AKAMAI 제품 설명서

Account Protector

계정 남용 방지를 통해 범죄자를 안전하게 차단하고 신뢰를 유지하세요

사용자가 진짜인지 사기꾼인지 어떻게 구별할 수 있을까요? 고객은 귀사에 의존해 이들을 구분합니다.

디지털 거래와 새로운 디지털 자산의 도입이 계속 확산됨에 따라 계정 도용의 리스크와 결과가 그 어느 때보다 심각해지고 있습니다. 디지털 비즈니스를 확장하고 고객을 보호할 수 있는 능력은 사기 기법이 끊임없이 진화하는 환경에서 신뢰를 유지하는 데 달려 있습니다.

사기성 계정 개설(신규 계정 사기) 및 계정 탈취(ATO)와 같은 계정 관련 남용은 모든 업계의 기업들에게 상당한 어려움과 비용을 초래합니다. 감염된 계정과 가짜 계정은 기업의 재정과 평판에 심각한 결과를 초래할 수 있습니다. 계정이 감염되면 공격자는 잔액을 빼내거나, 사기 거래를 하거나, MFA와 같은 보안 기능을 비활성화하거나, 민감한 개인 정보를 훔치는 등 자유롭게 계정을 악용할 수 있습니다. 반면에 가짜 계정은 무료 체험이나 크레딧과 같은 프로모션을 이용하고, SMS 펌핑을 실행하고, 스팸이나 부적절한 콘텐츠로 플랫폼을 가득 채우는 데 사용될 수 있습니다. 이러한 공격의 영향은 매우 크며, 기업은 고객 신뢰가 약화되고, 사기로 인해 수백만 달러를 잃고, 규제 벌금과 평판 손상의 리스크에 직면하게 됩니다.

Akamai Account Protector

Account Protector는 계정의 전체 수명 주기 동안 계정 도용을 방지하도록 설계된 보안 솔루션으로, 머신 러닝과 리스크 및 신뢰 지표의 중요한 데이터 세트를 사용해 사용자 요청의 진위 여부를 판단합니다. 그리고 실시간으로 행동을 분석해 계정 생성부터 로그인 이후까지 미묘한 사기 행위의 징후를 식별합니다. 의심스럽거나 비정상적인 행동이 탐지되면 Account Protector는 엣지에서 차단 및 조치, 암호화 및 행동 문제 해결, 대체 콘텐츠 제공 등 원활한 사용자 경험을 유지하기 위한 즉각적인 방어 옵션을 제공합니다.

기업이 누릴 수 있는 혜택

사용자와 사용자 고객 간의 신뢰 강화:
어떤 상호 작용이 정상인지 파악하고, 사용자가 경험하는 문제를 줄이고, 사기 행위로부터 사용자를 보호하세요.

비즈니스에 고유하게 맞춤화된 보안 기능 개발:
자동 조정된 봇 탐지 기능과 사용자가 사이트와 상호 작용하는 방식을 기반으로 사용자 집단 프로필을 파악하세요.

심층적인 인사이트와 가시성 확보:
투명한 신호와 지표를 기반으로 자신 있게 조치를 취하세요.

복구로 인한 영향 감소:
감염된 계정을 조사하고, 도난당한 자산을 교체하면서 발생하는 재정 및 리소스 낭비를 줄이세요.

데이터 기반 보안 및 신원 관련 의사 결정 강화:
사기 툴, SIEM, 기타 보안 툴과 통합해 Account Protector의 리스크 및 신뢰 신호를 사용함으로써 정확도를 높이고 해당 툴에 대한 투자를 강화할 수 있습니다.

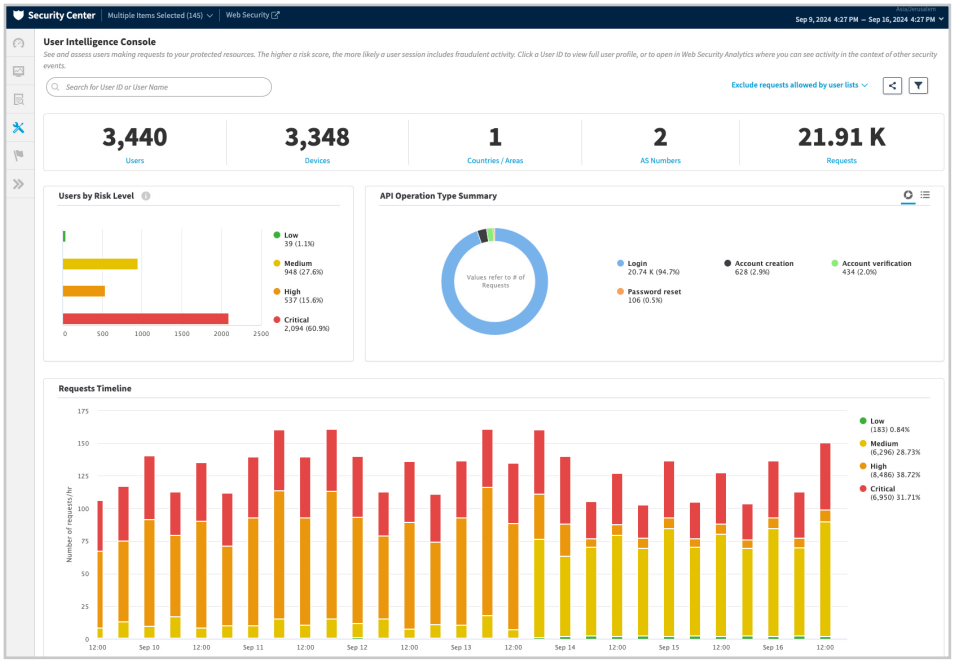
계정 남용에 대한 종합적인 방어 확보

전체 수명 주기 동안 사용자 계정을 남용으로부터 보호해, 계정 개설 남용, 계정 탈취 공격 및 이를 통한 공격 체계에 대한 최신 보안 기능을 제공합니다.

계정 개설 남용 - 프로모션 이용, SMS 펌핑, 도난당한 신용카드 정보 테스트, 인벤토리 비축 등에 사용되는 가짜 계정 생성을 방어합니다.

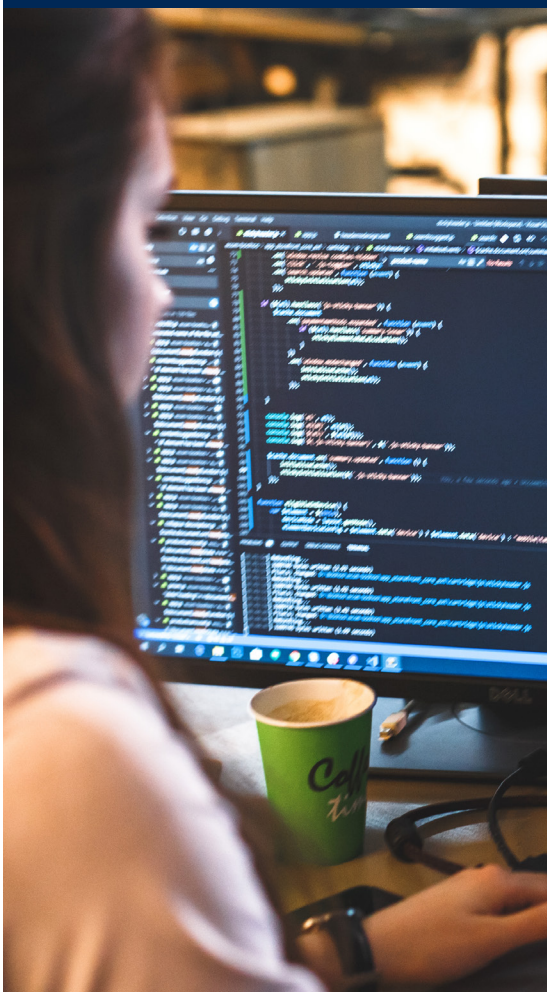
계정 탈취 - 사기범이 정상적인 고객 계정에 접속해 계정의 가치를 빼앗고, 민감한 데이터를 훔치고, 사기 거래를 저지르는 것을 방지합니다.

정교한 악성 봇 공격 - 귀중품, 돈 또는 기타 소중한 자산을 훔치기 위해 종종 계정 개설 남용 또는 ATO와 함께 시작되는 크리덴셜 스터핑, 인벤토리 조작, 기타 자동화된 공격으로부터 사용자 계정을 보호합니다.



보호, 신뢰, 사용자 경험

전체 수명 주기 동안 의심스러운 행동의 징후가 발생하는지 지속적으로 모니터링해 실시간으로 리스크를 분석하고 악용을 차단합니다.



핵심 기능

포괄적인 계정 수명 주기 보호 - 계정 생성부터 계정 업데이트, 비밀번호 변경, 결제와 같은 로그인 후 활동까지 모든 단계에서 사용자 리스크를 식별하고 분석합니다.

실시간 사용자 세션 리스크 점수 산정 - 사용자 세션 전반에 걸쳐 리스크와 신뢰를 평가해 사용자 요청이 정상 사용자로부터 오는 것인지 아니면 사기꾼으로부터 오는 것인지 평가합니다.

이메일 주소 인텔리전스 - 이메일 주소의 구문과 이메일의 비정상적인 사용을 분석해 악성 패턴을 탐지합니다.

이메일 도메인 인텔리전스 - 일회용 도메인 및 이메일 도메인의 과도한 사용을 포함해 개별 이메일 도메인에서 발생하는 활동 패턴을 평가합니다.

신뢰할 수 있는 사용자를 글로벌하게 인식 - Akamai 네트워크 전반의 사용자 행동에 대한 가시성을 제공해 로그인의 신뢰성에 대한 보다 정확한 정보를 바탕으로 의사 결정을 내릴 수 있도록 지원합니다.

사용자 행동 프로필 - 다시 찾아오는 사용자를 인식하기 위해 이전에 관측된 위치, 네트워크, 디바이스, IP 주소, 활동 시간을 기반으로 사용자 행동 프로필을 구성합니다.

집단 프로필 - 기업의 사용자 프로필을 상위 집합으로 집계하고 행동의 차이를 전체 사용자 집단과 비교해 비정상 행동을 탐지할 수 있습니다.

소스 평판 - 세계에서 가장 규모가 크고 많은 트래픽이 발생하며 자주 공격을 받는 웹사이트를 비롯해 전체 Akamai 고객에게서 관측된 과거의 악성 공격을 기반으로 소스의 평판을 평가합니다.

지표 - 리스크, 신뢰, 일반 지표로 각각의 요청을 평가해 계정 도용의 리스크를 평가합니다. 지표는 최종 사용자 리스크 점수와 함께 제공되며 분석에 활용할 수 있습니다.

정교한 봇 탐지 - 다양한 AI, 머신 러닝 모델, 기술을 사용해 첫 번째 상호 작용에서 알려지지 않은 봇을 탐지합니다. 여기에는 사용자 행동 및 텔레메트리 분석, 브라우저 핑거프린팅(fingerprinting), 자동 브라우저 탐지, 비정상 HTTP 탐지, 높은 요청률 등이 포함됩니다.

애널리틱스 및 보고 - 실시간 및 과거 기록 보고 기능을 모두 제공합니다. 개별 엔드포인트의 활동을 분석하고, 특정 사용자를 조사하고, 리스크 수준별로 사용자를 검토하고, 심층 인사이트를 얻을 수 있습니다.

최신 대응 조치 - 알림, 차단, 지연, 암호 및 행동 챌린지 제공, 대체 콘텐츠 제공 등 악용을 막기 위해 적용할 수 있는 다양한 조치를 제공합니다. 또한 기업은 URL, 시간, 지리적 위치, 네트워크 또는 트래픽 비율에 따라 다양한 조치를 할당할 수 있습니다.

헤더 삽입 - 분석 및 실시간 방어를 위해 사용자 리스크 정보를 전송합니다. 추가 분석과 실시간 방어를 위해 사용자 리스크 점수 및 점수에 기여한 리스크, 신뢰 및 일반 지표에 대한 정보와 함께 추가 요청 헤더가 전달된 요청에 삽입됩니다.

머신 러닝을 통한 자동화 - 행동 패턴에서부터 최신 평판 점수까지 Akamai 플랫폼 전반에서 사람의 사기 활동과 봇을 탐지하기 위해 사용하는 여러 특성과 행동에 대한 정보를 자동으로 업데이트합니다.

SIEM 통합(옵션) - 더욱 통합된 보안 가시성을 원하는 고객을 위해 사용자 리스크 정보를 SIEM 툴에 통합합니다. Account Protector의 인사이트로 기존 툴의 가치를 강화할 수 있습니다.

자세한 내용을 알아보려면 Akamai 담당자에게 문의하시거나 Akamai.com을 방문하시기 바랍니다.