IBM Trusteer Fraud Protection (IBM Trusteer Sahtekarlığa Karşı Koruma)

Bu Hizmet Tanımında, IBM tarafından Müşteriye sağlanan Bulut Hizmeti açıklanır. Müşteri, sözleşmeyi imzalayan taraf ile onun yetkili kullanıcılarını ve Bulut Hizmetinin alıcılarını ifade eder. İlgili Fiyat Teklifi ile Yetki Belgesi, ayrı İşlem Belgeleri olarak sağlanır.

1. Bulut Hizmeti

Aşağıda belirtilen Bulut Hizmetleri bu Hizmet Tanımı kapsamındadır:

Pinpoint Assure Bulut Hizmetleri:

- IBM Trusteer Pinpoint Assure
- IBM Trusteer Pinpoint Assure Application
- IBM Trusteer Mobile Carrier Intelligence (IBM Trusteer Mobil Taşıyıcı İstihbaratı)

Rapport Bulut Hizmetleri:

- IBM Trusteer Rapport for Business Premium Support (Ticari Faaliyet İçin IBM Trusteer Rapport Premium Destek)
- IBM Trusteer Rapport for Retail Premium Support (Perakende İçin IBM Trusteer Rapport Premium Destek)
- 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 (Ticari Faaliyet İçin IBM Trusteer Rapport Sahtekarlık Veri Akışları Premium Destek)
- IBM Trusteer Rapport Fraud Feeds for Retail
- IBM Trusteer Rapport Fraud Feeds for Retail Premium Support (Perakende İçin IBM Trusteer Rapport Sahtekarlık Veri Akışları Premium Destek)
- IBM Trusteer Rapport Phishing Protection for Business
- IBM Trusteer Rapport Phishing Protection for Business Premium Support (Ticari Faaliyet İçin IBM Trusteer Rapport Kimlik Avı Dolandırıcılığına Karşı Koruma Premium Destek)
- IBM Trusteer Rapport Phishing Protection for Retail
- IBM Trusteer Rapport Phishing Protection for Retail Premium Support (Perakende İçin IBM Trusteer Rapport Kimlik Avı Dolandırıcılığına Karşı Koruma Premium Destek)
- IBM Trusteer Rapport Mandatory Service for Business
- IBM Trusteer Rapport Mandatory Service for Retail
- IBM Trusteer Rapport Additional Applications for Retail (Perakende İçin IBM Trusteer Rapport Ek Uygulamaları)
- IBM Trusteer Rapport Additional Applications for Business (Ticari Faaliyet İçin IBM Trusteer Rapport Ek Uygulamaları)
- IBM Trusteer Rapport Large Redeployment (IBM Trusteer Rapport Büyük Ölçekli Yeniden Devreye Alımı)
- IBM Trusteer Rapport Small Redeployment (IBM Trusteer Rapport Küçük Ölçekli Yeniden Devreye Alımı)

Pinpoint Bulut Hizmetleri:

- IBM Trusteer Pinpoint Malware Detection Standard Edition for Business Premium Support (Ticari Faaliyet için IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Saptama Standart Sürüm Premium Destek)

- IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail Premium Support (Perakendecilik için IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Saptama Standart Sürüm Premium Destek)
- IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business Premium Support (Ticari Faaliyet için IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Saptama Gelişmiş Sürüm Premium Destek)
- IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail Premium Support (Perakendecilik için IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Saptama Gelişmiş Sürüm Premium Destek)
- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Rapport Remediation for Retail Premium Support (Perakende İçin IBM Trusteer Rapport İyileştirme Premium Destek)
- IBM Trusteer Rapport Remediation for Business (Ticari Faaliyet İçin IBM Trusteer Rapport İyileştirme)
- IBM Trusteer Rapport Remediation for Business Premium Support (Ticari Faaliyet İçin IBM Trusteer Rapport İyileştirme Premium Destek)
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail (Perakendecilik için IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Saptama Standart Sürüm II)
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business (Ticari Faaliyet için IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Saptama Standart Sürüm II)
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail (Perakendecilik için IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Saptama Gelişmiş Sürüm II)
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business (Ticari Faaliyet için IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Saptama Gelişmiş Sürüm II)
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail (Perakende İçin IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Tespiti Ek Uygulamaları)
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Business (Ticari Faaliyet İçin IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Tespiti Ek Uygulamaları)
- IBM Trusteer Pinpoint Malware Detection Redeployment
- IBM Trusteer Pinpoint Detect Standard for Retail (Perakende İçin IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Tespiti - Standart)
- IBM Trusteer Pinpoint Detect Premium for Retail (Perakende İçin IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Tespiti - Premium)
- IBM Trusteer Pinpoint Detect Standard for Business (Ticari Faaliyet İçin IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Tespiti - Standart)
- IBM Trusteer Pinpoint Detect Premium for Business (Ticari Faaliyet İçin IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Tespiti - Premium)
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business (Ticari Faaliyet İçin IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Tespiti - Standart Ek Uygulamaları)
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business
- IBM Trusteer Rapport for Mitigation for Retail (Perakende İçin Risk Azaltmaya Yönelik IBM Trusteer Rapport)
- IBM Trusteer Rapport for Mitigation for Retail Premium Support (Perakende İçin Risk Azaltmaya Yönelik IBM Trusteer Rapport - Premium Destek)
- IBM Trusteer Rapport for Mitigation for Business (Ticari Faaliyet İçin Risk Azaltmaya Yönelik IBM Trusteer Rapport
- IBM Trusteer Rapport for Mitigation for Business Premium Support (Ticari Faaliyet İçin Risk Azaltmaya Yönelik IBM Trusteer Rapport - Premium Destek)
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail (Perakende İçin IBM Trusteer Pinpoint Tespit Premium Ek Uygulamaları)

- IBM Trusteer Pinpoint Detect Standard Redeployment (IBM Trusteer Pinpoint Tespit Standart Yeniden Devreye Alımı)
- IBM Trusteer Pinpoint Detect Premium Redeployment (IBM Trusteer Pinpoint Tespit Premium Yeniden Devreye Alımı)
- IBM Trusteer Pinpoint Detect Standard For Retail Premium Support (Perakendecilik için IBM Trusteer Pinpoint Tespit Standart Premium Destek)
- IBM Trusteer Digital Content Pack for Retail
- IBM Trusteer Digital Content Pack for Business
- IBM Trusteer New Account Fraud for Business (Ticari Faaliyet İçin IBM Trusteer Yeni Hesap Sahtekarlığı)
- IBM Trusteer New Account Fraud for Retail (Perakende İçin IBM Trusteer Yeni Hesap Sahtekarlığı)
- IBM Trusteer Project Management and Consultancy Services (IBM Trusteer Proje Yönetimi ve Danışmanlık Hizmetleri)
- IBM Trusteer Security Research and Consultancy Services (IBM Trusteer Güvenlik Araştırması ve Danışmanlık Hizmetleri)
- IBM Trusteer Training Services (IBM Trusteer Eğitim Hizmetleri)
- IBM Trusteer Pinpoint Detect Standard Application (IBM Trusteer Pinpoint Tespit Standart Uygulaması)
- IBM Trusteer Pinpoint Detect Premium Application (IBM Trusteer Pinpoint Tespit Premium Uygulaması)
- IBM Trusteer Pinpoint Detect Standard (IBM Trusteer Pinpoint Tespit Standart)
- IBM Trusteer Pinpoint Detect Premium
- IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect (IBM Trusteer Pinpoint Tespit için Mobil Taşıyıcı İstihbaratı)
- IBM Trusteer Pinpoint Verify (IBM Trusteer Pinpoint Doğrulama)

Mobil Bulut Hizmetleri:

- IBM Trusteer Mobile SDK for Business (Ticari Faaliyet İçin IBM Trusteer Mobil Yazılım Geliştirme Kiti)
- IBM Trusteer Mobile SDK for Retail (Perakende İçin IBM Trusteer Mobil Yazılım Geliştirme Kiti)

1.1 Ticari Faaliyet ve Perakende Uygulamaları İçin Bulut Hizmetleri

IBM Trusteer Bulut Hizmetleri, belirli türde Uygulamalarla birlikte kullanılmak üzere sağlanır. Bir Uygulama, şu türlerden biri olarak tanımlanır: Perakende veya Ticari Faaliyet. Perakende Uygulamaları ve Ticari Faaliyet Uygulamaları için ayrı olanaklar sağlanır.

a. Perakende Uygulaması; tüketicilere hizmet etmek için tasarlanmış çevrimiçi bankacılık uygulaması, mobil uygulama veya e-ticaret uygulaması olarak tanımlanır. Müşterinin ilkesinde, belirli küçük işletmeler, perakende erişimine hak kazanan olarak sınıflandırılabilir.

b. Ticari Faaliyet Uygulaması; kuruluş, kurum veya eşdeğer şirketlere hizmet etmek için tasarlanmış çevrimiçi bankacılık uygulaması, mobil uygulama veya e-ticaret uygulaması veya Perakende olarak sınıflandırılmayan her tür uygulama olarak tanımlanır.

1.1.1 Ticari Faaliyet Bulut Hizmetleri

- IBM Trusteer Rapport II for Business
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business (Ticari Faaliyet için IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Saptama Standart Sürüm II)
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business (Ticari Faaliyet için IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Saptama Gelişmiş Sürüm II)
- IBM Trusteer Pinpoint Detect Standard for Business (Ticari Faaliyet İçin IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Tespiti - Standart)

- IBM Trusteer Pinpoint Detect Premium for Business (Ticari Faaliyet İçin IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Tespiti - Premium)
- IBM Trusteer Digital Content Pack for Business
- IBM Trusteer New Account Fraud for Business (Ticari Faaliyet İçin IBM Trusteer Yeni Hesap Sahtekarlığı)
- IBM Trusteer Mobile SDK for Business (Ticari Faaliyet İçin IBM Trusteer Mobil Yazılım Geliştirme Kiti)

1.1.2 Perakende Bulut Hizmetleri

- IBM Trusteer Rapport II for Retail
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail (Perakendecilik için IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Saptama Standart Sürüm II)
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail (Perakendecilik için IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Saptama Gelişmiş Sürüm II)
- IBM Trusteer Pinpoint Detect Standard for Retail (Perakende İçin IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Tespiti - Standart)
- IBM Trusteer Pinpoint Detect Premium for Retail (Perakende İçin IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Tespiti - Premium)
- IBM Trusteer Digital Content Pack for Retail
- IBM Trusteer New Account Fraud for Retail (Perakende İçin IBM Trusteer Yeni Hesap Sahtekarlığı)
- IBM Trusteer Mobile SDK for Retail (Perakende İçin IBM Trusteer Mobil Yazılım Geliştirme Kiti)

Ticari Faaliyet ve Perakende Bulut Hizmetlerinin her biri için, IBM Trusteer Mobile SDK Bulut Hizmetleri hariç olmak üzere, ek ücret karşılığında sağlanan ilişkili bir Premium Destek ürünü vardır.

1.1.3 IBM Trusteer Rapport II için Ek Bulut Hizmetleri

a. IBM Trusteer Rapport II for Business için mevcut olan ek Bulut Hizmetleri:
   - 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 (Ticari Faaliyet İçin IBM Trusteer Rapport Ek Uygulamaları)

b. IBM Trusteer Rapport II for Retail için mevcut olan ek Bulut Hizmetleri:
   - 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

IBM Trusteer Rapport Bulut Hizmetlerine yönelik her Ticari Faaliyet ve Perakende eklentisi için, IBM Trusteer Rapport Mandatory Service eklentileri dışında, ek ücret karşılığında ilişkili bir Premium Destek ürünü sağlanır.

IBM Trusteer Rapport II for Business veya IBM Trusteer Rapport II for Retail aboneliği, bu maddede sıralanan ilgili ek Bulut Hizmetleri için ön koşul niteliğindedir.

1.1.4 IBM Trusteer Pinpoint Malware Detection II için ek Bulut Hizmetleri

a. IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business veya IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business için mevcut olan ek Bulut Hizmetleri:
   - IBM Trusteer Rapport Remediation for Business (Ticari Faaliyet İçin IBM Trusteer Rapport İyileştirme)
   - IBM Trusteer Pinpoint Malware Detection Additional Applications for Business (Ticari Faaliyet İçin IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Tespiti Ek Uygulamaları)

b. IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail veya IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail için mevcut olan ek Bulut Hizmetleri:

- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail (Perakende İçin IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Tespiti Ek Uygulamaları)

Premium destek, bu belgede belirtildiği şekilde belirli olanaklar için sağlanır. IBM Trusteer Pinpoint Malware Detection II for Business veya IBM Trusteer Pinpoint Malware Detection II for Retail aboneliği, bu maddede sıralanan ilgili ek Bulut Hizmetleri için ön koşul niteliğindedir.

