IBM Trusteer Mobile

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

1. 클라우드 서비스

IBM Trusteer Mobile 은 실시간 디바이스 및 세션 위험을 감지하도록 돕습니다. 이 서비스는 고급 분석 및 실시간 디바이스 위험 감지 기능을 활용하여 내장된 애플리케이션의 무결성을 유지하도록 지원합니다. Trusteer Mobile 은 악성 소프트웨어, Remote Access Trojans, jailbroken/rooted 감지, 오버레이 공격 증거, SMS 도용 앱과 같이, 디바이스의 손상 여부를 확인하기 위해 디바이스를 평가합니다. 추가적인 교차 채널 인디케이터가 동작 이상, 탐색 불일치, 피싱 손상과 같은 고급 기술을 통해 지속적으로 처리됩니다.

1.1 오퍼링

고객은 사용 가능한 다음 오퍼링 중에서 선택할 수 있습니다.

1.1.1 IBM Trusteer Mobile SDK for Business 및/또는 IBM Trusteer Mobile SDK for Retail

IBM Trusteer Mobile SDK 클라우드 서비스는 고객이 클라우드 서비스 커버리지에 등록한 고객의 Business 및/또는 Retail 애플리케이션에 대한 안전한 웹 액세스, 디바이스의 위험 평가 및 피싱 방지를 제공하는 또다른 보호 계층(layer)을 추가하도록 설계되었습니다. 보안 Wi-Fi 감지는 Android 플랫폼에서만 가능합니다.

IBM Trusteer Mobile SDK 클라우드 서비스에는 고객이 클라우드 서비스 커버리지에 등록한 고객의 보호된 독립형 iOS 또는 Android 모바일 애플리케이션에 내장되어 통합이 가능한 IBM Trusteer Mobile SDK 에서 생성한 고유 코드인 "재배포 가능 항목" 또는 "런타임 구성요소"와 함께, 문서, 프로그래밍 고유 소프트웨어 라이브러리 및 기타 관련 파일 및 항목이 포함된 소프트웨어 패키지(IBM Trusteer 모바일 라이브러리라고 함)인 고유 모바일 소프트웨어 개발자 킷(이하 "SDK")이 포함되어 있습니다 (이하 "Client Integrated Mobile App", "고객 통합 모바일 앱").

IBM Trusteer Mobile SDK for Retail 은 적격 참여자 100 명 단위의 팩이나 클라이언트 디바이스 100 대 단위의 팩으로 사용이 가능하며 IBM Trusteer Mobile SDK for Business 는 적격 참여자 10 명 단위의 팩 또는 클라이언트 디바이스 10 대 단위의 팩으로 사용 가능합니다.

고객(과 무제한의 고객의 허가된 직원)은 TMA 를 통해 이벤트 데이터 보고 및 위험 경향 평가를 수신할 수 있습니다. IBM Trusteer Pinpoint Detect 및 IBM Trusteer Pinpoint Verify 는 TMA 로그인의 일부로 사용됩니다. 고객은 고객 통합 모바일 앱을 통해 고객 통합 모바일 앱을 다운로드한 적격 참여자의 모바일 디바이스와 관련된 모바일 디바이스 정보와 위험 분석을 수신할 수 있으며 이를 통해 고객은 이러한 위험에 대한 완화 조치를 수행하는 사기 방지 정책을 구성할 수 있습니다. 본 오퍼링의 목적상, "모바일 디바이스"에는 지원되는 휴대전화와 태블릿만 포함되며 PC 또는 MAC 은 포함되지 않습니다.

고객은 다음을 수행할 수 있습니다.

a. 고객 통합 모바일 앱을 개발하기 위한 목적으로만 IBM Trusteer Mobile SDK 를 내부적으로 사용할 수 있습니다.

b. 고객 통합 모바일 앱에서 분리할 수 없는 방식으로 (오브젝트 코드 형식으로만) 재배포 가능 항목을 내장합니다. 재배포 가능 항목 중 본 라이센스에 따라 수정하거나 병합한 부분에는 본 서비스 명세서의 조건이 적용됩니다.

c. 다음을 전제 조건으로, 적격 참여자의 모바일 디바이스 또는 클라이언트 디바이스 홀더에 다운로드하도록 재배포 가능 항목을 마케팅하고 배포합니다.

- 본 계약에서 구체적으로 허용하는 경우를 제외하고, 고객은 (1) SDK 를 사용, 복사, 수정 또는 배포할 수 없으며 (2) 법률에서 계약상 면제하지 못하게 하고 구체적으로 허용하는 경우를 제외하고, SDK 를 리버스 어셈블, 리버스 컴파일, 달리 변환 또는 리버스 엔지니어링할 수

없고 (3) SDK 를 재라이센스, 임대 또는 리스할 수 없고 (4) 재배포 가능 항목에 포함된 저작권 또는 통지 파일을 제거할 수 없고 (5) 원본 재배포 가능 파일/모듈과 동일한 경로 이름을 사용할 수 없으며 (6) IBM, IBM 라이센스 제공자 또는 판매자의 사전 서면 동의 없이 고객 통합 모바일 앱의 마케팅과 관련하여 IBM, IBM 의 라이센스 제공자 또는 판매자의 이름과 상표를 사용할 수 없습니다.

- 재배포 가능 항목은 고객 통합 모바일 앱(Client Integrated Mobile App)에서 분리할 수 없는 통합된 상태를 유지해야 합니다. 재배포 가능 항목은 오브젝트 코드 양식이어야 하고 SDK 및 관련 문서의 모든 지시사항과 명세를 준수해야 합니다. 고객 통합 모바일 앱에 관한 최종 사용자 라이센스 계약에서는 재배포 가능 항목을 i) 고객 통합 모바일 앱을 사용하기 위한 목적 외의 용도로 사용할 수 없으며 ii) 복사할 수 없으며(백업 용도는 제외) iii) 추가로 배포하거나 이전할 수 없으며 iv) 법률에서 계약상 면제하지 못하게 하고 구체적으로 허용하는 경우를 제외하고 리버스 어셈블, 리버스 컴파일 또는 달리 변환할 수 없다는 것을 최종 사용자에게 통지해야 합니다. 고객의 라이센스 계약은 최소한 본 계약 조건의 수준으로 IBM 을 보호해야 합니다.
- 고객의 지정 모바일 테스트 디바이스에 대한 유닛 테스트 및 내부 개발의 일환으로만 SDK 를 사용할 수 있습니다. 고객은 프로덕션 워크로드를 처리하거나 프로덕션 워크로드를 시뮬레이션하거나 코드, 애플리케이션 또는 시스템의 확장성을 테스트하는 용도로는 SDK 를 사용할 수 없습니다. 고객은 SDK 의 어떠한 부분도 기타 다른 용도를 위해서 사용할 수 없습니다.

고객 통합 모바일 앱의 개발, 테스트 및 지원에 대한 책임은 전적으로 고객이 집니다. 고객은 고객 통합 모바일 앱 및 본 계약에서 허용한 대로 고객이 작성한 재배포 가능 항목의 수정사항에 대한 모든 기술 지원을 제공해야 할 책임이 있습니다.

고객은 클라우드 서비스의 사용을 지원하기 위한 용도로만 재배포 가능 항목과 IBM Security Mobile SDK 를 설치하고 사용할 수 있습니다.

IBM 은 IBM Security Mobile SDK 에 포함된 모바일 도구를 사용하여 애플리케이션 또는 출력을 생성하는 것이 특정 모바일 운영 체제 플랫폼 또는 모바일 디바이스와 기능하거나 상호 운용되거나 호환된다는 것을 보장하지 않습니다.

소스 구성요소 및 샘플 자료 – IBM Trusteer Mobile SDK 에는 소스 코드 양식의 일부 구성요소("소스 구성요소"(Source Components))와 샘플 자료에 해당하는 기타 자료가 포함될 수 있습니다. 고객은 본 계약에 의거한 라이센스 권리의 제한 범위 내에서 사용하는 경우에 한해 내부적인 용도로만 소스 구성요소 및 샘플 자료를 복사하고 수정할 수 있습니다. 단, 고객은 소스 구성요소 및 샘플 자료에 포함된 저작권 정보나 주의사항은 변경하거나 삭제할 수 없습니다. IBM 은 소스 구성요소와 샘플 자료를 지원 의무 없이 "현 상태대로" 제공합니다. Source Components of Sample Materials(소스 구성요소 및 샘플 자료)는 내장 가능 항목(Embeddable)을 CIMA 에 구현하는 방법에 대한 예시로만 제공되며 소스 구성요소 및 샘플 자료는 고객의 개발 환경에서 호환 가능하지 않을 수 있고 CIMA 에서 내장 가능 항목의 테스트 및 구현에 대한 책임은 전적으로 고객이 집니다.

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 Mobile SDK

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

IBM Trusteer Mobile Secure Browser

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

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.

- 적격 참여자(Eligible Participant)는 클라우드 서비스에서 관리하거나 추적하는 서비스 제공 프로그램에 참여할 수 있는 개인이나 법인을 의미합니다.
- 클라이언트 디바이스(Client Device)는 클라우드 서비스에 액세스하는 서버 환경에서 실행 명령, 프로시저 또는 애플리케이션을 요청하거나 수신하는 디바이스입니다.

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 네델란드.

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 서비스의 경우 (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.

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 확인

고객은 i) IBM 또는 IBM 의 외부 감사원이 고객의 본 계약 준수를 확인하기 위해서 합리적으로 필요한 기록 및 시스템 도구 출력물을 유지하고, IBM 의 요청이 있는 경우 그러한 기록과 시스템 도구 출력을 제공하며, ii) 여하한의 필요한 권한을 즉시 주문하고, 해당 시점에 유효한 IBM 요율에 따라 해당 권한에 대해 그리고 이러한 확인 결과 결정된 기타 대금 및 채무에 대해 IBM 이 청구서에 명시한 대로 지급해야 합니다. 이러한 준수 확인 의무는 클라우드 서비스 기간 및 그 후 2 년 간 효력이 유지됩니다.

5.4 배치 과정에서 수집된 데이터

고객은 클라우드 서비스를 배치하는 과정에서 특정 데이터를 IBM 에게 제공하게 될 수 있습니다. 배치 과정에서 고객이 IBM 에게 제공한 데이터에 대한 추가 지침은 고객에게 제공하는 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 서비스 과정에서 고객 식별 항목을 제거하는 조건으로 추가적인 정보의 사용 없이는 여하한 개인 정보가 더 이상 특정 개인에게 귀속될 수 없게 된 컨텐츠 및 컨텐츠에서 발생하는 다른 정보를 사용합니다. IBM 은 연구, 테스트 및 오퍼링 개발 목적으로만 해당 데이터를 사용합니다.