Akamai 고객 사례

Akamai API Security로 고객 보호

수천 개 고객사의 컴플라이언스와 수만 개의 API의 안전을 지원하는 보안 리더

Netskope는 클라우드, 데이터, 네트워크 보안을 재정의하는 글로벌 사이버 보안 선도업체입니다. Fortune 100대 기업 중 25여 곳의 기업을 포함해 수천 개의 고객이 진화하는 위협에 대응하고, 기술 전환을 촉진하고, 규제 의무를 준수하기 위해 Netskope를 신뢰합니다.

Netskope는 수많은 미션 크리티컬 기술 영역 중 전 세계 수만 개의 API 보안을 책임지고 있으며, 이를 위해서는 기존의 애플리케이션 보안을 넘어서는 새로운 접근 방식이 필요하다는 사실을 깨달았습니다. 고객사 중 한 곳의 API 보안 체계에 허점이 있음을 발견한 Netskope는 악성 API 공격으로부터 고객을 보호하는 데 필요한 차세대 툴로 Noname Security (현재 Akamai가 인수한 기업)를 선택했습니다.

방화벽을 넘어선 보안

고객이 소규모 애플리케이션을 배포하든 무수히 많은 마이크로서비스가 포함된 대규모 애플리케이션을 배포하든, 실제로는 모두 API를 사용하고 있으며, 이는 노출된 모든 API가 공격표면의 일부가 된다는 것을 의미합니다. 예를 들어, Netskope는 고객의 API 자산 내에서 탐지되지 않았고 Netskope가 볼 수 없었던 남용이 있다는 사실을 발견했습니다. 이러한 이유로 Netskope의 AppSec 팀은 자체 API는 물론 고객의 API와 기타 공개 디지털 자산을 모두 보호할 수 있는 솔루션을 찾기 시작했습니다.

Netskope는 이 문제가 기존의 문제와 다르다는 것을 알았고, 이는 웹 애플리케이션 방화벽과 같은 레거시 솔루션을 사용하거나 기존의 애플리케이션 보안 테스트를 진행할 수 없음을 의미했습니다. 로그의 양, 공격의 종류, API 남용 종류를 고려할 때 새로운 접근 방식이 필요했습니다.

netskope

위치

캘리포니아주
샌타클래라
netskope.com

업계

첨단 기술

솔루션

Akamai API Security

주요 효과

- 완벽하게 보호되는 API 수명 주기
- API 공격 실시간 차단
- API 스펙 자동 생성

Akamai

Netskope의 부CISO인 제임스 로빈슨(James Robinson)도 엔터프라이즈급으로 확장하려면 머신 러닝과 고급 툴을 활용해 API 자산에 대한 완벽한 가시성을 확보해야 한다는 사실을 잘 알고 있었습니다. 하지만 보안팀은 새로운 툴을 도입하려면 개발자가 파트너가 되어야 한다는 사실을 잘 알고 있었습니다.

보안팀의 승리

Netskope는 Noname API Security Platform(현재 Akamai API Security의 일부)을 사용해 프리프로덕션과 프로덕션 중 모두에서 API를 보호하기로 결정했습니다. 프로덕션 중인 API를 보호하기 위해 Akamai API Security의 검색 모듈을 사용해 고객의 내부, 외부, 써드파티 API에 대한 정확한 인벤토리를 확보하고 해당 API를 통과하는 모든 민감한 데이터를 분류했습니다. 정확한 인벤토리를 확보한 후에는 런타임 보호 모듈을 사용해 비정상을 탐지하고 API 공격을 실시간으로 차단했습니다.

프리프로덕션 관점에서 Netskope는 기업이 API 배포 전에 취약점과 잘못된 설정을 테스트하는 데 도움이 되는 Akamai의 API 보안 테스트 솔루션을 사용했습니다. 이 솔루션은 악성 트래픽을 시뮬레이션하는 100개 이상의 동적 테스트를 자동으로 실행할 수 있어 기업의 개발자가 코드를 보호하는 데 도움이 될 뿐만 아니라 고객에게 출시하려는 API 제품의 안전성을 보장합니다.

평가 단계에서 개발자는 작업을 더 쉽게 만들어줄 기능을 즉시 확인했습니다. 개발자는 너무 오래된 API 스펙을 가지고 있지 않을 때 Akamai가 도움을 줄 수 있다는 것을 알았고 이제 신속하게 스펙을 구축할 수 있게 되었습니다. 스펙이 자동으로 생성되기 때문에 API를 이해하기 위해 코드를 살펴볼 필요가 없습니다. 로그와 트랜잭션도 마찬가지입니다. 개발자는 여러 시스템에서 쿼리를 실행하고 로그라인을 살펴볼 수 있습니다.

당연히 이 플랫폼은 보안팀에게도 큰 도움이 되었습니다. 보안팀은 기존의 공격을 탐지하기 시작했을 뿐만 아니라 더 정교한 위협도 발견했습니다.

> 내부적으로 솔루션을 검토하기 시작했을 때 파트너가 될 개발자가 필요했습니다. 개발자의 지원 없이는 애플리케이션의 핵심인 중요 시스템에 접근할 수 없을 것입니다.
>
> - 제임스 로빈슨
> 부CISO, Netskope

향후 전망: 고객 컴플라이언스 유지

앞으로 Netskope는 Akamai를 사용해 API 거버넌스를 해결함으로써 자사와 고객이 전 세계적으로 확대되고 있는 데이터 개인정보 보호법 및 요구 사항을 계속 준수할 수 있도록 할 계획입니다. 또한 클라우드와 온프레미스 모두에 Akamai API Security를 배포하면서 다양한 사용 사례를 지속적으로 탐색할 계획입니다. 온프레미스 배포는 Netskope와 공공 부문 및 기타 규제가 엄격한 업계의 고객들에게 획기적인 전환점이 되었습니다.

> “Noname은성공적이었을 뿐만 아니라, 더 빠르고 효과적인 배포를 지원해 시장에 더 빨리 진출할 수 있도록 도와주었습니다.
>
> - 제임스 로빈슨
> 부CISO, Netskope

기업은 데이터가 이동하는 모든 곳에서 데이터를 보호하고, 디지털 전환 노력을 지원하고, 기술로부터 더 높은 효율성과 투자 수익률(ROI)을 실현하기 위해 SASE(Secure Access Service Edge) 아키텍처를 빠르게 도입하고 있습니다. Netskope는 성공적인 SASE 아키텍처에 필요한 보안 서비스를 설명하는 SSE(Security Service Edge)의 CASB, SWG, ZTNA, 서비스형 방화벽 및 기타 구성요소 분야에서 이미 널리 인정받는 전문가이자 혁신 기업입니다.

그러나 SASE의 인기에도 불구하고 'SASE'로 의심스럽게 판매되는 단편적인 제품 세트에는 종종 혼란스러운 벤더사 메시지가 수반됩니다. 이러한 제품 대부분은 기본적으로 통합되어 있지 않거나 기술 환경을 간소화할 수 없으며, 중요한 네트워크 및 인프라 혁신 기능이 부족해 보안 인시던트, 네트워크 다운타임, 형편없는 ROI 등의 리스크가 높습니다.

Netskope Borderless SD-WAN은 완전히 통합된 SASE 플랫폼에서 Netskope 인텔리전트 SSE와 결합해 이러한 문제를 해결합니다.

| 2024년 9월 발행

Akamai