API 런타임 보안 최종 가이드

목차

서론

API 보안이 필수 과제인 이유

기업들은 고객의 요구사항을 충족하기 위한 경쟁에서 애플리케이션, 서비스, 생성형 AI 툴을 신속하게 개발, 생산, 개선해야 하는 압박에 직면합니다. 이렇게 빠른 속도가 필요한 환경에는 숨은 리스크가 발생하기 마련인데, 바로 이러한 모든 혁신의 기반이 되는 API가 종종 설정 오류, 코딩 오류가 있거나 보안 제어 기능이 누락된 채로 구축된다는 점입니다. 그리고 이러한 API가 프로덕션 단계에 도달하면, 최종 사용자와 상호작용할 뿐 아니라 API를 감염시키고 API가 교환하는 데이터에 접속할 방법을 끊임없이 테스트하는 공격자들이 나타나게 됩니다.

설정 오류가 있고 감염된 API는 점차 심각한 데이터 유출의 주요 원인이 되고 있지만, 디지털 생태계 내에서 수천 건의 API 호출을 파악할 수 있는 기업은 거의 없습니다. 런타임 API 위협으로부터 완전히 보호되는 기업은 훨씬 더 적습니다.

예를 들어, 2021년 한 피트니스 유통회사는 나이, 성별, 도시, 체중, 생일을 포함한 데이터에 대한 무단 요청을 허용하는 버그를 사용자 계정 데이터용 API에서 발견했습니다. 다행히 한 보안 연구원이 이 취약점을 탐지해 기업에 보고했지만, 이와 같은 버그는 몇 주 또는 몇 달 동안 발견되지 않은 채로 악용될 수 있습니다.

API 보안과 관련해, 기업이 일반적으로 사용하는 기존 툴(예: API 게이트웨이 및 웹 애플리케이션 방화벽)을 사용해도 기본적인 보안이 가능합니다. 그러나 API 공격이 증가하고 더 정교함에 따라 오늘날의 보안팀은 추가적인 보안 레이어를 필요로 합니다. 핵심은 취약점, 잠재적 공격 경로, 악의적 활동 및 API 행동에 대한 심층적인 인사이트를 통해 기존 제어를 강화하는 것입니다.

기업은 다음의 4가지 영역을 아우르는 포괄적 API 보안 솔루션을 통해 이러한 역량을 확보할 수 있습니다.

1. API 검색
2. API 체계 관리
3. API 런타임 보안
4. API 보안 테스트

이 가이드에서 다루는 내용

API 런타임 보안은 API가 정상적으로 작동하는 동안 요청을 운영 및 관리할 때 API를 보호하는 프로세스입니다. 이 가이드에서는 설정 오류 및 악용 방어를 위한 API 모니터링과 API 공격 방어를 비롯한 API 런타임 보안에 대한 주요 요구사항에 대해 설명합니다. 또한 런타임 방어에 관한 기본 사항을 살펴보고 Akamai API Security가 제공하는 런타임 방어 기능을 소개합니다.

런타임 보안이 필요한 이유

API 런타임 보안은 API가 작동하고 의도한 최종 사용자 및 공격자와 상호 작용할 수 있는 수명 주기의 프로덕션 단계 전반에서 API를 보호합니다. 효과적인 런타임 보안 기능은 기업이 악성 API 요청을 신속하게 탐지하고 해결하도록 지원하는 기능을 통해, 배포 후에 발생하는 다음과 같은 다양한 위협으로부터 API를 보호할 수 있습니다.

- API에서 대량의 민감한 데이터를 빼내는 공격자
- 보안 버그를 악용하는 권한 상승 공격
- 정상 프로세스 외부에서의 무단 API 배포

런타임 API 위협을 차단하려면 API 접속, 사용, 행동 등 개별 API의 작업 맥락을 이해해야 합니다. 우선 API 자산의 범위를 알아야 합니다. Akamai의 API 검색에 대한 최종 가이드는 API 인벤토리의 중요성을 설명합니다. 완전한 API 인벤토리를 갖추면 모든 API 트래픽을 모니터링할 수 있고 각 API의 '일반적인' 행동을 이해할 수 있습니다. 또한 이러한 일반적인 행동을 기반으로 비정상 동작을 파악할 수 있습니다. API 런타임 보안은 다음을 탐지할 수 있습니다.

- 데이터 유출
- 데이터 정책 위반
- API 보안 공격
- 데이터 변조
- 의심스러운 행동

또한 런타임 보안 기능은 API 트래픽을 로깅하고, 민감한 데이터 접속을 모니터링하고, 위협을 탐지하며, 공격을 차단하거나 해결합니다.

공격에 대비한 API 트래픽 모니터링

API 트래픽 행동 관찰은 리스크를 파악하는 데 필수입니다. API 자산에 대한 정확한 파악 없이 모니터링 솔루션을 배포하면 가시성이 제한됩니다. API 풋프린트를 인벤토리화한 후에 API 런타임 보안은 트래픽 및 API 사용량을 지속적으로 모니터링하고 취약점과 설정 오류를 찾아내야 합니다.

비정상 행동 탐지

정상 API 행동의 기준을 정해두면 비정상적인 것을 파악할 수 있습니다. 과거 데이터를 재생하면 비정상 행동을 탐지하는 데 도움이 되며, 이를 통해 공격자의 의도를 알아낼 수도 있습니다.

잠재적인 비정상은 모두 애플리케이션이나 네트워크 내에서 발생하는 다른 작업의 맥락에서 추가로 조사해야 합니다. 예를 들어, 데이터 요청이 일반적으로 특정한 크기이고 API 호출이 일반적인 요청 범위를 벗어난 데이터를 요청하는 경우 플래그 지정을 해야 합니다. 악성 호출일 수도 있고 아닐 수도 있지만, 비정상에 대한 추가 조사가 필요합니다.

데이터 노출 탐지

자산 내에 있는 일부 API는 민감한 데이터를 전송하고 수신할 가능성이 높습니다. 공격자는 보안 취약점으로 인해 노출된 민감한 정보를 통해 권한을 확대하거나 기타 부적절한 접속 제어를 구성할 수 있습니다. AI와 머신 러닝은 실시간 트래픽 분석과 비정상 탐지에 도움이 되어 데이터 유출, 데이터 변조, 데이터 정책 위반, 의심스러운 행동, API 보안 공격에 대한 맥락별 인사이트를 제공할 수 있습니다.

점점 더 흔해지고 있는 공격 유형 중 하나는 사이버 범죄자가 유효한 API 키를 손에 넣는 것입니다. 공격자가 유효한 키를 손에 넣은 경우, 부적절한 API 사용 및 잠재적인 데이터 유출을 방지하는 단 하나의 방법은 비정상 행동과 데이터 노출을 탐지하여 차단하는 것입니다.

API 보안 감사

API 보안 감사 툴은 실시간으로 트래픽을 모니터링하고 공격 및 기타 악의적인 의도를 알려야 합니다. API 보안 감사는 최소한 다음을 수행해야 합니다.

- 지속적인 모니터링을 수행해 공격자와 악의적인 요청 탐지
- 내부 및 외부에서 API를 수동으로 스캔하여 유출을 촉진하거나, 악화하거나, 방어를 약화할 수 있는 설정 오류 및 간과한 부분 파악
- API에서 전송 또는 수신해야 하는(그리고 그래서는 안 되는) 데이터에 대한 정책 적용

API 런타임 보안은 또한 설정 오류 및 알려진 취약점을 파악하는 API 체계 관리를 통해 보완되어야 합니다. Akamai의 API 체계 관리 최종 가이드에서 더 많은 인사이트를 확인하세요.

필수적인 런타임 보안 기능

API를 적극적으로 개발 및 배포하는 기업의 경우, API 보안 프로그램의 일부로 강력한 런타임 보안이 필요합니다. 다음은 런타임 보안 툴에 반드시 포함되어야 하는 핵심 기능입니다.

실시간 아웃오브밴드 모니터링

API 보안 모니터링은 API 트래픽에 영향을 미치거나 느리게 만들거나 지연 시간을 발생시켜서는 안 됩니다. 네트워크 변경이나 번거롭고 설치하기 어려운 에이전트 없이 완전히 아웃오브밴드 형식으로 실행되어야 합니다. 런타임 보안 툴은 식별된 데이터 소스의 트래픽을 미러링하고 백그라운드에서 해당 트래픽 데이터를 분석해 발견된 모든 문제를 실시간으로 알려야 합니다.

Akamai는 기본적으로 에이전트리스 아웃오브밴드 실행을 지원하지만, 필요한 경우 에이전트 기반 탐지 및 인라인 차단 옵션을 제공합니다.

API 비정상 및 악용 탐지

API 수와 API 트래픽의 전체 규모가 계속해서 확장되기 때문에 수동적인 데이터 수집만으로는 충분하지 않습니다. API 활동을 지속적으로 분석해 비정상적인 이벤트를 탐지하고 보안 및 운영팀에 통보해야 합니다. 최첨단 플랫폼 툴은 AI와 머신 러닝 기능을 통합해 트래픽을 실시간으로 분석하고 데이터 유출, 데이터 변조, 데이터 정책 위반, 의심스러운 동작 및 API 보안 공격에 대한 맥락별 인사이트를 활용합니다.

API 공격 방어 및 리스크 해결

비정상이나 기타 다른 문제가 식별되고 알림이 만들어지면 이제는 시간이 가장 중요합니다. API를 통한 민감한 데이터의 무단 이동 또는 그밖에 다른 API의 오용으로 의심되는 경우 이를 탐지하고 해결해야 합니다. 런타임 보안은 기존 방화벽 및 API 게이트웨이와 통합해 API 오용을 방지할 뿐 아니라 가능한 경우 자동화된 수정 옵션을 제공해야 합니다. 팀에서 남용, 공격 또는 유출의 신호가 정상적이고 확장이 필요한지 여부를 판단하는 데 도움이 되는 공격자 신뢰 점수가 포함된 기능을 찾아보세요.

인시던트 대응 통합

일반적으로 런타임 보안 툴은 기업에서 사용하는 다른 보안, 모니터링 및 관리 툴과 쉽게 통합되어야 합니다. 예를 들어 인시던트가 발생하는 경우 런타임 보안 툴에는 적절한 팀에 해결 작업이 배정되도록 하는 데 필요한 통합 작업 기능이 포함되어 있어야 합니다. 설정 오류, 데이터 정책 위반 또는 의심스러운 행동이 탐지되면 올바른 수준의 상황 인식을 보장할 수 있도록 API 게이트웨이, SIEM 시스템 및 기타 정보 보안 엔진에 보고되어야 합니다. 팀은 공격자 신뢰 점수 기능을 사용해 불필요한 정보를 걸러내고 실제 API 보안 우선순위에 집중할 수 있습니다.

Rapyd

글로벌 결제 처리 및 핀테크 기업인 Rapyd는 100개국 이상에서 결제 시스템을 운영합니다. API 사용 및 행동에 대한 정밀한 가시성이 부족한 이 기업은 AWS 클라우드에서 운영되는 매우 복잡한 글로벌 시스템에서 공개 API와 수백 개의 내부 API를 보호하는 더 나은 방법이 필요했습니다. Rapyd는 모든 API에 대한 정밀한 인벤토리, 설정 오류 및 취약점에 대한 가시성, 그리고 더 논리적인 해결 방법을 위해 지능적으로 우선순위가 지정된 알림이 필요했습니다.

Akamai API Security는 머신 러닝을 사용해 모든 API에 대한 트래픽 기준선을 생성하는 런타임 보안 기능과 포괄적 가시성, 자동화된 비정상 탐지 및 해결을 통해 Rapyd의 요구사항을 충족했습니다.

고객 사례 전문 보기

"이제 Raptyd는 가능한 가장 과학적인 방법으로 리스크를 평가하고 운명을 통제할 수 있습니다.

- 니르 로텐버그(Nir Rothenberg)
Rapyd CISO

Akamai API Security의 런타임 보안

API 공격이 발생하는 경우 이를 탐지하고 차단할 수 있는 능력은 컴플라이언스 및 리스크 평가 프로그램의 필수 요소입니다. 다른 보안 제어 수단이 부족한 경우 이를 최후의 방어선으로 생각할 수 있습니다.

Akamai API Security의 런타임 보안 모듈에는 이전 섹션에서 설명한 모든 기능이 포함되어 있습니다. 가장 큰 기능은 실시간으로 API 공격을 탐지하고 차단하는 것입니다. 자동화된 머신 러닝 기반 모니터링 기능은 트래픽을 분석하고 데이터 유출, 데이터 변조, 데이터 정책 위반, 의심스러운 행동 및 API 보안 공격에 대한 맥락별 인사이트를 제공하는 데 사용됩니다. 런타임 보안은 API 트래픽에서 비정상 및 잠재적 위협을 탐지하고 사전에 선택한 인시던트 대응 정책을 기반으로 문제 해결을 용이하게 합니다.

런타임 보안은 WAF, API 게이트웨이, ITSMS, SIEM 및 기타 워크플로우 툴과 통합되어 공격에 대한 종합적인 방어 기능을 제공합니다. 사용자는 위협 해결을 완전히 자동화하거나 더 나은 가시성 및 제어를 위해 다양한 수준의 수동 개입을 요구할 수 있습니다. Akamai API Security 솔루션은 또한 Akamai 플랫폼과의 기본 통합을 통해 공격자 IP를 엣지에서 바로 차단할 수 있습니다.

이슈 생성

Akamai는 머신 러닝을 사용해 각 API에 대한 모델을 구축합니다. 그런 다음, 정상적인 행동에 관한 이 기준선을 사용해 개인이 접속 권한이 없는 데이터에 접근할 수 있는 BOLA(손상된 오브젝트 수준의 권한 확인)와 같은 API 비즈니스 로직 공격을 탐지합니다.

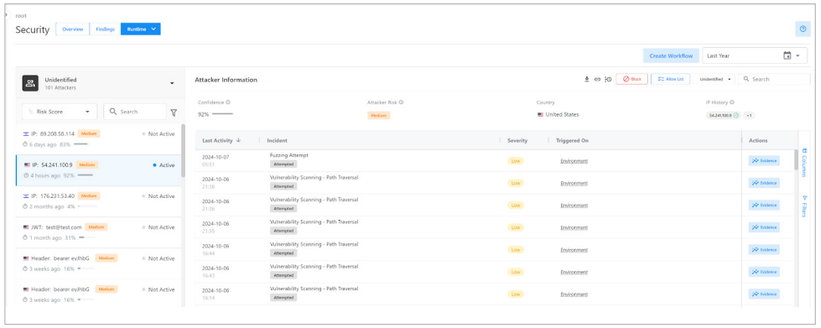
Akamai는 API 트래픽이 정상 행동에서 벗어날 때마다 실시간으로 이슈를 생성합니다. 이슈는 알림과 비슷하며, 비정상 API 행동이 탐지되거나 설정 오류가 발견될 때마다 생성됩니다. 이슈가 생성되면 Splunk 또는 QRadar와 같은 SIEM에 자동으로 알림을 전송할 수 있습니다. 또한 ServiceNow 또는 Jira와 같은 티켓팅 시스템으로 알림을 자동으로 전송할 수 있습니다.

이슈 세부 정보

Akamai API Security의 런타임 보안 모듈에서 발생하는 모든 문제에는 심각도, 상태, OWASP 10대 API 리스크에 대한 매핑, 그리고 해당되는 경우 공격자 세부 정보가 포함됩니다.

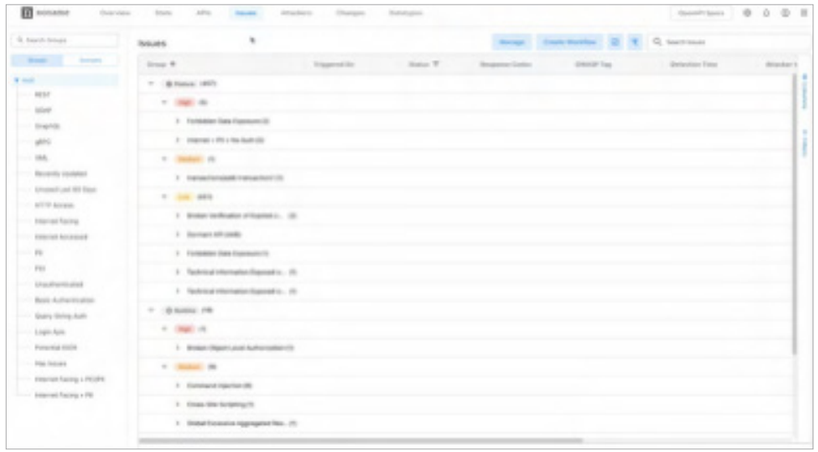
이슈 세부 정보 페이지에는 이슈에 대한 설명 및 기업에 미치는 잠재적 영향이 포함되어 있으며 해결 권장 사항을 제공합니다. 또한 기업은 Akamai API Security를사용해 특정 기간 동안 공격자가 어떤 유형의 행동을 취했는지 살펴보고, 각 공격에 대한 이전 기록을 확인하며, 악성 공격자에 대해 조치를 취할 수 있습니다.

예: 공격자의 행동에 대한 가시성

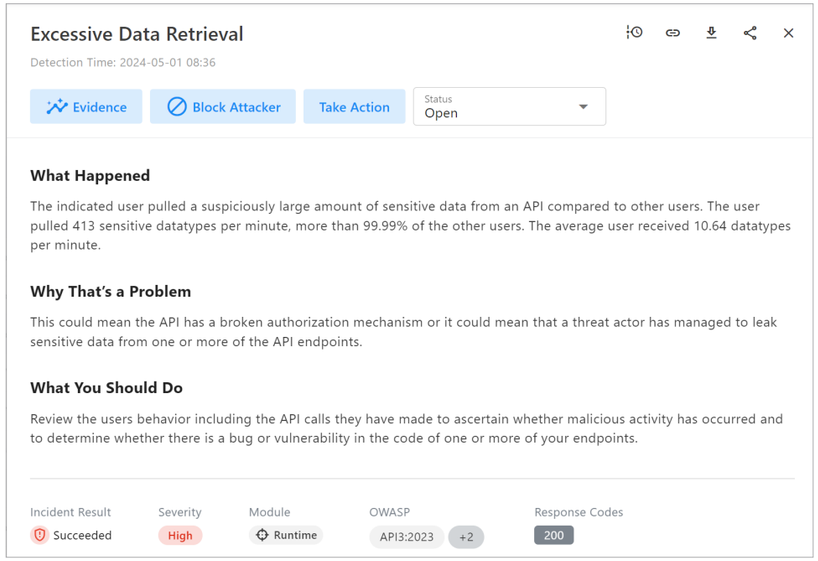


모든 이슈는 증거를 포함합니다. 증거는 문제가 발생하게 된 공격자 세션 세부 정보와 API 요청 및 응답 사본(헤더와 본문 모두)으로, 문제를 신속하게 분류하고 해결하는 데 도움이 됩니다. 직관적인 대시보드, 필터링 기능, 알림, 보고 기능을 갖춘 Akamai API Security 솔루션의 런타임 보안 모듈을 통해 기업은 발생한 일과 그 이유, 정확히 해야 할 사항을 파악할 수 있습니다.

예: API 이슈를 증거와 함께 보고



예: 과도한 데이터 검색에 대한 인사이트



정책 조치

Akamai API Security는 생성된 모든 이슈에 대해 반자동화된 정책 조치를 취할 수 있는 기능을 제공합니다. 티켓을 열거나 SIEM에 정보를 전송하거나 써드파티 시스템에 웹훅을 전송하는 등의 조치를 취할 수 있습니다. 공격자 차단도 포함될 수 있습니다. 사용 가능한 작업 유형은 Akamai 플랫폼에 구성된 통합 유형에 따라 결정됩니다.

이 솔루션에는 API 공격 및 API 설정 오류 탐지를 위해 미리 정의된 수많은 정책이 포함되어 있습니다. 또한 Akamai API Security는 20개 이상의 사전 구성된 데이터 유형을 포함하고 있어 민감한 데이터 유형이 API를 통과할 때 탐지하고 조치를 취하는 데 필요한 데이터 정책을 생성할 수 있습니다.

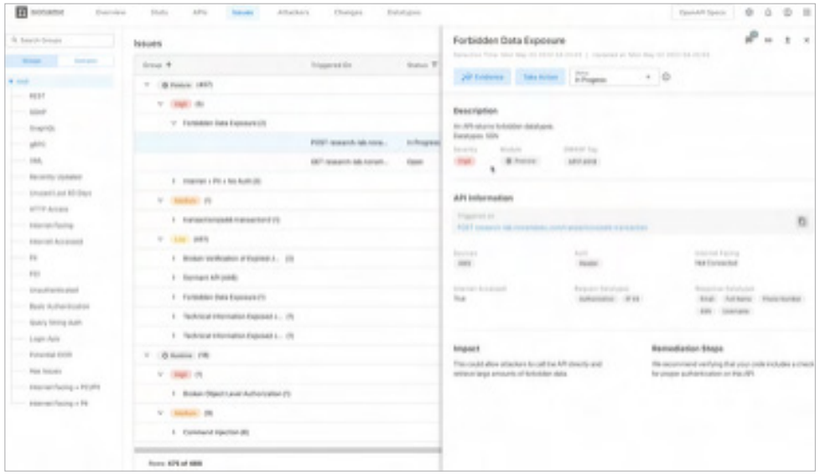
요약하면, Akamai API Security 솔루션의 런타임 보안 모듈은 실시간으로 API 공격을 탐지 및 예방하며 지속적으로 API 설정 오류를 탐지합니다. 또한 인기 있는 다양한 워크플로우의 통합을 통해 운영 및 해결을 간소화합니다.

API 보안 인시던트의 구조

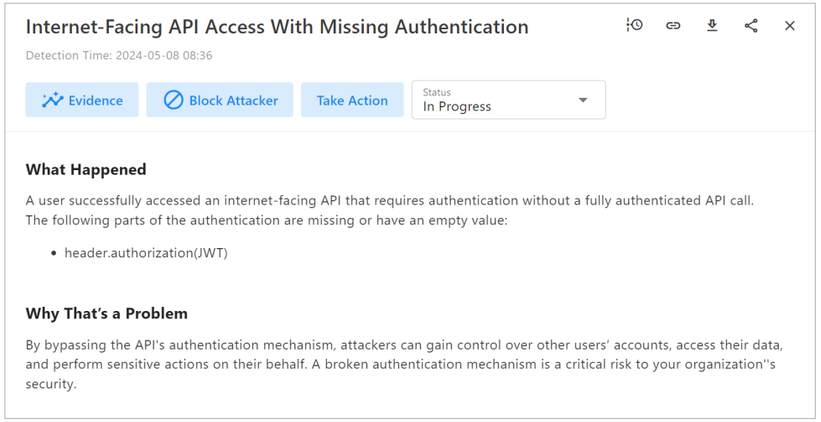
금지된 데이터 노출의 예를 자세히 살펴보겠습니다. 이 예시는 API 내부의 체계 이슈를 보여줍니다. Akamai 플랫폼은 모든 API와 관련된 데이터 유형과 값을 맥락에 맞게 인식합니다.

아래 그림에서 금지된 데이터는 API에 의해 노출되는 중입니다. Akamai 플랫폼은 전송되는 데이터 유형(이 경우 사회보장번호)을 감지했고, 해당 사회보장번호 데이터 유형이 이전에 금지된 것으로 태그가 지정되었음을 파악했습니다. Akamai는 또한 인터넷 접속이 가능하지만 API 게이트웨이에 등록되지 않은 API와 같은 API 외부의 설정 오류도 탐지할 수 있습니다.

예: 금지된 데이터 노출에 대한 인사이트



예: 인증이 누락된 API 파악



효과적인 API 런타임 보안 달성을 위한 다음 단계

고객, 파트너 또는 벤더사가 디지털 방식으로 기업과 소통할 때마다, (종종 민감한) 데이터의 신속한 교환을 촉진하는 API가 배후에서 작동합니다. 주요 API 런타임 보안 기능(예: 설정 오류 및 악용을 방어하는 API 모니터링, API 공격 방지)을 구축하면 빠르게 증가하는 공격 기업으로부터 기업을 보호할 수 있습니다.

중요한 런타임 보안 기능을 제공받기 위한 API 보안 벤더사 평가 방법을 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.com** 및 **akamai.com/blog**를 확인하거나 **X**(기존의 Twitter), **LinkedIn**에서 Akamai Technologies를 팔로우하시기 바랍니다. 2024년 12월 발행.

Akamai