1.1.5 IBM Trusteer Pinpoint Detect Standard ve/veya IBM Trusteer Pinpoint Detect Premium ve/veya IBM Trusteer Pinpoint Detect Standard for Retail ve/veya IBM Trusteer Pinpoint Detect Premium for Retail ve/veya IBM Trusteer Pinpoint Detect Standard for Business ve/veya IBM Trusteer Pinpoint Detect Premium for Business için mevcut olan ek Bulut Hizmetleri

a. IBM Trusteer Detect Standard for Business ve/veya IBM Trusteer Pinpoint Detect Premium for Business için mevcut olan ek Bulut Hizmetleri:

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business (Ticari Faaliyet İçin IBM Trusteer Pinpoint Kötü Amaçlı Yazılım Tespiti - Standart Ek Uygulamaları)
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business
- IBM Trusteer Digital Content Pack for Business
- IBM Trusteer New Account Fraud for Business (Ticari Faaliyet İçin IBM Trusteer Yeni Hesap Sahtekarlığı)

b. IBM Trusteer Detect Standard for Retail ve/veya IBM Trusteer Pinpoint Detect Premium for Retail için mevcut olan ek Bulut Hizmetleri:

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail (Perakende İçin IBM Trusteer Pinpoint Tespit Premium Ek Uygulamaları)
- IBM Trusteer Digital Content Pack for Retail
- IBM Trusteer New Account Fraud for Retail (Perakende İçin IBM Trusteer Yeni Hesap Sahtekarlığı)

c. IBM Trusteer Pinpoint Detect Standard ve/veya IBM Trusteer Pinpoint Premium için mevcut olan ek Bulut Hizmetleri:

- IBM Trusteer Pinpoint Detect Standard Application (IBM Trusteer Pinpoint Tespit Standart Uygulaması)
- IBM Trusteer Pinpoint Detect Premium Application (IBM Trusteer Pinpoint Tespit Premium Uygulaması)

d. IBM Trusteer Pinpoint Detect Premium için mevcut olan ek Bulut Hizmetleri

- IBM Trusteer Pinpoint Verify (IBM Trusteer Pinpoint Doğrulama)

IBM Trusteer Pinpoint Detect Standard veya IBM Trusteer Pinpoint Detect Premium veya IBM Trusteer Pinpoint Detect Standard for Retail veya IBM Trusteer Pinpoint Detect Premium for Retail veya IBM Trusteer Pinpoint Detect Standard for Business veya IBM Trusteer Pinpoint Detect Premium for Business aboneliği, bu maddede belirtilen ilgili ek Bulut Hizmetleri için ön koşul niteliğindedir.

1.1.6 Diğer Ek Bulut Hizmetleri

Burada sıralanmayan ve yukarıda belirtilen temel abonelikler için şu anda mevcut veya halen geliştirilmekte olan herhangi bir ek IBM Cloud Hizmetleri aboneliği, güncelleme olarak kabul edilmez; bunlar ayrı olarak verilmelidir.

1.2 Tanımlar

Hesap Sahibi – Müşterinin, istemci etkinleştirme yazılımı kurmuş, son kullanıcı lisans sözleşmesini ("EULA") kabul etmiş ve Müşterinin Bulut Hizmetleri kapsamına abone olduğu Müşterinin Ticari Faaliyet ve/veya Perakende Uygulamasında en az bir kez kimliği doğrulanmış olan, Müşterinin son kullanıcısı anlamına gelir.

Hesap Sahibi İstemci Yazılımı – IBM Trusteer Rapport istemci etkinleştirme yazılımını veya son kullanıcının aygıtı üzerinde kurulum için bazı Bulut Hizmetleri ile sağlanan diğer her türlü istemci etkinleştirme yazılımını ifade eder.

Trusteer Splash – mevcut açılış ekranı şablonlarına dayalı olarak Müşteriye sağlanan açılış ekranı anlamına gelir.

Açılış Sayfası – Müşteriye, Müşterinin açılış ekranı ve karşıdan yüklenebilir Hesap Sahibi İstemci Yazılımı ile sağlanan, IBM tarafından barındırılan sayfa anlamına gelir.

1.3 IBM Trusteer Rapport Bulut Hizmetleri

1.3.1 IBM Trusteer Rapport II for Retail ve/veya IBM Trusteer Rapport II for Business ("Trusteer Rapport II")

Trusteer Rapport II Bulut Hizmeti, IBM Trusteer Rapport'un, birden fazla Uygulamanın korunmasıyla ilgili ücretlerin standartlaştırılmasına yardımcı olmak için tasarlanmış yeni bir oluşumudur ve Uygulamalar eklenirken bir kerelik ücretlerin yerine geçer.

Trusteer Rapport II, kimlik avı dolandırıcılığı ve Man-in-the-Browser (MitB) kötü amaçlı yazılım saldırılarına karşı bir koruma katmanı sağlar. IBM Trusteer Rapport, dünya genelinde on milyonlarca uç noktadan oluşan bir ağı kullanarak, dünya çapındaki kuruluşlara karşı gerçekleştirilen aktif kimlik avı dolandırıcılığı (phishing) ve kötü amaçlı yazılım saldırılarına ilişkin bilgileri toplar. IBM Trusteer Rapport, kimlik avı dolandırıcılığı saldırılarını engellemeyi ve MitB kötü amaçlı yazılım türlerinin kurulmasını ve çalışmasını önlemeyi hedefleyen, davranışa dayalı algoritmalar uygular.

Bu Bulut Hizmetine, Hak Kazanan Katılımcıya ilişkin ücret ölçüsü ya da İstemci Aygıta ilişkin ücret ölçüsü kapsamında hak kazanılır. Ticari Faaliyet olanağı, 10 Hak Kazanan Katılımcıdan ya da 10 İstemci Aygıttan oluşan paketler halinde satılır. Perakende olanağı, 100 Hak Kazanan Katılımcıdan veya 100 İstemci Aygıttan oluşan paketler halinde satılır.

Bu Bulut Hizmeti ürününe aşağıda belirtilenler dahildir:

a. Trusteer Management Application ("TMA"):

   TMA, IBM Trusteer'ın bulutta barındırılan ortamında sağlanır. Müşteri (ve onun sınırsız sayıdaki yetkili personeli), bu ortam aracılığıyla sayılanları yapabilir: (i) olay verilerine ilişkin raporlamayı ve risk değerlendirmelerini görüntüleyebilir ve yükleyebilir, ve (ii) son kullanıcı lisans sözleşmesi ("EULA") kapsamında, ücretsiz olarak Müşterinin Hak Kazanan Katılımcılarına lisanslanan ve Hak Kazanan Katılımcının masaüstüne veya aygıtlarına yüklemek üzere sağlanan Trusteer Rapport yazılım grubu ("Hesap Sahibi İstemci Yazılımı") olarak da bilinen istemci etkinleştirme yazılımının yapılandırmasını görüntüleyebilir. Müşteri, Hesap Sahibi İstemci Yazılımını, yalnızca Trusteer Splash'i veya Rapport API'yi kullanarak pazarlayabilir ve bu yazılımı, dahili iş operasyonları veya çalışanlarının kullanımı (çalışanların kişisel kullanımı dışında) için kullanamaz.

b. Web Komut Dosyası:

   Bulut Hizmetine erişme veya bu hizmeti kullanma amacıyla bir web sitesinde erişim için

c. Olay verileri:

   Müşteri (ve onun sınırsız sayıdaki yetkili personeli), Müşterinin, Bulut Hizmetleri kapsamına abone olduğu Ticari Faaliyet veya Perakende Uygulaması ile Hesap Sahiplerinin çevrimiçi etkileşimlerinin sonucunda, Hesap Sahibi İstemci yazılımı tarafından üretilen olay verilerini almak için TMA'yı kullanabilir. Olay verileri, son kullanıcı lisans sözleşmesini kabul etmiş ve en az bir kez Müşterinin Ticari Faaliyet veya Perakende Uygulamalarında kimliği doğrulanmış olan Hak Kazanan Katılımcıların aygıtlarının üzerinde çalıştığı Hesap Sahibi İstemci Yazılımından elde edilecektir ve İstemcinin yapılandırması Kullanıcı Kimliklerinin derlemini içermelidir.

d. Trusteer Splash:

   Trusteer Splash pazarlama platformu, Müşterinin Bulut Hizmetleri kapsamına abone olduğu Müşterinin Ticari Faaliyet ve/veya Perakende Uygulamalarına erişen Hak Kazanan Katılımcıları tanımlar ve bunlara Hesap Sahibi İstemci Yazılımını pazarlar. Müşteri, mevcut "Splash Templates" açılış ekranlarından seçim yapabilir. Özelleştirilmiş açılış ekranı için, ayrı bir sözleşme veya hizmet bildirimi kapsamında bir anlaşma yapılabilir.

Müşteri, markalarını, logolarını veya simgelerini, TMA ile bağlantılı olarak kullanım için, yalnızca Trusteer Splash ile birlikte kullanılmak ve Hesap Sahibi İstemci Yazılımında veya IBM tarafından barındırılan açılış

sayfasında ve IBM Trusteer web sitesinde gösterilmek üzere sağlamayı kabul edebilir. Sağlanan tüm markalarının, logolarının veya simgelerinin kullanımı, IBM'in reklam ve marka kullanımıyla ilgili makul ilkelerine uygun olacaktır.

Müşterinin, Hesap Sahibi İstemci Yazılımına ilişkin herhangi türde zorunlu devreye alma işlemini kullanmak istemesi halinde, Müşteri, IBM Trusteer Rapport Mandatory Service Bulut Hizmetine abone olmalıdır.

Müşterinin, Hesap Sahibi İstemci Yazılımına ilişkin zorunlu devreye alma işlemi aşağıdakileri içerir, ancak bunlarla sınırlı değildir: Hak Kazanan Katılımcıyı, Hesap Sahibi İstemci Yazılımını yüklemeye doğrudan veya dolaylı olarak zorlayan herhangi bir mekanizma veya araç tarafından yapılan herhangi bir türde zorunlu devreye alma işlemi veya Hesap Sahibi İstemci Yazılımının bu zorunlu devreye alma işlemine ilişkin lisanslama gereksinimlerini atlamak için oluşturulan, IBM tarafından oluşturulmamış veya onaylanmamış olan herhangi bir yöntem, araç, prosedür, sözleşme veya mekanizma.

Trusteer Rapport II for Business ve/veya Trusteer Rapport II for Retail ürünlerinin her biri bir Uygulama için korumayı içerir. Her ek Uygulama için, Müşterinin IBM Trusteer Rapport Additional Applications için yetki edinmesi gerekir.

1.3.2 IBM Trusteer Rapport II for Business ve/veya IBM Trusteer Rapport II for Retail için İsteğe Bağlı Ek Bulut Hizmetleri

IBM Trusteer Rapport II Bulut Hizmetleri aboneliği, aşağıda belirtilen ek Bulut Hizmetlerinden herhangi birine abonelik için ön koşul niteliğindedir. Bulut Hizmetleri, "Ticari Faaliyet için" olarak belirlendiyse, edinilen ek Bulut Hizmetleri de "Ticari Faaliyet için" olarak belirlenmelidir. Bulut Hizmetleri, "Perakende için" olarak belirlendiyse, edinilen ek IBM Cloud Hizmetleri de "Perakende için" olarak belirlenmelidir. Müşteri, olay verilerini, son kullanıcı lisans sözleşmesini kabul etmiş, en az bir kez Müşterinin Ticari Faaliyet ve/veya Perakende Uygulamalarında kimliği doğrulanmış olan ve Hesap Sahibi İstemci Yazılımını çalıştıran Hak Kazanan Katılımcılardan ya da İstemci Aygıtlardan alacaktır ve İstemcinin yapılandırması Kullanıcı Kimliklerinin elde edilmesini içermelidir.

1.3.3 IBM Trusteer Rapport Fraud Feeds for Business ve/veya IBM Trusteer Rapport Fraud Feeds for Retail

Bu eklenti Bulut Hizmetine abone olurken, Müşteri (ve onun sınırsız sayıdaki yetkili personeli), Trusteer Rapport Bulut Hizmetinden üretilen tehdit akışlarını görüntülemek, bunlara abone olmak ve bunların sağlanmasını yapılandırmak için TMA'yı kullanabilir. Akışlar, saptanmış e-posta adreslerine e-posta ile veya SFTP aracılığıyla metin dosyaları olarak gönderilebilir.

Bu olanak, yalnızca Hak Kazanan Katılımcıya ilişkin ücret ölçüsü kapsamında geçerlidir.

1.3.4 IBM Trusteer Rapport Phishing Protection for Business ve/veya IBM Trusteer Rapport Phishing Protection for Retail

Müşteri (ve onun sınırsız sayıdaki yetkili personeli), Hesap Sahibinin oturum açmaya ilişkin kimlik bilgilerini, dolandırıcı olduğundan şüphelenilen veya potansiyel olarak dolandırıcı nitelikte bir siteye göndermeyle ilgili olay verisi bildirimlerini almak için TMA'yı kullanabilir. Yasalara uygun çevrimiçi uygulamalar (URL adresleri), yanlışlıkla kimlik avı dolandırıcılığı sitesi olarak işaretlenebilir ve Bulut Hizmetleri, Hesap Sahiplerini, meşru bir sitenin kimlik avı dolandırıcılığı sitesi olduğu konusunda uyarabilir. Bu gibi durumlarda, Müşteri, bu tür bir hatayı IBM'e bildirmelidir. IBM hatayı düzeltecektir. Bu, Müşterinin bu tür bir hataya yönelik tek çözüm yolu olacaktır.

Bu Bulut Hizmetine, Hak Kazanan Katılımcıya ilişkin ücret ölçüsü ya da İstemci Aygıta ilişkin ücret ölçüsü kapsamında hak kazanılır. Ticari Faaliyet olanağı, 10 Hak Kazanan Katılımcıdan ya da 10 İstemci Aygıttan oluşan paketler halinde satılır. Perakende olanağı, 100 Hak Kazanan Katılımcıdan veya 100 İstemci Aygıttan oluşan paketler halinde satılır.

Bu bulut hizmetleri için premium destek, Hak Kazanan Katılımcıya ilişkin ücret ölçüsü ya da İstemci Aygıta ilişkin ücret ölçüsü kapsamında alınabilir. Ticari Faaliyet olanağı, 10 Hak Kazanan Katılımcıdan ya da 10 İstemci Aygıttan oluşan paketler halinde satılır. Perakende olanağı, 100 Hak Kazanan Katılımcıdan veya 100 İstemci Aygıttan oluşan paketler halinde satılır.

1.3.5 IBM Trusteer Rapport Mandatory Service for Business ve/veya IBM Trusteer Rapport Mandatory Service for Retail

Müşteri (ve onun sınırsız sayıdaki yetkili personeli), Müşterinin, Bulut Hizmetleri kapsamına abone olduğu Müşterinin Ticari Faaliyet ve/veya Perakende Uygulamalarına erişen Hak Kazanan Katılımcılara Hesap

Sahibi İstemci Yazılımını yüklemeyi zorunlu kılmak için, Trusteer Splash pazarlama platformunun bir eşgörünümünü kullanabilir.

IBM Trusteer Rapport Premium Support for Business, IBM Security Rapport Mandatory Service for Business için ön koşul niteliğindedir.

IBM Trusteer Rapport Premium Support for Retail, IBM Security Rapport Mandatory Service for Retail için ön koşul niteliğindedir.

Müşteri, yalnızca Müşterinin, Bulut Hizmetleri kapsamına abone olduğu Müşterinin Ticari Faaliyet veya Perakende Uygulaması ile birlikte kullanılmak üzere sipariş edilmiş veya yapılandırılmış olması kaydıyla, IBM Trusteer Rapport Mandatory Service'ın ek işlevlerini uygulayabilir.

Bu Bulut Hizmetine Hak Kazanan Katılımcıya ilişkin ücret ölçüsü kapsamında hak kazanılır. Ticari Faaliyet olanağı, 10'luk paketler halinde satılır. Perakende olanağı, 100 Hak Kazanan Katılımcıdan oluşan paketler halinde satılır.

1.3.6 IBM Trusteer Rapport Large Redeployment ve/veya IBM Trusteer Rapport Small Redeployment

Kendi çevrimiçi bankacılık Uygulamalarını hizmet süresi içerisinde yeniden devreye alan ve bunun sonucunda da kendi IBM Trusteer Rapport II devreye alımlarında değişiklik yapması gereken Müşteriler, IBM Trusteer Rapport Redeployment Bulut Hizmetini satın almalıdır.

Yeniden devreye alma, Müşterinin Uygulamanın etki alanını veya anasistem URL adresini değiştirmesi, değişiklikleri Splash yapılandırmasında uygulaması veya yeni çevrimiçi bankacılık platformuna geçmesi nedeniyle ortaya çıkabilir.

Müşteri, 6 aylık yeniden devreye alma geçiş dönemi için, halihazırda abone olunan Uygulamaların üzerinde çalışan birebir temelinde ek Uygulamalara hak kazanır.

IBM Trusteer Rapport Large Redeployment, 20.000'den fazla kullanıcısı olan ortamlar için, IBM Trusteer Rapport Small Redeployment ise 20.000 veya daha az kullanıcısı olan ortamlar için uygulanır.

1.3.7 IBM Trusteer Rapport Additional Applications for Business ve/veya IBM Trusteer Rapport Additional Applications for Retail

IBM Trusteer Rapport II for Business için; ilk Uygulamadan sonraki herhangi bir ek Ticari Faaliyet Uygulamasında devreye alma işlemi için IBM Trusteer Rapport Additional Applications for Business Bulut Hizmeti yetkisi olması gerekir. IBM Trusteer Rapport II for Retail için; ilk Uygulamadan sonraki herhangi bir ek Perakende Uygulamasında devreye alma işlemi için IBM Trusteer Rapport Additional Applications for Retail Bulut Hizmeti yetkisi olması gerekir.

1.4 IBM Trusteer Pinpoint Bulut Hizmetleri

IBM Trusteer Pinpoint, ek bir koruma katmanı sağlamak üzere tasarlanmış, bulut tabanlı bir hizmettir ve kötü amaçlı yazılım, kimlik avı dolandırıcılığı ve hesap ele geçirme saldırılarını tespit etmeyi ve azaltmayı amaçlar. Trusteer Pinpoint, Müşterinin, Bulut Hizmetleri kapsamına abone olduğu Müşterinin Ticari Faaliyet ve/veya Perakende Uygulamalarıyla ve dolandırıcılığı önleme süreçleriyle bütünleştirilebilir.

Bu Bulut Hizmetine aşağıda belirtilenler dahildir:

a. TMA:

   TMA, IBM Trusteer'ın bulutta barındırılan ortamında sağlanır. Müşteri (ve onun sınırsız sayıdaki yetkili personeli), bu ortam aracılığıyla sayılanları yapabilir: i) olay verilerine ilişkin raporlamayı ve risk değerlendirmelerini görüntüleyebilir ve karşıdan yükleyebilir ve (ii) Pinpoint olanaklarından üretilen tehdit akışlarını görüntüleyebilir, bunlara abone olabilir ve bunların sağlanmasını yapılandırabilir.

b. Web Komut Dosyası ve/veya Uygulama Programı Arabirimleri (API'ler):

   Bulut Hizmetine erişmek veya bu hizmeti kullanmak amacıyla bir web sitesinde devreye almak için

1.4.1 IBM Trusteer Pinpoint Malware Detection

Müşteri, IBM Trusteer Pinpoint Malware Detection II Bulut Hizmetlerinde kötü amaçlı yazılım tespit edilmesi durumunda, Pinpoint En İyi Uygulamalar Kılavuzunu takip etmelidir. IBM Trusteer Pinpoint Malware Detection II Bulut Hizmetleri, başkalarının IBM Trusteer Pinpoint Bulut Hizmetlerinin kullanılmasıyla Müşteri eylemleri arasında bağlantı kurmasını sağlayacak şekilde bir kötü amaçlı yazılımın veya hesap ele geçirme saldırısının tespit edilmesinden hemen sonra Hak Kazanan Katılımcının deneyimini etkileyecek hiçbir şekilde kullanılmamalıdır (örneğin, kötü amaçlı yazılımın tespit edilmesinden

veya hesabın ele geçirilmesinin tespit edilmesinden hemen sonra bildirimler, iletiler, aygıtların engellenmesi veya Ticari Faaliyet ve/veya Perakendecilik Uygulamasına erişimin engellenmesi).

1.4.2 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business ve/veya IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail ve/veya IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business ve/veya IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

IBM Security Pinpoint Malware Detection II, IBM Trusteer Pinpoint Malware Detection'ın birden fazla Uygulamanın korunmasıyla ilgili ücretlerin standartlaştırılmasına yardımcı olmak için tasarlanmış yeni bir oluşumudur ve Uygulamalar eklenirken bir kerelik ücretlerin yerine geçer.

Ticari Faaliyet ve/veya Perakende Uygulamasına bağlanan Man in the Browser (MitB) adlı finansal kötü amaçlı yazılımın bulaştığı tarayıcıların istemci olmadan tespit edilmesidir. IBM Trusteer Pinpoint Malware Detection Bulut Hizmetleri, bir başka koruma katmanı sağlar ve MitB finansal kötü amaçlı yazılım varlığına ilişkin uyarıları ve değerlendirmeleri sağlayarak, kuruluşların, kötü amaçlı yazılım riskine dayalı dolandırıcılık önleme süreçlerine odaklanmasına olanak tanımayı hedefler.

a. Olay verileri:

   Müşteri (ve onun sınırsız sayıdaki yetkili personeli), Müşterinin Ticari Faaliyet ve/veya Perakende Uygulamaları ile Hak Kazanan Katılımcıların çevrimiçi etkileşimlerinin sonucunda oluşturulan olay verilerini almak için TMA'yı kullanabilir.

b. Advanced Edition:

   Ticari Faaliyet ve/veya Perakendecilik teklifleri için Advanced Sürümleri, Müşterinin Ticari Faaliyet ve/veya Perakendecilik Uygulamalarının yapısına ve akışına göre ayarlanıp özelleştirilen ek tespit ve koruma katmanı sunar ve Müşteriyi hedefleyen belirli tehdit ortamlarına göre özelleştirilebilir. Müşterinin Ticari Faaliyet ve/veya Perakende Uygulamalarında çeşitli lokasyonlara dahil edilebilir.

   Advanced Edition, Müşteriye minimum miktarlarda sunulur. Bu miktarlar, Perakendecilik için 100 adet Hak Kazanan Katılımcı içeren 1000 paket veya Ticari Faaliyet için 10 adet Hak Kazanan Katılımcı içeren 1000 paket olmak üzere en az 100.000 Perakendecilik İçin Hak Kazanan Katılımcı veya 10.000 Ticari Faaliyet İçin Hak Kazanan Katılımcıdır.

c. Standard Edition:

   Ticari Faaliyet veya Perakendecilik için Standard Sürümleri, burada açıklandığı gibi, bu Bulut Hizmetinin temel işlevlerini sağlayan, hızlı devreye alınan çözümlerdir.

Bu Bulut Hizmetine bir adet Uygulamanın korunması dahildir. Müşterinin, her ek Uygulama için, IBM Trusteer Pinpoint Malware Detection Additional Applications için yetki edinmesi gerekir.

1.4.3 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail ve/veya IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail ve/veya IBM Pinpoint Trusteer Pinpoint Malware Detection Standard Edition II for Business ve/veya IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business için İsteğe Bağlı Ek Bulut Hizmetleri

- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail ya da IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail; IBM Trusteer Rapport Remediation for Retail Cloud Service için ön koşul niteliğindedir.
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business ya da IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business; IBM Trusteer Rapport Remediation for Business Bulut Hizmeti için ön koşul niteliğindedir.

1.4.4 IBM Trusteer Rapport Remediation for Retail ve/veya IBM Trusteer Rapport Remediation for Business

IBM Trusteer Rapport Remediation for Retail ve IBM Trusteer Rapport Remediation for Business ürünleri, MitB kötü amaçlı yazılım bulaşmasının, IBM Trusteer Pinpoint Malware Detection'ın olay verileriyle saptandığı durumda, Müşterinin Uygulamasına özel amaçlı olarak erişen, Müşterinin Hak Kazanan Katılımcılarının etkilenen aygıtlarındaki man-in-the-browser (MitB) kötü amaçlı yazılım bulaşmasını araştırmayı, düzeltmeyi, engellemeyi ve kaldırmayı amaçlar. Müşteri, halihazırda Müşterinin Uygulaması üzerinde çalışan IBM Trusteer Pinpoint Malware Detection II aboneliğine sahip olmalıdır. Müşteri, bu Bulut Hizmeti olanağını, sadece Müşterinin Uygulamasına erişimi olan Hak Kazanan Katılımcılar ile bağlantılı olarak ve yalnızca kötü amaçlı yazılım bulaşan aygıtı (PC/MAC) özel amaçlı olarak araştırıp düzeltmeyi amaçlayan bir araç olarak kullanabilir. IBM Trusteer Rapport Remediation, etkilenen Hak

Kazanan Katılımcının aygıtı (PC/MAC) üzerinde fiili olarak çalışmalıdır. Etkilenen Hak Kazanan Katılımcı, son kullanıcı lisans sözleşmesini kabul etmeli, Müşterinin Uygulamasında/Uygulamalarında en az bir kez kimliği doğrulanmalı ve Müşterinin yapılandırması ise Kullanıcı kimliklerinin derlemini içermelidir. Herhangi bir şüpheye yer vermemek için, bu Bulut Hizmeti olanağı, Trusteer Splash'ı kullanma hakkını içermez ve/veya başka herhangi bir şekilde Hesap Sahibi İstemci Yazılımının Müşterinin genel Hak Kazanan Katılımcı topluluğuna tanıtımını yapmaz.

1.4.5 IBM Trusteer Pinpoint Malware Detection Redeployment

Kendi çevrimiçi bankacılık Uygulamalarını hizmet süresi içerisinde yeniden devreye alan ve bunun sonucunda da kendi IBM Trusteer Pinpoint Malware Detection II devreye alımlarında değişiklik yapması gereken Müşteriler, IBM Trusteer Pinpoint Malware Detection Redeployment satın almalıdır.

Yeniden devreye alma, Müşterinin Uygulamanın etki alanını veya anasistem URL adresini değiştirmesi, çevrimiçi Uygulamasını yeni teknolojiye dönüştürmesi, yeni çevrimiçi bankacılık platformuna geçmesi veya mevcut bir Uygulamaya yeni oturum açma akışı eklemesi nedeniyle ortaya çıkabilir.

Müşteri, 6 aylık yeniden devreye alma geçiş dönemi için, halihazırda abone olunan Uygulamaların üzerinde çalışan birebir temelinde ek Uygulamalara hak kazanır.

