IBM Security
솔루션 개요

고객의 디지털 여정 전 범위에서 완벽한 경험 제공

옴니채널 고객의 여정에서 ID 신뢰를 완벽하게 확립할 수 있도록 지원하는 IBM Trusteer

서론

오늘날의 디지털 세상에서 소비자는 쇼핑하거나 계정을 등록하거나 거래하거나 회원 프로그램 또는 서비스에 가입하거나 단순히 연락처 정보를 업데이트하는 등 모든 상황에서 완벽한 경험을 기대합니다.

어떤 업종에서든 모든 채널에서 이와 같은 완벽한 경험을 제공해야 디지털 성장과 혁신을 이루고 경쟁력을 강화할 수 있습니다. 소비자에게 추가 인증 단계가 요구될 때 불만이 커져 포기율(abandonment rate)이 증가하고 NPS(net promoter score)가 하락하며 영업 기회가 사라질 수 있습니다.

귀사는 신뢰할 수 있는 사용자를 확인하기 위해 어떤 위험 평가 방식을 사용합니까?

IBM® Trusteer® 플랫폼을 선택한 기업은 빠르고 투명한 방식으로 디지털 ID 신뢰 체계를 확립하여 손쉽게 진짜 고객을 환영하고 디지털 여정 전반에서 신뢰 관계를 구축하고 발전시키면서 변함없이 강력한 보안을 실현할 수 있습니다.

IBM Trusteer는 다음과 같은 특징을 통해 디지털 ID 신뢰 확립을 지원합니다.

- 신규 고객, 게스트, 기존 저위험/고위험 고객의 디지털 옴니채널 라이프사이클 전체를 대상으로 하는 지속적인 디지털 ID 보증
- 구축하기 간편하고 최신 인텔리전스를 바탕으로 실시간 위험 평가를 지원하는 확장 가능하고 민첩한 클라우드 플랫폼
- 첨단 AI 및 머신 러닝으로 강화된 인텔리전스 서비스

지속적인 디지털 ID 보증

기업은 사전 정보 또는 고객 기록이 없을 때, 공개된 정보에 의존할 때, 사이버 범죄자가 최신 디지털 기능을 악용하거나 도난당한 ID를 사용하거나 여러 채널을 포괄하는 전술을 구사할 때 사용자 ID 확인에 어려움을 겪곤 합니다.

IBM Trusteer 플랫폼에서는 사용자가 다중 계층으로 구성된 뷰에서 거시적 관점을 확보하고 모듈형 방식으로 무단 접근 및 활동을 투명하게 파악할 수 있습니다. 위험도가 낮은 사용자에게는 더 완벽한 경험을 제공하고, 고위험군으로 분류된 사용자에게는 더 강력한 추가 인증을 적용할 수 있습니다.

Trusteer 플랫폼은 위험 평가를 위해 다양한 네트워크, 디바이스, 환경, 행동 인텔리전스를 활용합니다.

- 행동 분석 - 행동 기반 생체 인식, 사용자 여정 분석 등
- 디바이스 식별, 연결, 인증, 위생, 스푸핑 증거
- 전화 번호 및 이메일 인텔리전스
- ID 연계
- 세션 및 네트워크 속성

이 데이터를 IBM의 분석 및 인텔리전스 서비스와 연계함으로써 진짜 고객을 받아들이고 고위험군으로 분류된 사용자에게는 강력한 추가 인증을 적용하면서 완벽한 경험을 제공할 수 있습니다.

첨단 분석으로 강화된 인텔리전스 서비스

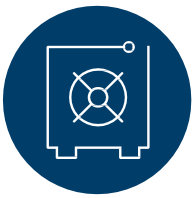
사용자의 액세스 기대 수준이 높아지고 있으며, 그에 따라 공격자의 전략도 진화합니다. IBM Trusteer는 애자일 인텔리전스 서비스를 포함하고 있어 새로운 패턴 및 진화하는 위협을 식별하도록 도우며, 위협 환경의 변화에 발맞춰 신속히 보호 기능을 조정할 수 있습니다.

IBM의 보안 인프라는 다음과 같이 구성됩니다.

- 첨단 AI 및 머신 러닝 기능 - 매일 수십억 개의 세션 분석
- 범조직적인 글로벌 실시간 위협 데이터 - 클라우드를 통해 전달
- IBM X-Force®에서 식별하는 새로운 패턴 - 세계 최고의 숙련도를 자랑하는 민간 보안 연구 조직

지속적인 디지털 ID 보증
투명한 방식으로 무단 접근 및 활동 파악

확장 가능하고 민첩한 클라우드 플랫폼
실시간 평가를 통해 실행 가능한 범조직 차원의 인사이트 확보



첨단 AI 및 머신 러닝이 접목된 인텔리전스 서비스
위험 및 운영 비용 평가, 효율성 및 보안 향상

IBM은 이러한 인텔리전스 기능을 숙련된 위협 연구 팀의 인지(human intelligence) 능력과 연계함으로써 기업이 더 효과적으로 위험을 평가하고 보안 조치를 개선하며 고위험군 사용자에 한해 이중 인증과 같은 추가 단계를 적용하게 할 수 있습니다.

확장성과 민첩성을 모두 갖춘 클라우드 플랫폼에서 이루어지는, 실용적인 실시간 평가

IBM Trusteer 솔루션은 확장 가능하고 민첩한 클라우드 플랫폼을 기반으로 하므로, 손쉽게 구축한 다음 최신 인텔리전스 기반의 실시간 위험 평가를 통해 운영 효율성을 높이고 비용을 절감합니다. Trusteer 클라우드 기반 서비스는 각각의 비즈니스와 함께 확장하면서 임의 개수의 세션을 실시간으로 처리하고 타사 솔루션과 유연하게 통합할 수도 있습니다.

단일 플랫폼에서 다양한 디지털 ID 신뢰 관련 문제 해결

IBM Trusteer의 다층적인 모듈형 접근 방식으로 다양한 디지털 ID 신뢰 관련 문제를 해결할 수 있습니다.

신뢰 구축: 신규 사용자 및 게스트 사용자에 대한 ID 검증(identity proofing)

새 고객이나 익명 고객을 검증해야 할 때 어떻게 하십니까? 사용자가 진짜 고객일까요 아니면 오로지 결제 사기를 시도하거나 귀사의 회원 프로그램을 악용하려는 것일까요? 어떤 게스트나 신규 고객은 아무런 제약 없이 받아들여야 할까요? 또한 추가 인증을 거쳐야 하는 사람은 어떤 사람일까요?

첨단 인텔리전스 및 글로벌 가시성을 활용하는 IBM Trusteer Pinpoint™ Assure 솔루션은 신규 고객과 게스트 고객을 대상으로 사기성 목적의 위험을 탐지하고 예측할 수 있습니다. 그뿐만 아니라 신규 계정에 대해 조기에 계정 모니터링을 수행할 수 있습니다. 이러한 유형의 인사이트를 확보해야 보안 조치에 대한 불만으로 인한 포기를 줄이고 회원 프로그램 등록을 늘리며 디지털 채널을 성장시킬 수 있습니다.

신뢰 지속: 신뢰할 수 있는 사용자에 대한 지속적 인증

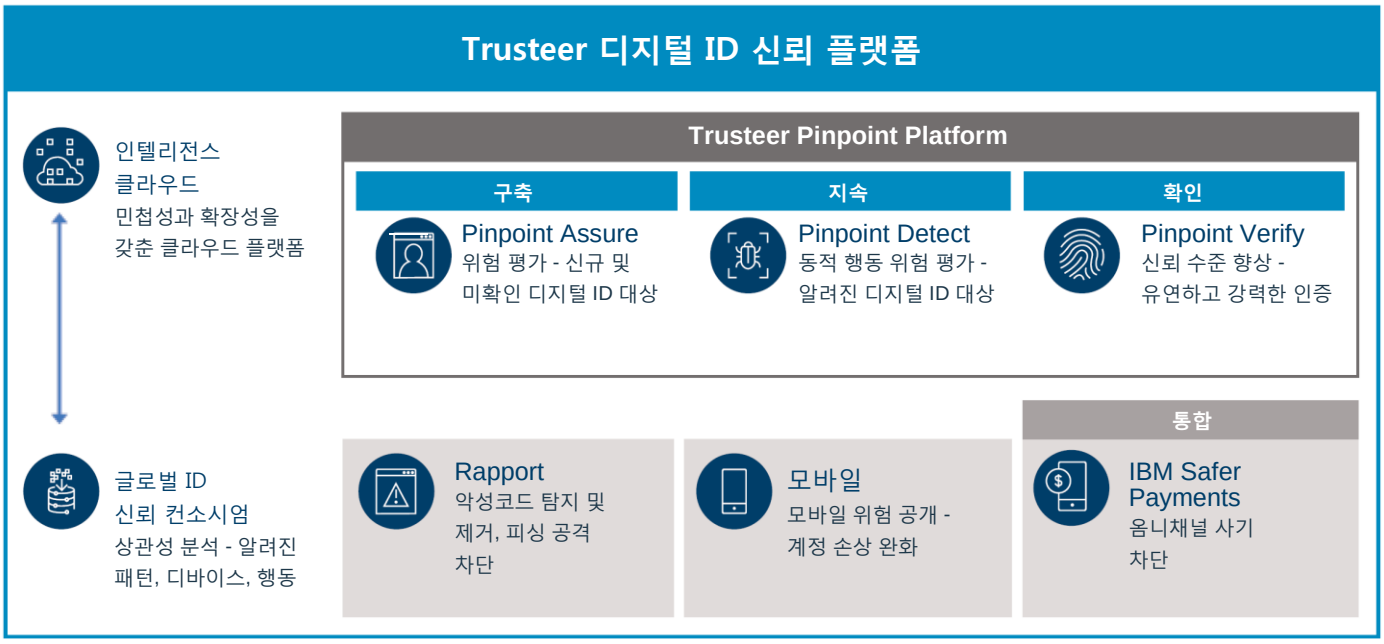
고객 계정 및 그 결제 과정이 감염되지 않도록 더 확실하게 보호할 수 있는 방법은 무엇일까요? 계정 탈취 또는 무단 로그인 및 활동을 탐지하려면 디바이스, 세션, 사용자의 측면에서 계정 액세스를 종합적으로 모니터링할 수 있어야 합니다. IBM Trusteer Pinpoint Detect가 바로 이와 같은 가시성을 제공합니다. 즉 행동 기반 생체 인식 기능 및 행동 분석을 모두 활용하면서 투명한 방식으로 사용자 프로필을 생성하고 지속적으로 온라인 ID를 인증합니다.

이 플랫폼은 머신 러닝 및 특허 받은 분석 기술을 통해 마우스 이동의 패턴을 놀라운 속도 및 규모로 분석하여 계정 사용자의 "정상적인" 디지털 행동과 비정상적인 행동을 구별합니다. 이 인사이트가 디바이스 활동 및 증거, 트랜잭션 데이터, 지리 위치 데이터와 통합됩니다. 비정상적인 사용자 행동이나 알려진 사기 행동 중 하나가 탐지되면 Trusteer Pinpoint Detect에서 바람직한 조치를 상세한 근거 및 세션 정보와 함께 실시간으로 제안하므로, 귀사는 필요할 때 신뢰 확인 절차를 진행할 수 있습니다.

신뢰 확인: 옴니채널 위험 평가와 강력한 적응형 인증의 조합

비정상적인 사용자 행동 또는 의심스러운 활동이 포착되면 어떻게 신뢰를 확인합니까? IBM Trusteer Pinpoint Verify 클라우드 기반 인증 서비스는 Pinpoint Assure 및 Pinpoint Detect와 간단히 통합되어 필요에 따라 강력한 추가 인증을 적용할 수 있게 합니다.

애플리케이션 개발자는 공개된 서비스 인터페이스를 통해 사용자에게 디지털 애플리케이션에서 2차 인증을 수행하도록 요구하면 됩니다. 그러면 사용자는 이메일, SMS, 모바일 푸시 알림을 통해 전달되는 일회용 패스코드부터 생체 인식 인증에 이르기까지 다양한 형태의 이중 인증 방식 중에서 선택하여 등록할 수 있습니다.



악성코드 및 피싱 차단

사이버 범죄자는 신중하게 계획되고 면밀하게 조정되는 옴니채널 공격의 일부로 악성코드 및 피싱을 사용하곤 합니다. 따라서 소비자 기기에서 그러한 위험 및 감염을 모니터링하고 고려하지 않는 기업은 더 큰 그림을 보지 못해 전반적인 위험이 증가할 수 있습니다. IBM 오퍼링은 이러한 대표적인 전술을 뒷받침하도록 설계되었습니다.

- Trusteer Pinpoint Detect는 통합 악성코드/범죄 탐지 기능으로 클라이언트 없이 사기를 밝혀냅니다.
- IBM Trusteer Rapport®는 엔드포인트 사기 차단 기능을 제공하여 MitB(man-in-the-browser) 공격을 막아내고 엔드포인트 디바이스에서 악성코드를 제거하도록 지원합니다. Trusteer Rapport는 머신 러닝 및 특허 받은 분석 기술도 활용하면서 새로운 피싱 사이트를 신속히 찾아내고 고객이 피싱 사이트에 접속하려 할 때 경고합니다.
- IBM Trusteer Mobile 솔루션은 다양한 모바일 위험 지표 및 행동 이상 요소를 모니터링합니다. 또한 영구적인 모바일 디바이스 ID도 생성하는데, 이 ID로 어떤 모바일 디바이스(iOS 또는 Android)도 확실히 식별할 수 있습니다.

Trusteer 솔루션은 간단하고 표준화된 인터페이스를 제공하며 기존 인프라와도 손쉽게 통합할 수 있습니다.

솔루션	주요 기능
IBM Trusteer Pinpoint Assure: 새로운 디지털 계정을 생성하는 과정에서 게스트 및 신규 사용자에 대한 ID 위험을 탐지하고 예측하도록 지원합니다.	• 신규 사용자 및 익명 사용자와 관련된 방대한 독점적 인사이트, 모바일 통신사 인텔리전스, 글로벌 보안 인텔리전스의 상관성을 분석합니다. – 행동 및 사용자 여정 분석 - 악성 봇 공격 또는 알려진 악의적 활동의 사용 패턴 탐지 – 디바이스 식별, 연결, 인증, 위생 - 신뢰할 수 없는 디바이스인지 여부 확인 – 전화 번호 및 이메일 인텔리전스 – ID 연계 - 동일한 ID 또는 ID 특성으로 새로운 계정이 생성되고 있는지 여부 또는 IBM Trusteer 솔루션을 사용하는 다른 기업의 정당한 활동과 일치하지 않는 속도 및 비율로 트랜잭션을 수행하고 있는지 여부 규명 – 전 세계적인 네트워크로부터 수집되는 악의적 활동 증거 컨소시엄 데이터 • 에코시스템에 최적화된 방식으로 IBM Trusteer 신규 계정 인텔리전스를 공개하고 올바른 활용을 지원합니다.
IBM Trusteer Pinpoint Detect: 모든 디지털 채널에서 계정 탈취 사기를 탐지하도록 지원합니다. IBM Safer Payments와 함께 구축할 경우 이 통합 솔루션은 광범위한 옴니채널 가시성을 제공하여 디지털 및 캐시리스 결제 채널의 활동을 컨텍스트와 보여줍니다.	• 실시간 위험 평가를 지원하고, 사기 행위 탐지 및 차단을 위한 조치를 제안합니다. • 사기 분석가가 IBM Trusteer 범죄 로직을 파악하여 새로운 맞춤형 정책을 개발하고 신속하게 대응책을 시행하도록 지원합니다. • 행동 기반 생체 인식 기능을 활용하여 손쉽게 사용자를 인증합니다. 이를 위해 마우스 이동 패턴을 기반으로 한 모델을 실시간으로 개발하고, 학습된 사용자 행동 및 알려진 사기 패턴과 비교하면서 패턴을 분석합니다. • 손상된 인증 정보를 사용한 액세스를 식별합니다. • 트랜잭션을 모니터링합니다.
IBM Trusteer Pinpoint Verify: 고위험군 사용자에 대한 강력한 인증을 제공하여 ID 위험을 최소화하도록 지원합니다.	• 이메일, SMS 또는 모바일 푸시 알림을 통해 일회용 패스코드를 제공합니다. • 생체 인식 인증(지문, 안면, 사용자 프레즌스 등)을 지원합니다.
IBM Trusteer Rapport: 악성코드 및 피싱 공격을 막는 클라이언트 기반 엔드포인트 보호를 제공합니다.	• 악성코드 감염으로부터 보호하고 감염된 사용자 디바이스에서 악성코드를 제거합니다. • 활동 중인 악성코드가 있더라도 브라우징 세션을 보호하도록 지원합니다. • 피싱 사이트를 탐지하고 손상된 계정 인증 정보 및 결제 카드 데이터를 확인하여 사용자에게 경고하고 사기 전담 팀에 알립니다. • 사기 전담 팀에 악성코드 감염 및 제거 사실을 알려 사용자 재인증을 지원하고 향후 위협을 차단할 수 있게 합니다.
IBM Trusteer Mobile: 디바이스 위험 요소를 분석하고 영구적인 모바일 디바이스 ID를 활용하여 기본 모바일 애플리케이션을 보호합니다. 모바일 채널에서 더 강력한 탐지를 지원하기 위해 IBM Trusteer 모바일 솔루션을 단독으로 사용하거나 Trusteer Pinpoint Detect와 손쉽게 통합하여 더 광범위하게 디지털 사기를 탐지할 수 있습니다.	• 모바일 기반 위험 요소를 탐지하도록 지원합니다. – 탈옥/루팅되었고 스푸핑을 당한 디바이스 – 악성코드 감염 및 SMS 해킹 – 활성 오버레이 악성코드 – 신뢰할 수 없는 출처의 애플리케이션 설치 – 안전하지 않은 세션 및 연결 – 오래된 운영 체제 – SIM 스왑 및 포팅을 위한 SIM 정보 – 사용자 행동 데이터(예: 위치) • 애플리케이션을 재설치하더라도 유지되는 하드웨어 및 소프트웨어 특성을 토대로 영구적인 디바이스 ID를 생성합니다.

추가 정보

완벽한 디지털 ID 신뢰에 대한 자세한 내용은 IBM 영업대표 또는 IBM 비즈니스파트너에게 문의하거나 **ibm.com**/security/fraud-protection/trusteer 웹 사이트에서 알아보세요.

IBM Security
75 Binney Street
Cambridge MA 02142

Produced in the United States of America
2018년 11월