Akamai

백서

# 소프트웨어 기반의 세그멘테이션으로 사이버 보안의 장애물 제거

유럽 금융 부문에서 보안에 대한 접속을 개선하고 사이버 리스크 비용을 줄이는 데 도움을 주는 Akamai Guardicore Segmentation

# 개요

금융 부문은 유럽 연합 경제의 중요한 부분이며, 금융 시스템은 일부 유럽 정부와 규제 기관에서 중요한 인프라로 여겨집니다. 금융 서비스 기업이 제공하는 상품과 서비스는 고가용성 IT 시스템과 여러 채널 및 당사자를 통해 제공되는 정보에 대한 적시 접속에 크게 의존합니다.

그러나 랜섬웨어와 암호화폐 채굴 공격은 공격자들이 얼마나 빠르게 이 중요한 인프라를 며칠 또는 몇 주 동안이나 무력화하고 연결된 써드파티 및 업계 동료에게까지 확산시킬 수 있는지 보여주었습니다.

그래서 유럽의 금융 기업은 경쟁력 확보, 고객 유치 및 이탈 방지를 위해 최첨단 디지털 기능을 도입해야만 합니다. 하지만 보안 제어 및 보고에 대한 규제 요구사항이 증가함에 따라 클라우드 도입률이 크게 떨어지고 있습니다. 예를 들어 유럽 연합의 GDPR(General Data Protection Regulation)은 고객을 보호하지 못하는 기업에 대해 전 세계 매출의 최대 4%에 해당하는 벌금을 부과할 수 있습니다.[1]

또한 SWIFT CSP(Society for Worldwide Interbank Financial Telecommunication Customer Security Programme) 및 ECB CROE(European Central Bank의 사이버 안정성 감독 기대치)와 같은 최근 규정은 특히 더 세분화된 네트워크 세그멘테이션을 요구합니다.

기존의 세그멘테이션 접근 방식 및 이와 관련된 수동 절차는 기술 혁신, 증가하는 보안 리스크, 지속적인 규제 강화의 속도를 따라잡기에 적합한 접근 방식이 아닙니다.

기업은 새로운 툴을 도입할 뿐만 아니라 단순성, 투명성, 자동화를 수용하기 위해 보안 및 세그멘테이션 프로세스를 근본적으로 바꾸어야 합니다.

이 백서에서는 다음과 같은 주제를 다룹니다.

- 오늘날 유럽 금융 부문이 직면한 주요 사이버 보안 과제
- 은행과 금융 기업이 비용 효율적이고 간편한 세그멘테이션 접근 방식을 통해 이러한 리스크를 해결하는 방법
- Akamai Guardicore Segmentation의 접근 방식을 통해 기업이 보안 프로세스를 간소화함으로써 비용을 대폭 절감하고 컴플라이언스를 가속하는 방법

# 오늘날의 사이버 보안은 복잡하고 비용이 많이 듭니다

유럽 은행과 금융 기업은 기업의 보안과 고객 데이터 보호를 위해 노력하고 있지만, 리스크, 써드파티 접속 요구사항, 컴플라이언스 요구사항이 나날이 진화하는 오늘날의 환경에서 보다 강력한 보안 체계를 구축할 방법을 찾기는 쉽지 않습니다.

## 사이버 리스크 증가로 금전적 손실 증가

사이버 범죄와 관련된 리스크는 금융 기업에 특히 심각한 영향을 미칩니다. 금융 업계는 데이터 유출 건당 평균 572만 달러의 손실을 입었으며, 이는 공격을 받고 있는 모든 업계를 통틀어 두 번째로 높은 수치입니다.[2]

하지만 강력한 보안 체계를 갖추는 데는 많은 비용이 듭니다. 여러 플랫폼을 보호하는 동시에 비즈니스 서비스 제공에 중요한 써드파티 접속을 보호하기 위해 보안 제어를 적용하는 복잡한 작업은 복잡할 뿐만 아니라 인프라 비용과 인건비도 크게 증가합니다.

## 컴플라이언스 비용의 지속적인 증가

유럽의 금융 서비스 기업들은 컴플라이언스를 준비하고 검증하는 데 필요한 비용, 시간, 전체 리소스가 크게 증가했습니다. 규정은 금융 부문의 안정성을 보장하는 데 도움이 되지만, 새로운 사이버 보안 규정이 거듭 도입됨에 따라 디지털 전환 속도가 늦어지고 상당한 투자가 요구되면서 수익성과 성장에 지장을 주고 있습니다.

GDPR부터 시작해 정책 강화에 대한 압력은 더욱 증가했고 네트워크 및 정보 시스템(NIS) 보안에 관한 지침, ECB CROE 가이드 그리고 가장 최근에는 EU 사이버 보안법이 뒤이어 시행되었습니다. SWIFT CSP와 같은 벤더사 규정이 추가됨에 따라 오늘날 컴플라이언스를 달성하려면 수많은 보고와 기술 요구사항을 충족해야 합니다.

그러므로 기술을 업그레이드함에 따라 은행과 금융 기업도 관리를 간소화하고 사이버 보안 및 컴플라이언스와 관련된 운영 비용을 낮출 수 있는 방법을 찾아야 합니다.

## 써드파티와 금융 시장 상호 작용의 보안 취약점

사용자의 편의와 투명성을 개선하기 위한 EU의 Payment Services Directive(PSD2) 개정안은 써드파티 접속 및 개인 데이터 감염의 리스크를 증폭시켰습니다. 비즈니스 및 기술 프로세스의 효율성과 투명성에 대한 금융 서비스 동종 기업과 규제 기관의 압박도 커지고 있습니다.

보안, 이동성, 새로운 서비스에 대한 고객의 추가적인 요구사항으로 인해 써드파티 정보 및 통신 기술 인프라, 아웃소싱 공급업체 및 이들의 공급망에 대한 의존도도 높아졌습니다.

그 어느 때보다 환경의 연결성이 강화됨에 따라, 자동화된 은행 내부 및 은행 간 트랜잭션을 비롯해 각종 통신을 보호하는 데 더 많은 리소스가 집중되고 있습니다.

이제 공격자들은 단일 자산을 악용하기만 하면 동종 금융 기업과 금융 시장을 비롯한 상호 연결된 당사자 사이에서 측면으로 이동할 수 있기 때문에, 한 곳의 데이터 센터에서 한 번의 유출이 발생하기만 해도 도미노처럼 전체 유럽 금융 서비스 생태계의 보안과 비즈니스 연속성이 리스크에 노출됩니다.

## 새로운 보안 접근 방식이 필요한 하이브리드 클라우드

컴플라이언스 규정과 유럽 은행 기관[3]의 지침은 금융 부문의 클라우드 도입 트렌드를 뒷받침하고 있습니다. 유럽에서는 클라우드 도입이 늘고 있지만, 관련 규정으로 인해 온프레미스 시스템을 클라우드로 전환하는 작업이 더욱 복잡해졌습니다.

이 때문에 유럽 기업들은 전체 클라우드 환경보다는 핵심 기능을 온프레미스에 유지하고 하이브리드 클라우드 환경을 도입할 가능성이 더 큽니다. 또한 많은 은행이 여러 클라우드 서비스 사업자를 통해 멀티클라우드 인프라를 구축했습니다.

그러나 기업은 보통 보안 강화만을 추구하지는 않습니다. 프로세스 수정을 통해 비용을 절감하고 운영 효율성을 개선할 방안도 모색하고 있습니다. 성공의 열쇠는 자동화와 프로세스 최신화에 있습니다.

# 네트워크 가시성 및 세그멘테이션으로 주요 사이버 보안 과제 해결

이러한 과제를 해결하려면 중요 애플리케이션과 워크로드를 안전하게 격리하는 것이 중요하며, 일반적으로 이를 세그멘테이션이라 부릅니다. 이를 통해 금융 기업은 비즈니스 요구사항에 따라 대규모 보안을 실현하고 규제 요구사항에 부합하는 리스크 기반 접근 방식을 제시할 수 있습니다.

## 레거시 방화벽으로는 부족한 이유

유럽 은행과 금융 기업에서 세그멘테이션을 보다 광범위하게 수용하고 배포하지 못한 데에는 몇 가지 이유가 있습니다.

**유지 관리 및 리소스 집중도:** 많은 보안 및 IT 전문가는 시간이 너무 오래 걸리고 여러 팀과 막대한 양의 리소스가 묶여 있게 된다는 이유로 세그멘테이션 이니셔티브 추진을 주저합니다. 기존 방식은 복잡하고 시간이 많이 소요되는 경향이 있어 충분히 망설여질 만합니다. 예를 들어 여러 위치와 환경에 VLAN, ACL, 방화벽을 설정하는 작업은 번거롭고 느리며 오류가 발생하기 쉬운 프로세스인 경우가 많습니다. 또한 기존 방식은 의미 없을 뿐 아니라 자주 변경될 수 있는 IP와 같이 신뢰할 수 없는 ID 데이터에 크게 의존합니다.

**가시성 부족:** 기업은 동서 트래픽에 대한 가시성이 부족하기 때문에 세그먼트 간 의존성을 파악하고 중요한 구성요소를 훼손하지 않는 세그멘테이션 룰을 생성하기 어렵습니다. 트래픽 탭이나 유사한 기술을 사용하더라도 결과적으로는 IP와 포트 간에 필요한 맥락과 정교한 해석이 부족해 보이는 경우가 많습니다. PaaS(Platform as a Service) 같은 동적 환경에서는 이것이 아예 불가능합니다.

**인프라의존성:** 워크로드가 클라우드로 확장되는 상황은 점점 더 일반화되고 있으며 이러한 경우 프로세스가 더욱 복잡해집니다. 모든 데이터 이그레스 지점에 하드웨어 방화벽을 설치하려면 비용이 많이 듭니다. 복잡한 네트워킹 설정으로 인해 관리 문제도 더욱 심화됩니다. 그러나 클라우드 및 컨테이너 외에도 가상화된 자산이나 레거시 자산을 포함하는 다양한 환경의 요구사항을 충족하려면 이러한 설정이 필요합니다.

> **"일부 영역의 규제 체제는 기술 혁신과 보조를 맞추는 데 어려움을 겪었지만, 기업의 리스크 관리 및 제어 프레임워크도 이와 마찬가지였습니다."**
>
> **- 2023년 금융 시장 규제 전망, Deloitte의 EMEA 규제 전략 센터**

# 프로세스의 근본적인 변화 도입

수백 대의 서버를 보유한 중간 규모의 금융 서비스 기업도 수천 개의 세그멘테이션 정책 라인 항목을 생성할 수 있습니다. 특히 맥락이 중요한 Jenkins 및 CI/CD 주기와 같은 툴을 사용해 자동화된 애플리케이션 전송을 지원하는 환경에서 이를 수동으로 관리하는 것은 효과적이지 못합니다.

Akamai Guardicore Segmentation은 한 단계 더 나아가 기업이 정책 생성 및 업데이트 주기를 근본적으로 수동적인 프로세스에서 자동화된 프로세스로 전환할 수 있도록 지원합니다.

Akamai Guardicore Segmentation을 사용하는 경우 애플리케이션 프로파일링이 자동화되고, 모든 의존성이 매핑되면 룰 생성 및 업데이트가 반복 가능한 프로세스로 전환될 수 있으며 이해관계자와 애플리케이션 소유자는 자동 생성된 정책을 승인하기만 하면 됩니다. 그러면 프로젝트 속도를 현저히 늦출 수 있는 수동 개입이 거의 필요하지 않으며 설정 오류 및 인적 오류의 리스크가 줄어듭니다.

자동화된 룰 생성은 룰의 구조적 일관성과 정책 자체의 확장성을 유지함으로써 방화벽을 더욱 최적화합니다.

## IT 혁신의 가속으로 진정한 제로 트러스트 환경 구축

금융 기업이 대규모 세그멘테이션을 실현하지 못하는 이유가 수동 프로세스와 제한된 리소스 때문이어서는 안 됩니다. 진정한 제로 트러스트를 위해서는 올바른 기술뿐만 아니라 보안 정책 생성, 변경, 유지 관리 프로세스의 최신화도 필요합니다.

호스트 또는 소프트웨어 기반 방화벽은 애플리케이션 수준 보안에 대한 간단하면서도 비용 효율적인 접근 방식으로 부상했습니다. 이러한 접근 방식은 구축 속도를 크게 높이고 지속적인 유지 관리를 간소화하며 궁극적으로 위협을 방어하는 데 보다 효과적입니다. Akamai Guardicore Segmentation은 기본적으로 모든 규모의 기업이 간단하고 비용 효율적이며 빠르게 세그멘테이션할 수 있도록 구축되었습니다.

데이터 센터의 모든 애플리케이션과 그 의존성에 대한 비주얼 맵을 제공합니다. 이제 보안 운영자는 네트워크 및 개별 프로세스 수준 보안 정책을 생성하고 적용해 중요 애플리케이션과 자산을 격리하고 세그멘테이션할 수 있습니다. 이 소프트웨어 정의 오버레이 접근 방식은 기본 인프라로부터 독립적이며 온프레미스 레거시 시스템, VM, 컨테이너, 클라우드 등에 걸쳐 있는 워크로드를 보호합니다. 위치에 상관없이 개별 또는 논리적으로 그룹화된 애플리케이션을 중심으로 정책을 생성할 수 있습니다. 이러한 정책은 어떤 구성요소가 서로 통신할 수 있고 통신할 수 없는지를 지정함으로써 보안에 대한 제로 트러스트 접근 방식의 기반을 마련합니다.

## 사이버 리스크와 비용을 효율적으로 절감

Akamai Guardicore Segmentation을 사용하는 금융 기업은 가장 시급한 몇 가지 보안 문제를 단기간에 해결하면서 비용을 절감할 수 있다는 사실을 알게 되었습니다.

**사이버 리스크 비용 절감** - 점점 복잡해지며 상호 연결된 환경에서 네트워크 보안 지침과 모범 사례를 적용합니다.

**컴플라이언스 관리 간소화** - 정밀한 맥락 가시성과 세그멘테이션 정책을 통해 컴플라이언스 관련 자산과 비즈니스 크리티컬 애플리케이션을 신속하게 매핑하고 격리합니다. 금융 기업은 하나의 창 접근 방식을 통해 중요한 자산을 보호하고 사기 리스크를 방어하며 고객 개인 정보를 보호하기 위한 조치를 취하고 있음을 합리적으로 입증할 수 있습니다.

**써드파티 접속 보호**-ID 기반의 세그멘테이션을 통해 써드파티 트래픽을 라우팅하고 네트워크에서의 사용자 이동을 차단하고 제한합니다. 이 방식으로 써드파티 및 금융 시장 상호 작용에 대한 보안을 강화해 공격자가 감염된 다른 시스템으로부터 '침입 후 확장'하는 것을 방지합니다.

**일반적인 IT와 송금 및 결제 시스템 분리** - 기관의 일반 IT 환경에서 SWIFT 서비스를 엄격하게 분리하기 위해 전자 자금 이체 및 결제 시스템, 특히 SWIFT의 요구사항을 충족합니다. 세분화된 세그멘테이션을 통해 은행의 IT 팀은 서비스 공급업체의 '구역' 주위에 맥락 기반(사용자, 도메인) 경계를 설정함으로써 무단 접속을 더욱 제한할 수 있습니다.

**안전하고 신속하게 클라우드로 전환** - 전환에 앞서 워크로드를 매핑하고 모든 중요 애플리케이션과 그 의존성을 대한 인벤토리를 조사합니다. 링펜싱 정책은 이러한 맵을 바탕으로 전환 프로세스 전반에서 워크로드에 따라 일관된 보안을 유지할 수 있습니다. 이 접근 방식을 통해 애플리케이션이나 인프라 변경에 관계없이 동일한 보안 제어를 유지하면서 보다 빠르고 안전하게 클라우드로 전환할 수 있습니다.

**효율적인 유출 방어로 비즈니스 연속성 보장** - 동서 트래픽과 유출 지표에 대한 정밀한 가시성을 통해 공격자가 민감한 금융 및 고객 데이터를 유출하기 전에 공격자를 저지하도록 비정상적인 움직임을 알립니다.

**측면 이동 제한을 통한 리스크 감소** - 오늘날 데이터 센터 트래픽의 대부분은 외부(남북)에서 데이터 센터로 유입되는 것이 아니라 애플리케이션 사이(동서)에서 측면으로 이동합니다. 비즈니스 크리티컬 애플리케이션 및 시스템을 링펜싱해 내부 경계를 설정하면 공격표면이 효과적으로 감소하므로 공격의 측면 확산을 방지하고 유출 시 피해를 제한할 수 있습니다.

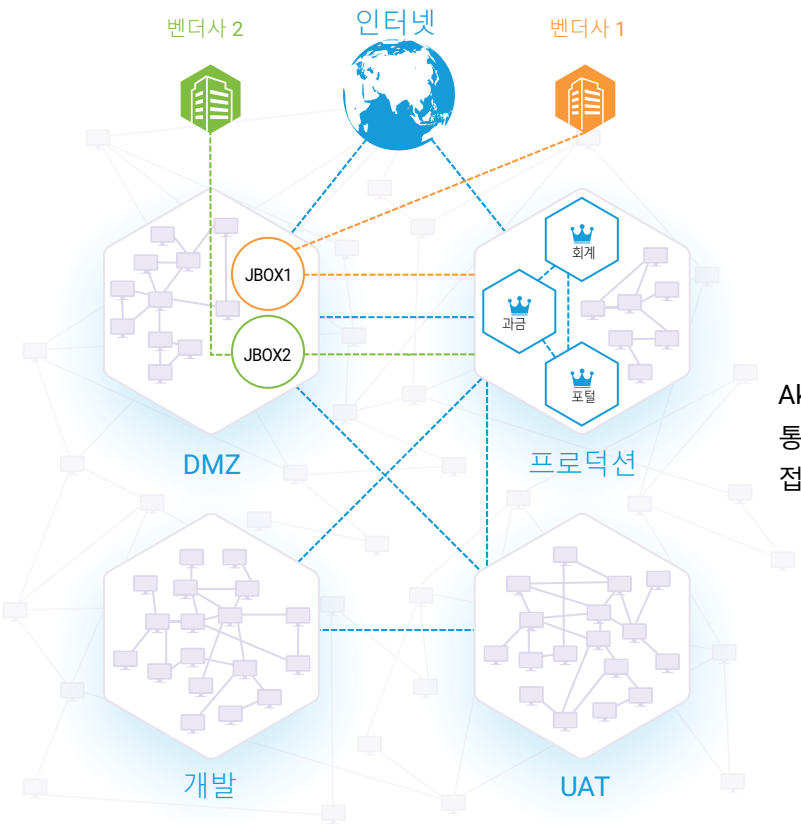
# 사례 연구: 컴플라이언스 비용을 절감한 유럽의 대형 다국적 은행

유럽의 한 대형 은행에서 뉴욕 연방준비은행(FRBNY), 싱가포르 통화감독청(MAS), ECB 등 여러 규제 기관의 기술 요구사항을 준수하는 데 필요한 새롭고 효율적인 네트워크 세그멘이션 접근 방식을 찾고 있었습니다.

은행이 사용하던 기존의 세그멘테이션 접근 방식, 방화벽 룰, VLAN의 효율성이 떨어지면서 매년 높은 컴플라이언스 위반 비용이 발생했습니다. 또한 정책을 생성하고 업데이트하는 데 상당한 프로덕션 다운타임과 리소스가 필요해 IT 운영에 영향을 미치고 있었습니다.

은행의 세그멘테이션 목표를 달성하기 위해서는 보다 비용 효율적이고 구축하기 쉬운 접근 방식이 필요했습니다. 새로운 솔루션의 핵심 요구사항은 은행의 인프라와 리소스에 미치는 영향을 최소화하면서 관련 규정을 완벽하게 준수하는 것이었습니다.

여러 벤더사가 관여한 전체 평가 프로세스를 마친 후 은행의 인프라 및 IT 보안 팀 의사 결정자들은 Akamai Guardicore Segmentation이 마이크로세그멘테이션에 이르는 가장 빠르고 간단한 경로를 제공한다는 데 의견이 일치했습니다.



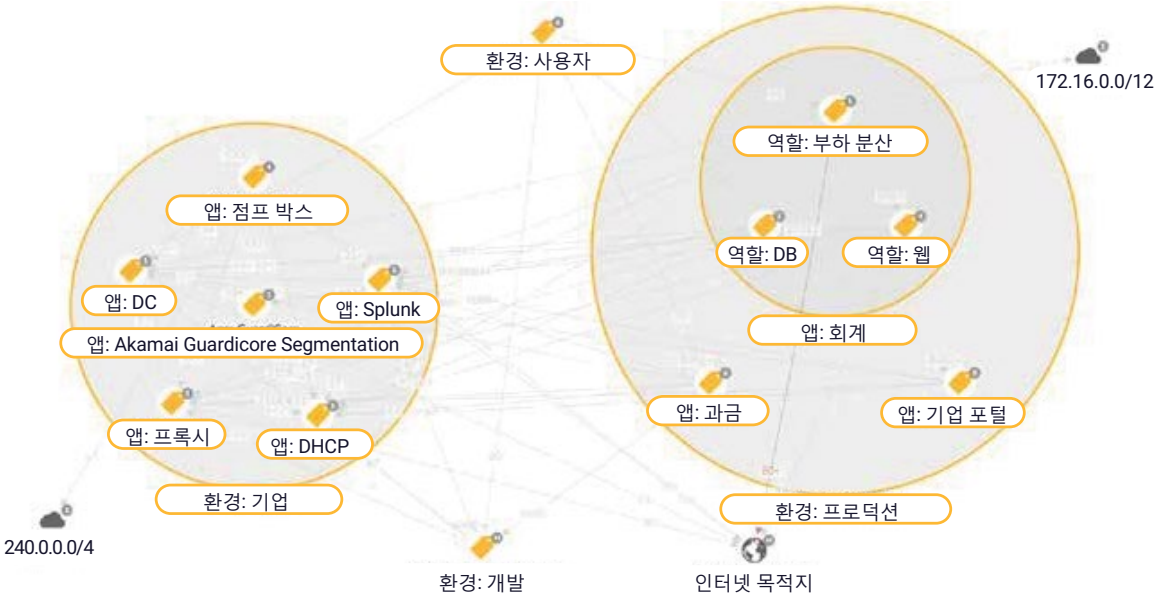

Akamai Guardicore Segmentation을 통한 환경 세그멘테이션 및 써드파티 접속 제어

## 세그멘테이션의 간소화 및 가속

은행은 컨테이너를 포함한 여러 IT 인프라 종류와 여러 지역에 걸쳐 Akamai Guardicore Segmentation을 배포했습니다. 애플리케이션을 변경할 필요가 없었기 때문에 프로덕션 환경에서 다운타임이 발생하지 않았습니다.또한이를통해은행은데이터센터워크로드에대한중앙집중화된가시성을신속하게확보하고 프로덕션, 테스트, 개발 환경을 격리할 수 있었습니다. 고객은 Akamai Guardicore Segmentation을 사용해 프린터, 기타 IoT 디바이스, 무단 사용자의 서버 접속을 제한할 수도 있었습니다.

이 프로젝트는 3개월 이내에 완료되었습니다. 기존 세그멘테이션 방법을 사용했을 때 예상된 것보다 10배 더 빠른 속도였습니다. 은행은 환경을 신속하게 매핑하고 수집한 정보를 기반으로 정책을 생성함으로써 1만 개 이상의 미준수 자산에 대한 컴플라이언스 요구사항을 해결하고 보안 체계를 개선했습니다. 신속한 배포로 리스크가 감소하고 상당한 비용 및 리소스 절감 효과를 얻었습니다.

Akamai의 전문 서비스 팀은 은행이 세그멘테이션 프로세스를 완전히 혁신할 수 있도록 지원했습니다. 오늘날 자산 레이블링 및 세그멘테이션 정책은 완전히 자동화되어 애플리케이션 개발 및 배포 프로세스에 내장됩니다. 레이블 생성, 변경 관리, 보안 인시던트, 서비스 요청은 ServiceNow 워크플로우에완전히통합되었습니다.고객은고객은플랫폼의결과와플랫폼이제공하는가치,Akamai의 숙련된 전담 기술 서비스 팀에 매우 만족했습니다.



## akamai.com/guardicore에서 Akamai Guardicore Segmentation에 대해 자세히 알아보세요.

1 "What are the GDPR Fines?" GDPR.eu, 2019년 2월 13일.

2 "Cost of a data breach 2022", IBM.

3 "A comprehensive guide to cloud adoption in Europe's banking sector", Techerati, 2019년 10월 31일.

Akamai는 어디에서 구축하고 제공하든지 생성하는 모든 것에 보안 기능을 내장하도록 지원함으로써 고객 경험, 인력, 시스템, 데이터를 보호합니다. Akamai 플랫폼은 글로벌 위협에 대한 가시성을 바탕으로 제로 트러스트 지원, 랜섬웨어 차단, 앱 및 API 보안 또는 DDoS 공격 차단을 목표로 보안 체계를 조정하고 발전시켜 지속적으로 안심하고 혁신하며 확장하고 가능성을 현실로 구현할 수 있습니다. Akamai의 보안, 컴퓨팅, 전송 솔루션에 관해 자세히 알아보려면 akamai.com와 akamai.com/blog를 방문하거나 Twitter와 LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2023년 06월 발행.