İlk Uygulamadan sonraki herhangi bir ek Uygulama üzerindeki IBM Trusteer Pinpoint Malware Detection Additional Applications veya IBM Trusteer Pinpoint Malware Detection II Standard Edition veya IBM Trusteer Pinpoint Malware Detection II Advanced Edition devreye alımı için IBM Trusteer Pinpoint Malware Detection Additional Applications yetkisi gerekir.

1.4.6 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail ve/veya IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail veya IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail için ilk Uygulamadan sonraki herhangi bir ek Perakendecilik Uygulaması devreye alımı için IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail yetkisi gereklidir.
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business veya IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business için ilk Uygulamadan sonraki herhangi bir ek Ticari Faaliyet Uygulaması devreye alımı için IBM Trusteer Pinpoint Malware Detection Additional Applications for Business yetkisi gereklidir.

1.5 IBM Trusteer Fraud Protection Suite

IBM Trusteer Fraud Protection Suite ("Ürün Grubu"), sahtekarlığa karşı koruma katmanı sağlamak için tasarlanmış olan, bulut tabanlı hizmetlerden oluşan bir ürün grubudur ve bir yaşam döngüsü yönetim çözümü sağlamak için ek IBM ürünleriyle bütünleştirilebilir. Bu Ürün Grubu aşağıdaki bulut tabanlı hizmetleri içerir:

- IBM Trusteer Pinpoint Detect, kötü amaçlı yazılım, kimlik avı dolandırıcılığı ve hesap ele geçirme saldırılarını tespit edip azaltmayı hedefler. Trusteer Pinpoint Detect, Müşterinin Bulut Hizmetleri kapsamına abone olduğu Müşterinin Ticari Faaliyet ve/veya Perakende Uygulamalarıyla ve sahtekarlığı önleme süreçleriyle bütünleştirilebilir.
- IBM Trusteer Rapport for Mitigation, saldırılardan etkilenen uç noktaları iyileştirmeyi ve korumayı hedefler.

Bulut Hizmetleri aşağıdakileri içerir:

a. TMA:

   TMA, IBM Trusteer'ın bulutta barındırılan ortamında sağlanır. Müşteri (ve onun sınırsız sayıdaki yetkili personeli), bu ortam aracılığıyla sayılanları yapabilir: i) olay verilerine ilişkin raporlamayı ve risk değerlendirmelerini alabilir ve (ii) olay verilerinin raporlanmasıyla ilgili güvenlik ilkelerini ve ilkeleri görüntüleyebilir, yapılandırabilir ve belirleyebilir.

b. Olay verileri:

   Müşteri (ve onun sınırsız sayıdaki yetkili personeli), Müşterinin Bulut Hizmeti kapsamına abone olduğu Uygulamaları ile Hak Kazanan Katılımcıların çevrimiçi etkileşimlerinin sonucunda oluşturulan olay verilerini almak için TMA'yı kullanabilir veya Müşteri, olay verilerini arka uç Uygulama Programı Arabirimi (API) sağlama kipi aracılığıyla alabilir.

c. Web Komut Dosyası ve/veya Uygulama Programı Arabirimleri (API'ler):

Bulut Hizmetine erişmek veya bu hizmeti kullanmak amacıyla bir web sitesinde devreye almak için

Pinpoint En İyi Uygulamaları

Kötü niyetli yazılım olduğunun veya hesapların ele geçirildiğinin tespit edilmesi durumunda, Müşteri, Pinpoint En İyi Uygulamalar Kılavuzuna (Pinpoint Best Practices Guide) uymalıdır. IBM Trusteer Pinpoint Detect Bulut Hizmetleri, başkalarının, IBM Trusteer Pinpoint Detect olanaklarının kullanılmasıyla Müşteri eylemleri arasında bağlantı kurmasını sağlayacak şekilde bir kötü amaçlı yazılımın veya hesap ele geçirme saldırısının tespit edilmesinden hemen sonra Hak Kazanan Katılımcının deneyimini etkileyecek hiçbir şekilde kullanılmamalıdır (örn: kötü amaçlı yazılımın tespit edilmesinden veya hesabın ele geçirilmesinin tespit edilmesinden hemen sonra bildirimler, iletiler, aygıtların engellenmesi veya Ticari Faaliyet ve/veya Perakende Uygulamasına erişimin engellenmesi).

1.5.1 IBM Trusteer Pinpoint Detect Standard for Retail ve/veya IBM Trusteer Pinpoint Detect Standard for Business

Bu Bulut Hizmeti, tek ve birleşik bir çözüm sunmak üzere IBM Trusteer Pinpoint Criminal Detection ve IBM Trusteer Pinpoint Malware Detection ürünlerini birleştirir.

Bu çözüm, aygıt kimliği, kimlik avı tespit edilmesi ve kötü amaçlı yazılım odaklı kimlik bilgisi hırsızlığının tespit edilmesi yoluyla, bir Perakendecilik ya da Ticari Faaliyet Uygulamasına bağlı tarayıcılarda yapıldığından şüphelenilen hesap ele geçirme etkinliğinin ve/veya bir kötü amaçlı yazılımın istemci olmadan tespit edilmesini sağlar. IBM Trusteer Pinpoint olanakları, ek bir koruma katmanı sağlar, hesap ele geçirme girişimlerini tespit etmeyi hedefler ve bir Perakendecilik veya Ticari Faaliyet Uygulamasına erişen mobil aygıtlara veya tarayıcılara ilişkin risk değerlendirme puanlarını Müşteriye doğrudan sağlar (yerel tarayıcı veya müşteri mobil uygulaması yoluyla).

Standart Destek (yukarıda Teknik Destek maddesinde tanımlandığı şekilde) bu Bulut Hizmetine dahildir. Premium destek için Müşterinin Pinpoint Standard Premium Support satın alması gerekir.

Bu Bulut Hizmetine bir adet Uygulamanın korunması dahildir. Müşterinin, her ek Uygulama için, IBM Trusteer Pinpoint Detect Standard Additional Applications için yetki edinmesi gerekir.

Hizmet, 100 Hak Kazanan Katılımcıdan oluşan paketler halinde veya 100 Bağlantıdan oluşan paketler halinde satın alınmak üzere sunulur. Müşterinin Bağlantılara göre hizmeti satın almayı seçmesi durumunda, ilk uygulamadan itibaren Ek Uygulama ücreti uygulanır.

1.5.2 IBM Trusteer Pinpoint Detect Premium for Retail ve/veya IBM Trusteer Pinpoint Detect Premium for Business

Bu Bulut Hizmeti, tek ve bütünleştirmesi kolay olan bir birleşik çözüm sunmak üzere IBM Trusteer zere Pinpoint Criminal Detection ve IBM Trusteer Pinpoint Malware Detection ürünlerini birleştirir.

Bu çözüm, aygıt kimliği, kimlik avı tespit edilmesi ve kötü amaçlı yazılım odaklı kimlik bilgisi hırsızlığının tespit edilmesi yoluyla, bir Perakendecilik ya da Ticari Faaliyet Uygulamasına bağlı tarayıcılarda yapıldığından şüphelenilen hesap ele geçirme etkinliğinin ve/veya bir kötü amaçlı yazılımın istemci olmadan tespit edilmesini sağlar. IBM Trusteer Pinpoint olanakları, ek bir koruma katmanı sağlar, hesap ele geçirme girişimlerini tespit etmeyi hedefler ve Ticari Faaliyet veya Perakende Uygulamasına erişen mobil aygıtlara veya tarayıcılara ilişkin risk değerlendirme puanlarını Müşteriye doğrudan sağlar (yerel tarayıcı veya müşteri mobil uygulaması yoluyla).

Bu hizmet, genişletilmiş devreye alma ve kurulum hizmetleri, uyarlanmış güvenlik ilkeleri, araştırma hizmetleri ve benzer hizmetler dahil olmak üzere geliştirilmiş işlevsellik ve hizmetler içerir. Hizmet, uygulama başına devreye alma hizmetleri için 200 saate kadar paylaşılan kaynak ve kurulum sonrası uygulama başına güvenlik analizi için 200 saat paylaşılan kaynak içerir. Sürekli hizmetler, uygulama başına yıllık 20 saat devreye alma bakımı ve uygulama başına yıllık 100 saat güvenlik araştırması içerir. Ek çalışma ek ücrete tabidir.

Pinpoint Detect, hem Mobil hem Web kanallarındaki işlemleri kullanabilir. Mobil işlemlerin dahil edilmesi durumunda, Bağlantı bazında Pinpoint uygulanır. Bu Bulut Hizmetine bir adet Uygulamanın korunması dahildir. Müşterinin, her ek Uygulama için, IBM Trusteer Pinpoint Detect Premium Additional Applications için yetki edinmesi gerekir.

Premium destek bu Bulut Hizmetine dahildir.

IBM Trusteer Pinpoint Detect Premium for Retail ve Business hizmetleri, 100 Hak Kazanan Katılımcıdan oluşan paketler halinde veya IBM Trusteer Pinpoint Detect Premium için 100 Bağlantıdan oluşan paketler

halinde satın alınmak üzere sunulur. Müşterinin Bağlantılara göre hizmeti satın almayı seçmesi durumunda, ilk uygulamadan itibaren Ek Uygulama ücreti uygulanır.

Pinpoint Detect Policy Manager:

Policy Manager, Pinpoint Detect Premium hizmetine dahildir ve IBM Trusteer bulutta barındırılan ortamında kullanıma sunulur. Müşteri (ve onun sınırsız sayıdaki yetkili personeli), bu özellik aracılığıyla sayılanları yapabilirler: (i) sahtekarlık faaliyetlerini saptamak için mantık tasarlanması, test edilmesi ve üretim ortamında devreye alınması, (ii) raporların ve gösterge panolarının tasarlanması, ve (iii) müşterinin Uygulaması üzerinde yapılan şüpheli faaliyetleri saptamak için güvenlik ilkelerinin ve politikaların görüntülenmesi, yapılandırılması ve belirlenmesi.

Policy Manager özelliğinin etkinleştirilmesi ve daha ayrıntılı araştırmanın gerektiği destek için danışmanlık hizmetleri gerekir. Danışmanlık hizmetlerinin ayrıntıları, ayrı bir hizmet bildiriminde belirtilecektir.

IBM, Policy Manager etkinleştirildiğinde, ilke değişikliklerinden kaynaklanan önemli sorunları gidermek için Müşterinin ilkelerini ayarlama desteği sunmak amacıyla Müşterinin ortamına erişme hakkını saklı tutar.

Müşteri, Policy Manager aracılığıyla kullanıma açılabilecek herhangi bir verinin kötü amaçlı kullanımına karşı verileri koruyacağını taahhüt eder.

Müşteri, Policy Manager özelliği etkinleştirildiğinde, kural ayarları için belgelerde açıklandığı şekilde IBM'in yönergelerini izlemelidir. Müşteri, Müşterinin bu önerilere uymamasından kaynaklanan durumlarda IBM'in sorumlu olmayacağını kabul eder.

Policy Manager özelliğinin Müşteri tarafından yanlış yapılandırılması nedeniyle ortaya çıkan herhangi bir durağanlık ve/veya hizmet performansında bir düşüş olması sorunu Hizmet Seviyesi Sözleşmesi hesaplamasında Kapalı Kalma Süresi olarak değerlendirilecektir.

1.5.3 IBM Trusteer Pinpoint Detect Standard ve/veya IBM Trusteer Pinpoint Detect Premium İçin İsteğe Bağlı Hizmetler

Bu maddedeki Bulut Hizmetleri için ön koşul olarak, IBM Trusteer Pinpoint Detect Premium veya IBM Trusteer Pinpoint Detect Standard ürünü için yetki edinilmesi gerekir.

1.5.4 IBM Trusteer Rapport for Mitigation for Retail ve/veya IBM Trusteer Rapport for Mitigation for Business

- IBM Trusteer Rapport for Mitigation for Retail ürünü, kötü amaçlı yazılım bulaşmasının IBM Trusteer Pinpoint Detect Premium veya IBM Trusteer Pinpoint Detect Standard olay verileriyle saptandığı durumlarda, Müşterinin Perakendecilik Uygulamasına özel amaçlı olarak erişen Müşterinin Hak Kazanan Katılımcılarının etkilenen aygıtlarındaki (PC/MAC) kötü amaçlı yazılım bulaşmalarını araştırmayı, düzeltmeyi, engellemeyi ve kaldırmayı amaçlar. Müşterinin, kendi Perakende Uygulaması üzerinde fiili olarak çalışan IBM Trusteer Pinpoint Detect Premium veya IBM Trusteer Pinpoint Standard için geçerli bir aboneliğinin olması gerekir. Müşteri, bu Bulut Hizmetini, sadece Müşterinin Perakende Uygulamasına erişimi olan Hak Kazanan Katılımcılar ile bağlantılı olarak ve yalnızca kötü amaçlı yazılım bulaşan aygıtı (PC/MAC) özel amaçlı olarak araştırıp düzeltmeyi amaçlayan bir araç olarak kullanabilir. IBM Trusteer Rapport for Mitigation for Retail, etkilenen Hak Kazanan Katılımcının aygıtı (PC/MAC) üzerinde fiili olarak çalışmalıdır. Etkilenen Hak Kazanan Katılımcı, son kullanıcı lisans sözleşmesini kabul etmeli, Müşterinin Ticari Faaliyet ve/veya Perakende Uygulamalarında en az bir kez kimliği doğrulanmalı ve Müşterinin yapılandırması ise kullanıcı kimliklerinin derlemini içermelidir. Herhangi bir şüpheye yer vermemek için, bu Bulut Hizmeti, Trusteer Splash'ı kullanma hakkını içermez ve/veya Hesap Sahibi İstemci Yazılımını başka herhangi bir şekilde Müşterinin genel Hak Kazanan Katılımcı topluluğuna yönlendirmez.
- IBM Trusteer Rapport for Mitigation for Business ürünü, kötü amaçlı yazılım bulaşmasının IBM Trusteer Pinpoint Detect Premium veya IBM Trusteer Pinpoint Detect Standard olay verileriyle saptandığı durumlarda, Müşterinin Ticari Faaliyet Uygulamasına özel amaçlı olarak erişen Müşterinin Hak Kazanan Katılımcılarının etkilenen aygıtlarındaki (PC/MAC) kötü amaçlı yazılım bulaşmalarını araştırmayı, düzeltmeyi, engellemeyi ve kaldırmayı amaçlar. Müşterinin, kendi Ticari Faaliyet Uygulaması üzerinde fiili olarak çalışan IBM Trusteer Pinpoint Detect Premium veya IBM Trusteer Pinpoint Standard için geçerli bir aboneliğinin olması gerekir. Müşteri, bu Bulut Hizmetini sadece Müşterinin Ticari Faaliyet Uygulamasına erişimi olan Hak Kazanan Katılımcılar ile bağlantılı olarak ve yalnızca kötü amaçlı yazılım bulaşan aygıtı (PC/MAC) özel amaçlı olarak araştırıp düzeltmeyi amaçlayan bir araç olarak kullanabilir. IBM Trusteer Rapport for Mitigation for Business, etkilenen Hak Kazanan Katılımcının aygıtı (PC/MAC) üzerinde fiili olarak çalışmalıdır. Etkilenen Hak

Kazanan Katılımcı, son kullanıcı lisans sözleşmesini kabul etmeli, Müşterinin Ticari Faaliyet Uygulamasında/Uygulamalarında en az bir kez kimliği doğrulanmalı ve Müşterinin yapılandırması ise kullanıcı kimliklerinin derlemini içermelidir. Herhangi bir şüpheye yer vermemek için, bu Bulut Hizmeti, Trusteer Splash'ı kullanma hakkını içermez ve/veya Hesap Sahibi İstemci Yazılımını başka herhangi bir şekilde Müşterinin genel Hak Kazanan Katılımcı topluluğuna yönlendirmez.

1.5.5 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail ve/veya IBM Trusteer Pinpoint Detect Standard Additional Applications for Business ve/veya IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail ve/veya IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

Hizmet, uygulama başına devreye alma hizmetleri için 200 saate kadar paylaşılan kaynak ve kurulum sonrası uygulama başına güvenlik analizi için 200 saat paylaşılan kaynak içerir. Sürekli hizmetler, uygulama başına yıllık 20 saat devreye alma bakımı ve uygulama başına yıllık 100 saat güvenlik araştırması içerir.

- IBM Trusteer Pinpoint Detect Standard for Retail için ilk Uygulamadan sonraki herhangi bir ek Perakendecilik Uygulaması devreye alımı için IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail yetkisi gereklidir.
- IBM Trusteer Pinpoint Detect Standard for Business için ilk Uygulamadan sonraki herhangi bir ek Ticari Faaliyet Uygulaması devreye alımı için IBM Trusteer Pinpoint Detect Standard Additional Applications for Business yetkisi gereklidir.
- IBM Trusteer Pinpoint Premium for Retail için ilk Uygulamadan sonraki herhangi bir ek Perakendecilik Uygulaması devreye alımı için IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail yetkisi gereklidir.
- IBM Trusteer Pinpoint Premium for Business için ilk Uygulamadan sonraki herhangi bir ek Ticari Faaliyet Uygulaması devreye alımı için IBM Trusteer Pinpoint Detect Premium Additional Applications for Business yetkisi gereklidir.

1.5.6 IBM Trusteer Pinpoint Detect Standard Application ve/veya IBM Trusteer Pinpoint Detect Premium Application

Bu hizmet, Web ve Mobil kanalları için geçerlidir.

Hizmet, uygulama başına devreye alma hizmetleri için 200 saate kadar paylaşılan kaynak ve kurulum sonrası uygulama başına güvenlik analizi için 200 saat paylaşılan kaynak içerir. Sürekli hizmetler, uygulama başına yıllık 20 saat devreye alma bakımı ve uygulama başına yıllık 100 saat güvenlik araştırması içerir.

- IBM Trusteer Pinpoint Detect Standard devreye alımında her Uygulama için IBM Trusteer Pinpoint Detect Standard Application yetkisi gereklidir.
- IBM Trusteer Pinpoint Premium devreye alımında her Uygulama için IBM Trusteer Pinpoint Detect Premium Application yetkisi gereklidir.

1.5.7 IBM Trusteer Pinpoint Detect Standard Redeployment ve/veya IBM Trusteer Pinpoint Detect Premium Redeployment

Kendi çevrimiçi bankacılık Uygulamalarını hizmet süresi içinde yeniden devreye alan ve bunun sonucunda da kendi IBM Trusteer Pinpoint Detect devreye alımlarında değişiklik yapması gereken Müşteriler, IBM Trusteer Pinpoint Detect Redeployment ürününü satın almalıdır.

Yeniden devreye alma, Müşterinin Uygulamanın etki alanını veya anasistem URL adresini değiştirmesi, çevrimiçi Uygulamasını yeni teknolojiye dönüştürmesi, yeni çevrimiçi bankacılık platformuna geçmesi veya mevcut bir Uygulamaya yeni oturum açma akışı eklemesi nedeniyle ortaya çıkabilir.

Müşteri, 6 aylık yeniden devreye alma geçiş dönemi için, halihazırda abone olunan Uygulamaların üzerinde çalışan birebir temelinde ek Uygulamalara hak kazanır.

1.5.8 IBM Trusteer Pinpoint Detect Standard for Retail Premium Support ve/veya IBM Trusteer Pinpoint Detect Standard for Business Premium Support

Pinpoint Detect Standard Bulut Hizmetini satın alan Müşteriler, Premium Destek hizmeti satın alabilirler. Premium Destek hizmetlerinin kapsamı, aşağıda Madde 4'te belirtilmiştir.

1.5.9 IBM Trusteer Digital Content Pack for Retail ve/veya IBM Trusteer Digital Content Pack for Business

IBM Trusteer Digital Content Pack, güvenlik analistlerinin, bir yandan gelişmekte olan tehditlere tepki göstermek için özel amaçlı raporların oluşturulmasını ve değiştirilmesini tam olarak desteklerken diğer yandan yeni sahtekarlık modellerini bütünleştirmelerini sağlar. Çözümün ek ve ayrılmaz bir parçası olarak satın alınabilecek kapsamlı bir dizi kural, içgörü ve ilkeden oluşur. Digital Content Pack, Trusteer'ın dijital sahtekarlığı önleme yetenekleri ile IBM Safer Payments nakitsiz ödeme kanalları arasındaki bütünleştirmeyi daha da artırmaya yardımcı olur. Digital Content Pack, kendi yerleşik kurallarından ve özel iş mantığından yararlanarak, bankaların ve diğer finansal kuruluşların, mevcut sahtekarlığı saptama ve önleme yeteneklerini daha da geliştirmelerini sağlar.

IBM Trusteer Digital Content Pack for Retail, 100 Hak Kazanan Katılımcı paketleri halinde sunulur. IBM Trusteer Digital Content Pack for Business, 10 Hak Kazanan Katılımcı paketleri halinde sunulur.

Digital Content Pack'in Pinpoint Detect ve IBM Safer Payments ile bütünleştirilmesi için danışmanlık hizmetleri ve bunun yanı sıra önemli ölçüde dikkat gerektiren destek hizmetleri gereklidir. Danışmanlık hizmetleri, ayrı bir hizmet bildirimi uyarınca ayrıca satın alınır.

1.5.10 IBM Trusteer New Account Fraud for Retail ve/veya IBM Trusteer New Account Fraud for Business

Pinpoint abonelerine sağlanan bu hizmet, yeni hesap yaratma sürecindeki anormalliklerin saptanması, şüpheli faaliyetlerin işaretlenmesi ve uyarıların erken aşamada oluşturulması amacıyla tasarlanmıştır. Bu hizmet, hesap kurulumu sonrası sahtekârlık ile bağlantılı yeni faaliyetleri belirlemek ve TMA üzerinde mevcut olan raporların kullanılması aracılığıyla yeni bir hesabın bir paravan hesap olabileceğine ya da sahtekârlık için kullanılabileceğine dair erken uyarı sağlamak amacıyla yeni hesapları izler.

IBM Trusteer New Account Fraud for Retail ile IBM Trusteer New Account Fraud for Business, 10 API Çağrısından oluşan paketler halinde satılır.

1.5.11 IBM Trusteer Pinpoint Verify (IBM Trusteer Pinpoint Doğrulama)

Müşteri, bu Bulut Hizmetine abone olmadan önce, IBM Trusteer Pinpoint Detect Premium için güncel bir aboneliğe sahip olmalıdır.

Bu Bulut Hizmeti, bir dijital hizmete erişirken kimliklerini doğrulamak için kullanıcıların ikinci bir kimlik doğrulama faktörü kullanmalarını sağlayan yetenekler sunar. Bu hizmet, korunan uygulamalar için ikinci kimlik doğrulama faktörü sağlamak üzere Pinpoint Detect Premium için kullanılabilir. Kullanıcılara ikinci kimlik doğrulaması faktörünün ne zaman sorulacağına ilişkin karar, korunan uygulama tarafından alınır ve Pinpoint Detect Premium platformu tarafından döndürülen önerileri ya da korunan uygulama tarafından tanımlanan diğer herhangi bir ilkeyi esas alabilir.

1.6 IBM Trusteer Pinpoint Assure

Bu hizmet, şüpheli faaliyetleri işaretler ve yeni hesap oluşturma / kayıt sürecinde uyarılar oluşturur. Bu hizmet, sahtekarlık ile bağlantılı faaliyetleri belirlemek ve TMA üzerinde mevcut olan raporların kullanılması aracılığıyla yeni bir hesabın bir paravan hesap olabileceğine ya da sahtekarlık için kullanılabileceğine dair erken uyarı sağlamak amacıyla hesap kaydı sürecini izler.

IBM Trusteer Pinpoint Assure, 100 Bağlantıdan oluşan paketler halinde sunulur.

1.6.1 IBM Trusteer Pinpoint Assure İçin İsteğe Bağlı Hizmetler

1.6.2 IBM Trusteer Pinpoint Assure Application

Herhangi bir Uygulama üzerinde IBM Trusteer Pinpoint Assure devreye alımı için IBM Trusteer Pinpoint Assure Application yetkisi gerekir.

IBM Trusteer Pinpoint Assure, uygulama bazında satın alınmak üzere sunulur.

1.6.3 IBM Trusteer Mobile Carrier Intelligence ve/veya IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

Müşteri, bu Bulut Hizmetine abone olmadan önce, IBM Trusteer Pinpoint Assure ya da IBM Trusteer Pinpoint Detect için güncel bir aboneliğe sahip olmalıdır.

Bu Bulut Hizmeti, IBM Trusteer Pinpoint Assure ve/veya IBM Trusteer Pinpoint Detect Bulut Hizmetlerine sağlanan cep telefonu numaralarına ilişkin ek bilgiler ve bağlam sağlayarak bu Bulut Hizmetlerini geliştirir ve her oturum için sahtekârlık riskinin belirlenmesine yardımcı olur. Müşteri, numarayla ilişkili taşıyıcı

bilgileri gibi herhangi bir cep telefonu numarasına ilişkin nitelikleri öğrenmek için Bulut Hizmetini sorgulayabilir.

Bu Bulut Hizmeti tarafından cep telefonu numaralarına ilişkin olarak sağlanan veriler ("Mobil İstihbarat"), Müşteri tarafından yalnızca dahili amaçlarla kullanılabilir ve yalnızca otuz (30) gün boyunca saklanabilir. Müşteri, aynı cep telefonu numarasına ilişkin Mobil İstihbaratı elde etmek için Bulut Hizmetini aynı numaraya ilişkin olarak anılan süre sona erdikten sonra yeniden sorgulamalıdır ve önceki sorgulamadan elde edilen Mobil İstihbaratını yeniden kullanamaz. Müşteri, yukarıda izin verilenin dışında, Mobil İstihbaratı kısmen ya da tamamen önbelleğe alamaz, yeniden kullanamaz ya da herhangi bir veri madenciliği ile bağlantılı olarak kullanamaz ya da arşivleyemez.

1.7 IBM Trusteer Remotely Delivered Services (IBM Trusteer Uzaktan Sağlanan Hizmetler)

IBM Trusteer Remotely Delivered Services; Pinpoint Detect Premium ve Pinpoint Assure Bulut Hizmetleri için isteğe bağlı bir eklenti olarak sunulur.

