백서

강력한 API 보안을 통한 아시아 태평양 지역의 금융 서비스 발전

핵심 요약

국제통화기금(IMF)에 따르면, 아시아 태평양(APAC) 지역은 2024년에 4.2%의 높은 경제 성장을 이어갈 것으로 전망됩니다. 이러한 성장, 특히 금융 서비스 부문에서 끊임없이 진화하는 환경 속에서 애플리케이션 프로그래밍 인터페이스(API)는 업계의 디지털 혁신을 이끄는 핵심 원동력으로 부상했습니다. API는 은행 시스템의 다양한 구성요소를 연결하는 기술적 가교 역할을 하며 데이터와 기능을 원활하게 교환할 수 있도록 돕습니다. 또한, 금융 서비스 제공 방식을 혁신함으로써 고객에게 다양한 장점을 제공하고 있습니다.

2026년까지 APAC 지역의 보안 지출이 550억 달러(USD)에 달할 것이라는 IDC의 에서 알 수 있듯이, API 사용의 급속한 성장은 도전과제를 동반합니다. 금융 기관이 API를 통해 디지털 서비스를 확장하면서 의도치 않게 수많은 보안 취약점에 노출된 것입니다. API 사용이 급증하면서 사이버 범죄자들의 잠재적 공격 표면이 기하급수적으로 증가했으며, 공격자들은 금융 데이터의 고유한 가치를 인식하고 새로운 엔트리 포인트를 악용하기 위해 기법을 조정하고 있습니다.

금융 기관은 이러한 위협 환경의 확산에 대응하기 위해 사이버 보안 조치에 막대한 투자를 해야만 했습니다. 자체 시스템을 보호하는 것뿐 아니라 고객의 민감한 데이터와 자산을 보호하는 데에도 주력하고 있습니다. 이에 따라 사이버 공격으로 인한 리스크를 방어하기 위해 위협 탐지, 대응 전략, 업계 동료 및 사이버 보안 전문가와의 협업 중요성이 더욱 커지고 있습니다.

API가 주도하는 APAC 지역 금융 서비스 업계의 디지털 혁신은 고객의 요구사항 변화에 대응하고자 하는 업계의 적응력과 헌신을 보여줍니다. 그럼에도 불구하고 이러한 변화가 전개됨에 따라 금융 서비스 업계는 사이버 보안 체계를 강화하고, 보안 취약점을 해결하며, 디지털 혁신의 장점이 사이버 공격의 위협에 굴복하지 않도록 경계를 늦추지 말아야 합니다.

점차 중요해지는 API

APAC 지역은 금융 서비스 부문에서 디지털 혁신을 경험하고 있습니다. API는 단순한 시스템 간 통신 툴에서 인터넷 트래픽의 중심으로 진화해 다양한 애플리케이션과 서비스를 지원하고 있습니다. 이제 고객은 계좌 잔액 확인 및 자금 이체부터 대출 신청, 투자 관리까지 다양한 금융 활동을 손안에서 처리할 수 있습니다. 이러한 편리함은 고객 경험을 재편했을 뿐 아니라 금융 업계를 디지털 시대로 이끌었습니다. API는 단순한 시스템 간 통신 툴에서 인터넷 트래픽의 중추로 진화해 다양한 애플리케이션과 서비스를 지원하고 있습니다.

Polaris Market Research의 보고서에 따르면, 2021년 글로벌 오픈 뱅킹 시장 규모는 161억 4000만 달러(USD)이며, 2030년에는 예측 기간 동안 연평균 26.8%의 성장률로 성장해 1281억 2000만 달러(USD)에 달할 것으로 예상됩니다. Polaris의 리서치는 또한 예측 기간 동안 가장 큰 성장을 이룰 지역으로 APAC 지역을 꼽았습니다. APAC 지역의 금융 서비스 업계가 오픈 뱅킹의 잠재력을 최대한 활용하기 위해서는 API 보안의 도전 과제를 해결하기 위한 공동의 노력이 필요합니다.

이 지역의 선두 주자는 싱가포르로, MAS(Monetary Authority of Singapore)는 API 플레이북을 출간했습니다. MAS는 2018년 World Bank Group의 IFC(International Finance Corporation) 및 ABA(ASEAN Bankers Association)와 공동으로 APIX(API Exchange)의 설립을 주도하기도 했습니다. APIX는 금융 기관과 금융 기술 기관 간의 협업을 위한 온라인 글로벌 마켓플레이스 겸 샌드박스입니다.

아시아의 다른 여러 국가에서도 오랫동안 오픈 뱅킹을 개발하기 위한 이니셔티브를 진행해 왔습니다. 인도는 자국의 은행 계좌가 없는 많은 사람 및 금융 소외 계층을 위한 금융 포용성을 개선하기 위해 노력해 왔습니다.

인도 정부의 초기 이니셔티브 중 하나는 2016년 통합 결제 인터페이스로, 일반 국민이 API 프로토콜을 사용해 공인된 써드파티를 통해 은행 계좌에 접속하고 거래를 실행하도록 하는 것이었습니다. 2021년 RBI(Reserve Bank of India)는 동의 관리자를 생성하고, 소비자가 자신의 금융 기록에 디지털 방식으로 접속 및 제어하며, 금융 서비스 공급업체와의 데이터 공유 프로세스를 간소화하는 프레임워크인 Account Aggregators를 출시했습니다.

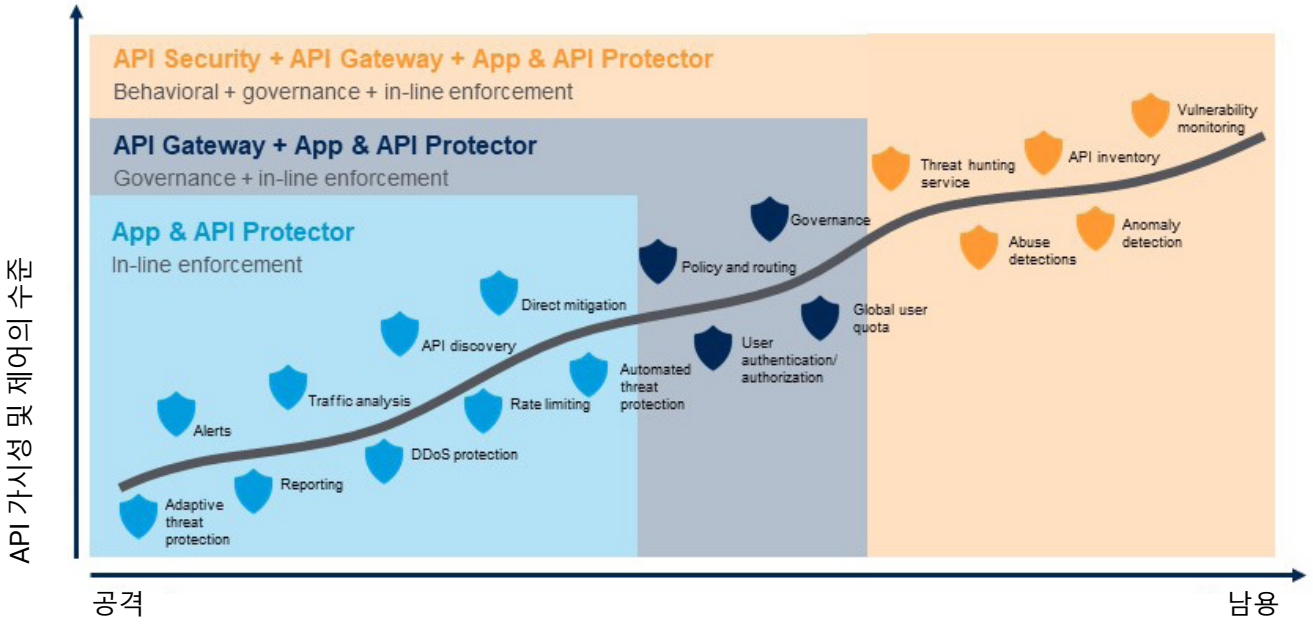
이러한 노력에도 불구하고 APAC 지역의 금융 서비스 업계는 2022년 2분기부터 2023년 2분기까지 웹 애플리케이션 및 API 공격이 36% 증가해 18개월 동안 무려 37억 건의 공격이 발생하는 등 세계에서 가장 많은 공격을 받는 업계 중 하나입니다. 수많은 금융 허브가 있는 APAC 지역에서는 웹 애플리케이션 및 API 공격이 급격히 증가했습니다.

APAC 지역의 API 관련 위협

APAC 지역에서는 2021년부터 2022년까지 금융 서비스에 대한 공격이 248% 증가하며 웹 애플리케이션 및 API 공격이 급격히 증가했습니다. API의 취약점으로 인해 호주 Optus 데이터 유출과 미국 T-mobile API 데이터 유출 등 수많은 대규모 주요 유출이 발생했습니다. 이러한 인시던트는 엔드포인트 보안과 인증정보 확인을 넘어서는 강력한 API 보안 솔루션의 필요성을 강조합니다.

이 백서에서는 이 중요한 공격 표면을 해결하고 API를 효과적으로 보호하기 위한 전략을 살펴봅니다. 또한, API 보안에 대한 선제적 접근 방식을 통해 컴플라이언스와 데이터 보안을 보장하는 방법을 설명합니다.

진화하는 API 공격



주요 API 보안 리스크

API는 광범위한 보안 리스크에 취약할 수 있으며, 이로 인해 데이터 유출, 무단 접속 및 기타 형태의 악용이 발생할 수 있습니다. 주요 API 보안 리스크에는 섀도 API, 취약한 API, API 남용, 민감한 정보의 과다 공유, 크리덴셜 스터핑 공격이 포함됩니다.

- **섀도 API.** 많은 금융 기관에는 모든 API를 총괄하는 특정인이나 특정한 팀이 없습니다. 이러한 감독 부족은 보안에 상당한 공백을 야기합니다. API의 관리와 보호에는 전사적인 API 발견과 분류가 매우 중요합니다. 개발자와 보안 팀 간의 격차를 해소하고 개발자의 환경에서 섀도 API를 탐지하는 일도 중요합니다. 지속적인 검색을 통해 새로 발견된 API나 기존 API의 변경 사항을 계속 업데이트하면 섀도 API를 제거할 수 있습니다.

- **취약한 API.** API가 발견되면 금융 기관은 리스크 체계를 평가하고 특히 민감한 데이터를 전달하는 API의 취약점을 식별해야 합니다. 이 단계는 보안 노력의 우선순위를 효과적으로 정하기 위해 반드시 필요한 부분입니다.

- **API 남용.** 디지털화가 가속됨에 따라 APAC 지역에서 웹 공격 건수가 계속 증가하고 있습니다. 공격자들은 끊임없이 API를 표적으로 삼기 때문에 남용과 오용을 막기 위한 강력한 보안 조치가 필요합니다.

- **민감한 정보의 과다 공유.** 최신 앱은 종종 민감한 데이터를 과도하게 공유해 새로운 공격 기법을 제공합니다. 공격자는 트래픽을 가로채고 민감한 정보에 무단으로 접속할 수 있습니다.

- **크리덴셜 스터핑 공격.** 공격자들은 API를 사용해 크리덴셜 스터핑 공격을 자동화함으로써 금융 기관을 표적으로 삼고 있습니다.

API 보안 관련 도전 과제

탐지되지 않고 보고되지 않은 공격

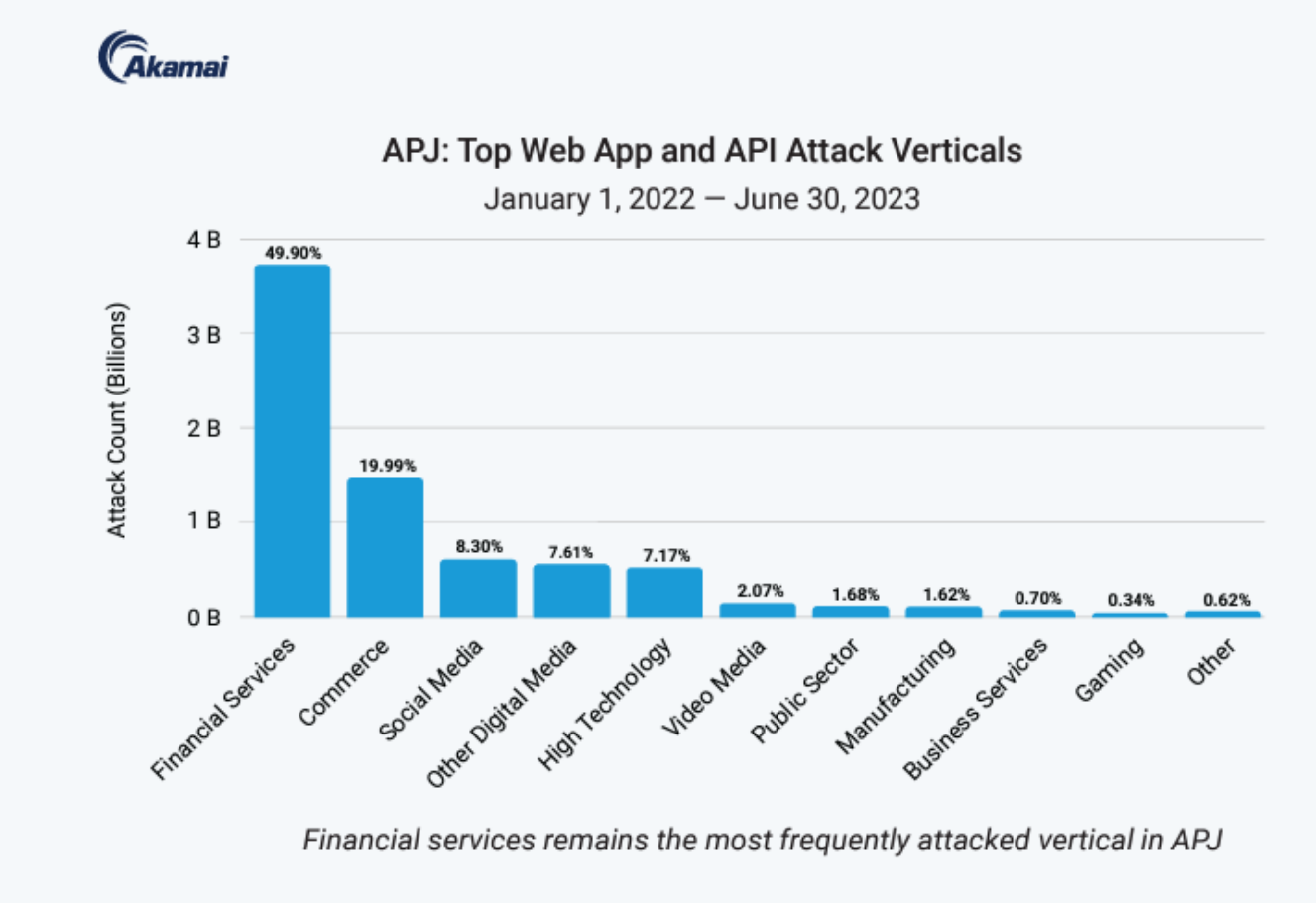
최근 SANS의 설문 조사에 따르면, API 인벤토리는 여전히 금융 기관에게 중요한 문제입니다. 금융 기관은 인프라 내에 있는 모든 API를 인지하지 못할 수도 있으며, 이러한 경우에는 거버넌스 및 보안 사각지대가 발생합니다. 이러한 가시성 부족은 API 공격이 종종 탐지되지 않고 보고되지 않는 주요 요인 중 하나일 수 있습니다. API 보안의 첫 번째 단계는 API를 포괄적으로 발견하고 분류하는 것입니다.

파괴적인 API 공격의 영향

웹 애플리케이션과 API의 가용성이 중단되면 고객 만족도와 브랜드 충성도에 큰 영향을 미칠 수 있습니다. 디지털 우선 접근 방식의 도입이 증가함에 따라 API는 특히 핀테크 기업과 기존 은행이 도입한 오픈 뱅킹의 측면에서 금융 기관의 성공에 더욱 중요해졌습니다.

API 트래픽의 급격한 증가

금융 부문의 API 트래픽은 세 자릿수로 증가하는 등 빠르게 성장하고 있습니다. 이러한 성장으로 인해 보안 제어가 API 관련 위협의 환경 변화를 따라잡아야 하는 과제를 안고 있습니다.



Financial services remains the most frequently attacked vertical in APJ

규정과 보안

API와 기타 혁신적인 기술을 활용하는 금융 기관들은 공공 정책과 금융 안정성 목표의 교차점에 서 있습니다. APAC 지역 내 여러 금융 규제 기관이 존재하는 상황에서 고객 성과를 개선하려는 공동의 노력이 만들어지고 있습니다. 가장 중요한 목표는 다양한 금융 옵션을 확대하고, 경쟁과 접근성을 높이며, 금융 포용을 촉진하는 것입니다. APAC 지역의 규제 기관은 금융 서비스의 범위를 넓혀 개인과 기업 모두에게 혜택을 제공하기 위해 노력하고 있습니다.

World Bank에 따르면, 전 세계에 은행 계좌가 없는 성인은 무려 17억 명에 달합니다. 특히 은행 계좌가 없는 사람의 비율이 가장 높은 3개 국가는 아시아에 있는데 중국이 13%(약 2억 2500만 명), 인도 11%(1억 9000만 명), 인도네시아 6%(9600만 명)입니다. APAC 지역에서 은행 계좌를 갖고 있지 않거나 금융 소외 계층인 개인 및 기업이 많은데 아직 개발되지 않은 이 거대한 시장의 규모는 550억 달러에서 1150억 달러(USD)에 이르는 것으로 추정됩니다.

API 보안에서 규제의 역할

PSD2(Revised Payment Services Directive)와 같은 규제은 기존 기관이 외부 기관과 데이터를 공유하도록 요구함으로써 투명성을 제고합니다. 이러한 규제는 최종 사용자의 데이터, 개인정보, 보안을 보호하는 것을 목표로 합니다. 금융 기관은 혁신을 지속하면서 이러한 규제를 준수해야 합니다.

규제는 데이터 공유를 촉진하는 동시에 기업이 어떻게 데이터와 데이터 접속을 저장하고 보호해야 하는지 명시합니다. Akamai 솔루션은 혁신 노력을 방해하지 않으면서 금융 기관이 이러한 규제를 준수할 수 있도록 지원합니다.

강력한 API 보안 전략을 구축하기 위한 6단계

엔드포인트를 보호하고 인증정보를 확인하는 것만으로는 더 이상 API 기반 공격을 방어할 수 없습니다. 강력한 API 보안 전략에는 다음 6가지 단계가 포함되어야 합니다.

1. 파트너와의 협업

금융 기관과 보안 파트너는 긴밀한 협업을 통해 인력, 프로세스, 기술을 조정하고 API 보안 리스크에 대한 강력한 방어 체계를 구축해야 합니다. 이러한 협업에는 개발팀, 네트워크 및 보안 운영팀, ID팀, 리스크 관리자, 보안 설계자, 법무 및 컴플라이언스팀이 포함됩니다.

2. API 검색 및 분류

API 보안의 첫 번째 단계는 전사적으로 API를 발견하고 분류하는 것입니다. 이 프로세스를 통해 보안 엔지니어는 공격 표면의 범위와 민감한 정보의 잠재적 노출 가능성을 파악할 수 있습니다.

3. 취약점 테스트 및 리스크 평가

API가 발견되면 금융 기관은 취약점 테스트와 리스크 평가를 통해 적시에 취약점을 식별하고 해결해야 합니다. 이 프로세스는 지속적인 보안을 보장하기 위해 API 개발 및 업그레이드 주기에 통합되어야 합니다.

4. 행동 탐지 구축

API 보안은 전체 애플리케이션 보안 프레임워크의 중요한 구성요소입니다. 행동 탐지는 취약한 API가 악용되는 문제를 방지하기 위한 핵심 전략입니다. 이 접근 방식에는 잠재적인 위협을 식별하기 위한 API 행동의 지속적인 모니터링 및 분석이 수반됩니다.

5. OWASP 상위 10대 리스크에 대한 우선순위 지정

금융 기관은 포괄적인 보안을 보장하기 위해 OWASP (Open Worldwide Application Security Project)의 10대 API 보안 리스크에 우선순위를 두어야 합니다. 이러한 통제는 API에 영향을 미치는 가장 중요한 취약점과 공격 기법을 다룹니다.

OWASP API Top 10 coverage by Akamai

- ☑ **API1:2023 — Broken Object Level Authorization:** BOLA vulnerabilities can occur when a client's authorization is not properly validated to access specific object IDs.
- ☑ **API2:2023 — Broken Authentication:** BA refers to broad vulnerabilities in the authentication process, exposing the system to attackers that can exploit these weaknesses to compromise API object protection.
- ☑ **API3:2023 — Broken Object Property Level Authorization:** BOPLA is a security flaw where an API endpoint unnecessarily exposes more data properties than required for its function, neglecting the principle of least privilege.
- ☑ **API4:2023 — Unrestricted Resource Consumption:** This is a type of vulnerability, sometimes called API resource exhaustion, where APIs do not limit the number of requests or the volume of data they serve within a given time.
- ☑ **API5:2023 — Broken Function Level Authorization:** BFLA can occur when access control models for API endpoints are incorrectly implemented.
- ☑ **API6:2023 — Unrestricted Access to Sensitive Business Flows:** This risk arises when an API exposes critical operations like business logic without sufficient access control.
- ☑ **API7:2023 — Server Side Request Forgery:** SSRF allows an attacker to induce the server-side application to make HTTPS requests to an arbitrary domain of the attacker's choosing.
- ☑ **API8:2023 — Security Misconfiguration:** This refers to the improper setup of security controls, which can leave a system vulnerable to attacks.
- ☑ **API9:2023 — Improper Inventory Management:** This is a challenge for every organization managing APIs. API security solutions can protect known APIs, but unknown APIs — including deprecated, legacy, and/or outdated APIs — may be left unpatched and vulnerable to attack.
- ☑ **API10:2023 — Unsafe Consumption of APIs:** This refers to the risks associated with the use of third-party APIs without putting proper security measures in place.

6. 동료에게 배우기

금융 기관은 업계 동료에게 배우고 모범 사례를 공유해야 합니다. FS-ISAC(Financial Services Information Sharing and Analysis Center)의 회원은 사이버 위협을 예측하고, 방어하고, 대응하기 위한 인텔 플랫폼, 리소스, 신뢰할 수 있는 피어 투 피어 전문가 네트워크의 장점을 누릴 수 있습니다. 다른 기업이 API 보안 문제를 어떻게 해결하는지 명확히 이해하면 업계 전반의 보안 조치를 강화하는 데 도움이 될 수 있습니다.

결론

다양한 소프트웨어, 디바이스, 데이터 소스 전반에 걸쳐 유연하고 신속하며 비용 효율적으로 통합할 수 있도록 설계된 API가 빠르게 도입되고 디지털 전환이 이루어지고 있는 시대에 API를 보호하는 것은 APAC 지역 금융 기관에게 가장 중요한 도전 과제입니다. 그럼에도 불구하고 API 보안은 다양한 특징과 기능, 비즈니스 요구사항이 얽혀 있는 복잡한 작업입니다. API 보안을 소홀히 하면 사이버 공격, 데이터 유출, 규제 위반, 기관의 평판 손상 등 심각한 결과를 초래할 수 있습니다.

Akamai 데이터에 따르면, API 기능은 공격 방법을 지속적으로 발전시키고 적응시키는 공격자들의 최우선 표적 중 하나입니다. 따라서 API 보안은 엣지로 이동함으로써 인프라에서 벗어나고 고객이 데이터와 애플리케이션을 사용하는 디지털 터치포인트와 더 가까워져야 합니다. 이러한 전략적 조정은 디지털 자산에 대한 강력한 보안을 보장하는 데 매우 중요합니다.

금융 서비스 업계를 위한 Akamai 솔루션에 관한 더 자세한 내용은 akamai.com/finserv에서 확인하세요