IBM Trusteer Pinpoint Assure

본 서비스 명세서는 본 클라우드 서비스에 대해 설명합니다. 관련 주문 서류에서는 고객의 주문에 대한 가격 책정과 추가적인 세부사항을 제공합니다.

1. 클라우드 서비스

IBM Trusteer Pinpoint Assure 는 사기적 의도가 있는 개인이 도용된 ID 를 사용하거나 거짓 정보를 실제 ID 에 추가하거나 게스트 트랜잭션 작성, 신규 계정 작성, 기존 고객을 대신한 신규 디지털 계정 작성 등에 사용할 수 있는 합성 ID 를 작성하지 못하도록 하기 위해 설계된 강력한 보안의 레이어드 솔루션입니다.

1.1 오퍼링

1.1.1 IBM Trusteer Pinpoint Assure

이 서비스는 의심스러운 활동에 플래그를 지정하고 새 계정 작성/등록 프로세스에서 경보를 생성합니다. 이 서비스는 계정 등록 프로세스를 모니터하여 사기성이 있는 활동을 파악하고 TMA(Trusteer Management Application)에서 사용할 수 있는 이용 보고서를 통해 신규 계정이 mule 계정이거나 사기에 사용되는지에 대해 초기 경고 신호를 제공합니다. IBM Trusteer Pinpoint Detect 및 IBM Trusteer Pinpoint Verify 는 TMA 로그인의 일부로 사용됩니다.

IBM Trusteer Pinpoint Assure 는 연간 연결 100 회선 단위의 팩으로 제공됩니다.

1.2 선택적 서비스

1.2.1 IBM Trusteer Pinpoint Assure Application

애플리케이션에서 IBM Trusteer Pinpoint Assure 를 배치하기 위해서는 IBM Trusteer Pinpoint Assure Application 에 대한 권한이 필요합니다.

IBM Trusteer Pinpoint Assure 는 애플리케이션별로 구입할 수 있습니다.

1.2.2 IBM Trusteer Mobile Carrier Intelligence

고객이 이 클라우드 서비스에 사용등록하기 전에 먼저 IBM Trusteer Pinpoint Assure 의 당시 유효한 사용등록을 보유하고 있어야 합니다.

이 클라우드 서비스는 해당 클라우드 서비스 중 하나에 제공된 휴대전화 번호에 대한 추가 정보와 컨텍스트를 제공하여 특정 세션의 부정 행위 위험을 파악함으로써 IBM Trusteer Pinpoint Assure 를 개선합니다. 고객이 클라우드 서비스에 조회하여 해당 번호와 관련된 통신사 정보와 같은 특정 휴대전화 번호에 대한 특성을 알아볼 수 있습니다.

이 클라우드 서비스에서 제공하는 휴대전화 번호 관련 데이터("모바일 인텔리전스")는 고객 내부 용도로만 사용할 수 있으며 30 일 동안만 보존할 수 있습니다. 고객은 해당 기간 이후 동일한 휴대전화 번호에 대해 클라우드 서비스에 다시 조회해야 해당 번호에 대해 모바일 인텔리전스를 얻을 수 있으며, 이전 조회로부터 받은 모바일 인텔리전스를 다시 사용할 수 없습니다. 위에서 허용된 경우를 제외하고 고객은 모든 데이터 마이닝과 전체 또는 부분적으로 연관하여 또는 모든 모바일 인텔리전스를 보관하기 위해 캐시하거나 재사용하거나 사용할 수 없습니다.

2. 데이터 처리 및 보호 데이터 시트

IBM 데이터 처리 부칙(Data Processing Addendum: DPA)(http://ibm.com/dpa 참조) 및 아래 링크의 데이터 처리 및 보호 데이터 시트(Data Processing and Protection Data Sheet(s))(데이터 시트(들) 또는 DPA 별표(들)로 참조됨)는 클라우드 서비스에 대한 추가적인 데이터 보호 정보와 처리할 수 있는 컨텐츠의 유형, 관련 처리 활동, 데이터 보호 기능 및 컨텐츠의 보관 및 반환 정보와 관련한 옵션을 제공합니다. DPA 는 컨텐츠에 포함된 개인 데이터에 i) European General Data Protection Regulation

(EU/2016/679)(GDPR) 또는 ii) http://ibm.com/dpa/dpl 에 명시된 기타 데이터 보호법이 적용되는 경우 그 범위에 한해 적용됩니다.

데이터 시트에는 일반적으로 서비스가 배치된 데이터 센터와 관계 없이 IBM(제 3 의 재처리자 포함)이 개인 데이터를 호스트하고 처리하는 모든 위치가 명시됩니다. 서비스가 배치된 데이터 센터별 호스팅 및 처리 위치 목록은 아래 5.1 항 (추가 처리 위치 정보)를 참조하십시오.

IBM Trusteer Assure

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

IBM Trusteer Mobile SDK

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

3. 서비스 레벨(Service Levels) 및 기술 지원

3.1 SLA(Service Level Agreement)

IBM 은 다음 가용성 "서비스 레벨 계약"(이하 SLA)을 고객에게 제공합니다. IBM 은 아래 표와 같이 누적 클라우드 서비스 가용성에 따라 적용 가능한 최대의 보상을 적용합니다. 가용률은 약정 월의 총 시간(분)에서 약정 월의 총 Service Down(분)을 차감한 후 이를 약정 월의 총 시간(분)으로 나누어 산출합니다. Service Down 의 정의, 클레임 절차, 서비스 가용성 문제에 관한 IBM 문의 방법은 IBM Cloud 서비스 지원 핸드북(https://www.ibm.com/software/support/saas_support_overview.html)에서 확인할 수 있습니다.

가용성	크레디트 (월별 사용등록료*의 %)
99.9% 미만	2%
99.0% 미만	5%
95.0% 미만	10%

* 사용등록료는 클레임 대상이 되는 해당 월의 약정 요금입니다.

3.2 기술 지원

지원 문의 상세 정보, 심각도 레벨, 가용성 지원 시간, 응답 시간 및 기타 지원 정보와 절차를 포함하여, 클라우드 서비스에 대한 기술 지원은 IBM 지원 안내서(https://www.ibm.com/support/home/pages/support-guide/ 참조)에서 클라우드 서비스를 선택하면 확인할 수 있습니다.

4. 요금

4.1 청구 체계

클라우드 서비스에 대한 과금 체계는 거래서류에 명시됩니다.

이 클라우드 서비스에는 다음 청구 체계가 적용됩니다.

- 연결(Connection)은 데이터베이스, 애플리케이션, 서버 또는 가용케 되었거나 가용케 되는 기타 유형의 디바이스를 클라우드 서비스에 링크 또는 연관하는 것입니다.
- 애플리케이션은 클라우드 서비스에서 개발되거나 클라우드 서비스에 액세스하도록 가용케 되거나 클라우드 서비스에서 사용된, 고유하게 이름이 지정된 소프트웨어 프로그램입니다.

5. 추가 조항

2019 년 1 월 1 일 이전에 작성된 클라우드 서비스 계약들(또는 동등한 기본 클라우드 계약들)에는 https://www.ibm.com/acs 에서 제공한 조건들이 적용됩니다.

5.1 추가 처리 위치 정보

데이터 시트에 명시된 제 3 의 재처리자에 의한 경우를 포함하여, 개인 데이터의 모든 호스팅 및 처리는 아래 지정된 위치에서 수행됩니다.

독일 데이터 센터를 통해 제공되는 모든 서비스의 경우, IBM 은 개인 데이터의 호스팅과 처리를 IBM 계약 법인의 국가와 다음 국가들로 제한합니다: 독일, 이스라엘, 아일랜드 및 네덜란드.

일본 데이터 센터를 통해 제공되는 모든 서비스의 경우, IBM 은 개인 데이터의 호스팅과 처리를 IBM 계약 법인의 국가와 다음 국가들로 제한합니다: 일본, 이스라엘 및 아일랜드.

미국 데이터 센터를 통해 제공되는 모든 서비스의 경우, IBM 은 개인 데이터의 호스팅과 처리를 IBM 계약 법인의 국가와 다음 국가들로 제한합니다: 미국, 이스라엘, 아일랜드, 싱가포르 및 호주.

위의 위치들 외에 독일, 일본 및 미국 데이터 센터를 통해 제공된 모든 서비스와 관련하여 (1) 지원 데이터는 IBM 의 제 3 의 재처리자로 Salesforce.Com 에 의해 독일과 프랑스에서 호스트되거나 처리될 수 있고 (2) 데이터를 Mobile Carrier Intelligence 공급자에게 전송하기로 선택한 고객의 경우, 개인 데이터는 데이터 시트에 지정된 해당 제 3 의 재처리자의 국가에서 호스트되고 처리될 수 있습니다. 데이터 시트의 상반되는 내용에도 불구하고, 전술한 조항의 (2) 항에 지정된 제 3 의 재처리자는 ISO 27001 또는 SOC2 를 준수하지 않을 수 있습니다.

관련 IBM 인력의 가용성, 고객의 위치 및 데이터를 관리하는 데이터 센터에 따라 IBM Trusteer 지원 및 계정 유지보수 서비스도 필요에 맞게 제공될 수 있습니다.

5.2 통합 솔루션

명확히 말해서, Trusteer 브랜드의 다양한 오퍼링들이 하나의 통합된 솔루션을 구성할 수 있습니다. 그러므로 고객이 이러한 클라우드 서비스들 중 하나를 해지하는 경우, IBM 은 본 서비스 명세서 하의 나머지 클라우드 서비스들과 기타 다른 Trusteer 서비스에 관한 서비스 명세서에 따른 그러한 다른 Trusteer 서비스를 고객에게 제공하기 위한 목적으로 고객 데이터를 보관할 수 있습니다.

5.3 배치 과정에서 수집된 데이터

고객은 클라우드 서비스를 배치하는 과정에서 특정 데이터를 IBM 에게 제공하게 될 수 있습니다. 이러한 데이터는 특정 개인을 식별하거나 특정 개인에게 귀속될 수 있는 정보를 포함해서는 안됩니다. 배치 과정에서 IBM 에게 제공된 데이터에 대한 추가 지침은 고객에게 제공되는 Trusteer 배치 가이드라인에서 확인할 수 있습니다.

6. 우선 적용 조항

6.1 데이터 사용

다음이 당사자들 간의 기본 클라우드 서비스 조건 중 컨텐츠 및 데이터 보호 조항에서 상반되는 내용보다 우선하여 적용됩니다: IBM 은 고객의 클라우드 서비스 사용(즉 고객의 컨텐츠(인사이트)에 고유한 사항 또는 달리 고객을 식별할 수 있는 사항)으로부터 발생하는 결과를 활용하거나 공개하지 않습니다. 그러나 IBM 은 클라우드 서비스의 향상을 위해서 클라우드 서비스의 일부로 컨텐츠 및 컨텐츠에서 생성된 기타 정보(인사이트 제외)를 사용합니다. IBM 은 또한 위협 감지 및 보호 용도로 컨텐츠에 내장된 위협 식별자 및 기타 보안 정보를 공유할 수 있습니다.