IBM Trusteer Pinpoint Detect

Uraian Layanan ini menguraikan Layanan Cloud. Dokumen pemesanan yang berlaku memberikan penentuan harga dan rincian tambahan tentang pemesanan Klien.

1. Layanan Cloud

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 Aplikasi Retail Klien yang untuknya Klien telah berlangganan cakupan Layanan Cloud dan proses pencegahan penipuan.

Layanan Cloud ini mencakup:

a. Aplikasi Trusteer Management (Trusteer Management Application - "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. IBM Trusteer Pinpoint Detect dan IBM Trusteer Pinpoint Verify digunakan sebagai bagian dari login TMA.

b. Skrip Web dan/atau API:

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

Sesi Pinpoint diukur antara awal dan akhir interaksi pengguna. Awal sesi diukur setelah pengiriman kredensial atau alternatif verifikasi kredensial pada halaman login pelanggan. Akhir sesi direkam jika salah satu peristiwa berikut terjadi:

- Sesi diatur ulang dengan cara logout normal dari aplikasi.
- Browser atau tab ditutup.
- Cookies dihapus.
- Batas Waktu (Timeout)

1.1 Tawaran

Klien dapat memilih dari tawaran berikut yang tersedia.

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

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 atas malware dan/atau aktivitas pengambilalihan akun mencurigakan pada browser yang menghubungkan ke Aplikasi Retail atau Bisnis, 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 Retail atau Bisnis secara langsung kepada Klien.

Dukungan standar (sebagaimana yang ditentukan dalam pasal Dukungan Teknis di bawah) tercakup dalam Layanan Cloud ini. Untuk dukungan Premium, Klien harus membeli Pinpoint Standard Premium Support.

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

Layanan tersedia untuk dibeli dengan paket 100 Peserta yang Memenuhi Syarat atau dengan paket 100 Koneksi. Apabila Klien memilih untuk membeli Layanan dengan Koneksi, biaya Aplikasi Tambahan berlaku sejak aplikasi pertama.

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

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 atas malware dan/atau aktivitas pengambilalihan akun mencurigakan pada browser yang menghubungkan ke Aplikasi Retail atau Bisnis, 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 Aplikasi Retail secara langsung kepada Klien.

Layanan tersebut mencakup fungsionalitas dan layanan yang ditingkatkan, termasuk: penyebaran yang diperluas dan layanan pengaturan, kebijakan keamanan yang disesuaikan, layanan investigasi, dll. Layanan tersebut mencakup hingga 200 jam sumber daya bersama untuk layanan penyebaran per aplikasi, dan 200 jam sumber daya bersama untuk analisis keamanan per aplikasi setelah pengaturan. Layanan yang sedang berjalan mencakup 20 jam pemeliharaan penyebaran per tahun per aplikasi, dan 100 jam penelitian keamanan per aplikasi per tahun. Setiap upaya tambahan dibebankan biaya tambahan.

Pinpoint Detect dapat menggunakan transaksi dari saluran Mobile dan Web. Apabila transaksi Mobile termasuk, PinPoint dengan Koneksi akan berlaku. 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.

Layanan IBM Trusteer Pinpoint Detect Premium for Retail and Business tersedia untuk dibeli dengan paket 100 Peserta yang Memenuhi Syarat atau IBM Trusteer Pinpoint Detect Premium dengan paket 100 Koneksi. Apabila Klien memilih untuk membeli Layanan dengan Koneksi, biaya Aplikasi Tambahan berlaku sejak aplikasi pertama.

Pinpoint Detect Policy Manager:

Policy Manager disertakan dalam layanan Pinpoint Detect Premium dan tersedia di lingkungan yang diselenggarakan (hosted) oleh cloud IBM Trusteer, yang melaluinya Klien (dan jumlah personelnya yang sah dalam jumlah tidak terbatas) dapat: (i) merancang, menguji dan menyebarkan ke logika lingkungan produksi untuk mendeteksi aktivitas penipuan, (ii) merancang laporan dan dasbor, dan (iii) 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.

1.1.3 IBM Trusteer Pinpoint Detect for Connections

Layanan Cloud ini memberikan perlindungan dan bertujuan mendeteksi upaya pengambilalihan akun dan menyampaikan skor penilaian risiko / kepercayaan browser dan/atau perangkat mobile (melalui browser asli dari aplikasi mobile Klien) yang mengakses aplikasi Bisnis atau Retail. Solusi tersebut menggunakan berbagai indikator risiko yang menganalisis perangkat pengguna akhir, koneksi, dan perilaku serta membandingkannya dengan riwayat pengguna guna mengidentifikasi penggunaan yang mencurigakan.

Layanan Cloud dapat menggunakan koneksi dari saluran Mobile maupun Web. IBM Trusteer Pinpoint Detect mencakup kepemilikan atas IBM Trusteer Mobile SDK, jika berhubungan.

Layanan Cloud tersedia untuk dibeli dengan paket 100 Koneksi per tahun.

1.2 Layanan Opsional

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

1.2.1 IBM Trusteer Pinpoint Detect Standard Application

Aplikasi Klien mengacu pada Aplikasi Web dan/atau Aplikasi Mobile. Aplikasi Web mengelompokkan semua fungsi yang ditawarkan kepada Peserta yang Memenuhi Syarat dari Klien melalui beberapa halaman web, dari suatu login atau layar identifikasi dan dipantau sebagai Aplikasi tunggal pada konsol Trusteer (Aplikasi Trusteer Management). Aplikasi Mobile mengelompokkan secara bersama-sama semua fungsi yang ditawarkan kepada Peserta yang Memenuhi Syarat dari Klien melalui satu program perangkat lunak yang dapat diunduh dari toko aplikasi (toko), dari suatu login atau layar identifikasi dan dipantau sebagai Aplikasi tunggal pada konsol Trusteer (Aplikasi Trusteer Management).

Integrasi IBM Trusteer Pinpoint memerlukan kepemilikan atas IBM Trusteer Pinpoint Application untuk setiap Aplikasi.

- Penyebaran IBM Trusteer Pinpoint Detect Standard memerlukan kepemilikan atas IBM Trusteer Pinpoint Detect Standard Application untuk setiap Aplikasi.

1.2.2 IBM Trusteer Pinpoint Detect Premium Application

Aplikasi Klien mengacu pada Aplikasi Web dan/atau Aplikasi Mobile. Aplikasi Web mengelompokkan semua fungsi yang ditawarkan kepada Peserta yang Memenuhi Syarat dari Klien melalui beberapa halaman web, dari suatu login atau layar identifikasi dan dipantau sebagai Aplikasi tunggal pada konsol Trusteer (Aplikasi Trusteer Management). Aplikasi Mobile mengelompokkan secara bersama-sama semua fungsi yang ditawarkan kepada Peserta yang Memenuhi Syarat dari Klien melalui satu program perangkat lunak yang dapat diunduh dari toko aplikasi (toko), dari suatu login atau layar identifikasi dan dipantau sebagai Aplikasi tunggal pada konsol Trusteer (Aplikasi Trusteer Management).

Layanan ini mencakup hingga 200 jam sumber daya bersama untuk layanan penyebaran per aplikasi, dan 200 jam sumber daya bersama untuk analisis keamanan per aplikasi setelah pengaturan. Layanan yang sedang berjalan mencakup 20 jam pemeliharaan penyebaran per tahun per aplikasi, dan 100 jam penelitian keamanan per aplikasi per tahun.

- Penyebaran IBM Trusteer Pinpoint Premium memerlukan kepemilikan atas IBM Trusteer Pinpoint Detect Premium Application untuk setiap Aplikasi.

1.2.3 IBM Trusteer New Account Fraud for Retail dan/atau IBM Trusteer New Account Fraud for Business

Layanan ini, yang tersedia untuk pelanggan Pinpoint, dirancang untuk mendeteksi anomali, menandai aktivitas mencurigakan, dan menghasilkan peringatan dini dalam proses pembuatan akun baru. Layanan memantau akun baru untuk mengidentifikasi aktivitas baru yang berhubungan dengan penipuan pascapembuatan akun dan pembuatan profil akun yang masih baru untuk memberikan tanda peringatan dini bahwa akun baru mungkin adalah akun yang bertujuan buruk atau digunakan untuk melakukan penipuan, melalui laporan penggunaan yang tersedia dalam TMA.

IBM Trusteer New Account Fraud for Retail dan IBM Trusteer New Account Fraud for Business tersedia dalam paket berisi 10 Panggilan API.

1.2.4 IBM Trusteer Digital Content Pack for Retail dan/atau IBM Trusteer Digital Content Pack for Business

IBM Trusteer Digital Content Pack memungkinkan analis keamanan untuk mengintegrasikan model penipuan baru saat mendukung sepenuhnya pembuatan dan modifikasi model ad-hoc untuk bereaksi terhadap ancaman yang berkembang. Layanan ini terdiri dari berbagai kumpulan aturan, wawasan, dan kebijakan yang dapat dibeli sebagai bagian tambahan dan integral dari solusi. Selanjutnya, Digital Content Pack membantu mempererat integrasi antara kemampuan pencegahan penipuan digital Trusteer dan saluran pembayaran non-tunai IBM Safer Payments. Dengan memanfaatkan logika bisnis spesifik dan aturan bawaan, Digital Content Pack memungkinkan bank dan institusi keuangan lainnya untuk meningkatkan lebih jauh kemampuan pencegahan dan deteksi penipuan yang telah ada.

IBM Trusteer Digital Content Pack for Retail tersedia dalam paket 100 Peserta yang Memenuhi Syarat. IBM Trusteer Digital Content Pack for Business tersedia dalam paket 10 Peserta yang Memenuhi Syarat.

Layanan konsultasi diperlukan untuk integrasi Digital Content Pack dengan Pinpoint Detect dan IBM Safer Payments, serta untuk layanan dukungan yang memerlukan perhatian yang signifikan. Layanan konsultasi diperoleh secara terpisah sesuai dengan pernyataan kerja yang terpisah.

1.2.5 IBM Trusteer Pinpoint Malware Detection

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

1.2.6 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 Retail. 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 Retail Klien.

b. Edisi Tingkat Lanjut:

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

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

c. Edisi Standar:

   Edisi Standar untuk Bisnis dan/atau Retail merupakan solusi cepat untuk menyebarkan yang menyediakan fungsionalitas inti 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.

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

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

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

IBM Trusteer Rapport Remediation 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 II yang benar-benar berjalan di 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) terinfeksi tertentu 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, mengautentikasi 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. Untuk tujuan Uraian Layanan ini, Pemegang Akun – adalah pengguna akhir dari Klien, yang telah memasang perangkat lunak klien yang diaktifkan, yang menerima perjanjian lisensi pengguna akhir (end user license agreement - "EULA"), dan mengautentikasi setidaknya satu kali dengan Aplikasi Retail atau Aplikasi 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 apa pun lainnya yang disediakan dengan beberapa Layanan Cloud untuk dipasang pada perangkat pengguna akhir.

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

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

- IBM Trusteer Rapport for Mitigation for Retail bertujuan untuk menginvestigasi, memulihkan, memblokir, dan menghapus infeksi malware dari perangkat (PC/MAC) Peserta yang Memenuhi Syarat yang terinfeksi yang mengakses Aplikasi Retail Klien secara ad-hoc, di mana infeksi malware telah dideteksi 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 Retail Klien. Klien dapat menggunakan Layanan Cloud ini hanya sehubungan dengan Peserta yang Memenuhi Syarat yang mengakses Aplikasi Retail 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, mengautentikasi dengan Aplikasi(-aplikasi) Retail 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 Pemegang Akun dengan cara lain apa pun untuk populasi umum Peserta yang Memenuhi Syarat dari Klien.

- IBM Trusteer Rapport for Mitigation for Business bertujuan untuk menginvestigasi, memulihkan, memblokir, dan menghapus infeksi malware dari perangkat (PC/MAC) terinfeksi Peserta yang Memenuhi Syarat yang mengakses Aplikasi Ritel Klien secara ad-hoc, di mana infeksi malware telah dideteksi 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 Bisnis Klien. Klien dapat menggunakan Layanan Cloud ini hanya sehubungan dengan Peserta yang Memenuhi Syarat yang mengakses Aplikasi Bisnis Klien, serta semata-mata sebagai alat yang bertujuan untuk menginvestigasi dan memulihkan perangkat (PC/MAC) terinfeksi tertentu secara ad-hoc. IBM Trusteer Rapport for Mitigation for Business harus benar-benar berjalan pada perangkat (PC/MAC) Peserta yang Memenuhi Syarat yang terpengaruh tersebut, dan Peserta yang Memenuhi Syarat yang terpengaruh tersebut harus menyetujui EULA, mengautentikasi dengan Aplikasi(-aplikasi) Bisnis Klien setidaknya satu kali, serta konfigurasi Klien harus mencakup kumpulan ID Pengguna. Untuk menghindari keraguan, 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 dari Klien.

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

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

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

Layanan ini mencakup hingga 200 jam sumber daya bersama untuk layanan penyebaran per aplikasi, dan 200 jam sumber daya bersama untuk analisis keamanan per aplikasi setelah pengaturan. Layanan yang sedang berjalan mencakup 20 jam pemeliharaan penyebaran per tahun per aplikasi, dan 100 jam penelitian keamanan per aplikasi per tahun.

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

1.2.13 IBM Trusteer Pinpoint Detect Standard for Retail Premium Support dan/atau IBM Trusteer Pinpoint Detect Standard for Business Premium Support

Klien yang membeli Layanan Cloud Pinpoint Detect Standard dapat membeli layanan Premium Support. Cakupan layanan Premium Support tercantum dalam pasal 4 di bawah ini.

1.2.14 IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

Klien harus memiliki langganan saat ini untuk IBM Trusteer Pinpoint Detect sebelum berlangganan Layanan Cloud ini.

Layanan Cloud ini meningkatkan IBM Trusteer Pinpoint Detect dengan memberikan informasi dan konteks tambahan seputar nomor mobile yang disediakan untuk salah satu Layanan Cloud tersebut, yang membantu untuk menentukan risiko penipuan pada sesi tertentu. Klien dapat meminta (query) Layanan Cloud untuk mempelajari karakteristik tentang nomor mobile yang diberikan, misalnya informasi penyedia layanan (carrier) yang terkait dengan nomor tersebut.

Data yang diberikan oleh Layanan Cloud mengenai nomor mobile ("Mobile Intelligence") ini dapat digunakan hanya untuk tujuan internal Klien, dan hanya dapat disimpan selama periode tiga puluh (30) hari. Klien harus meminta ulang (requery) Layanan Cloud mengenai nomor mobile yang sama setelah periode tersebut untuk memperoleh Mobile Intelligence mengenai nomor tersebut dan tidak dapat sekedar menggunakan kembali Mobile Intelligence yang diterima dari kueri sebelumnya. Klien tidak dapat menyembunyikan (cache), kecuali sebagaimana diizinkan di atas, menggunakan kembali, atau

menggunakan sehubungan dengan seluruh atau sebagian penambangan data (data mining) apa pun atau untuk mengarsipkan bagian apa pun dari Mobile Intelligence.

1.3 Layanan Percepatan

1.3.1 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.

1.3.2 IBM Trusteer Pinpoint Malware Detection 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 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.

IBM Trusteer Pinpoint Malware Detection Additional Applications untuk IBM Trusteer Pinpoint Malware Detection II Standard Edition atau IBM Trusteer Pinpoint Malware Detection II Advanced Edition, penyebaran pada setiap Aplikasi tambahan di luar Aplikasi pertama memerlukan kepemilikan atas IBM Trusteer Pinpoint Malware Detection Additional Applications.

2. Lembar Data Perlindungan dan Pemrosesan Data

Adendum Pemrosesan Data IBM di http://ibm.com/dpa (Data Processing Addendum - "DPA") dan Lembar(-Lembar) Data Perlindungan dan Pemrosesan Data (disebut sebagai lembar(-lembar) data atau Ekshibit(-Ekshibit) DPA) dalam tautan di bawah memberikan informasi perlindungan data tambahan untuk Layanan Cloud dan opsinya sehubungan dengan tipe Konten yang dapat diproses, aktivitas pemrosesan yang terlibat, fitur perlindungan data, serta pokok-pokok mengenai retensi dan pengembalian Konten. DPA tersebut berlaku untuk data pribadi yang terkandung dalam Konten, apabila dan sejauh i) Peraturan Perlindungan Data Umum Eropa (EU/2016/679) (European General Data Protection Regulation - "GDPR"); atau ii) peraturan perundang-undangan perlindungan data lainnya yang diidentifikasi di http://ibm.com/dpa/dpl berlaku.

Terklarifikasi bahwa Lembar Data secara umum mencantumkan semua lokasi tempat IBM (termasuk setiap subprosesor pihak ketiga) menyelenggarakan dan memroses Data Pribadi, yang tidak berkaitan dengan pusat data tempat asal penyebaran layanan. Untuk daftar lokasi pemrosesan dan hosting yang spesifik untuk pusat data tempat asal penyebaran layanan, lihat Pasal 5.2 di bawah (Informasi Lokasi Pemrosesan Tambahan).

IBM Trusteer Pinpoint Criminal Detect

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

IBM Trusteer Pinpoint Detect

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

IBM Trusteer Pinpoint Malware Detection

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

IBM Trusteer Mobile SDK

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

3. Tingkat Layanan dan Dukungan Teknis

3.1 Perjanjian Tingkat Layanan

IBM memberikan perjanjian tingkat layanan (SLA) ketersediaan berikut kepada Klien. IBM akan memberlakukan kompensasi yang berlaku yang paling tinggi berdasarkan ketersediaan kumulatif Layanan Cloud sebagaimana yang ditunjukkan dalam tabel di bawah. Persentase ketersediaan dihitung sebagai total jumlah menit dalam suatu bulan masa kontrak, dikurangi total jumlah menit Layanan Berhenti dalam bulan masa kontrak, dibagi dengan total jumlah menit dalam bulan masa kontrak. Definisi Layanan Berhenti, proses klaim dan cara menghubungi IBM terkait permasalahan ketersediaan layanan berada pada buku petunjuk dukungan Layanan Cloud IBM di https://www.ibm.com/software/support/saas_support_overview.html.

Ketersediaan	Kredit (% biaya langganan bulanan*)
Kurang dari 99,9%	2%
Kurang dari 99,0%	5%
Kurang dari 95,0%	10%

* Biaya langganan adalah harga pada masa kontrak untuk bulan yang sesuai dengan klaim.

3.2 Dukungan Teknis

Dukungan teknis untuk Layanan Cloud, termasuk rincian kontak dukungan, level tingkat permasalahan, jam dukungan ketersediaan, waktu tanggapan, dan informasi serta proses dukungan lain, ditemukan dengan memilih Layanan Cloud dalam panduan dukungan IBM yang tersedia di https://www.ibm.com/support/home/pages/support-guide/.

Dukungan Premium:

Langganan Dukungan Premium tersedia untuk Layanan Cloud dengan biaya tambahan dan mencakup:

- 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.ibm.com/software/security/trusteer/support/.

4. Biaya

4.1 Metrik Biaya

Metrik(-metrik) biaya untuk Layanan Cloud ditetapkan dalam Dokumen Transaksi.

