IBM Trusteer Fraud Protection

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:

Rapport Bulut Hizmetleri:

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

Pinpoint Bulut Hizmetleri:

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

- IBM Trusteer Pinpoint Carbon Copy for Retail
- IBM Trusteer Pinpoint Carbon Copy for Retail Premium Support
- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Rapport Remediation for Retail Premium Support
- IBM Trusteer Pinpoint Criminal Detection II for Business
- IBM Trusteer Pinpoint Criminal Detection II for Retail
- IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Advanced Edition
- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Rapport Remediation for Business Premium Support
- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail
- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Business
- IBM Trusteer Pinpoint Malware Detection Redeployment
- IBM Trusteer Pinpoint Criminal Detection Redeployment
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Rapport for Mitigation for Retail
- IBM Trusteer Rapport for Mitigation for Retail Premium Support
- IBM Trusteer Rapport for Mitigation for Business
- IBM Trusteer Rapport for Mitigation for Business Premium Support
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Retail (Perakende için erişim yönetimi bütünleştirmesiyle birlikte)
- IBM Trusteer Pinpoint Detect Standard with access management integration for Business (Ticari Faaliyet için erişim yönetimi bütünleştirmesiyle birlikte)
- IBM Trusteer Pinpoint Detect Premium with access management integration for Retail (Perakende için erişim yönetimi bütünleştirmesiyle birlikte)
- IBM Trusteer Pinpoint Detect Premium with access management integration for Business (Ticari Faaliyet için erişim yönetimi bütünleştirmesiyle birlikte)
- IBM Trusteer Pinpoint Detect Standard Redeployment
- IBM Trusteer Pinpoint Detect Premium Redeployment
- IBM Trusteer Pinpoint Detect Standard For Retail Premium Support
- IBM Trusteer Pinpoint Detect Standard For Business Premium Support

Mobile Bulut Hizmetleri:

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

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

1.1 Ticari Faaliyet ve Perakende Bulut Hizmetleri

IBM Trusteer Bulut Hizmetleri, belirli türde Uygulamalarla birlikte kullanılmak üzere sağlanır. 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 for Business
- IBM Trusteer Rapport II for Business
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition
- IBM Trusteer Pinpoint Criminal Detection II for Business
- IBM Trusteer Pinpoint Criminal Detection for Business
- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile Browser for Business
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Pinpoint Detect Standard with access management integration for Business (Ticari Faaliyet için erişim yönetimi bütünleştirmesiyle birlikte)
- IBM Trusteer Pinpoint Detect Premium with access management integration for Business (Ticari Faaliyet için erişim yönetimi bütünleştirmesiyle birlikte)

1.1.2 Perakende Bulut Hizmetleri

- IBM Trusteer Rapport for Retail
- IBM Trusteer Rapport II for Retail
- IBM Trusteer Pinpoint Criminal Detection for Retail
- IBM Trusteer Pinpoint Criminal Detection II for Retail
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Standard Edition
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Retail (Perakende için erişim yönetimi bütünleştirmesiyle birlikte)
- IBM Trusteer Pinpoint Detect Premium with access management integration for Retail (Perakende için erişim yönetimi bütünleştirmesiyle birlikte)

- IBM Trusteer Mobile SDK for Retail
- IBM Trusteer Mobile Browser for Retail

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 İçin Ek Bulut Hizmetleri

a. IBM Trusteer Rapport for Business için sunulan 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

b. IBM Trusteer Rapport for Retail için sunulan 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 for Business veya IBM Trusteer Rapport for Retail aboneliği, bu maddede sıralanan ilgili ek Bulut Hizmetlerine yönelik bir ön koşul niteliğindedir.

1.1.4 IBM Trusteer Pinpoint Malware Detection ve/veya IBM Trusteer Pinpoint Malware Detection II İçin Ek Bulut Hizmetleri

a. IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition veya IBM Trusteer Pinpoint Malware Detection for Business Standard Edition veya IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business veya IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business için sunulan ek Bulut Hizmetleri:
   - IBM Trusteer Pinpoint Carbon Copy for Business
   - IBM Trusteer Rapport Remediation for Business
   - IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

b. IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition veya IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition veya IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition veya IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition için sunulan ek Bulut Hizmetleri:
   - IBM Trusteer Pinpoint Carbon Copy for Retail
   - IBM Trusteer Rapport Remediation for Retail
   - IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail

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

1.1.5 IBM Trusteer Pinpoint Criminal Detection ve/veya IBM Trusteer Pinpoint Criminal Detection II İçin Ek Bulut Hizmetleri

a. IBM Trusteer Pinpoint Criminal Detection for Business veya IBM Trusteer Pinpoint Criminal Detection II için sunulan ek Bulut Hizmetleri:
   - IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business

b. IBM Trusteer Pinpoint Criminal Detection for Retail ve/veya IBM Trusteer Pinpoint Criminal Detection II for Retail için sunulan ek Bulut Hizmetleri:
   - IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

Premium destek, bu belgede belirtildiği şekilde belirli olanaklar için sağlanır.

IBM Trusteer Pinpoint Criminal Detection for Business veya IBM Trusteer Pinpoint Criminal Detection for Retail veya IBM Trusteer Pinpoint Criminal Detection II for Business veya IBM Trusteer Pinpoint Criminal Detection II for Retail aboneliği, bu maddede sıralanan ilgili ek Bulut Hizmetlerine yönelik bir ön koşuldur.

1.1.6 IBM Trusteer Pinpoint Detect Standard ve/veya IBM Trusteer Pinpoint Detect Premium ve/veya IBM Security Pinpoint Detect Standard (erişim yönetimi bütünleştirmesiyle birlikte) ve/veya IBM Security Detect Premium (erişim yönetimi bütünleştirmesiyle birlikte) İçin Ek Bulut Hizmetleri

a. IBM Trusteer Detect Standard for Business ve/veya IBM Trusteer Pinpoint Detect Premium for Business ve/veya IBM Security Pinpoint Detect Standard (Ticari Faaliyet için erişim yönetimi bütünleştirmesiyle birlikte) ve/veya IBM Security Detect Premium (Ticari Faaliyet için erişim yönetimi bütünleştirmesiyle birlikte) için sunulan ek Bulut Hizmetleri:

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

b. IBM Trusteer Detect Standard for Retail ve/veya IBM Trusteer Pinpoint Detect Premium for Retail ve/veya IBM Security Pinpoint Detect Standard (Perakende için erişim yönetimi bütünleştirmesiyle birlikte) ve/veya IBM Security Detect Premium (Perakende için erişim yönetimi bütünleştirmesiyle birlikte) için sunulan ek Bulut Hizmetleri:

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

IBM Trusteer Detect Standard veya IBM Trusteer Pinpoint Detect Premium veya IBM Security Pinpoint Detect Standard (erişim yönetimi bütünleştirmesiyle birlikte) veya IBM Security Detect Premium (erişim yönetimi bütünleştirmesiyle birlikte) aboneliği, bu maddedesıralanan ilgili ek Bulut Hizmetlerine yönelik bir ön koşuldur.

1.1.7 Diğer Ek Bulut Hizmetleri

Burada sıralanmayan ve yukarıda belirtilen temel abonelikler için şu anda mevcut veya halen geliştirilmekte olan herhangi bir ek IBM Bulut 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 yazılımı veya IBM Trusteer Mobile Browser istemci etkinleştirme yazılımı veya son kullanıcının aygıtı üzerinde kurulum için bazı Bulut Hizmetleri ile sağlanan diğer her türlü istemci etkinleştirme yazılımı anlamına gelir.

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.

2. IBM Trusteer Rapport Bulut Hizmetleri

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

Trusteer Rapport, dolandırıcılık ve Man-in-the-Browser (MitB) kötü niyetli yazılım saldırılarına karşı 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 niyetli yazılım saldırılarına ilişkin bilgileri toplar. IBM Trusteer Rapport, kimlik avı dolandırıcılığı saldırılarını engellemeyi ve MitB kötü niyetli yazılım türlerinin kurulmasını ve çalışmasını önlemeyi hedefleyen, davranışa dayalı algoritmalar uygular.

Bu Bulut Hizmeti, bir Hak Kazanan Katılımcı ücret ölçüsüne sahiptir. Ticari Faaliyet (Business) olanağı, 10 Hak Kazanan Katılımcıdan oluşan paketler halinde satılır. Perakende olanağı, 100 Hak Kazanan Katılımcıdan 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 şunları 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 ekranları arasından 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.

2.2 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 niyetli 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 niyetli yazılım saldırılarına ilişkin bilgileri toplar. IBM Trusteer Rapport, kimlik avı dolandırıcılığı saldırılarını engellemeyi ve MitB kötü niyetli yazılım türlerinin kurulmasını ve çalışmasını önlemeyi hedefleyen, davranışa dayalı algoritmalar uygular.

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

2.3 IBM Trusteer Rapport for Business ve/veya IBM Trusteer Rapport for Retail ve/veya IBM Trusteer Rapport II for Business ve/veya IBM Trusteer Rapport II for Retail İçin İsteğe Bağlı Ek Bulut Hizmetleri

IBM Trusteer Rapport Bulut Hizmetleri veya IBM Trusteer Rapport II Bulut Hizmetleri aboneliği, aşağıdaki ek Bulut Hizmetlerinin 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 Bulut Hizmetleri de "Perakende için" olarak belirlenmelidir. Müşteri, olay verilerini, son kullanıcı lisans sözleşmesini kabul etmiş, en az bir kez Müşterinin Genel Sektör ve/veya Perakende Uygulamalarında kimliği doğrulanmış olan ve Hesap Sahibi İstemci Yazılımını çalıştıran Hak Kazanan Katılımcılardan alacaktır ve İstemcinin yapılandırması Kullanıcı Kimliklerinin derlemini içermelidir.

2.3.1 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.

2.3.2 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.

2.3.3 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.

2.3.4 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 veya 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.

2.3.5 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.

3. IBM Trusteer Pinpoint Bulut Hizmetleri

IBM Trusteer Pinpoint, ek bir koruma katmanı sağlamak üzere tasarlanmış, bulut tabanlı bir hizmettir ve kötü niyetli yazılım, kimlik avı dolandırıcılığı ve hesap ele geçirme saldırılarını algılamayı 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 şunları 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

3.1 IBM Trusteer Pinpoint Malware Detection ve IBM Trusteer Pinpoint Criminal Detection Best Practices (En İyi Uygulamalar)

IBM Trusteer Pinpoint Malware Detection Bulut Hizmetlerinde veya IBM Trusteer Pinpoint Malware Detection II Bulut Hizmetlerinde kötü niyetli yazılım algılanması veya IBM Trusteer Pinpoint Crimnal Detection Bulut Hizmetlerinde veya IBM Trusteer Pinpoint Criminal Detection II Bulut Hizmetlerinde hesap ele geçirme saldırısının algılanması durumunda, Müşteri, Pinpoint En İyi Uygulamalar Kılavuzuna (Pinpoint Best Practices Guide) uymalıdır. IBM Trusteer Pinpoint Malware Detection Bulut Hizmetleri veya IBM Trusteer Pinpoint Malware Detection II Bulut Hizmetleri veya IBM Trusteer Pinpoint Criminal Detection Bulut Hizmetleri veya IBM Trusteer Pinpoint Criminal Detection II Bulut Hizmetleri, başkalarının, IBM Trusteer Pinpoint Bulut Hizmetlerinin kullanılmasıyla Müşteri eylemleri arasında bağlantı kurmasını sağlayacak şekilde, bir kötü niyetli yazılımın veya hesap ele geçirme saldırısının algılanmasından hemen sonra Hak Kazanan Katılımcının deneyimini etkileyecek hiçbir şekilde kullanılmamalıdır (örn: kötü niyetli yazılım algılanmasından veya hesabın ele geçirilmesinin algılanmasından hemen sonra bildirimler, iletiler, aygıtların engellenmesi veya Ticari Faaliyet ve/veya Perakende Uygulamasına erişimin engellenmesi).

3.2 IBM Trusteer Pinpoint Criminal Detection for Business ve/veya IBM Trusteer Pinpoint Criminal Detection for Retail

Aygıt kimliği, dolandırıcılık algılama ve kötü niyetli yazılım odaklı kimlik bilgisi hırsızlığını algılama yoluyla, Ticari Faaliyet veya Perakende Uygulamasına bağlı tarayıcıların şüpheli hesap ele geçirme etkinliğinin istemci olmadan algılanması IBM Trusteer Pinpoint Criminal Detection Bulut Hizmetleri, ek bir koruma katmanı sağlar, hesap ele geçirme girişimlerini algılamayı 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).

a. Olay verileri:

   Müşteri (ve onun sınırsız sayıdaki yetkili personeli), Müşterinin, Bulut Hizmetleri kapsamına abone olduğu Ticari Faaliyet veya Perakende 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 sağlama kipi aracılığıyla alabilir.

3.3 IBM Trusteer Pinpoint Criminal Detection II for Business ve/veya IBM Trusteer Pinpoint Criminal Detection II for Retail

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

Aygıt kimliği, dolandırıcılık algılama ve kötü niyetli yazılım odaklı kimlik bilgisi hırsızlığını algılama yoluyla, Ticari Faaliyet veya Perakende Uygulamasına bağlı tarayıcıların şüpheli hesap ele geçirme etkinliğinin istemci olmadan algılanması IBM Trusteer Pinpoint Criminal Detection II Bulut Hizmetleri, ek bir koruma katmanı sağlar, hesap ele geçirme girişimlerini algılamayı 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).

a. Olay verileri:

Müşteri (ve onun sınırsız sayıdaki yetkili personeli), Müşterinin, Bulut Hizmetleri kapsamına abone olduğu Ticari Faaliyet veya Perakende 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 sağlama kipi aracılığıyla alabilir.

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

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

Ticari Faaliyet ve/veya Perakende Uygulamasına bağlanan Man in the Browser (MitB) adlı finansal kötü niyetli yazılımın bulaştığı tarayıcıların istemci olmadan algılanmasıdır. IBM Trusteer Pinpoint Malware Detection Bulut Hizmetleri, bir başka koruma katmanı sağlar ve MitB finansal kötü niyetli yazılım varlığına ilişkin uyarıları ve değerlendirmeleri sağlayarak, kuruluşların, kötü niyetli 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 Perakende teklifleri için Advanced Editions, Müşterinin Ticari Faaliyet ve/veya Perakende Uygulamalarının yapısına ve akışına göre ayarlanıp özelleştirilen ek algılama 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; en az 100.000 Perakende İçin Hak Kazanan Katılımcı veya 10.000 Ticari Faaliyet İçin Hak Kazanan Katılımcıdır. Bu da 1000 paketlik 100 adet Perakende İçin Hak Kazanan Katılımcı veya 1000 paketlik 10 adet Ticari Faaliyet İçin Hak Kazanan Katılımcıya karşılık gelir.

c. Standard Edition:

Ticari Faaliyet veya Perakende için Standard Edition, burada açıklandığı gibi, bu Bulut Hizmetinin temel işlevlerini sağlayan, hızlı devreye alınan bir çözümdür.

3.5 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 niyetli yazılımın bulaştığı tarayıcıların istemci olmadan algılanmasıdır. IBM Trusteer Pinpoint Malware Detection Bulut Hizmetleri, bir başka koruma katmanı sağlar ve MitB finansal kötü niyetli yazılım varlığına ilişkin uyarıları ve değerlendirmeleri sağlayarak, kuruluşların, kötü niyetli 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 Perakende teklifleri için Advanced Editions, Müşterinin Ticari Faaliyet ve/veya Perakende Uygulamalarının yapısına ve akışına göre ayarlanıp özelleştirilen ek algılama 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; en az 100.000 Perakende İçin Hak Kazanan Katılımcı veya 10.000 Ticari Faaliyet İçin Hak Kazanan Katılımcıdır. Bu da 1000 paketlik 100 adet Perakende İçin Hak Kazanan Katılımcı veya 1000 paketlik 10 adet Ticari Faaliyet İçin Hak Kazanan Katılımcıya karşılık gelir.

c. Standard Edition:

Ticari Faaliyet veya Perakende için Standard Edition, burada açıklandığı gibi, bu Bulut Hizmetinin temel işlevlerini sağlayan, hızlı devreye alınan bir çözümdür.

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

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

- IBM Trusteer Rapport Remediation for Retail Bulut Hizmeti için; IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail veya IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail veya IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail veya IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail ön koşul niteliğindedir.
- IBM Trusteer Rapport Remediation for Business Bulut Hizmeti için; IBM Trusteer Pinpoint Malware Detection Standard Edition for Business veya IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business veya IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business veya IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business ön koşul niteliğindedir.
- IBM Trusteer Pinpoint Carbon Copy for Retail için; IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail veyaIBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail veya IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail veya IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail ön koşul niteliğindedir.
- IBM Trusteer Pinpoint Carbon Copy for Business için; IBM Trusteer Pinpoint Malware Detection Standard Edition for Business veya IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business veya IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business veya IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business ön koşul niteliğindedir.

3.6.1 IBM Trusteer Pinpoint Carbon Copy for Business ve/veya IBM Trusteer Pinpoint Carbon Copy for Retail

IBM Trusteer Pinpoint Carbon Copy olanakları, Hak Kazanan Katılımcının kimlik bilgilerinin, Müşterinin, Bulut Hizmetleri olanakları kapsamına abone olduğu Ticari Faaliyet veya Perakende Uygulamasına yönelik kimlik avı dolandırıcılığı saldırılarından tehlike altına girdiği zamanların belirlemesine yardımcı olabilecek izleme hizmeti ve ek bir koruma katmanı sağlamak üzere tasarlanmıştır.

3.6.2 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 niyetli 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 niyetli yazılım bulaşmasını araştırmayı, düzeltmeyi, engellemeyi ve kaldırmayı amaçlar. Müşterinin, kendi Uygulaması üzerinde fiili olarak çalışan IBM Trusteer Pinpoint Malware Detection veya IBM Trusteer Pinpoint Malware Detection II için geçerli bir aboneliğinin olması gerekir. Müşteri, bu Bulut Hizmeti olanağını, sadece Müşterinin Uygulamasına erişimi olan Hak Kazanan Katılımcılar ile bağlantılı olarak ve yalnızca kötü niyetli 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.

3.6.3 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 ve/veya 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.

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

İlk Uygulamadan sonraki herhangi bir ek Ticari Faaliyet Uygulaması üzerindeki IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business veya IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business devreye alımı için IBM Trusteer Pinpoint Malware Detection Additional Applications for Business yetkisi gerekir. İlk Uygulamadan sonraki herhangi bir ek Perakende Uygulaması üzerindeki IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail veya IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail devreye alımı için IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail yetkisi gerekir.

3.7 IBM Trusteer Pinpoint Criminal Detection for Business ve/veya IBM Trusteer Pinpoint Criminal Detection for Retail ve/veya for IBM Trusteer Pinpoint Criminal Detection II for Business ve/veya IBM Trusteer Pinpoint Criminal Detection II for Retail İçin İsteğe Bağlı Ek Bulut Hizmetleri

3.7.1 IBM Trusteer Pinpoint Criminal Detection Redeployment

Kendi çevrimiçi bankacılık Uygulamalarını hizmet süresi içerisinde yeniden devreye alan ve bunun sonucunda da kendi IBM Trusteer Pinpoint Criminal Detection Bulut Hizmeti devreye alımlarında değişiklik yapması gereken Müşteriler, IBM Trusteer Pinpoint Criminal 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.

3.7.2 IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business ve/veya IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

İlk Uygulamadan sonraki herhangi bir Ticari Faaliyet Uygulaması üzerindeki IBM Trusteer Pinpoint Criminal Detection II for Business devreye alımı için IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business yetkisi gerekir. İlk Uygulamadan sonraki herhangi bir Perakende Uygulaması üzerindeki IBM Trusteer Pinpoint Criminal Detection II for Retail devreye alımı için IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail yetkisi gerekir.

4. 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 niyetli yazılım, kimlik avı dolandırıcılığı ve hesap ele geçirme saldırılarını algılayıp 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 şunları 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 Ticari Faaliyet veya Perakende 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 algılanması 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 niyetli yazılımın veya hesap ele geçirme saldırısının algılanmasından hemen sonra Hak Kazanan Katılımcının deneyimini etkileyecek hiçbir şekilde kullanılmamalıdır (örn: kötü niyetli yazılım algılanmasından veya hesabın ele geçirilmesinin algılanmasından hemen sonra bildirimler, iletiler, aygıtların engellenmesi veya Ticari Faaliyet ve/veya Perakende Uygulamasına erişimin engellenmesi).

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

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, e-dolandırıcılık algılama ve kötü niyetli yazılım odaklı kimlik bilgisi hırsızlığını algılama yoluyla, Ticari Faaliyet veya Perakende Uygulamasına bağlı tarayıcılarında yapıldığından şüphelenilen hesap ele geçirme etkinliğinin ve/veya bir kötü niyetli yazılımın istemci olmadan algılanmasını sağlar. IBM Trusteer Pinpoint olanakları, ek bir koruma katmanı sağlar, hesap ele geçirme girişimlerini algılamayı 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).

Standart Destek (yukarıda Teknik Destek bölümünde tanımlandığı şekilde) bu Bulut Hizmetine dahildir. Premium destek için Müşterinin Detect Premium 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.

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

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, e-dolandırıcılık algılama ve kötü niyetli yazılım odaklı kimlik bilgisi hırsızlığını algılama yoluyla, Ticari Faaliyet veya Perakende Uygulamasına bağlı tarayıcılarında yapıldığından şüphelenilen hesap ele geçirme etkinliğinin ve/veya bir kötü niyetli yazılımın istemci olmadan algılanmasını sağlar. IBM Trusteer Pinpoint olanakları, ek bir koruma katmanı sağlar, hesap ele geçirme girişimlerini algılamayı 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.

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.

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 şunları 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 aktive edilmesi ve daha ayrıntılı araştırmanın gerektiği destek için danışmanlık hizmetleri gerekir. Danışmanlık hizmetlerinin ayrıntıları, ayrı bir hizmet bildiriminde belirtilecektir.

Policy Manager aktive edildiğinde, IBM, 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.

Policy Manager özelliği aktive edildiğinde, Müşteri, 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.

4.3 IBM Trusteer Pinpoint Detect Standard with access management integration for Business (Ticari Faaliyet için erişim yönetimi bütünleştirmesiyle birlikte) ve/veya IBM Trusteer Pinpoint Detect Standard with access management integration for Retail (Perakende için erişim yönetimi bütünleştirmesiyle birlikte)

IBM Trusteer Pinpoint Detect Standard with access management integration Bulut Hizmeti, yukarıda madde 4.1'de ayrıntılarıyla verildiği şekilde IBM Security Pinpoint Detect Standard'ın işlevlerini içerir.

IBM Trusteer Pinpoint Detect Standard with access management integration, IBM Security Access Management ("ISAM") gibi erişim yönetimi sistemleriyle birlikte satın alındığında kullanılır. ISAM ile birlikte satın alındığında, her iki olanağın da etkinleştirilmesi gerekir. Bu olanak, erişim yönetimi sistemiyle bütünleştirme seçeneğini içerir. Erişim yönetimi sistemi için yetkiyi içermez.

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

Standart Destek (yukarıda Teknik Destek bölümünde tanımlandığı şekilde) bu Bulut Hizmetine dahildir. IBM Trusteer Pinpoint Detect Premium with access management integration for Business (Ticari Faaliyet için erişim yönetimi bütünleştirmesiyle birlikte) ve/veya IBM Trusteer Pinpoint Detect Premium with access management integration for Retail (Perakende için erişim yönetimi bütünleştirmesiyle birlikte)

IBM Trusteer Pinpoint Detect Premium with access management integration Bulut Hizmeti, yukarıda madde 4.2'de ayrıntılarıyla verildiği şekilde IBM Security Pinpoint Detect Premium'un işlevlerini ve erişim yönetimi sistemiyle bütünleştirme seçeneğini içerir.

IBM Trusteer Pinpoint Detect Premium with access management integration, IBM Security Access Management ("ISAM") gibi erişim yönetimi sistemleriyle birlikte satın alındığında kullanılır. ISAM ile birlikte satın alındığında, her iki olanağın da etkinleştirilmesi gerekir. Bu Bulut Hizmeti, erişim yönetimi sistemiyle bütünleştirme seçeneğini içerir. Erişim yönetimi sistemi için yetkiyi içermez.

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 olanağa dahildir.

4.4 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 for Retail veya IBM Trusteer Pinpoint Detect Standard for Retail ürünü için yetki edinilmesi gerekir.

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

IBM Trusteer Rapport for Mitigation ürünü, kötü niyetli yazılım bulaşmasının IBM Trusteer Pinpoint Detect Premium veya IBM Trusteer Pinpoint Detect Standard olay verileriyle saptandığı durumlarda, Müşterinin Perakende Uygulamasına özel amaçlı olarak erişen, Müşterinin Hak Kazanan Katılımcılarının etkilenen aygıtlarındaki (PC/MAC) kötü niyetli 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 niyetli 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 başka herhangi bir şekilde Hesap Sahibi İstemci Yazılımının Müşterinin genel Hak Kazanan Katılımcı topluluğuna tanıtımını yapmaz.

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

İlk Uygulamadan sonraki herhangi bir ek Ticari Faaliyet Uygulaması üzerindeki IBM Trusteer Pinpoint Detect Standard for Business devreye alımı için IBM Trusteer Pinpoint Detect Standard Additional Applications for Business yetkisi gerekir.

İlk Uygulamadan sonraki herhangi bir ek Perakende Uygulaması üzerindeki IBM Trusteer Pinpoint Detect Standard for Retail devreye alımı için IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail yetkisi gerekir.

İlk Uygulamadan sonraki herhangi bir ek Ticari Faaliyet Uygulaması üzerindeki IBM Trusteer Pinpoint Premium for Business devreye alımı için IBM Trusteer Pinpoint Detect Premium Additional Applications for Business yetkisi gerekir.

İlk Uygulamadan sonraki herhangi bir ek Perakende Uygulaması üzerindeki IBM Trusteer Pinpoint Premium for Retail devreye alımı için IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail yetkisi gerekir.

4.5.2 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.

5. IBM Trusteer Mobile Bulut Hizmetleri

5.1 IBM Trusteer Mobile Browser for Business ve/veya IBM Trusteer Mobile Browser for Retail

IBM Trusteer Mobile Browser, bir başka koruma katmanı sağlamak üzere tasarlanmıştır ve Müşterinin, Bulut Hizmetleri kapsamına abone olduğu Ticari Faaliyet veya Perakende Uygulamalarına erişimi olan Hak Kazanan Katılımcıların mobil aygıtlarına güvenli çevrimiçi erişim, mobil aygıtlara ilişkin risk

değerlendirmesi ve kimlik avı dolandırıcılığına karşı koruma sağlamayı amaçlar. Güvenli Wi-Fi algılaması, yalnızca Android platformları için sağlanır. Mobil aygıtlar, bu Bulut Hizmetinin amacı doğrultusunda, cep telefonlarını veya tabletleri kapsar, ancak dizüstü kişisel bilgisayarları veya Apple Mac bilgisayarları kapsamaz.

Müşteri, TMA aracılığıyla, Hak Kazanan Katılımcıların aşağıda belirtilenleri gerçekleştirdiği Aygıtlarla ilgili olay verilerini, analiz ve istatistik bilgilerini alabilir: (i) son kullanıcı lisans sözleşmesi ("EULA") kapsamında ücretsiz ve genel kullanıma açık olarak lisanslanan bir uygulama ve Hak Kazanan Katılımcıların mobil aygıtlarına indirilmesine olanak sağlanan olan Hesap Sahibi İstemci Yazılımının indirilmesi ve (ii) son kullanıcı lisans sözleşmesinin kabul edilmesi ve Müşterinin, Bulut Hizmetleri kapsamına abone olduğu Müşterinin Ticari Faaliyet ve/veya Perakende Uygulamasında en az bir kez kimliğinin doğrulanması Müşteri, Hesap Sahibi İstemci Yazılımını, yalnızca Trusteer Splash'i kullanarak pazarlayabilir ve bu yazılımı, dahili iş operasyonları için kullanamaz.

a. Olay verileri:

   Müşteri (ve onun sınırsız sayıdaki yetkili personeli), Müşterinin, Bulut Hizmetleri kapsamına abone olduğu Müşterinin Ticari Faaliyet veya Perakende Uygulaması ile mobil aygıtların çevrimiçi etkileşimlerinin sonucunda oluşturulan olay verilerini almak için TMA'yı kullanabilir.

b. 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, "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 kullanılması için, yalnızca Trusteer Splash ile birlikte kullanılmak ve Hesap Sahibi İstemci Yazılımında veya IBM tarafından barındırılan açılış sayfalarında 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.

5.2 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 şunları 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 Aygıtından oluşan paketler halinde sunulur; IBM Trusteer Mobile SDK for Business ise 10 Hak Kazanan Katılımcıdan oluşan paketler halinde veya 10 İstemci Aygıtından 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 şunları 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 şunları 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 devredilemeyecektır 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, Apple (iOS) ve Google (Android) ve diğerleri tarafından sağlanan mobil işletim sistemi platformlarının (topluca "Mobil İşletim Sistemi Platformları" olarak anılacaktır) belirli sürümlerinde yürütülmesinin mümkün olup olmadığını belirlemek amacıyla, IBM Trusteer Mobile SDK içerisinde sağlanan mobil araçlarla ("Mobil Araçlar") oluşturulan örnek uygulamaları test etmiştir, ancak Mobil İşletim Sistemi Platformları üçüncü kişiler tarafından sağlanır, IBM'in denetiminde değildir ve IBM'e bildirilmeksizin değiştirilebilir. IBM, buna bağlı olarak ve aksini ifade eden herhangi bir hüküm dikkate alınmaksızın, Mobil Araçlar kullanılarak oluşturulan herhangi bir uygulamanın veya diğer çıktıların Mobil İşletim Sistemi Platformları veya mobil aygıtlar üzerinde doğru şekilde yürütülebileceğini, bunlarla birlikte çalışabilir olacağını ve 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 Bileşenleri ve Örnek Malzemeleri herhangi bir

destek yükümlülüğü olmaksızın ve MÜLKİYETE, HAK İHLALİ YAPILMAYACAĞINA VEYA MÜDAHALEDE BULUNULMAYACAĞINA DAİR GARANTİLER İLE BİR ÜRÜN VEYA HİZMETİN TİCARİ SATIŞ KOŞULLARINA VE BELİRLİ BİR AMACA UYGUNLUĞA İLİŞKİN ZIMNİ GARANTİLER DE DAHİL OLMAK ÜZERE AÇIK VEYA ZIMNİ HİÇBİR GARANTİ VERMEKSİZİN "OLDUĞU GİBİ" ESASIYLA 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.

Müşteri, IBM Trusteer Mobile SDK programını kullanımının bu Hizmet Tanımı Belgesinin koşullarına uygun olduğunun denetlenip doğrulanmasını sağlamak için yeterli olan doğru yazılı kayıtları, sistem araçları çıktılarını ve diğer sistem bilgilerini oluşturmayı, bunları saklamayı ve IBM'e ve denetçilerine sağlamayı kabul eder.

6. Premium Destek

Müşteri, yalnızca ilgili Premium Destek olanağına abone olduğu IBM Bulut Hizmetleri için Premimum Desteğe hak kazanır.

7. 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 ek bir ücret karşılığında ve imzalanacak ayrı bir sözleşme kapsamında edinilebilir.

8. Veri Gizliliği ve Güvenliği

Bu Bulut Hizmeti, IBM'inhttp://www.ibm.com/cloud/data-security adresinde sağlanan Bulut Hizmetlerine ilişkin veri güvenliğine ve gizlilik ilkelerine ve bu maddede sağlanan tüm ek koşullara uygundur. IBM'in veri güvenliği ve gizlilik ilkelerinde yapılacak hiçbir değişiklik, Bulut Hizmetinin güvenliğinin derecesini azaltmayacaktır.

Bu Bulut Hizmeti, veri sorumlusu olan Müşterinin, Bulut Hizmetinin teknik ve kurumsal güvenlik önlemlerinin, korunacak verilerin işlenmesinden ve niteliklerinden kaynaklanan riskler için uygun olduğunu saptaması kaydıyla, kişisel veriler içeren içeriğin işlenmesinde kullanılabilir. Müşteri, bu Bulut Hizmetinin özel nitelikli kişisel verilerin ya da ek yasal gereksinimlere tabi olan verilerin korunmasına yönelik özellikler sunmadığını kabul eder.

Bu Bulut Hizmeti, IBM'in Privacy Shield (Gizlilik Kalkanı) sertifikasyonunda yer alır ve Müşteri, Bulut Hizmetini ABD'de bulunan bir veri merkezinde barındırmayı seçtiğinde, aşağıdaki adreste sağlanan IBM Privacy Shield Gizlilik İlkesine tabidir: http://www.ibm.com/privacy/details/us/en/privacy_shield.html.

8.1 Güvenlik Özellikleri ve Sorumlulukları

Bulut Hizmeti aşağıdaki güvenlik özelliklerini uygular:

Bulut Hizmeti, IBM ağı ile Müşteri konumu arasında yapılan veri aktarımı sırasında ve uç noktadan veri aktarımını beklerken içeriği şifreler.

8.2 Yasalara Uygun Kullanım ve Onay

Yasalara Uygun Kullanım

Bu Bulut Hizmetinin kullanımı, çeşitli yasa veya yönetmelikleri kapsayabilir. Bulut Hizmeti, yalnızca hukuka uygun amaçlarla ve hukuka uygun biçimde kullanılabilir. Müşteri, Bulut Hizmetini geçerli yasa, yönetmelik ve ilkelere uygun olarak kullanmayı kabul eder ve bunlara uymaya ilişkin tüm sorumluluğu üstlenir.

Verileri Toplama ve İşleme Yetkisi

Bulut Hizmeti, Müşterinin Bulut Hizmeti kapsamında abone olduğu Ticari Faaliyet veya Perakende Uygulamaları ile etkileşim kuran Hak Kazanan Katılımcılardan ve İstemci Aygıtlarından bilgi toplayacaktır. Bulut Hizmeti, tek başına veya birlikte, bazı yargı yetkisi alanlarında Kişisel Veri olarak kabul edilebilecek bilgileri toplayacaktır. Kişisel Veriler IBM'e Müşterinin adına saklaması, işlemesi veya aktarması için sağlanan ve belirli bir kişinin tanımlanmasında kullanılabilen ad, e-posta adresi, ev adresi veya telefon numarası gibi her türlü bilgiyi ifade eder.

Veri toplama ve işleme uygulamaları, Bulut Hizmetinin işlevlerini iyileştirmek için güncellenebilir. Veri toplama ve işleme uygulamalarının tam açıklamasını içeren belge, gerektiği şekilde güncellenir ve talep halinde Müşteriye sağlanır. Müşteri, IBM'e bu bilgileri, bu Hizmet Tanımının Sınır Ötesi Aktarımlar ve Veri Gizliliği bölümlerine uygun olarak toplama ve işleme yetkisi verir.

Trusteer Management Application (TMA) içeren IBM Trusteer olanakları için:

Sponsor teşebbüsteki TMA yöneticileri için aşağıdaki bilgiler toplanır ve Trusteer Management Application (TMA) içinde depolanır: e-posta adresi (oturum açma kimliği), hash algoritmalı parola, verilen ad, soyadı, iş unvanı ve bölüm.

IBM Trusteer Pinpoint Bulut Hizmetleri için:

Toplanan veriler aşağıdakileri içerebilir:

- Şifrelenmiş veya tek yönlü hash algoritmalı Kullanıcı Kimliği, Kalıcı Kullanıcı Kimliği, Rapport Agent Anahtarı ve Müşteri Oturumu Kimliği gibi kullanıcı veya uç nokta tanımlayıcıları;
- Son kullanıcının tarayıcısında, web sitesi ziyaretlerinde ve tarama geçmişinde oluşturulduğu şekilde müşterilerin çevrimiçi bankacılık uygulamasından alınan belirli öznitelikler/öğeler gibi korunan uygulamayla ilgili veriler;
- Kurulu yazılım ortamı bilgileri, tarayıcı ve aygıt öznitelikleri ve ayarları ile tarama geçmişi uzunluğu;
- Donanım bilgileri ve zaman damgası;
- Kullanıcı IP adresi, tanımlayıcı bilgiler, başvuran üstbilgisi ve diğer HTTP üstbilgileri gibi tarayıcı üstbilgileri ve iletişim protokolü verileri;
- Müşterinin çevrimiçi bankacılık uygulamasıyla etkileşimli çalışırken fare işaretçisinin koordinatları, tıklamalar ve fare tekerleği hareketleri (ve bunların eşdeğerleri) gibi son kullanıcının yaptığı fare hareketlerine ilişkin veriler ve zaman damgası;
- Kimlik avı dolandırıcılığı siteleri ve bu sitelere gönderilen bilgiler; ve
- Müşterinin münhasır takdiri doğrultusunda, işlemsel veriler (işlem tutarı, işlem para birimi ve hedef kodları, tek yönlü hash algoritmalı işlem hedef banka tanıtıcısı, tek yönlü hash algoritmalı hedef hesap tanıtıcısı, işlem yeni bir alıcıysa ikili değer ve işlem tarihi/saati) ve isteğe bağlı risk verileri puanı.
- Müşterinin münhasır takdiri doğrultusunda, kullanıcı adı, parola ve diğer metinleri (harf, rakam ya da özel karakterler değil; kullanıcı adı veya parolasını anlama yeteneği olmaksızın) girmek için son kullanıcı tarafından kullanılan tuşa basma sıraları ve klavyedeki yazma ritimleri;

Policy Manager aktive edildiğinde, genişletilmiş tüm verilerin kullanılmasından Müşterinin tek başına sorumludur. IBM, Kişisel Tanımlayıcılar olarak değerlendirilebilecek herhangi bir veri için hash algoritmasını kullanmayı veya veriyi şifrelemeyi önerir.

Müşteri, IBM'in Müşteriye ait resmi defterleri ve/veya kayıtları toplamadığını, yönetmediğini veya elinde tutmadığını anlar ve kabul eder.

Müşteri, IBM Trusteer Rapport for Remediation olanağına abone olduğunda veya bazı Pinpoint destek vakalarında, IBM, süpheli kötü niyetli yazılımdan etkilenip etkilenmediğini araştırmak için Rapport'un Hesap Sahibi İstemci Yazılımının, Hak Kazanan Katılımcının makinesine kurulmasını önerebilir. Rapport olanakları için toplanan veriler aşağıda belirtilmektedir.

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

Toplanan veriler aşağıdakileri içerebilir:

- IBM'in sahtekarlıkla, kimlik avı dolandırıcılığıyla veya bilgilerin açığa çıkmasıyla ilgili olabileceğini düşündüğü, bir Hesap Sahibinin ziyaret ettiği URL adresleri ve IP adresleri ve belirlenen tehditlerin niteliğiyle ilgili bilgiler;
- Çevrimiçi bankacılık siteleri gibi Müşteri tarafından denetlenen ve Bulut Hizmetiyle korunan, Hesap Sahibinin ziyaret ettiği web sitelerinin URL adresleri ve IP adresleri; Hesap Sahibinin IP adresleri;
- Donanım belirleme, işletim sistemleri, uygulama yazılımları, çevrebirim donanımı, güvenlik yapılandırması, sistem ayarları ve uç noktanın ağ bağlantıları ve bunların yanı sıra kullanıcı kimliği, adı, kullanım kalıpları ve uç noktanın diğer tanımlanabilir bilgileri;
- Programın kurulumu ve çalıştırılması ile ilgili bilgiler, programın kimliği, programın sürümü, uç noktadan oluşturulan güvenlik olayları ve programın hatalarıyla ilgili bilgiler;
- Kullanım istatistikleri ve program tarafından algılanan tehditlerle ilgili istatistik bilgileri; tarayıcılarda çökmeleri, bulaşma tarihini ve saatini içeren günlük dosyaları ve belirlenen tehditlerin veya arızaların niteliği hakkındaki bilgiler;
- Sponsor Teşebbüs olarak da atıfta bulunulan müşteri bağlantılı kuruluşu. Son kullanıcı, Müşterinin web sitesinden Rapport yüklediğinde, Trusteer destek sitesinden Rapport yüklerken belirli bir Müşteriyi seçtiğinde ya da Müşterinin bankacılık uygulamasında oturum açtığında bir bağlantılı kuruluş oluşturulur. Bir son kullanıcının birden çok Müşteri bağlantılı kuruluşu olabilir;
- Hesap Sahibinin Müşteriyle etkileşim kurmak için kullandığı şifrelenmiş kullanıcı kimliğinin bir kopyası (isteğe bağlıdır);
- Programın Hesap Sahibine programın bir siteyi riskli bulduğunu bildirmesinden sonra, Hesap sahibinin bu siteye girdiği kredi kartı numarasının şifrelenmiş bir kopyası;
- IBM güvenlik uzmanlarının, kötü niyetli yazılımlar veya diğer kötü niyetli etkinliklerle ilgili olabileceğinden veya programdaki genel arızayla ilişkili olabileceğinden şüphe ettikleri, uç noktadan alınan dosyalar ve diğer bilgiler; ve
- Son kullanıcı Destekle iletişim kurduğunda, adı ve e-posta adresi dahil olmak üzere kişisel iletişim bilgileri.

IBM Trusteer Mobile SDK olanakları ve IBM Trusteer Mobile Browser Bulut Hizmetleri için:

Toplanan veriler aşağıdakileri içerebilir:

- Şifrelenmiş veya tek yönlü hash algoritmalı kullanıcı kimliği gibi kullanıcı tanıtıcıları;
- IP adresi, hash algoritmalı aygıt kimliği, zaman damgası, kurulu paket MD5 değerleri ve diğer aygıtların donanım ve yazılım bilgileri gibi aygıt bilgileri;
- Mobile SDK veya Mobile Browser sürümü ve kurulum tarihi;
- Korunan uygulamalara yapılan ziyaretler;
- Müşterinin üyeliklerine ilişkin bilgiler; ve
- Aygıttaki riskli veriler [örneğin; kötü amaçlı yazılımın varlığı, kaynak gizleyiciler (root hiders), Wi-Fi şifreleme durumu, bir aygıtta üretici tarafından konmuş kısıtlamaların kaldırılmış olması (jailbroken)];
- Çöken ürünlerin izlenmesi (bir uygulamanın beklenmedik bir şekilde sona ermesi durumunda);
- Telefon üretim verileri (örneğin; model, üretici);
- X, Y koordinatları, dokunma alanları ve işlem tipi (aşağı, yukarı ve taşıma) dahil olmak üzere son kullanıcıların dokunmatik ekranda gerçekleştirdiği etkileşimler;

- Hareket sensörü verileri, güç/kaynak kullanımı, bağlanırlık ayarları, sıcaklık, ışık ve hava basıncı gibi ortam sensörleri ve bunların yanı sıra genel aygıt ayarları (ses, zil, ekran parlaklığı vb.).

8.3 Veriyle İlgili Kişilerden Alınan Bilgilendirilmiş Onay

IBM Trusteer Pinpoint Bulut Hizmetleri ve IBM Trusteer Mobile SDK Bulut Hizmetleri için:

Müşteri, Bulut Hizmetini yasalara uygun olarak kullanmak için gereken tamamen bilgilendirilmiş olarak verilen rızaları, izinleri veya lisansları aldığını veya almayı ve ayrıca bilgilerin, IBM tarafından Bulut Hizmeti aracılığıyla toplanıp işlenmesine izin vermeyi kabul eder.

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

Müşteri, IBM'e, https://www.trusteer.com/support/end-user-license-agreement adresinde bulunan Son Kullanıcı Lisans Sözleşmesinde açıklandığı gibi, Bulut Hizmetlerinin yasalara uygun kullanımına ve bilgilerin toplanıp işlenmesine olanak tanımak için gereken, tamamen bilgilendirilmiş olarak verilen onayları alma yetkisi verir. Müşterinin, son kullanıcılar ile onay iletişimlerini, kendisinin (IBM'in değil) yönetmesine karar vermesi durumunda, Bulut Hizmeti aracılığıyla Müşterinin veri işleyeni olarak, bilgilerin IBM tarafından toplanıp işlenmesine izin vermek ve Bulut Hizmetinin yasalara uygun kullanımına olanak tanımak için gereken, tamamen bilgiye dayalı onayları, izinleri ve lisansları aldığını veya alacağını kabul eder.

8.4 Güvenlik Verilerinin Kullanımı

IBM; raporlama etkinliklerini içeren Bulut Hizmetinin kapsamında, Bulut Hizmetinden toplanan önceden tanımlanan ve/veya bir araya getirilen bilgileri ("Güvenlik Verileri") hazırlayacak ve sağlayacaktır. Güvenlik Verileri, Müşteriyi, Müşterinin Hak Kazanan Katılımcılarını veya aşağıda (d) bölümünde sağlananlar dışındaki bir kişiyi tanımlamayacaktır. Müşteri, IBM'in Güvenlik Verilerini yalnızca aşağıdaki amaçlarla sürekli olarak kullanabileceğini ve/veya kopyalayabileceğini kabul eder:

a. Güvenlik Verilerinin yayınlanması ve/veya dağıtılması (örneğin; siber güvenlikle ilgili derlemelerde ve/veya analizlerde)

b. Ürün veya hizmetlerin geliştirilmesi veya iyileştirilmesi;

c. Dahili olarak veya üçüncü kişilerle birlikte araştırma yürütülmesi;

d. Doğrulanmış üçüncü kişi fail bilgilerinin yasalara uygun olarak paylaşılması; ve

e. Policy Manager'daki kuralların kimliksizleştirilmesi.

8.5 Sınır Ötesi Aktarımlar

Müşteri, IBM'in, yukarıdaki Yasal Kullanım ve Onay başlıklı maddede belirtildiği şekilde her türlü Kişisel Veri dahil olmak üzere içeriği, ilgili yasa ve gereklilikler kapsamında, Avrupa Komisyonunun yeterli düzeyde güvenliğe sahip olduğunu düşündüğü ve Avrupa Ekonomik Alanı dışında bulunan, aşağıda belirtilen ülkelerdeki işleyenlere ve alt işleyenlere göndererek, sınır ötesi olarak işleyebileceğini kabul eder: ABD.

8.6 Veri Gizliliği

Müşterinin, Kişisel Verileri, AB Üyesi Devletler, İzlanda, Lihtenştayn, Norveç veya İsviçre'de bulunan Bulut Hizmetine sağlaması veya Müşterinin, bu ülkelerde Hak Kazanan Katılımcılarının veya İstemci Aygıtlarının bulunması durumunda, Müşteri, tek veri sorumlusuolarak, IBM'i kişisel verileri işlemek üzere veri işleyen olarak yetkilendirir (bu terimlerin, AB Direktifi 95/46/EC'de tanımlandığı şekilde). IBM, anılan Kişisel Verileri, sadece Bulut Hizmeti olanağını IBM'in Bulut Hizmetiyle ilgili olarak yayınlanmış açıklamalara göre sağlamak için gerektiği ölçüde işleyecektir. Müşteri, anılan tüm işlemlerin kendi yönergelerine uygun olduğunu kabul eder. IBM, Bulut Hizmetinin bir parçası olarak, işleme yerinde veya Kişisel Verilerin güvenliğini sağlama şeklinde önemli bir değişiklik yaparsa, bu konuda Müşteri Portalı aracılığıyla makul süre öncesinden bildirimde bulunacaktır. Müşteri, etkilenen Bulut Hizmetine ilişkin geçerli Abonelik Süresini IBM'in değişikliği Müşteriye bildiriminden sonra otuz (30) gün içinde IBM'e yazılı bildirim sağlayarak sona erdirebilir.

Taraflar ya da ilgili bağlı şirketleri AB Kararı 2010/87/EU uyarınca üstlendikleri ilgili rollerine uygun olarak ayrı değişiklik yapılmamış ve isteğe bağlı maddeleri kaldırılmış AB Model Madde sözleşmeleri imzalayabilirler. Bu sözleşmelerden kaynaklanan tüm ihtilaflar ya da sorumluluklar, bağlı şirketler tarafından imzalanmış olsa dahi, taraflar arasında ihtilaf ya da sorumluluk kendi aralarında bu Sözleşmenin koşullarından kaynaklanmış gibi kabul edilecektir.

a. Müşteri, hizmet sağlama sürecinde belirlendiği şekilde, Almanya veri merkezi aracılığıyla sağlanan hizmetler için, herhangi bir Kişisel Veri dahil olmak üzere İçeriğin, aşağıdaki işleyenlere ve alt işleyenlere gönderilerek, IBM tarafından uluslararası işlenebileceğini kabul eder:

İşleyenin/Alt İşleyenin Adı	Görev (Veri İşleyen veya Alt İşleyen)	Yer
IBM'in sözleşmeye taraf olan kuruluşu	İşleyen	İşlem Belgesinde belirtildiği gibi
Amazon Web Services (Almanya)	Alt işleyen	Almanya
IBM Ireland Ltd.	İşleyen	İrlanda
IBM Israel Ltd.	İşleyen	İsrail

Almanya veri merkezi aracılığıyla sağlanan hizmetler için, bazı müşteri destek hizmetleri herhangi bir Avrupa Birliği ülkesinde bulunan Trusteer çalışanları tarafından sağlanabilir.

b. Müşteri, hizmet sağlama sürecinde belirlendiği şekilde, Japonya veri merkezi aracılığıyla sağlanan hizmetler için, herhangi bir Kişisel Veri dahil olmak üzere İçeriğin, aşağıdaki işleyenlere ve alt işleyenlere gönderilerek, IBM tarafından uluslararası işlenebileceğini kabul eder:

İşleyenin/Alt İşleyenin Adı	Görev (Veri İşleyen veya Alt İşleyen)	Yer
IBM'in sözleşmeye taraf olan kuruluşu	İşleyen	İşlem Belgesinde belirtildiği şekilde Japonya
Amazon Web Services (Japonya)	Alt işleyen	Japonya
IBM Ireland Ltd.	İşleyen	İrlanda
IBM Israel Ltd.	İşleyen	İsrail

c. Müşteri, hizmet sağlama sürecinde belirlendiği şekilde, ABD veri merkezi aracılığıyla sağlanan hizmetler için, herhangi bir Kişisel Veri dahil olmak üzere İçeriğin, aşağıdaki işleyenlere ve alt işleyenlere gönderilerek, IBM tarafından uluslararası işlenebileceğini kabul eder:

İşleyenin/Alt İşleyenin Adı	Görev (Veri İşleyen veya Alt İşleyen)	Yer
IBM'in sözleşmeye taraf olan kuruluşu	İşleyen	İşlem Belgesinde belirtildiği gibi
Amazon Web Services LLC	Alt işleyen	Amerika Birleşik Devletleri
IBM Ireland Ltd.	İşleyen	İrlanda
IBM Israel Ltd.	İşleyen	İsrail
IBM Corp	İşleyen	Amerika Birleşik Devletleri

d. IBM, yukarıda 8.5.c numaralı maddede listelenen veri merkezleri ("ABD veri merkezi") aracılığıyla sağlanan hizmetler için hizmet sağlama süreci sırasında belirlendiği şekilde, bu verileri aşağıdaki geçerli alt işleyenlerden biri veya birkaçı aracılığıyla da işleyebilir:

İşleyenin/Alt İşleyenin Adı	Görev (Veri İşleyen veya Alt İşleyen)	Yer
Amazon Web Services (Avustralya)	Alt işleyen	Avustralya
Amazon Web Services (Singapur)	Alt işleyen	Singapur
Amazon Web Services (İrlanda)	Alt işleyen	İrlanda

e. Müşteri, IBM'in, işleme sürecini, Müşteri Portalı aracılığıyla bildirildikten sonra Amazon Web Services'ten IBM'in veri merkezlerine taşıyabileceğini kabul eder. Ayrıca, Müşteri Portalı aracılığıyla bildirildikten sonra, IBM, yukarıdaki alt işleyenlerin listesini de değiştirebilir.

f. 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.

g. Müşteri destek verileri, İrlanda'da bulunan bir Salesforce.com bulut sunucusunda depolanır.

h. 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.

9. Hizmet Seviyesi Sözleşmesi

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

9.1 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 koşulları karşılanamadığında, 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 başlayıp 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.

9.2 Hizmet Seviyeleri

Bir sözleşmenin yürürlükte olduğu ay boyunca Bulut Hizmetinin kullanılabilirliği

Bir sözleşmenin yürürlükte olduğu ay boyunca kullanılabilirlik	**Ödemeler (Talebe konu olan sözleşmenin yürürlükte olduğu ay için aylık abonelik ücretinin* yüzdesi)**
< %99,5	%2
< %98,0	%5
< %96,0	%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 Hizmet Alacakları, her Bulut Hizmeti ve her İstemci Uygulaması için ayrı ayrı ölçülür.

Uygulama yetkilerini esas alan Bulut Hizmetleri için SLA alacakları hesaplanırken, Kullanılabirlik, 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:

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

10. 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 Premimum Desteğin ön koşuluna sahiptir.

IBM Trusteer Mobile SDK Bulut Hizmetleri ve IBM Trusteer Rapport Mandatory Service Bulut Hizmetleri dışında her Bulut Hizmeti için ek ücret karşılığında Premium Destek aboneliği sunulur. IBM satış temsilcisiyle ya da IBM Çözüm Ortağıyla iletişim kurulabilir.

Standart Destek:

- Yerel saatle 08.00-17.00 arası destek
- 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-01.ibm.com/software/security/trusteer/support/ adresindeki Müşteri Destek Portalına erişebilir.
- Destek seçenekleri ve ayrıntılar için, http://www-01.ibm.com/software/support/handbook.html adresindeki Hizmet Olarak Sunulan Yazılım Desteği El Kitabına erişin.

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-01.ibm.com/software/security/trusteer/support/ adresindeki Müşteri Destek Portalına erişebilir.

- Destek seçenekleri ve ayrıntılar için, http://www-01.ibm.com/software/support/handbook.html adresindeki Hizmet Olarak Sunulan Yazılım Desteği El Kitabına erişin.

11. Yetki ve Faturalandırma Bilgileri

11.1 Ücret Ölçüleri

Bulut Hizmeti, İşlem Belgesinde belirtilen ücret ölçüsünde sağlanır:

a. 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 kapsayacak yeterli sayıda yetkinin edinilmesi gerekir.

   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.

b. 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.

c. 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.

   Bulut Hizmeti için, bir uygulama Müşterinin tek bir Ticari Faaliyet veya Perakende Uygulamasıdır.

d. Taahhüt, hizmetlerin edinilebileceği bir ölçü birimidir. Bir Taahhüt, Bulut Hizmetleriyle bağlantılı profesyonel hizmetlerden ve/veya eğitim hizmetlerinden oluşur. Her Taahhüdü kapsamaya yetecek sayıda yetki edinilmelidir.

12. Uygunluk ve Denetim

IBM Trusteer Fraud Protection Bulut Hizmetlerine erişim, İşlem Belgesinde belirtildiği gibi, bir maksimum Uygulama, Hak Kazanan Katılımcı ve/veya İstemci Aygıtı miktarıyla sınırlıdır. Müşteri, Uygulamaların, Hak Kazanan Katılımcıların ve/veya İstemci Aygıtların sayısının, İşlem Belgesinde belirtilen maksimum miktarı aşmamasını sağlamaktan sorumludur.

Uygulama, Hak Kazanan Katılımcı veya İstemci Aygıtın maksimum sayısına uygunluğu doğrulamak için IBM tarafından bir denetim yürütülebilir.

13. Süre ve Yenileme Seçenekleri

Bulut Hizmetinin süresi, Yetki Belgesinde belgelenmiş olduğu şekilde, Bulut Hizmetine erişimlerinin 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 olanağı kullanımını yenilemeyeceğini bildirmediği sürece, Bulut Hizmeti Yetki Belgesinde belirtilen süreye uygun olarak kendiliğinden yenilenir.

Sürekli kullanım için: Müşteri, doksan (90) gün önce yazılı olarak olanağı kullanımını sona erdireceğine 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.

14. Ek Koşullar

14.1 Etkinleştirme Yazılımları

Bu Bulut Hizmeti, yalnızca Bulut Hizmetinin süresi boyunca ve Müşterinin Bulut Hizmetini kullanımı ile bağlantılı olarak kullanılacak olan etkinleştirme yazılımları içerir.

14.2 IBM Trusteer Yıllık Abonelik Ücreti Artışı

IBM, Bulut Hizmetleri için abonelik ücretini belirleme hakkını saklı tutar. Abonelik ücreti ayarlaması, geçerli Fiyat Teklifi koşullarında belirtilen fiyatlara yansıtılacaktır. Bulut Hizmetlerinin süresi otomatik yenileme ya da sürekli kullanımla uzatıldığında IBM tarafından %3'ü geçmeyecek şekilde belirlenecek yüzdeyle her on iki (12) ayda bir kezden fazla olmamak koşuluyla ek abonelik ücreti ayarlamaları geçerli olur. Bu ücret ayarlamaları, Müşterinin Bulut Hizmetlerine ilişkin yetkisini ya da Bulut Hizmetinin edinilmesinde esas alınan ücret ölçüsünü değiştirmez. IBM Çözüm Ortakları, IBM'den bağımsızdır ve fiyatları ile koşullarını tek taraflı olarak belirlerler.

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: