Akamai 고객 사례

위협으로부터 API를 안전하게 보호하는 아시아 선도 통신 사업자

자산의 모든 API에 대한 가시성과 보호 기능을 확보한 통신 사업자

관리되지 않는 API 발견 | API 보안 강화 | 민감한 데이터 보안

아시아 지역의 통신 업계는 모바일 디바이스의 확산에 따라 더 나은 디지털 서비스에 대한 고객의 요구를 충족하기 위해 새로운 기술을 개발하고 네트워크를 확장하는 데 막대한 투자를 하고 있습니다. 이 과정에서 API는 다음과 같은 역할을 합니다.

- 통신 업계의 혁신에 필요한 연결성을 제공하는 동시에 DevOps 팀의 프로세스 가속
- 아시아 전역의 고객에게 휴대 전화 서비스, 인터넷 접속, 기타 통신 상품을 제공할 수 있는 기반
- 보다 개인 맞춤화된 솔루션을 제공하고 궁극적으로 고객 경험을 개선할 수 있는 역량

아시아 지역의 선도적인 통신 사업자 중 한 곳은 특히 새로운 디지털 음성 및 데이터 솔루션을 제공하는 데 API가 큰 기회를 제공한다고 생각하고 있습니다. 그리고 5G 시대가 다가옴에 따라 전화 통신을 넘어 빅 데이터, AI, IoT, 기타 새로운 디지털 애플리케이션으로 관심을 돌리고 있습니다. 동시에 API의 수가 급증하고 있으며 이로 인한 리스크도 커지고 있다는 사실도 잘 알고 있습니다. 2022년과 2023년에 다른 주요 통신 사업자들이 API 공격의 영향을 받는 것을 목격하면서 이 통신사는 Noname Security(현재 Akamai가 인수한 기업)와 협력했습니다.

Telecommunications Company

위치

아시아

업계

네트워크 운영자

솔루션

Akamai API Security

Akamai

모든 API와 그 리스크에 대한 가시성 확보의 필요성

많은 기업이 그렇듯이 보안팀은 API와 그 리스크에 대한 가시성이 부족하다는 도전 과제에 직면해 있습니다. Akamai의 리서치에 따르면 전체 API 인벤토리를 보유한 기업 10곳 중 4곳만이 어떤 API가 민감한 데이터를 반환하는지 알고 있는 것으로 나타났습니다. Akamai는 API 보안 솔루션의 Discovery 모듈을 사용해 통신 사업자 고객도 비슷한 도전 과제에 직면해 있다는 것을 확인했습니다.

Akamai와 협력하기 전 해당 고객의 API 보안 제어는 주로 레거시 API 관리 플랫폼과 웹 애플리케이션 방화벽(WAF)으로 구성되었습니다. 애플리케이션 보안과 API 전송 관점에서 보면 이러한 방식이 적절했습니다. 하지만 두 솔루션 모두 오늘날의 공격 방법으로부터 API를 포괄적으로 보호하는 데 필요한 높은 수준의 보안 제어와 옵저버빌리티를 제공하지 못했습니다. 그 이유는 모든 API가 WAF나 API 게이트웨이와 같은 프록시를 통해 라우팅되는 것은 아니며 관리되지 않는 이러한 API는 악성 공격자에게 매력적인 표적이 되기 때문입니다.

그러나 해당 통신사는 API 인벤토리를 정확하게 감사하더라도 API가 작동하고 요청을 관리하면서 정상적으로 작동하는 동안에 API를 보호할 수 있는 기능이 필요했습니다. 간단히 말해, 기업의 보안팀이 자체 환경에서 악성 행동을 수동으로 탐지하는 것은 불가능합니다.

실시간으로 보호해야 하는 API 엔드포인트는 수백 혹은 수천 개에 달합니다. 일반적으로 사용되는 AppSec 솔루션은 일반적으로 고객 환경의 모든 API 호출에 대응할 수 없기 때문에 적절한 API 런타임 보호 기능이 없으면 기업의 IT 환경이 사이버 공격에 취약해질 수 있습니다.

모든 API를 확인하고 API 위협을 방어하는 솔루션

계약의 첫 번째 단계에서 파일럿 배포를 통해 통신사의 내부 API를 찾고, 설정을 평가하고, API를 통과하는 데이터 종류를 파악했습니다. 고객은 검색이 실행되는 속도, 정확한 인벤토리 결과, 툴이 식별한 민감한 데이터 노출에 즉시 깊은 인상을 받았습니다.

파일럿의 긍정적인 결과에 힘입어 해당 고객은 Noname API Security Platform(현재 Akamai API Security의 일부)의 적용 범위를 내부 및 외부 API 자산 전체로 확장했습니다. 이 연습을 통해 숨겨진 프로덕션 API가 더 많이 발견되었고, 환경이 직면한 가장 시급한 위협을 발견했습니다.

Akamai는 해당 고객이 향후 공격으로부터 API를 보호하려면 주요 보안 취약점에 대한 더욱 강력한 방어가 필요하다는 것을 알게 되었습니다. Akamai API Security를 배포한 해당 고객은 이제 실시간으로 의심스러운 비정상 행동을 탐지하고 인시던트 대응 프로토콜을 트리거할 수 있습니다. 따라서, 지연된 보고 및 접속 로그에 의존해 문제 해결 프로세스를 진행할 필요가 없습니다. Akamai API Security로 의심스러운 행동이 탐지되면 고객의 API 게이트웨이, SIEM 시스템, 기타 정보 보안 엔진에 보고되어 전체 보안팀에 알려집니다. 고객은 취약점의 사용 사례와 심각도에 따라 직원이 수동, 반자동 또는 완전 자동으로 문제를 해결하도록 선택할 수 있습니다.