Metrik biaya berikut berlaku untuk Layanan Cloud ini:

- Pengikatan adalah layanan pelatihan atau profesional yang berkaitan dengan Layanan Cloud.
- Peserta yang Memenuhi Syarat adalah individu atau entitas yang memenuhi syarat untuk berpartisipasi dalam program penyampaian layanan apa pun yang dikelola atau dilacak dengan Layanan Cloud.
- Aplikasi adalah program perangkat lunak yang ditentukan secara unik yang dikembangkan oleh atau disediakan untuk mengakses atau digunakan oleh Layanan Cloud.
- Panggilan API adalah permohonan Layanan Cloud melalui antarmuka programatik.

- Koneksi adalah suatu tautan atau asosiasi basis data, aplikasi, server, atau jenis perangkat lain apa pun yang telah atau tersedia ke Layanan Cloud.

4.2 Biaya Layanan Jarak Jauh

Layanan jarak jauh akan berakhir 90 hari dari pembelian terlepas dari apakah layanan jarak jauh telah digunakan.

5. Syarat-syarat Tambahan

Untuk Perjanjian Layanan Cloud (atau perjanjian cloud dasar yang setara) yang ditandatangani sebelum tanggal 1 Januari 2019, syarat-syarat yang tersedia di https://www.ibm.com/acs adalah yang berlaku.

5.1 EULA dan Basis untuk Memproses Data Subjek Data

Untuk Layanan Cloud IBM Trusteer Rapport (termasuk Rapport Remediation atau Rapport for Mitigation ketika disebarkan sehubungan dengan Layanan Cloud Pinpoint): Kecuali apabila disetujui secara lain, dan menurut basis untuk pemrosesan yang telah dibuat oleh Klien secara independen, Klien memberi wewenang kepada IBM untuk memberikan Perjanjian Lisensi Pengguna Akhir yang tersedia di https://trusteer.secure.force.com/PKB/articles/en_US/FAQ/RAPPORT-DATA-PRIVACY-NOTICE-AND-END-USER-LICENSE-AGREEMENT-EULA Untuk memungkinkan IBM mengumpulkan dan memproses informasi yang diperlukan untuk memberikan Layanan Cloud.

Untuk Layanan Cloud IBM Trusteer Rapport, Klien mengizinkan IBM, sebagai prosesor data Perusahaan Sponsor, untuk menggunakan Program tersebut guna mengumpulkan malware dan artefak malware, yaitu, file-file yang berkaitan dengan aktivitas yang merugikan, atau file-file yang berkaitan dengan gangguan fungsi Program yang tidak biasa. IBM tidak menggunakan Program untuk menarget file dengan informasi pribadi pengguna akhir; namun, file yang dikumpulkan dapat berisi data pribadi yang telah diperoleh oleh malware tanpa izin pengguna akhir. IBM akan 1) segera menghapus setiap file yang tidak relevan dengan analisis tersebut, dan 2) mempertahankan file yang relevan hanya selama durasi analisis dan dalam hal apa pun tidak lebih dari tiga bulan.

5.2 Informasi Lokasi Pemrosesan Tambahan

Semua hosting dan pemrosesan Data Pribadi, termasuk oleh subprosesor pihak ketiga mana pun yang teridentifikasi dalam Lembar Data, akan dilakukan di lokasi yang ditetapkan di bawah ini:

Untuk semua layanan yang diberikan melalui pusat data Jerman, IBM akan membatasi hosting dan pemrosesan Data Pribadi ke negara yang merupakan entitas kontrak IBM dan ke negara-negara berikut: Jerman, Israel, Irlandia dan Belanda.

Untuk semua layanan yang diberikan melalui pusat data Jepang, IBM akan membatasi hosting dan pemrosesan Data Pribadi ke negara yang merupakan entitas kontrak IBM dan ke negara-negara berikut: Jepang, Israel dan Irlandia.

Untuk semua layanan yang diberikan melalui pusat data AS, IBM akan membatasi hosting dan pemrosesan Data Pribadi ke negara yang merupakan entitas kontrak IBM dan ke negara-negara berikut: AS, Israel, Irlandia, Singapura dan Australia.

Selain lokasi-lokasi tersebut di atas, sehubungan dengan semua layanan yang diberikan melalui pusat data AS, Jepang dan Jerman, (1) data pendukung dapat dihost atau diproses di Jerman dan Prancis oleh Salesforce.Com sebagai subprosesor pihak ketiga IBM dan (2) bagi klien yang memilih mengirim data ke penyedia Mobile Carrier Intelligence, Data Pribadi dapat dihost dan diproses di negara subprosesor pihak ketiga yang berlaku sebagaimana yang ditetapkan dalam Lembar Data. Terlepas dari hal-hal yang bertentangan dalam Lembar Data, subprosesor pihak ketiga yang ditetapkan dalam klausul (2) dari kalimat tepat sebelum ini mungkin tidak mematuhi ISO 27001 atau SOC2.

Layanan pemeliharaan akun dan dukungan IBM Trusteer juga dapat diberikan sesuai kebutuhan, berdasarkan ketersediaan personel IBM terkait, lokasi Klien dan pusat data di mana data diselenggarakan (di-host).

5.3 Data Pemegang Akun

Untuk tujuan kejelasan, jika terdapat lebih dari satu pelanggan IBM yang berafiliasi dengan Perangkat Lunak Klien Pemegang Akun dari Pemegang Akun tertentu (seperti pelanggan IBM, "Pelanggan Afiliasi") dan layanan berdasarkan Uraian Layanan ini diberikan oleh IBM kepada Pelanggan Afiliasi tersebut melalui pusat data di wilayah lain, kemudian data Pemegang Akun dapat diproses di setiap dan semua

lokasi yang berkaitan dengan tiap pusat data tersebut sebagaimana yang ditetapkan dalam Pasal 5.2 di atas.

5.4 Solusi Terintegrasi

Untuk tujuan kejelasan, berbagai tawaran berdasarkan merek Trusteer dapat berupa solusi terintegrasi. Sehingga, 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 serta layanan Trusteer lainnya sesuai dengan uraian layanan yang berlaku pada layanan Trusteer lain tersebut.

5.5 Perangkat Lunak yang Diaktifkan

Layanan Cloud berisi Perangkat Lunak yang Diaktifkan berikut:

- IBM Rapport Agents

5.6 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 Aplikasi Retail segera setelah deteksi malware atau pengambilalihan akun).

5.7 Data yang Dikumpulkan sebagai Bagian dari Penyebaran

Penyebaran Layanan Cloud dapat mencakup Klien yang memberikan data tertentu kepada IBM. Data tersebut tidak boleh mencakup informasi yang dapat mengidentifikasi atau dapat dikaitkan dengan individu tertentu. Pedoman lebih lanjut tentang data yang diberikan kepada IBM sebagai bagian dari penyebaran, disertakan dalam Pedoman Penyebaran Trusteer yang akan diberikan kepada Klien.

6. Syarat-syarat Utama

6.1 Penggunaan Data

Hal-hal berikut ini berlaku di atas apa pun yang bertentangan dalam pasal Perlindungan Data dan Konten dari syarat-syarat Layanan Cloud dasar di antara para pihak: IBM tidak akan menggunakan atau mengungkapkan hasil yang muncul dari penggunaan Klien atas Layanan Cloud yang bersifat khusus untuk Konten Klien (Wawasan) atau yang mengidentifikasi Klien. Namun demikian, IBM akan menggunakan Konten dan informasi lainnya yang dihasilkan dari Konten sebagai bagian dari Layanan Cloud yang tunduk pada penghapusan pengidentifikasi pribadi; sehingga setiap data pribadi tidak dapat lagi dikaitkan dengan individu tertentu tanpa menggunakan informasi tambahan. IBM akan menggunakan data tersebut hanya untuk penelitian, pengujian, dan pengembangan tawaran.

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.