IBM Trusteer Pinpoint Detect

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 는 또다른 보안 계층(layer)을 제공하도록 설계된 클라우드 기반 서비스로, 악성 소프트웨어, 피싱 및 계정 탈취 공격을 감지 및 보완하고자 하는 오퍼링입니다. Trusteer Pinpoint 는 고객이 클라우드 서비스 커버리지에 등록한 Business 및/또는 Retail 애플리케이션과 사기 방지 프로세스에 통합될 수 있습니다.

본 클라우드 서비스에는 다음이 포함됩니다.

a. TMA(Trusteer Management Application) 및 Trustboard:

TMA 는 고객이 경보를 평가하고 분류할 수 있도록 해주는 Trusteer 의 기본 관리 애플리케이션입니다. Trustboard 는 주로 리서치에 사용되는 새로운 관리 애플리케이션입니다. 고객은 TMA 또는 Trustboard 중에서 언제든지 한 번에 하나를 선택하여 사용할 수 있습니다. TMA 및 Trustboard 는 각각 고객(및 고객의 제한없는 수의 허가된 직원)이 다음을 수행할 수 있는 IBM Trusteer 클라우드 호스트 환경에서 제공됩니다. (i) 특정 이벤트 데이터 보고 및 위험 평가 보기 및 다운로드 및 (ii) Pinpoint 오퍼링에서 생성된 위협 피드의 전달에 대한 보기, 등록 및 구성. IBM Trusteer Pinpoint Detect 및 IBM Trusteer Pinpoint Verify 는 TMA 및 Trustboard 로그인의 일부로 사용됩니다.

b. Web Script 및/또는 API:

클라우드 서비스에 액세스하거나 테스트하거나 사용하기 위한 목적의 웹 사이트 배치 용도.

"세션(Session)"은 고객의 애플리케이션(웹 또는 모바일)과 하나 이상의 실시간 위험 평가를 생성하는 클라우드 서비스 간의 상호작용입니다. 세션은 상호작용이 시작되는 시간부터 상호작용이 끝나는 시간까지 측정됩니다. 상호작용의 종료는 다음 이벤트 중 하나가 발생할 때 기록됩니다.

- 애플리케이션의 정상 로그아웃 시 상호작용이 재설정됩니다.
- 브라우저, 애플리케이션 또는 탭이 종료됩니다.
- 쿠키가 삭제됩니다.
- 제한시간이 초과됩니다.

세션에는 로그인, 찾아보기, 체크아웃, 대금지급 설정, 고객의 애플리케이션에서 정의한 기타 활동 등, 여러 가지 활동이 포함될 수 있습니다. 본 클라우드 서비스의 목적상, 하나의 연결(Connection)(아래 정의 참조)은 하나의 세션입니다.

1.1 오퍼링

고객은 사용 가능한 다음 오퍼링 중에서 선택할 수 있습니다.

1.1.1 IBM Trusteer Pinpoint Detect Standard for Retail 및/또는 IBM Trusteer Pinpoint Detect Standard for Business

이 클라우드 서비스는 IBM Trusteer Pinpoint Criminal Detection 과 IBM Trusteer Pinpoint Malware Detection 클라우드 서비스를 결합하여 통합된 단일 솔루션을 제공합니다.

해당 솔루션은 디바이스 ID 를 사용하여 Retail 또는 Business 애플리케이션에 연결하는 브라우저에서 의심되는 계정 탈취 활동의 클라이언트리스(clientless) 감지, 피싱 감지 및 악성 소프트웨어 구동 신임정보 도용 감지를 지원합니다. IBM Trusteer Pinpoint 오퍼링은 또다른 보호 계층(layer)을 제공하며 계정 탈취 시도를 감지하고 (기본 브라우저나 고객 모바일 애플리케이션을 통해) Retail 또는 Business 애플리케이션에 액세스(접근)하는 브라우저 또는 모바일 디바이스의 위험 평가 점수를 고객에게 직접

전달합니다. 이 서비스는 관리 및 비관리 디바이스의 위험을 평가하기 위해서 원격 인력 액세스에도 사용될 수 있습니다.

이 클라우드 서비스에는 프리미엄 지원(아래 기술 지원 조항에서 정의 참조)이 포함되어 있습니다.

이 서비스는 적격 참여자 100 명 또는 연결 100 회선 단위의 팩으로 구매될 수 있습니다.

1.1.2 IBM Trusteer Pinpoint Detect Premium for Retail 및/또는 IBM Trusteer Pinpoint Detect Premium for Business

이 클라우드 서비스는 IBM Trusteer Pinpoint Criminal Detection 과 IBM Trusteer Pinpoint Malware Detection 을 결합하여 통합이 용이한 통일된 단일 솔루션을 제공합니다.

해당 솔루션은 디바이스 ID 를 사용하여 Retail 또는 Business 애플리케이션에 연결하는 브라우저에서 의심되는 계정 탈취 활동의 클라이언트리스(clientless) 감지, 피싱 감지 및 악성 소프트웨어 구동 신임정보 도용 감지를 지원합니다. IBM Trusteer Pinpoint 오퍼링은 또다른 보호 계층(layer)을 제공하며 계정 탈취 시도를 감지하고 (기본 브라우저나 고객 모바일 애플리케이션을 통해) Business(업무용) 또는 Retail(소매용) 애플리케이션에 액세스(접근)하는 브라우저 또는 모바일 디바이스의 위험 평가 점수를 고객에게 직접 전달합니다.

이 서비스에는 확장 배치 및 설정 서비스, 맞춤 보안 정책, 조사 서비스 등을 포함한 개선 기능 및 서비스가 포함되어 있습니다. 이 서비스에는 애플리케이션당 배치 서비스를 위한 최대 200 시간의 공유 자원과 설치(set-up) 후 애플리케이션당 보안 분석을 위한 최대 200 시간의 공유 자원이 포함되어 있습니다. 지속적 서비스에는 애플리케이션당 연 20 시간의 배치 유지보수와 애플리케이션당 연 100 시간의 보안 리서치가 포함됩니다. 추가 서비스에는 추가 요금이 부과됩니다.

Pinpoint Detect 은 모바일과 웹 채널 모두에서 거래를 이용할 수 있습니다. 모바일 거래가 포함된 경우 Pinpoint by Connection 이 적용 가능합니다. 이 클라우드 서비스에는 하나의 애플리케이션에 대한 보호가 포함됩니다. 고객은 모든 각 추가 애플리케이션에 대해 IBM Trusteer Pinpoint Detect Premium Additional Applications 에 대한 권한을 취득해야 합니다.

이 클라우드 서비스에는 프리미엄 지원이 포함되어 있습니다.

IBM Trusteer Pinpoint Detect Premium for Retail 및 Business 서비스는 적격 참여자 100 명 또는 IBM Trusteer Pinpoint Detect Premium 연결 100 회선 단위의 팩으로 구매될 수 있습니다. 연결(Connections)별로 서비스를 구매하고자 하는 경우, Additional Application 요금은 최초 애플리케이션부터 적용됩니다.

Pinpoint Detect Policy Manager:

이 Policy Manager 는 Pinpoint Detect Premium 서비스에 포함되며 고객(및 고객의 제한없는 수의 허가된 직원)이 다음을 수행할 수 있는 IBM Trusteer 클라우드 호스트 환경에서 제공됩니다. (i) 사기적 활동을 감지하도록 프로덕션 환경 로직에서 설계, 테스트 및 배치, (ii) 보고서 및 대시보드 설계, 및 (iii) 고객 애플리케이션에 대한 의심스러운 활동을 감지하는 정책 및 보안 정책 보기, 구성 및 설정.

Policy Manager 기능을 활성화하고 추가적인 심층 필수 지원을 제공받기 위해서는 컨설팅 서비스가 필요합니다. 컨설팅 서비스에 대한 세부사항은 별도의 작업명세서에 기술됩니다.

Policy Manager 활성화 시, IBM 은 정책 변화로 인해 발생하는 주요 문제점을 해결하기 위해 고객의 정책을 조정하도록 지원할 목적으로 고객의 환경에 액세스할 수 있는 권리를 보유합니다.

고객은 Policy Manager 를 통해 노출되는 데이터가 오용되지 않도록 데이터를 보호할 것을 약속합니다.

Policy Manager 기능 활성화 시, 고객은 문서에서 설명한 대로 규칙을 설정하기 위해 IBM 가이드라인을 준수해야 합니다. 고객은 이러한 권장사항을 준수하지 않음으로 해서 발생할 수 있는 상황에 대해서는 IBM 이 책임지지 않는다는 점을 인정합니다.

고객이 Policy Manager 기능을 잘못 구성하여 발생할 수 있는 안정성 및/또는 서비스 성능의 저하는 SLA 산정 시 다운타임(Downtime)으로 간주되지 않습니다.

1.1.3 IBM Trusteer Pinpoint Detect for Connections

이 클라우드 서비스는 보호 기능을 제공하며 계정 탈취 시도를 감지하고 (고객 모바일 애플리케이션의 기본 브라우저를 통해) Business(업무용) 또는 Retail(소매용) 애플리케이션에 액세스(접근)하는

브라우저 및/또는 모바일 디바이스의 위험/신뢰 평가 점수를 전달합니다. 이 솔루션은 최종 사용자의 디바이스, 연결 및 작동을 분석하는 다양한 위험 지표를 사용하여 사용자의 히스토리와 비교하고 의심되는 사용을 확인합니다.

이 클라우드 서비스는 모바일과 웹 채널 모두에서 연결을 이용할 수 있습니다. IBM Trusteer Pinpoint Detect 에는 IBM Trusteer Mobile SDK 에 대한 권한이 포함됩니다(관련이 있는 경우).

이 클라우드 서비스는 연간 연결 100 회선 단위의 팩으로 구매될 수 있습니다.

1.1.4 IBM Trusteer Pinpoint Detect 번들

이 클라우드 서비스 번들은 IBM Trusteer Pinpoint Detect, IBM Trusteer Mobile SDK 및 IBM Trusteer Rapport 에서 제공됩니다. 이 클라우드 서비스는 보호 기능을 제공하며 계정 탈취 시도를 감지하고 (고객 모바일 애플리케이션의 기본 브라우저를 통해) Business(업무용) 또는 Retail(소매용) 애플리케이션에 액세스(접근)하는 브라우저 및/또는 모바일 디바이스의 위험/신뢰 평가 점수를 전달합니다. 이 솔루션은 최종 사용자의 디바이스, 연결 및 작동을 분석하는 다양한 위험 지표를 사용하여 사용자의 히스토리와 비교하고 의심되는 사용을 확인합니다.

이 서비스는 활성 사용자가 구입할 수 있습니다.

이 클라우드 서비스는 모바일과 웹 채널 모두에서 연결을 이용할 수 있습니다. IBM Trusteer Pinpoint Detect 에는 IBM Trusteer Mobile SDK 에 대한 액세스가 포함되어 있습니다.

IBM Trusteer Pinpoint Detect Bundle 에는 IBM Trusteer Rapport 에 대한 액세스가 포함되어 있습니다. IBM 이 서면으로 달리 명시하지 않는 한, 이 액세스는 Trusteer Splash 및 IBM Trusteer Rapport Mandatory Service 를 제외합니다.

IBM Trusteer Mobile SDK

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").

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.

본 조항의 다음 조항은 본 계약에 따라 클라우드 서비스가 뉴욕 법인인 International Business Machines Corporation("IBM Corporation") 이외의 법인이 제공하는 경우에 적용됩니다. 본 문서에 포함된 SDK 및 재배포 가능 항목은 IBM Corporation 에서 제공합니다. IBM 은 디스트리뷰터로서 본 계약에 따라 SDK 및 재배포 가능 제품을 제공하고, SDK 및 재배포 가능 항목에 관한 모든 의무사항을 이행할 책임이 있으며, IBM Corporation 에 대해서는 본 계약상 어떠한 고객의 권리나 청구원인도 발생하지 않습니다. 고객은 IBM Corporation 에 대한 모든 클레임과 청구원인에 대한 권리를 포기하며 SDK 및 재배포 가능 항목에 대한 여하한 권리 및 구제책에 대해서는 오로지 IBM 에만 행사한다는 데 동의합니다.

IBM Trusteer Rapport

Trusteer Rapport 는 피싱 및 MitB(Man-in-the-Browser) 악성 소프트웨어 공격을 방지하는 보호 계층(layer)을 제공합니다. IBM Trusteer Rapport 는 전세계 수천만의 엔드포인트 네트워크를 사용하여 전세계 조직에 대한 활성 피싱 및 악성 소프트웨어 공격에 대한 정보를 수집합니다. IBM Trusteer Rapport 는 피싱 공격을 차단하고 MitB 악성 소프트웨어류의 설치 및 운영을 방지하기 위한 행위기반 알고리즘을 적용합니다.

본 클라우드 서비스 오퍼링에는 다음이 포함됩니다.

a. Web Script:

   클라우드 서비스에 액세스하거나 테스트하거나 사용하기 위한 목적의 웹 사이트 액세스 용도.

1.2 선택적 서비스

본 조항의 클라우드 서비스의 경우, 다음과 같은 선행 조건이 있습니다: IBM Trusteer Pinpoint Detect Premium, IBM Trusteer Pinpoint Detect Standard, IBM Trusteer Pinpoint for Connections 또는 IBM Trusteer Pinpoint Detect Bundle.

1.2.1 IBM Trusteer Pinpoint Detect Standard Application

고객 애플리케이션(Client Application)은 웹 애플리케이션(Web Application)이나 모바일 애플리케이션(Mobile Application)을 의미합니다. 웹 애플리케이션은 여러 웹 페이지를 통해 고객의 적격 참여자(Eligible Pariticipant)에게 제공되고 Trusteer 콘솔의 단일 애플리케이션(Trusteer Management Application)으로 모니터되는 모든 기능을 로그인 또는 식별 화면에서 그룹화합니다. 모바일 애플리케이션은 애플리케이션 스토어(스토어)에서 다운로드할 수 있는 하나의 소프트웨어 프로그램을 통해 고객의 적격 참여자에게 제공되고 Trusteer 콘솔의 단일 애플리케이션(Trusteer Management Application)으로 모니터되는 모든 기능을 로그인 또는 식별 화면에서 함께 그룹화합니다.

IBM Trusteer Pinpoint 의 통합에는 IBM Trusteer Pinpoint Application for every Application 에 대한 권한이 필요합니다.

- IBM Trusteer Pinpoint Detect Standard 의 배치에는 IBM Trusteer Pinpoint Detect Standard Application for every Application 에 대한 권한이 필요합니다.

1.2.2 IBM Trusteer Pinpoint Detect Premium Application

고객 애플리케이션(Client Application)은 웹 애플리케이션(Web Application)이나 모바일 애플리케이션(Mobile Application)을 의미합니다. 웹 애플리케이션은 여러 웹 페이지를 통해 고객의 적격 참여자(Eligible Pariticipant)에게 제공되고 Trusteer 콘솔의 단일 애플리케이션(Trusteer Management Application)으로 모니터되는 모든 기능을 로그인 또는 식별 화면에서 그룹화합니다. 모바일 애플리케이션은 애플리케이션 스토어(스토어)에서 다운로드할 수 있는 하나의 소프트웨어 프로그램을 통해 고객의 적격 참여자에게 제공되고 Trusteer 콘솔의 단일 애플리케이션(Trusteer Management Application)으로 모니터되는 모든 기능을 로그인 또는 식별 화면에서 함께 그룹화합니다.

이 서비스에는 애플리케이션당 배치 서비스를 위한 최대 200 시간의 공유 자원과 설치(set-up) 후 애플리케이션당 보안 분석을 위한 최대 200 시간의 공유 자원이 포함되어 있습니다. 지속적 서비스에는 애플리케이션당 연 20 시간의 배치 유지보수와 애플리케이션당 연 100 시간의 보안 리서치가 포함됩니다.

- IBM Trusteer Pinpoint Premium 의 배치에는 IBM Trusteer Pinpoint Detect Premium Application for every Application 에 대한 권한이 필요합니다.

1.2.3 IBM Trusteer New Account Fraud for Retail 및/또는 IBM Trusteer New Account Fraud for Business

Pinpoint 가입자에게 제공되는 이 서비스는 신규 계정의 작성 초기 단계에서 특이점을 감지하고 의심 활동에 대해 플래그 지정하며 경보를 생성하도록 설계되어 있습니다. 이 서비스는 신규 계정을 모니터하여 사기성이 있는 사후 계정 및 신생 계정의 프로파일링과 관련된 새로운 활동을 파악하고 TMA 에서 사용할 수 있는 이용 보고서를 통해 신규 계정이 mule 계정이거나 사기에 사용되는지에 대해 초기 경고 신호를 제공합니다.

IBM Trusteer New Account Fraud for Retail 및 IBM Trusteer New Account Fraud for Business 는 10 API 호출(10 API Calls) 단위의 팩으로 제공됩니다.

1.2.4 IBM Trusteer Digital Content Pack for Retail 및/또는 IBM Trusteer Digital Content Pack for Business

IBM Trusteer Digital Content Pack 은 보안 분석가로 하여금 진화하는 위협에 대응하기 위한 임시 모델을 작성하고 수정하는 작업을 전적으로 지원하면서 새로운 사기 행위 모델을 통합할 수 있도록 합니다. 이 팩은 솔루션의 추가 파트 및 필수 파트로 구입이 가능한 광범위한 규칙, 인사이트 및 정책 세트로 구성됩니다. Digital Content Pack 은 Trusteer 의 디지털 사기 방지 기능과 IBM Safer Payments 캐시리스 결제(cashless-payments) 채널 간의 통합을 더 강화하도록 돕습니다. Digital Content Pack 은 기본(built-in) 규칙과 특정 비즈니스 로직을 활용하여 은행 및 기타 금융 기관에서 기존의 사기 감지 및 방지 기능을 더 개선할 수 있도록 합니다.

IBM Trusteer Digital Content Pack for Retail 은 100 적격 참여자(100 Eligible Participants) 단위의 팩으로 판매됩니다. IBM Trusteer Digital Content Pack for Business 는 10 적격 참여자(10 Eligible Participants) 단위의 팩으로 판매됩니다.

상당한 주의가 필요한 지원 서비스뿐만 아니라 Pinpoint Detect 가 포함된 Digital Content Pack 과 IBM Safer Payments 의 통합에는 컨설팅 서비스가 필요합니다. 컨설팅 서비스는 별도의 작업명세서에 준하여 별도로 취득됩니다.

1.2.5 IBM Trusteer Pinpoint Malware Detection

IBM Trusteer Pinpoint Malware Detection II 클라우드 서비스에서 악성 소프트웨어를 감지한 경우 고객은 Pinpoint 베스트 프랙티스 가이드에 따라야 합니다. 악성 소프트웨어 또는 계정 탈취를 감지한 직후 적격 참여자의 사용 경험에 영향을 주어 다른 사용자가 IBM Trusteer Pinpoint Malware Detection II 클라우드 서비스를 사용하여 고객의 조치를 링크할 수 있는 방식(예: 악성 소프트웨어 또는 계정 탈취를 감지한 직후 알림, 메시지, 디바이스 차단 또는 Business 및/또는 Retail(소매용) 애플리케이션 액세스(접근) 차단)으로는 IBM Trusteer Pinpoint 클라우드 서비스를 사용하지 마십시오.

1.2.6 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business 및/또는 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail 및/또는 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business 및/또는 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

IBM Security Pinpoint Malware Detection II 는 다중 애플리케이션 보호에 관한 요금을 표준화하기 위한 새로운 IBM Trusteer Pinpoint Malware Detection 구성이며 애플리케이션 추가 시의 일시불 과금을 대체합니다.

Business 및/또는 Retail 애플리케이션에 연결하는 MitB(Man in the Browser) 파이낸셜 악성 소프트웨어 감염 브라우저에서 클라이언트리스 감지. IBM Trusteer Pinpoint Malware Detection 클라우드 서비스는 또다른 보호 계층(layer)을 제공하며 MitB 파이낸셜 악성 소프트웨어 존재여부의 검사 및 경보 기능을 고객에게 제공하여 조직이 악성 소프트웨어 위험성에 따른 사기 방지 프로세스에 중점을 둘 수 있도록 지원하는 서비스입니다.

a. 이벤트 데이터:

   고객(및 제한없는 수의 허가된 직원)은 TMA 를 사용하여 고객의 Business 및/또는 Retail 애플리케이션과 함께 적격 참여자의 온라인 상호작동의 결과로 생성된 이벤트 데이터를 수신할 수 있습니다.

b. Advanced Edition:

   Business 및/또는 Retail 의 Advanced Edition 은 고객의 Business 및/또는 Retail 애플리케이션의 구조와 플로우에 맞게 조정되고 사용자 정의되며 고객에 대한 특정 위협 동향에 따라 사용자 정의될 수 있는, 추가적인 감지 및 보호 계층(layer)을 제공합니다. 이는 고객의 Business 및/또는 Retail 애플리케이션의 다양한 위치에서 통합될 수 있습니다.

   Advanced Edition 은 최소 Retail 적격 참여자 10 만명 또는 Business 적격 참여자 1 만명(즉, Retail 적격 참여자 100 명 단위 1000 팩 또는 Business 적격 참여자 10 명 단위 1000 팩)에 해당하는 최소 수량 한도로 고객에게 제공됩니다.

c. Standard Edition:

   Business 및/또는 Retail 의 Standard Editions 은 본 이용 약관에 명시된 클라우드 서비스의 핵심 기능을 제공하는 빠른 배치 솔루션입니다.

이 클라우드 서비스에는 하나의 애플리케이션에 대한 보호가 포함됩니다. 고객은 모든 각 추가 애플리케이션에 대해 IBM Trusteer Pinpoint Malware Detection Additional Applications 에 대한 권한을 취득해야 합니다.

1.2.7 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail 및/또는 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail 및/또는 IBM Pinpoint Trusteer Pinpoint Malware Detection Standard Edition II for Business 및/또는 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business 를 위한 선택적 추가 클라우드 서비스

- IBM Trusteer Rapport Remediation for Retail 클라우드 서비스의 경우 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail 또는 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail 의 선행 조건이 있습니다.
- IBM Trusteer Rapport Remediation for Business 클라우드 서비스의 경우 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business 또는 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business 의 선행 조건이 있습니다.

1.2.8 IBM Trusteer Pinpoint Criminal Detection for Business 및/또는 IBM Trusteer Pinpoint Criminal Detection for Retail

디바이스 ID 를 사용하여 Business 또는 Retail 애플리케이션에 연결하는 브라우저에서 의심되는 계정 탈취 활동의 클라이언트리스(clientless) 감지, 피싱 감지 및 악성 소프트웨어 구동 신임 도용 감지. IBM Trusteer Pinpoint Criminal Detection 클라우드 서비스는 또다른 보호 계층(layer)을 제공하며 계정 탈취 시도를 감지하고 (기본 브라우저나 고객 모바일 애플리케이션을 통해) Business 또는 Retail 애플리케이션에 액세스하는 브라우저 또는 모바일 디바이스의 위험 평가 점수를 고객에게 직접 전달합니다.

a. 이벤트 데이터:

   고객은 TMA 또는 Trustboard 중에서 언제든지 한 번에 하나를 선택하여 사용할 수 있습니다. 고객(및 고객의 제한없는 수의 허가된 직원)은 TMA 또는 Trustboard 를 사용하여 고객이 클라우드 서비스 커버리지에 등록한 Business(업무용) 및/또는 Retail(소매용) 애플리케이션과 함께 적격 참여자의 온라인 상호작동의 결과로 생성된 이벤트 데이터를 수신하거나 백엔드 API 전달 모드를 통해 이벤트 데이터를 수신할 수 있습니다.

1.2.9 IBM Trusteer Pinpoint Criminal Detection II for Business 및/또는 IBM Trusteer Pinpoint Criminal Detection II for Retail

IBM Security Pinpoint Criminal Detection II 는 다중 애플리케이션 보호에 관한 요금을 표준화하기 위한 새로운 IBM Trusteer Pinpoint Criminal Detection 구성이며 애플리케이션 추가 시의 일시불 과금을 대체합니다.

디바이스 ID 를 사용하여 Business 또는 Retail 애플리케이션에 연결하는 브라우저에서 의심되는 계정 탈취 활동의 클라이언트리스(clientless) 감지, 피싱 감지 및 악성 소프트웨어 구동 신임 도용 감지. IBM Trusteer Pinpoint Criminal Detection II 클라우드 서비스는 또다른 보호 계층(layer)을 제공하며 계정 탈취 시도를 감지하고 (기본 브라우저나 고객 모바일 애플리케이션을 통해) Business 또는 Retail 애플리케이션에 액세스하는 브라우저 또는 모바일 디바이스의 위험 평가 점수를 고객에게 직접 전달합니다.

a. 이벤트 데이터:

   고객은 TMA 또는 Trustboard 중에서 언제든지 한 번에 하나를 선택하여 사용할 수 있습니다. 고객(및 고객의 제한없는 수의 허가된 직원)은 TMA 또는 Trustboard 를 사용하여 고객이 클라우드 서비스 커버리지에 등록한 Business(업무용) 및/또는 Retail(소매용) 애플리케이션과 함께 적격 참여자의 온라인 상호작동의 결과로 생성된 이벤트 데이터를 수신하거나 백엔드 API 전달 모드를 통해 이벤트 데이터를 수신할 수 있습니다.

이 클라우드 서비스에는 하나의 애플리케이션에 대한 보호가 포함됩니다. 고객은 모든 각 추가 애플리케이션에 대해 IBM Trusteer Pinpoint Criminal Detection Additional Applications 에 대한 권한을 취득해야 합니다.

1.2.10 IBM Trusteer Rapport Remediation for Retail 및/또는 IBM Trusteer Rapport Remediation for Business

IBM Trusteer Rapport Remediation for Retail 및 IBM Trusteer Rapport Remediation for Business 는 IBM Trusteer Pinpoint Malware Detection 이벤트 데이터를 통해 MitB(man-in-the-browser) 악성 소프트웨어 감염을 감지한 경우 고객의 애플리케이션에 임시로 액세스하는 고객의 적격 참여자의 감염된 디바이스(PC/MAC)에서 MitB 악성 소프트웨어 감염을 조사하고 치료하며 차단하고 제거합니다. 고객은 고객의 애플리케이션에서 실제로 실행 중인 IBM Trusteer Pinpoint Malware Detection II 의 당시 유효한 사용등록을 보유하고 있어야 합니다. 고객은 고객의 애플리케이션에 액세스(접근)하는 적격 참여자와 관련해서 감염된 특정 디바이스(PC/MAC)를 임시로 조사하고 개선하기 위한 도구로만 이 클라우드 서비스 오퍼링을 사용할 수 있습니다. IBM Trusteer Rapport Remediation 은 관련 적격 참여자의 디바이스(PC/MAC)에서 실제로 실행되어야 하며 해당 적격 참여자는 EULA 를 승인해야 하고 고객의 애플리케이션에서 최소 한 번 인증되어야 하며 고객의 구성에는 사용자 ID 수집내용이 포함되어야 합니다. 이 클라우드 서비스 오퍼링에는 Trusteer Splash 를 사용할 수 있는 권리는 포함되지 않으며 및/또는 고객의 일반 적격 참여자 그룹에 기타 다른 방법으로 계정 소유자 클라이언트 소프트웨어를 판촉합니다. 본 서비스 명세서의 목적상, 계정 소유자(Account Holder)는 클라이언트 인에이블링 소프트웨어를 설치하였고 최종 사용자 라이센스 계약("EULA")을 수락하였으며 고객이 클라우드 서비스 커버리지에 등록한 고객의 Retail(소매용) 또는 Business(업무용) 애플리케이션에서 최소 한 번 인증된 고객의 최종 사용자를 의미합니다. 계정 소유자 클라이언트 소프트웨어(Account Holder Client Software)는 IBM Trusteer Rapport 클라이언트 인에이블링 소프트웨어 또는 최종 사용자의 디바이스에 설치하도록 일부 클라우드 서비스에서 제공되는 기타 클라이언트 인에이블링 소프트웨어를 의미합니다.

1.2.11 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail 및/또는 IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail 또는 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail 의 경우, 최초의 애플리케이션 외에 추가적인 Retail 애플리케이션을 배치하기 위해서는 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail 에 대한 권한이 필요합니다.
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business 또는 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business 의 경우, 최초의 애플리케이션 외에 추가적인 Business 애플리케이션을 배치하기 위해서는 IBM Trusteer Pinpoint Malware Detection Additional Applications for Business 에 대한 권한이 필요합니다.

1.2.12 IBM Trusteer Rapport for Mitigation for Retail 및/또는 IBM Trusteer Rapport for Mitigation for Business

- IBM Trusteer Rapport for Mitigation for Retail 은 IBM Trusteer Pinpoint Detect Premium 또는 IBM Trusteer Pinpoint Detect Standard 이벤트 데이터를 통해 악성 소프트웨어 감염을 감지한 경우 고객의 Retail(소매용) 애플리케이션에 임시로 액세스(접근)하는 고객의 적격 참여자의 감염된 디바이스(PC/MAC)에서 악성 소프트웨어 감염을 조사하고 치료하며 차단하고 제거합니다. 고객은 고객 Retail(소매용) 애플리케이션에서 실제로 실행 중인 IBM Trusteer Pinpoint Detect Premium 또는 IBM Trusteer Pinpoint Detect Standard 의 당시 유효한 사용등록을 보유하고 있어야 합니다. 고객은 고객의 Retail(소매용) 애플리케이션에 액세스(접근)하는 적격 참여자와 관련해서 감염된 특정 디바이스(PC/MAC)를 임시로 조사하고 개선하기 위한 도구로만 이 클라우드 서비스를 사용할 수 있습니다. IBM Trusteer Rapport for Mitigation for Retail 은 관련 적격 참여자의 디바이스(PC/MAC)에서 실제로 실행되어야 하며 해당 적격 참여자는 EULA 를 승인해야 하고 고객의 Retail(소매용) 애플리케이션에서 최소 한 번 인증되어야 하며 고객의 구성에는 사용자 ID 수집내용이 포함되어야 합니다. 이 클라우드 서비스에는 Trusteer Splash 를 사용할 수 있는 권리는 포함되지 않으며 및/또는 고객의 일반 적격 참여자 그룹에 기타 다른 방법으로 계정 소유자 클라이언트 소프트웨어를 판촉합니다.
- IBM Trusteer Rapport for Mitigation for Business 는 IBM Trusteer Pinpoint Detect Premium 또는 IBM Trusteer Pinpoint Detect Standard 이벤트데이터를 통해 악성 소프트웨어 감염을 감지한 경우 고객의 Business 애플리케이션에 임시로 액세스(접근)하는 고객의 적격 참여자의 감염된 디바이스(PC/MAC)에서 악성 소프트웨어 감염을 조사하고 치료하며 차단하고 제거합니다. 고객은

고객 Business 애플리케이션에서 실제로 실행 중인 IBM Trusteer Pinpoint Detect Premium 또는 IBM Trusteer Pinpoint Detect Standard 의 당시 유효한 사용등록을 보유하고 있어야 합니다. 고객은 고객의 Business 애플리케이션에 액세스(접근)하는 적격 참여자와 관련해서 감염된 특정 디바이스(PC/MAC)를 임시로 조사하고 개선하기 위한 도구로만 이 클라우드 서비스를 사용할 수 있습니다. IBM Trusteer Rapport for Mitigation for Business 는 관련 적격 참여자의 디바이스(PC/MAC)에서 실제로 실행되어야 하며 해당 적격 참여자는 EULA 를 승인해야 하고 고객의 Business 애플리케이션에서 최소 한 번 인증되어야 하며 고객의 구성에는 사용자 ID 수집내용이 포함되어야 합니다. 이 클라우드 서비스에는 Trusteer Splash 를 사용할 수 있는 권리는 포함되지 않으며 및/또는 고객의 일반 적격 참여자 그룹에 기타 다른 방법으로 계정 소유자 클라이언트 소프트웨어를 판촉합니다.

1.2.13 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail 및/또는 IBM Trusteer Pinpoint Detect Standard Additional Applications for Business

- IBM Trusteer Pinpoint Detect Standard for Retail 의 경우 최초의 애플리케이션 외에 추가적인 Retail 애플리케이션을 배치하기 위해서는 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail 에 대한 권한이 필요합니다.
- IBM Trusteer Pinpoint Detect Standard for Business 의 경우 최초의 애플리케이션 외에 추가적인 Business 애플리케이션을 배치하기 위해서는 IBM Trusteer Pinpoint Detect Standard Additional Applications for Business 에 대한 권한이 필요합니다.

1.2.14 IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail 및/또는 IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

이 서비스에는 애플리케이션당 배치 서비스를 위한 최대 200 시간의 공유 자원과 설치(set-up) 후 애플리케이션당 보안 분석을 위한 최대 200 시간의 공유 자원이 포함되어 있습니다. 지속적 서비스에는 애플리케이션당 연 20 시간의 배치 유지보수와 애플리케이션당 연 100 시간의 보안 리서치가 포함됩니다.

- IBM Trusteer Pinpoint Premium for Retail 의 경우 최초의 애플리케이션 외에 추가적인 Retail 애플리케이션을 배치하기 위해서는 IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail 에 대한 권한이 필요합니다.
- IBM Trusteer Pinpoint Premium for Business 의 경우 최초의 애플리케이션 외에 추가적인 Business 애플리케이션을 배치하기 위해서는 IBM Trusteer Pinpoint Detect Premium Additional Applications for Business 에 대한 권한이 필요합니다.

1.2.15 IBM Trusteer Pinpoint Detect Standard for Retail Premium Support 및/또는 IBM Trusteer Pinpoint Detect Standard for Business Premium Support

Pinpoint Detect Standard Cloud Service 를 구입한 고객은 Premium Support 서비스를 구입할 수 있습니다. Premium Support 서비스의 범위는 아래 4 조에 기재되어 있습니다.

1.2.16 IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

고객이 이 클라우드 서비스에 사용등록하기 전에 먼저 IBM Trusteer Pinpoint Detect 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 Detect 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.

1.3 Acceleration 서비스

1.3.1 IBM Trusteer Pinpoint Detect Standard Redeployment 및/또는 IBM Trusteer Pinpoint Detect Premium Redeployment

서비스 기간 동안 온라인 뱅킹 애플리케이션을 재배치하기 위해 결과적으로 IBM Trusteer Pinpoint Detect 배치를 변경해야 하는 고객은 IBM Trusteer Pinpoint Detect Redeployment 를 구입해야 합니다.

애플리케이션의 도메인 또는 호스트 URL 을 변경하거나 온라인 애플리케이션을 새로운 기술로 변환하거나 새로운 온라인 뱅킹 플랫폼으로 이동하거나 새로운 로그인 플로우를 기존 애플리케이션에 추가하고자 하는 고객의 경우 재배치 작업이 필요할 수 있습니다.

고객은 6 개월의 재배치 전환 기간 동안 이미 사용등록한 애플리케이션 외에 실행되는 추가 애플리케이션을 일대일로 제공받을 수 있습니다.

1.3.2 IBM Trusteer Pinpoint Malware Detection Redeployment

서비스 기간 동안 온라인 뱅킹 애플리케이션을 재배치하기 위해 결과적으로 IBM Trusteer Pinpoint Malware Detection II 배치를 변경해야 하는 고객은 IBM Trusteer Pinpoint Malware Detection Redeployment 를 구입해야 합니다.

애플리케이션의 도메인 또는 호스트 URL 을 변경하거나 온라인 애플리케이션을 새로운 기술로 변환하거나 새로운 온라인 뱅킹 플랫폼으로 이동하거나 새로운 로그인 플로우를 기존 애플리케이션에 추가하고자 하는 고객의 경우 재배치 작업이 필요할 수 있습니다.

고객은 6 개월의 재배치 전환 기간 동안 이미 사용등록한 애플리케이션 외에 실행되는 추가 애플리케이션을 일대일로 제공받을 수 있습니다.

IBM Trusteer Pinpoint Malware Detection II Standard Edition 또는 IBM Trusteer Pinpoint Malware Detection II Advanced Edition 에 대한 IBM Trusteer Pinpoint Malware Detection Additional Applications 의 경우 최초의 애플리케이션 외에 추가적인 애플리케이션을 배치하기 위해서는 IBM Trusteer Pinpoint Malware Detection Additional Applications 에 대한 권한이 필요합니다.

1.3.3 IBM Trusteer Pinpoint Criminal Detection Redeployment

서비스 기간 동안 온라인 뱅킹 애플리케이션을 재배치하기 위해 결과적으로 IBM Trusteer Pinpoint Criminal Detection 클라우드 서비스의 배치를 변경해야 하는 고객은 IBM Trusteer Pinpoint Criminal Detection Redeployment 를 구입해야 합니다.

애플리케이션의 도메인 또는 호스트 URL 을 변경하거나 온라인 애플리케이션을 새로운 기술로 변환하거나 새로운 온라인 뱅킹 플랫폼으로 이동하거나 새로운 로그인 플로우를 기존 애플리케이션에 추가하고자 하는 고객의 경우 재배치 작업이 필요할 수 있습니다.

고객은 6 개월의 재배치 전환 기간 동안 이미 사용등록한 애플리케이션 외에 실행되는 추가 애플리케이션을 일대일로 제공받을 수 있습니다.

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 5.2 항 (추가 처리 위치 정보)를 참조하십시오.

IBM Trusteer Pinpoint Criminal Detect

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. 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.

프리미엄 지원:

클라우드 서비스에 대한 프리미엄 지원 등록 시 추가 요금이 부과되며 프리미엄 지원에는 다음이 포함됩니다.

- 모든 심각도 상태에 대한 24x7 지원.
- 고객이 지원 팀에 전화 및 콜백 요청으로 직접 연락할 수 있습니다.
- 고객과 고객의 적격 참여자는 지원 티켓을 전자적으로 제출할 수 있습니다(Software as a Service [SaaS] Support Handbook 참조).
- 고객은 고객 지원 포털을 통해 알림사항, 문서, 사례 보고서, FAQ(http://www.ibm.com/software/security/trusteer/support/)를 확인할 수 있습니다.

4. 요금

4.1 청구 체계

클라우드 서비스에 대한 과금 체계는 거래서류에 명시됩니다.

이 클라우드 서비스에는 다음 청구 체계가 적용됩니다.

- 인게이지먼트(Engagement)는 클라우드 서비스들과 관련된 전문 서비스 또는 교육 서비스입니다.
- 적격 참여자(Eligible Participant)는 클라우드 서비스에서 관리하거나 추적하는 서비스 제공 프로그램에 참여할 수 있는 개인이나 법인을 의미합니다.
  - 활성 사용자란 어떠한 방법으로든(예, 다중 송신 프로그램, 디바이스 또는 애플리케이션 서버 등을 통해) 직접 또는 간접적으로 클라우드 서비스에 액세스하는 고유한 개인을 의미합니다.
- IBM Trusteer Pinpoint Detect Bundle 의 경우 활성 사용자는 지난 12 개월 동안(이전까지) 한 번 이상 모든 수단을 통해 클라우드 서비스에 액세스하는 고유한 사용자입니다.
- 애플리케이션은 클라우드 서비스에서 개발되거나 클라우드 서비스에 액세스하도록 가용케 되거나 클라우드 서비스에서 사용된, 고유하게 이름이 지정된 소프트웨어 프로그램입니다.
- API 호출은 프로그래밍 가능 인터페이스를 통한 클라우드 서비스의 호출입니다.
- 연결(Connection)은 데이터베이스, 애플리케이션, 서버 또는 가용케 되었거나 가용케 되는 기타 유형의 디바이스를 클라우드 서비스에 링크 또는 연관하는 것입니다.

4.2 원격 서비스 요금

원격 서비스는 원격 서비스를 사용했는지 여부에 관계 없이 구입한 후 90 일에 만료됩니다.

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 데이터 주체의 데이터 처리에 관한 EULA 및 기준

IBM Trusteer Rapport 클라우드 서비스(Pinpoint 클라우드 서비스와 관련한 배치 시 Rapport Remediation 또는 Rapport for Mitigation 포함)의 경우: 달리 합의하지 않은 한, 고객이 독립적으로 정한 처리 기준에 준하여 고객은 클라우드 서비스를 제공하는 데 필요한 정보를 IBM 이 수집하고 처리할 수 있도록 하는 최종 사용자 라이센스 계약(End User License Agreement)(https://trusteer.secure.force.com/PKB/articles/en_US/FAQ/RAPPORT-DATA-PRIVACY-NOTICE-AND-END-USER-LICENSE-AGREEMENT-EULA 참조)을 제공하도록 IBM 에게 권한을 부여합니다.

IBM Trusteer Rapport 클라우드 서비스에 대해 고객은 본 프로그램을 사용하여 악성 소프트웨어 및 악성 소프트웨어 아티팩트, 즉 악의적인 활동과 관련된 파일이나 비정상적인 프로그램 오작동과 관련된 파일을 수집하도록 IBM 에게 후원 기업집단에 대한 데이터 처리자로 권한을 부여합니다. IBM 은 최종 사용자의 개인 정보가 포함된 파일을 대상으로 본 프로그램을 사용하지 않으며 단, 최종 사용자의 허가 없이 악성 소프트웨어에서 취득된 개인 데이터가 수집된 파일에 포함될 수 있습니다. IBM 은 1) 그러한 분석과 관련 없는 파일을 즉시 삭제하고 2) 관련 파일은 분석 기간 동안에만 보관하며 어떠한 경우에도 3 개월을 초과하여 보관하지 않습니다.

5.2 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.

5.3 계정 소유자 데이터

명확히 말해서, 둘 이상의 IBM 고객이 특정 계정 소유자의 계정 소유자 클라이언트 소프트웨어와 연계되고(그러한 IBM 고객을 이하 "제휴 고객"이라 함) 본 서비스 명세서 하의 서비스가 여러 지역의 데이터 센터를 통해 해당 제휴 고객에게 제공되는 경우에 계정 소유자의 데이터는 위의 5.2 항에 지정된 해당 각 데이터 센터와 연관된 모든 위치에서 처리될 수 있습니다.

5.4 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.

5.5 인에이블링 소프트웨어(Enabling Software)

클라우드 서비스에는 다음 인에이블링 소프트웨어가 포함됩니다.

- IBM Rapport Agents

5.6 Pinpoint Best Practices

악성 소프트웨어를 감지하거나 계정 탈취를 감지한 경우 고객은 Pinpoint 베스트 프랙티스 가이드에 따라야 합니다. 악성 소프트웨어 또는 계정 탈취를 감지한 직후 적격 참여자의 사용 경험에 영향을 주어 다른 사용자가 IBM Trusteer Pinpoint Detect 클라우드 서비스를 사용하여 고객의 조치를 링크할 수 있는 방식(예: 악성 소프트웨어 또는 계정 탈취를 감지한 직후 알림, 메시지, 디바이스 차단 또는 Business 및/또는 Retail(소매용) 애플리케이션 액세스(접근) 차단)으로는 IBM Trusteer Pinpoint Detect 오퍼링을 사용하지 마십시오.

5.7 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.