

# FOSS

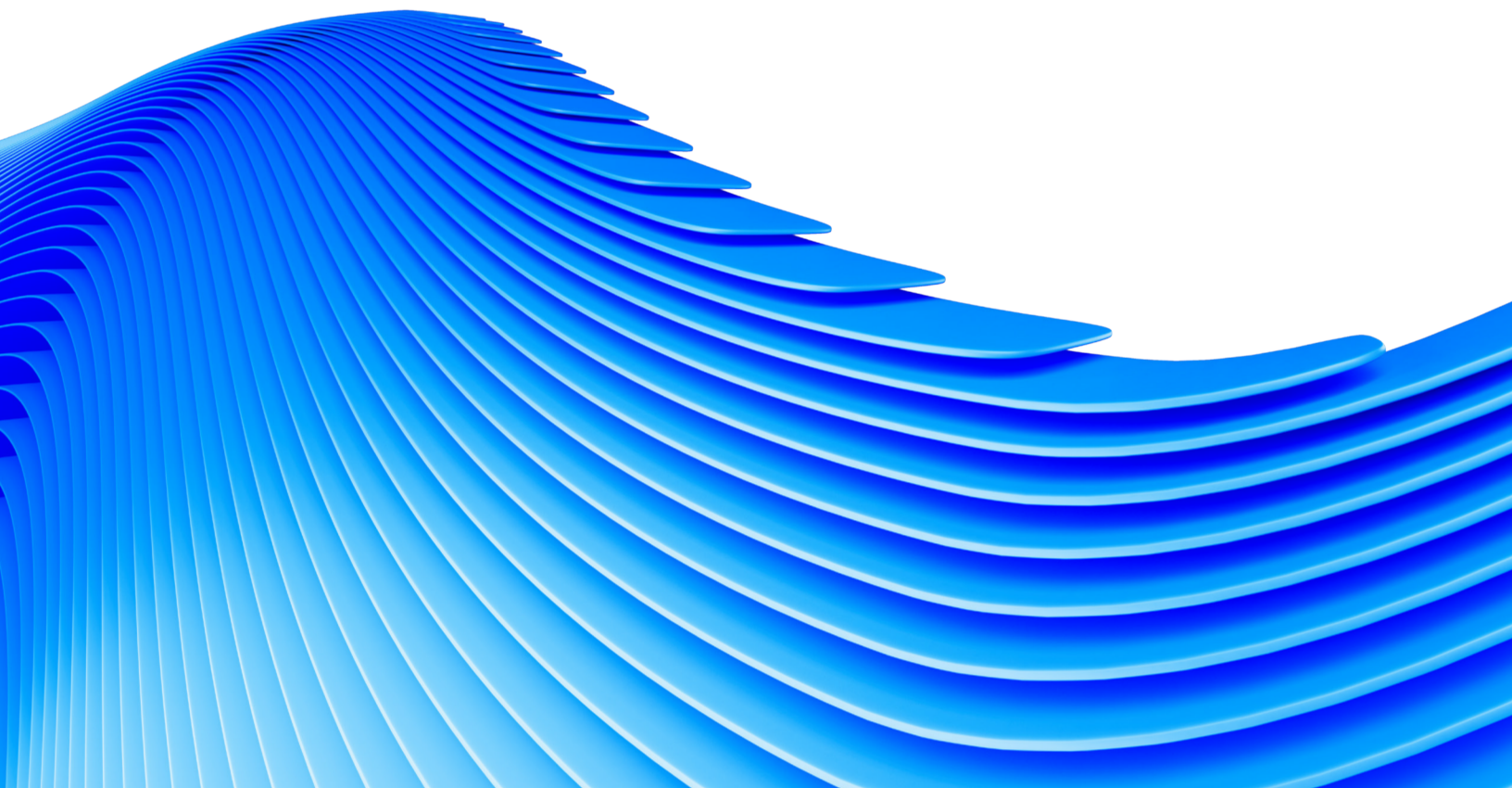
제11권, 제2호

## 2025년 앱 및 API 보안 현황

AI가 디지털 환경을 변화시키는 방법

## 콘텐츠

|    |                              |
|----|------------------------------|
| 02 | 서론                           |
| 04 | 보고서의 핵심 인사이트                 |
| 06 | API 위협 인텔리전스의 진화             |
| 13 | 웹 공격 : 연도별 비교 및 트렌드          |
| 17 | 레이어 7 DDoS 공격 : 연도별 비교 및 트렌드 |
| 21 | 업계 트렌드                       |
| 27 | 지역별 트렌드                      |
| 39 | 컴플라이언스                       |
| 44 | 방어                           |
| 46 | 방법론                          |
| 47 | 크레딧                          |





## 서론

2025년 초 웹 애플리케이션 보안 환경에서는 과거와는 완전히 다른 복잡성과 정교함을 발휘하는 위협 기법이 두드러집니다. 기업은 웹 애플리케이션을 표적으로 삼는 공격의 급격한 증가에 직면하고 있습니다. Akamai는 2024년 한 해 동안 3110억 건 이상의 웹 애플리케이션 및 API 공격을 관찰했으며, 이는 전년 대비 33% 증가한 수치입니다. 이러한 공격 급증 현상은 클라우드 서비스, 마이크로서비스 아키텍처, AI(Artificial Intelligence) 기반 애플리케이션이 더욱 빠른 속도로 도입되는 상황과 직접적인 관련이 있습니다. 지정학적 [요인](#)으로 상황이 더욱 심각해졌으며, 첨단 기술, 커머스, 소셜 미디어 업계가 가장 큰 규모의 레이어 7(애플리케이션 레이어) DDoS(Distributed Denial-of-Service) 공격을 겪고 있습니다. 특히, 공격자는 이제 AI로 생성된 킷 체인을 [배포](#)해 공격 라이프사이클 전체를 자동화하고 있습니다.

동시에 API는 주요 표적으로 부상했으며, Akamai는 2023년 1월부터 2024년 12월까지 1500억 건 이상의 API 공격을 기록했습니다. AI 기반 SaaS(Software as a Service) 툴이 API를 통해 핵심 플랫폼과 통합되면서 공격 표면이 크게 확대되었습니다. 재정적 [영향](#)이 심각합니다. API 보안 문제는 현재 기업에 연간 약 US\$870억의 비용을 초래하고 있으며, 적절한 대응이 없을 경우 비용이 US\$1000억을 초과할 것으로 예상됩니다. 새도 및 좀비 API는 점점 복잡해지는 API 생태계 내에서 특히 취약한 공격 기법으로 작용하고 있습니다.

## 웹 애플리케이션 및 API 보안에서 AI의 역할

AI는 위협 탐지 및 대응 능력을 강화함으로써 웹 애플리케이션 및 API 보안 환경을 혁신하고 있지만 동시에 새로운 도전 과제도 제기하고 있습니다. 웹 애플리케이션에서는 AI가 위협 탐지를 자동화하고, 잠재적 유출을 예측하고, 인시던트 대응 시간을 단축하는 데 **사용**됩니다. 그러나 AI는 공격자가 AI 기반 멀웨어를 생성하고, 고급 웹 스크레이핑을 수행하고, 동적 공격 방법을 활용해 공격 라이프사이클을 자동화하는 데도 **활용**됩니다.

API의 경우, AI는 방대한 양의 API 상호작용을 관리하고 보호하는 데 핵심적인 **역할**을 합니다. AI 기반 툴은 비정상 탐지, 악용 패턴 식별, 실시간 위협 대응 자동화에 필수적입니다. AI 기반 API 관리는 예측 애널리틱스와 자동화된 보안 조치를 통합해 점점 더 정교해지는 공격으로부터 보호하기 위해 계속 **발전**할 것입니다. 이러한 발전에도 불구하고, 크리덴셜 스티핑 및 비즈니스 로직 취약점 악용과 같은 AI 기반 API **공격**은 여전히 심각한 위협으로 남아 있으며 이러한 위협에 효과적으로 대응하기 위해 강력한 보안 프레임워크가 필요합니다.

## 다르지만 서로 연결된 웹 애플리케이션 및 API 공격 전략

웹 애플리케이션 공격과 API 공격은 관련이 있지만 애플리케이션 인프라의 서로 다른 측면을 표적으로 삼습니다.



**웹 애플리케이션 공격**은 웹 애플리케이션의 공개 로그인 페이지 같은 사용자 인터페이스 구성요소를 표적으로 삼으며 일반적으로 덜 복잡한 기술을 사용합니다.



**API 공격**은 애플리케이션의 API 엔드포인트와 백엔드 로직의 취약점을 악용하며 API의 구조와 동작에 대한 깊은 이해가 필요합니다.

주요 차이점은 공격 표면과 복잡성에 있습니다. 웹 애플리케이션 공격은 일반적으로 애플리케이션의 가시적인 부분을 표적으로 삼는 반면, API 공격은 서로 다른 소프트웨어 구성요소 간의 통신 채널을 악용합니다. 그러나 성공 시 모두 민감한 데이터와 시스템 리소스에 무단 접속을 허용할 수 있습니다.

현대 애플리케이션이 기능 구축을 위한 API 의존도가 점점 더 커지고 있기 때문에 웹 애플리케이션과 API 공격에 대한 사이버 보안 조치를 동시에 이해해야 합니다. 기업은 2년 내에 웹 애플리케이션이 39% **증가**할 것으로 예상하고 있으며 이로 인해 웹과 API 보안의 상호 의존성이 더욱 강조되고 있습니다. 두 측면 중 하나를 소홀히 하면 기업은 애플리케이션의 프론트엔드와 백엔드에서 **취약점**을 악용하는 복잡한 멀티 기법 공격에 노출될 수 있습니다.

## Akamai의 독특한 관점: 위협 패턴 공개

Akamai의 복잡성 분석은 전 세계 웹 트래픽의 1/3 이상을 처리하는 네트워크 인프라를 통해 위협 패턴에 대한 최고의 가시성을 제공합니다. Akamai는 이러한 관점을 리서치 및 데이터 과학 팀의 인사이트와 결합해 포괄적이고 실행 가능한 인텔리전스를 제공할 수 있습니다. 이를 바탕으로 보안 리더들이 보안 투자 수익을 극대화하기 위해 리스크 감소에 집중해야 할 부문을 결정하는 데 필요한 전략적 인사이트를 제공합니다.



## 보고서의 핵심 인사이트

### AI 기반 API가 그렇지 않은 API보다 보안에 더 취약합니다.

대부분의 AI(인공지능) 기반 API는 외부에서 접속할 수 있으며, 불충분한 인증 메커니즘에 의존하는 경우가 많습니다. 이러한 취약점은 해당 API를 노리는 AI 기반 공격 유형이 점점 다양해지고 있는 상황에서 더욱 심각해지고 있습니다.

### AI가 공격자의 기술적 진보를 촉진합니다.

이에는 AI 기반 멀웨어, 취약점 스캔, AI 통합 시스템 공격, 고도화된 웹 스크레이핑 기능 등이 포함됩니다.

# 32%

#### OWASP API 보안 상위 10대 리스크 관련 인시던트의 증가율

API 보안 인시던트가 증가하고 있으며 OWASP(Open Worldwide Application Security Project) API 보안 상위 10대 문제에서 인증 및 권한 확인 취약점이 민감한 데이터와 기능을 노출시키는 것으로 드러났습니다.

# 30%

#### MITRE 보안 프레임워크 관련 보안 알림 증가율

공격자는 자동화 및 AI를 포함한 고급 기술을 활용해 API를 악용하고 있습니다. MITRE 프레임워크는 보안팀이 이러한 공격을 더 빠르게 정확히 식별하는 데 도움을 줄 수 있습니다.

# 33%

#### 전 세계 웹 공격의 연간 증가율

공격 급증은 클라우드 서비스, 마이크로서비스, AI 애플리케이션의 빠른 도입과 직접적으로 연관되어 있으며 이에 따라 공격 표면이 확장되고 새로운 보안 과제가 등장하고 있습니다.

# 2300억 이상

#### 커머스 기업을 표적으로 한 웹 공격 건수

영향을 가장 많이 받은 커머스는 첨단 기술(두 번째로 많은 공격을 받은 업계)의 약 3배에 달하는 공격을 받고 있습니다.

## 73%

아시아-태평양 및 일본(APJ)  
지역에서 연간 웹 공격 건수가  
2023년 290억 건에서 2024년 510억  
건으로 증가했습니다.

## 37%

유럽, 중동, 아프리카(EMEA)  
지역에서 발생한 웹 공격 중 API를  
표적으로 삼은 공격의 비율로,  
모든 지역 중 가장 높은 집중도를  
기록했습니다.

## 94%

분기별 Layer 7 DDoS(Distributed  
Denial-of-Service) 공격 증가율  
2023년 1분기부터 2024년 4분기까지.

## 11조 9000억

북미 지역을 표적으로 삼은 레이어  
7 DDoS 공격의 건수  
2023년 1분기부터 2024년 4분기까지  
2년간.

## 7조

가장 많이 영향을 받은 첨단 기술 업계를 표적으로 한 레이어 7 DDoS 공격 건수  
2023년 1월부터 2024년 12월까지

## 7조 4000억

APJ 지역을 표적으로 한 레이어  
7 DDoS 공격 건수  
2023년 1분기부터 2024년 4분기까지  
2년간.

## 20%

EMEA 지역을 표적으로 한 레이어  
7 DDoS API 관련 공격의 비율로  
모든 지역 중 가장 높은 집중도를  
보였습니다.

## API 위협 인텔리전스의 진화

Akamai는 Nomenclature Security와의 통합을 통해 API 위협 연구 및 보고 능력을 크게 강화했으며 API 특화 리스크에 대한 새로운 관점을 제공합니다. Akamai는 이 새로운 데이터 세트(데이터 통합 초기 단계에 있음)을 활용해 기존 위협 인텔리전스를 강화하고 API 보안 문제에 대한 확장된 관점을 제공합니다.

### 알림을 보안 프레임워크에 매핑

시간이 지나면서 새로운 데이터 세트가 다음과 같은 중요한 사이버 보안 프레임워크 및 컴플라이언스 기준과 연결됨에 따라 보안 알림 세부 정보를 더 깊이 분석할 수 있게 됩니다.

- MITRE ATT&CK(Adversarial Tactics, Techniques, and Common Knowledge)
- GDPR(General Data Protection Regulation)
- PCI DSS(Payment Card Industry Data Security Standard)
- ISO(International Organization for Standardization)
- OWASP(Open Worldwide Application Security Project)

이러한 개선 사항은 Akamai가 클라이언트에 강력한 보호를 제공하는 능력을 크게 강화합니다. 이러한 프레임워크에 따라 기업은 보안 체계를 더 명확히 이해하고, 규제 요건을 충족하고, 보안 노력을 효과적으로 우선시할 수 있습니다. 기업은 이러한 포괄적인 접근 방식으로 리소스를 전략적으로 배분하고 API 및 민감한 데이터를 보호하기 위한 맞춤형 전략을 개발할 수 있습니다.

### 30일 데이터 샘플 분석

이 보고서에서는 각 사이버 보안 프레임워크 및 컴플라이언스 기준에서 공격자의 일반적인 활동을 강조하기 위해 30일 데이터 샘플을 분석했습니다(그림 1). MITRE 및 OWASP 알림에 대한 더 깊은 분석도 제공합니다. 또한 리스크 및 보안 인시던트가 컴플라이언스 기준에 미치는 영향도 살펴봅니다.

|         | 30일 활동 건수 | 월별 증가 |
|---------|-----------|-------|
| OWASP   | 5,907,000 | 32%   |
| MITRE   | 2,817,000 | 30%   |
| ISO     | 832,000   | 22%   |
| GDPR    | 669,000   | 21%   |
| PCI DSS | 881,000   | 16%   |

그림 1: 보안 프레임워크 및 컴플라이언스 기준별 보안 알림 분석



## MITRE 알림

30일 동안 고객사에서 MITRE 기술과 관련된 인시던트가 30% 증가했습니다. 특히 공격자는 T1078(유효한 계정)을 자주 활용해 정상적인 인증정보를 이용하고 시스템이나 네트워크에 무단 접속했습니다. API가 권한 확인에 토큰을 자주 사용하기 때문에 공격자는 이러한 토큰을 획득하면 탐지 없이 민감한 데이터에 접근할 수 있습니다.

또한 T1566(피싱)을 통해 공격자가 API 토큰이나 인증정보를 훔쳐 향후 공격에 활용하기 위해 피싱 캠페인을 전개한 사례도 확인되었습니다. API가 공격 표면을 확장함에 따라 이를 공격자가 침투 수단으로 악용하는 경우가 증가하고 있습니다. T1190(공개 애플리케이션 취약점 악용)과 관련된 알림에서는 공격자가 애플리케이션 취약점을 악용해 네트워크에 침투한 사례가 드러났습니다. 이외에도 T1580(클라우드 인프라 탐색)에서는 공격자가 API 호출을 통해 노출된 클라우드 엔드포인트를 탐색해 정찰 활동을 수행했습니다.

MITRE는 전용 API 보안 매트릭스를 제공하지 않지만 그 프레임워크는 API를 표적으로 삼는 공격자의 기술에 대한 인사이트를 원하는 보안팀과 기업에 여전히 필수적입니다. 보안팀은 공격자의 기법을 API 특정 행동에 매핑함으로써 공격 단계와 관련된 전술, 기술, 절차를 식별해 인시던트 대응 및 위협 탐지 능력을 강화할 수 있습니다. 보안팀은 이러한 접근 방식을 통해 리스크를 더 효과적으로 방어할 수 있습니다.

## OWASP 알림

OWASP API 보안 상위 10대 리스크는 취약점의 영향력과 심각성에 대한 유용한 정보를 제공하는 중요한 리소스입니다. 개발자와 보안팀이 빠르게 변화하는 위협 환경에서 정보를 최신 상태로 유지하며 이니셔티브를 효과적으로 우선시할 수 있도록 지원합니다.

30일 샘플 기간 동안 분석 결과 OWASP 관련 인시던트가 32% 증가했습니다. 특히, BOPLA(Broken Object Property Level Authorization), 손상된 기능 수준의 권한 확인, 손상된 권한 확인과 같은 취약점은 민감한 데이터나 핵심 기능을 공격자에게 직접 노출시킵니다. 부족한 권한 확인 메커니즘은 공격자가 이용해 권한을 상승시키고, 계정을 탈취하고, 기밀 정보에 접속할 수 있으므로 API를 표적으로 삼는 가장 위험한 공격 기법 중 하나입니다.

BOLA(Broken Object Level Authorization)는 여전히 중요한 API 보안 취약점이지만 비즈니스 로직 취약점에 의존하기 때문에 탐지가 어렵습니다. 따라서 보고가 부족하거나 탐지율이 낮은 경우가 많습니다. 이를 해결하기 위해 기업은 사용자와 그들이 일반적으로 접속하는 리소스 간의 명확한 관계를 수립하는 API 보안 솔루션을 도입해야 합니다. 이를 위해 고급 머신 러닝 알고리즘을 통해 비정상 접속 패턴을 인식할 수 있는 행동 기준선을 설정하는 것이 필요합니다.

BOPLA는 보안 테스트 시 자주 간과되는 API의 정밀 필드 수준 접속 문제를 악용합니다. BOLA와 달리 BOPLA 공격은 전체 오브젝트 ID를 변경하는 대신 오브젝트 내 특정 속성을 표적으로 삼습니다. 예를 들어, 응답에 민감한 PII(Personally Identifiable Information)를 노출하는 DELETE API 호출은 BOPLA 취약점을 구성합니다. 이 미묘함으로 인해 BOPLA 문제는 BOLA 공격보다 더 빈번하게 발생합니다.

실제로 이메일 주소만 사용한 구독 취소 요청에서 API 응답에 사용자의 전체 이름과 주소가 우연히 포함된 사례가 있습니다. 민감한 데이터가 무권한 당사자에게 노출되는 이유는 보안 테스트가 일반적으로 전체 오브젝트에 초점을 맞추고 개별 속성을 검사하지 않기 때문입니다. 이 같은 소홀함으로 인해 API 보안 평가에서 BOPLA 취약점의 탐지율이 증가합니다.

또 다른 중요한 취약점은 무제한 리소스 사용으로, 공격자가 리소스 고갈이나 DDoS 유사 공격을 악용하여 서비스 중단을 유발할 수 있습니다. 이 취약점은 서비스 영향을 넘어 클라우드 리소스 과다 사용으로 인한 운영 비용 증가와 무차별 대입 공격 리스크 증가 등 추가적인 리스크를 초래합니다. 적절한 속도 제한이 없으면 공격자가 API를 빠르게 탐색해 보안 감염을 유발할 수 있습니다. 또한 이러한 공격은 대규모 트래픽을 생성해 기업의 비용 증가로 이어집니다.

써드파티 API 통합 시 데이터 검증, 필터링 부족 및 보안 메커니즘 부재로 인한 API의 안전하지 않은 사용은 또 다른 주요 위협 기법입니다. 기업이 디지털 전환을 위해 써드파티 API에 더 많이 의존함에 따라 이 문제에 대한 우려가 더 커지고 있습니다. [최근 연구](#)에 따르면 조사 대상 기업의 80% 이상이 써드파티 API 관련 문제를 겪음으로써 제로 트러스트 보안 모델 도입의 중요성이 강조됐습니다. 이 취약점만으로 즉시 치명적인 결과가 초래되지 않을 수 있지만 검증 부족이나 보안이 취약한 의존성 등과 같은 다른 약점과 결합될 경우 심각한 보안 위협으로 발전할 수 있습니다. 예를 들어, 금융 API가 검증되지 않은 써드파티 거래를 신뢰할 경우 보안 유출로 이어질 수 있습니다.



PCI DSS 및 GDPR과  
관련된 보안 알림은 각각  
16%와 21% 증가했으며  
ISO 27001 관련 알림은  
22% 증가했습니다.

## API 컴플라이언스 보장

API 컴플라이언스 보장을 위한 최선의 방법은 각 알림에 위반된 특정 컴플라이언스 및 규제 기준을 태그하는 것입니다. 이를 통해 기업은 중요한 컴플라이언스 문제에 대한 인사이트를 즉시 확보하고 문제 해결을 위한 실행 가능한 가이드를 마련할 수 있습니다. 이 사전 예방적 접근 방식은 기업의 규제 컴플라이언스 유지에 기여해 규제 벌금, 법적 제재, 평판 손상 등 심각한 재정적 손실을 초래할 수 있는 리스크를 줄이는 데 도움이 됩니다. 일례로 API 취약점으로 인해 40만 명의 고객 데이터가 노출된 [한 항공사에 2000만 파운드의 벌금이 부과되며](#), GDPR 하에서 API 보안이 부적절한 경우 심각한 결과가 초래될 수 있다는 것이 강조됐습니다.

컴플라이언스 기준은 기업이 민감한 데이터를 보호하고, 고객을 안전하게 지키고, 법적 및 규제 의무를 충족하는 데 필수적인 가이드라인입니다. PCI DSS, GDPR, HIPAA(Health Insurance Portability and Accountability Act) 같은 표준에 따라 결제 데이터와 PII(Personally Identifiable Information) 같은 민감한 정보를 안전하게 처리해야 합니다. Akamai의 데이터 분석에 따르면 PCI DSS 및 GDPR과 관련된 보안 알림은 각각 16%와 21% 증가했으며 ISO 27001과 관련된 알림은 22% 증가했습니다.

### GDPR

GDPR은 API 라이프사이클 전반에 걸쳐 데이터 보호와 고객 개인정보를 통합하는 데 주력합니다. 여기에는 안전한 설계, 강력한 인증 및 권한 확인, 속도 제한, 정기적인 취약점 테스트, 암호화, 초기 개발 단계부터 지속적인 리스크 평가가 포함됩니다. 이러한 조치들은 데이터의 기밀성, 무결성, 가용성을 보장합니다.

### PCI DSS

마찬가지로 [PCI DSS](#)는 결제 카드 데이터를 처리하는 API의 보안을 강화하기 위해 설계, 코딩, 테스트 단계에 보안을 통합하도록 요구합니다. 웹 취약점으로부터의 보호 및 보안 취약점을 식별하고 해결하기 위한 정기적인 테스트를 의무화합니다.

요구사항 10 및 11은 API 활동(요청, 응답, 인증 시도, 시스템 변경 등)에 대한 포괄적인 로그 기록 및 모니터링을 구체적으로 요구합니다. 로그는 최소 12개월 동안 보관되어야 하며 최근 3개월 분은 분석을 위해 즉시 접근 가능해야 합니다. 또한 기업에 주요 변경 사항 후 외부 취약점 스캔을 수행할 것을 권장합니다. PCI 컴플라이언스를 위해 기업은 API가 위협과 리스크에 대한 안정성을 갖도록 속도 제한, 로그 기록, RBAC(Role-Based Access Control), 세션 관리 등의 엄격한 통제 조치를 구축해야 합니다.



## ISO 27001

ISO 27001 표준은 정보 보안 리스크를 효과적으로 관리하고, 기업의 보안 체계를 강화하고, 동종 업체 및 고객 간의 신뢰를 구축하는 데 탄탄한 프레임워크를 제공합니다. 다음과 같은 사항을 권장합니다.

- 사용자 ID를 확인하기 위한 접속 제어(예: API 키) 구축
- 엔드투엔드 데이터 암호화 적용
- API의 비정상 행동 모니터링
- 잠재적 API 취약점을 식별하기 위한 철저한 리스크 평가 실시

이러한 컴플라이언스 요구사항은 API 보안과 규제 프레임워크 간의 중요한 교차점을 강조합니다. 적절한 구축은 민감한 데이터를 보호할 뿐만 아니라 여러 컴플라이언스 요구사항을 동시에 충족합니다. 기존 및 신규 글로벌 표준에 대한 자세한 내용은 보고서의 [컴플라이언스](#) 섹션을 참고하세요.

## API 가시성 격차: 숨겨진 데이터 통로

### API 악용

2024년 11월, [Bleeping Computer](#)는 전자 서명 솔루션 공급업체를 대상으로 한 대규모 공격을 보도했습니다. 공격자는 해당 공급업체의 문서 관리 및 추적 API의 핵심 구성요소를 악용해 다수의 잠재적 피해자에게 위조된 청구서를 전송할 수 있었습니다. 수신자가 문서에 무심코 서명하면 공격자는 다양한 기업에 결제를 요청할 수 있었습니다.

이 인시던트에서 API 악용의 악영향이 부각됐습니다. 즉 공격자는 API를 원래 설계 목적을 벗어난 목적으로 악용해 공격 경로로 활용할 수 있습니다. 생성형 AI의 등장으로 리스크가 더욱 악화되었습니다. 생성형 AI는 취약점 발견과 속도 제한 우회 과정을 자동화해 더 빠르고 정교한 공격을 촉진합니다.

출처: bleepingcomputer/Wallarm

### Please Review & Act on These Documents

 **Elaina harrs**  
Symantec

Norton  
Receipts & Invoice  
[View More](#)

**Norton**  
Internet Security

Powered by  docusign

Please review the documents below.

CONTINUE

OTHER ACTIONS ▾

 Signature

 Initial

 Stamp

 Date Signed

 Name

 First Name

 Last Name

 Email Address

 Company

 Title

- Comprehensive protection against viruses and malware
- Identity theft protection
- Performance optimization tools
- 24/7 customer support

#### DETAILS:

| PRODUCT             | TENURE             | AMOUNT            |
|---------------------|--------------------|-------------------|
| Norton LifeLock 360 | 2 Users/1 Year     | 249.00 USD        |
|                     | Activation Charges | 49.00 USD         |
| <b>TOTAL</b>        |                    | <b>298.00 USD</b> |

#### POLICY:

We understand that circumstances can change and you may need to cancel your subscription. We



## API 악용 탐지의 과제

보안팀은 정상적인 행동과 의심스러운 행동을 구분하기 위한 기준을 수립해야 한다는 점에서 API 악용 탐지에 상당한 장애물을 직면하고 있습니다. 이 과제는 비정상과 위협을 사전에 식별하기 위한 실시간 행동 모니터링의 중요성을 강조합니다.

Akamai의 [2024년 API 보안 영향 연구](#)에서 우려스러운 트렌드가 드러났습니다. 조사 대상 기업 중 API를 매일 테스트하는 곳은 13%에 불과하며 2023년의 37%에서 크게 감소했습니다. 이 감소는 현재의 위협 환경을 고려할 때 특히 우려스럽습니다. 일일 API 테스트가 급격히 감소하면 기업이 보안 리스크에 노출될 가능성이 커집니다. 빠르게 진화하는 위협을 탐지하고 대응하는 능력이 크게 저하되어 중요한 취약점이 장기간 방치될 수 있기 때문입니다.

기업은 개발 사이클 동안 자동화 테스트를 자주 수행하면 문제를 조기에 식별하고 해결해 프로덕션 환경에서 비용이 많이 드는 복구 작업을 방지할 수 있습니다. API 악용이 자동화되고 은밀한 방법을 점점 더 많이 활용하는 시대에, 사전 예방적 테스트는 리스크 방어에서 핵심적인 역할을 합니다.

## 관리되지 않은 API: 좀비 및 새도 API

API 자산 가시성은 공식 API 추적과 민감한 데이터 식별을 아우르는 기업의 핵심 과제입니다. [2024년 API 보안 영향 연구](#)에서 심각한 격차가 드러났습니다. AppSec팀의 47%가 전체 API 인벤토리를 유지하고 있지만 민감한 데이터를 처리하는 API를 식별하지 못했습니다. 수석 보안 전문가들도 유사한 한계를 보고했으며 42%가 같은 문제를 겪고 있습니다. 우려스럽게도, 완전한 API 인벤토리를 관리하고 민감한 데이터 노출을 인지한 기업의 비율이 2023년 40%에서 2024년 27%로 감소했습니다. 보안 영향 연구에서는 좀비 및 새도 API를 API 보안 인시던트의 주요 원인 중 하나로 강조합니다.

좀비 및 새도 API가 누락되는 주요 원인은 불완전한 인벤토리입니다. 좀비 API(즉, 불완전한 폐지, 직원 교체 또는 기타 이유로 인해 활성화된 채로 남아 있는 구형 인터페이스)는 취약한 공격 기법을 생성합니다. 새도 API(표준 승인 프로세스를 벗어나 신속한 해결책으로 개발된 API)는 유사한 위협을 초래합니다. [리서치 결과](#), 악성API 거래의 1/3이 새도 API를 표적으로 삼는 것으로 나타났습니다.

WAF(Web Application Firewall)와 같은 전통적인 보안 조치는 이러한 위협에 대해 효과적이지 않습니다. 기업은 취약한 엔드포인트를 효과적으로 식별하기 위해 고급 API 탐색 및 모니터링 솔루션이 필요합니다.

포괄적인 API 인벤토리는 효과적인 보안 전략의 기반이 되며, 기업이 사용 패턴을 모니터링하고, 버전 이력을 추적하고, 취약점을 식별하고, 컴플라이언스 및 규제 요구사항을 충족하는 데 도움을 줍니다. 기업은 이러한 전략적 접근 방식으로 디지털 인프라에 대한 명확한 가시성을 확보해, 궁극적으로 리스크 관리를 강화하고 전체 보안 체계를 강화할 수 있습니다.

## 보안 스포트라이트

2025년 1분기에, API를 악용해 이커머스 기업을 공격한 사례가 발견되었습니다. 해당 기업의 SMS 전송 API는 적절한 인증이 부족했으며 공격자는 200개 이상의 서로 다른 IP 주소, 단일 인증 토큰, 수많은 무작위 휴대전화 번호(정상 및 가짜 모두)를 사용해 취약점을 악용했습니다.

공격 전략은 단순하지만 효과적이었습니다. 다수의 휴대전화 번호를 등록하고 사기 번호로 SMS 메시지를 전송해 기업을 마비시킴으로써 직접적인 재정 손실을 입혔습니다. 공격자가 휴대전화 번호를 등록할 때마다, 해당 기업은 애플리케이션과 모바일 디바이스 간 텍스트 메시지를 위해 SMS 게이트웨이 서비스 이용 비용을 부담하게 되어 예상치 못한 재정적 손실이 발생했으며 이는 브랜드나 명성에 손상을 입힐 수 있었습니다. 다중 보안 레이어를 갖춘 방어 전략은 이러한 종류의 공격을 차단하고 관련된 리스크를 크게 줄일 수 있습니다.

Akamai의 알림에 따르면 공격자는 공격 중에 1만1057개의 POST 요청을 발송했으며 이 중 5659개가 성공적으로 응답을 받았습니다(그림 2).

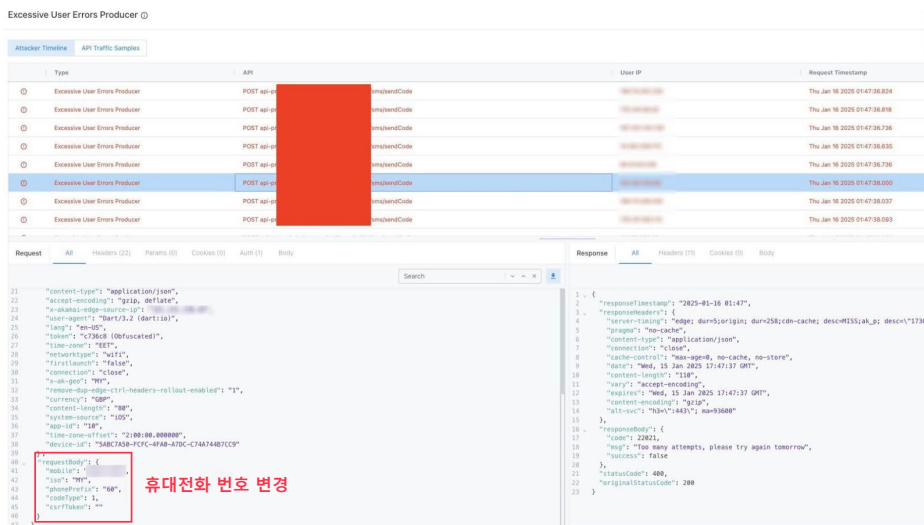


그림 2: 공격자가 보안이 취약한 API에 요청을 대량으로 전송합니다

자동화된 요청은 한 가지 중요한 매개변수를 제외하고 동일했습니다.

Body param **mobile**: 다음 패턴이 탐지됨 - <number>

이러한 요청은 서버 과부하로 서비스 거부를 유발하거나 API에 대한 무단 접속이 성공했음을 나타낼 수 있습니다. 기존 WAF는 이러한 고도화된 공격을 탐지할 수 없습니다. 그러나 정상적인 API 행동의 기준선을 설정하는 고급 API 보안 솔루션은 행동 분석을 통해 이러한 공격을 탐지하고, 리스크를 사전 예방적으로 방어하고, 공격자가 피해를 확대하는 것을 방지할 수 있습니다.

## 웹 공격: 연도별 비교 및 트렌드

Akamai의 리서치 결과, 2023년 1월부터 2024년 12월까지 보고 기간 동안 웹 애플리케이션 및 API를 대상으로 한 웹 공격이 크게 증가했습니다(그림 3). 월별 공격량은 2023년 초 약 140억 건에서 2024년 10월에는 290억 건을 넘어섰습니다. 즉, 2023년 1분기부터 2024년 4분기까지 웹 공격이 65% 증가했습니다.

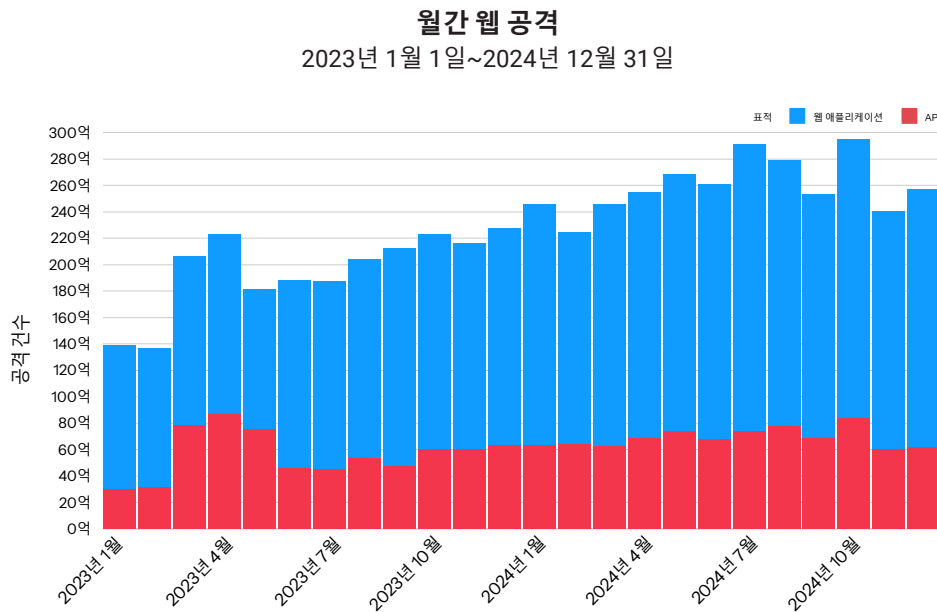


그림 3: 웹 애플리케이션과 API를 표적으로 삼은 기존 웹 공격은 2023년 1분기부터 2024년 4분기까지 65% 증가하며 계속 증가하는 트렌드를 보이고 있습니다

## 주요 기법: 기존 및 최신 행동 기반 리스크의 결합

사이버 보안 전문가는 기존 웹 공격부터 내재된 취약점과 설정 오류를 노리는 최신 공격까지 다양한 위협으로부터 기업의 디지털 인프라를 보호하는 과정에서 급증하는 복잡성을 직면하고 있습니다.

## API 요청 제약 조건 위반: 증가하는 위협

2년간의 포괄적인 API 엔드포인트 분석 결과, API 요청 제약 조건 위반이 기업의 주요 우려 사항으로 부상했습니다(그림 4). 이러한 위반은 요청이나 응답이 사전 정의된 매개변수를 따르지 않거나 속도 제한 초과 또는 유효하지 않은 데이터 입력 제출 등을 비롯한 요구사항을 준수하지 않을 때 발생합니다.

**기법별 API 공격**  
2023년 1월 1일~2024년 12월 31일

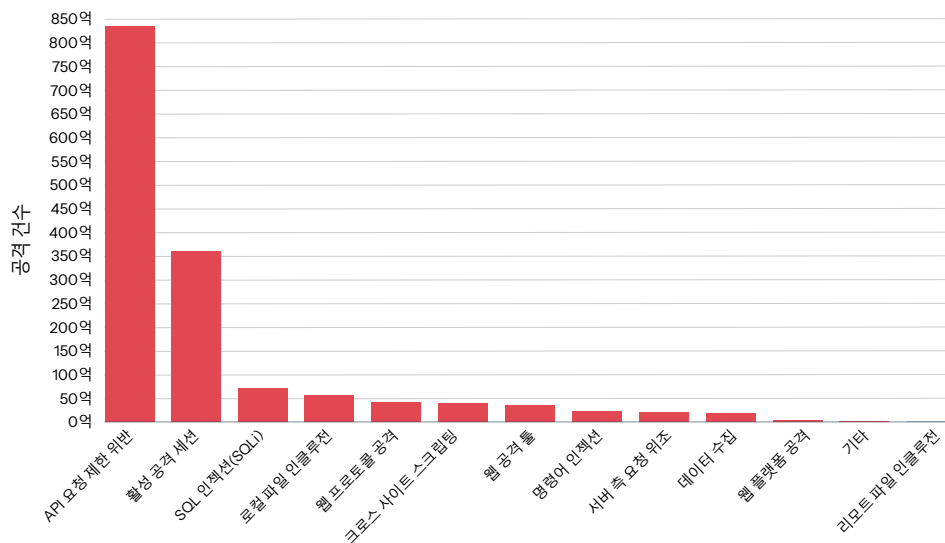


그림 4: 2년간 830억 건 이상의 요청 제약 조건 위반이 기록되었습니다

API 요청 제약 조건 위반은 2년간 830억 건 이상의 공격이 기록되며 점차 증가하고 있습니다. 이 공격 기법이 2023년부터 2024년까지 24% 급증함에 따라 API 악용의 위험성이 부각됐습니다. 이러한 위반의 확산은 잠재적 API 악용을 나타내는 중요한 지표로, 시스템 성능 저하, 서비스 중단, 표적 공격에 대한 취약점 증가 등 부정적인 영향을 연쇄적으로 초래할 수 있습니다.

## 활성 공격 세션: 창의적인 해결책이 필요한 고유한 공격

Akamai의 솔루션은 API 특유의 공격이 제기하는 독특한 도전 과제를 극복하기 위해 혁신적인 보안 툴을 활용합니다. 솔루션의 핵심에는 활성 공격 세션을 탐지하는 독점적 메커니즘이 있으며 전략적 방어 툴의 역할을 합니다. 시스템이 Akamai의 자체 위협 인텔리전스를 활용해 의심스러운 행동을 식별하고 추적하므로 기업은 위협이 대규모 공격으로 발전하기 전에 사전 차단할 수 있습니다.

시스템은 공격자를 표시하고 “페널티 박스” 접근 방식을 적용합니다. 최신 공격에서 공격자는 주로 자동화를 활용해 정찰과 공격을 실행합니다. Akamai는 클라이언트를 일시적으로 차단하고 활성 공격 세션으로 분류해 취약점 스캐닝 세션을 신속히 식별합니다. 이 전략은 잠재적 공격자가 정찰하거나 네트워크 취약점을 악용하는 것을 효과적으로 억제합니다.

기업은 공격자의 공격 기회를 제한함으로써 API 보안 체계를 크게 강화할 수 있습니다. 이 접근 방식은 다양한 잠재적 공격에 대한 강력한 보호를 제공하며 전체 사이버 보안 안정성을 크게 향상시킵니다.

이 전략의 중요성은 Akamai 데이터에서 명확히 드러납니다. 활성 공격 세션은 웹 애플리케이션과 API 모두에서 전체 1위를 차지했습니다(그림 5). 2023년에는 690억 건 이상의 공격이 활성 공격 세션이었습니다. 이 수치는 2024년에 1130억 건 이상으로 급증했으며 전년 대비 63%라는 놀라운 증가율을 기록했습니다.

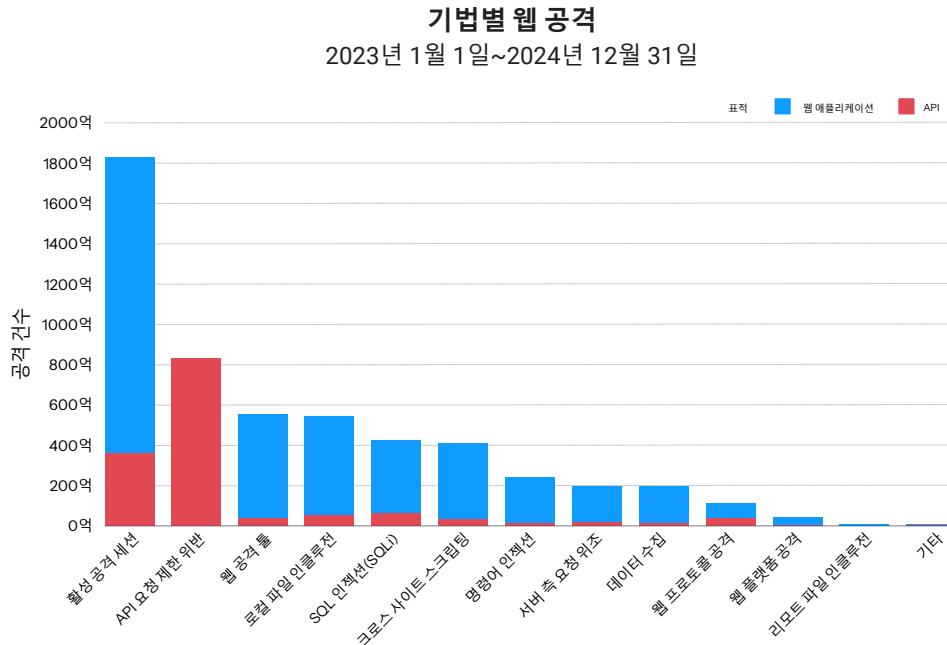


그림 5: 활성 공격 세션은 웹 애플리케이션과 API에서 다른 모든 기법을 압도하며 공격자가 목표 네트워크의 취약점을 지속적으로 노리고 있음을 강조합니다.



## 최신 인프라에서 기존 웹 취약점을 무시할 수 없는 이유

인젝션 공격은 고급 행동 기반 공격 방법론의 등장과 기존 웹 취약점에 대한 인식 향상에도 불구하고 여전히 높은 효과를 보여주고 있습니다. 2023년 1월부터 2024년 12월까지 데이터에 따르면 공격량이 급증했으며 SQLi(Structured Query Language injection)와 명령어 인젝션이 각각 전년 대비 60%, 34% 증가했습니다. 이러한 취약점을 통해 악성 공격자가 무단 명령을 실행하고, 시스템 무결성을 감염시키고, 적절한 인증 없이 민감한 데이터에 접속할 수 있으므로 사이버 보안 부문에서 꾸준히 주목을 받고 있습니다.

SQL 데이터베이스는 데이터 저장 부문에서 뛰어난 신뢰성과 확장성으로 꾸준히 유행함에 따라 지속적으로 표적이 되고 있습니다. 특히, **가장 널리 사용되는 4대 데이터베이스**가 SQL 기반 아키텍처를 도입하고 있어 이 공격 기법의 중요성이 더욱 강조되고 있습니다.

OWASP 상위 10대 API 보안 취약점 목록은 2023년 업데이트에서 인젝션 공격을 보안 설정 오류로 대체하는 등 개편을 거쳤지만 인젝션 공격과 관련된 리스크는 여전히 가장 중요합니다. 동시에 LFI(Local File Inclusion)와 XSS(Cross-Site Scripting) 같은 다른 확립된 공격 기법도 높은 빈도로 발생하고 있습니다. Akamai의 **2025년 보안팀 가이드**는 2024년에 관찰된 실제 공격 사례를 기반으로 원격 리소스 인젝션, 쿠키 도용, 웹사이트 훼손, 세션 탈취를 비롯한 XSS 공격 기술의 고도화를 설명합니다.

가이드는 멀티레이어 방어 전략의 구축이 필수적임을 강조합니다. 사이버 보안 전문가는 적절한 출력 인코딩, 강력한 콘텐츠 보안 정책, 고급 WAF를 결합해 점점 더 정교해지는 공격을 효과적으로 방어해야 합니다.

## 레이어 7 DDoS 공격: 연도별 비교 및 트렌드

2023년 1월부터 2024년 12월까지 Akamai 리서치는 웹 애플리케이션 및 API를 대상으로 한 레이어 7(애플리케이션 레이어) DDoS 공격이 급격히 증가한 기록을 문서화했습니다(그림 6). 2023년 초 5000억 건을 약간 넘는 수준이었던 월별 공격량은 2024년 12월에 1조 1000억 건을 넘어섰습니다. 즉 2023년 1분기부터 2024년 4분기까지 레이어 7 DDoS 공격이 94% 증가했습니다.

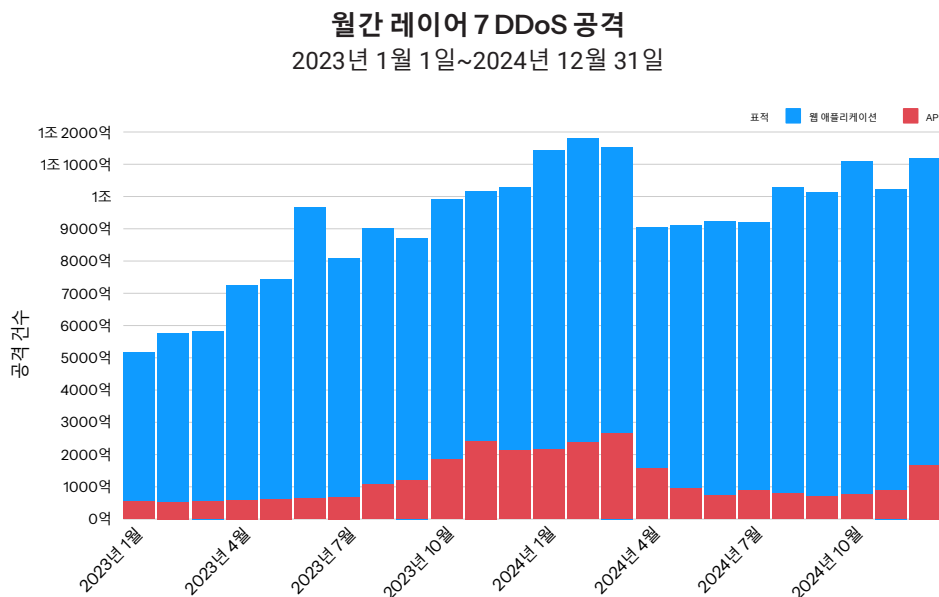


그림 6: 웹 애플리케이션 및 API를 대상으로 한 레이어 7 DDoS 공격은 2023년 1분기부터 2024년 4분기까지 94% 증가했습니다.

### 애플리케이션 및 API를 노리는 레이어 7 DDoS 공격

**HTTP 플러드**는 웹 애플리케이션 및 API 엔드포인트를 대상으로 한 레이어 7 DDoS 공격의 지속적인 진화 과정에서 여전히 주요 위협 기법으로 사용되고 있습니다. 이 공격은 리소스 소모가 높은 작업에 초점을 맞춘 대규모의 정상적인 요청으로 API 리소스에 과부하와 마비를 유발합니다. 공격자는 웹 애플리케이션 로직이나 API의 특정 취약점을 악용하기 위해 레이어 7 DDoS 공격 기술을 정교화해 탐지 및 방어 노력을 복잡하게 만들고 있습니다. 또한, 봇 기반 공격은 정상적인 API 사용 패턴을 모방하는 트래픽 패턴을 생성하며 점점 더 정교해지고 있습니다.

## 공격자의 AI 전송: 수동 또는 자동을 통해 API 경로 주행

생성형 AI 기술은 API를 통해 비즈니스 통합을 혁신하며 API의 광범위한 도입과 실용적 적용을 “주도”하고 있습니다. AI API 시장은 연평균 32.2% 성장하며 2025년 444억 1400만 달러에서 2030년 1791억 4000만 달러로 **폭발적인 성장**을 기록할 것으로 예상됩니다. 그러나 AI 도입의 급증과 동시에 **AI 기반 API 공격도 급증**했습니다. 공격자가 수동이나 자동화된 방식으로 AI를 정찰 및 악용 톨로 활용함에 따라 노출된 API 취약점이 증가했습니다.

### AI 기반 API 공격 전략

-  **전략적 공략:** 공격자는 AI 톨을 활용해 대상 API의 특정 구성요소를 식별하고 분석한 후, **AI가 생성한 악성 코드**를 활용해 특정 취약점에 대해 맞춤형 공격을 설계합니다. 이러한 접근 방식으로 API 취약점을 정밀하고 효과적으로 공격할 수 있습니다.
-  **자동화 공격:** 사이버 범죄자는 공격 프로세스를 자동화함으로써 시간과 노력을 크게 줄이고 API 보안 취약점을 신속하게 식별하고 악용합니다. 자동화에는 기업과 개인을 심각히 위협하는 **AI 기반 봇**이 포함되는 경우가 많습니다.
-  **증폭 공격:** 공격자는 AI를 활용해 API를 트래픽으로 과부하시켜 보안 시스템을 대규모로 침투합니다. 이러한 전략의 대표적인 사례는 AI 기반 봇이 방어 조치를 동적으로 적용해 지속적으로 공격하는 **자동화된 DDoS 공격**입니다.
-  **행동 기반 공격:** AI는 트래픽 패턴을 분석하고 일반적인 알림 임계값 아래에서 작동해 탐지를 회피하는 **저속 및 저강도 공격**을 생성합니다. 이러한 공격은 BOLA 및 Broken Authentication과 같은 일반적인 API 취약점을 자주 표적으로 삼습니다.

### AI 기반 API의 아이러니

아이러니하게도 AI로 구동되는 API가 특히 취약한 것으로 드러났습니다. 대부분의 **AI 기반 API**는 외부에서 접속 가능하며 상당수는 부적절한 인증 메커니즘에 의존해 공격에 더 취약합니다. **2024년 API 보안 영향 연구**에 따르면, 리테일/이커머스 보안팀이 보고한 API 인시던트의 주요 원인은 생성형 AI 톨 내 API였습니다.

## 변화하는 AI 위협 환경

AI 기술의 발전은 API에 대한 위협 환경의 변화에 크게 기여했습니다. 지난 1년간 AI 기반 API 취약점의 **기록적인 증가**가 보고되었으며 미국 사이버 보안 및 인프라 보안국이 기록한 모든 **악용된 취약점** 중 처음으로 과반수가 API 관련 취약점이었습니다.

## AI 기반 웹 애플리케이션 공격 및 방어 전략

AI는 새로운 공격 기법과 방어 기능을 도입함으로써 웹 애플리케이션 보안에 깊은 영향을 미쳤습니다. AI가 웹 애플리케이션 공격의 사이버 보안 환경을 크게 변화시킨 주요 부문에는 AI 기반 멀웨어, AI 기반 취약점 스캔, AI 관련 시스템에 대한 공격, 고도화된 웹 스크레이핑, AI 기반 WAF 시스템 등이 포함됩니다.

### AI 기반 멀웨어

사이버 보안 전문가는 AI를 활용해 웹 애플리케이션을 공격하는 고급 멀웨어를 관찰했습니다. 2024년 프랑스 사용자를 표적으로 한 이메일 캠페인에서 공격자는 생성형 AI의 도움을 받아 설계된 것으로 추정되는 악성 코드를 배포해 **AsyncRAT 멀웨어**를 실행했습니다. 이 사례는 AI를 활용한 멀웨어의 제작 및 배포 트렌드가 증가하고 있음을 보여주며 웹 애플리케이션 보안 전문가에게 새로운 도전 과제를 제시합니다.

### AI 기반 취약점 스캔

AI는 웹 애플리케이션의 **취약점 스캔**을 혁신했으며 방어적 및 공격적 목적으로 모두 활용될 수 있습니다. 이러한 AI 기반 툴은 SQLi, XSS, 크로스사이트 요청 위조, SSRF(Server-Side Request Forgery)와 같은 일반적인 취약점을 자동으로 검색합니다. 또한 AI에 기반해 잠재적 영향을 분석하고 AI 기반 권장 사항을 생성해 대응 조치를 제안합니다.

### AI가 포함된 시스템에 대한 공격

AI, 특히 LLM(Large Language Model)의 웹 애플리케이션 통합은 **새로운 보안 취약점**을 도입했습니다. 프롬프트 인젝션 공격은 AI 시스템을 표적으로 삼아 AI 시스템의 모델 보호 조치를 우회합니다. 대표적인 사례로는 현재 패치됐지만 간접적인 프롬프트 인젝션을 통해 프라이빗 채널에서 데이터를 수집할 수 있었던 **Slack AI 취약점**이 있습니다. 데이터 포이즈닝 공격은 데이터셋의 작은 부분을 조작해 AI 모델의 행동을 왜곡하고 시스템 무결성을 감염시킬 수 있습니다. LLM의 안전 장치를 우회할 수 있는 제일브레이킹 기술을 사용하면 제한을 무력화하고, 민감한 데이터를 추출하고, 유해한 출력을 생성할 수 있습니다. 이러한 새로운 공격 기법은 강화된 경계와 혁신적인 방어 전략이 필요합니다.

## 정교한 웹 스크레이핑

AI로 웹 스크레이핑 기능이 향상됨에 따라 웹 애플리케이션 보안에 새로운 도전 과제가 제기되고 있습니다. AI 기반 스크레이핑 툴은 더 효율적인 데이터 추출 방법과 반스크레이핑 조치 회피 능력을 제공합니다. 2020년대 초반부터 **정교한 웹 스크레이핑**은 AI를 활용해 데이터를 처리해 왔으며 최근 LLM 스크레이핑의 빈도가 급격히 증가했습니다. 이 중 대부분은 에이전트 기반 크롤링의 확산으로 인해 실시간(비정적) 데이터 소스에 대한 수요가 증가했기 때문입니다.

불행히도 이로 인해 웹 애플리케이션 요청의 평균 비용(요청 복잡도, 호스팅 인프라 등 요인에 따라)이 요청당 US\$0.01에서 US\$0.50까지 다양해졌습니다. 초기에는 커머스 부문이 LLM 스크레이핑 증가로 가장 큰 영향을 받았지만 이제는 금융 서비스, 도박, 디지털 미디어, 비디오 미디어 등 다른 업계들이 변화의 직격탄을 맞고 있습니다.

## AI 기반 WAF 시스템

긍정적인 측면에서 보면, 고급 WAF 시스템은 AI를 통해 봇, DDoS 공격, 스크레이퍼, 스캐너 등 다양한 사이버 위협을 더 효과적으로 식별하고 방어할 수 있습니다. 정적 룰세트를 사용하는 기존 WAF는 제로데이 위협에 대응하기 어렵고 수동 업데이트가 필요한 반면, **AI 기반 WAF 시스템**은 복잡한 사이버 공격과 싸우는 데 유용합니다.

멀티레이어 머신 러닝 전략으로 패턴 인식, 적응형 학습, 비정상 탐지, 향상된 응답 시간을 실현할 수 있습니다. AI 기반 WAF 시스템은 수십억 개의 일일 이벤트를 통해 훈련되고 지속적인 모니터링을 포함한 멀티레이어 접근 방식을 구축해 진화하는 위협을 사전 예방하고 고객을 보호하는 것을 목표로 합니다.



## 업계 트렌드

업계별로는 커머스 부문이 2023년 1분기부터 2024년 4분기까지 전체 웹 공격 건수가 첨단 기술 업계(두 번째로 많이 공격받은 업계)의 약 3배에 달하며 모든 업계를 압도했습니다(그림 7). 또한 같은 기간에 커머스 업계가 경험한 API 공격 건수는 나머지 상위 10개 업계의 총 API 공격 건수를 크게 초과했습니다.

**업계별 웹 공격**  
2023년 1월 1일~2024년 12월 31일

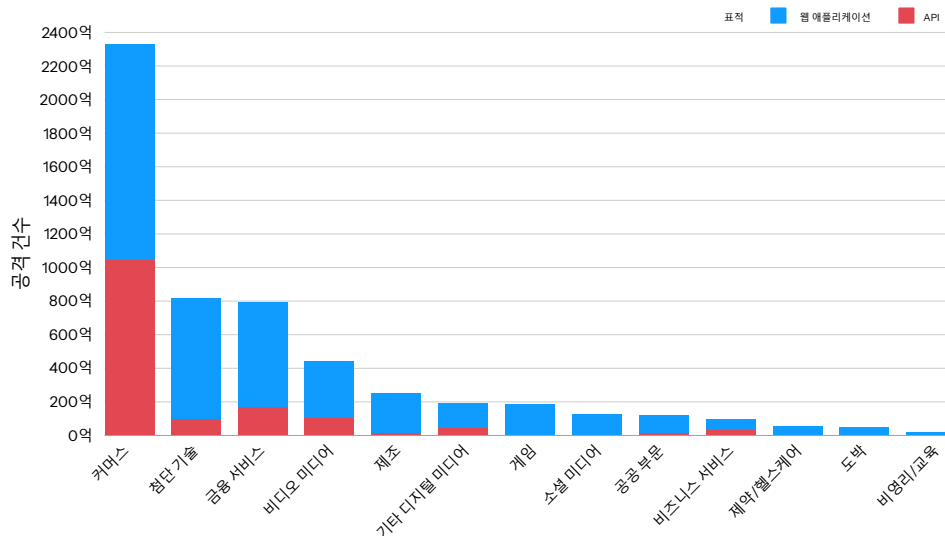


그림 7: 웹 공격의 주요 표적이 된 상위 3개 업계는 커머스, 첨단 기술, 금융 서비스입니다.

전체 레이어 7(애플리케이션 레이어) DDoS 공격의 경우, 첨단 기술 업계가 2023년 1분기부터 2024년 4분기까지 공격 건수가 7조 건을 넘어서며 다른 모든 업계보다 더 많은 공격을 받았습니다. 소셜 미디어와 커머스 업계가 첨단 기술 업계의 뒤를 이었습니다(그림 8). 그러나 동일한 기간 동안 커머스 업계를 표적으로 한 API 기반 레이어 7 DDoS 공격 건수는 다른 모든 업계의 공격 건수를 모두 합친 수치를 다시 한 번 크게 초과했습니다.

## 업계별 레이어 7 DDoS 공격 2023년 1월 1일~2024년 12월 31일

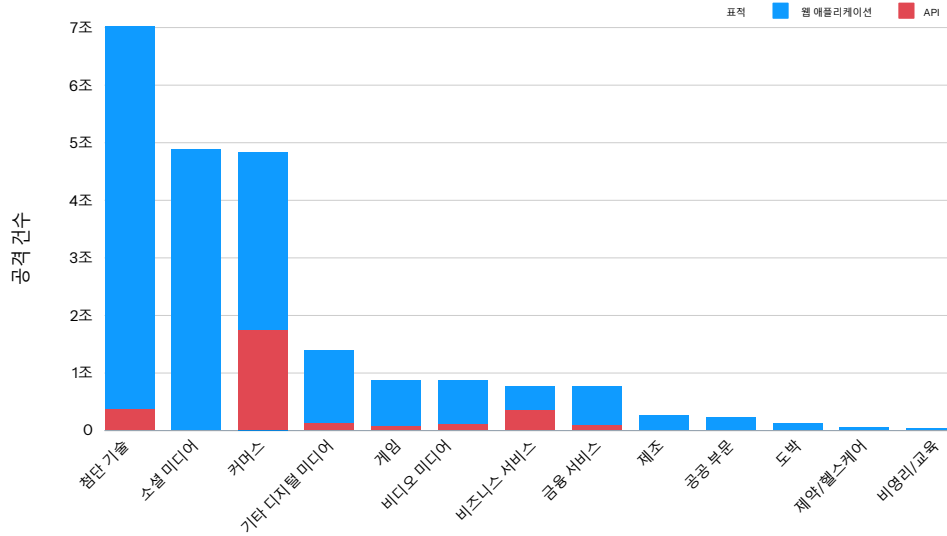


그림 8: 업계별 레이어 7 DDoS 공격

## 커머스

2023년부터 2024년까지 전체 웹 공격의 40%를 넘는 2300억 건 이상의 웹 공격을 받은 커머스 업계는 Akamai 데이터에 따르면 2023년부터 2024년 사이에 4조 8000억 건 이상의 레이어 7 DDoS 공격을 겪으며 전례 없는 규모를 기록했습니다.

이러한 규모는 웹 애플리케이션이 약 64.25%의 공격을 흡수하고 API가 나머지 35.75%를 차지하는 전략적 표적화 패턴을 보여줍니다. 이러한 분산은 공격자가 커머스 플랫폼을 감염시키기 위해 사용하는 이중 공격 기법을 반영하며 최신 위협 환경의 다면적 특성을 강조합니다.

커머스 기업은 민감한 고객 데이터, 결제 정보, 금융 거래가 집중되어 있어 특히 매력적인 표적입니다. 도난된 결제 인증정보, 감염된 고객 계정, PII를 통해 직접적인 수익 창출 경로가 존재하기 때문에 공격자에게 즉시 금전적 이익을 차지할 인센티브가 있습니다. 일부 업계에서는 감염된 데이터를 재정적 이익으로 전환하기 위해 추가 단계가 필요하지만 커머스 플랫폼은 공격자에게 직접 활용 가능한 자산을 제공하기 때문에 이 과정이 간소합니다.

## 주요 표적으로서 리테일

리테일은 커머스 업계 내 가장 집중적으로 공격받는 업계 부문으로, 여러 독특한 특성으로 인해 상대적으로 막대한 양의 공격을 받고 있습니다.

리테일 운영은 다양한 플랫폼과 시스템을 통합하는 복잡한 디지털 생태계를 유지하고 있습니다. 디지털 전환 이니셔티브는 포괄적인 보안보다 시장 진출 속도를 우선시하는 경우가 많아 보안 취약점을 초래합니다. 옴니채널 전략의 도입에 따라 공격 표면 복잡성이 의도치 않게 증가합니다. 또한 써드파티 공급업체에 과도하게 의존함에 따라 수많은 잠재적 감염 지점을 가진 복잡한 공급망이 탄생합니다.

계절별 트래픽 패턴은 공격자가 집중적으로 노리는 예측 가능한 고트래픽 기간을 생성하며 FBI의 인터넷 범죄 신고 센터에 따르면 겨울 휴가 시즌 동안 사이버 범죄 사건이 **25%에서 30%**로 급증합니다. 이커머스 플랫폼도 위협이 증가하며 12월에 사이버 공격이 연간 평균 대비 **31%** 증가했습니다.

### 웹 애플리케이션 공격의 진화

웹 애플리케이션 공격은 기술적 진보와 공격자의 방법론 변화에 따라 큰 변화를 겪고 있습니다. 공격자는 웹 애플리케이션의 취약점을 악용하기 위해 점점 더 정교한 기술을 사용하며 진화하는 보안 조치를 회피하기 위해 전략을 조정하고 있습니다. 공격자는 자동화된 공격 툴과 머신 러닝 알고리즘을 통합해 리테일 기업의 웹 애플리케이션에 대해 더 정밀하고 표적화된 캠페인을 수행할 수 있습니다.

또한 마이크로서비스 아키텍처와 API 기반 개발로 전환하면서 공격 표면이 확대됨에 따라 기존 보안 패러다임을 재검토해야 하는 필요성이 부각하고 있습니다. 이러한 변화에 따라 지속적인 모니터링, 적응형 방어 메커니즘, 웹 애플리케이션 환경에서 등장하는 새로운 공격 기법에 대한 깊은 이해를 강조하는 사이버 보안 전문가의 선제적 접근 방식이 필요합니다.

### 봇 위협 환경

봇 위협 환경은 기술적 진보, 특히 공격자가 생성형 AI 기능을 통합함에 따라 급속히 진화하고 있습니다. 이러한 진화는 기존 방어 체계를 우회하는 더 빠른 제로데이 취약점 악용과 정교한 회피 기술로 공격 전략을 강화했습니다. 증거에 따르면 2022년 8월부터 2024년 4월까지 리테일 기업을 표적으로 한 AI 기반 봇 사기 공격이 2024년 1월에 137%의 급증세를 보이며 지속적으로 **증가**했습니다. 탐지 어려움은 이러한 위협을 더욱 악화시키고 있으며 기업은 봇 공격을 식별하는 데 평균 4개월이 소요되며 이 과정에서 재정적 및 명성 손실을 입습니다.

봇은 이제 리테일 사이버 보안 환경에서 핵심 공격 기법으로 기능하며 계정 탈취, 신용카드 사기, 상품권 남용을 촉진합니다. 봇은 감염된 사이트에서 도난당한 데이터를 활용해 다른 사이트에 대한 크리덴셜 스테핑 공격을 수행함으로써, 리테일 생태계 전반에 증폭 효과를 일으키는 광범위한 공격 캠페인의 촉진제 역할을 합니다. 이러한 활동이 온라인 사기의 “산업화”에 기여함에 따라 글로벌 범죄 기업은 자동화 툴을 활용해 수동적으로 달성할 수 없는 규모로 운영을 확장하고 있습니다.

AI 및 봇 관련 공격으로부터 리테일 운영의 웹 애플리케이션 및 API를 보호하기 위한 권장 사항 목록은 [방어](#) 섹션을 참고하세요.

## 금융 서비스

금융 서비스 업계는 웹 공격의 주요 표적이 되었으며 레이어 7 DDoS 공격이 계속 발생하고 있습니다. 2023년 1월부터 2024년 12월까지 웹 공격은 790억 건을 초과했으며 같은 기간 웹 애플리케이션과 API를 노린 레이어 7 DDoS 공격은 7610억 건을 초과했습니다.

이러한 전례 없는 규모는 금융 서비스 업계가 얼마나 취약하고 공격자에게 매력적인 대상인지를 알려주는 방증입니다. 급증을 일으킨 요인에는 글로벌 경제 인프라에서 금융 서비스의 핵심 역할, 금융 데이터의 높은 가치, 심각한 [혼란](#) 등이 있습니다.

### 금융 서비스의 디지털화

금융 서비스의 디지털화는 사이버 범죄자의 공격 표면을 확대했습니다. AI 기반 개인화, 서비스로서 बैंकिंग, 내장형 금융 솔루션의 도입으로 새로운 취약점이 발생했습니다. 지정학적 갈등, 특히 러시아-우크라이나 전쟁은 금융 기관을 [표적으로 한](#) 해티비스트 활동을 촉진했습니다. 경제적 요인, 특히 암호화폐의 확산과 암호화폐 준비금 도입 가능성은 공격자의 금융 업계에 대한 [관심](#)을 높였습니다.

웹 애플리케이션 공격은 새로운 기술에 적응하고 새로운 취약점을 악용하며 빠르게 변모하고 있습니다. 공격자는 기존 보안 조치를 우회하고 보다 타깃팅된 지속 가능한 공격을 수행하기 위해 고급 AI 및 머신 러닝 알고리즘을 활용하고 있습니다. 서버리스 아키텍처와 마이크로서비스의 확산으로 새로운 공격 기법을 생성되었으며 API의 사용 증가로 공격자의 잠재적 엔트리 포인트가 확대되었습니다. 또한 모바일 및 클라우드 기반 애플리케이션으로 전환되면서 데이터 보호 및 접속 제어 측면에서 독특한 도전 과제가 제기됨에 따라 필수적으로 보안 전략을 재검토해야 합니다.

## 공격 표적으로서 बैं킹 부문의 중요성

금융 서비스 업계 내에서 बैं킹 부문은 웹 공격의 가장 주요한 표적으로 부상했습니다(그림 9). 커머스 업계와 마찬가지로 बैं킹 부문에서도 [크리덴셜 스테핑](#) 공격이 주요 위협 기법으로 부상하고 있습니다.

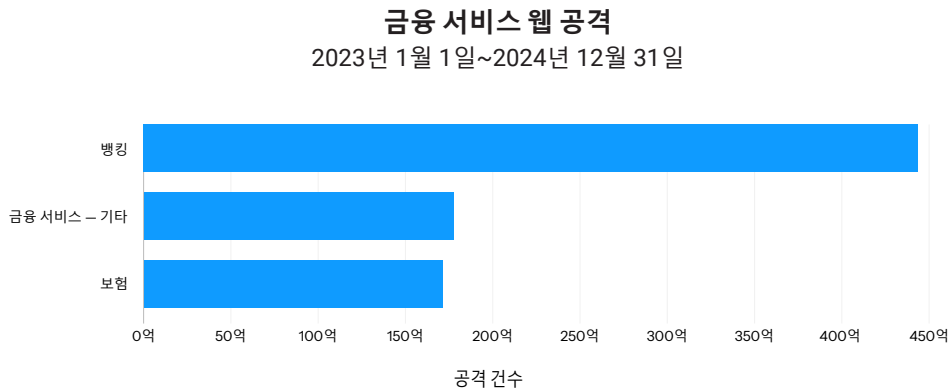


그림 9: बैं킹은 금융 서비스 웹 공격에서 가장 표적이 되는 업계 부문입니다

온라인 बैं킹 서비스의 보편화와 계정 접속의 중요성이 사이버 범죄자들의 관심을 끌고 있습니다. 성공적인 공격에 대한 재정적 인센티브가 상당하며 소수의 계정만 감염시켜도 큰 이익을 얻을 수 있습니다. बैं킹 부문은 사용자 불편을 초래할 수 있는 멀티팩터 인증 같은 엄격한 보안 조치를 구축하는 데 소극적이었기 때문에 의도치 않게 [취약점](#)을 높이게 되었습니다.

