백서

Akamai 보안을 통해 컴플라이언스를 경쟁력으로 전환

4가지 핵심 접근 방식으로
보안 강화 및 감사 준비

4가지 보안 핵심 요소에 집중해 컴플라이언스 준수 체계를 강화하세요

오늘날 전 세계 기업들은 GDPR, HIPAA, PCI DSS를 비롯해 점점 더 다양해지는 지역별 규제 의무라는 복잡하고 까다로운 환경을 헤쳐 나가고 있습니다. 그러나 컴플라이언스 준수 준비성을 입증하는 일은 단순히 규제 기관을 만족시키는 차원을 넘어 고객과 경영진, 이사회 등 내부 이해관계자와의 신뢰를 유지하는 데 필수적인 요소입니다.

실제로 컴플라이언스 준수 실패의 영향은 규제 벌금에 그치지 않고 훨씬 더 심각합니다. 컴플라이언스 미준수로 인한 비용에는 조사 및 시정 절차 중 발생하는 업무 중단, 평판 손상, 법적 리스크 증가가 포함됩니다. 기업이 컴플라이언스 요구사항을 충족하지 못할 경우, 혁신보다는 문제 해결에 리소스를 더 많이 투입하게 되어 고객 손실과 상당한 운영 비용이 발생하고, 결국 이는 매출 감소로 이어질 수 있습니다. Forrester에 따르면, 2024년 전 세계에서 발생한 가장 큰 35건의 유출 사건으로 인해 총 30억 달러의 벌금이 부과됐으며, 이 중 23건은 유럽연합 GDPR(General Data Protection Regulation) 규정 위반이 원인이었습니다.

과거에는 새로운 규제가 등장할 때마다 보안팀이 컴플라이언스에 대응했습니다. 하지만 이제는 기술이 빠르게 발전하고 공격의 규모와 강도가 증가하고 있기 때문에 툴과 성숙도 모델을 평가하는 과정에 컴플라이언스도 포함되어야 합니다. 이 과정에서 스스로 다음과 같은 질문을 던져야 합니다. "오늘의 보안 선택이 현재와 미래의 컴플라이언스 요구사항을 충족하는 데 어떤 도움을 줄 수 있는가?"

Akamai는 고객이 이 질문에 답할 수 있도록 보안 모범 사례의 4가지 핵심 요소에 중점을 두고 논의를 진행하며, 그 과정에서 자연스럽게 컴플라이언스 준비와 관련된 주요 사안도 깊이 있게 알아볼 수 있습니다. 이 4가지 핵심 요소는 다음과 같습니다.

- IT 자산 전반에 대한 가시성 확보
- 네트워크, 애플리케이션, API 전반에서 측면 이동 차단
- 무단 접속 방지
- 민감한 고객 데이터와 계정 정보 보호

그 결과, 명확한 경쟁 우위를 확보할 수 있습니다. 기업은 보안이 강화될 뿐 아니라 규제 장벽을 넘을 준비도 더 잘 갖추게 됩니다. 보안성과 컴플라이언스를 동시에 강화해 고객과 내부 경영진의 신뢰를 얻을 수 있는 역량도 향상됩니다.

핵심 요소 1
IT 자산 전반에 대한 가시성 확보

컴플라이언스 준비의 토대는 모든 디지털 자산에 대한 포괄적인 가시성에서 시작됩니다. 기업이 볼 수 없는 것을 보호하는 것은 불가능하며, 규제 기관은 자산 인벤토리, 지속적인 모니터링 및 위협 인식 역량을 완벽히 갖추고 있다는 증거를 점점 더 많이 요구하고 있습니다.

물론 이건 말처럼 쉽지 않습니다. 최근 Forrester 연구에 따르면 금융 기업의 과반수(52%)가 **IT 인프라에 대한 완전한 가시성이 부족하다**는 데 동의하거나 강력하게 동의했습니다. 안타깝게도 업계에 관계없이 컴플라이언스 미준수의 대가는 매우 큽니다. 2023년부터 2024년까지 규제 벌금으로 **10만 달러 이상을 지불한** 기업의 수는 약 20% 증가했습니다.

대부분의 기업들에게 가시성에 대한 문제는 네트워크 트래픽과 API를 모니터링하는 데 있습니다. 다음은 리스크를 명확하게 파악할 것을 요구하는 규제와 표준입니다.

- PCI DSS(Payment Card Industry Data Security Standard)에는 기업의 소프트웨어가 외부 구성요소의 기능을 안전하게 사용하고 있는지 확인하는 가이던스를 제공합니다. 예를 들어, 모바일 앱에서 결제 데이터를 은행 시스템으로 전송하는 API가 이에 해당합니다.
- ISO(International Organization for Standardization)/IEC 27001과 같은 국제 표준은 공격자가 네트워크를 침해했을 경우를 대비해 데이터와 데이터 처리 시설을 분리할 것을 요구합니다.
- 중국의 데이터 보안법은 서로 다른 IT 시스템 간에 민감한 데이터를 교환하는 기술을 통해 고객의 개인정보에 접근하는 경우, 강력한 보안 통제를 적용할 것을 요구합니다.

많은 기업이 이러한 요구사항 중 일부를 충족할 수 있는 툴이나 프로세스를 보유하고 있습니다. 그러나 이러한 요구사항이 하이브리드 컴퓨팅 환경과 지역 전반에 걸쳐 더욱 폭넓게 적용됨에 따라 모니터링이 훨씬 어려워지고 있습니다. 이 문제는 특히 API에서 두드러집니다. Akamai의 리서치에 따르면 전체 API 인벤토리를 보유한 보안 전문가 중 **실제로 자사 API 중 어떤 것이 민감 데이터를 반환하는지 파악하고 있는 비율**은 27%에 불과합니다. 이는 2023년의 이미 우려스러운 수준이었던 40%에서 더 하락한 수치입니다.

궁극적으로 기업은 보안 노력을 어디에 집중해야 할지 결정하기 위해 민감 데이터가 어디에 존재하는지, 그리고 어떤 주체가 해당 데이터에 접속하는지를 반드시 파악해야 합니다. 이를 위해서는 다음 사항에 대한 가시성이 필요합니다.

- 하이브리드 클라우드 및 온프레미스 환경에서 레이어 7 프로세스와 엣지 트래픽 등의 네트워크와 통신하는 자산(실시간 보기와 기록 보기 포함)
- 섀도 및 좀비 API를 포함한 API 인벤토리, 그리고 해당 API가 어떤 트래픽 소스 및 코드와 통합되는지에 대한 정보
- 클라이언트 측 JavaScript(최근의 PCI DSS 요구사항에서 특히 중요한 요소)

Akamai의 포트폴리오는 보안 팀이 필요한 가시성을 확보할 수 있도록 지원합니다.

Akamai Guardicore Segmentation은 IT 자산 전반에서 네트워크 내부와 통신하는 자산을 식별하고 시각화할 수 있으며, 여기에는 레이어 7 프로세스, 해시, 명령줄 세부 정보까지 포함됩니다. 또한 컴플라이언스 감사를 위한 증거 제공을 위해 해당 범위 내 자산이 감염되지 않았음을 입증할 수 있도록 이력 기반 가시성도 제공합니다. 남북 및 동서 트래픽 시각화를 통해 접속이 이루어지는 위치도 확인할 수 있습니다.

API Security는 기업이 컴플라이언스를 위해 필요로 하는 API의 실시간 인벤토리를 제공하며, 암호화되지 않은 데이터가 API를 통해 언제 어디서 흐를 수 있는지 식별하는 데 도움을 줍니다.

App & API Protector는 API 인벤토리, 민감 데이터 노출 탐지, 실시간 트래픽 분석 등 애플리케이션 수준의 가시성을 제공합니다.

Client-Side Protection & Compliance는 PCI DSS v4에서 요구하는 클라이언트 측 스크립트 가시성을 제공합니다.

한 **헬스케어** 기업은 HIPAA 및 SOC 2 컴플라이언스 요건을 충족하기 위해 Akamai Guardicore Segmentation을 도입했습니다. 이 제품은 다양한 애플리케이션 간의 트래픽 흐름에 대한 귀중한 가시성을 제공했습니다. 보안팀은 레이어 4 로그를 넘어 사용자 ID, 명령줄 입력, 심지어 서비스 상관관계에 이르기까지 세분화된 세부 정보를 검사할 수 있었습니다.

핵심 요소 2
측면 이동의 방지

보안팀과 마찬가지로 많은 규제 기관은 강력한 보안 체계를 갖추고 있더라도 유출이 발생할 수 있다는 점을 인정하고 이러한 경우 기업이 피해를 최소화할 수 있는 확실한 대책을 요구하고 있습니다. 예를 들어

- GDPR 제32조는 "처리 시스템 및 서비스의 지속적인 기밀성, 무결성, 가용성, 안정성을 보장할 수 있는 능력"과 "물리적 또는 기술적 인시던트 발생 시 개인정보에 대한 가용성과 접속을 적시에 복구할 수 있는 능력"을 요구합니다.
- PCI DSS v4에서도 마찬가지로 기업은 "신용카드 소지자의 데이터를 보호하기 위해 방화벽을 구축하고, 방화벽이 신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 연결을 제한하도록 설정해야 합니다."
- ISO/**IEC(International Organization for Standardization/International Electrotechnical Commission) 27001**에서는 정보 및 데이터 처리 시설을 분리해 정보의 기밀성, 무결성, 가용성을 보호할 것을 요구합니다.

대부분의 기업은 방화벽을 갖추고 있지만, 공격자가 네트워크 내부에 침입한 경우 측면 이동을 제한하려면 더 높은 수준의 제어가 필요합니다. 이러한 이유로 마이크로세그멘테이션, 특히 소프트웨어 기반의 마이크로세그멘테이션은 컴플라이언스 준수에 핵심적인 툴이 됩니다. Akamai는 측면 이동에 대한 감사자의 우려를 해소할 수 있는 유리한 입지를 확보하고 있습니다.

Akamai Guardicore Segmentation은 기업이 컴플라이언스를 지속적으로 유지하는 데 필요한 측면 이동 제한 기능을 제공합니다. 즉시 사용 가능한 정책 템플릿은 세분화된 레이어 7 제어를 통해 컴플라이언스 관련 이니셔티브를 신속하게 적용할 수 있도록 지원합니다. 또한 소프트웨어 기반이기 때문에 자산의 위치와 관계없이 동일한 수준의 세분화된 보호를 제공합니다. 뿐만 아니라 네트워크 내에서 통신하는 앱과 분할된 영역 간의 통신 시도를 탐지할 수 있기 때문에 감사자는 기업의 위협 방어 역량에 대한 확신을 가질 수 있습니다.

API의 확산으로, 공격자들은 특히 BOLA(손상된 오브젝트 수준 권한) 공격에 취약한 API 엔드포인트에서 측면 이동을 일으킬 새로운 기회를 찾고 있습니다. 공격자는 API 요청에서 오브젝트 ID를 조작해 네트워크 내에서 측면 이동을 가능하게 만들 수 있습니다. 내부에 침투한 공격자는 권한 확인을 우회하고 권한을 에스컬레이션해 고객 데이터에 접속할 수 있습니다.

Akamai API Security는 적절한 인증 없이 민감한 데이터를 노출하는 API를 탐지하고, 접속 제어가 취약하거나 잘못 구성되어 무단 데이터 접속과 측면 이동을 유발할 수 있는 API를 찾아낼 수 있습니다. 또한 API Security는 Akamai WAF(웹 애플리케이션 방화벽)와 통합되어 악성 위협을 실시간으로 차단할 수 있습니다.

Akamai의 **한 글로벌 금융 서비스 기업** 고객은 자사 환경에서 알 수 없는 API로 인해 어려움을 겪고 있었고, 이를 해결하기 위해 API Security를 구축했습니다. Akamai API Security는 민감한 데이터를 분류해 GDPR, HIPAA 등과 같은 규정을 준수할 수 있도록 지원함으로써 API 확산을 획기적으로 줄이고 컴플라이언스를 개선했습니다. 규제 감사 과정에서 이러한 구축은 회사가 적절한 기술적 조치를 취했다는 직접적인 증거가 됩니다.

오늘날의 AI 위협은 내일의 규제 장벽이 됩니다

오늘날 기업의 사이버 보안 방어 체계를 점검할 때는 AI라는 새로운 위협 요소를 반드시 고려해야 합니다. AI 기반 애플리케이션, LLM(대규모 언어 모델), 생성형 AI와 연결된 API의 급속한 확산으로 대부분의 기업이 아직 알지 못하는 새로운 취약점이 등장하고 있습니다. 이러한 유형의 애플리케이션 사례로는 AI 기반 챗봇, 리테일 추천 엔진, 건강 진단 툴, 리스크 의사결정 엔진 등이 있습니다. 한편, 공격자들은 AI를 활용해 더욱 정교한 공격을 수행하고 있습니다.

또한 비즈니스 운영과 대중에 대한 위협이 발생하는 곳이라면 어디든지 규제가 적용될 가능성이 높습니다.

자사의 AI 투자, 데이터, 고객을 보호하려는 기업들은 Akamai에 도움을 요청하고 있습니다. 보안 공급업체 Akamai는 현재의 가시성, 측면 이동, 접속 제어 요구사항을 충족해 온 강력한 실적을 바탕으로 미래의 AI 요구사항을 충족하기 위해 선제적으로 투자해 왔습니다. Akamai는 자사 보안 솔루션을 강화하기 위해 첨단 AI 기능을 개발했으며, 이제 기업이 자사의 AI 투자를 보호할 수 있도록 지원하는 새로운 솔루션을 선보였습니다.

Akamai Firewall for AI는 기존 보안 툴로는 해결할 수 없도록 설계된 AI 고유의 위협과 공격을 탐지하고 방어함으로써 AI 기반 애플리케이션에 대한 포괄적인 보안을 제공합니다. Firewall for AI의 목적에 맞게 설계된 보호 기능은 다음과 같습니다.

- **프롬프트 삽입 차단** — 공격자가 교묘한 입력을 통해 AI 모델을 조작하지 못하도록 방지
- **데이터 유출 차단(DLP)** — AI 응답에서 민감한 데이터 유출을 탐지하고 차단하는 것은 물론, 요청을 통해 민감한 데이터를 수신하지 못하도록 보호
- **유해하고 해로운 콘텐츠 필터링** — 혐오 표현, 가짜 정보, 공격적인 콘텐츠를 전송 전에 식별 및 차단
- **적대적 AI 보안** — 원격 코드 실행, 모델 백도어, 데이터 중독 공격으로부터 보호
- **DoS 방어** — 과도한 쿼리 사용과 모델 과부하를 제어해 AI 기반 DoS 공격 방어

또한 Firewall for AI는 기업이 기존 프라이버시, 안전, 보안 지침을 준수하는 데 도움이 될 수 있습니다. 기업은 AI 전용 보안 정책을 시행함으로써 데이터 보호 규정, 윤리적 AI 사용, 기업 거버넌스 의무와 관련된 리스크를 방어할 수 있습니다.

핵심 요소 3
무단 접속 방지

민감한 시스템과 데이터에 대한 접속을 제어하는 것은 사실상 모든 규제 프레임워크에서 컴플라이언스의 핵심 요소입니다. 기업은 자사 애플리케이션과 API의 보안 체계를 명확히 파악하고, 무단 접속과 악용을 방지해야 합니다. 이를 위해서는 사용자를 적절히 인증하고, 반드시 알아야 하는 경우에만 접속을 승인하며, 모든 접속 활동에 대한 상세 기록을 유지해야 합니다.

규제 요구사항을 충족하는 완전한 접속 제어를 위해 기업은 다음 3가지 핵심 과제를 해결해야 합니다. Akamai의 보안 포트폴리오는 각 과제를 해결하는 심층 방어를 제공합니다.

1. **애플리케이션과 API 보안 체계를 종합적으로 파악**

Akamai의 App & API Protector는 기업이 운영 중인 모든 환경에서 트래픽 정책을 적용할 수 있도록 하며, Akamai API Security**를 통해 비정상적 활동, 무단 데이터 접속 또는 설정 오류를 기업에 알립니다. 이러한 요소들은 감사자가 중점적으로 검토하는 핵심 사항입니다. 한편,** Akamai Guardicore Segmentation**은 네트워크 내에서 통신하는 모든 애플리케이션을 추적하고 활동 기준선을 설정할 수 있습니다.**

2. **사용자 행동 모니터링 및 민감한 정보 접속 제한**

Akamai Guardicore Segmentation은 사용자 ID를 기반으로 네트워크 내 접속을 제한하며, **App & API Protector**는 AI 기반 위협 탐지를 통해 트래픽 정책을 적용해 유출을 방지합니다. 마지막으로 **Client-Side Protection & Compliance**는 JavaScript 실행 행동을 모니터링해 클라이언트 측 공격을 방어합니다.

3. **사기 활동 탐지 및 차단**

API Security**는 비정상적인 API 행동과 잘못 설정된 인증 제어를 탐지해 고위험 공격을 차단하는 데 도움을 줍니다.** Akamai Guardicore Segmentation**은 사기 활동을 나타낼 수 있는 의심스러운 연결을 식별 및 차단해 네트워크를 보호합니다.** App & API Protector**는** OWASP**에서 정의한 위협을 탐지하고 방어해 사기 리스크를 추가로 줄여줍니다.**

NIS2 및 접속 보안

개정된 NIS2(네트워크 및 정보 보안 지침)은 EU 회원국 전역에서 공통된 수준의 사이버 보안을 구축하도록 설계되었습니다. NIS2에 최근 추가된 사항에 따르면 기업은 민감한 데이터를 보호하고 안정성을 보장하기 위해 인력, 정책, 기술을 평가하는 정보 보안 관리 시스템을 구축해야 합니다. 또한 NIS2는 IT 공급망과 써드파티 공급업체 관계의 보안을 한층 더 강조하고 있습니다.

핵심 요소 4

민감한 고객 데이터와 계정 정보 보호

포괄적인 규정 준수 준비 과정의 마지막 핵심 요소는 기업이 민감한 데이터에 대한 계획을 갖추는 것입니다. 고객, 환자, 파트너 등의 데이터를 보호하는 것은 대부분의 보안 중심 규제의 핵심에 해당합니다.

예를 들어, 일본의 개인정보보호법은 대규모 개인정보 처리나 고위험 데이터 처리 활동과 관련된 기술에 대해 리스크를 식별하고 방어할 수 있는 데이터 보호 영향 평가를 요구합니다.

미국 금융 기관의 경우, FFIEC(The Federal Financial Institutions Examination Council)는 모니터링, 로깅, 보고 등 계층화된 보안을 통해 API가 권한이 있는 사용자에게만 특정 데이터에 접속하도록 보장하는 통제를 요구합니다.

이 핵심 요소를 다루는 첫 단계는 위협 탐지입니다. Akamai의 웹 애플리케이션 및 API 보안 솔루션인 **App & API Protector**는 첫 번째 방어 레이어를 제공하며, **Akamai Guardicore Segmentation**은 남북 및 동서 트래픽을 모니터링하고 세그멘테이션합니다. Akamai의 **Bot Abuse & Protection 솔루션 포트폴리오**는 자동화된 위협 및 인적 기반 공격에 대한 보안 레이어를 더욱 강화합니다.

그러나 위협을 제대로 탐지하려면 기업이 네트워크 내에서 기준 행동 패턴을 이해하는 것도 중요합니다. 다음은 Akamai 보안 기능이 이러한 중요한 인사이트를 제공하는 방식입니다.

- Akamai API Security와 Akamai Guardicore Segmentation은 각각 네트워크 내에서 통신하는 API 및 앱에 대한 기본적인 이해를 바탕으로 비정상 행동을 탐지하고 차단합니다.
- App & API Protector의 핵심 기술인 Adaptive Security Engine은 로컬 및 글로벌 데이터를 활용해 공격 패턴을 학습하고, 고객별 보호 설정을 조정하며, 향후 위협에 적응합니다.
- Akamai의 전문 리서치팀이 지원하는 관리형 위협 헌팅 서비스인 Akamai Hunt를 통해 기업은 보다 선제적인 방어 전략을 펼칠 수 있습니다.

DORA 및 데이터 보안

DORA(Digital Operational Resiliency Act)는 EU 회원국의 금융 서비스 기업이 사이버 공격을 견디고 복구하는 것을 돕기 위해 설계되었습니다. DORA를 통해 금융 부문은 정보통신 기술(ICT)에 대한 구속력 있는 포괄적인 리스크 관리 프레임워크를 갖추게 됩니다. DORA 제3조에 따라 기업은 ICT 솔루션 및 프로세스를 사용해 다음을 충족해야 합니다.

- 데이터 관련 리스크, 무단 접속, 기술적 취약점 최소화
- 데이터 불가용성, 데이터 손실, 무결성 및 기밀성 유출 방지
- 데이터 전송 보안 보장

컴플라이언스 사일로를 해소하고 경쟁 우위 확보

효과적인 컴플라이언스 프로그램은 단순히 규제 요건을 '충족했다'는 수준을 넘어 비즈니스에 미치는 실질적인 영향을 입증해야 합니다. Akamai의 컴플라이언스 중심 보안 솔루션을 구축한 기업들은 다음 3 가지 핵심 영역에서 측정 가능한 성과를 보고했습니다.

컴플라이언스 비용 절감

성숙한 컴플라이언스 프로그램을 보유한 기업은 임시 대응 방식에 의존하는 기업보다 컴플라이언스 활동에 드는 비용이 적습니다. 통합 보안 플랫폼을 통해 증거 수집을 자동화하고, 개별 솔루션을 종합 플랫폼으로 통합하면 감사 준비 시간을 크게 단축할 수 있습니다.

리스크 체계 개선

컴플라이언스 개선은 비용 절감뿐 아니라 측정 가능한 리스크 체계 개선으로 이어져야 합니다. Akamai의 세그멘테이션 솔루션을 구축한 기업은 취약한 측면 이동 경로를 제한해 기업의 리스크를 줄이는 동시에 주요 컴플라이언스 요구사항을 직접 해결할 수 있습니다.

포괄적인 모니터링 기능은 컴플라이언스 위반이 탐지되지 않을 수 있는 사각 지대를 제거해 가시성을 개선하며 이는 리스크 감소와도 직결됩니다.

운영 효율성

컴플라이언스 영향의 세 번째 영역은 운영 효율성 향상입니다. 사전 승인된 제어와 일관된 보안 패턴은 신규 애플리케이션의 보안 승인 속도를 크게 높일 수 있습니다. 이로써 보안 검토 프로세스에서의 제약 조건을 줄이고 신규 애플리케이션의 시장 출시 기간을 단축해 개발자 만족도를 높입니다.

컴플라이언스의 미세 조정

규제 요구사항이 계속 변화하고 기업이 성장함에 따라 변화에 적응할 수 있는 컴플라이언스 접근 방식이 필요합니다. Akamai의 통합 보안 포트폴리오는 규제 트렌드를 예측하고 기업 성장에 맞춰 확장할 수 있는 컴플라이언스 전략의 토대를 제공합니다.

- 설정 가능한 정책 프레임워크는 대규모 재설계 없이 새로운 요구사항에 대응할 수 있으며, 확장 가능한 보고 기능은 규제 변화에 따라 새롭게 등장하는 증거 요구사항에 대응할 수 있습니다.
- 새로운 자산에 대한 정책 자동 배포를 통해 비즈니스 확장 시 자동으로 컴플라이언스 범위를 확장합니다.
- 중앙 집중식 관리 기능은 규모와 관계없이 포괄적인 가시성을 유지하며, 포괄적인 API 지원을 통해 복잡성이 증가하는 상황에서도 컴플라이언스 프로세스를 자동화할 수 있습니다.

또한 기업은 규제를 정기적으로 검토하고 그에 맞춰 컴플라이언스 제어를 업데이트하는 주기를 선제적으로 설정해야 합니다. Akamai는 변화하는 컴플라이언스 요구사항에 대응할 수 있도록 설계된 보안 솔루션 업데이트를 정기적으로 제공해, 규제 변경과 관계없이 고객이 지속적인 컴플라이언스를 유지할 수 있도록 지원합니다.

결론: 경쟁력을 높이는 컴플라이언스

효과적인 컴플라이언스는 이제 단순히 규제 요구사항을 충족하는 것을 넘어 조직의 성과, 고객 신뢰, 경쟁 포지셔닝에 직접적인 영향을 미치는 전략적 비즈니스 과제가 되었습니다. 업계나 지역과 관계없이 선제적인 컴플라이언스 접근 방식은 강력하고 민첩한 보안 체계를 보장합니다.

IT 자산 전반에 대한 가시성 확보, 측면 이동 방지, 무단 접속 방지, 민감한 고객 데이터 및 계정 정보 보호라는 컴플라이언스 준비의 4가지 핵심 요소 전반에 걸쳐 통합 보안 접근 방식을 구현함으로써, 기업은 규제 준수를 넘어 측정 가능한 비즈니스 가치를 제공하는 지속 가능한 컴플라이언스 기반을 구축할 수 있습니다.

가장 큰 성공을 거두고 있는 기업은 비즈니스에 불가피한 비용을 발생시키는 컴플라이언스를 전략적 우위로 탈바꿈해 디지털 혁신을 지원하는 동시에 고객 신뢰, 데이터 무결성, 비즈니스 평판 등의 가장 중요한 요소를 보호하고 있습니다.

Akamai가 컴플라이언스를 어떻게 지원할 수 있는지 궁금하시면 문의해 주시기 바랍니다.

문의하기

©2025 Akamai Technologies | 지원 |
| 2025년 7월 발행