OWASP 10대 API 보안 리스크 방어를 위한 게임 플랜

Akamai가 일반적인 API 취약점 및 위협 방어를 지원하는 방법

OWASP 10대 API 보안 리스크		Akamai 지원
API1:2023	손상된 오브젝트 수준의 권한 확인	✓
API2:2023	손상된 인증	✓
API3:2023	손상된 오브젝트 프로퍼티 수준의 권한 확인	✓
API4:2023	무제한 리소스 사용	✓
API5:2023	손상된 기능 수준의 권한 확인	✓
API6:2023	민감한 비즈니스 플로우에 대한 무제한 접속	✓
API7:2023	서버 측 요청 위조	✓
API8:2023	잘못된 보안 설정	✓
API9:2023	부적절한 인벤토리 관리	✓
API10:2023	안전하지 않은 API 사용	✓

API는 기업의 디지털 제품, 서비스, 클라우드 환경의 핵심입니다. 또한 기업들이 앱 개발을 위해 점점 더 마이크로서비스 기반 아키텍처로 전환함에 따라 API는 애플리케이션 구축 및 연결의 표준이 되고 있습니다. 하지만 API는 데이터와 중요 시스템에 지속적으로 접속할 수 있기 때문에 매출 창출의 원동력이자 운영상의 리스크가 될 수 있습니다.

바로 노출되거나 잘못 설정된 API가 널리 퍼져 있고, 쉽게 감염될 수 있으며, 보호되지 않는 경우가 많기 때문입니다. 그리고 단 한 번의 API 유출로 수백만 개의 기록이 도난당할 수 있습니다.

기업의 78%가 지난 1년 동안 API 보안 인시던트를 경험했다고 응답한 것을 보면 API를 보호하는 것이 우선순위가 되어야 한다는 것은 분명합니다. 그러나 API 공격 표면은 대부분의 기업이 다음 3가지를 이해하는 것보다 훨씬 더 빠르게 공격의 표적으로 부상하고 있습니다.

API 리스크

API 공격 방법

API 보안 제어 및 기능

API 공격 표면은 무엇으로 구성될까요? 결론부터 말하자면, 많은 기업이 생각하는 것보다 훨씬 광범위합니다. API에 대한 기존의 이해(머신투머신 또는 써드파티 API)는 마이크로서비스 기반 아키텍처의 일부인 모바일 및 웹 애플리케이션 서비스를 포함하도록 확장될 수 있으며, 확장되어야 합니다. 즉, 해당 아키텍처 내의 웹 요청은 다양한 마이크로서비스에 대한 일련의 호출 중 하나로 제공되는 API입니다.

78%

지난 1년 동안 API 보안 인시던트를 경험했다고 보고한 기업의 비율. API를 보호하는 것이 우선순위가 되어야 한다는 점은 분명합니다.

2023년 6월 5일, 권위 있는 OWASP(Open Worldwide Application Security Project)는 2019년에 발표한 10대 API 보안 리스크 목록에 대한 첫 번째 주요 업데이트를 발표했습니다. 업데이트된 목록은 다음과 같은 API 호출이 어떻게 잠재적으로 보안 허점을 유발해 개인정보 리스크를 초래할 수 있는지를 다룹니다.

잘못된 데이터 검증

설정 오류

구축 취약점

보안 구성요소 간의 통합 격차

OWASP가 식별한 주요 리스크와 Akamai의 API 보안 솔루션이 이를 방어하는 데 어떤 도움을 줄 수 있는지 계속해서 알아봅시다.

문제는 API에 대한 전체 인벤토리를 보유하고 있다고 주장하는 기업조차도 심각한 격차가 있다는 것입니다.

10곳 중 4곳만 어떤 API가 호출 시 민감한 데이터를 반환하는지 알고 있습니다.

API1:2023 - 손상된 오브젝트 수준의 권한 확인

특정 오브젝트 ID에 접속하는 클라이언트의 권한이 제대로 검증되지 않은 경우 손상된 오브젝트 수준의 권한 확인(BOLA) 취약점이 발생할 수 있습니다. 이 취약점은 공격자가 리소스에 직접 접속해 예상되는 애플리케이션 워크플로우를 우회하고 민감한 데이터에 무단으로 접속할 기회를 제공할 수 있습니다. 클라이언트가 요청에서 전달한 오브젝트 ID에만 의존하지 않으면 이러한 리스크를 줄일 수 있습니다. 대신, 기업은 추측할 수 없는 임의의 ID를 오브젝트에 사용해 모든 오브젝트를 강력하게 검증할 수 있습니다. 적절한 경우 오브젝트의 실제 ID를 마스킹하면 추가적인 보안 레이어를 제공할 수 있습니다.

Akamai가 지원하는 방법

Akamai의 경계 감시 시스템은 위협을 추적하고 BOLA 악용 시도에 대한 알림을 생성해 즉각적인 주의와 조치를 취하도록 지원합니다.

Akamai는 다음과 같은 방법으로 리스크를 방어합니다.

- BOLA 악용 시도 식별
- 수신된 입력(열거 가능한 파라미터 등)과 API 오브젝트와 속성 간의 관계를 기반으로 BOLA 악용에 취약한 API 엔드포인트를 분류
- 시도되거나 성공한 BOLA 악용에 대한 알림 생성

API2:2023 - 손상된 인증

손상된 인증은 인증 프로세스의 광범위한 취약점을 의미하며, 이러한 취약점을 악용해 API 오브젝트 보안을 손상시킬 수 있는 공격자에게 시스템을 노출시킵니다. 일반적으로 손상된 인증 취약점을 이용하는 공격자는 취약한 비밀번호나 세션 리플레이와 같은 시스템의 허점을 조작합니다. 기업은 손상된 인증 취약점을 방어하기 위해 강력한 비밀번호 정책, 키 로테이션, 강력한 토큰 서명, 암호화 키와 같은 강력한 인증 및 비밀 관리 메커니즘을 구축할 수 있습니다. 이러한 엄격한 정책을 기업 전체에 적용하면 리스크를 크게 줄일 수 있습니다.

Akamai가 지원하는 방법

Akamai는 취약한 인증 지점을 식별하고 수정하고, 자동화된 공격을 차단하고, 악용 시도를 사전에 알림으로써 API 보안을 강화합니다.

Akamai는 다음과 같은 방법으로 이러한 리스크를 방어합니다.

- 인증이 필요하지 않거나 인증 모범 사례(약한 토큰 시그니처 또는 암호화 키, 만료된 인증 토큰 수락)를 따르지 않는 API 엔드포인트 식별
- 봇 관리 기능을 통해 자동화된 사전 공격이나 크리덴셜 스터핑 공격 차단
- Akamai API Gateway 기능으로 강력한 토큰 시그니처를 사용해 JSON 웹 토큰의 권한 처리
- BUA 악용 시도에 대한 알림 생성

API3:2023 - 손상된 오브젝트 프로퍼티 수준의 권한 확인

손상된 오브젝트 프로퍼티 수준의 권한 확인(BOPLA)은 API 엔드포인트가 최소 권한 원칙을 무시하고 해당 기능에 필요한 것보다 더 많은 데이터 속성을 불필요하게 노출하는 보안 취약점입니다.

이 취약점으로 인해 공격자에게 실수로 과도한 데이터가 제공되어 더 많은 취약점을 발견하거나 민감한 데이터를 마이닝하는 데 사용될 수 있습니다. 여기에는 관리자 수준의 접속 권한만 있는 프로퍼티를 권한이 없는 사용자가 조작해 시스템 무결성을 더욱 손상시킬 수 있는 시나리오가 포함됩니다. 보안을 보장하고 공격자가 잉여 정보를 얻거나 조작하지 못하도록 하려면, 적절한 접속 수준과 데이터 노출을 제공해 잠재적 공격자가 이러한 감독 소홀을 악용하지 못하도록 막아야 합니다.

Akamai가 지원하는 방법

기업은 Akamai의 포괄적인 기법을 활용해 API 엔드포인트와 관련 프로퍼티를 식별하고 카탈로그화함으로써 BOPLA의 리스크를 방어할 수 있습니다.

Akamai는 다음과 같은 방법으로 이러한 리스크를 방어합니다.

- 모든 엔드포인트와 해당 엔드포인트가 노출하는 PII(Personally Identifiable Information) 같은 API 프로퍼티 식별 및 레이블링
- 문서화되지 않은 API 엔드포인트 또는 섀도 API 엔드포인트, 오브젝트, 프로퍼티는 물론 비정상적인 프로퍼티 식별
- 허용 가능하고 정의된 파라미터와 프로퍼티에 보안 정책을 적용해 데이터 위생 보장
- 전체 OpenAPI/Swagger 사양을 기반으로 보안 정책을 적용하고, 잘 정의된 API 엔드포인트와 방법만 API 오브젝트와 프로퍼티에 접속하도록 허용
- BOPLA 악용 시도에 대한 알림 생성

API4:2023 - 무제한 리소스 사용

무제한 리소스 사용(또는 'API 리소스 고갈'이라고도 부름)은 API가 주어진 시간 내에 제공하는 요청 수나 데이터의 양을 제한하지 않는 취약점의 한 종류입니다. 이러한 관리 소홀은 정상 사용자가 시스템을 사용할 수 없게 만드는 서비스 거부(DoS) 공격을 일으키려는 공격자에게 문을 열어줄 수 있습니다. 이러한 악용은 서비스 중단 기간과 범위에 따라 서비스 가용성 손실, 고객 불만, 잠재적 매출 손실 등 비즈니스에 심각한 영향을 미칠 수 있습니다. 서비스 손실을 방지하려면 API 요청 속도와 데이터 반환 크기를 제한하는 조치를 마련해야 합니다.

Akamai가 지원하는 방법

Akamai는 다음과 같은 방법으로 무제한 리소스 사용 위협으로부터 API를 보호합니다.

- 리스크에 처한 엔드포인트 식별 및 증폭 공격 시도에 대한 실시간 알림 제공
- 과도한 오류, 로그인 시도 또는 리스크를 나타내는 비정상적인 행동 탐지

Akamai는 다음과 같은 방법으로 이러한 리스크를 방어합니다.

- 전송률 제한이 없거나 대규모 증폭 사전 공격이나 크리덴셜 스터핑 공격을 받고 있는 API 엔드포인트 식별
- 증폭 공격 속도를 늦추거나 차단하기 위한 워크플로우 시작
- 증폭 공격 시도에 대한 알림 생성

API5:2023 - 손상된 기능 수준의 권한 확인

API 엔드포인트에 대한 접속 제어 모델이 잘못 구축된 경우 손상된 기능 수준의 권한 확인(BFLA)이 발생할 수 있습니다. 부정확하거나 오래된 접속 제어 방법은 무단 접속을 적절히 제한하지 못해 공격자가 민감한 정보나 시스템 전체에 접속할 수 있도록 허용할 수 있습니다. 이러한 리스크를 방어하려면 최소 권한 원칙을 도입해 모든 기능, 특히 관리 기능에 적절한 권한이 있는 사용자만 접속할 수 있도록 보장해야 합니다.

Akamai가 지원하는 방법

행동 타임라인 추적, 민감한 기능에 대한 보안 정책 적용, 키 로테이션 및 해지 관리, 의심스러운 시도에 대한 즉각적인 알림을 통해 Akamai는 기업의 BFLA 예방 및 대응 전략을 강화할 수 있도록 지원합니다.

Akamai는 다음과 같은 방법으로 이러한 리스크를 방어합니다.

- 사용자, API 키, 접속 토큰, 세션 ID 등을 캡처해 API 엔드포인트 접속에 대한 행동 타임라인 파악
- Akamai API Gateway를 통해 키 로테이션 또는 노출된 키 해지 적용
- 관리 기능에 접속하려는 의심스러운 시도에 대한 알림 생성

API6:2023 - 민감한 비즈니스 플로우에 대한 무제한 접속

민감한 비즈니스 플로우에 대한 무제한 접속은 API가 충분한 접속 제어 없이 비즈니스 로직과 같은 중요한 작업을 노출할 때 발생합니다. 이는 무단 접속 및 악용으로 이어져 기업에 심각한 피해를 초래할 수 있습니다. 일반적으로 공격자들은 API가 뒷받침하는 비즈니스 모델을 이해하고, 민감한 비즈니스 흐름을 식별하며 이러한 흐름의 허점을 악용합니다. 이는 정상적인 사용자의 제품 구매를 방해하는 등의 영향을 미칠 수 있습니다.

Akamai가 지원하는 방법

민감한 엔드포인트 식별, 실시간 악용 알림, 전문가 컨설팅을 통해 중요한 데이터와 운영을 보호하는 Akamai의 포괄적인 API 보안 솔루션으로 비즈니스를 안전하게 보호하세요.

Akamai는 다음과 같은 방법으로 이러한 리스크를 방어합니다.

- 결제 흐름이나 PII를 처리하는 엔드포인트 같은 민감한 API 엔드포인트 식별
- 데이터 유출, 데이터 조작 등 다양한 잠재적 악용과 이러한 민감한 API 엔드포인트에 대한 의심스러운 시도에 대한 알림 생성

API7:2023 - 서버 측 요청 위조

공격자는 서버 측 요청 위조(SSRF)를 사용해 서버 측 애플리케이션이 공격자가 선택한 임의의 도메인에 HTTPS 요청을 하도록 유도할 수 있습니다. 일반적인 SSRF 공격에서 공격자는 서버를 속여 내부 리소스에 대한 요청을 생성해 방화벽을 우회하고, 내부 서비스에 접속함으로써 데이터를 노출하거나 원격 코드를 실행할 수 있습니다. 이러한 리스크를 방어하려면 사용자 인풋을 검사, 필터링 또는 삭제하고 중요한 서비스만 서버와 통신할 수 있도록 아웃바운드 연결을 제한해야 합니다.

Akamai가 지원하는 방법

신뢰할 수 있는 API 연결에서 비정상 탐지, 효과적인 키 관리, SSRF 악용 시도에 대한 즉각적인 알림을 제공하는 Akamai로 보안 체계를 강화하세요.

Akamai는 다음과 같은 방법으로 이러한 리스크를 방어합니다.

- SSRF 공격에 대응하는 웹 애플리케이션 및 API 보안 정책을 통해 보안 강화
- API Gateway를 통해 키 로테이션 또는 노출된 키 해지 적용

API8:2023 - 잘못된 보안 설정

잘못된 보안 설정은 보안 제어를 부적절하게 설정해 시스템을 공격에 취약하게 만드는 것을 의미합니다. 여기에는 안전하지 않은 기본 설정, 불완전 또는 임시 설정, 오픈 클라우드 스토리지, 잘못 설정된 HTTP(S) 헤더, 민감한 정보가 포함된 장황한 오류 메시지 등이 포함될 수 있습니다. 리스크를 방어하려면 애플리케이션과 API의 모든 측면에 걸쳐 보안 제어를 올바르게 설정했는지 확인해야 합니다. 이를 위해서는 정기적인 업데이트, 철저한 테스트, 지속적인 모니터링을 통해 잘못된 설정을 즉시 식별하고 수정해야 합니다.

Akamai가 지원하는 방법

섀도, 로그 또는 좀비 API 엔드포인트를 식별하고, 보안 모범 사례를 준수하고, 강력한 HTTPS를 구축하고, 보안 설정 오류에 대한 즉각적인 알림을 수신하는 Akamai의 지원을 통해 인사이트를 강화할 수 있습니다.

Akamai는 다음과 같은 방법으로 이러한 리스크를 방어합니다.

- 낮은 수준의 환경(테스트 및 스테이징 환경)에 노출될 수 있는 섀도 API 엔드포인트 식별
- 보안 설정 모범 사례 및 표준에 따라 API 엔드포인트, 오브젝트, 프로퍼티 식별 및 매칭
- 올바른 형식의 HTTPS 요청 및 응답, 올바른 HTTP 헤더 설정 또는 제거, 교차 오리진 리소스 공유(CORS) 및 캐시 제어 헤더에 대한 완전한 제어 보장 등 API 보안 모범 사례를 통해 보안 정책 적용
- 정확하고 안전한 암호 제품군을 포함해 SSL/TLS를 통해 적절한 HTTPS 구축
- 잘못된 설정 또는 API 보안 모범 사례 및 표준 미준수에 대한 알림 생성

API9:2023 - 부적절한 인벤토리 관리

부적절한 인벤토리 관리는 API를 관리하는 모든 기업이 직면한 도전 과제입니다. API 보안 솔루션은 알려진 API를 보호할 수 있지만 섀도 API를 비롯한 알려지지 않은 API는 패치되지 않은 채로 방치되어 공격에 취약할 수 있습니다. 이로 인해 오래된 구성요소, 사용하지 않는 페이지 또는 API, 민감한 정보의 불필요한 노출이 발생할 수 있습니다. 유지 관리되지 않는 서비스 관리는 시스템을 위협에 취약하게 만들 수 있으며, 공격자는 동일한 데이터베이스에 연결된 알 수 없는 API를 통해 민감한 데이터나 서버에 접속할 수 있습니다. 지속적으로 변경되는 기업 서비스의 구성요소를 방지하려면 접속 제어와 정기적인 감사가 필수적입니다.

Akamai가 지원하는 방법

Akamai는 API 트래픽을 지속적으로 감독해 숨겨진 API 엔드포인트와 잠재적 리스크가 있는 API를 발견하고 안전한 데이터 스토리지, 고급 위협 분석, 잠재적 악용에 대한 즉각적인 알림을 제공합니다.

Akamai는 다음과 같은 방법으로 이러한 리스크를 방어합니다.

- 공개적으로 접속 가능한 API를 대상으로 하는 남북 API 엔드포인트와 동서 내부 API 엔드포인트를 포함해 환경을 통해 이동하는 노출된 API 트래픽을 지속적으로 모니터링
- 낮은 수준의 환경(테스트 및 스테이징 환경) 또는 문서화되지 않았거나 더 이상 사용되지 않는 API 버전을 노출할 수 있는 섀도 API 엔드포인트 식별
- 리스크 점수 및 데이터 분류를 기반으로 최신 API 인벤토리 생성
- 데이터 유출, 데이터 조작 등 다양한 잠재적 악용과 이러한 민감한 API 엔드포인트에 대한 의심스러운 시도에 대한 알림 생성

API10:2023 - 안전하지 않은 API 사용

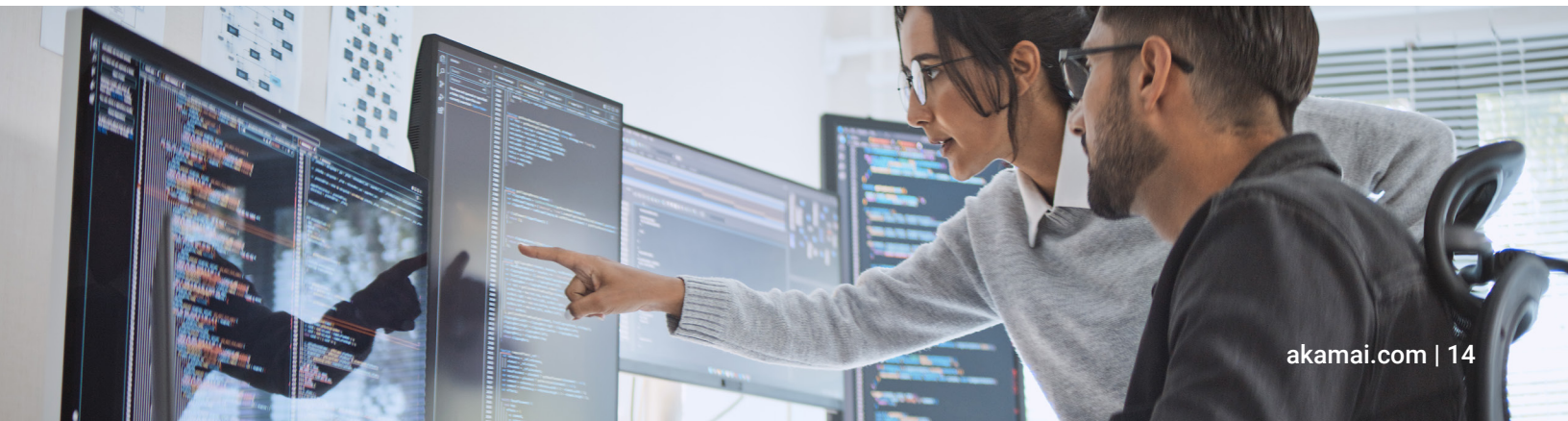
안전하지 않은 API 사용은 적절한 보안 조치를 취하지 않고 써드파티 API를 사용할 때 발생할 수 있는 리스크를 의미합니다. 기업은 서비스와 기능을 확장하기 위해 써드파티 API에 점점 더 의존하고 있으며, 이런 API를 디폴트로 신뢰하는 경우가 많습니다. 이로 인해 심각한 보안 취약점이 발생할 수 있습니다. 적절한 암호화, 데이터 검사, 삭제, 리소스 소비 제한을 구축하지 않으면 기업은 심각한 취약점에 노출될 수 있습니다. 이러한 리스크를 방어하기 위해 기업은 네트워크를 통해 전송되는 모든 데이터를 암호화하고, 모든 데이터 입력을 검사 및 삭제하고, 리소스 소비에 대한 합리적인 제한을 설정할 수 있습니다.

Akamai가 지원하는 방법

Akamai의 모니터링, 알림, 컨설팅 서비스를 통해 서비스를 모니터링하고 검증해 보안을 보장함으로써 시스템을 지속적으로 보호합니다.

Akamai는 다음과 같은 방법으로 이러한 리스크를 방어합니다.

- B2B 및 써드파티 통합을 용이하게 하는 동서 및 아웃바운드 API를 포함해 기업 환경 전반에 걸쳐 모든 노출된 API 트래픽을 지속적으로 모니터링합니다.
- 데이터 유출, 데이터 조작 등 다양한 잠재적 악용과 이러한 민감한 API 엔드포인트에 대한 의심스러운 시도에 대한 알림 생성
- 공격 그룹에서 수집된 다양한 API 공격을 대상으로 하는 웹 애플리케이션 및 API 보안 정책을 통해 보안 강화



OWASP가 공개한 추가 보안 리스크

2023년 OWASP 10대 API 보안 리스크는 2019년 이후 OWASP가 처음으로 업데이트한 주요 목록입니다. 그러나 인젝션 공격과 같이 현재 환경과 여전히 관련성이 있는 추가 보안 리스크에 대해 논의한 기존 목록도 다시 살펴볼 가치가 있습니다.

Akamai는 다음과 같은 방법으로 이러한 보안 리스크에 대응할 수 있습니다.

- 시그니처 매칭 및 비정상 탐지를 통해 API 인젝션에 취약한 엔드포인트 및 인젝션 시도 식별
- API 요청에 대한 JSON 및 XML 검사를 통해 보안 정책을 적용하고 SQLi, XSS, CMDi, RFI, LFI 등 다양한 인젝션 공격을 스캔
- 인젝션 악용에 대한 알림 생성

OWASP는 OWASP 10대 웹 애플리케이션 보안 리스크 등의 다른 10대 보안 리스크 목록도 발표했습니다. Akamai의 보안 포트폴리오는 이러한 보안 리스크를 방어하도록 지원합니다.

Akamai가 도와드리겠습니다!

기업과 기업의 보안 벤더사가 OWASP 10대 API Security 리스크에 설명된 보안 리스크에 대비해 강력한 방어 체계를 구축하려면 인력, 프로세스, 기술을 조율하며 서로 긴밀하게 협력해야 합니다.

Akamai는 업계 최고의 보안 솔루션과 경험이 풍부한 전문가, 수백만 건의 웹 애플리케이션 공격, 수십억 건의 봇 요청, 매일 수조 건의 API 요청으로부터 인사이트를 확보하는 플랫폼을 제공합니다.

Akamai의 웹 애플리케이션 및 API 보안 솔루션은 가장 발전된 형태의 웹 애플리케이션, DDoS, API 기반 공격으로부터 기업을 보호합니다. 또한 Akamai의 Managed Security Service는 연중무휴 24시간 모니터링, 보안 관리, 위협 방어를 제공합니다.

Akamai의 보안 포트폴리오에 대해 자세히 알아보려면 Akamai의 웹사이트를 방문하시기 바랍니다. Akamai와의 파트너십을 통해 완벽한 비즈니스 보안 체계를 구축하는 방법에 대해 알아보고 이에 대해 논의하고 싶으시다면 지금 Akamai 영업 담당자에게 연락하시기 바랍니다.

Akamai Security는 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 관한 자세한 정보를 보려면 akamai.com과 akamai.com/blog를 방문하거나 X(기존의 Twitter)와 LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2024년 9월 발행.