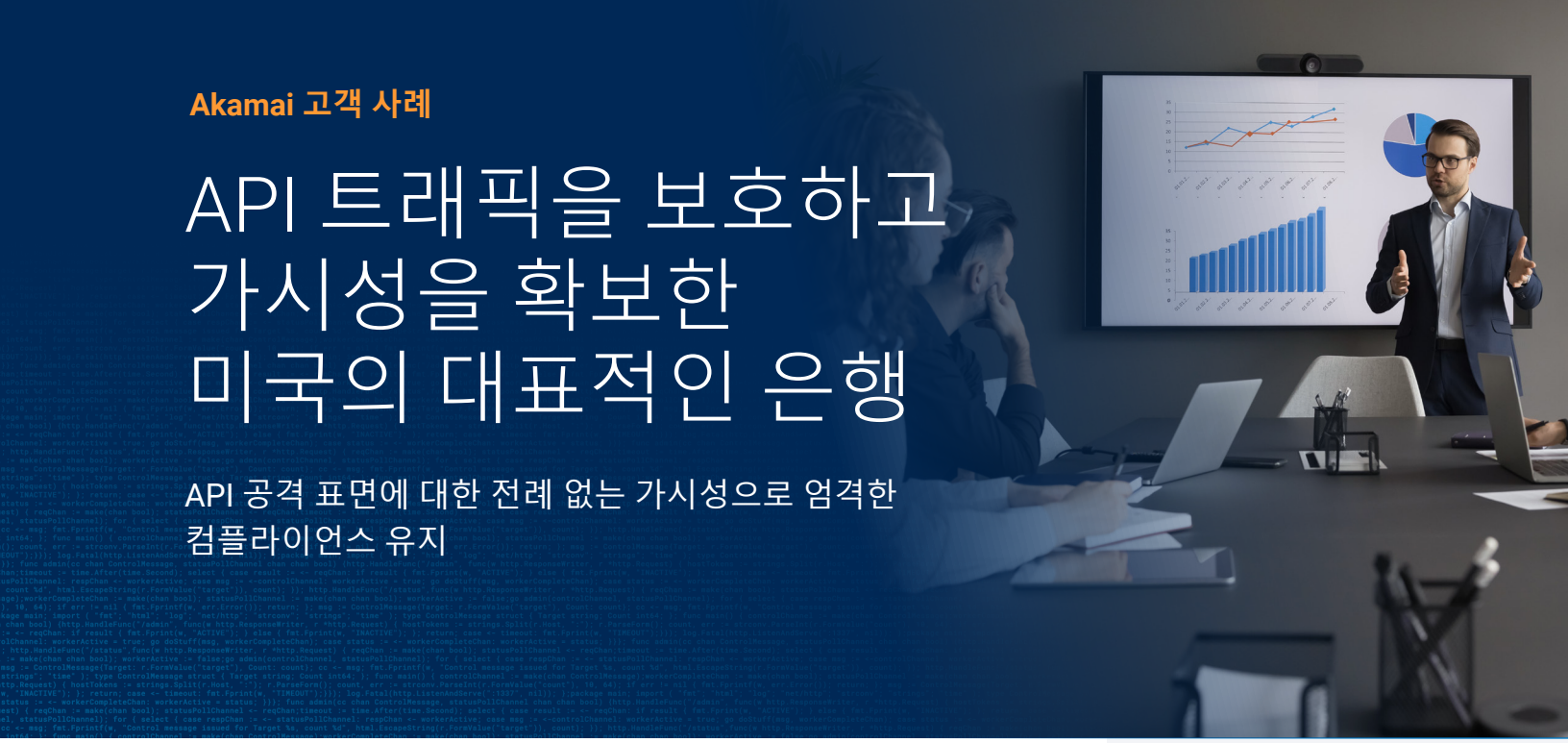
Akamai 고객 사례

API 트래픽을 보호하고 가시성을 확보한 미국의 대표적인 은행

API 공격 표면에 대한 전례 없는 가시성으로 엄격한 컴플라이언스 유지



은행 업계는 최근 몇 년 동안 API(Application Programming Interface)의 도입으로 인해 큰 변화를 겪었습니다. 이러한 API의 확산으로 은행은 새로운 기회를 활용하고, 고객 경험을 개선하고, 비즈니스 성장을 촉진할 수 있게 되었습니다.

API는 은행 생태계 내에서 서로 다른 시스템과 애플리케이션 간의 원활한 통합을 가능하게 하는 데 중요한 역할을 해왔습니다. 이제 은행은 API를 통해 서비스와 데이터를 노출함으로써 써드파티 개발자, 핀테크 스타트업, 기타 금융 기관과 협력해 혁신적인 솔루션을 만들고 서비스를 확장할 수 있습니다. 그러나 이러한 분명한 장점에도 불구하고 API 노출에는 리스크가 따르기도 합니다.

API 보안 리스크는 API의 기밀성, 무결성 및 가용성에 심각한 위협이 될 수 있습니다. 이러한 리스크에는 무단 접속, 인젝션 공격, 서비스 거부 공격, 안전하지 않은 데이터 전송, 불충분한 권한 부여 및 권한 상승, 입력 유효성 검사 부족, 안전하지 않은 인증정보 저장, 부적절한 로깅 및 모니터링이 포함됩니다. 이러한 리스크를 해결하기 위해 이 선도적인 은행은 Noname Security(현재 Akamai 자회사)와 협력했습니다.

컴플라이언스 유지

금융 서비스 업계에서는 공정하고 투명한 관행을 보장하고, 소비자를 보호하고, 금융 시스템의 무결성을 유지하기 위해 컴플라이언스가 가장 중요합니다. 고객알기제도(KYC) 및 자금세탁방지법(AML) 규정에 따라 금융기관은 고객의 신원을 확인하고, 자금세탁 및 테러 자금 조달과 관련된 잠재적 리스크를 평가하고, 의심스러운 활동을 보고해야 합니다.

Banking Leader

위치

미국

업계

금융 서비스

솔루션

Akamai API Security

주요 효과

- 컴플라이언스 강화
- F5 프로덕션 환경과 통합
- 지속적인 API 식별 제공

Akamai

다른 규정으로는 카드 소유자의 데이터를 보호하기 위해 주요 신용카드 회사에서 제정한 보안 표준인 PCI DSS(Payment Card Industry Data Security Standard)가 있습니다. 이러한 규정은 금융 규제와 관련해 빙산의 일각에 불과합니다. 이러한 이유로 금융 서비스 리더는 어떤 데이터가 API를 통해 이동하는지 파악해야 했습니다.

이 회사는 API 검색, 데이터 분류, 취약점 및 비정상 탐지에 중점을 두고 API 생태계의 전반적인 가시성을 개선해 리스크를 이해하고, 관리하고, 방어해야 했습니다. 또한 F5 프로덕션 환경과의 통합을 우선시했습니다.

API 풋프린트 파악

Noname API Security Platform(현재 Akamai API Security의 일부)은 고객 네트워크뿐만 아니라 고객 네트워크 내부에서 전송되는 API 트래픽에 대한 가시성을 제공했습니다. Akamai API Security 엔진은 트래픽을 분석해 금융 서비스 리더의 모든 API를 발견했습니다. 실시간 트래픽 분석을 통해 새로운 API와 기존 API의 변경 사항을 식별하고 고객사의 대시보드에 데이터를 기록 및 업데이트했습니다.

이 플랫폼은 에이전트나 사이드카에 의존하지 않고 클라우드 인프라와 통합되기 때문에 API 게이트웨이에 등록되어 있는지 여부에 관계없이 모든 API를 볼 수 있습니다. 내부 및 외부 API, 레거시 API(API 게이트웨이 이전의 API), 섀도 또는 로그 API(게이트웨이를 통해 라우팅되지 않는 API)가 모두 검색되어 고객에게 전례 없는 API 공격 표면에 대한 가시성을 제공합니다.

미래 전망

이 선도적인 은행은 일련의 기준을 사용하여 API 보안의 성공 여부를 평가합니다. 이 기준 중 하나는 신속한 분류이며, Akamai는 이를 지원하고 있습니다. 핵심 목표는 보안관제센터(SOC)가 알림을 신속하게 평가하고, 분류하고, 대응할 수 있도록 각 발견의 심각도를 분석하는 방법을 결정하는 것입니다.

 | 2024년 8월 발행