1.7.1 IBM Trusteer Project Management and Consultancy Services (IBM Trusteer Proje Yönetimi ve Danışmanlık Hizmetleri)

Bu hizmet, 200 saate kadar danışmanlık hizmetleri sağlar ve IBM, bu süre içinde aşağıda belirtilenlerden bazılarını ya da tamamını yerine getirecektir:

a. İlk kurulum hizmetleri: Sık sık gerçekleştirilen düzenli toplantılar, proje yönetimi hizmetleri

b. Policy Manager (İlke Yöneticisi): Sürekli destek

Olanak, Taahhüt bazında satın alınmak üzere sunulur.

1.7.2 IBM Trusteer Security Research and Consultancy Services (IBM Trusteer Güvenlik Araştırması ve Danışmanlık Hizmetleri)

Bu danışmanlık hizmeti, tanımlı çözüm ve Premium Destek (varsa) ile birlikte ek hizmetler sağlamak üzere, güvenlik analizi için 200 saate kadar paylaşılan kaynak içerir ve hizmete aşağıdakiler dahildir:

a. Kapsamlı sahtekarlık araştırması: Haftalık toplantılar ve eğitim.

b. Yüksek öncelikli Müşteri bülteni desteği

c. Özelleştirilmiş kurallar için sürekli araştırma ve destek

Olanak, Taahhüt bazında satın alınmak üzere sunulur.

1.7.3 IBM Trusteer Training Services (IBM Trusteer Eğitim Hizmetleri)

Bu danışmanlık hizmeti, tanımlı çözüm ve Premium Destek (varsa) ile birlikte ek hizmetler sağlamak üzere tasarlanmış olup Müşterinin çalışanları için Trusteer portföyüne yönelik eğitim hizmetleri içerir.

Olanak, Taahhüt bazında satın alınmak üzere sunulur.

1.8 IBM Trusteer Mobile Bulut Hizmetleri

1.8.1 IBM Trusteer Mobile SDK for Business ve/veya IBM Trusteer Mobile SDK for Retail

IBM Trusteer Mobile SDK Bulut Hizmetleri, Müşterinin, Bulut Hizmetleri kapsamına abone olduğu Ticari Faaliyet ve/veya Perakende Uygulamalarına güvenli web erişimi, aygıtlara ilişkin risk değerlendirmesi ve kimlik avı dolandırıcılığına karşı koruma sağlamak amacıyla, ek koruma katmanı sağlamak üzere tasarlanmıştır. Güvenli Wi-Fi algılaması, yalnızca Android platformları için sağlanır.

IBM Trusteer Mobile SDK Bulut Hizmetleri sayılanları içerir: mülkiyet hakkına tabi mobil yazılım geliştiricisi kiti ("SDK"); belgeleri, mülkiyet hakkına tabi programlama yazılım kitaplıklarını ve diğer ilgili dosyaları ve öğeleri içeren ve IBM Security Trusteer mobil kitaplığı olarak bilinen bir yazılım paketi; ayrıca Müşterinin, Bulut Hizmetleri kapsamına abone olduğu korunan bağımsız iOS veya Android mobil uygulamalarına eklenebilen veya bunlarla bütünleştirilebilen IBM Security Trusteer Mobile SDK tarafından oluşturulmuş "Çalıştırma Zamanı Bileşeni" veya "Yeniden Dağıtılabilir" mülkiyet hakkına tabi bir kod. ("Müşterinin Bütünleşik Mobil Uygulaması").

IBM Trusteer Mobile SDK for Retail, 100 Hak Kazanan Katılımcıdan oluşan paketler halinde veya 100 İstemci Aygıttan oluşan paketler halinde sunulur; IBM Trusteer Mobile SDK for Business ise 10 Hak Kazanan Katılımcıdan oluşan paketler halinde veya 10 İstemci Aygıttan oluşan paketler halinde sunulur.

Müşteri (Müşterinin sınırsız sayıda yetkili personeli), TMA aracılığıyla, olay verileri raporlama ve risk eğilimi değerlendirmelerini alabilir. Müşteri, Müşterinin Bütünleşik Mobil Uygulamasını yüklemiş Hak

Kazanan Katılımcıların mobil aygıtları ile ilgili verileri ve risk analizini, Müşterinin Bütünleşik Mobil Uygulaması aracılığıyla alabilir. Bu da Müşterinin bu risklere karşılık risk azaltma eylemlerini uygulayan bir dolandırıcılığı önleme ilkesi oluşturmasını sağlar. Bu olanağın amacı doğrultusunda, "mobil aygıtlar", yalnızca desteklenen cep telefonlarını ve tabletleri kapsar, kişisel bilgisayarları veya Apple Mac bilgisayarları kapsamaz.

Müşteri sayılanları gerçekleştirebilir:

a. IBM Trusteer Mobile SDK ürününü, yalnızca Müşterinin Bütünleşik Mobil Uygulamasını geliştirmek için dahili olarak kullanabilir;

b. Yeniden Dağıtılabilir kodu, (yalnızca nesne kodu biçiminde), bütünleşik ve ayrılamaz bir biçimde Müşterinin Bütünleşik Mobil Uygulamasında yerleşik hale getirebilir. Yeniden Dağıtılabilir kodun verilen bu lisans uyarınca değiştirilmiş ya da birleştirilmiş herhangi bir bölümü, bu Hizmet Tanımının koşullarına tabi olacaktır; ve

c. Aşağıdaki koşulların yerine getirilmesi kaydıyla, Yeniden Dağıtılabilir kodu Hak Kazanan Katılımcıların ya da İstemci Aygıt sahibinin taşınabilir aygıtlarına yüklenmek üzere pazarlayabilir ve dağıtabilir:

- Müşteri bu Sözleşmede açıkça izin verildiği durumlar dışında sayılanları gerçekleştiremez: (1) SDK programını kullanamaz, kopyalayamaz, değiştiremez veya dağıtamaz; (2) geçerli yasaların sözleşme ile değiştirilmesine olanak tanımayarak açıkça izin verdiği durumlar dışında SDK programını tersine düzenleyemez, tersine derleyemez, başka bir şekilde çeviremez veya üzerinde tersine mühendislik işlemleri yapamaz; (3) SDK programı için alt lisans veremez, bu programı kiralayamaz veya finansal olarak kiralayamaz; (4) Yeniden Dağıtılabilir kodlarda bulunan telif hakkı veya bildirim dosyalarını çıkaramaz; (5) orijinal Yeniden Dağıtılabilir dosyalarla/modüllerle aynı yol adını kullanamaz; ve (6) IBM'in, IBM'in lisans verenlerinin veya distribütörlerinin adlarını veya markalarını, bunların önceden yazılı iznini almaksızın, Müşterinin Bütünleşik Mobil Uygulamasının pazarlanmasıyla bağlantılı olarak kullanamaz.
- Yeniden Dağıtılabilir Kod, Müşterinin Bütünleşik Mobil Uygulaması içerisinde ayrılması mümkün olmayan bir şekilde bütünleşik olarak kalmalıdır. Yeniden Dağıtılabilir Kodun Yalnızca nesne kodu biçiminde olması ve SDK ve belgelerinde belirtilen bütün yönlendirmelere, yönergelere ve belirtimlere uygun olması gerekir. Müşterinin Bütünleşik Mobil Uygulaması için son kullanıcı lisans sözleşmesinde şu konularda son kullanıcıya bildirimde bulunulacaktır: Yeniden Dağıtılabilir Kodlar i) Müşterinin Bütünleşik Mobil Uygulamasının etkinleştirilmesi dışında herhangi bir amaçla kullanılamayacaktır, ii) kopyalanamayacaktır (yedekleme amaçları hariç olmak üzere), iii) üçüncü kişilere dağıtılamayacak ya da devredilemeyecektir ya da iv) yasaların sözleşme ile değiştirilmesine olanak sağlamaksızın açıkça izin verdiği durumlar hariç olmak üzere, tersine derlemeye, tersine mühendisliğe ya da diğer herhangi bir şekilde çeviriye tabi tutulamayacaktır. Ayrıca, Müşterinin lisans sözleşmesinin IBM açısından en az bu Sözleşmenin koşulları kadar koruyucu olması gerekir.
- SDK, yalnızca Müşterinin belirlenen mobil test aygıtlarında dahili geliştirme ve birim testi gerçekleştirme amaçlarıyla devreye alınabilir. Müşteriye, üretim iş yüklerini işlemek, üretim iş yüklerinin benzetimini yapmak ya da herhangi bir kodun, uygulamanın veya sistemin ölçeklenebilirliğini test etmek amacıyla SDK programını kullanma yetkisi verilmez. Müşteri, SDK programının olanağının hiçbir parçasını başka hiçbir amaçla kullanamaz.

Müşterinin Bütünleşik Mobil Uygulamasının geliştirilmesinden, test edilmesinden ve desteklenmesinden Müşteri tek başına sorumludur. Müşterinin Bütünleşik Mobil Uygulamasına ilişkin tüm teknik destekten ve Yeniden Dağıtılabilir Kodlarda, işbu belgede izin verilen, yapılan herhangi bir değişiklikten Müşteri sorumludur.

Müşteri, yalnızca Müşterinin, Bulut Hizmetlerinin kullanmasını desteklemek amacıyla, Yeniden Dağıtılabilir Kodları ve IBM Security Mobile SDK'yı kurma ve kullanma yetkisine sahiptir.

IBM, IBM Security Mobile SDK kitine dahil olan mobil araçlar kullanılarak oluşturulan herhangi bir uygulamanın ya da çıktının herhangi bir mobil işletim sistemi platformu ya da mobil aygıt ile işlevlerini yerine getireceğini, birlikte çalışacağını ya da bunlarla uyumlu olacağını garanti etmez.

Kaynak Bileşenler ve Örnek Malzemeler – IBM Trusteer Mobile SDK, kaynak kodundaki bazı bileşenleri ("Kaynak Bileşenler") ve Örnek Malzemeler olarak tanımlanan diğer malzemeleri içerebilir. Müşteri, Kaynak Bileşenleri ve Örnek Malzemeleri yalnızca dahili kullanım amacıyla kopyalayabilir ve değiştirebilir;

ancak bu tür bir kullanımın bu Sözleşme kapsamındaki lisans haklarının sınırları içinde olması gerekir. Ayrıca Müşteri, Kaynak Bileşenler veya Örnek Malzemeler içinde yer alan herhangi bir telif hakkı bilgisini veya bildirimini değiştiremez veya silemez. IBM, Kaynak Bileşenlerini ve Örnek Malzemeleri herhangi bir destek yükümlülüğü olmaksızın ve "OLDUĞU GİBİ" esasıyla sağlar. Kaynak Bileşenler veya Örnek Malzemeler, yalnızca CIMA içine Yerleştirilebilir öğelerin nasıl uygulanacağına örnek olarak sağlanır. Kaynak Bileşenler veya Örnek Malzemeler, Müşterinin geliştirme ortamıyla uyumlu olmayabilir ve bunların Müşterinin CIMA'sı içine Yerleştirilebilir öğelerinin test edilmesinden ve uygulanmasından Müşteri tek başına sorumludur.

2. İçeriğin ve Verilerin Korunması

Veri İşleme ve Veri Koruma Veri sayfasında (Veri Sayfası), işlenmesi mümkün olan İçeriğin türü, ilgili işleme etkinlikleri, veri koruma özellikleri ve İçeriğin saklanmasına ve iadesine ilişkin Bulut Hizmetine özgü bilgiler sağlanır. Bulut Hizmetinin ve varsa, veri koruma özelliklerinin kullanımına ilişkin herhangi bir ayrıntı ya da açıklama ve koşullar, Müşterinin sorumlulukları da dahil olmak üzere bu maddede belirtilmiştir. Müşteri tarafından seçilen seçeneklere bağlı olarak, Müşterinin Bulut Hizmetini kullanımı için geçerli olabilecek birden fazla Veri Sayfası mevcut olabilir. Veri Sayfası, yalnızca İngilizce dilinde kullanılabilir ve yerel dilde mevcut değildir. Taraflar, yerel kanunların ya da teamüllerin uygulamaları dikkate alınmaksızın, İngilizce dilini anladıklarını ve bu dilin, Bulut Hizmetlerinin satın alınmasına ve kullanımına ilişkin uygun bir dil olduğunu kabul ederler. Aşağıdaki Veri Sayfası/Sayfaları, Bulut Hizmeti ve bu kapsamda mevcut olan hizmetler için geçerlidir. Müşteri, i) IBM'in yalnızca kendi takdirinde olmak üzere Veri Sayfasını/Sayfalarını muhtelif zamanlarda değiştirebileceğini ve ii) anılan değişikliklerin önceki sürümlerin yerini alacağını kabul eder. Veri Sayfasında/Sayfalarında yapılacak herhangi bir değişikliğin amacı, i) mevcut taahhütlerin iyileştirilmesi ya da daha açık hale getirilmesi, ii) benimsenmiş güncel standartlara ve geçerli yasalara uyumluluğun sürdürülmesi ya da iii) ek taahhütler sağlanması olacaktır. Veri Sayfasında/Sayfalarında yapılacak hiçbir değişiklik, bir Bulut Hizmetinin veri korumasını esaslı olarak azaltmayacaktır.

Geçerli Veri Sayfasının/Sayfalarının Bağlantısı/Bağlantıları:

IBM Trusteer Mobile SDK

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

IBM Trusteer Mobile Secure Browser

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

IBM Trusteer Pinpoint Assure

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

IBM Trusteer Pinpoint Criminal Detect (IBM Trusteer Pinpoint Ceza Tespit)

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

IBM Trusteer Pinpoint Detect

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

IBM Trusteer Pinpoint Malware Detection

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

IBM Trusteer Rapport

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

IBM Trusteer Pinpoint Verify (IBM Trusteer Pinpoint Doğrulama)

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

(IBM Cloud Identity Verify veri sayfası, IBM Trusteer Pinpoint Verify ürününü yansıtır)

Müşteri, bir Bulut Hizmeti için mevcut veri koruma özelliklerini sipariş etmek, etkinleştirmek ya da kullanmak üzere gerekli işlemleri gerçekleştirmekten sorumludur ve İçeriğe ilişkin herhangi bir veri koruma kanununun gereksinimlerinin ya da diğer hukuki gereksinimlerin yerine getirilmesi de dahil olmak üzere anılan işlemleri gerçekleştirmemesi durumunda Bulut Hizmetlerinin kullanımına ilişkin sorumluluğu kabul eder.

İçeriğe dahil olan kişisel veriler için Avrupa Genel Veri Koruma Yönetmeliği'nin (EU/2016/679) (GVKY/GDPR) geçerli olması halinde ve geçerli olduğu ölçüde, IBM'in http://ibm.com/dpa adresinde yer alan Veri İşleme Ek Sözleşmesi ve Veri İşleme Ek Sözleşmesi Ek(ler)i geçerli olur ve atıf yoluyla Sözleşmeye dahil edilir. Bu Bulut Hizmeti için geçerli olan Veri Sayfaları, Veri İşleme Ek Sözleşmesi Eki olarak geçerli olacaktır. Veri İşleme Ek Sözleşmesi uygulanıyorsa, IBM'in değişiklikleri Alt İşleyenlere bildirme yükümlülüğü ve Müşterinin söz konusu değişikliklere itiraz etme hakkı Veri İşleme Ek Sözleşmesinde belirtildiği şekilde uygulanacaktır.

2.1 Son Kullanıcı Lisans Sözleşmesi ve İlgili Kişilerin Verilerinin İşlenmesine Dair Gerekçe

IBM Trusteer Rapport Bulut Hizmetleri (Pinpoint Bulut Hizmetleriyle bağlantılı olarak devreye alındığında Rapport Remediation veya Rapport for Mitigation dahil) için:

Müşteri, aksi kararlaştırılmadıkça ve Müşteri tarafından bağımsız olarak belirlenen işleme gerekçesi uyarınca, IBM'in Bulut Hizmetlerini sağlaması için gerekli olan bilgileri elde etmesine ve işlemesine olanak sağlamak amacıyla https://www.trusteer.com/support/end-user-license-agreement adresinde bulunan Son Kullanıcı Lisans Sözleşmesini sağlaması için IBM'e yetki verir.

2.2 Veri Kullanımı

IBM, Müşterinin Bulut Hizmetinden kaynaklanan ve Müşterinin İçeriğine (İçgörüler) özgü olan veya başka bir şekilde Müşteriyi tanımlayan sonuçları kullanmayacak veya açıklamayacaktır. Bununla birlikte IBM, herhangi bir kişisel verinin ek bilgiler kullanmadan belirli bir kişiyle ilişkilendirilmemesini sağlamak için kişisel tanıtıcıların kaldırılmasına tabi olarak, İçeriği ve Bulut Hizmetinin sağlanması sırasında İçerikten kaynaklanan diğer bilgileri (İçgörüler hariç) kullanabilir. IBM, bu verileri yalnızca araştırma, testler ve olanak geliştirmesi amaçlarıyla kullanacaktır.

2.3 Verilerin İşlenmesi ve Depolanması

2.3.1 Ek İşleme Konumu Bilgileri

Trusteer Pinpoint Verify hizmetleri için tüm barındırma ve işleme lokasyonları ilgili Veri Sayfasında belirtilmiştir.

IBM, Almanya'da bulunan veri merkezi aracılığıyla sağlanan tüm diğer hizmetler için, Kişisel Verilerin işlenmesini sözleşmeyi imzalayan IBM kuruluşunun ülkesiyle ve şu ülkelerle sınırlayacaktır: Almanya, İsrail, İrlanda, Hollanda ve IBM'in Üçüncü Kişi Alt İşleyenleri için geçerli veri sayfasında belirtilen herhangi bir ek ülke.

IBM, Japonya'da bulunan veri merkezi aracılığıyla sağlanan tüm diğer hizmetler için, Kişisel Verilerin işlenmesini sözleşmeyi imzalayan IBM kuruluşunun ülkesiyle ve şu ülkelerle sınırlayacaktır: Japonya, İsrail, İrlanda ve IBM'in Üçüncü Kişi Alt İşleyenleri için geçerli veri sayfasında belirtilen herhangi bir ek ülke.

IBM, ABD'de bulunan veri merkezi aracılığıyla sağlanan tüm diğer hizmetler için, Kişisel Verilerin işlenmesini sözleşmeyi imzalayan IBM kuruluşunun ülkesiyle ve şu ülkelerle sınırlayacaktır: ABD, İsrail, İrlanda, Singapur, Avustralya ve IBM'in Üçüncü Kişi Alt İşleyenleri için geçerli veri sayfasında belirtilen herhangi bir ek ülke.

IBM Trusteer destek ve hesap bakımı hizmetleri de, ilgili IBM personeli, Müşterinin konumu ve verilerin barındırıldığı veri merkezi temelinde ihtiyaç oldukça sağlanabilir.

2.3.2 Hesap Sahibinin Verileri

Hesap Sahibinin verileri, Hesap Sahibinin Hesap Sahibi İstemci Yazılımını ilk olarak kurduğu bölgede işlenecektir. Bu, Hesap Sahibinin içeriğinin, hem içeriğin kaynağı olan bölgede hem de Müşteri ile kararlaştırılan bölgede işlenebileceği anlamına gelir.

2.3.3 Bütünleşik Çözümler

Netleştirmek amacıyla, Trusteer Fraud Protection bütünleşik bir çözüm olduğundan, Müşteri bu Bulut Hizmetlerinden birini sona erdirirse, IBM, Müşteriye geri kalan Bulut Hizmetlerini sağlamak amacıyla bu Hizmet Tanımı uyarınca Müşteri verilerini saklayabilir.

3. Hizmet Seviyesi Sözleşmesi

IBM, Yetki Belgesinde belirtildiği şekilde Bulut Hizmeti için aşağıda belirtilen kullanılabilirlik hizmet seviyesi sözleşmesini sağlar. Hizmet Seviyesi Sözleşmesi bir garanti değildir. Hizmet Seviyesi Sözleşmesi yalnızca Müşteriye sağlanır ve yalnızca üretim ortamlarındaki kullanımlar için geçerli olur.

3.1 Kullanılabilirlik Alacakları

Müşteri, Bulut Hizmetinin kullanımını etkileyen bir Olaydan ilk kez haberdar olmasını izleyen yirmi dört (24) saat içinde IBM teknik destek yardım masasına Önem Derecesi 1 olan bir destek bildirim kaydını kaydettirmelidir. Müşteri, her türlü sorun tanılama ve çözümleme sürecinde makul sınırlar içinde IBM'e yardımcı olmalıdır.

Hizmet Seviyesi Sözleşmesinin koşullarının karşılanamaması halinde, sözleşmenin yürürlükte olduğu ayın sona ermesinden itibaren üç iş günü içinde bir destek sorun kaydı talebinin gönderilmesi gerekir. Geçerli Hizmet Seviyesi Sözleşmesi talebine ilişkin telafi ücreti, Bulut Hizmetinin sağlanmadığı üretim sistemi işlemleri boyunca geçen süre ("Kapalı Kalma Süresi") esas alınarak Bulut Hizmeti için gelecekte Müşteri tarafından düzenlenecek bir faturaya alacak olarak kaydedilecektir. Kapalı Kalma Süresi, Müşterinin kapalı kalma olayını raporladığı zamandan itibaren Bulut Hizmetinin yeniden çalışmaya başladığı zamana kadar geçen süre esas alınarak ölçülür ve bu süreye şunlar dahil değildir: planlı ya da önceden duyurulmuş bir bakım için yapılan kesintiler, IBM'in kontrolü dışında ortaya çıkan nedenler, Müşteri ya da üçüncü kişi içeriğinin veya teknolojisinin, tasarımlarının ya da yönergelerinin yarattığı sorunlar, desteklenmeyen sistem yapılandırmaları ve platformları ya da diğer Müşteri hataları ya da Müşteriden kaynaklanan güvenlik sorunları veya Müşterinin güvenlik testleri. IBM, aşağıdaki tabloda gösterildiği şekilde, Sözleşmenin yürürlükte olduğu her ay boyunca Bulut Hizmetinin kümülatif kullanılabilirliği doğrultusunda geçerli olan en yüksek telafi ücretini uygulayacaktır. Sözleşmenin yürürlükte olduğu herhangi bir aya ilişkin toplam telafi ücreti, Bulut Hizmetinin yıllık ücretinin on ikide birinin (1/12) yüzde onundan (%10) fazla olmayacaktır.

3.2 Hizmet Seviyeleri

Bir sözleşmenin yürürlükte olduğu ay boyunca Bulut Hizmetinin kullanılabilirliği

Bir sözleşmenin yürürlükte olduğu ay boyunca kullanılabilirlik	Telafi ücreti (Talebe konu olan sözleşmenin yürürlükte olduğu ay için aylık abonelik ücretinin* yüzdesi)
<%99,9	%2
< %99,0	%5
< %95,0	%10

* Aylık abonelik ücreti, Bulut Hizmetinin bir IBM Çözüm Ortağından edinilmiş olması durumunda, talebe konu olan sözleşmenin yürürlükte olduğu ayda geçerli olan Bulut Hizmeti güncel liste fiyatına %50 oranında indirim uygulanarak hesaplanır. IBM, geri ödemeyi doğrudan Müşteriye yapacaktır.

Hizmet Seviyeleri ve ilişkili Telafi alacakları, her Bulut Hizmeti ve her Müşteri Uygulaması için ayrı ayrı ölçülür.

Uygulama yetkilerini esas alan Bulut Hizmetleri için SLA alacakları hesaplanırken, Kullanılabilirlik, aşağıdaki yönergelere dayalı olarak hesaplanacaktır:

- Her Uygulamanın, sözleşmenin yürürlükte olduğu ay boyunca oturumların hacmine ilişkin olarak sayılmış olan sayı esas alınarak atanmış bir ağırlıklı payı olacaktır.
- Her Uygulama için her Bulut Hizmetine ilişkin kapalı kalma süresi, sözleşmenin yürürlükte olduğu ay için ayrıca toplanacaktır.

Aşağıda, bir aylık etkinlik ve onun ilişkili ağırlığının hesaplanmasına bir örnek yer alır. Bu örnek yalnızca bilgilendirme amacıyla verilmektedir:

Perakende Uygulamaları	Sözleşmenin yürürlükte olduğu belirli bir aydaki toplam oturum sayısı üzerinden pay	Sözleşmenin yürürlükte olduğu ay boyunca Toplam Kapalı Kalma Süresi	Kapalı Kalma Süresi İçin Ağırlıklı Dakika Sayısı
Perakende Uygulaması A	%40	300 dakika	40% x. 300 dakika = 120 dakika
Perakende Uygulaması B	%20	250 dakika	20% x 250 dakika = 50 dakika
Perakende Uygulaması C	%40	150 dakika	40% x 150 dakika = 60
			Kapalı Kalma Süresi için toplam ağırlıklı dakika = 230

Kullanılabilirlik, yüzdesel olarak ifade edilir ve aşağıda belirtilen şekilde hesaplanır: sözleşmenin yürürlükte olduğu ay içindeki toplam dakika sayısından sözleşmenin yürürlükte olduğu ay içindeki toplam Kapalı Kalma Süresi dakikalarının sayısı çıkartılır ve sonuç sözleşmenin yürürlükte olduğu ay içindeki toplam dakika sayısına bölünür. Yukarıdaki ağırlıklandırma örneğine dayalı olarak yapılan örnek hesaplama aşağıda verilmektedir:

$$\frac{\text{30 günlük sözleşmenin yürürlükte olduğu ayda toplam 43.200 dakika - 230 dakika ağırlıklı kapalı kalma süresi = 42.970 dakika}}{\text{43.200 toplam dakika}} = \text{Sözleşmenin yürürlükte olduğu ay içinde \%99,4 oranında kullanılabilirlik için \%2 oranında kullanılabilirlik alacağı}$$

4. Teknik Destek

Bulut Hizmetlerine ilişkin Teknik Destek, Bulut Hizmetlerini kullanmalarına yardımcı olmak için, Müşteriye ve onun Hak Kazanan Katılımcılarına sağlanır.

Standart Destek, tüm olanakların aboneliğine dahil edilir. Trusteer Rapport eklentisi olan Trusteer Rapport Mandatory Service, temel Trusteer Rapport aboneliği için Premium Destek ön koşuluna sahiptir.

IBM Trusteer Mobile SDK Cloud Services ile **IBM Trusteer Rapport Mandatory Service Cloud Services**, **IBM Trusteer New Account Fraud**, **IBM Trusteer Pinpoint Assure**, **IBM Trusteer Digital Content Pack** ve **IBM Trusteer Mobile Carrier Intelligence** hariç olmak üzere her Bulut Hizmeti için ek ücret karşılığında bir Premium Destek aboneliği mevcuttur. IBM satış temsilcisiyle ya da IBM Çözüm Ortağıyla iletişim kurulabilir.

Standart Destek:

- Yerel saatle 08.00-17.00 arası destek
- Müşteriler ve onların Hak Kazanan Katılımcıları, IBM'in https://www.ibm.com/software/support/saas_support_guide.html adresinde bulunan hizmet olarak sunulan yazılım desteği kılavuzunda ayrıntılı olarak açıklandığı şekilde destek bildirim kayıtlarını elektronik ortamda gönderebilirler.
- Müşteriler; bildirimler, belgeler, vaka raporları ve sık sorulan sorular için http://www-01.ibm.com/software/security/trusteer adresindeki Müşteri Destek Portalına erişebilirler.

Premium Destek:

- Tüm önem dereceleri için haftanın 7 günü, günde 24 saat destek
- Müşteriler, desteğe doğrudan telefonla ve geri arama isteğiyle ulaşabilirler.
- Müşteriler ve Hak Kazanan Katılımcıları, Hizmet Olarak Sunulan Yazılım Desteği El Kitabında ayrıntılı olarak açıklandığı gibi, destek bildirim formlarını elektronik ortamda gönderebilir.

- Müşteriler; bildirimler, belgeler, vaka raporları ve sık sorulan sorular için http://www.ibm.com/software/security/trusteer/support/ adresindeki Müşteri Destek Portalına erişebilirler.
- Destek seçenekleri ve ayrıntılı bilgi için IBM'in https://www.ibm.com/software/support/saas_support_guide.html adresinde yer alan hizmet olarak sunulan yazılım destek kılavuzuna erişilebilir.

5. Yetki ve Faturalandırma Bilgileri

5.1 Ücret Ölçüleri

Bulut Hizmeti İşlem Belgesinde belirtilen ücret ölçüsünde sağlanır:

- Taahhüt, hizmetlerin edinilebileceği bir ölçü birimidir. Taahhüt, Bulut Hizmeti ile bağlantılı profesyonel hizmetlerden ve/veya eğitim hizmetlerinden oluşur. Her Taahhüdün kapsamaya yetecek sayıda yetki edinilmelidir.
- Hak Kazanan Katılımcı, Bulut Hizmetinin edinilebileceği bir ölçü birimidir. Bulut Hizmeti tarafından yönetilen ya da izlenen herhangi bir hizmet teslimatı programına katılmaya hak kazanan her özel ya da tüzel kişi bir Hak Kazanan Katılımcıdır. Müşterinin Yetki Belgesinde veya İşlem Belgesinde belirtilen ölçüm süresi boyunca Bulut Hizmeti içinde yönetilen ya da izlenen tüm Hak Kazanan Katılımcıları kapsamaya yetecek sayıda yetkinin edinilmelidir.

  Bulut Hizmeti tarafından yönetilen her hizmet sağlama programı, ayrı ayrı analiz edilip birbirine eklenir. Birden fazla hizmet sağlama programı için hak kazanan kişi veya kuruluşlar için ayrı yetkiler gerekir.

  Bir Hak Kazanan Katılımcı, bu Bulut Hizmetlerinin yetkilendirme amaçları uyarınca, Müşterinin bir Ticari Faaliyet ya da Perakende Uygulamasına ilişkin özgün oturum açma kullanıcı bilgilerine sahip bir Müşteri son kullanıcısıdır.
- İstemci Aygıt, Bulut Hizmetinin edinilebileceği bir ölçü birimidir. Bir İstemci Aygıt, tipik olarak sunucu adıyla anılan bir başka bilgisayar sisteminden bir dizi komutun, prosedürün veya uygulamanın yürütülmesini talep eden veya bunları yürütmek üzere alan ya da sunucu tarafından bir başka şekilde yönetilen, tek kullanıcısı bulunan bir bilgi işlem aygıtı veya özel amaçlı algılayıcı veya telemetre aygıtıdır. Birden fazla İstemci Aygıt, ortak bir sunucuya erişimi paylaşabilir. Bir İstemci Aygıt, belirli ölçüde işlem yeteneğine sahip olabilir veya bir kullanıcının iş yapması için programlanabilir. Müşteri, Yetki Belgesinde ya da İşlem Belgesinde belirtilen ölçüm süresi boyunca Bulut Hizmetini çalıştıran, buna veri sağlayan, bunun sağladığı hizmetleri kullanan veya bir başka şekilde buna erişen her İstemci Aygıt için yetkiler edinmelidir.
- Uygulama, Bulut Hizmetinin edinilebileceği bir ölçü birimidir. Bir Uygulama, özgün bir şekilde adlandırılmış bir yazılım programıdır. Müşterinin Yetki Belgesinde veya İşlem Belgesinde belirtilen ölçüm süresi içerisinde erişilmesine ve kullanılmasına izin verilen her Uygulama için yeterli sayıda yetki edinmesi zorunludur.

  Bu Bulut Hizmetinin amaçları doğrultusunda bir Uygulama, Müşterinin tek bir Ticari Faaliyet veya Perakende Uygulamasıdır.
- API Çağrısı, Bulut Hizmetinin edinilebileceği bir ölçü birimidir. Bir Uygulama Programı Arabirimi (API) Çağrısı, Bulut Hizmetinin bir programlanabilir arabirimi aracılığıyla başlatılmasıdır. Müşterinin Yetki Belgesinde veya İşlem Belgesinde belirtilen ölçüm süresi boyunca API Çağrılarının toplam sayısını kapsamaya yetecek şekilde en yakın onluk basamağa yuvarlanmış olarak yeterli sayıda yetki edinilmelidir.
- Bağlantı, Bulut Hizmetinin edinilebileceği bir ölçü birimidir. Bir Bağlantı, Bulut Hizmeti ile ilgili olan bir veritabanı, uygulama, sunucu ya da başka bir aygıt türüne ilişkin bir bağlantı (link) ya da ilişkidir. Müşteri, Yetki Belgesinde veya İşlem Belgesinde belirtilen ölçüm süresi boyunca Bulut Hizmeti ile ilişkilendirilmiş veya ilişkilendirilecek olan toplam Bağlantı sayısını kapsamaya yetecek sayıda yetki edinmelidir.

  Bir Bağlantı, bu Bulut Hizmetinin amaçları doğrultusunda, Müşterinin Uygulamasındaki bir oturum veya akıştır.

5.2 Limit Aşımı Ücretleri

Ölçüm süresi boyunca Bulut Hizmetinin fiili kullanımı Yetki Belgesinde belirtilen yetkiyi aşarsa, limit aşımı ücreti için, limit aşımını izleyen ayda İşlem Belgesinde belirtilen şekilde ücret üzerinden Müşteriye fatura düzenlenecektir.

5.3 Faturalama Sıklığı

IBM, vade bitiminde ödenecek olan limit aşım ücretleri ve kullanım tipi ücretleri dışında, seçili faturalama sıklığına bağlı olarak, ödenmesi gereken ücretler için faturalama sıklığı süresinin başında Müşteriye fatura düzenleyecektir.

6. Süre ve Yenileme Seçenekleri

Bulut Hizmetinin süresi, Yetki Belgesinde belgelendiği şekilde, Bulut Hizmetine erişiminin etkinleştirildiğinin IBM tarafından Müşteriye bildirildiği tarihte başlar. Yetki Belgesinde Bulut Hizmetinin, otomatik olarak mı yenileneceği, sürekli kullanım esasına göre mi işleneceği yoksa kullanım süresinin sonunda sona mı ereceği belirtilir.

Otomatik yenileme için: Müşteri, sürenin sona erme tarihinden en az doksan (90) gün önce yazılı olarak olanağın kullanımını yenilemeyeceğini bildirmediği sürece, Bulut Hizmeti Yetki Belgesinde belirtilen süreye uygun olarak kendiliğinden yenilenir. Yenilemeler, fiyat teklifinde belirtilen yıllık fiyat artışına tabidir. Otomatik yenilemenin, IBM'in Bulut Hizmetinin geri çekileceğine dair bildiriminden sonra olması durumunda, yenileme süresi, hangisi önce ise, mevcut yenileme süresinde veya duyurulan geri çekme tarihinde sona erecektir.

Sürekli kullanım için: Müşteri, doksan (90) gün önce yazılı olarak olanağın kullanımının sona erdirileceğine ilişkin bildirimi gönderinceye kadar, Bulut Hizmeti aylık kullanım esasına göre kullanılmaya devam edecektir. Bulut Hizmeti, doksan (90) günlük bu bildirim süresinin sona ermesini izleyen takvim ayının sonuna kadar kullanılmaya devam edilebilir.

7. Ek Koşullar

7.1 Genel

Müşteri, IBM'in, basın veya pazarlama iletişimlerinde Müşteriyi Bulut Hizmetlerinin bir abonesi olarak kamuya açık bir şekilde referans verebileceğini kabul eder.

Müşteri, Bulut Hizmetlerini tek başına veya diğer ürünlerle veya hizmetlerle birlikte, aşağıda belirtilen yüksek riskli faaliyetlerden herhangi birini desteklemek amacıyla kullanamaz: Nükleer tesisler, toplu taşıma sistemleri, hava trafik kontrol sistemleri, otomotiv kontrol sistemleri, silah sistemleri, hava aracı navigasyonu veya iletişimi veya Bulut Hizmeti hatasının ölüm veya ciddi bir bedensel yaralanma tehdidi doğurabileceği diğer herhangi bir etkinliğin tasarlanması, inşası, denetimi veya bakımı.

7.2 Etkinleştirme Yazılımı

Bulut Hizmeti için, Bulut Hizmetinin kullanımını kolaylaştırmak amacıyla Müşterinin kendi sistemlerine karşıdan yüklediği etkinleştirme yazılımının kullanılması gerekir. Müşteri, etkinleştirme yazılımını yalnızca Bulut Hizmetinin kullanımıyla bağlantılı olarak kullanabilir. Etkinleştirme yazılımı "OLDUĞU GİBİ" esasıyla sağlanır.

7.3 IBM Trusteer Fraud Protection'ın Devreye Alınması

Müşterinin temel aboneliği, abone olduğu her Uygulama için; bir kerelik ilk çalıştırma, yapılandırma, Splash Template, test ve eğitim dahil olmak üzere IBM Trusteer bulutu üzerinde gereken kurulum ve ilk devreye alma etkinliklerini kapsar.

Devreye alma etkinlikleri, Müşterinin Uygulamalarında veya sistemlerinde gereken uygulama etkinliklerini içermez.

Bulut Hizmetlerinin uygulama aşaması, ilgili devreye alma kılavuzlarında ayrıntılarıyla belirtilen zaman çerçevelerinde uygulanacaktır.

Bu uygulama aşamalarının belirlenen zaman çerçevesi içinde tamamlanması, Müşteri yönetiminin ve personelinin bu çalışmaya bağlılıklarına ve tam olarak katılmalarına bağlıdır. Müşteri, gerekli bilgileri zamanında sağlayacaktır. IBM'in performansı, Müşterinin bilgileri zamanında sağladığı ve kararları

zamanında aldığı esasına dayanır ve herhangi bir gecikme, ek maliyetlere ve/veya bu uygulama hizmetlerinin tamamlanmasının gecikmesine neden olabilir.

Müşterinin abone olduğu her Uygulama için, Müşterinin temel aboneliği; bir kerelik ilk çalıştırma, yapılandırma, Splash Template, test ve eğitim dahil olmak üzere IBM Trusteer bulutu üzerinde gereken kurulum ve ilk devreye alma etkinliklerini kapsar.

Müşterinin temel aboneliği, Müşterinin bu tür bir uygulamasında bulunan ve ilk devreye alımda IBM tarafından önerildiği şekilde etiketlenecek olan sayfalar için desteği ve testi kapsar. IBM şu durumlardan sorumlu değildir: (i) kısmi devreye alma, (ii) Müşterinin, Bulut Hizmetlerini IBM'in önerdiği şekilde devreye almamayı seçmesi, veya (iii) Müşterinin, devreye alma, kurulum ve test etkinliklerini kendisinin yapmayı seçmesi. (IV) Müşteri tarafından yetersiz bilgi sağlanmasından kaynaklanan kısmi devreye alma veya koruma. İlk kurulumdan sonraki devreye alma etkinlikleri dahil olmak üzere ek hizmetler için ayrı bir sözleşme kapsamında ek bir ücret karşılığında sözleşme yapılabilir.

Kabul eden:

Müşteri Şirketinin Ticari Unvanı adına (“**Müşteri**”)

İmza_____

Yetkili imza

Unvan:

İsim (el yazısı veya daktiloyla):

Tarih:

Müşteri Numarası:

Müşteri Adresi:

Kabul eden:

<İlgili IBM Şirketinin Ticarı Unvanı adına> (“**IBM**”)

İmza_____

Yetkili imza

Unvan:

İsim (el yazısı veya daktiloyla):

Tarih:

Sözleşme Numarası:

IBM Adresi: