

Hizmet Tanımı

IBM Financial Crimes Insight (IBM Mali Suçlar İlgörüsü)

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

1. Bulut Hizmeti

1.1 Olanaklar

Müşteri, aşağıda belirtilen mevcut olanaklar arasından seçim yapabilir.

1.1.1 IBM Financial Crimes Insight Basic (IBM Mali Suçlar İlgörüsü - Temel)

Bu Bulut Hizmeti, Financial Crimes Insights olanaklarının temel aldığı ortak bir dizi hizmet ve ortak bir altyapı sağlar. IBM Financial Crimes Insight, olanaklar arasında gerekli bütünleştirmeyi sağlayarak Müşterilerin mali suçlara karşı sunulan bütünlük olanaklardan yararlanmasına imkan tanır.

1.1.2 IBM Financial Crimes Insight Advanced (IBM Mali Suçlar İlgörüsü - Gelişmiş)

Bu Bulut Hizmeti, IBM Financial Crimes Insight Basic ile aynı yetenek dizisini sağlar ve aynı zamanda IBM Financial Crimes Insight – Data Science içinde belirtilen yetenekleri de içerir.

IBM Financial Crimes Insight Basic veya IBM Financial Crimes Insight Advanced, Bulut Hizmetinin Eşgörünümünü sağlayan zorunlu bir bileşendir.

1.1.3 IBM Financial Crimes Insight Basic Non-Production (IBM Mali Suçlar İlgörüsü - Temel - Üretim Dışı)

Bu Bulut Hizmeti, Müşterinin, IBM Financial Crimes Insight Non-Production işlevlerine bir bulut olanağı olarak erişmesini sağlar.

1.1.4 IBM Financial Crimes Insight Advanced Non-Production (IBM Mali Suçlar İlgörüsü - Gelişmiş - Üretim Dışı)

Bu Bulut Hizmeti, Müşterinin, IBM Financial Crimes Insight Non-Production işlevlerine bir bulut olanağı olarak erişmesini sağlar.

1.1.5 IBM Financial Crimes Insight Advanced BYOL (IBM Mali Suçlar İlgörüsü - Gelişmiş - Kendi Lisansını Getir)

Bu Bulut Hizmeti, Müşterinin, IBM Financial Crimes Insight Advanced işlevlerine bir bulut olanağı olarak erişmesini sağlar. Kendi Lisansını Getir (BYOL) olanakları, Müşterinin ilgili IBM programlarına yönelik uygun lisans yetkilerini önceden edinmiş olmasını gerektirir. IBM Financial Crimes Insight Advanced BYOL olanağının gerektirdiği IBM Programı, IBM Cloud Pak for Data Financial Crimes Insight'tır.

1.1.6 IBM Financial Crimes Insight Advanced Non-Production BYOL (IBM Mali Suçlar İlgörüsü - Gelişmiş - Üretim Dışı - Kendi Lisansını Getir)

Bu Bulut Hizmeti, Müşterinin, IBM Financial Crimes Insight Advanced Non-Production işlevlerine bir bulut olanağı olarak erişmesini sağlar. Kendi Lisansını Getir (BYOL) olanakları, Müşterinin ilgili IBM programlarına yönelik uygun lisans yetkilerini önceden edinmiş olmasını gerektirir. IBM Financial Crimes Insight Advanced Non-Production BYOL olanağının gerektirdiği IBM Programı, IBM Cloud Pak for Data Financial Crimes Insight for Non-Production Environment'tir.

1.1.7 IBM Financial Crimes Insight for Entity Research Negative News API (IBM Kuruluş Araştırması Olumsuz Haber API'si için Mali Suçlar İlgörüsü)

Bu Bulut Hizmeti, filtre edilmiş ve sıralanmış maddelerden bir liste oluşturarak, potansiyel mali suç riskini ortaya çıkarmak amacıyla, yapılandırılmamış haberleri ve ortamları aramak, analiz etmek ve öncelik sırasına koymak için kognitif bilişim teknolojisini ve gelişmiş analitiği kullanır. Olanak, kuruluşların çağırması veya iş akışlarına ve süreçlerine yerleştirmesi için bir API (uygulama programlama arabirimi) olarak sunulur.

1.1.8 IBM Financial Crimes Insight for Entity Research Enrichment API (IBM Kuruluş Araştırması Zenginleştirme API'si İçin Mali Suçlar İlgörüsü)

Bu Bulut Hizmeti, kuruluşların, varlık veya müşteri kayıtlarını güncel tutarak ve bir varlığın potansiyel mali suç riskini ortaya çıkararak bir varlığı daha iyi anlamalarına yardımcı olunmasına destek olan yapılandırılmış kaynaklardan veriler toplamak için kognitif bilişim teknolojisini kullanır. Varlıklar; müşterileri, karşı tarafları veya yüklenicileri içerebilir. Olanak, kuruluşların çağırması veya iş akışlarına ve süreçlerine yerleştirmesi için bir API (uygulama programlama arabirimi) olarak sunulur.

1.2 İsteğe Bağlı Hizmetler

Müşterinin IBM Financial Crimes Insight veya IBM Financial Crimes Insight Non-Production aboneliğine ek olarak aşağıdaki Bulut Hizmetlerinden birine de abone olması gerekir:

1.2.1 IBM Financial Crimes Insight Data Science (IBM Mali Suçlar İlgörüsü - Veri Bilimi)

Bu Bulut Hizmeti, veri hazırlama; modelleri oluşturma, eğitme ve yönetme yetenekleri ve bunların yanı sıra kurumsal veri ve yapay zeka modeli yönetişimini, kalitesini ve işbirliğini yönetmek için bir veri kataloğu sağlar.

1.2.2 IBM Financial Crimes Insight for Anti-Money Laundering (IBM Kara Para Aklamaya İlişkin Mali Suçlar İlgörüsü)

IBM Financial Crimes Insight for Anti-Money Laundering (FCI for AML), mali etkinliği izlemek ve Müşterinin, kuruluşların kara para aklama eğilimini tespit etmesine yardımcı olmak amacıyla, gelişmiş analitik katmanlarını uygular. FCI for AML, demografik, davranışsal verileri ve ilişki verilerini kullanarak, müşterinin bilinen risklere yönelik inceleme sürecine yardımcı olur ve ayrıca, gizli risklere ilişkin açıklanabilir içgörüler sağlayarak risk kapsamını da artırabilir.

1.2.3 IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring (IBM Uyarı Önceliğini Belirlemeye İlişkin Mali Suçlar İlgörüsü - Kara Para Aklama İşlemini İzleme)

Bu Bulut Hizmeti, uyarı önceliklerinin belirlenmesi sürecinin sorunsuz hale getirilmesi, yanlış pozitiflerin azaltılması, uyarının oluşturulmasının hızlandırılması ve varlık riskinin daha iyi anlaşılması aracılığıyla karar almanın iyileştirilmesi amacıyla, geçmiş senaryolardaki verileri, bağlamsal kanıtlara ilişkin verilerin birleştirilmesini ve makine öğrenimi yeteneklerini kullanır. Hizmet, Müşterinin mevcut işlem izleme ve vaka yönetimi sistemleri arasına yerleştirilen bir ek bileşendir.

1.2.4 IBM Financial Crimes Insight for Alert Triage – Transaction List Screening (IBM Uyarı Önceliğini Belirlemeye İlişkin Mali Suçlar İlgörüsü - İşlem Listesini Tarama)

Bu Bulut Hizmeti, yapılandırılabilir, genişletilebilir ve API'ye dayalı bir işlem hattını kullanarak ve uyarı verilmiş işlemleri analiz ederek, mevcut yaptırım tarama sistemlerini güçlendirir. İşlem verileri temizlenir, ayrıştırılır, ele alınır ve ardından, sezgisel yöntemler ve kognitif bilişim teknikleri ile işlenir. Sonuçlar, isabetlerin puanlanması, yanlış pozitiflerin belirlenmesi ve bilgiye dayalı, özelleştirilebilir içgörülerin geri sağlanması amacıyla kullanılır.

1.2.5 IBM Financial Crimes Insight for Entity Research (IBM Kuruluş Araştırması İçin Mali Suçlar İlgörüsü)

Bu Bulut Hizmeti, kuruluşlara ve/veya bunlarla iş yapmakla ilgili riske ilişkin anlayışın iyileştirilmesi ve Müşterinizi Tanıyın (KYC; Know Your Customer) etkinliklerinin tamamlanması için gerekli olan sürenin kısaltılması amacıyla ilgili içeriğin yapılandırılmış ve yapılandırılmamış veri kaynaklarından taranması, alınması ve bağlantılı hale getirilmesi için kognitif bilişim teknolojisinden yararlanır. Bu çözüm, çeşitli veri kaynakları birleştirilerek müşterinin bilgileri aramasını ve analiz etmesini otomatikleştirmesine ve standartlaştırmasına yardımcı olur. Bu hizmetin amacı, aramanın ve durum tespiti faaliyetlerinin kolaylaştırılarak tamamlanması aracılığıyla iyileştirilen müşteri deneyimine ek olarak KYC kayıtlarının kalitesinin artırılmasıdır.

Müşteri, aşağıda belirtilen yetki seçenekleri arasından seçim yapabilir:

- IBM Financial Crimes Insight for Entity Research – Enterprise (IBM Kuruluş Araştırması İçin Mali Suçlar İlgörüsü - Kurumsal), her Olay, 5'ten fazla ilgili tarafın incelenmesine olanak tanır.
- IBM Financial Crimes Insight for Entity Research – Advanced (IBM Kuruluş Araştırması İçin Mali Suçlar İlgörüsü - Gelişmiş), her Olay, 5'e kadar ilgili tarafın incelenmesine olanak tanır.
- IBM Financial Crimes Insight for Entity Research – Temel (IBM Kuruluş Araştırması İçin Mali Suçlar İlgörüsü - Gelişmiş), her Olay, 2'ye kadar ilgili tarafın incelenmesine olanak tanır.

İlgili taraf, Madde 4.1'de tanımlandığı şekilde Ana Soruşturma için incelemenin bir parçası olarak araştırılması gereken bir varlıktır (kuruluş veya kişi). Bu, genel olarak organizasyon şemasında yer alan imza sahipleri, memurlar, nihai intifa hakkı sahipleri, ana kuruluş veya yan kuruluş şeklinde olabilir. Hiçbir şüpheye mahal vermemek için, ilgili bir tarafın, ayrı ayrı veya ilişkili üyelerinin araştırılması gereken bir varlık olması halinde, her ayrı veya ilişkili üye de ilgili taraf olarak sayılır.

1.2.6 IBM Financial Crimes Insight for Entity Research with Material Change (IBM Önemli Değişiklik İçeren Kuruluş Araştırması İçin Mali Suçlar İlgörüsü)

Bu Bulut Hizmeti, kuruluşlara ve/veya bunlarla iş yapmakla ilgili riske ilişkin anlayışın iyileştirilmesi ve Müşterinizi Tanıyın (KYC; Know Your Customer) etkinliklerinin tamamlanması için gerekli olan sürenin kısaltılması amacıyla ilgili içeriğin yapılandırılmış ve yapılandırılmamış veri kaynaklarından taranması, alınması ve bağlantılı hale getirilmesi için kognitif bilişim teknolojilerinden yararlanır. Bu çözüm, çeşitli veri kaynakları birleştirilerek müşterinin bilgileri aramasını ve analiz etmesini otomatikleştirmesine ve standartlaştırmasına yardımcı olur. Bu hizmetin amacı, aramanın ve durum tespiti faaliyetlerinin kolaylaştırılarak tamamlanması aracılığıyla iyileştirilen müşteri deneyimine ek olarak KYC kayıtlarının kalitesinin artırılmasıdır. Bu, varlıkların herhangi bir önemli fark için zaman planı üzerinde incelenmesine ve analistin incelemek üzere uyarılmasına olanak tanıyan, Önemli Değişiklik işlevselliğini içerir.

Müşteri, aşağıda belirtilen yetki seçenekleri arasından seçim yapabilir:

- IBM Financial Crimes Insight for Entity Research – Enterprise (IBM Kuruluş Araştırması İçin Mali Suçlar İlgörüsü - Kurumsal), her Olay, 5'ten fazla ilgili tarafın incelenmesine olanak tanır.
- IBM Financial Crimes Insight for Entity Research – Advanced (IBM Kuruluş Araştırması İçin Mali Suçlar İlgörüsü - Gelişmiş), her Olay, 5'e kadar ilgili tarafın incelenmesine olanak tanır.
- IBM Financial Crimes Insight for Entity Research – Temel (IBM Kuruluş Araştırması İçin Mali Suçlar İlgörüsü - Gelişmiş), her Olay, 2'ye kadar ilgili tarafın incelenmesine olanak tanır.

İlgili taraf, Madde 4.1'de tanımlandığı şekilde Ana Soruşturma için incelemenin bir parçası olarak araştırılması gereken bir varlıktır (kuruluş veya kişi). Bu, genel olarak organizasyon şemasında yer alan imza sahipleri, memurlar, nihai intifa hakkı sahipleri, ana kuruluş veya yan kuruluş şeklinde olabilir. Hiçbir şüpheye mahal vermemek için, ilgili bir tarafın, ayrı ayrı veya ilişkili üyelerinin araştırılması gereken bir varlık olması halinde, her ayrı veya ilişkili üye de ilgili taraf olarak sayılır.

1.2.7 IBM Financial Crimes Insight for Claims Fraud – Property and Casualty (IBM Ödeme Taleplerine İlişkin Dolandırıcılık İçin Mali Suçlar İlgörüsü - Mal ve Kaza)

Bu Bulut Hizmeti, kuruluşların müşterileri, sağlık hizmetleri sağlayıcıları ya da diğer kurumlar tarafından gönderilen sahtekârlık amaçlı ödeme taleplerinden kaynaklanan riski saptamak için verileri analiz etmesine, soruşturma yaşam döngüsünün tamamını yönetmesine ve sonuçları rapor etmesine yardımcı olan bir olanaktır.

1.2.8 IBM Financial Crimes Insight for Claims Fraud – Investigation (IBM Ödeme Taleplerine İlişkin Dolandırıcılık İçin Mali Suçlar İlgörüsü - Soruşturma)

Bu Bulut Hizmeti, kuruluşların şüpheli faaliyetlere ve potansiyel dolandırıcılığa ilişkin soruşturmanın yaşam döngüsünün tamamını yönetmesine yardımcı olur.

1.2.9 IBM Electronic Communication Surveillance Analytics on Cloud

Bu Bulut Hizmeti, finansal hizmet kuruluşlarının, çeşitli şüpheli iletişim kalıplarını saptamak için çalışanların birden fazla kanaldaki etkileşim verilerini etkili bir şekilde analiz etmelerine ve izlemelerine yardımcı olmaya yönelik bir araçtır. Bu araç, piyasadaki kötüye kullanım ve manipülasyonlarla ilgili sahte davranışlara ilişkin çeşitli kalıpların saptanmasına yardımcı olur. Bu araç, metin bilgilerini anlamak ve bağlama dayalı olarak belirsiz terimleri ayırt etmek için doğal dil işleme yeteneğinden yararlanır. Aynı zamanda, iletişimlerin analiz edilmesi için kullanılabilen duygu ve düşünce analizi yeteneklerini de kullanır. Bu yetenekler, kişilerin kişilik niteliklerini ortaya çıkarma amacı taşımaz ve bunu yapmaz. Bu analizin sonuçları, genel akıl yürütme motoruna gönderilir ve böylece çeşitli içgörüler birbiriyle bağlantılı hale getirilir ve uyumluluk görevlerine riskler konusunda tahminler sağlanır.

1.2.10 IBM Voice Surveillance Analytics on Cloud (Bulut Üzerinde IBM Ses Gözetim Analitiği)

Bu Bulut Hizmeti, finansal hizmet kuruluşlarının, şüpheli etkinliklerin saptanması için birden fazla kanaldaki çalışanların sesli iletişimlerini analiz edip izlemesine yardımcı olan bir araçtır. Bu araç, dil bilgisini ve dil yapısını saptamak üzere makine öğreniminden yararlanarak insan sesini yazılı metne çevirmek için konuşmayı metne dönüştürme teknolojisini kullanır. Bu araç, konuşmanın metne

dönüştürülmüş hali ile telefon sisteminin oluşturduğu zengin meta veriler arasında bağlantı kurar ve ilgilenilen sesli sohbetleri hızlı ve kolay aramak ve kayıttan izlemek için metne Speaker Diarisation uygular. Konuşmanın metne dönüştürülmüş hali, meta verilerle birlikte Müşteriye iyi tanımlanmış biçimde sunulur. Bu araç ek seçenekler olarak konuları, tonları, duygu ve hisleri saptamak için içerik ve dilbilimi analizinden anlamsal meta veriler çıkarmak amacıyla doğal dil işlemeyi kullanabilir. Bu yetenekler, kişilerin kişilik niteliklerini ortaya çıkarma amacı taşımaz ve bunu yapmaz. Konuşmayı metne dönüştürme işleminin tamamı, mükerrer dosyaların ve video metni dosyalarının depolanmasını azaltmak için "bellek içinde" gerçekleştirilir ve işleme sonrasında Bulutta hiçbir ses verisi depolanmaz.

1.2.11 IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics (IBM Yürütme İzlemeye İlişkin Mali Suçlar İlgörüsü - Şikayet Analitiği)

Bu Bulut Hizmeti, kuruluşların şikayetleri, iddiaları ve diğer faaliyetleri belirlemesini, bir araya getirmesini ve kategorize etmesini sağlar. Bu araç, yasal düzenlemelerle ilgili artan beklentileri karşılamak için ortaya çıkan sorunlar hakkında içgörüler sağlar. Bu araç, geleneksel sistemlerin atlayabileceği şikayetleri belirlemek ve analiz etmek için gelişmiş analitikten yararlanır. Müşteri verileri, e-postalar, hizmet notları, sosyal medya şikayetleri ve ses kayıtları gibi yapılandırılmış ve yapılandırılmamış olan verileri de alabilir. Daha sonra, sistemsel riskleri belirlemek amacıyla şikayetleri bir araya getirip zenginleştirmek için kognitif yetenekleri kullanır. Bu araç aynı zamanda değişiklikleri ve eğilimleri izlemek amacıyla dinamik segmentasyon ve zaman serisi profili oluşturma işlemlerini de uygular.

Müşterinin IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics'i kullanabilmesi için aynı zamanda IBM Electronic Communication Surveillance Analytics on Cloud veya IBM Voice Surveillance Analytics on Cloud ürünlerinden birine de abone olması gerekir.

1.2.12 IBM Electronic Communication Surveillance Analytics on Cloud BYOL (Bulut Üzerinde IBM Elektronik İletişim Gözetim Analitiği - Kendi Lisansını Getir)

Bu Bulut Hizmeti, Müşterinin, IBM Electronic Communication Surveillance Analytics on Cloud işlevlerine bir bulut olanağı olarak erişmesini sağlar. Kendi Lisansını Getir (BYOL) olanakları, Müşterinin ilgili IBM programlarına yönelik uygun lisans yetkilerini önceden edinmiş olmasını gerektirir. IBM Electronic Communication Surveillance Analytics on Cloud BYOL olanağının gerektirdiği IBM Programı, IBM Financial Crimes Insight for Conduct Surveillance Software – Electronic Communication'dır.

1.2.13 IBM Voice Surveillance Analytics on Cloud BYOL (Bulut Üzerinde IBM Ses Gözetim Analitiği - Kendi Lisansını Getir)

Bu Bulut Hizmeti, Müşterinin, IBM Voice Surveillance Analytics on Cloud işlevlerine bir bulut olanağı olarak erişmesini sağlar. Kendi Lisansını Getir (BYOL) olanakları, Müşterinin ilgili IBM programlarına yönelik uygun lisans yetkilerini önceden edinmiş olmasını gerektirir. IBM Voice Surveillance Analytics on Cloud BYOL olanağının gerektirdiği IBM Programı, IBM Financial Crimes Insight for Conduct Surveillance Software – Voice'tur.

1.2.14 IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics BYOL (IBM Yürütme İzlemeye İlişkin Mali Suçlar İlgörüsü - Şikayet Analitiği - Kendi Lisansını Getir)

Bu Bulut Hizmeti, Müşterinin, IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics işlevlerine bir bulut olanağı olarak erişmesini sağlar. Kendi Lisansını Getir (BYOL) olanakları, Müşterinin ilgili IBM programlarına yönelik uygun lisans yetkilerini önceden edinmiş olmasını gerektirir. IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics BYOL olanağının gerektirdiği IBM Programı, IBM Financial Crimes Insight for Conduct Surveillance Software – Complaint Analytics'tir.

1.3 Hızlandırma Hizmetleri

1.3.1 IBM Financial Crimes Insight Set-up (IBM Mali Suçlar İlgörüsü - Kurulum)

İlgili Bulut Hizmetinin kullanılmak üzere Müşteriye tahsis edilmesi için aşağıdaki kurulum hizmetleri gereklidir:

- IBM Financial Crimes Insight for Anti-Money Laundering (IBM Kara Para Aklamaya İlişkin Mali Suçlar İlgörüsü - Kurulum)
- IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring Set-up (IBM Uyarı Önceliğini Belirlemeye İlişkin Mali Suçlar İlgörüsü - Kara Para Aklama İşlemini İzleme - Kurulum)

- IBM Financial Crimes Insight for Alert Triage – Transaction List Screening Set-up (IBM Uyarı Önceliğini Belirlemeye İlişkin Mali Suçlar İlgörüsü - İşlem Listesini Tarama - Kurulum)
- IBM Financial Crimes Insight for Entity Research – Enterprise Set-up (IBM Kuruluş Araştırması İçin Mali Suçlar İlgörüsü - Kurumsal Kurulum)
- IBM Financial Crimes Insight for Entity Research – Advanced Set-up (IBM Kuruluş Araştırması İçin Mali Suçlar İlgörüsü - Gelişmiş Kurulum)
- IBM Financial Crimes Insight for Entity Research – Basic Set-up (IBM Kuruluş Araştırması İçin Mali Suçlar İlgörüsü - Temel Kurulum)
- IBM Financial Crimes Insight for Entity Research with Material Change – Enterprise Set-up (IBM Önemli Değişiklik İçeren Kuruluş Araştırması İçin Mali Suçlar İlgörüsü - Kurumsal Kurulum)
- IBM Financial Crimes Insight for Entity Research with Material Change – Advanced Set-up (IBM Önemli Değişiklik İçeren Kuruluş Araştırması İçin Mali Suçlar İlgörüsü - Gelişmiş Kurulum)
- IBM Financial Crimes Insight for Entity Research with Material Change – Basic Set-up (IBM Önemli Değişiklik İçeren Kuruluş Araştırması İçin Mali Suçlar İlgörüsü - Temel Kurulum)
- IBM Financial Crimes Insight for Entity Research Negative News API Set-up (IBM Kuruluş Araştırması Olumsuz Haber API'si İçin Mali Suçlar İlgörüsü - Kurulum)
- IBM Financial Crimes Insight for Entity Research Enrichment API Set-up (IBM Kuruluş Araştırması Zenginleştirme API'si İçin Mali Suçlar İlgörüsü - Kurulum)
- IBM Financial Crimes Insight for Claims Fraud – Property and Casualty Set-up (IBM Ödeme Taleplerine İlişkin Dolandırıcılık İçin Mali Suçlar İlgörüsü - Mal ve Kaza Kurulumu)
- IBM Financial Crimes Insight for Claims Fraud – Investigation Set-up (IBM Ödeme Taleplerine İlişkin Dolandırıcılık İçin Mali Suçlar İlgörüsü - Soruşturma Kurulumu)
- IBM Surveillance Insight for Financial Services on Cloud Set-up (IBM Bulut Üzerinde Finansal Hizmetler için Gözetim İlgörüler - Kurulum)

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 saklanması 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://www.ibm.com/dpa/dpl> adresinde belirtilen diğer veri koruma kanunlarının geçerli olması halinde ve geçerli olduğu ölçüde, Veri İşleme Ek Sözleşmesi geçerli olur.

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=14BD7780D65B11E99EAF519926DF897>

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'dan daha az	%2
%99,0'dan az	%5

Kullanılabilirlik	Alacak (aylık abonelik ücretine oranı*)
%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.

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.
- Eşgörünüm, Bulut Hizmetlerinin belirli bir yapılandırmasına olan her erişimi ifade eder.
- Olay, Bulut Hizmetleri tarafından işlenen veya Bulut Hizmetlerinin kullanımıyla bağlantılı belirli bir olayın gerçekleşmesini ifade eder.
 - IBM Financial Crimes Insight for Anti-Money Laundering için bir Olay, bir takvim ayı içinde 10 milyon mali işlemdir.
 - IBM Financial Crimes Insight for Claims Fraud – Property and Casualty ve IBM Financial Crimes Insight for Claims – Investigation için bir Olay, bir Ödeme Talebinin oluşmasıdır. Bir Ödeme Talebi, teminat kapsamındaki bir zararın ya da olayın karşılanması ya da tazmin edilmesi için bir kuruluşa yönelik olarak yapılan resmi bir talebe ilişkin bir dizi yönergedir.
 - IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring için bir Olay, bir takvim ayı içerisinde kaynak sistemden Bulut Hizmetine işlenen bağımsız bir uyarı / olaydır. Genellikle kaynak sistem, bir işlem izleme sistemi veya vaka yönetimi sistemidir.
 - IBM Financial Crimes Insight for Alert Triage – Transaction List Screening için bir Olay, bir takvim ayı içerisinde kaynak sistemden Bulut Hizmetine işlenen 1.000 adede kadar bağımsız uyarıdır. Genellikle kaynak sistem, bir işlem izleme sistemi veya vaka yönetimi sistemidir.
 - IBM Financial Crimes Insight for Entity Research ve IBM Financial Crimes Insight for Entity Research with Material Change için bir Olay, bir takvim ayında, yinelenen aynı aramalar da dahil olmak üzere, Bulut Hizmeti tarafından işlenen herhangi bir ana soruşturmadır. Bir ana soruşturma, başka bir soruşturmaya alt kayıt olarak bağlanmamış olan herhangi bir kayıttır. Bir alt soruşturma, başka şekilde ana soruşturmaya tabi olmayan ilgili bir taraftır (madde 1.2.5'te açıklandığı şekilde).
- Hak Kazanan Katılımcı, Bulut Hizmetleri tarafından yönetilen ya da izlenen herhangi bir hizmet sağlama programına katılmaya hak kazanan bir gerçek ya da tüzel kişidir.
- Öğe, Bulut Hizmeti tarafından işlenen, yönetilen veya Bulut Hizmetinin kullanımıyla bağlantılı olan belirli bir öğenin gerçekleşmesini ifade eder.
 - IBM Voice Surveillance Analytics on Cloud için, Öğe, bir takvim gününde Bulut Hizmeti tarafından işlenen bir saatlik Ses Akışıdır. Ses Akışı, ses iletişimlerinin gerçek zamanlı olarak ya da kayıtlı biçimde yakalanmasıdır.
- Uygulama Programlama Arabirimi (API) Çağrısı, Bulut Hizmetlerinin bir programlanabilir arabirim aracılığıyla başlatılmasıdır.
- Kuruluş Kimliği, Bulut Hizmetleri içinde tanımlanan herhangi bir kuruluşa verilen özgün bir tanıtıcıdır.
- Dijital İleti, Bulut Hizmetleri tarafından yönetilen veya işlenen elektronik iletişimdir.

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 Destekleyici Programlar

IBM Financial Crimes Insight ve IBM Financial Crimes Insight Non-Production, bulut ortamında devreye alınan belirli programlara ("Destekleyici Programlar") erişimi içerir. Müşteri, bu Destekleyici Programları, yalnızca dolandırıcılık, mali suçlar ve uygun olmayan ödemeler ile mücadele etme veya başka şekilde bunları tespit etmeyi ve/veya engellemeyi hedefleyen eylemleri gerçekleştirme amacıyla kullanabilir.

5.1.1 Kullanım Sınırlamaları – Belirli Destekleyici Programlara Özel

Aşağıdaki Destekleyici Programlar, aşağıda belirtilen kısıtlamalar kapsamında sağlanır:

- IBM Watson Studio – Yetki: 5 Eşzamanlı Kullanıcı
- IBM Watson Machine Learning - Yetki: 50 Model
- IBM Openscale – Yetki: 50 Model
- IBM SPSS Modeler Premium – Yetki: 4 Yetkili Kullanıcı
- IBM SPSS Statistics Standard – Yetki: 4 Yetkili Kullanıcı
- Watson Explorer Advanced Edition - Yetki: Aşağıda tanımlandığı şekilde X Gigabayt başına.
Müşterinin aşağıda belirtilenleri analiz etmesine izin verilir:
 - Analitik Dışı Toplama İşlemleriyle birlikte kullanılmak üzere Bulut Hizmetinin havuzunda depolanan tüm İçerikler.
 - Analitik Dışı Toplama İşlemleriyle birlikte kullanılmak üzere Bulut Hizmetinin havuzunda depolanmayan 10 Gigabayt kadar İçerik.
 - Analitik Toplama İşlemleriyle birlikte kullanılmak üzere Bulut Hizmetinin havuzunda depolanan 100 Gigabayt İçerik.
Analitik Toplama İşlemleri, Watson Explorer Annotation Administration Console içinde veya Watson Explorer Content Analytics Administration Console içinde ya da "İçerik Analitiği" veya "Analitik" türü olarak API aracılığıyla oluşturulan toplama işlemlerini ifade eder.
Analitik Dışı Toplama İşlemleri, Program Bulut Hizmeti tarafından analiz edilen diğer tüm içerikleri kapsar.
- IBM InfoSphere DataStage – IBM InfoSphere DataStage and QualityStage Designer Yetkisi: 2 Yetkili Kullanıcı
- IBM Operational Decision Manager – Yetki: Aylık 1 Milyon Kural Kararı ve Aylık 1.000 Yönetilen Karar Çıktısı

Yetki Tanımları

- a. Eşzamanlı Kullanıcı, Destekleyici Programa herhangi bir belirli zaman içinde erişen bir kişidir. Söz konusu kişinin Destekleyici Programa eşzamanlı olarak birden çok kez erişip erişmediğinden bağımsız olarak, bu kişi yalnızca tek bir Eşzamanlı Kullanıcı olarak değerlendirilir.
- b. Model, Destekleyici Programda benzetim ve açıklama yapmak ve tahminde bulunmak için kullanılan temel veri veya veri oluşturma süreciyle ilgili matematiksel bir model veya algoritmadır.
- c. Yetkili Kullanıcı, Destekleyici Programa doğrudan veya dolaylı olarak herhangi bir araçla (örneğin, bir multipleks programı, aygıtı veya uygulama sunucusu aracılığıyla) herhangi bir şekilde erişme yetkisine sahip olan tek bir kullanıcıdır.
- d. Gigabayt (GB), Destekleyici Program tarafından analiz edilen, işlenen ya da Destekleyici Program dahilinde kullanılan, depolanan ya da yapılandırılan 2 üssü 30 veri baytını ifade eder.
- e. Aylık Kural Kararları, bir takvim ayı içinde, Destekleyici Program tarafından yürütülen ya da işlenen bir kural yürütme sunucusundan bir kural grubunu başlatmanın sonucudur.
- f. Aylık Yönetilen Karar Çıktıları, herhangi bir takvim ayında Destekleyici Program tarafından yönetilen bir nesnedir.

5.2 IBM Financial Crimes Insight BYOL için geçerli koşullar

Kendi Lisansını Getir (BYOL) olanakları, Müşterinin aşağıdaki tabloda tanımlanan ilgili IBM programlarına yönelik uygun lisans yetkilerini önceden edinmiş olmasını gerektirir. Müşterinin Kendi Lisansını Getir (BYOL) olanağına ilişkin yetkileri, Müşterinin aşağıda belirtilen oranlardaki ilgili IBM programı yetkilerini aşamaz.

Kendi Lisansını Getir olanağı, ilgili IBM programına ilişkin Abonelik ve Destek hizmetlerini içermez. Müşteri, ilgili IBM programı için geçerli (1) lisans yetkilerini ve (2) Abonelik ve Desteği edinmiş olduğunu beyan eder. Müşterinin, Kendi Lisansını Getir olanağı yetkileriyle bağlantılı olarak kullanılan IBM programı yetkileri için mevcut Abonelik ve Destek ilişkisini Kendi Lisansını Getir olanağının abonelik süresi boyunca sürdürmesi gerekir. Müşterinin ilgili IBM programını kullanma lisansı veya ilgili IBM programına ilişkin Abonelik ve Destek hizmetleri sona erdirilirse, Kendi Lisansını Getir olanağını kullanma hakkı da sona erecektir.

Müşteri, aşağıda belirtilen dönem ("Eşzamanlı Kullanım Dönemi") için Kendi Lisansını Getir olanağını kullanımı ile eşzamanlı olarak ilgili IBM programını devreye almak amacıyla Kendi Lisansını Getir olanağının kullanımı için uygulanan ilgili IBM programına ilişkin yetkileri kullanmaya devam edebilir: (3) yıldan az abonelik süresine sahip olan Müşteriler için, Müşterinin Kendi Lisansını Getir olanağına ilk aboneliğinin başlangıcından itibaren en fazla doksan (90) gün; üç (3) veya 3 yıldan uzun abonelik süresine sahip olan Müşteriler için, Müşterinin Kendi Lisansını Getir olanağına ilk aboneliğinin başlangıcından itibaren en fazla bir (1) yıl. Eşzamanlı Kullanım süresi sona erdikten sonra, Müşterinin Kendi Lisansını Getir olanağını kullandığı süre boyunca, Kendi Lisansını Getir olanağının kullanımı için geçerli olan ilgili IBM programına yönelik Müşteri yetkileri askıya alınır ve Müşteri, ilgili IBM programını devreye almak için söz konusu yetkileri daha fazla kullanamaz (belirtilen her tür istisnaya tabi olarak).

Aşağıdaki tabloda, belirtilen ilgili yetki kapsamında Kendi Lisansını Getir olanağının kullanımı için gereken ilgili IBM programı yetkilerinin oranı özetlenmiştir. Müşteri, Kendi Lisansını Getir olanağını elde ettiğinde ve Müşterinin Kendi Lisansını Getir olanağını kullandığı süre boyunca, Kendi Lisansını Getir olanağının kullanımı için geçerli olan ilgili IBM programına yönelik Müşteri yetkileri askıya alınır ve Müşteri, ilgili IBM programını devreye almak için söz konusu yetkileri daha fazla kullanamaz (belirtilen her tür istisnaya tabi olarak).

İlgili IBM Programı	Kendi Lisansını Getir Olanağı	Oran n/m*
IBM Cloud Pak for Data Financial Crimes Insight	IBM Financial Crimes Insight BYOL (IBM Mali Suçlar İçgörüsü - Kendi Lisansını Getir)	Oran: 1 Kurulum / 1 Eşgörünüm
IBM Cloud Pak for Data Financial Crimes Insight for Non-Production Environment	IBM Financial Crimes Insight Non-Production BYOL (IBM Mali Suçlar İçgörüsü - Üretim Dışı - Kendi Lisansını Getir)	Oran: 1 Kurulum / 1 Eşgörünüm
IBM Financial Crimes Insight for Conduct Surveillance Software – Electronic Communication (IBM İzleme Yürütme Yazılımlarına İlişkin Dolandırıcılık için Mali Suçlar İçgörüsü - Elektronik İletişim)	IBM Electronic Communication Surveillance Analytics on Cloud BYOL (Bulut Üzerinde IBM Elektronik İletişim Gözetim Analitiği - Kendi Lisansını Getir)	Kümülatif Oranlar: Seviye 1 (1-100 Kaynak Değer Birimi): ● 1 Kaynak Değer Birimi / 1 Hak Kazanan Katılımcı Seviye 2 (101-235 Kaynak Değer Birimi): ● 0,9 Kaynak Değer Birimi / 1 Hak Kazanan Katılımcı Seviye 3 (236-435 Kaynak Değer Birimi): ● 0,8 Kaynak Değer Birimi / 1 Hak Kazanan Katılımcı Seviye 4 (436-585 Kaynak Değer Birimi): ● 0,6 Kaynak Değer Birimi / 1 Hak Kazanan Katılımcı Seviye 5 (586-835 Kaynak Değer Birimi): ● 0,5 Kaynak Değer Birimi / 1 Hak Kazanan Katılımcı Seviye 6 (836-1135 Kaynak Değer Birimi): ● 0,4 Kaynak Değer Birimi / 1 Hak Kazanan Katılımcı

İlgili IBM Programı	Kendi Lisansını Getir Olanağı	Oran n/m*
		Seviye 7 (1136+ Kaynak Değer Birimi): ● 0,3 Kaynak Değer Birimi / 1 Hak Kazanan Katılımcı
IBM Financial Crimes Insight for Conduct Surveillance Software – Voice (IBM İzleme Yürütme Yazılımlarına İlişkin Dolandırıcılık İçin Mali Suçlar İçgörüsü - Ses)	IBM Voice Surveillance Analytics on Cloud BYOL (Bulut Üzerinde IBM Ses Gözetim Analitiği - Kendi Lisansını Getir)	Kümülatif Oranlar: Seviye 1 (1-100 Kaynak Değer Birimi): ● 1 Kaynak Değer Birimi / 1 Öğe Seviye 2 (101-235 Kaynak Değer Birimi): ● 0,9 Kaynak Değer Birimi / 1 Öğe Seviye 3 (236-435 Kaynak Değer Birimi): ● 0,8 Kaynak Değer Birimi / 1 Öğe Seviye 4 (436-585 Kaynak Değer Birimi): ● 0,6 Kaynak Değer Birimi / 1 Öğe Seviye 5 (586-835 Kaynak Değer Birimi): ● 0,5 Kaynak Değer Birimi / 1 Öğe Seviye 6 (836-1135 Kaynak Değer Birimi): ● 0,4 Kaynak Değer Birimi / 1 Öğe Seviye 7 (1136+ Kaynak Değer Birimi): ● 0,3 Kaynak Değer Birimi / 1 Öğe
IBM Financial Crimes Insight for Conduct Surveillance Software – Complaint Analytics (IBM İzleme Yürütme Yazılımlarına İlişkin Dolandırıcılık İçin Mali Suçlar İçgörüsü - Şikayet Analitiği)	IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics BYOL	Kümülatif Oranlar: Seviye 1 (1-100 Kaynak Değer Birimi): ● 5.000 Kaynak Değer Birimi (RVU) / 1 Dijital İleti Seviye 2 (101-235 Kaynak Değer Birimi): ● 4.500 Kaynak Değer Birimi (RVU) / 1 Dijital İleti Seviye 3 (236-435 Kaynak Değer Birimi): ● 4.000 Kaynak Değer Birimi (RVU) / 1 Dijital İleti Seviye 4 (436-585 Kaynak Değer Birimi): ● 3.000 Kaynak Değer Birimi (RVU) / 1 Dijital İleti Seviye 5 (586-835 Kaynak Değer Birimi): ● 2.500 Kaynak Değer Birimi (RVU) / 1 Dijital İleti Seviye 6 (836-1135 Kaynak Değer Birimi): ● 2.000 Kaynak Değer Birimi (RVU) / 1 Dijital İleti Seviye 7 (1136+ Kaynak Değer Birimi): ● 1.500 Kaynak Değer Birimi (RVU) / 1 Dijital İleti

* "Oran n/m", ilişkili IBM programı için belirtilen ölçünün her yetkisi ('n') için; Müşterinin bu yetkileri, Kendi Lisansını Getir olanağı için belirtilen ölçünün belirtilen yetki ('m') sayısına uygulayabileceği anlamına gelir. İlişkili IBM Programından BYOL Olanağına dönüştürme işlemi tam sayıyla sonuçlanmazsa, en yakın tam sayıya yuvarlanır.

Örnek 1:

Hak Kazanan Katılımcı için 710 Kaynak Değer Birimi (Saniye Başına Olay)

(IBM Trade Surveillance Analytics ve IBM Electronic Communication Surveillance Analytics için geçerlidir)

Seviye 1: 710>100 ise, 100/1 = 100 Saniye Başına Olay

Seviye 2: 710>235 ise, (235-100)/.9 = +150 Saniye Başına Olay

Seviye 3: 710>435 ise, (435-235)/.8 = +250 Saniye Başına Olay

Seviye 4: 710>585 ise, (585-435)/.6 = +250 Saniye Başına Olay

Seviye 5: 710>835 değilse, (710-585)/.5 = +250 Saniye Başına Olay

Toplam Saniye Başına Olay: 100 + 150 + 250 + 250 + 250 = 1000 Saniye Başına Olay

Örnek 2:

500.000 Kaynak Değer Birimi (RVU) - Dijital İleti (5.000'lik paket)

(IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics için geçerlidir)

Tier 1: 500.000>100 ise, 100/5.000 = .02 Dijital İleti

Tier 2: 500.000>235 ise, (235-100)/4.500 = + .03 Dijital İleti

Tier 3: 500.000>435 ise $\rightarrow (435-235)/4.000 = + .05$ Dijital İleti
Tier 4: 500.000>585 ise $\rightarrow (585-435)/3.000 = + .05$ Dijital İleti
Tier 5: 500.000>835 ise $\rightarrow (835-585)/2.500 = + .1$ Dijital İleti
Tier 6: 500.000>1.135 ise $\rightarrow (1.135-835)/2.000 = + .15$ Dijital İleti
Tier 7: 500.000>1.135 ise $\rightarrow (500.000-1135)/1.500 = + 99,6$ Dijital İleti
Toplam Dijital İleti: $.02 + .03 + .05 + .1 + .15 + 99,6 = 100$ Dijital İleti

5.3 Arama Sonuçları

Müşteri, işbu belgede açıklanan Bulut Hizmetlerinin bir parçası olarak oluşturulan raporlarda elde edilen ve bu raporlarda atıfta bulunulan arama sonuçlarının ("Arama Sonuçları"), üçüncü kişilerin sahip olduğu verileri veya içeriği içerebileceğini ve IBM'in söz konusu Arama Sonuçlarına veya içeriğe ilişkin herhangi bir lisansı veya başka herhangi bir hakkı satmadığını veya sağlamadığını kabul eder. Arama Sonuçları, bu Bulut Hizmetleri için içerik olarak değerlendirilir.

5.4 Bulut Hizmetinin Süresinin Sona Ermesi

Müşteri, Bulut Hizmetinin kullanım süresi sona ermeden veya sona erdirilmeden önce, veri çıkarmak için Bulut Hizmetinin sağlanan raporlama veya dışa aktarma özelliklerinden herhangi birini kullanabilir. Özel veri çıkarma hizmetleri ayrı bir sözleşme kapsamında sağlanır.

Bulut Hizmetinin kullanım süresinin sona ermesinden veya sona erdirilmesinden sonra 30 gün içinde Müşteriden bu yönde bir istek alması durumunda, IBM, Müşteri içeriğinin bir elektronik kopyasını yerel uygulama biçiminde Müşteriye sağlayacaktır.

Kabul eden:

{Müşteri Şirketinin Ticari Unvanı adına} ("Müşteri")

Kabul eden:

{İlgili IBM Şirketinin Ticari Unvanı adına} ("IBM")

İmza _____

Yetkili imza

İmza _____

Yetkili imza

Unvan:

Unvan:

İsim (el yazısı veya daktiloyla):

İsim (el yazısı veya daktiloyla):

Tarih:

Tarih:

Müşteri Numarası:

Sözleşme Numarası:

Müşteri Adresi:

IBM Adresi: