Akamai

세계적 수준의 보안 체계 로드맵

제로 트러스트를 기반으로 한 맞춤형 전환 계획

Akamai는 지속적으로 진화하는 보안 환경에서 보안을 유지하고 현재에 안주하지 않도록 최근 제로 트러스트 성숙도 모델(ZTMM)을 사용해 보안 성능을 시각화했습니다. 이 자료에서는 기업에 이러한 시각화를 사용하는 것이 개선이 필요한 중요 영역을 어떻게 드러내고 세계적 수준의 보안 체계를 달성하기 위한 명확한 로드맵을 어떻게 제시하는지 소개하겠습니다.

제로 트러스트로의 여정 간소화

기업 접속 및 보안은 복잡하며 계속 변하고 있습니다. 이러한 상황에서 제로 트러스트 보안 체계로 나아갈 때 어디에 집중해야 할지 알아내기 어려울 수 있습니다.

따라서 현재 보안 체계를 평가하고 시각화하기 위한 툴로 ZTMM을 사용하는 것이 좋습니다. Akamai는 ZTMM을 사용해 자사의 보안 체계를 평가하고 여러 고객의 보안 체계를 평가했습니다. 프로세스가 끝나면 제로 트러스트 아키텍처로 전환하기 위한 실용적인 활동으로 구성된 로드맵을 확보하게 될 것입니다. (제로 트러스트의 개념에 대한 자세한 내용은 부록 A를 참조하세요.)

제로 트러스트 성숙도 모델이 의미 있는 이유

보다 강력한 보안 체계를 구축하기 위한 가장 중요한 단계는 바로 시작 단계입니다. 하지만 끊임없이 변화하는 복잡한 사이버 보안 문제를 해결하기 위해 시작한다는 것이 말처럼 쉽지는 않습니다. 많은 기업이 제로 트러스트를 달성하기 위해 무엇을, 얼마나, 어떤 순서로 바꿔야 하는지 결정하는 데 어려움을 겪고 있습니다.

이때 ZTMM이 도움이 될 수 있습니다. ZTMM은 제로 트러스트 중심의 프레임워크를 만들어 일관된 방향성을 제공함으로써 구축이 더욱 쉬워집니다. 기업은 이를 통해 변경 계획을 세우고 업데이트에 필요한 예산을 책정할 수 있습니다. 또한 IT 전문가가 아닌 의사 결정권자에게 제로 트러스트 개념을 설명함으로써 IT 팀이 필요한 승인을 받는 데 도움을 줄 수도 있습니다.

ZTMM은 이미 검증되었습니다. 미국 CISA(Cybersecurity and Infrastructure Security Agency)가 ZTMM을 개발했고 미국 연방 행정기관들이 광범위하게 도입했습니다.

제로 트러스트 성숙도 모델의 5가지 핵심 요소와 3가지 기능

ZTMM은 5가지 핵심 요소를 통해 구축의 점진적 단계를 구분합니다. 따라서 시간에 걸쳐 조금씩 개선해 나가는 것이 가능합니다. 이 핵심 요소는 바로 ID, 디바이스, 네트워크, 애플리케이션 및 워크로드, 데이터입니다(그림 1). 또한 ZTMM에서는 5가지 요소를 모두 관통하는 다음 3가지 기능을 고려해야 합니다.

- 가시성 및 애널리틱스
- 자동화 및 오케스트레이션
- 거버넌스

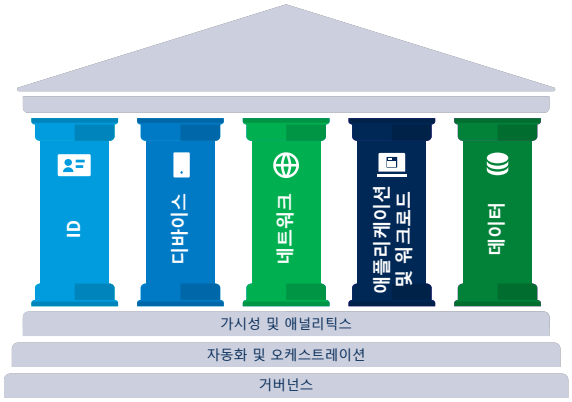


그림 1: CISA의 ZTMM은 제로 트러스트로의 전환을 지원하는 여러 경로 중 하나입니다(출처: CISA)

이러한 각 영역에는 기업이 제로 트러스트 접근 방식을 달성하는 데 얼마나 근접했는지 설명하는 성숙도 상태가 부여됩니다. 기존, 시작, 고급, 최적의 4단계 성숙도 단계는 수동 설정과 VPN으로부터 이상적인 '경계 없는 보안' 설정으로 나아가는 여정을 설명합니다(그림 2). '최적'이라는 마지막 성숙도 단계에서 기업은 애플리케이션에 최소 권한을 부여하고, 취약한 디바이스에 대한 인증 및 접속을 거부하며, 내부 위협의 확산을 방지하고, 보안 인시던트를 즉시 탐지해 이에 대응합니다. (ZTMM 프레임워크에 대한 자세한 설명은 부록 B를 참조하세요.)

제로 트러스트 성숙도 여정

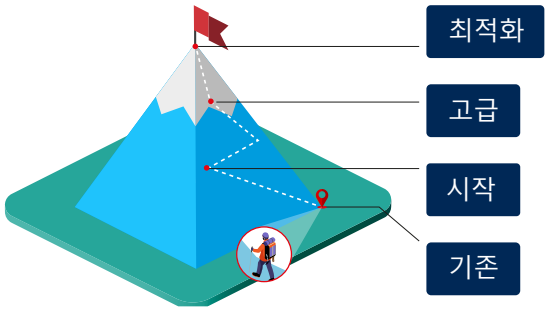


그림 2: 제로 트러스트 성숙도 여정(출처: CISA)

ZTMM은 성숙도가 가장 낮은 영역을 찾아 기업이 보다 균형 잡힌 보안 환경을 개발할 수 있도록 지원합니다. Akamai의 전문 기술과 함께 업계 최고의 보안 솔루션 제품군을 활용하면 성숙한 보안 체계로 그 어느 때보다 쉽게 전환할 수 있습니다.

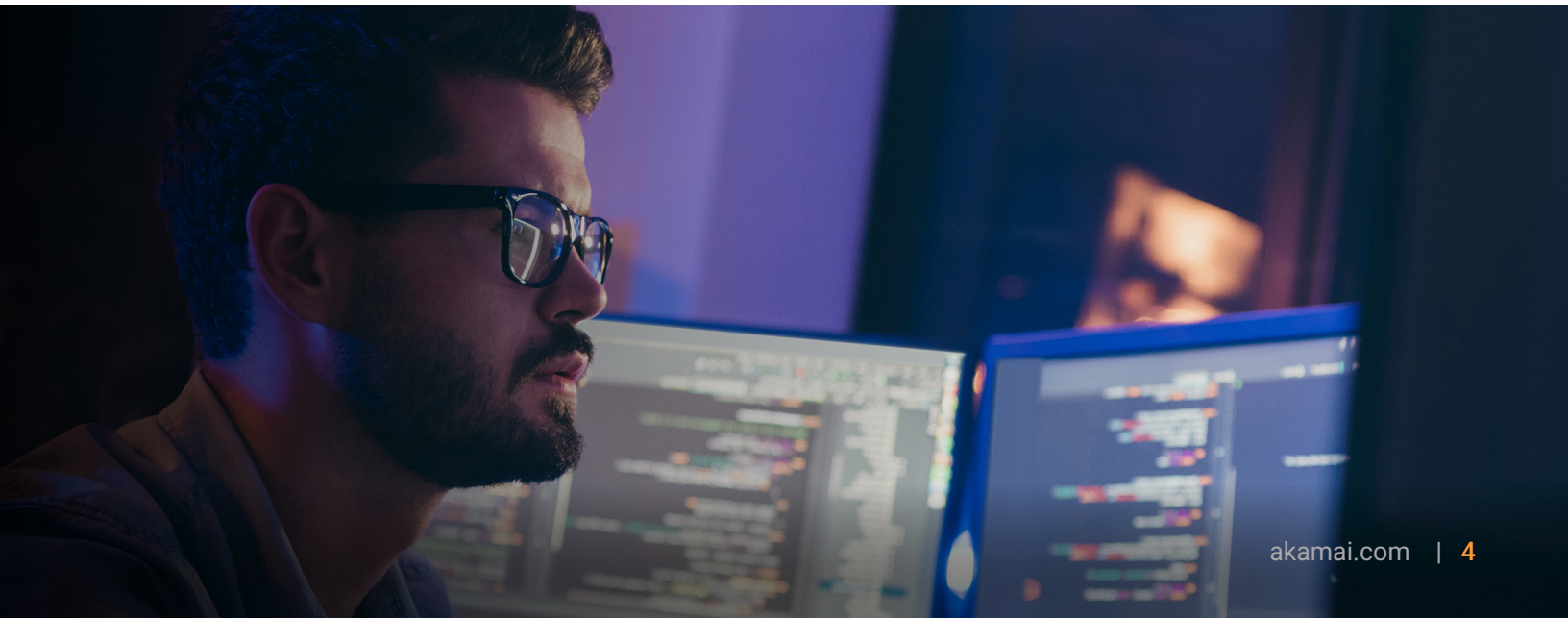
제로 트러스트를 구축하는 데 어려움을 겪고 계신가요? 혼자 고민하지 마세요.

제로 트러스트 아키텍처를 구축하는 책임은 한 부서에만 있지 않습니다. 기업 내 모든 직급의 이해관계자들로부터 지지를 받아야 하며 유연성과 승인이 필요합니다.

Akamai는 온라인 비즈니스를 지원하고 보호하는 사이버 보안 및 클라우드 컴퓨팅 기업입니다. Akamai의 시장을 선도하는 보안 솔루션, 탁월한 위협 인텔리전스, 글로벌 운영팀은 전 세계적으로 모든 터치포인트에서 중요한 데이터와 애플리케이션을 보호합니다. Akamai는 이렇게 전체적으로 파악하고 있기 때문에 제로 트러스트 보안 체계로 나아갈 때 가장 흔하게 발생하는 도전과제를 이해하고 있으며 솔루션을 찾는 데 도움을 드릴 수 있습니다.

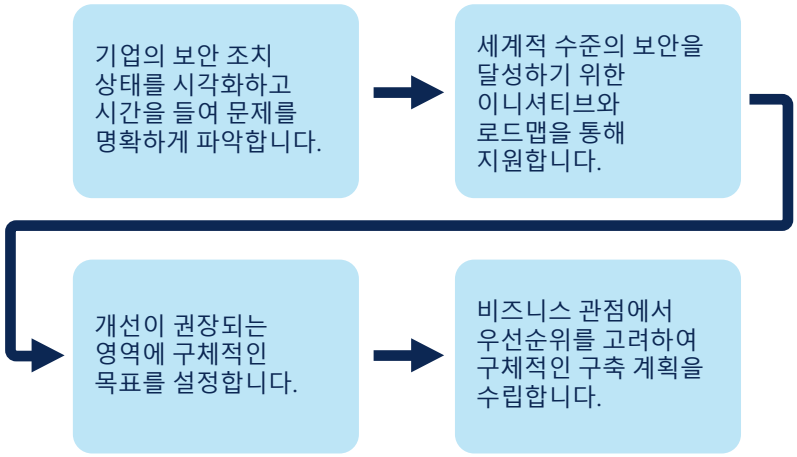
일반적인 제로 트러스트 관련 도전 과제 3가지

1. **시작 지점 파악하기:** 일반적으로 처음에는 워크로드 가시성을 확보하고 공격 표면을 줄여 사이버 안정성을 강화하는 것이 좋습니다. 이는 물론 기업의 현재 보안 체계에 따라 달라질 수 있습니다.
2. **신속하게 성공하기:** 제로 트러스트의 달성이 매우 큰 목표처럼 보여서 어느 하나에 집중하거나 목표를 향한 작은 진전에 기뻐하기 어려울 수 있습니다.
3. **ROI 입증하기:** 제로 트러스트 프로젝트는 저렴하지 않으며 기업 내에서 문화적 및 기술적 변화가 필요합니다. 특히 의사 결정권자와 보안 리더에게 공격 표면 감소, 유출 방어, 취약점 보안, 재무성과 등 투자 수익을 입증할 수 있는 능력은 매우 중요합니다.



제로 트러스트 여정을 시작하고 보안 체계를 시각화할 준비가 되셨습니까?

Akamai가 했던 것처럼 누구나 ZTMM을 사용해 기업의 현재 보안 조치의 성숙도 상태를 시각화할 수 있습니다. 그러면 제로 트러스트 아키텍처를 달성하기 위해 필요한 변화와 프로세스 간에 어떻게 균형을 맞출지 확인하는 데 도움이 될 것입니다.



Akamai가 제로 트러스트 보안 체계를 향해 이끄는 방법

성공적인 제로 트러스트 아키텍처는 보안 과제를 해결하기 위해 다양한 보안 제어와 원칙을 활용합니다.

Akamai는 세계적 수준의 보안을 달성하기 위해 전체 비즈니스와 그 목표가 반영된 구축 계획을 세울 수 있는 이니셔티브 및 로드맵을 통해 지원합니다. 이러한 접근 방식을 통해 장기적으로 효과적이고 지속가능한 보안 시스템 및 프로세스를 구축할 수 있습니다.

Akamai Cloud와 함께 Akamai의 보안 제품군(고급 분산 ZTNA 솔루션, 업계 최고의 마이크로세그멘테이션, 피싱 방지 멀티팩터 인증(MFA), 선제적 DNS 방화벽 등)을 사용하면 제로 트러스트 성숙도 규모의 마지막 단계인 최적화를 향해 보안 체계를 향상시킬 수 있습니다. 또한 단일 콘솔, 단일 에이전트를 사용해 전체 시스템을 운영할 수 있습니다(그림 3).

Akamai의 제로 트러스트 보안 제품군

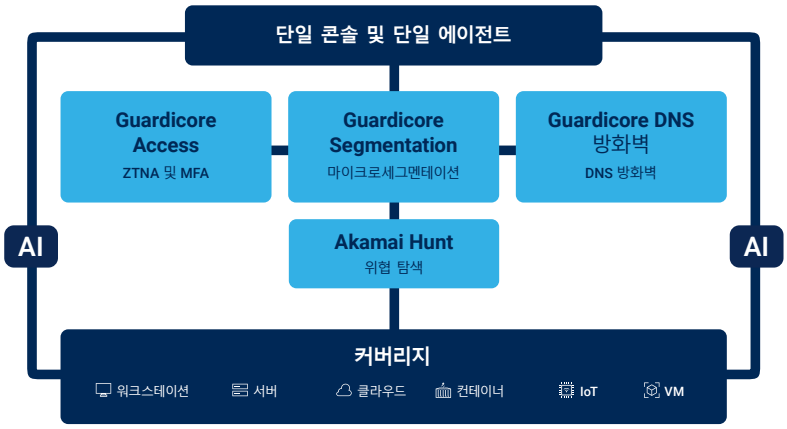


그림 3: Akamai가 제공하는 보안 제품군은 단일 에이전트가 단일 콘솔을 사용하여 실행할 수 있습니다.

사례 연구

제로 트러스트 성숙도 모델을 사용한 다국적 리테일 기업의 이커머스 보안 체계 시각화

최근 다국적 리테일 기업의 이커머스 보안 체계를 분석해 보안 상태를 시각화하고 세계 최고 수준의 보안 체계로 전환하기 위한 로드맵을 제공했습니다. Akamai 전문가로 구성된 팀은 ZTMM 전반에 걸쳐 개선이 필요한 영역을 식별하고 이를 중요도에 따라 순위를 매겼습니다. 여기서 그 결과를 공유합니다.

구축 과정에 변동이 많은 불균형 시스템

각 핵심 요소에서 모바일 디바이스 관리 및 애플리케이션 배포 자동화 등 일부 기능은 가장 높은 수준의 성숙도(최적, Optimal)로 구축되었습니다. 그러나 각 요소의 일부 기능은 기존(Traditional) 수준에서 유지되고 있으며, 이는 심각한 리스크를 나타냅니다.

특히 'ID' 및 '네트워크' 요소의 중요 기능은 강화되지 않았습니다. 이러한 핵심 요소는 제로 트러스트 아키텍처의 토대입니다. 이러한 기능에는 MFA, ID 인프라의 통합 관리, 맥락 기반 접속 제어 및 마이크로세그멘테이션이 포함되어 있었습니다.

위험한 ID 인프라

당사의 분석가들은 ID 및 비밀번호 인증이 리테일 기업의 표준이며 MFA는 몇 가지 시스템에 제한적으로 사용된다는 사실을 발견했습니다. 이로 인해 인증 정보가 남용될 리스크가 높아집니다. 또한 Microsoft Entra ID, 온프레미스 AD(Active Directory) 및 LDAP(Lightweight Directory Access Protocol)와 같은 여러 ID 인프라가 있었습니다. 리테일 기업의 관리가 통합되지 않았기 때문에 LDAP와 같은 보안 수단이 약한 ID 인프라부터 유출이 시작될 리스크가 있었습니다.

통합되지 않은 권한 확인 제어

권한 확인 제어가 통합되지 않아 각 애플리케이션이 개별적으로 처리되었습니다. 이에 따라 취약한 디바이스의 접속 또는 의심스러운 접속을 차단할 수 없었습니다. 즉, 회사 네트워크에 접속하는 직원이나 파트너의 PC가 멀웨어에 감염된 경우, 측면 이동을 통해 시스템 및 리소스에 무단 접속이 이루어질 리스크가 높아집니다.

부적절한 세그멘테이션

Akamai는 리테일 기업의 보안 조치가 외부 위협에 크게 집중되어 있기 때문에 이미 네트워크에 침입한 공격자들이 일으키는 리스크가 간과되고 있다는 사실을 발견했습니다. 강력한 내부 세그멘테이션이 없다면 유통 창고의 Wi-Fi 네트워크 또는 VPN의 취약점을 통한 침입으로 인해 측면 이동이 통제되지 않을 수 있습니다. 이러한 내부 방어 장벽의 부족으로 시스템 감염, 데이터 유출, 운영 중단의 리스크가 크게 증가했습니다. 격리 조치가 없어 공격이 네트워크를 자유롭게 이동할 수 있기 때문입니다.

불충분한 취약점 관리 및 대응

리테일 기업에는 SBOM(Software Bill Of Materials)을 취약점 정보에 연결하는 관리 시스템이 없었습니다. 즉, 애플리케이션 취약점을 신속하게 탐지하고 대응할 수 없기 때문에 리스크가 높아졌습니다.

Akamai의 권장 사항

보안 체계를 강화하기 위한 다음 5단계를 리테일 기업에 권장했습니다.

1. 현재 설정에서 무단 침입과 측면 이동의 리스크를 줄이는 선제적 조치 취하기
2. ID 인프라를 기존 기술 스택에 계속 통합하기
3. 제로 트러스트 네트워크 접속과 함께 인증 및 권한 확인 기능을 확장하기 위한 계획 수립하기
4. 세분화된 워크로드 및 애플리케이션 보호를 구축하는 가장 효과적인 방법 결정하기
5. 알려지지 않은 미래의 위협에 대한 대응 시스템과 프로세스를 구축하고, 취약점 관리 및 대응을 강화하는 시스템과 프로세스를 개발하며, 계획 수립하기

제로 트러스트 여정에 관심이 있으시다면 Akamai에 문의하시고 무료 보안 평가를 받아보세요.

부록 A: 제로 트러스트 개념의 개요

제로 트러스트는 기업의 네트워크 경계 내부 또는 외부의 사용자, 디바이스 또는 시스템을 신뢰하면 안 된다는 개념을 기반으로 하는 보안 철학입니다.

대신 리스크를 최소화하기 위해서 검증 프로세스와 모니터링이 사용됩니다. 여기에는 엄격한 ID 및 접속 관리(IAM) 정책 적용, 멀티팩터 인증(MFA) 사용, 업무 기반 접속 제어(RBAC)의 우선순위 지정 등의 접근 방식이 포함됩니다.

제로 트러스트 개념이 소개된지 약 15년이 지났지만, 코로나19 팬데믹 기간에 기업의 원격 접속 요구사항이 증가하면서 더욱 중요해졌습니다. 사용자와 디바이스가 중앙 집중화되지 않고 분산된 경우 기존 보안 조치의 효과가 떨어진다는 것을 많은 기업이 깨달았습니다.

현재에는 제로 트러스트 아키텍처, 제로 트러스트 네트워크 접속(ZTNA), 제로 트러스트 보안 웹 게이트웨이(SWG), 마이크로세그멘테이션을 포함해 제로 트러스트 원칙을 구축한 많은 사례가 있습니다.

제로 트러스트에 대해 자세히 알아보기

부록 B: ZTMM 2.0 프레임워크

5가지 핵심 요소

각 핵심 요소는 각자의 속도에 맞춰 진행할 수 있으며, 핵심 요소 사이에 조정이 필요할 때까지 다른 요소보다 빠르게 진행할 수도 있습니다.

핵심 요소	설명
ID	기관 사용자 또는 엔티티(사람이 아닌 엔티티 포함)를 고유하게 설명하는 속성 또는 속성 집합
디바이스	서버, 데스크톱 및 노트북, 프린터, 휴대폰, 사물 인터넷(IoT) 디바이스, 네트워킹 장비 등을 포함하여 네트워크에 연결할 수 있는 모든 자산
네트워크	기관 내부 네트워크, 무선 네트워크, 인터넷 등 일반적인 채널과 메시지를 전송하는 데 사용되는 기타 잠재 채널을 포함한 개방형 통신 미디어
애플리케이션 및 워크로드	온프레미스, 모바일 디바이스 및 클라우드 환경에서 실행되는 기관 시스템, 컴퓨터 프로그램 및 서비스
데이터	시스템, 디바이스, 네트워크, 애플리케이션, 데이터베이스, 인프라, 백업에 저장되어 있거나 저장되었던 정형 및 비정형 파일과 조각, 그리고 그 관련 메타데이터

핵심 요소 간 기능

이 3가지 기능은 전체 제로 트러스트 프레임워크를 지원하여 통합되고 응답성이 뛰어나며 일관된 보안 수단을 만듭니다.

기능	설명
가시성 및 애널리틱스	기업은 모든 사용자 활동, 디바이스 상태 및 네트워크 상호작용을 명확하고 실시간으로 확인할 수 있어야 합니다. 위협을 탐지하고 신속하게 대응하면 리스크가 줄어듭니다. 또한 기업은 정보를 바탕으로 선제적인 보안 결정을 내립니다.
자동화 및 오케스트레이션	인적 오류는 보안 문제의 흔한 원인입니다. 자동화 및 오케스트레이션이 최적화되면 인적 오류 가능성이 최소화됩니다. 또한 자동화는 일상적인 작업을 간소화하고, 오케스트레이션은 다양한 시스템에서의 보안 활동을 체계적으로 정리합니다. 이에 따라 위협에 보다 빠르고 체계적으로 대응할 수 있는 적절한 환경을 조성할 수 있습니다.
거버넌스	훌륭한 보안 거버넌스는 책임 소재를 명확히 하고 모든 사람이 동일한 보안 관행과 규제를 따르도록 합니다. 이를 통해 안전한 운영을 위한 탄탄한 기반을 구축할 수 있습니다. 또한 제로 트러스트 지침을 명확하게 설정하고 기업이 컴플라이언스 표준을 준수할 수 있도록 지원하기도 합니다.

제로 트러스트 성숙도 모델의 성숙도 측면

ZTMM 2.0은 각 기능에 대한 4가지 성숙도 수준을 정의합니다. 목표는 5대 핵심 요소 및 3가지 기능의 현재 성숙도 수준을 결정한 다음 각 영역을 가장 높은 성숙도 수준으로 향상시키기 위한 계획을 세우는 것입니다.

성숙도 수준	설명
기존	수동 설정, 대응 및 방어, 정적 및 고립된 정책과 솔루션
시작	자동화 시작, 핵심 요소 간 초기 솔루션, 최소 권한에 대한 약간의 대응 변경, 내부 시스템에 대한 통합된 가시성
고급	해당되는 경우 자동화된 제어, 핵심 요소 간 정책 적용, 리스크 체계에 따른 최소 권한 변경, 사전 정의된 방어 조치에 대한 대응
최적화	해당되는 경우 자동화된 제어, 핵심 요소 간 정책 적용, 리스크 체계에 따른 최소 권한 변경, 사전 정의된 방어 조치에 대한 대응

Akamai 보안 제품군 및 장기적으로 기업 보안에 미치는 영향이 궁금하시면 Akamai로 문의하세요.

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.com, akamai.com/blog를 방문하거나 X(기존의 Twitter)와 LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2025년 2월 발행.