Akamai

백서

API 탐지 및 대응을 위한 11 가지 핵심 기능

API 보안 전략의 진화

서론

API는 기업이 고객에게 제공하거나, 내부적으로 사용하거나, 벤더사 및 공급업체에 제공하는 모든 애플리케이션에서 중요한 역할을 합니다. API는 기술 사이의 정보를 교환하는 역할을 하는데 민감한 데이터를 다루는 경우가 많습니다. 또한 API는 애플리케이션뿐만 아니라 클라우드 전환, 생성형 AI 툴, 디지털 공급망에서 사용됩니다.

문제는 API가 기업의 공격 표면에서 눈에 띄는 자리를 차지하고 있다는 점입니다.

기업이 서둘러 혁신을 추구하는 상황에서 API를 급히 개발하고, 충분한 테스트를 거치지 못하며, 설정 오류가 발생하고 보안 제어 기능이 없는 상태에서 프로덕션에 출시됩니다. 또한 이러한 API는 보안팀이 API 자산의 주요 부분에 대한 가시성을 제대로 확보하지 못할 정도로 복잡하고 광범위하게 확산되고 있습니다. 적절한 가시성을 갖추지 못한 기업의 특징은 다음과 같습니다.

1. 민감한 데이터, 인터넷 및 공격자에 대한 노출 상태가 확인되지 않은 채 관리되지 않거나, 잊혀졌거나, 잔존하는 API를 탐지할 수 없습니다.
2. 따라서 API 리스크를 평가할 수 없습니다. 예를 들어, 전체 API 인벤토리를 보유한 기업의 27%만이 민감한 데이터를 반환하는 API를 알고 있는 것으로 나타났으며, 이는 2023년의 40%보다 낮은 수치입니다.
3. 결국 공격자들이 자주, 그리고 쉽게 악용하는 API 중심 취약점으로 가득 찬 공격 표면에 노출됩니다.

지금까지 많은 기업들은 API 관리와 기본적인 보안을 확보하기 위해 일반적으로 사용되는 툴에 의존해 왔습니다. 그러나 지난 12개월 동안 이러한 기업에서 API 보안 인시던트를 경험한 비율이 84%(2023년의 경우 최대 78%)에 달하면서 변화가 요구되고 있습니다.

API 공격 건수가 늘어나고 더욱 정교해짐에 따라 API 게이트웨이, 웹 애플리케이션 방화벽(WAF), 웹 애플리케이션 및 API 보안(WAAP) 플랫폼 등의 툴에 새로운 보호 레이어를 추가하는 방법을 모색해야 합니다.

이러한 새로운 레이어는 사용자 환경의 모든 API 및 관련 리스크에 대해 보다 효과적인 가시성을 제공해야 합니다. 여기에는 다음과 같이 관리되지 않는 상당수의 API가 포함됩니다.

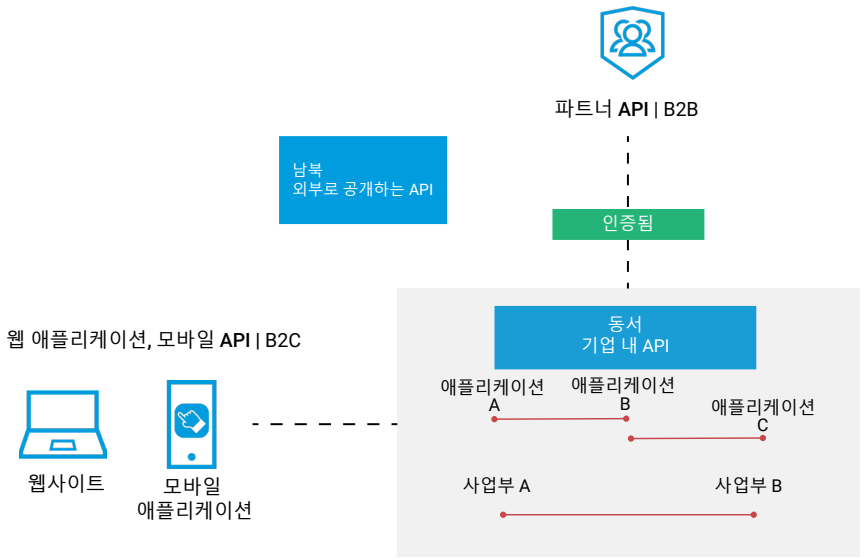
- 더 이상 사용하지 않아야 하지만 여전히 활성 상태인 좀비 API
- 문서화되지 않았으며 제거 또는 공식적인 거버넌스 프로세스로 이관되어야 하는 섀도 API

또한 기업은 OWASP 10대 API 보안 리스크에 자세히 설명되어 있는 모든 위협을 비롯한 API 남용 및 공격을 탐지하고 해결하기 위해 보다 심층적인 기능이 필요합니다. 그리고 API의 전체 수명 주기 동안 취약점을 찾아내고 해결하는 것을 목표로 초기 개발 단계부터 프로덕션에 이르기까지 엄격한 실시간 보안 테스트를 API에 도입해야 합니다.

그렇다면 앞으로 발생하는 모든 문제에 새로운 툴을 계속 도입해야 할까요? 그렇지 않습니다. 대신 오케스트라에서 해당 파트에 적절한 연주자를 배치해 올바른 타이밍에 올바른 음을 연주하게 하듯이 상대와 정확하게 협업하는 방법이 적합합니다.

API 보안 스택에 새로운 레이어를 추가하는 방법에 대해 생각할 때에는 보안팀이 다른 위협에 적용하는 심층 보안 접근 방식(예: 랜섬웨어 공격 탐지, 예방 및 그 효과를 방어하기 위한 강력한 관리 수단 배포)을 고려하세요. 기업은 API에 대해 이렇게 생각해야 합니다.

이 백서에서는 API 위협 탐지 및 대응에 중점을 두고 API 보안 전략에 포함시킬 수 있는 11가지 주요 기능을 살펴봅니다.



핵심은 바로 '맥락'

API 위협 탐지 및 대응은 API 보안 전략의 어떤 부분에 대응할까요?

직접 경험하셨듯이 API는 더 많은 활용 사례를 가능하게 하고, 변화를 가속화하고, 보다 민감한 데이터를 전송하며, 더 많은 사용자에게 개방됨으로써 기업의 운영 방식을 변화시켰습니다. 기업들이 웹 애플리케이션 인터페이스보다 많은 API 채널을 만들었다는 것은 놀라운 일이 아닙니다. 그리고 이렇게 급증하는 API가 점점 더 많은 핵심 비즈니스 데이터 및 비즈니스 로직을 포함한 채 내장됨에 따라 리스크는 더욱 복잡해집니다.

보안팀이 이미 보호하고 있는 다양한 기술(애플리케이션 등)에서 API가 널리 사용되기 때문에 대부분의 보안 제품은 API를 어떤 형태로든 지원하고 있습니다. 그러나 API와 애플리케이션은 동일하지 않으며 일부 컴플라이언스 프레임워크에서는 서로 다른 자산으로 나타납니다. 가령 기존의 애플리케이션 보안 제품에 단편적인 API 위협 방어 기능을 추가하는 것만으로는 충분하지 않습니다. API는 대부분의 기업에서 일반적으로 기울이는 것보다 더 큰 관심을 필요로 합니다. 오늘날 보안팀은 API를 고유한 리스크 특성을 지닌 별도의 자산 클래스로 인식하고 모든 API를 대규모로 확인 및 보호하는 핵심 기능을 찾아야 합니다.

과거에 기업이 API 인벤토리와 API 관리 및 보안을 위한 몇 가지 기본 툴을 갖고 있었다면 알려진 범위의 일반적인 API 공격을 효과적으로 차단할 수 있었을 것입니다. 그러나 오늘날의 공격자들은 기업과 마찬가지로 지속적인 개선을 위해 혁신하고 있습니다.

- 공격자들은 대부분의 기업이 API를 방어하기 위해 사용하는 툴을 우회하기 위해 논리적으로 기법을 발전시키고 있습니다.
- 대부분의 기업이 AI를 사용하는 방식과 비슷하게 공격자들도 생성형 AI 기능의 24시간 지원을 통해 제한된 인적 역량을 보강하고 있습니다.
- 또한 공격자들은 기업의 API 연결 디지털 공급망에서 취약한 링크(예: API 보안을 우선하지 않는 B2B 파트너)를 점점 더 많이 노리고 있습니다.

예를 들어, 일부 형태의 API 남용은 부여받은 API 인증정보를 허가되지 않은 방식으로 사용하는 고객과 파트너로부터 발생합니다. 정상적으로 보이는 API 인증정보나 보안 토큰을 탈취하는 방법도 있습니다. API 클라이언트 구축에 숨겨진 취약점은 공격자가 기존 보안 툴로는 탐지할 수 없는 방식으로 API를 남용하기 위해 악용할 수 있는 또 다른 공격 기법입니다.

다행히 기업은 이렇게 빠르게 진화하는 공격 방법으로부터 API를 보호하는 데 필요한 중요 기능을 대규모로 이용할 수 있습니다. API 및 교환되는 데이터를 공격으로부터 보호하기 위한 조치를 취하기 시작할 때 사용할 수 있는 11가지 핵심 기능에 대해 자세히 알아보세요.

중요 기능 #1

지속적인 API 검색 및 체계 관리

기업 전체에서 사용 중인 API에 대한 포괄적이고 지속적으로 업데이트되는 인벤토리는 모든 API 보안 전략의 중요한 토대입니다. 기업은 자사 환경에 존재하는지 모르는 대상을 보호할 수 없기 때문입니다. 많은 API 보안 제품이 일정 수준의 API 검색을 수행한다고 주장하지만 온디맨드 또는 일상적인 작업으로 제한됩니다. 따라서 플랫폼의 API 검색 기능에 다음과 같은 기능이 포함되어 있는지 확인해야 합니다.

- 한 번만 사용되는 API의 검색을 포함해 24시간 내내 API를 자동으로 지속적으로 검색(온디맨드 또는 일일 검색만으로는 불충분)
- 다양한 기술 및 인프라 전반의 API 검색
- 새로 배포된 API를 검색하고 잘 문서화된 API와 비교해 섀도 API 탐지
- 각 API 서비스 및 엔드포인트의 리스크 점수를 산정해 보안 및 개발팀이 핵심을 찾아내고, 감염된 경우 잠재적으로 가장 중대한 영향에 따라 API의 우선순위를 지정하는 데 도움이 됩니다.
- OWASP 10대 API 보안 리스크에 나온 취약점 등 알려진 API 취약점 사례 파악

가시성 개선

API 인벤토리에 대한 가시성 유지

중요 기능 #2
API 행동의 시각화

실제 API 행동(API 호출)을 시각화하는 기능은 API 보안 플랫폼의 기본 기능입니다. 이 기능은 보안, 개발, 운영팀의 주요 이해관계자가 API가 어떻게 사용되거나 남용되는지 확인하고 파악해 팀 간에 소통하고 사례를 조사할 수 있도록 하는 데 필요합니다. 구체적으로 살펴봐야 할 시각화 기능은 다음과 같습니다.

- **조사:** 알림의 특정 트리거를 탐지할 수 있도록 모든 알림에는 호출별로 원래의 API 활동을 조사할 수 있는 기능이 포함되어야 합니다.
- **데이터 충실도 및 보강:** 모든 API 호출에 대해 사용자가 누구인지, 어떤 작업을 사용했는지, 어떤 레코드에 접속하거나 조작했는지, 어떤 헤더와 매개 변수를 사용했는지 등을 파악할 수 있어야 합니다.
- **데이터 프라이버시:** 데이터 충실도는 중요하지만, 민감한 데이터를 유휴 상태로 저장할 수는 없습니다. 솔루션은 트래픽을 분석하고 관련 메타데이터만 전송해 대시보드를 업데이트해야 합니다.

중요 기능 #3

사용자 엔티티의 맥락을 통해 API 남용 시도 탐지

보안팀은 IP 주소와 같은 엔티티, 비즈니스 프로세스 엔티티(예: 결제 ID)에 대한 악성 활동을 추적할 수 있는 기능이 필요합니다. 특히 이러한 기능은 다른 관련 식별자가 API 남용에 대한 맥락을 제공할 수 있는 경우 여러 IP의 공격을 상호 연관시키는 기능과 함께 사용할 때 더욱 효과적입니다.

예를 들어 알 수 없는 사용자가 /api/getpaymentID/50을 ID로 사용해 유통회사의 API를 호출한다고 가정해 봅시다. 이 시나리오에서 유통회사의 보안팀은 회사의 플랫폼에 있는 다른 모든 사용자가 한 종류의 결제 ID에 연결되어 있음을 알고 있습니다. 갑자기 알 수 없는 사용자가 매번 ID 번호를 조금씩 조정하며(예: /api/getPaymentID/51, ...52, ...53, ...54) 반복 호출을 수행하고 있다는 것을 보안 분석가가 발견한 경우 이는 API 남용 시도를 나타내는 주요 지표입니다.

비정상적인 사용자 행동에 대한 실시간 인사이트 확보 여부로 유출 시도가 차단되는지, 아니면 API 공격이 성공하는지가 좌우됩니다.

$943,162

지난 12개월 동안 API 보안 인시던트를 경험했다고 보고한 미국의 CISO, CIO, CTO에 따르면, 이 금액은 인시던트를 해결하는 데 드는 평균 비용입니다.

2024년 API 보안 영향 연구에서 업계 동료의 관점과 경험에 대해 자세히 알아보세요.

중요 기능 #4
행동 애널리틱스 및 탐지

사용자 엔티티나 심지어는 개별 세션의 개별 API 호출을 분석하면 보안팀에 도움이 될 수 있지만, 전반적인 상황에 초점을 맞춰 포괄적인 API 위협 탐지를 수행하는 것이 중요합니다. 전체 API 자산에서 행동 패턴과 비정상을 심층적으로 파악하기 위한 기능을 확보하는 것이 좋습니다. API 행동이 비정상적인지, 즉 API가 감염되었을 가능성을 확인하려면 API 사용을 장기간 분석해야 하며, 오랜 기간 면밀한 행동 추적을 통해 구축된 맥락을 기반으로 분석해야 합니다. 이는 지속적으로 행동을 모니터링해 비정상을 탐지하는 보안팀에게 안정적인 기준을 제공합니다.

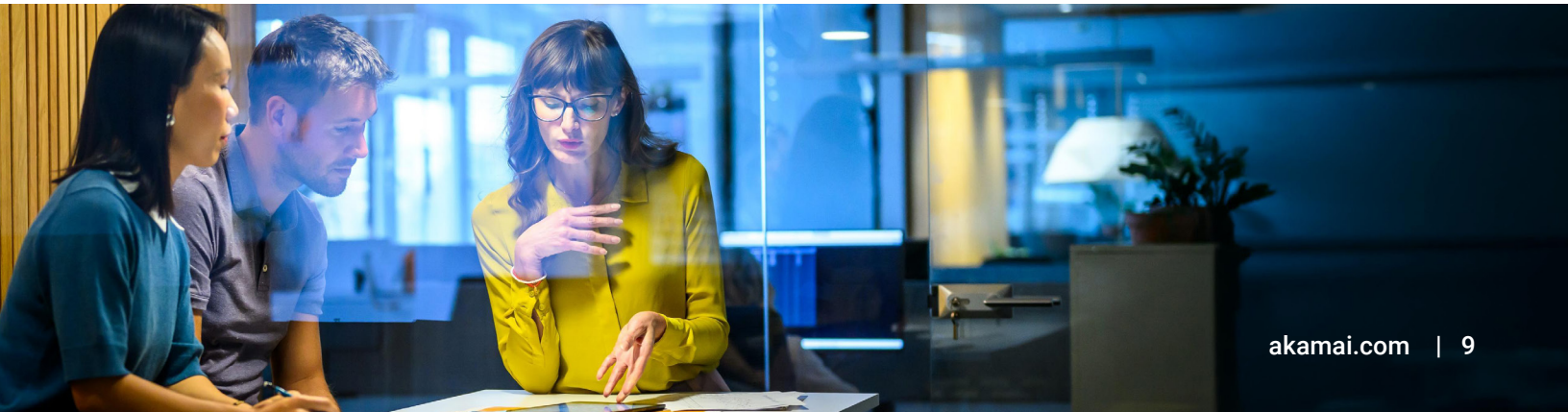
중요 기능 #5
API의 사양 변경 파악

시장 수요와 비즈니스 요구 사항이 변화하는 상황에서 API는 끊임없이 변화하고 있습니다. 그 결과 빠르게 발전하는 기업의 요구사항을 충족하고, 버그를 해결하고, 개선된 기술을 도입하기 위해 기업들은 새로운 엔드포인트 구축을 지속적으로 출시하고 있습니다. API 사양을 기반으로 이러한 변경에 따라 API 문서를 업데이트하는 것이 중요하며, API 트래픽이 항상 해당 사양과 일치하도록 특별한 주의를 기울여야 합니다.

남용과 공격 속에서 안정적인 API를 만들려면 기업은 API의 사양 변경을 파악하기 위한 기능을 확보해야 합니다. 이를 통해 기업은 실시간 API 트래픽을 정의된 사양과 지속적으로 비교해 API 문서의 불일치 또는 격차를 정확히 찾아낼 수 있습니다.

API 사양 변경 기능은 프로덕션에 접속하는 문서화되지 않은 엔드포인트나 불일치를 발견하는 경우 개발자 및 보안팀에 알림을 보내 다음과 같은 효과를 얻을 수 있습니다.

- 문제가 심각해지기 전에 먼저 해결
- API가 의도한 대로 작동하도록 보장
- 이러한 API가 지원하는 애플리케이션의 보안 강화
- 기업의 API 생태계의 무결성 유지



중요 기능 #6
B2B 및 동서 API 범위

API 사용의 가장 큰 성장 영역은 내부와 외부를 모두 대상으로 하는 B2B 사용 사례입니다. API 보안은 남북(외부 대상) 및 동서(내부 대상) 인스턴스를 모두 포함한 B2B, 머신 대 머신 API를 지원해야 합니다.

B2C 웹 애플리케이션은 WAAP 및 WAF 플랫폼의 보호를 받지만, 내부 동서 API 또는 B2B API를 통해 파트너에게 노출되는 독점 애플리케이션 기능과 같이 가장 민감한 종류의 API 활동은 WAAP를 통과하는 경우에도 여전히 감염될 수 있습니다.

B2B 파트너 API에서 사용자가 인증을 받으면 안전한 것으로 간주해 추가 모니터링을 수행하지 않는 경우가 많습니다. 이로 인해 많은 기업의 API 보안 체계에 심각한 공백이 발생합니다. API 활동과 광범위한 위협 환경을 전체적으로 파악하려면 모든 사용 사례에 대해 효과적인 가시성, 옵저버빌리티, 모니터링을 제공하는 접근 방식을 취해야 합니다.

중요 기능 #7
맥락이 포함된 의미 있는 알림

기업이 API 활동과 행동 애널리틱스에 대해 대규모로 가시성을 확보하면 API 활동에 대한 알림이 훨씬 더 많은 의미를 가지게 됩니다. 그러면 실제 API 위협에 주의를 기울이고 리소스를 집중할 수 있는 방법은 무엇일까요? 공격자 신뢰도 엔진은 API 행동, 네트워크 트래픽 패턴, 지리적 위치 데이터, 위협 인텔리전스 피드 및 기타 맥락 요소 등 외부 및 내부 신호를 평가하도록 훈련된 고급 머신 러닝 알고리즘을 사용하며, 이를 통해 탐지된 런타임 인시던트가 악성 활동의 결과인지 확인할 수 있습니다. 보안팀은 이 기능을 통해 중요한 위협을 신속하게 파악할 수 있습니다. 이 기능은 확률이 높은 공격에 대한 자동적인 문제 해결 및 알림 흐름을 만드는 기능과 함께 사용해야 합니다.

중요 기능 #8
맞춤형 자동 대응

기존의 인라인 API 접근 방식은 자동화된 조치를 취해 의심스러운 API 공격을 차단할 수 있지만, 기업이 공격을 탐지할 수 있어야 한다는 단점이 있습니다. API에 대한 행동 애널리틱스와 비정상 탐지는 시간이 지남에 따라 훨씬 더 많은 비즈니스 맥락에서 수행되기 때문에 심층적인 탐지를 통해 비정상이 드러날 수 있습니다. 이를 통해 광범위한 자동화된 맞춤형 대응의 정확도를 높일 수 있습니다. 사례는 다음과 같습니다.

- 지원되는 API 게이트웨이 및 콘텐츠 전송 네트워크(CDN) 엣지 필터에서 트래픽 차단 또는 스로틀링
- 보안 및 비즈니스 이해관계자를 위한 이메일 알림
- 개발자를 위한 티켓 생성
- 웹훅 트리거

API 위협이 증가함에 따라 기업이 확장된 보안팀의 역량을 극대화하기 위해 무엇을 할 수 있을까요? 멀티 액션 워크플로우의 생성 및 관리를 간소화해 효율성과 생산성을 향상시키는 자동화 기능을 찾아야 합니다. 적절한 자동화 기능은 복잡한 이벤트 대응 프로세스를 생성하고 ServiceNow, Jira, Azure DevOps를 비롯한 수많은 써드파티 서비스와 핵심 API 보안 솔루션 간에 인시던트 관련 데이터를 동기화할 수 있는 노코드 시각디자이너 인터페이스를 제공해야 합니다.

중요 기능 #9
API 트래픽 분석

기업은 데이터 레이크를 배포하지 않고 해당 환경에서 API 트래픽을 기록, 시각화 및 분석하는 상시가동형 기능을 필요로 합니다. 전형적이고 비정상적인 API 활동을 포함해 애플리케이션 환경 전반에 걸쳐 특정 기준에 맞는 API 데이터 흐름을 기록함으로써, 기업은 위협을 보다 효과적으로 찾아내고 의심스러운 사용자 리스크 노출 및 비정상적인 API 행동을 관리할 수 있습니다. 또한 기업이 사전 정의된 필터 및 룰에 따라 트래픽을 캡처 및 유지할 수 있도록 특정 사용 사례에 맞게 맞춤화할 수 있는 API 트래픽 감사 기능을 갖추는 것이 중요합니다.

중요 기능 #10
엄격한 실시간 API 테스트

혁신을 추구하는 과정에서 기업은 취약점과 설계 결함을 발견하지 못하고 이를 포함한 API를 프로덕션에 출시하고 있습니다. 기업은 개발 중인 API 테스트에 대해 시프트 레프트 접근 방식을 도입함으로써 이러한 문제를 방지할 수 있습니다. 핵심 기능은 다음과 같습니다.

- OWASP 10대 API 보안 리스크에 있는 종류를 포함한 악성 트래픽을 시뮬레이션하는 자동 테스트 실행
- 확립된 거버넌스 정책 및 룰에 따라 API 사양 검사
- 요청 시 API 테스트 또는 CI/CD 파이프라인의 일부로 테스트

중요 기능 #11
플랫폼 중립적 보호

API 서비스는 일반적으로 기업 내 여러 그룹에서 다양한 플랫폼과 기술을 사용해 구축하는 경우가 많습니다. 예를 들어 일부 API는 온프레미스에서 구축되는 반면, 퍼블릭 클라우드에서 실행되는 API도 있습니다. 종종 기업은 역방향 프록시, API 게이트웨이, WAF, CDN 등의 중간 기술을 사용하곤 합니다. 이러한 기술은 비즈니스적 가치를 제공하지만 API 가시성의 복잡성을 가중시킵니다.

이러한 각 기술로부터 API 활동 데이터에 접속할 수 있는 기능이 반드시 필요합니다. 플랫폼 중립적인 API 위협 방어 접근 방식은 구축 세부 정보나 사용 중인 인프라에 관계없이 기업이 항상 API 활동을 포괄적으로 파악하도록 지원합니다. 이를 통해 다음과 같은 보호 범위를 제공합니다.

- 모든 부서, 인수한 회사, 환경
- API 게이트웨이 사용 여부와 상관없이 승인된 API 및 섀도 API 모두

또한 플랫폼 중립적인 접근 방식은 남북 API를 넘어 가시성을 확장하며 퍼블릭, 파트너, 내부 동서 API를 포함합니다.

API 위협 방어 플랫폼으로 최대한 넓은 가시성을 확보하면 외부 공격자의 리스크뿐만 아니라 내부자 위협과 파트너 기업의 API 남용으로부터 기업을 보호할 수 있습니다.

결론

API는 오늘날 디지털 및 클라우드 중심의 경제에서 고객에게 서비스를 제공하고 매출을 창출하며 효율적으로 운영할 수 있게 하는 기업의 핵심 구성요소입니다. 그러나 지속적인 성장, 민감한 데이터에 대한 근접성, 보안 제어의 부재로 인해 API는 주요 리스크 소스가 되고 있습니다.

Akamai API Security는 이 백서에서 다룬 11가지 중요한 기능을 모두 제공합니다. 따라서 기업은 기존의 접근 방식에 기반해 다음과 같은 필수 기능을 구축할 수 있습니다.

- API 검색
- 리스크 평가(민감한 데이터에 대한 노출 포함)
- API 남용 및 공격 탐지
- 보안 리스크 및 취약점에 대한 API 테스트

OWASP 10대 API 보안 리스크로부터 보호할 수 있는 방법에 대해 자세히 알아보세요.

맞춤 Akamai API Security 데모 일정을 예약하고 어떤 도움을 받을 수 있는지 알아보세요.

Akamai 보안은 성능이나 고객 경험에 영향을 주지 않으면서 모든 상호 작용 지점에서 비즈니스의 원동력이 되는 애플리케이션을 보호합니다. 글로벌 플랫폼의 규모와 위협에 대한 가시성을 활용해 고객과 협력함으로써 위협을 예방, 탐지, 방어하고 브랜드 신뢰를 쌓고 비전을 실현할 수 있도록 지원합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관해 자세히 알아보려면 akamai.com과 akamai.com/blog를 확인하거나 X(기존의 Twitter)와 LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2025년 1월 발행.