IBM Trusteer Pinpoint Detect

Bu Hizmet Tanımında, Bulut Hizmeti açıklanır. Müşterinin siparişine ilişkin fiyatlandırma ve ek ayrıntıları geçerli sipariş belgelerinde sağlanır.

1. Bulut Hizmeti

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 tespit etmeyi ve azaltmayı amaçlar. Trusteer Pinpoint, Müşterinin, Bulut Hizmetleri kapsamına abone olduğu Müşterinin Ticari Faaliyet ve/veya Perakende Uygulamalarıyla ve dolandırıcılığı önleme süreçleriyle bütünleştirilebilir.

Bu Bulut Hizmetine aşağıda belirtilenler dahildir:

a. Trusteer Management Application (Trusteer Yönetim Uygulaması; TMA) ve Trustboard:

   TMA, Trusteer'ın, Müşterilerin uyarıları değerlendirmesini ve sınıflandırmasını sağlayan geleneksel yönetim uygulamasıdır. Trustboard ise asıl olarak araştırma için kullanılan daha yeni bir yönetim uygulamasıdır. Müşteriler, herhangi bir seferde TMA'yı veya Trustboard'u kullanmayı seçebilirler. TMA ve Trustboard'un her biri IBM Trusteer bulutta barındırılan ortam üzerinde kullanıma sunulur. Müşteri (ve Müşterinin sınırsız sayıda yetkili personeli) bu ortam aracılığıyla (i) belirli olay verileri raporlamasını ve risk değerlendirmelerini görüntüleyebilir ve karşıdan yükleyebilir ve (ii) Pinpoint olanaklarından üretilen tehdit akışlarının sağlanmasını görüntüleyebilir, bunlara abone olabilir ve bunları yapılandırabilir. IBM Trusteer Pinpoint Detect ve IBM Trusteer Pinpoint Verify, TMA Trustboard oturum açmanın bir parçası olarak kullanılır.

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

   Bulut Hizmetine erişmek, bu hizmeti test etmek veya kullanmak amacıyla bir web sitesinde devreye alma için

Bir "Oturum", Müşterinin Uygulaması (Web veya Mobil) ile bir veya birden fazla gerçek zamanlı risk değerlendirmesi üreten Bulut Hizmeti arasındaki bir etkileşimdir. Bir Oturum, etkileşimin başlangıcından sonuna kadar ölçülür. Aşağıda belirtilen olaylardan biri gerçekleştiğinde etkileşimin sonu kaydedilir:

- Etkileşim, uygulamadan normal bir şekilde çıkış yapılarak sıfırlandığında.
- Tarayıcı, uygulama veya sekme kapatıldığında.
- Tanımlama bilgileri (cookies) silindiğinde.
- Zamanaşımı olduğunda.

Bir Oturum; oturum açma, göz atma, ödeme, ödeme kurulumu ve Müşterinin Uygulamasıyla tanımlandığı şekilde diğer işlemler gibi herhangi bir sayıda etkinliği içerebilir. Bu Bulut Hizmetinin amaçları doğrultusunda, bir Bağlantı (aşağıda tanımlandığı şekilde) bir Oturum anlamına gelir.

1.1 Olanaklar

Müşteri, aşağıda belirtilen mevcut olanaklar arasından seçim yapabilir.

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

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

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

Özel (Premium) Destek (yukarıda Teknik Destek maddesinde tanımlandığı şekilde) bu Bulut Hizmetine dahildir.

Hizmet, 100 Hak Kazanan Katılımcıdan oluşan paketler halinde veya 100 Bağlantıdan oluşan paketler halinde satın alınmak üzere sunulur.

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

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

Bu çözüm, aygıt kimliği, kimlik avı tespit edilmesi ve kötü amaçlı yazılım odaklı kimlik bilgisi hırsızlığının tespit edilmesi yoluyla, bir Perakendecilik ya da Ticari Faaliyet Uygulamasına bağlı tarayıcılarda yapıldığından şüphelenilen hesap ele geçirme etkinliğinin ve/veya bir kötü amaçlı yazılımın istemci olmadan tespit edilmesini sağlar. IBM Trusteer Pinpoint olanakları, ek bir koruma katmanı sağlar, hesap ele geçirme girişimlerini 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. Hizmet, uygulama başına devreye alma hizmetleri için 200 saate kadar paylaşılan kaynak ve kurulum sonrası uygulama başına güvenlik analizi için 200 saat paylaşılan kaynak içerir. Sürekli hizmetler, uygulama başına yıllık 20 saat devreye alma bakımı ve uygulama başına yıllık 100 saat güvenlik araştırması içerir. Ek çalışma ek ücrete tabidir.

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

Premium destek bu Bulut Hizmetine dahildir.

IBM Trusteer Pinpoint Detect Premium for Retail ve Business hizmetleri, 100 Hak Kazanan Katılımcıdan oluşan paketler halinde veya IBM Trusteer Pinpoint Detect Premium için 100 Bağlantıdan oluşan paketler halinde satın alınmak üzere sunulur. Müşterinin Bağlantılara göre hizmeti satın almayı seçmesi durumunda, ilk uygulamadan itibaren Ek Uygulama ücreti uygulanır.

Pinpoint Detect Policy Manager:

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

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

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

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

Müşteri, Policy Manager özelliği etkinleştirildiğinde, kural ayarları için belgelerde açıklandığı şekilde IBM'in yönergelerini izlemelidir. Müşteri, bu önerilere uyulmaması nedeniyle Müşteriden kaynaklanan durumlardan IBM'in sorumlu olmayacağını kabul eder.

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

1.1.3 IBM Trusteer Pinpoint Detect for Connections (Bağlantılar İçin IBM Trusteer Pinpoint Tespiti)

Bu Bulut Hizmeti koruma sağlar, hesap ele geçirme girişimlerini algılamayı hedefler ve Ticari Faaliyet veya Perakende uygulamasına erişen mobil aygıtlara ve/veya tarayıcılara ilişkin risk / güven değerlendirme puanları sağlar (Müşteri mobil uygulamasının yerel tarayıcısı yoluyla). Çözüm, çeşitli risk

göstergeleri kullanarak son kullanıcının aygıtını, bağlantısını ve davranışını analiz eder ve bunu kullanıcı geçmişiyle karşılaştırarak şüpheli kullanımları belirler.

Bulut Hizmeti, hem Mobil kanallardaki hem de Web kanallarındaki bağlantıları kullanabilir. IBM Trusteer Pinpoint Detect, ilgili olduğunda IBM Trusteer Mobile SDK yetkisi içerir.

Bulut Hizmeti, yıllık 100 Bağlantıdan oluşan paketler halinde sunulur.

1.1.4 IBM Trusteer Pinpoint Detect Bundle (IBM Trusteer Pinpoint Tespit Paketi)

Bu Bulut Hizmeti paketi, IBM Trusteer Pinpoint Detect, IBM Trusteer Mobile SDK ve IBM Trusteer Rapport ile desteklenir. Bu Bulut Hizmeti koruma sağlar, hesap ele geçirme girişimlerini algılamayı hedefler ve Ticari Faaliyet veya Perakende uygulamasına erişen mobil aygıtlara ve/veya tarayıcılara ilişkin risk / güven değerlendirme puanları sağlar (Müşteri mobil uygulamasının yerel tarayıcısı yoluyla). Çözüm, çeşitli risk göstergeleri kullanarak son kullanıcının aygıtını, bağlantısını ve davranışını analiz eder ve bunu kullanıcı geçmişiyle karşılaştırarak şüpheli kullanımları belirler.

Hizmet, Aktif Kullanıcı tarafından satın alınmak üzere sunulur.

Bulut Hizmeti, hem Mobil kanallardaki hem de Web kanallarındaki bağlantıları kullanabilir. IBM Trusteer Pinpoint Detect, IBM Trusteer Mobile SDK'ya erişimi içerir.

IBM Trusteer Pinpoint Detect Bundle, IBM Trusteer Rapport'a erişimi içerir. IBM tarafından aksi yazılı olarak belirtilmediği sürece, bu erişime Trusteer Splash ve IBM Trusteer Rapport Mandatory Service dahil değildir.

IBM Trusteer Mobile SDK

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

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

Müşteri sayılanları gerçekleştirebilir:

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

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

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

   - Müşteri bu Sözleşmede açıkça izin verildiği durumlar dışında sayılanları gerçekleştiremez: (1) SDK programını kullanamaz, kopyalayamaz, değiştiremez veya dağıtamaz; (2) geçerli yasaların sözleşme ile değiştirilmesine olanak tanımayarak açıkça izin verdiği durumlar dışında SDK programını tersine düzenleyemez, tersine derleyemez, başka bir şekilde çeviremez veya üzerinde tersine mühendislik işlemleri yapamaz; (3) SDK programı için alt lisans veremez, bu programı kiralayamaz veya finansal olarak kiralayamaz; (4) Yeniden Dağıtılabilir kodlarda bulunan telif hakkı veya bildirim dosyalarını çıkaramaz; (5) orijinal Yeniden Dağıtılabilir dosyalarla/modüllerle aynı yol adını kullanamaz; ve (6) IBM'in, IBM'in lisans verenlerinin veya distribütörlerinin adlarını veya markalarını, bunların önceden yazılı iznini almaksızın, Müşterinin Bütünleşik Mobil Uygulamasının pazarlanmasıyla bağlantılı olarak kullanamaz.

- Yeniden Dağıtılabilir Kod, Müşterinin Bütünleşik Mobil Uygulaması içerisinde ayrılması mümkün olmayan bir şekilde bütünleşik olarak kalmalıdır. Yeniden Dağıtılabilir Kodun Yalnızca nesne kodu biçiminde olması ve SDK ve belgelerinde belirtilen bütün yönlendirmelere, yönergelere ve belirtimlere uygun olması gerekir. Müşterinin Bütünleşik Mobil Uygulaması için son kullanıcı lisans sözleşmesinde şu konularda son kullanıcıya bildirimde bulunulacaktır: Yeniden Dağıtılabilir Kodlar i) Müşterinin Bütünleşik Mobil Uygulamasının etkinleştirilmesi dışında herhangi bir amaçla kullanılamayacaktır, ii) kopyalanamayacaktır (yedekleme amaçları hariç olmak üzere), iii) üçüncü kişilere dağıtılamayacak ya da devredilemeyecektir ya da iv) yasaların sözleşme ile değiştirilmesine olanak sağlamaksızın açıkça izin verdiği durumlar hariç olmak üzere, tersine derlemeye, tersine mühendisliğe ya da diğer herhangi bir şekilde çeviriye tabi tutulamayacaktır. Müşterinin lisans sözleşmesinin IBM açısından en az bu Sözleşmenin koşulları kadar koruyucu olması gerekmektedir.
- 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 tek başına Müşteri sorumludur. Müşterinin Bütünleşik Mobil Uygulamasına ilişkin tüm teknik destekten ve Yeniden Dağıtılabilir Kodlarda, işbu belgede izin verilen, yapılan herhangi bir değişiklikten Müşteri sorumludur.

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

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

Kaynak Bileşenler ve Örnek Malzemeler – IBM Trusteer Mobile SDK, kaynak kodundaki bazı bileşenleri ("Kaynak Bileşenler") ve Örnek Malzemeler olarak tanımlanan diğer malzemeleri içerebilir. Müşteri, Kaynak Bileşenleri ve Örnek Malzemeleri yalnızca dahili kullanım amacıyla kopyalayabilir ve değiştirebilir; ancak bu tür bir kullanımın bu Sözleşme kapsamındaki lisans haklarının sınırları içinde olması gerekir. Ayrıca Müşteri, Kaynak Bileşenler veya Örnek Malzemeler içinde yer alan herhangi bir telif hakkı bilgisini veya bildirimini değiştiremez veya silemez. IBM, Kaynak Bileşenlerini ve Örnek Malzemeleri herhangi bir destek yükümlülüğü olmaksızın ve "OLDUĞU GİBİ" esasıyla sağlar. Kaynak Bileşenlerin veya Örnek Malzemelerin, yalnızca CIMA içine Yerleştirilebilir öğelerin nasıl uygulanacağına örnek olarak sağlanmaktadır. Kaynak Bileşenler veya Örnek Malzemeler, Müşterinin geliştirme ortamıyla uyumlu olmayabilir ve bunların Müşterinin CIMA'sı içine Yerleştirilebilir öğelerinin test edilmesinden ve uygulanmasından tek başına Müşteri sorumludur.

Bu paragrafta belirtilen hükümler, işbu belgede yer alan Bulut Hizmetlerinin, merkezi New York'ta bulunan bir şirket olan International Business Machines Corporation ("IBM Corporation") dışında bir kuruluş tarafından sağlanması halinde geçerlidir. İşbu belge kapsamında bulunan SDK (Yazılım Geliştiricisi Kiti) ve Yeniden Dağıtılabilir Kodlara ilişkin haklar, IBM Corporation tarafından sağlanır. IBM, bu Sözleşme uyarınca bir distribütör olarak hizmet vermektedir ve Yazılım Geliştiricisi Kiti ile Yeniden Dağıtılabilir Kodu sağlamaktadır ve SDK ile Yeniden Dağıtılabilir Kod ile ilgili tüm yükümlülüklerin yerine getirilmesini ve koşulların uygulanmasını sağlamaktan sorumludur. Bu belge, Müşteri lehine, IBM Corporation şirketine karşı herhangi bir hak ya da yasal yollara başvurma gerekçesi sağlamaz. Müşteri, IBM Corporation şirketine karşı olan tüm iddialarından ve yasal yollara başvurma gerekçelerinden feragat eder ve SDK ile Yeniden Dağıtılabilir Koda ilişkin tüm haklar ve yasal çareler için münhasıran IBM'e başvurmayı kabul eder.

IBM Trusteer Rapport

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

Bu Bulut Hizmeti ürününe aşağıda belirtilenler dahildir:

a. Web Komut Dosyası:

Bulut Hizmetine erişmek, bu hizmeti test etmek veya kullanmak amacıyla bir web sitesinde erişim içindir.

1.2 İsteğe Bağlı Hizmetler

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

1.2.1 IBM Trusteer Pinpoint Detect Standard Application (IBM Trusteer Pinpoint Tespit Standart Uygulaması)

Müşteri Uygulaması, bir Web Uygulamasını ve/veya bir Mobil Uygulamayı ifade eder. Web Uygulaması, bir oturum açma veya kimlik belirleme ekranından birçok web sayfası aracılığıyla Müşterinin Hak Kazanan Katılımcılarına sunulan ve Trusteer konsolunda (Trusteer Management Application) tek bir Uygulama olarak izlenen tüm işlevleri gruplar. Mobil Uygulaması, bir oturum açma veya kimlik belirleme ekranından bir uygulama mağazasından (mağaza) indirilebilen bir yazılım programı aracılığıyla Müşterinin Hak Kazanan Katılımcılarına sunulan ve Trusteer konsolunda (Trusteer Management Application) tek bir Uygulama olarak izlenen tüm işlevleri birlikte gruplar.

IBM Trusteer Pinpoint bütünleştirmesinde her Uygulama için IBM Trusteer Pinpoint Application yetkisi gereklidir.

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

1.2.2 IBM Trusteer Pinpoint Detect Premium Application (IBM Trusteer Pinpoint Tespit Premium Uygulaması)

Müşteri Uygulaması, bir Web Uygulamasını ve/veya bir Mobil Uygulamayı ifade eder. Web Uygulaması, bir oturum açma veya kimlik belirleme ekranından birçok web sayfası aracılığıyla Müşterinin Hak Kazanan Katılımcılarına sunulan ve Trusteer konsolunda (Trusteer Management Application) tek bir Uygulama olarak izlenen tüm işlevleri gruplar. Mobil Uygulaması, bir oturum açma veya kimlik belirleme ekranından bir uygulama mağazasından (mağaza) indirilebilen bir yazılım programı aracılığıyla Müşterinin Hak Kazanan Katılımcılarına sunulan ve Trusteer konsolunda (Trusteer Management Application) tek bir Uygulama olarak izlenen tüm işlevleri birlikte gruplar.

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

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

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

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

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

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

IBM Trusteer Digital Content Pack, güvenlik analistlerinin, bir yandan gelişmekte olan tehditlere tepki göstermek için özel amaçlı raporların oluşturulmasını ve değiştirilmesini tam olarak desteklerken diğer yandan yeni sahtekarlık modellerini bütünleştirmelerini sağlar. Çözümün ek ve ayrılmaz bir parçası olarak satın alınabilecek kapsamlı bir kural, öngörü ve ilke setinden oluşur. Digital Content Pack, Trusteer'ın dijital sahtekarlığı önleme yetenekleri ile IBM Safer Payments nakitsiz ödeme kanalları arasındaki bütünleştirmeyi daha da artırmaya yardımcı olur. Digital Content Pack, yerleşik kurallarından ve belirli iş

mantığından yararlanarak, bankaların ve diğer finansal kuruluşların, mevcut sahtekarlığı saptama ve önleme yeteneklerini daha da geliştirmelerini sağlar.

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

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

1.2.5 IBM Trusteer Pinpoint Malware Detection

Müşteri, IBM Trusteer Pinpoint Malware Detection II Bulut Hizmetlerinde kötü amaçlı yazılım tespit edilmesi durumunda, Pinpoint En İyi Uygulamalar Kılavuzunu takip etmelidir. IBM Trusteer Pinpoint Malware Detection II Bulut Hizmetleri, başkalarının IBM Trusteer Pinpoint Bulut Hizmetlerinin kullanılmasıyla Müşteri eylemleri arasında bağlantı kurmasını sağlayacak şekilde bir kötü amaçlı yazılımın veya hesap ele geçirme saldırısının tespit edilmesinden hemen sonra Hak Kazanan Katılımcının deneyimini etkileyecek hiçbir şekilde kullanılmamalıdır (örneğin, kötü amaçlı yazılımın tespit edilmesinden veya hesabın ele geçirilmesinin tespit edilmesinden hemen sonra bildirimler, iletiler, aygıtların engellenmesi veya Ticari Faaliyet ve/veya Perakendecilik Uygulamasına erişimin engellenmesi).

1.2.6 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 algılanması. IBM Trusteer Pinpoint Malware Detection Bulut Hizmetleri, bir başka koruma katmanı sağlar ve MitB finansal kötü amaçlı yazılım varlığına ilişkin uyarıları ve değerlendirmeleri sağlayarak, kuruluşların, kötü amaçlı yazılım riskine dayalı dolandırıcılık önleme süreçlerine odaklanmasına olanak tanımayı hedefler.

a. Olay verileri:

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

b. Advanced Edition:

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

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

c. Standard Edition:

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

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

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

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

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

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

Aygıt kimliği, kimlik avı dolandırıcılığını 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 algılanmasıdır. IBM Trusteer Pinpoint Criminal Detection Bulut Hizmetleri, ek bir koruma katmanı sağlar, hesap ele geçirme girişimlerini tespit etmeyi hedefler ve Ticari Faaliyet veya Perakende Uygulamasına erişen mobil aygıtlara veya tarayıcılara ilişkin risk değerlendirme puanlarını Müşteriye doğrudan sağlar (yerel tarayıcı veya Müşteri mobil uygulaması yoluyla).

a. Olay verileri:

   Müşteriler, herhangi bir seferde TMA'yı veya Trustboard'u kullanmayı seçebilirler. Müşteri (ve onun sınırsız sayıdaki yetkili personeli), Müşterinin, Bulut Hizmetleri kapsamına abone olduğu Ticari Faaliyet veya Perakende Uygulaması/Uygulamaları ile Hak Kazanan Katılımcıların çevrimiçi etkileşimlerinin sonucunda oluşturulan olay verilerini almak için TMA'yı veya Trustboard'u kullanabilir veya Müşteri, olay verilerini arka uç API'si sağlama kipi aracılığıyla alabilir.

1.2.9 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, kimlik avı dolandırıcılığını 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 algılanmasıdır. IBM Trusteer Pinpoint Criminal Detection II Bulut Hizmetleri, ek bir koruma katmanı sağlar, hesap ele geçirme girişimlerini tespit etmeyi hedefler ve Ticari Faaliyet veya Perakende Uygulamasına erişen mobil aygıtlara veya tarayıcılara ilişkin risk değerlendirme puanlarını Müşteriye doğrudan sağlar (yerel tarayıcı veya Müşteri mobil uygulaması yoluyla).

a. Olay verileri:

   Müşteriler, herhangi bir seferde TMA'yı veya Trustboard'u kullanmayı seçebilirler. Müşteri (ve onun sınırsız sayıdaki yetkili personeli), Müşterinin, Bulut Hizmetleri kapsamına abone olduğu Ticari Faaliyet veya Perakende Uygulaması/Uygulamaları ile Hak Kazanan Katılımcıların çevrimiçi etkileşimlerinin sonucunda oluşturulan olay verilerini almak için TMA'yı veya Trustboard'u kullanabilir veya Müşteri, olay verilerini arka uç API'si 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.

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

IBM Trusteer Rapport Remediation for Retail ve IBM Trusteer Rapport Remediation for Business ürünleri, MitB kötü amaçlı yazılım bulaşmasının, IBM Trusteer Pinpoint Malware Detection'ın olay verileriyle saptandığı durumda, Müşterinin Uygulamasına özel amaçlı olarak erişen, Müşterinin Hak Kazanan Katılımcılarının etkilenen aygıtlarındaki man-in-the-browser (MitB) kötü amaçlı yazılım bulaşmasını araştırmayı, düzeltmeyi, engellemeyi ve kaldırmayı amaçlar. Müşteri, halihazırda Müşterinin Uygulaması üzerinde çalışan IBM Trusteer Pinpoint Malware Detection II aboneliğine sahip olmalıdır. Müşteri, bu Bulut Hizmeti olanağını, sadece Müşterinin Uygulamasına erişimi olan Hak Kazanan Katılımcılar ile bağlantılı olarak ve yalnızca kötü amaçlı yazılım bulaşan aygıtı (PC/MAC) özel amaçlı olarak araştırıp düzeltmeyi amaçlayan bir araç olarak kullanabilir. IBM Trusteer Rapport Remediation, etkilenen Hak Kazanan Katılımcının aygıtı (PC/MAC) üzerinde fiili olarak çalışmalıdır. Etkilenen Hak Kazanan Katılımcı, son kullanıcı lisans sözleşmesini kabul etmeli, Müşterinin Uygulamasında/Uygulamalarında en az bir kez kimliği doğrulanmalı ve Müşterinin yapılandırması ise Kullanıcı kimliklerinin derlemini içermelidir. Herhangi bir şüpheye yer vermemek için, bu Bulut Hizmeti olanağı, Trusteer Splash'ı kullanma hakkını içermez ve/veya başka herhangi bir şekilde Hesap Sahibi İstemci Yazılımının Müşterinin genel Hak Kazanan Katılımcı topluluğuna tanıtımını yapmaz. Bu Hizmet Tanımının amacı doğrultusunda Hesap Sahibi - Müşterinin istemci etkinleştirme yazılımını kurmuş, son kullanıcı lisans sözleşmesini ("EULA") kabul etmiş

ve Müşterinin Bulut Hizmeti kapsamına abone olduğu Müşterinin Ticari Faaliyet ve/veya Perakende Uygulamasında en az bir kez kimliği doğrulanmış olan son kullanıcısı anlamına gelir. Hesap Sahibi İstemci Yazılımı - IBM Trusteer Rapport istemci etkinleştirme yazılımını veya son kullanıcının aygıtı üzerinde kurulum için bazı Bulut Hizmetleri ile sağlanan diğer her türlü istemci etkinleştirme yazılımını ifade eder.

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

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

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

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

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

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

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

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

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

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

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

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

1.2.16 IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect (IBM Trusteer Pinpoint Tespit için Mobil Taşıyıcı İstihbaratı)

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

Bu Bulut Hizmeti, söz konusu Bulut Hizmetlerinden herhangi birine sağlanan cep telefonu numaralarına ilişkin ek bilgiler ve bağlam sağlayarak IBM Trusteer Pinpoint Detect'i geliştirir ve her oturum için sahtekârlık riskinin belirlenmesine yardımcı olur. Müşteri, numarayla ilişkili operatör bilgileri gibi herhangi bir cep telefonu numarasına ilişkin nitelikleri öğrenmek için Bulut Hizmetini sorgulayabilir.

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

1.3 Hızlandırma Hizmetleri

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

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

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

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

1.3.2 IBM Trusteer Pinpoint Malware Detection Redeployment

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

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

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

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

1.3.3 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.

2. Veri İşleme ve Veri Koruma Sayfaları

IBM'in http://ibm.com/dpa adresinde yer alan Veri İşleme Ek Sözleşmesi ile aşağıda belirtilen bağlantılarda yer alan Veri İşleme ve Veri Koruma Veri Sayfası/Sayfaları (veri sayfası/sayfaları ya da Veri İşleme Ek Sözleşmesi Eki/Ekleri olarak anılır), işlenebilecek İçerik türleri, ilgili işleme etkinlikleri, veri koruma özellikleri ve İçeriğin saklanmasına ve iadesine ilişkin belirli bilgiler dahil olmak üzere Bulut Hizmetlerine ve seçeneklerine ilişkin ek veri koruma bilgileri sağlar. İçerikte yer alan kişisel veriler için, i) Avrupa Genel Veri Koruma Yönetmeliği'nin (EU/2016/679) (GDPR veya GVKY) ya da ii) http://ibm.com/dpa/dpl adresinde belirtilen diğer veri koruma kanunlarının geçerli olması halinde ve geçerli olduğu ölçüde, Veri İşleme Ek Sözleşmesi geçerli olur.

Veri Sayfalarının genellikle IBM'in (üçüncü kişi alt işleyenler dahil), hizmetlerin devreye alındığı veri merkezine bakmaksızın, Kişisel Verileri barındırdığı ve işlediği tüm konumları listelediği açık bir şekilde ifade edilmektedir. Hizmetlerin devreye alındığı veri merkezine özgü olan barındırma ve işleme konumlarının bir listesi için aşağıda Madde 5.2'ye (Ek İşleme Konumu Bilgileri) bakılmalıdır.

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

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

IBM Trusteer Pinpoint Detect

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

IBM Trusteer Pinpoint Malware Detection

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

IBM Trusteer Mobile SDK

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

IBM Trusteer Rapport

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

3. Hizmet Seviyeleri ve Teknik Destek

3.1 Hizmet Seviyesi Sözleşmesi

IBM, Müşteriye aşağıda belirtilen kullanılabilirlik hizmet seviyesi sözleşmesini sağlar. IBM, aşağıdaki tabloda gösterildiği şekilde, Bulut Hizmetinin kümülatif kullanılabilirliği doğrultusunda geçerli olan en yüksek telafi ücretini uygulayacaktır. Kullanılabilirlik oranı, sözleşmenin yürürlükte olduğu bir ay içindeki toplam dakika sayısından sözleşmenin yürürlükte olduğu bir ay içindeki toplam Hizmet Kapalı Kalma Süresi dakikalarının sayısı çıkarılarak ve sonuç sözleşmenin yürürlükte olduğu bir ay içindeki toplam dakika sayısına bölünerek hesaplanır. Hizmet Kapalı Kalma Süresinin tanımı, ödeme talebi süreci ve hizmetin kullanılabilirliğine ilişkin sorunlar için IBM ile nasıl iletişim kurulacağı, https://www.ibm.com/software/support/saas_support_overview.html adresinde yer alan IBM Hizmet Olarak Sunulan Yazılım desteğine genel bakış sayfasında belirtilir.

Kullanılabilirlik	Alacak (aylık abonelik ücretine oranı*)
%99,9'den daha az	%2
%99,0'dan az	%5
%95'ten daha az	%10

* Abonelik ücreti, ödeme talebine konu olan ay için sözleşmede belirtilen fiyattır.

3.2 Teknik Destek

Destek iletişim bilgileri, önem dereceleri, desteğin sağlanacağı saatler, müdahale süreleri ve diğer destek bilgileri ile süreçleri dahil olmak üzere Bulut Hizmetine ilişkin teknik destek, https://www.ibm.com/support/home/pages/support-guide/ adresinde yer alan IBM destek kılavuzunda Bulut Hizmeti seçilerek bulunabilir.

Premium Destek:

Bulut Hizmeti için, ek ücret karşılığında Premium Destek aboneliği sağlanır ve aşağıdakileri içerir:

- Tüm önem dereceleri için haftanın 7 günü, günde 24 saat destek
- Müşteriler, desteğe doğrudan telefonla ve geri arama isteğiyle ulaşabilirler.
- Müşteriler ve Hak Kazanan Katılımcıları, Hizmet Olarak Sunulan Yazılım Desteği El Kitabında ayrıntılı olarak açıklandığı gibi, destek bildirim formlarını elektronik ortamda gönderebilir.
- Müşteriler; bildirimler, belgeler, vaka raporları ve sık sorulan sorular için http://www.ibm.com/software/security/trusteer/support/ adresindeki Müşteri Destek Portalına erişebilirler.

4. Ücretler

4.1 Ücret Ölçüleri

Bulut Hizmeti için ücret ölçüsü/ölçüleri, İşlem Belgesinde belirtilir.

Bu Bulut Hizmeti için aşağıda belirtilen ücret ölçüleri geçerlidir:

- Taahhüt, Bulut Hizmetleri ile bağlantılı bir profesyonel hizmet ya da eğitim hizmetidir.
- Hak Kazanan Katılımcı, Bulut Hizmetleri tarafından yönetilen ya da izlenen herhangi bir hizmet sağlama programına katılmaya hak kazanan bir gerçek ya da tüzel kişidir.
    - Etkin Kullanıcı, Bulut Hizmetlerine doğrudan veya dolaylı olarak herhangi bir araçla (örneğin, bir çoğullama programı, aygıtı veya uygulama sunucusu aracılığıyla) herhangi bir şekilde erişen tek bir kişidir.
- IBM Trusteer Pinpoint Detect Bundle için Aktif Kullanıcı, Bulut Hizmetlerine, son 12 aylık dönemde (söz konusu süreden önce) en az bir kez herhangi bir araç ile erişen tek bir kişidir.
- Uygulama, Bulut Hizmetlerine erişilmesi ya da Bulut Hizmetleri tarafından kullanılması için geliştirilen ya da kullanıma sunulan, özgün bir ada sahip olan bir yazılım programıdır.
- Uygulama Programlama Arabirimi (API) Çağrısı, Bulut Hizmetlerinin bir programlanabilir arabirim aracılığıyla başlatılmasıdır.

- Bağlantı, Bulut Hizmetleri için önceden kullanıma sunulmuş olan veya şu anda sunulan bir veritabanı, uygulama, sunucu ya da başka bir aygıt türüne ilişkin bir bağlantı (link) ya da ilişkidir.

4.2 Uzaktan Sağlanan Hizmet Ücretleri

Uzaktan sağlanan hizmetin süresi, uzaktan sağlanan hizmetin kullanılıp kullanılmadığı dikkate alınmaksızın, satın alınmasından 90 gün sonra sona erecektir.

5. Ek Koşullar

1 Ocak 2019 tarihinden önce imzalanmış olan Bulut Hizmeti Sözleşmeleri (ya da eşdeğer çerçeve bulut sözleşmeleri) için https://www.ibm.com/acs adresinde yer alan koşullar geçerlidir.

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

IBM Trusteer Rapport Bulut Hizmetleri (Pinpoint Bulut Hizmetleriyle bağlantılı olarak devreye alındığında Rapport Remediation veya Rapport for Mitigation dahil) için: Müşteri, aksi kararlaştırılmadıkça ve Müşteri tarafından bağımsız olarak belirlenen işleme gerekçesi uyarınca, IBM'in Bulut Hizmetlerini sağlaması için gereken bilgileri toplayıp işleyebilmesi amacıyla https://trusteer.secure.force.com/PKB/articles/en_US/FAQ/RAPPORT-DATA-PRIVACY-NOTICE-AND-END-USER-LICENSE-AGREEMENT-EULA adresinde bulunan Son Kullanıcı Lisans Sözleşmesini sağlaması için IBM'e yetki verir.

IBM Trusteer Rapport Bulut Hizmetleri için, Müşteri, Sponsor Teşebbüsünün veri işleyeni olarak IBM'e; Programı, kötü amaçlı yazılımları ve kötü amaçlı yazılım çıktılarını, diğer bir deyişle kötü amaçlı etkinliklerle ilgili dosyaları veya Programda olağan dışı arıza çıkmasıyla ilgili dosyaları toplamak için kullanma yetkisi verir. IBM, Programı son kullanıcının kişisel bilgilerini içeren dosyaları hedef alarak toplamak için kullanmaz; ancak toplanan dosyalar, kötü amaçlı yazılımlar tarafından son kullanıcının izni olmaksızın elde edilmiş olan kişisel verileri içerebilir. IBM, 1) söz konusu analizle ilgili olmayan her türlü dosyayı derhal silecektir ve 2) ilgili dosyaları yalnızca analiz süresince saklayacak ve hiçbir koşulda üç aydan fazla saklamayacaktır.

5.2 Ek İşleme Konumu Bilgileri

Kişisel Verilerin her türlü şekilde barındırılması ve işlenmesi, Veri Sayfasında belirtilen üçüncü kişi alt işleyenler tarafından gerçekleştirilecekler de dahil olmak üzere, aşağıda belirtilen konumlarda gerçekleştirilecektir:

IBM, Almanya'da bulunan veri merkezi aracılığıyla sağlanan tüm hizmetler için, Kişisel Verilerin barındırılmasını ve işlenmesini sözleşmeyi imzalayan IBM kuruluşunun ülkesiyle ve şu ülkelerle sınırlayacaktır: Almanya, İsrail, İrlanda ve Hollanda.

IBM, Japonya'da bulunan veri merkezi aracılığıyla sağlanan tüm hizmetler için, Kişisel Verilerin barındırılmasını ve işlenmesini sözleşmeyi imzalayan IBM kuruluşunun ülkesiyle ve şu ülkelerle sınırlayacaktır: Japonya, İsrail, ve İrlanda.

IBM, ABD'de bulunan veri merkezi aracılığıyla sağlanan hizmetler için, Kişisel Verilerin barındırılmasını ve işlenmesini sözleşmeyi imzalayan IBM kuruluşunun ülkesiyle ve şu ülkelerle sınırlayacaktır: ABD, İsrail, İrlanda, Singapur ve Avustralya.

Yukarıda bahsi geçen konumlara ek olarak, Almanya, Japonya ve ABD'de bulunan veri merkezleri aracılığıyla sağlanan tüm hizmetlerle ilgili olarak, (1) destek verileri IBM'in üçüncü kişi alt işleyeni olarak Salesforce.com tarafından Almanya ve Fransa'da barındırılabilir veya işlenebilir ve (2) Mobil Taşıyıcı İstihbaratı sağlayıcılarına veri göndermeyi tercih eden müşteriler için, Kişisel Veriler, Veri Sayfasında belirtilen şekilde geçerli üçüncü kişi alt işleyenlerin ülkelerinde barındırılabilir ve işlenebilir. Veri Sayfasında aksini belirten herhangi bir ifadeye etki etmeksizin, hemen önceki cümlede yer alan hüküm (2)'de belirtilen üçüncü kişi alt işleyenler ISO 27001 veya SOC2 uyumlu olmayabilir.

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

5.3 Hesap Sahibinin Verileri

Netleştirmek amacıyla, belirli bir Hesap Sahibinin Hesap Sahibi Müşteri Yazılımına bağlı birden fazla IBM müşterisi (bu tür IBM müşterileri “Bağlı Müşteri” olarak anılır) varsa ve bu Hizmet Tanımı kapsamındaki hizmetler söz konusu Bağlı Müşterilere IBM tarafından farklı bölgelerdeki veri merkezleri aracılığıyla

sağlanıyorsa, Hesap Sahibinin verileri yukarıdaki Madde 5.2'de belirtildiği şekilde bu tür her veri merkeziyle ilişkili her türlü konumda işlenebilir.

5.4 Bütünleşik Çözümler

Netleştirmek amacıyla, Trusteer markası altındaki çeşitli olanaklar, bütünleşik bir çözüm oluşturabilir. Bu nedenle, Müşteri bu Bulut Hizmetlerinden birini sona erdirirse, IBM, Müşteriye bu Hizmet Tanımı kapsamındaki geri kalan Bulut Hizmetlerini ve diğer Trusteer hizmetleri için geçerli olan hizmet tanımları uyarınca da diğer Trusteer hizmetlerini sağlamak amacıyla Müşteri verilerini saklayabilir.

5.5 Etkinleştirme Yazılımı

Bulut Hizmeti aşağıda belirtilen Etkinleştirme Yazılımlarını içerir:

- IBM Rapport Agents

5.6 Pinpoint En İyi Uygulamaları

Kötü niyetli yazılım olduğunun veya hesapların ele geçirildiğinin algılanması durumunda, Müşteri, Pinpoint En İyi Uygulamalar Kılavuzuna 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).

5.7 Devreye Almanın Bir Parçası Olarak Toplanan Veriler

Bulut Hizmetinin devreye alımı, Müşterinin IBM'e belirli veriler sağlamasını gerektirebilir. Bu veriler, belirli kişileri tanımlayabilecek veya belirli kişilerle ilişkilendirilebilecek bilgileri içermemelidir. Müşteri tarafından IBM'e devreye alımın bir parçası olarak sağlanan verilere ilişkin yönergeler, Müşteriye sağlanacak Trusteer Deployment Guidelines (Trusteer Devreye Alma Yönergeleri) içinde yer alır.

6. Geçersiz Kılan Hükümler

6.1 Veri Kullanımı

Aşağıda belirtilen hüküm, taraflar arasında yürürlükte olan temel Bulut Hizmeti hükümlerinin İçerik ve Veri Koruması maddesinin aksine herhangi bir hükümden öncelikli olarak uygulanır: IBM, Müşterinin Bulut Hizmetini kullanımından kaynaklanan ve Müşterinin İçeriğine (İçgörüler) özgü olan veya başka bir şekilde Müşteriyi tanımlayan sonuçları kullanmayacak veya açıklamayacaktır. Ancak IBM, İçeriği ve İçerikten kaynaklanan diğer bilgileri (İçgörüler hariç olmak üzere), Bulut Hizmetinin iyileştirilmesi amacıyla Bulut Hizmetinin bir parçası olarak kullanacaktır. Ayrıca IBM, İçeriğe yerleşik tehdit tanımlayıcılarını ve diğer güvenlik bilgilerini de tehdit algılama ve tehdide karşı koruma amacıyla paylaşabilir.

Kabul eden:	Kabul eden:
Müşteri Şirketinin Ticari Unvanı adına ("**Müşteri**")	***<İlgili IBM Şirketinin Ticarı Unvanı adına>*** ("**IBM**")
İmza_____	İmza_____
Yetkili imza	Yetkili imza
Unvan:	Unvan:
İsim (el yazısı veya daktiloyla):	İsim (el yazısı veya daktiloyla):
Tarih:	Tarih:
Müşteri Numarası:	Sözleşme Numarası:

Müşteri Adresi:

IBM Adresi: