat terjadi karena kesalahan konfigurasi fitur Policy Manager oleh Klien tidak akan dianggap sebagai Waktu Henti untuk perhitungan SLA.

4.3 IBM Trusteer Pinpoint Detect Standard with access management integration for Business dan/atau IBM Trusteer Pinpoint Detect Standard with access management integration for Retail

Layanan Cloud IBM Trusteer Pinpoint Detect Standard with access management integration mencakup fungsionalitas IBM Security Pinpoint Detect Standard sebagaimana yang diuraikan secara terperinci dalam pasal 4.1 di atas.

IBM Trusteer Pinpoint Detect Standard with access management integration digunakan saat dibeli dengan access management systems, misalnya IBM Security Access Management ("ISAM"). Saat dibeli bersama ISAM, kedua tawaran harus diaktifkan. Tawaran ini mencakup opsi integrasi dengan access management system. Tawaran ini tidak mencakup kepemilikan untuk access management system.

Tawaran ini mencakup perlindungan terhadap satu Aplikasi. Untuk setiap Aplikasi tambahan, Klien harus memperoleh kepemilikan Aplikasi Tambahan IBM Trusteer Pinpoint Detect Standard.

Dukungan standar (sebagaimana yang ditentukan dalam pasal Dukungan Teknis) tercakup dalam Layanan Cloud ini. IBM Trusteer Pinpoint Detect Premium with access management integration for Business dan/atau IBM Trusteer Pinpoint Detect Premium with access management integration for Retail

Layanan Cloud IBM Trusteer Pinpoint Detect Premium with access management integration mencakup fungsionalitas IBM Security Pinpoint Detect Premium sebagaimana yang diuraikan secara terperinci dalam pasal 4.2 di atas, dan opsi integrasi dengan access management system.

IBM Trusteer Pinpoint Detect Premium with access management integration digunakan saat dibeli dengan access management systems, misalnya IBM Security Access Management ("ISAM"). Saat dibeli bersama ISAM, kedua tawaran harus diaktifkan. Layanan Cloud ini mencakup opsi integrasi dengan

access management system. Tawaran ini tidak mencakup kepemilikan untuk access management system.

Layanan Cloud ini mencakup perlindungan terhadap satu Aplikasi. Untuk setiap Aplikasi tambahan, Klien harus memperoleh kepemilikan atas Aplikasi Tambahan IBM Trusteer Pinpoint Detect Premium.

Dukungan Premium termasuk dalam tawaran ini.

4.4 Layanan opsional untuk IBM Trusteer Pinpoint Detect Standard dan/atau IBM Trusteer Pinpoint Detect Premium

Untuk Layanan Cloud dalam pasal ini, terdapat prasyarat kepemilikan untuk IBM Trusteer Pinpoint Detect Premium for Retail atau IBM Trusteer Pinpoint Detect Standard for Retail.

4.5 IBM Trusteer Rapport for Mitigation for Retail dan/atau IBM Trusteer Rapport for Mitigation for Business

IBM Trusteer Rapport for Mitigation bertujuan untuk menyelidiki, memulihkan, memblokir dan menghapus infeksi *malware* dari perangkat terinfeksi (PC/MAC) Peserta yang Memenuhi Syarat Klien yang mengakses Aplikasi Ritel Klien secara *ad-hoc*, di mana infeksi *malware* telah terdeteksi oleh data peristiwa IBM Trusteer Pinpoint Detect Premium atau IBM Trusteer Pinpoint Detect Standard. Klien harus memiliki langganan saat ini untuk IBM Trusteer Pinpoint Detect Premium atau IBM Trusteer Pinpoint Detect Standard yang benar-benar berjalan pada Aplikasi Ritel Klien. Klien dapat menggunakan Layanan Cloud ini hanya sehubungan dengan Peserta yang Memenuhi Syarat yang mengakses Aplikasi Ritel Klien, dan semata-mata sebagai alat yang bertujuan untuk menginvestigasi serta memulihkan perangkat (PC/MAC) tertentu yang terinfeksi secara ad-hoc. IBM Trusteer Rapport for Mitigation for Retail harus benar-benar berjalan pada perangkat Peserta yang Memenuhi Syarat (PC/MAC) yang terpengaruh, dan Peserta yang Memenuhi Syarat yang terpengaruh tersebut harus menerima EULA, mengotentikasi dengan Aplikasi(-aplikasi) Ritel Klien setidaknya satu kali, dan konfigurasi Klien harus memasukkan koleksi ID Pengguna. Untuk menghindari keraguan, Layanan Cloud ini tidak termasuk hak untuk menggunakan Trusteer Splash dan/atau mempromosikan Perangkat Lunak Klien Pemilik Akun dengan cara lain apa pun untuk populasi umum Peserta yang Memenuhi Syarat dari Klien.

4.5.1 IBM Trusteer Pinpoint Detect Standard Additional Applications for Business dan/atau IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail dan/atau IBM Trusteer Pinpoint Detect Premium Additional Applications for Business dan/atau IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail

Untuk penyebaran IBM Trusteer Pinpoint Detect Standard for Business pada Aplikasi Bisnis tambahan apa pun di luar Aplikasi pertama memerlukan kepemilikan atas IBM Trusteer Pinpoint Detect Standard Additional Applications for Business.

Untuk penyebaran IBM Trusteer Pinpoint Detect Standard for Retail pada Aplikasi Ritel tambahan apa pun di luar Aplikasi pertama memerlukan kepemilikan atas IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail.

Untuk penyebaran IBM Trusteer Pinpoint Premium for Business pada Aplikasi Bisnis tambahan apa pun di luar Aplikasi pertama memerlukan kepemilikan atas IBM Trusteer Pinpoint Detect Premium Additional Applications for Business.

Untuk penyebaran IBM Trusteer Pinpoint Premium for Retail pada Aplikasi Ritel tambahan apa pun di luar Aplikasi pertama memerlukan kepemilikan atas IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail.

4.5.2 IBM Trusteer Pinpoint Detect Standard Redeployment dan/atau IBM Trusteer Pinpoint Detect Premium Redeployment

Klien yang menyebarkan ulang Aplikasi perbankan online mereka selama jangka waktu layanan dan sebagai akibatnya, memerlukan perubahan pada penyebaran mereka atas IBM Trusteer Pinpoint Detect harus membeli IBM Trusteer Pinpoint Detect Redeployment.

Penyebaran ulang dapat disebabkan oleh klien yang mengubah *domain* atau URL *host* Aplikasi, mengonversikan Aplikasi online ke teknologi baru, berpindah ke *platform* perbankan on-line yang baru atau menambah alur *login* baru pada Aplikasi yang telah ada.

Untuk periode transisi penyebaran ulang 6 bulan, Klien berhak atas Aplikasi tambahan secara satu per satu yang berjalan di atas Aplikasi yang telah dilanggankan.

5. Layanan Cloud IBM Trusteer Mobile

5.1 IBM Trusteer Mobile Browser for Business dan/atau IBM Trusteer Mobile Browser for Retail

IBM Trusteer Mobile Browser dirancang untuk menambah lapisan perlindungan lain dan bertujuan untuk memberikan akses online yang aman dari perangkat mobile Peserta yang Memenuhi Syarat yang mengakses Aplikasi Ritel atau Bisnis Klien yang untuknya Klien telah berlangganan cakupan Layanan Cloud, penilaian risiko perangkat mobile, dan perlindungan *phishing*. Deteksi Wi-Fi aman hanya tersedia untuk *platform* Android. Untuk tujuan perangkat mobile Layanan Cloud ini mencakup telepon seluler atau tablet dan tidak termasuk Laptop PC dan Mac.

Melalui TMA, Klien dapat menerima data peristiwa, analisis, dan informasi statistik yang berkaitan dengan Perangkat milik Peserta yang Memenuhi Syarat yang telah: (i) mengunduh Perangkat Lunak Klien Pemegang Akun, suatu aplikasi yang dilisensikan untuk publik berdasarkan perjanjian lisensi pengguna akhir ("EULA") tanpa biaya, dan tersedia untuk diunduh ke perangkat mobile Peserta yang Memenuhi Syarat, dan (ii) menerima EULA dan dikonfirmasi setidaknya satu kali dengan Aplikasi Bisnis atau Ritel Klien yang untuknya Klien telah berlangganan cakupan Layanan Cloud. Klien hanya dapat memasarkan Perangkat Lunak Klien Pemegang Akun menggunakan Trusteer Splash dan tidak dapat menggunakan Perangkat Lunak Klien Pemegang Akun untuk operasi bisnis internalnya.

a. Data peristiwa:

   Klien (dan personelnya yang sah dalam jumlah tidak terbatas) dapat menggunakan TMA untuk menerima data peristiwa yang dihasilkan dari interaksi online pada perangkat mobile dengan Aplikasi Ritel atau Bisnis Klien yang untuknya Klien telah berlangganan cakupan Layanan Cloud.

b. Trusteer Splash:

   Platform pemasaran Trusteer Splash mengidentifikasi dan memasarkan Perangkat Lunak Klien Pemegang Akun kepada Peserta yang Memenuhi Syarat yang mengakses Aplikasi Bisnis dan/atau Ritel Klien yang untuknya Klien telah berlangganan cakupan Layanan Cloud. Klien dapat memilih dari templat splash yang tersedia ("Templat Splash"). Splash yang disesuaikan dapat dikontrak berdasarkan perjanjian atau pernyataan kerja yang terpisah.

Klien dapat menyetujui untuk memberikan merek dagang, logo, atau lambangnya untuk penggunaan yang terkait dengan TMA dan hanya untuk penggunaan dengan Trusteer Splash dan untuk ditampilkan di Perangkat Lunak Klien Pemegang Akun atau pada halaman awal yang diselenggarakan (*hosted*) oleh IBM atau pada situs web IBM Trusteer. Setiap penggunaan merek dagang, logo, atau lambang yang diberikan akan sesuai dengan kebijakan IBM yang wajar mengenai iklan dan penggunaan merek dagang.

5.2 IBM Trusteer Mobile SDK for Business dan/atau IBM Trusteer Mobile SDK for Retail

Layanan Cloud IBM Trusteer Mobile SDK dirancang untuk menambah lapisan perlindungan lain untuk memberikan akses web aman ke Aplikasi Bisnis dan/atau Ritel Klien yang untuknya Klien telah berlangganan cakupan Layanan Cloud, penilaian risiko perangkat, dan perlindungan *pharming*. Deteksi Wi-Fi aman hanya tersedia untuk *platform* Android.

Layanan Cloud IBM Trusteer Mobile SDK mencakup alat pengembang perangkat lunak ("SDK") mobile hak milik, paket perangkat lunak yang berisi dokumentasi, pustaka perangkat lunak hak milik pemrograman serta file dan item terkait lainnya yang dikenal sebagai pustaka mobile IBM Trusteer serta "Komponen Run-time", atau "Redistributable (Dapat Didistribusikan Kembali)", kode hak milik yang dihasilkan oleh IBM Trusteer Mobile SDK yang dapat dilekatkan dan diintegrasikan ke dalam aplikasi mobile iOS atau Android Klien yang berdiri sendiri dan terlindungi yang untuknya Klien telah berlangganan cakupan Layanan Cloud. ("Aplikasi Mobile Terpadu Klien").

IBM Trusteer Mobile SDK for Retail tersedia dalam paket berisi 100 Peserta yang Memenuhi Syarat atau paket dari 100 Perangkat Klien, dan IBM Trusteer Mobile SDK for Business tersedia dalam paket berisi 10 Peserta yang Memenuhi Syarat atau paket dari 10 Perangkat Klien.

Melalui TMA, Klien (dan personelnya yang sah dalam jumlah tidak terbatas) dapat menerima pelaporan data peristiwa dan penilaian kecenderungan risiko. Melalui Aplikasi Mobile Terpadu Klien, Klien dapat menerima analisis risiko dan informasi perangkat mobile yang berkaitan dengan perangkat mobile Peserta yang Memenuhi Syarat yang telah mengunduh Aplikasi Mobile Terpadu Klien yang memungkinkan Klien untuk merumuskan kebijakan pencegahan penipuan yang menerapkan tindakan penanggulangan terhadap risiko-risiko ini. Untuk tujuan tawaran ini, "perangkat mobile" hanya mencakup ponsel dan tablet yang didukung serta tidak termasuk PC atau MAC.

Klien dapat:

a. secara internal menggunakan IBM Trusteer Mobile SDK hanya untuk tujuan mengembangkan Aplikasi Mobile Terintegrasi Klien;

b. menyematkan Redistributable (hanya dalam format kode objek) sebagai suatu cara yang integral dan tidak terpisahkan dalam Aplikasi Mobile Terpadu Klien. Setiap bagian Redistributable yang diubah atau digabung sesuai dengan pemberian lisensi ini tunduk pada syarat-syarat Uraian Layanan ini; dan

c. memasarkan dan mendistribusikan Redistributable untuk diunduh ke perangkat mobile Peserta yang Memenuhi Syarat atau ke pemegang Perangkat Klien, dengan ketentuan bahwa:

- Kecuali sebagaimana yang diizinkan secara tegas dalam Perjanjian ini, Klien tidak dapat (1) menggunakan, menyalin, memodifikasi, atau mendistribusikan SDK; (2) merakit balik, mengompilasi balik, atau jika tidak, menerjemahkan, atau merekayasa balik SDK, kecuali sebagaimana yang diizinkan oleh hukum tanpa kemungkinan pengabaian kontrak; (3) mensublisensikan, menyewakan, atau menyewagunakan SDK, (4) menghapus setiap file hak cipta atau file pemberitahuan yang terdapat dalam Redistributable; (5) menggunakan nama jalur (*path name*) yang sama dengan file/modul Redistributable asli; dan (6) menggunakan nama atau merek dagang IBM, pemberi lisensinya, atau distributornya sehubungan dengan pemasaran Aplikasi Mobile Terintegrasi Klien tanpa izin tertulis sebelumnya dari IBM atau pemberi lisensi atau distributor tersebut.
- Redistributable harus tetap terintegrasi dalam cara yang tidak dapat dipisahkan dalam Aplikasi Mobile Terpadu Klien. Redistributable harus berupa bentuk kode objek saja dan harus sesuai dengan semua panduan, petunjuk, dan spesifikasi dalam SDK dan dokumentasinya. Perjanjian lisensi pengguna akhir untuk Aplikasi Mobile Terintegrasi Klien harus memberi tahu pengguna akhir bahwa Redistributable tidak dapat i) digunakan untuk tujuan apa pun selain untuk mengaktifkan Aplikasi Mobile Terintegrasi Klien, ii) disalin (kecuali untuk tujuan pencadangan), iii) didistribusikan atau ditransfer lebih lanjut iv) dirakit balik, dikompilasi balik, atau jika tidak, diterjemahkan kecuali sebagaimana yang diizinkan secara spesifik oleh hukum dan tanpa kemungkinan pengabaian kontrak. Perjanjian lisensi Klien setidaknya harus memberi perlindungan kepada IBM yang setara dengan perlindungan yang diberikan oleh syarat-syarat dalam Perjanjian ini.
- SDK hanya dapat disebarkan sebagai bagian dari pengembangan internal Klien dan pengujian unit pada perangkat pengujian mobile Klien yang ditetapkan. Klien tidak berwenang untuk menggunakan SDK untuk memproses beban kerja produksi, melakukan simulasi beban kerja produksi atau menguji skalabilitas kode, aplikasi atau sistem apa pun. Klien tidak berwenang untuk menggunakan setiap bagian dari SDK untuk tujuan lain apa pun.

Klien sepenuhnya bertanggung jawab atas pengembangan, pengujian dan dukungan Aplikasi Mobile Terpadu Klien. Klien bertanggung jawab atas semua bantuan teknis untuk Aplikasi Mobile Terpadu Klien dan setiap modifikasi pada Redistributable yang dilakukan oleh Klien sebagaimana yang diizinkan dalam dokumen ini.

Klien berwenang untuk memasang dan menggunakan Redistributable dan IBM Security Mobile SDK hanya untuk mendukung penggunaan Klien atas Layanan Cloud.

IBM telah menguji contoh aplikasi yang dibuat dengan alat mobile yang tersedia dalam IBM Trusteer Mobile SDK ("Mobile Tool") untuk menentukan apakah contoh aplikasi tersebut akan berjalan dengan baik pada versi tertentu platform sistem operasi mobile dari Apple (iOS), Google (Android), dan lain-lain (secara bersama-sama disebut "Platform OS Mobile"), namun, Platform OS Mobile yang disediakan oleh pihak ketiga, tidak berada di bawah kendali IBM dan dapat berubah tanpa pemberitahuan kepada IBM. Dengan demikian, dan terlepas dari ketentuan apa pun yang mengatur sebaliknya, IBM tidak menjamin bahwa setiap aplikasi atau output lain yang dibuat dengan menggunakan Peralatan Mobile akan berjalan dengan baik pada, beroperasi bersama atau kompatibel dengan Platform OS Mobile atau perangkat mobile apa pun.

Komponen Sumber dan Materi Sampel – IBM Trusteer Mobile SDK dapat mencakup beberapa komponen dalam bentuk kode sumber ("Komponen Sumber") dan materi lainnya yang teridentifikasi sebagai Materi Sampel. Klien dapat menyalin dan memodifikasi Komponen Sumber dan Materi Sampel hanya untuk penggunaan internal dengan ketentuan bahwa penggunaan tersebut berada dalam batas-batas hak lisensi berdasarkan Perjanjian ini, namun dengan ketentuan bahwa Klien tidak dapat mengubah atau menghapus informasi atau pemberitahuan hak cipta apa pun yang terdapat dalam

Komponen Sumber atau Materi Sampel. IBM memberikan Komponen Sumber dan Materi Sampel tanpa adanya kewajiban dukungan dan "SEBAGAIMANA ADANYA", TANPA ADANYA JAMINAN DALAM BENTUK APA PUN, BAIK SECARA TEGAS ATAUPUN TERSIRAT, TERMASUK JAMINAN HAK MILIK, TIDAK ADANYA PELANGGARAN ATAU TIDAK ADANYA GANGGUAN SERTA JAMINAN DAN KETENTUAN TERSIRAT TENTANG KELAYAKAN UNTUK DIPERJUALBELIKAN DAN KESESUAIAN UNTUK TUJUAN TERTENTU. Harap diperhatikan bahwa Komponen Sumber atau Materi Sampel disediakan hanya sebagai contoh mengenai cara untuk mengimplementasikan Embeddable ke dalam CIMA, Komponen Sumber atau Materi Sampel mungkin tidak kompatibel dengan lingkungan pengembangan Klien, dan Klien sepenuhnya bertanggung jawab atas pengujian dan implementasi Embeddable ke dalam CIMA-nya.

Klien setuju untuk menciptakan, menyimpan, dan memberikan kepada IBM dan auditornya, catatan tertulis yang akurat, output alat sistem, dan informasi sistem lainnya yang memadai untuk memberikan verifikasi yang dapat diaudit bahwa penggunaan Klien atas IBM Trusteer Mobile SDK mematuhi syarat-syarat Uraian Layanan ini.

6. Dukungan Premium

Klien berhak atas Dukungan Premium hanya untuk Layanan Cloud yang untuknya Klien telah berlangganan tawaran Dukungan Premium terkait.

7. Penyebaran IBM Trusteer Fraud Protection

Untuk setiap Aplikasi yang dilangganken oleh Klien, langganan dasar Klien mencakup pengaturan wajib dan aktivitas penyebaran awal pada IBM Trusteer cloud, termasuk startup awal satu kali, konfigurasi, Templat Splash, pengujian, dan pelatihan.

Aktivitas penyebaran tidak termasuk aktivitas implementasi yang diperlukan pada sistem atau Aplikasi Klien.

Tahap implementasi dari berbagai macam Layanan Cloud dirancang untuk diimplementasikan dalam kerangka waktu sebagaimana yang diuraikan secara terperinci dalam panduan penyebaran yang sesuai.

Penyelesaian tahapan implementasi ini dalam kerangka waktu yang dialokasikan bergantung pada komitmen dan partisipasi penuh dari personel dan manajemen Klien. Klien harus memberikan informasi yang diperlukan dengan tepat waktu. Kinerja IBM didasarkan atas informasi dan keputusan yang tepat waktu dari Klien dan penundaan apa pun dapat mengakibatkan biaya tambahan dan/atau penundaan penyelesaian layanan implementasi ini.

Untuk setiap Aplikasi yang dilangganken oleh Klien, langganan dasar Klien mencakup pengaturan wajib dan aktivitas penyebaran awal pada IBM Trusteer cloud, termasuk startup awal satu kali, konfigurasi, Templat Splash, pengujian, dan pelatihan.

Langganan Klien mencakup dukungan dan pengujian untuk halaman dalam aplikasi Klien tersebut yang akan ditandai sebagai direkomendasikan oleh IBM dalam penyebaran awal. IBM tidak bertanggung jawab atas: (i) penyebaran sebagian, (ii) pilihan Klien untuk tidak menyebarkan layanan cloud IBM sebagaimana yang direkomendasikan oleh IBM, atau (iii) pilihan Klien untuk menjalankan penyebaran, pengaturan, dan pengujian sendiri. (IV) Penyebaran sebagian atau perlindungan yang dihasilkan dari informasi yang tidak cukup yang diberikan oleh Klien. Layanan tambahan, termasuk aktivitas penyebaran di luar penyebaran awal, dapat dikontrak untuk biaya tambahan berdasarkan perjanjian terpisah.

8. Kerahasiaan dan Keamanan Data

Layanan Cloud ini mematuhi prinsip-prinsip kerahasiaan dan keamanan data IBM untuk Layanan Cloud yang tersedia dihttp://www.ibm.com/cloud/data-security dan setiap syarat-syarat tambahan yang diatur dalam pasal ini. Setiap perubahan pada prinsip-prinsip kerahasiaan dan keamanan data IBM tidak akan menurunkan keamanan Layanan Cloud.

Layanan Cloud ini dapat digunakan untuk memproses konten yang berisi data pribadi apabila Klien, sebagai pengontrol data, memutuskan bahwa tindakan keamanan organisasi dan teknis sesuai dengan risiko yang ditimbulkan oleh pemrosesan dan sifat data yang akan dilindungi. Klien memahami bahwa Layanan Cloud ini tidak menawarkan fitur untuk perlindungan data pribadi sensitif atau data yang tunduk pada persyaratan peraturan tambahan.

Layanan Cloud ini dicakup dalam sertifikasi Perlindungan Kerahasiaan IBM dan berlaku ketika Klien memilih untuk memiliki Layanan Cloud yang diselenggarakan (*hosted*) dalam pusat data di Amerika Serikat, dan tunduk pada Kebijakan Kerahasiaan Perlindungan Kerahasiaan IBM, yang tersedia di http://www.ibm.com/privacy/details/us/en/privacy_shield.html.

8.1 Fitur Keamanan dan Tanggung Jawab

Layanan Cloud menerapkan fitur-fitur keamanan berikut ini:

Layanan Cloud mengenkripsi konten selama transmisi data ke dan dari jaringan IBM dan saat menunggu transmisi data dari titik akhir.

8.2 Persetujuan dan Penggunaan yang Sah Secara Hukum

Penggunaan yang Sah Secara Hukum

Penggunaan Layanan Cloud ini dapat melibatkan berbagai peraturan perundang-undangan atau regulasi. Layanan Cloud dapat digunakan hanya untuk tujuan yang sah dan dengan cara yang sah secara hukum. Klien setuju untuk menggunakan Layanan Cloud sesuai dengan, dan menanggung seluruh tanggung jawab untuk mematuhi peraturan perundang-undangan, regulasi dan kebijakan yang berlaku.

Kewenangan untuk Mengumpulkan dan Memproses Data

Layanan Cloud akan mengumpulkan informasi dari Peserta yang Memenuhi Syarat dan Perangkat Klien yang berinteraksi dengan Aplikasi Bisnis dan Ritel yang untuknya Klien telah berlangganan ke cakupan Layanan Cloud. Layanan Cloud mengumpulkan informasi yang secara sendiri atau gabungan dapat dianggap sebagai Data Pribadi dalam beberapa yurisdiksi. Data Pribadi adalah setiap informasi yang dapat digunakan untuk mengidentifikasi individu tertentu, seperti nama, alamat email, alamat rumah, atau nomor telepon yang diberikan kepada IBM untuk disimpan, diproses, atau ditransfer atas nama Klien.

Praktik pengumpulan dan pemrosesan data dapat diperbarui untuk meningkatkan fungsi Layanan Cloud. Dokumen dengan uraian lengkap mengenai praktik pengumpulan dan pemrosesan data diperbarui sesuai kebutuhan dan tersedia untuk Klien sesuai permintaan. Klien memberi wewenang kepada IBM untuk mengumpulkan informasi ini dan memprosesnya sesuai dengan pasal Transfer Lintas Batas dan pasal Kerahasiaan Data dalam Uraian Layanan ini.

Untuk tawaran IBM Trusteer yang mencakup Aplikasi Trusteer Management (Trusteer Management Application - "TMA"):

Data berikut ini dikumpulkan dan disimpan di Aplikasi Trusteer Management (TMA) untuk administrator TMA dari perusahaan sponsor: alamat email (sebagai *login*), kata sandi yang di-*hash*, nama yang diberikan, nama belakang, jabatan pekerjaan, dan departemen.

Untuk Layanan Cloud IBM Trusteer Pinpoint:

Data yang dikumpulkan dapat termasuk:

- pengenal pengguna atau titik akhir misalnya ID Pengguna terenkripsi atau yang di-hash satu arah, ID Pengguna Tetap (Persistent User ID - "PUID"), Kunci Agen Rapport, dan ID Sesi Pelanggan;
- data yang berkaitan dengan aplikasi yang dilindungi, seperti atribut/elemen spesifik dari aplikasi perbankan online pelanggan sebagaimana yang diberikan dalam *browser*, kunjungan situs web dan riwayat pencarian pengguna akhir;
- informasi lingkungan perangkat lunak yang dipasang, pengaturan dan atribut perangkat serta browser, dan panjang riwayat *browser*;
- informasi perangkat keras dan cap waktu (*timestamp*);
- *header browser* dan data protokol komunikasi, seperti alamat IP, *cookies*, *header* pengarah, dan *header* HTTP pengguna lainnya;
- data pergerakan *mouse* pengguna akhir, seperti koordinat penunjuk *mouse*, jumlah klik, dan gerakan roda gulir (dan yang setara) serta cap waktu ketika berinteraksi dengan aplikasi perbankan online Klien;
- situs *phishing* dan informasi yang dimasukkan ke dalam situs *phishing*; dan
- atas pilihan Klien sendiri, data transaksional (jumlah transaksi, mata uang transaksi dan kode tujuan, pengenal bank target transaksi yang di-*hash* satu arah, pengenal rekening target transaksi yang di-*hash* satu arah, nilai biner jika transaksi dilakukan pihak penerima pembayaran yang baru, dan tanggal/waktu transaksi) dan skor data risiko opsional.
- atas pilihan Klien sendiri, ritme ketikan pada *keyboard* dan urutan kelompok tombol (*keystroke*) yang digunakan oleh pengguna akhir untuk memasukkan nama pengguna, kata sandi, dan teks lain (namun bukan huruf, angka atau karakter khusus itu sendiri, dan tanpa kemampuan untuk mengenali nama pengguna atau kata sandi);

Apabila Policy Manager diaktifkan, semua data yang diperbanyak yang digunakan merupakan tanggung jawab Klien sepenuhnya. IBM menyarankan untuk menge-*hash* atau mengenkripsi data apa pun yang dapat dianggap sebagai Pengenal Pribadi.

Klien memahami dan menyetujui bahwa IBM tidak mengumpulkan, menyimpan, mengelola atau memelihara buku dan/atau catatan resmi tentang Klien.

Saat Klien berlangganan tawaran IBM Trusteer Rapport for Remediation atau dalam beberapa kasus dukungan Pinpoint, IBM dapat merekomendasikan agar Perangkat Lunak Klien Pemegang Akun Rapport dipasang pada mesin Peserta yang Memenuhi Syarat untuk meneliti dan menginvestigasi dugaan infeksi malware. Data yang dikumpulkan untuk tawaran Rapport tercantum di bawah ini.

Untuk Layanan Cloud IBM Trusteer Rapport (termasuk Rapport for Remediation atau Rapport for Mitigation saat disebarkan sehubungan dengan tawaran Pinpoint):

Data yang dikumpulkan dapat termasuk:

- URL dan alamat Protokol Internet (*Internet protocol* - "IP") situs web yang dikunjungi oleh Pemegang Akun yang dianggap oleh IBM berpotensi sebagai penipuan, *phishing* atau eksploitatif, bersama dengan informasi mengenai sifat ancaman yang teridentifikasi;
- URL dan alamat IP situs web yang dikunjungi Pemegang Akun situs web yang dikendalikan oleh Klien dan dilindungi oleh Layanan Cloud, misalnya situs perbankan online; alamat IP Pemegang Akun;
- informasi mengenai identifikasi perangkat keras, sistem pengoperasian, perangkat lunak aplikasi, perangkat keras periferal, konfigurasi keamanan, pengaturan sistem, dan koneksi jaringan titik akhir, serta ID, nama, pola penggunaan, dan informasi titik akhir yang dapat diidentifikasi lainnya;
- informasi yang berkaitan dengan pemasangan dan pengoperasian program, ID program, versi program, peristiwa keamanan yang dihasilkan dari titik akhir, dan informasi mengenai kesalahan program;
- statistik penggunaan dan informasi statistik mengenai ancaman yang terdeteksi oleh program; file *log* yang berisi gangguan *browser*, tanggal dan waktu infeksi, serta informasi mengenai sifat ancaman atau gangguan fungsi yang teridentifikasi;
- Afiliasi Klien, juga disebut sebagai Perusahaan Pemberi Sponsor. Suatu afiliasi didirikan saat pengguna akhir mengunduh Rapport dari situs web Klien, memilih Klien tertentu saat mengunduh Rapport dari situs dukungan Trusteer, atau masuk ke aplikasi perbankan Klien. Seorang pengguna akhir dapat memiliki lebih dari satu afiliasi Klien;
- salinan ID Pengguna terenkripsi yang digunakan oleh Pemegang Akun untuk berinteraksi dengan Klien (opsional);
- salinan nomor kartu kredit terenkripsi yang dimasukkan oleh Pemegang Akun ke dalam situs setelah program menginformasikan kepada Pemegang Akun bahwa program menganggap situs tersebut berisiko;
- file dan informasi lain dari titik akhir yang dicurigai oleh ahli keamanan IBM dapat berkaitan dengan *malware* atau aktivitas kejahatan lainnya, atau yang dapat dihubungkan dengan gangguan fungsi program secara umum; dan
- Informasi kontak pribadi, termasuk nama dan email, saat pengguna akhir menghubungi Dukungan.

Untuk tawaran IBM Trusteer Mobile SDK dan Layanan Cloud IBM Trusteer Mobile Browser:

Data yang dikumpulkan dapat termasuk:

- pengenal pengguna, seperti ID Pengguna terenkripsi atau yang di-*hash* satu arah;
- informasi perangkat, seperti alamat IP, ID perangkat yang di-*hash*, cap waktu (*timestamp*), nilai MD5 paket yang terpasang serta informasi perangkat keras dan perangkat lunak lainnya;
- versi SDK Mobile atau Browser Mobile dan tanggal pemasangan;
- kunjungan ke aplikasi yang dilindungi;
- Afiliasi Klien; dan
- data risiko perangkat (misalnya, kehadiran *malware*, *root hider*, status enkripsi Wi-Fi, apakah suatu perangkat di-*jailbreak*);
- *stack trace* gangguan (dalam hal pengakhiran aplikasi tidak terduga);

- data *build* telepon (misalnya, model, produsen);
- interaksi layar sentuh pengguna akhir termasuk koordinat x, y, area sentuh, dan jenis tindakan (turun, naik dan bergerak);
- data sensor gerakan, penggunaan daya/sumber daya, pengaturan konektivitas, sensor lingkungan seperti suhu, cahaya dan tekanan udara serta pengaturan perangkat umum (volume, dering, tingkat kecerahan layar, dll.).

8.3 Persetujuan yang Diinformasikan dari Subjek Data

Untuk Layanan Cloud IBM Trusteer Pinpoint dan untuk Layanan Cloud IBM Trusteer Mobile SDK:

Klien menyetujui bahwa pihaknya telah atau akan mendapatkan setiap persetujuan, izin, atau lisensi yang diinformasikan sepenuhnya yang diperlukan untuk memungkinkan penggunaan Layanan Cloud yang sah dan untuk mengizinkan pengumpulan dan pemrosesan informasi oleh IBM melalui Layanan Cloud.

Untuk Layanan Cloud IBM Trusteer Rapport (termasuk Rapport Remediation atau Rapport for Mitigation saat disebarkan sehubungan dengan Layanan Cloud Pinpoint), dan Layanan Cloud IBM Trusteer Mobile Browser:

Klien memberikan wewenang kepada IBM untuk mendapatkan persetujuan yang diinformasikan sepenuhnya yang diperlukan untuk memungkinkan penggunaan Layanan Cloud yang sah secara hukum serta untuk mengumpulkan dan memproses informasi sebagaimana yang diuraikan dalam Perjanjian Lisensi Pengguna Akhir yang tersedia di https://www.trusteer.com/support/end-user-license-agreement. Jika Klien menentukan bahwa pihaknya (dan bukan IBM) akan menangani komunikasi persetujuan dengan pengguna akhir, Klien setuju bahwa pihaknya telah atau akan memperoleh setiap persetujuan, izin, atau lisensi yang diinformasikan sepenuhnya yang diperlukan untuk memungkinkan penggunaan Layanan Cloud yang sah secara hukum dan untuk mengizinkan pengumpulan dan pemrosesan informasi oleh IBM sebagai prosesor data Klien melalui Layanan Cloud.

8.4 Penggunaan Data Keamanan

Sebagai bagian dari Layanan Cloud, yang mencakup aktivitas pelaporan, IBM akan mempersiapkan dan memelihara informasi yang di-deidentifikasi dan/atau agregat yang dikumpulkan dari Layanan Cloud ("Data Keamanan"). Data Keamanan tidak akan mengidentifikasi Klien, Peserta yang Memenuhi Syarat darinya, atau individu, kecuali sebagaimana yang diatur dalam butir (d) di bawah ini. Klien menyetujui bahwa IBM dapat secara terus-menerus menggunakan dan/atau menyalin Data Keamanan hanya untuk tujuan berikut ini:

a. memublikasikan dan/atau mendistribusikan Data Keamanan (misalnya dalam kompilasi dan/atau analisis yang berkaitan dengan keamanan dunia maya);

b. mengembangkan atau meningkatkan produk atau layanan;

c. menjalankan penelitian secara internal atau dengan pihak ketiga;

d. membagi informasi pelaku pihak ketiga yang dikonfirmasi secara sah menurut hukum; dan

e. aturan yang dideidentifikasi dari Policy Manager.

8.5 Transfer Lintas Batas

Klien menyetujui bahwa IBM dapat memproses konten, termasuk setiap Data Pribadi, sebagaimana yang diidentifikasi dalam pasal Penggunaan yang Sah secara Hukum dan Persetujuan di atas, berdasarkan peraturan perundang-undangan dan persyaratan yang relevan lintas batas negara ke prosesor dan sub-prosesor di negara berikut di luar Wilayah Ekonomi Eropa dan negara-negara yang dianggap oleh Komisi Eropa memiliki tingkat keamanan yang memadai: Amerika Serikat.

8.6 Kerahasiaan Data

Apabila Klien menyediakan Data Pribadi kepada Layanan Cloud di Negara Anggota Uni Eropa, Islandia, Liechtenstein, Norwegia, atau Swiss, atau apabila Klien memiliki Peserta yang Memenuhi Syarat atau Perangkat Klien di negara-negara tersebut, maka Klien sebagai satu-satunya pengendali menunjuk IBM sebagai prosesor untuk memproses (sebagaimana syarat-syarat tersebut ditentukan dalam EU Directive 95/46/EC) Data Pribadi. IBM hanya akan memproses Data Pribadi tersebut sejauh yang diperlukan untuk menyediakan tawaran Layanan Cloud sesuai dengan uraian Layanan Cloud yang dipublikasikan oleh IBM dan Klien menyetujui bahwa setiap pemrosesan tersebut sesuai dengan instruksi Klien. IBM akan memberikan pemberitahuan sebelumnya secara wajar melalui Portal Pelanggan jika IBM membuat

perubahan materi pada lokasi pemrosesan atau caranya mengamankan Data Pribadi sebagai bagian dari Layanan Cloud. Klien dapat mengakhiri periode langganan yang sedang berjalan untuk Layanan Cloud yang terpengaruh, dengan menyampaikan pemberitahuan tertulis kepada IBM dalam jangka waktu tiga puluh (30) hari sejak pemberitahuan IBM mengenai perubahan tersebut kepada Klien.

Para pihak atau afiliasi mereka yang terkait dapat mengadakan perjanjian EU Model Clause standar yang tidak dimodifikasi secara terpisah dalam peran mereka yang terkait sesuai dengan EC Decision 2010/87/EU dengan menghapus klausul opsional. Semua sengketa atau tanggung jawab yang timbul berdasarkan perjanjian-perjanjian ini, bahkan apabila disetujui oleh para afiliasi, akan diperlakukan oleh para pihak seolah-olah sengketa atau tanggung jawab tersebut timbul di antara mereka berdasarkan syarat-syarat Perjanjian ini.

a. Klien menyetujui bahwa untuk layanan yang disediakan melalui pusat data Jerman, sebagaimana yang ditentukan selama proses penyediaan, IBM dapat memproses konten termasuk setiap Data Pribadi lintas batas negara ke prosesor dan sub-prosesor berikut ini:

Nama Prosesor/Sub-prosesor	Peran (Prosesor atau Sub-prosesor Data)	Lokasi
Entitas IBM yang mengadakan kontrak	Prosesor	Sebagaimana yang dinyatakan dalam Dokumen Transaksi
Amazon Web Services (Jerman)	Sub-prosesor	Jerman
IBM Ireland Ltd.	Prosesor	Irlandia
IBM Israel Ltd.	Prosesor	Israel

Untuk layanan yang diberikan melalui pusat data Jerman, beberapa layanan dukungan pelanggan dapat diberikan oleh karyawan Trusteer yang berada di negara Uni Eropa mana pun.

b. Klien menyetujui bahwa untuk layanan yang disediakan melalui pusat data Jepang, sebagaimana yang ditentukan selama proses penyediaan, IBM dapat memproses konten termasuk Data Pribadi apa pun lintas batas negara ke prosesor dan sub-prosesor berikut ini:

Nama Prosesor/Sub-prosesor	Peran (Prosesor atau Sub-prosesor Data)	Lokasi
Entitas IBM yang mengadakan kontrak	Prosesor	Jepang, sebagaimana yang dinyatakan dalam Dokumen Transaksi
Amazon Web Services (Jepang)	Sub-prosesor	Jepang
IBM Ireland Ltd.	Prosesor	Irlandia
IBM Israel Ltd.	Prosesor	Israel

c. Klien menyetujui bahwa untuk layanan yang disediakan melalui pusat data Amerika Serikat, IBM dapat memproses konten termasuk Data Pribadi apa pun lintas batas negara ke prosesor dan sub-prosesor berikut ini:

Nama Prosesor/Sub-prosesor	Peran (Prosesor atau Sub-prosesor Data)	Lokasi
Entitas IBM yang mengadakan kontrak	Prosesor	Sebagaimana yang dinyatakan dalam Dokumen Transaksi
Amazon Web Services LLC	Sub-prosesor	Amerika Serikat
IBM Ireland Ltd.	Prosesor	Irlandia
IBM Israel Ltd.	Prosesor	Israel
IBM Corp	Prosesor	Amerika Serikat

d. Untuk layanan yang diberikan melalui pusat data yang tercantum dalam Pasal 8.5.c di atas, "pusat data Amerika Serikat", IBM juga dapat memproses melalui satu atau lebih sub-prosesor yang berlaku berikut ini, sebagaimana yang ditentukan selama proses penyediaan:

Nama Prosesor/Sub-prosesor	Peran (Prosesor atau Sub-prosesor Data)	Lokasi
Amazon Web Services (Australia)	Sub-prosesor	Australia
Amazon Web Services (Singapura)	Sub-prosesor	Singapura
Amazon Web Services (Irlandia)	Sub-prosesor	Irlandia

e. Klien menyetujui bahwa IBM dapat, dengan pemberitahuan melalui Portal Pelanggan, memindahkan pemrosesan dari Amazon Web Services ke pusat data IBM. Selain itu, IBM dapat, dengan pemberitahuan melalui Portal Pelanggan, menyesuaikan daftar dari sub-prosesor di atas.

f. Data Pemegang Akun akan diproses di wilayah di mana Pemegang Akun memasang Perangkat Lunak Klien Pemegang Akun pertama kalinya. Hal ini dapat berarti bahwa konten Pemegang Akun dapat diproses di wilayah asal serta di wilayah yang disetujui dengan Klien.

g. Data dukungan pelanggan disimpan di server cloud Salesforce.com yang berlokasi di Irlandia.

h. Untuk tujuan klarifikasi, karena Trusteer Fraud Protection merupakan suatu solusi terintegrasi, jika Klien mengakhiri salah satu dari Layanan Cloud ini, IBM dapat menyimpan data Klien untuk tujuan menyediakan Layanan Cloud yang tersisa kepada Klien sesuai dengan Uraian Layanan ini.

9. Perjanjian Tingkat Layanan

IBM memberikan perjanjian tingkat layanan (*Service Level Agreement* - "SLA") ketersediaan berikut untuk Layanan Cloud sebagaimana yang ditetapkan dalam Bukti Kepemilikan (PoE). SLA bukan merupakan suatu jaminan. SLA tersedia hanya untuk Klien dan berlaku hanya untuk penggunaan di lingkungan produksi.

9.1 Kredit yang Tersedia

Klien harus mencatatkan tiket dukungan Tingkat Permasalahan 1 dengan bagian bantuan (*help desk*) dukungan teknis IBM dalam waktu 24 jam sejak pertama kali menyadari bahwa suatu peristiwa telah berdampak pada ketersediaan Layanan Cloud. Klien harus membantu IBM secara wajar dalam setiap diagnosis dan penyelesaian masalah.

Klaim tiket dukungan atas kegagalan untuk memenuhi suatu SLA harus diajukan dalam waktu tiga hari kerja setelah akhir bulan masa kontrak. Kompensasi untuk klaim SLA yang sah akan menjadi kredit terhadap tagihan yang akan datang untuk Layanan Cloud berdasarkan durasi waktu saat pemrosesan sistem produksi untuk Layanan Cloud tidak tersedia ("Waktu Henti"). Waktu Henti dihitung dari waktu Klien melaporkan peristiwa tersebut hingga waktu Layanan Cloud dipulihkan dan tidak termasuk waktu yang berkaitan dengan penghentian untuk pemeliharaan yang terjadwal atau telah diumumkan; sebab-sebab di luar kendali IBM; masalah dengan rancangan atau instruksi, konten atau teknologi Klien atau pihak ketiga; konfigurasi sistem dan platform yang tidak didukung atau kesalahan Klien lainnya; atau insiden keamanan yang disebabkan oleh Klien atau pengujian keamanan Klien. IBM akan memberlakukan kompensasi yang berlaku paling tinggi berdasarkan ketersediaan kumulatif Layanan Cloud selama masing-masing bulan masa kontrak, sebagaimana yang ditunjukkan dalam tabel di bawah. Total kompensasi yang berkaitan dengan bulan masa kontrak mana pun tidak dapat melampaui 10 persen dari satu per dua belas (1/12) dari biaya tahunan untuk Layanan Cloud.

9.2 Tingkat Layanan

Ketersediaan Layanan Cloud selama suatu bulan masa kontrak

Ketersediaan selama suatu bulan masa kontrak	Kompensasi (% dari biaya langganan bulanan* untuk bulan masa kontrak yang merupakan pokok klaim)
< 99,5%	2%
< 98,0%	5%
< 96,0%	10%

* Jika Layanan Cloud diperoleh dari Mitra Bisnis IBM, biaya langganan bulanan akan dihitung sesuai daftar harga yang berlaku pada saat itu untuk Layanan Cloud yang berlaku selama bulan masa kontrak yang merupakan pokok klaim, yang didiskon sebesar 50%. IBM akan menyediakan suatu potongan harga secara langsung untuk Klien.

Tingkat Layanan dan Kredit Layanan yang terkait diukur secara terpisah per Layanan Cloud dan per Aplikasi Klien.

Ketika menghitung kredit SLA untuk Layanan Cloud berdasarkan kepemilikan Aplikasi, Ketersediaan akan dihitung berdasarkan pedoman berikut:

- Setiap Aplikasi akan memiliki bagian bobot tertentu yang ditetapkan berdasarkan pada jumlah volume sesi yang dihitung selama bulan masa kontrak.
- Waktu Henti setiap Layanan Cloud per Aplikasi akan diakumulasikan secara terpisah selama bulan masa kontrak.

Berikut ini adalah contoh penghitungan selama satu bulan aktivitas dan pembobotan yang terkait. Penghitungan ini hanya untuk tujuan ilustrasi:

Aplikasi Ritel	Bagian dari total # sesi dalam bulan masa kontrak yang diberikan	Total Waktu Henti Selama bulan masa kontrak	Jumlah Menit yang diukur dari Waktu Henti
Aplikasi Ritel A	40%	300 menit	40% x. 300 menit = 120 menit
Aplikasi Ritel B	20%	250 menit	20% x 250 menit = 50 menit
Aplikasi Ritel C	40%	150 menit	40% x 150 menit = 60
			Total menit Waktu Henti yang diukur = 230

Ketersediaan, yang dinyatakan sebagai persentase, dihitung dengan cara: total jumlah menit dalam suatu bulan masa kontrak, dikurangi total jumlah menit yang diukur dari Waktu Henti dalam bulan masa kontrak, dibagi dengan total jumlah menit dalam bulan masa kontrak. Contoh penghitungan berdasarkan contoh pembobotan di atas adalah sebagai berikut:

$$\frac{\text{43.200 total menit dalam suatu bulan masa kontrak selama 30 hari} - \text{230 menit Waktu Henti yang diukur} = \text{42.970 menit}}{\text{43.200 total menit}} = \text{2\% Kredit yang tersedia untuk 99,4\% ketersediaan selama bulan masa kontrak}$$

10. Dukungan Teknis

Dukungan Teknis untuk Layanan Cloud tersedia untuk Klien dan Peserta yang Memenuhi Syarat mereka untuk membantu dalam penggunaan Layanan Cloud.

Dukungan Standar termasuk dalam langganan semua tawaran. Trusteer Rapport Mandatory Service, yang merupakan *add-on* untuk Trusteer Rapport, memiliki prasyarat Dukungan Premium untuk langganan Trusteer Rapport dasar.

Untuk setiap Layanan Cloud, langganan Dukungan Premium tersedia dengan biaya tambahan, dengan pengecualian Layanan Cloud IBM Trusteer Mobile SDK dan Layanan Cloud IBM Trusteer Rapport Mandatory Service. Silakan hubungi Perwakilan penjualan IBM Anda atau Mitra Bisnis IBM.

Dukungan Standar:

- dukungan waktu lokal pukul 08.00-17.00.
- Klien dan Peserta yang Memenuhi Syarat mereka dapat mengajukan tiket dukungan secara elektronik, sebagaimana yang diuraikan secara terperinci dalam Buku Petunjuk Dukungan Perangkat Lunak Sebagai Layanan [Software as a Service - "SaaS"].
- Klien dapat mengakses Portal Dukungan Klien untuk pemberitahuan, dokumen, laporan kasus, dan FAQ di: http://www-01.ibm.com/software/security/trusteer/support/.
- Untuk opsi dukungan dan perincian, akses Buku Petunjuk Dukungan Perangkat Lunak sebagai Layanan [SaaS]: http://www-01.ibm.com/software/support/handbook.html.

Dukungan Premium:

- Dukungan 24x7 untuk semua tingkat permasalahan.
- Klien dapat memperoleh dukungan secara langsung melalui telepon dan permintaan pemanggilan kembali (*callback*).
- Klien dan Peserta yang Memenuhi Syarat mereka dapat mengajukan tiket dukungan secara elektronik, sebagaimana yang diuraikan secara terperinci dalam Buku Petunjuk Dukungan Perangkat Lunak Sebagai Layanan [Software as a Service - "SaaS"].
- Klien dapat mengakses Portal Dukungan Klien untuk pemberitahuan, dokumen, laporan kasus, dan FAQ di: http://www-01.ibm.com/software/security/trusteer/support/.
- Untuk opsi dukungan dan perincian, akses Buku Petunjuk Dukungan Perangkat Lunak sebagai Layanan [SaaS]: http://www-01.ibm.com/software/support/handbook.html.

11. Informasi Kepemilikan dan Penagihan

11.1 Metrik Biaya

Layanan Cloud tersedia berdasarkan metrik biaya yang ditetapkan dalam Dokumen Transaksi:

a. Peserta yang Memenuhi Syarat adalah suatu unit ukuran yang olehnya Layanan Cloud dapat diperoleh. Masing-masing individu atau entitas yang memenuhi syarat untuk berpartisipasi dalam program penyampaian layanan apa pun yang dikelola atau dilacak oleh Layanan Cloud adalah Peserta yang Memenuhi Syarat. Kepemilikan yang memadai harus diperoleh untuk mencakup semua Peserta yang Memenuhi Syarat yang dikelola atau dilacak dalam Layanan Cloud selama periode pengukuran yang ditetapkan dalam Dokumen Transaksi Klien.

   Setiap program penyampaian layanan yang dikelola oleh Layanan Cloud dianalisis secara terpisah dan kemudian ditambahkan bersama-sama. Individu atau entitas yang memenuhi syarat untuk beberapa program penyampaian layanan memerlukan kepemilikan yang terpisah.

   Untuk tujuan kepemilikan Layanan Cloud ini, Peserta yang Memenuhi Syarat adalah pengguna akhir Klien, yang memiliki kredensial login khusus ke Aplikasi Bisnis atau Ritel milik Klien.

b. Perangkat Klien adalah suatu unit ukuran yang olehnya Layanan Cloud dapat diperoleh. Perangkat Klien adalah perangkat komputasi pengguna tunggal atau sensor tujuan khusus atau perangkat telemetri yang meminta pelaksanaan atau menerima pelaksanaan serangkaian perintah, prosedur, atau aplikasi dari atau memberikan data ke sistem komputer lain yang biasanya disebut sebagai server atau jika tidak dikelola oleh server. Beberapa Perangkat Klien dapat berbagi akses ke server umum. Perangkat Klien dapat memiliki beberapa kemampuan pemrosesan atau dapat diprogram untuk memungkinkan pengguna melakukan pekerjaan. Klien harus memperoleh kepemilikan untuk setiap Perangkat Klien yang berjalan, memberikan data untuk, menggunakan layanan yang disediakan oleh, atau jika tidak, mengakses Layanan Cloud selama periode pengukuran yang ditetapkan dalam Dokumen Transaksi Klien.

c. Aplikasi adalah suatu unit ukuran yang olehnya Layanan Cloud dapat diperoleh. Aplikasi adalah program perangkat lunak yang diberi nama secara khusus. Kepemilikan yang memadai harus diperoleh untuk setiap Aplikasi yang tersedia untuk akses dan penggunaan selama periode pengukuran yang ditetapkan dalam PoE atau Dokumen Transaksi Klien.

   Untuk Layanan Cloud ini, suatu aplikasi merupakan Aplikasi Bisnis atau Ritel tunggal Klien.

d. Pengikatan adalah suatu unit ukuran yang olehnya layanan dapat diperoleh. Pengikatan terdiri atas layanan profesional dan/atau pelatihan yang berkaitan dengan Layanan Cloud. Kepemilikan yang memadai harus diperoleh untuk mencakup setiap Pengikatan.

12. Kepatuhan dan Audit

Akses ke Layanan Cloud IBM Trusteer Fraud Protection tunduk pada jumlah maksimum Aplikasi, Peserta yang Memenuhi Syarat dan/atau Perangkat Klien sebagaimana yang ditetapkan dalam Dokumen Transaksi. Klien bertanggung jawab untuk memastikan bahwa jumlah Aplikasi, Peserta yang Memenuhi Syarat dan/atau Perangkat Klien tidak melebihi jumlah maksimum sebagaimana yang ditetapkan dalam Dokumen Transaksi.

Audit dapat dilakukan oleh IBM untuk memverifikasi kepatuhan terhadap jumlah maksimum Aplikasi, Peserta yang Memenuhi Syarat dan/atau Perangkat Klien.

13. Jangka Waktu dan Opsi Pembaruan

Jangka waktu Layanan Cloud dimulai pada tanggal ketika IBM memberi tahu Klien mengenai akses mereka ke Layanan Cloud, sebagaimana yang didokumentasikan dalam PoE. PoE akan menetapkan apakah Layanan Cloud memperbarui secara otomatis, berlanjut berdasarkan penggunaan berkelanjutan atau berakhir pada akhir jangka waktu.

Untuk pembaruan otomatis, kecuali apabila Klien memberikan pemberitahuan tertulis untuk tidak memperbarui setidaknya 90 hari sebelum tanggal habis masa berlakunya jangka waktu, Layanan Cloud akan secara otomatis memperbarui untuk jangka waktu yang ditetapkan dalam PoE.

Untuk penggunaan berkelanjutan, Layanan Cloud akan terus tersedia dengan basis per bulan hingga Klien memberikan pemberitahuan tertulis 90 hari sebelumnya mengenai pengakhiran. Layanan Cloud akan tetap tersedia hingga akhir bulan kalender setelah periode 90 hari tersebut.

14. Syarat-syarat Tambahan

14.1 Perangkat Lunak yang Diaktifkan

Layanan Cloud ini mencakup perangkat lunak yang diaktifkan yang hanya dapat digunakan terkait dengan penggunaan Layanan Cloud oleh Klien dan hanya selama jangka waktu Layanan Cloud.

14.2 Kenaikan Biaya Langganan Tahunan IBM Trusteer

IBM berhak untuk menyesuaikan biaya langganan Layanan Cloud. Penyesuaian biaya langganan akan ditunjukkan dalam harga yang ditetapkan dalam dan selama jangka waktu Penawaran Harga yang berlaku. Penyesuaian biaya langganan tambahan yang akan berlaku tidak lebih dari satu kali setiap dua belas (12) bulan berdasarkan persentase yang akan ditentukan oleh IBM yang tidak melebihi 3% dapat berlaku saat jangka waktu Layanan Cloud diperpanjang melalui pembaruan otomatis atau penggunaan berkelanjutan. Penyesuaian biaya ini tidak mengubah kepemilikan Klien atas Layanan Cloud atau metrik biaya yang olehnya Layanan Cloud diperoleh. Mitra Bisnis IBM bersifat independen dari IBM dan dapat menentukan harga dan syarat-syarat mereka secara sepihak.

This document is made in the English and Indonesian languages. To the extent permitted by the prevailing law, the English language of this document will prevail in the case of any inconsistencies or differences of interpretation with the Indonesian language text of this document.

Dokumen ini dibuat dalam bahasa Indonesia dan bahasa Inggris. Sepanjang diperbolehkan oleh hukum yang berlaku, dalam hal terdapat ketidaksesuaian atau perbedaan penafsiran dengan teks bahasa Indonesia dari dokumen ini, maka teks dalam bahasa Inggris yang akan berlaku.