공격 표적으로서 बैं킹 부문의 중요성은 여러 요인으로 인해 더욱 악화되고 있습니다. 공격자가 서비스 중단에 대한 [우려](#)를 악용함에 따라 서비스 중단에 대한 민감성은 협박의 기회가 됩니다. 또한, AI와 머신 러닝을 활용해 탐지를 회피하는 등 공격 기술의 고도화는 기존 방어 메커니즘에 심각한 [도전 과제](#)를 제기하고 있습니다. 규제 환경은 엄격한 컴플라이언스 요건과 보안 유출 시 부과되는 벌금으로 인해 बैं킹 부문의 사이버 보안 과제에 또 다른 복잡성을 추가하고 있습니다.

## 침단 기술

침단 기술 업계는 여전히 웹 및 레이어 7 DDoS 공격의 주요 표적입니다. 본 보고서의 목적상 침단 기술 업계는 통신, 기업용 소프트웨어 및 하드웨어, 소비자용 소프트웨어 및 하드웨어 업계 부문을 포함합니다. Akamai의 데이터에 따르면 침단 기술 업계는 2023~2024년 동안 817억 건 이상의 웹 공격을 받으며 전체 웹 공격 건수에서 커머스에 이어 두 번째로 많은 공격을 받았습니다. 또한 침단 기술 업계는 2년간 7조 건 이상의 레이어 7 DDoS 공격을 가장 많이 받은 업계로 나타났습니다.



첨단 기술 웹 애플리케이션은 복잡한 데이터베이스 쿼리와 동적 콘텐츠를 자주 사용해 공격자가 악용하여 서버를 **쉽게 과부하**시킬 수 있는 취약점을 만듭니다. 이러한 취약점으로 인해 첨단 기술 업계는 높은 레이어 7 DDoS 공격률을 경험하고 있습니다. 특히 **블록체인** 네트워크는 DDoS 공격이 급증했으며 공격자는 HTTP 플러딩과 스팸 거래와 같은 방법을 사용해 블록체인의 분산형 아키텍처도 극복하며 정상적인 거래를 방해했습니다. 첨단 기술 업계에서 운영이 중단되면 심각한 재정적 영향이 발생하기 때문에 공격자는 DDoS 공격을 배포해 필수 서비스를 마비시키려 합니다. 공격자는 HTTP 플러딩 공격에서 보안이 취약한 엔드포인트를 자주 악용하기 때문에 최신 소프트웨어 개발 시 API 중심 아키텍처 사용으로 추가적인 리스크가 초래됩니다.

### 통신 부문도 유사한 도전 과제에 직면하고 있습니다

통신 업계는 API 공격의 영향을 크게 받는 업계로, 유사한 사이버 보안 문제를 직면하고 있습니다. 첨단 기술 업계 부문의 웹 애플리케이션 및 API 위협에는 데이터 유출, DDoS 공격, 공급망 취약점이 포함됩니다. 이러한 취약점은 여러 주요 데이터 유출 사건으로 이어졌습니다.

예를 들어, 2025년 1월 연구진은 **주요 통신 네트워크**의 API 취약점으로 인해 3000개의 기업이 보안 리스크에 노출된 것을 발견했습니다. 해당 조사에서 고객 검증 프로세스의 취약점과 내부 시스템에 접속을 허용하는 백엔드 API 경로 탐색 취약점 등 심각한 보안 간극이 드러났습니다.

### 사물 인터넷이 새로운 공격 기법을 도입합니다

첨단 기술 업계는 기술의 급속한 발전 시대에 진화하는 웹 애플리케이션 및 API 취약점에 고전하고 있습니다. 이러한 진화는 IoT(Internet of Things) 디바이스의 광범위한 도입을 포함하며 많은 디바이스가 강력한 보안 조치를 갖추지 않아 새로운 공격 기법이 탄생하고 있습니다. 멀티 클라우드 인프라가 빠르게 도입되면서 환경이 제대로 설정되지 않아 악용 가능성이 증가하고 있습니다.

보안 취약점이 있는 IoT 디바이스와 클라우드 시스템이 고도로 정교한 **AI 기반 공격**의 표적이 되고 있습니다. **SaaS 플랫폼**은 넓은 공격 표면으로 인해 API 공격의 리스크가 높아지고 있습니다. AI 솔루션의 확산과 써드파티 SaaS 플랫폼에 대한 의존도 증가로 인해 첨단 기술 업계의 전체 API 공격 표면이 크게 확대되었습니다. 기업이 이러한 기술을 계속 도입함에 따라 악용 가능성은 증가하고 있기 때문에 강력한 보안 조치와 지속적인 모니터링이 필수입니다.

## 지역별 트렌드

참고: 지역별 보고서의 형식을 변경해 독자들이 데이터를 더 쉽게 접속하고 지역별 공격 트렌드를 명확히 확인할 수 있도록 했습니다. 지역은 북미, 아시아-태평양 및 일본(APJ), 유럽, 중동, 아프리카(EMEA), 라틴 아메리카(LATAM)로 구분했습니다. 이 섹션에서 논의하는 데이터를 한눈에 확인할 수 있는 요약 차트도 포함했습니다(그림 10).

| 지역    | 웹 공격 건수        | 레이어 7 DDoS 공격 건수   | 주요 웹 공격 기법                  | 주요 표적 지역                                  | 주요 표적 업계                 |
|-------|----------------|--------------------|-----------------------------|-------------------------------------------|--------------------------|
| APJ   | 800억, 14% API  | 7조 4000억, 6% API   | 활성 공격 세션, LFI, XSS          | 호주(203억), 인도(173억), 싱가포르(159억)            | 금융 서비스, 커머스, 소셜 미디어      |
|       |                |                    |                             | 싱가포르(4조 7000억), 인도(6070억), 한국(2830억)      | 소셜 미디어, 기타 디지털 미디어, 커머스  |
| EMEA  | 1160억, 37% API | 2조 6000억, 20% API  | 활성 공격 세션, API 요청 제한 위반, LFI | 영국(303억), 네덜란드(195억), 스페인(142억), 독일(128억) | 커머스, 비디오 미디어, 금융 서비스     |
|       |                |                    |                             | 독일(5690억), 영국(5060억)                      | 커머스, 기타 디지털 미디어, 비디오 미디어 |
| LATAM | 30억, 12% API   | 2580억, 18% API     | 활성 공격 세션, WAT, SSRF         | 브라질(193억), 멕시코(20억)                       | 커머스, 금융 서비스              |
|       |                |                    |                             | 브라질(1750억), 멕시코(390억)                     | 커머스, 금융 서비스              |
| 북미    | 3270억, 29% API | 11조 9000억, 16% API |                             |                                           |                          |

그림 10: 지역별 개요, 2023년 1월–2024년 12월 (LFI: Local File Inclusion, XSS: Cross-Site Scripting, WAT: Web Attack Tool, SSRF: Server-Side Request Forgery)



## 두 가지 애플리케이션 및 API 공격 트렌드

2023년 1월부터 2024년 12월까지 24개월 보고 기간 동안 지역별 웹 애플리케이션 및 API 공격과 레이어 7 DDoS 공격을 비교 분석한 결과, 두 가지 주요 트렌드가 확인되었습니다(그림 11).

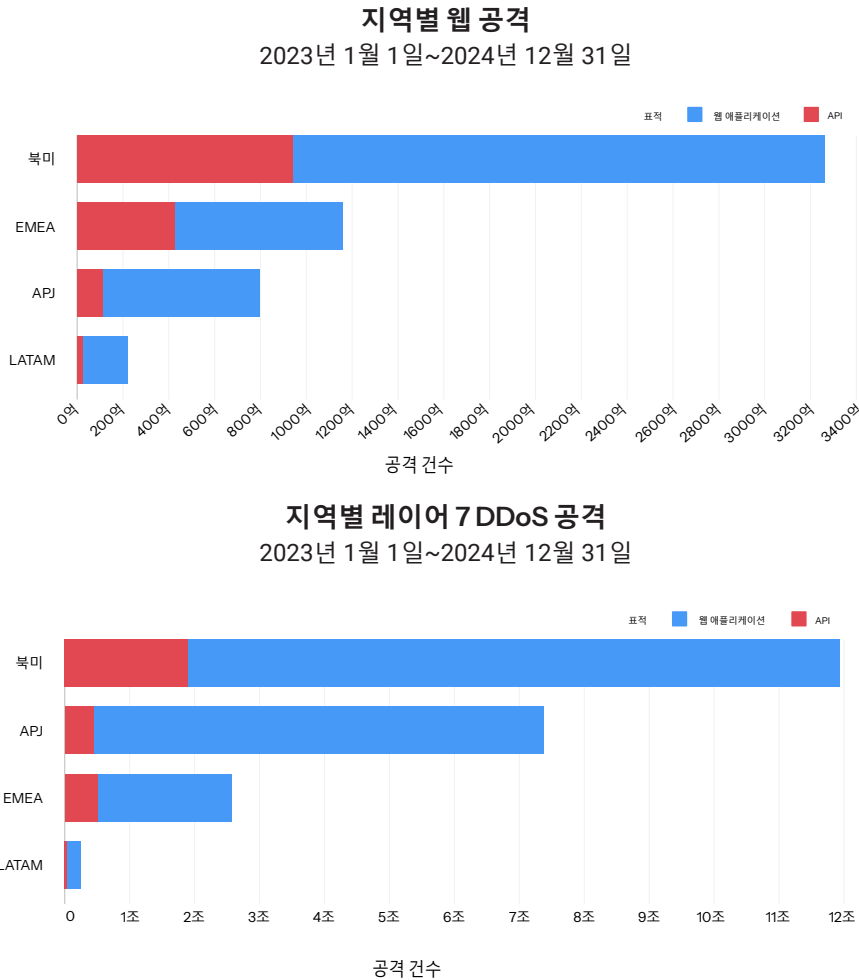


그림 11: 보고 기간 동안 전 세계적으로 EMEA 지역이 API 공격의 가장 높은 비율을 기록했으며 APJ 지역은 총 레이어 7 DDoS 공격 건수에서 두 번째로 높은 수치를 기록했습니다.

**공격 트렌드 1:** EMEA 지역에서 API 공격이 널리 확산되었으며 [다른 지역보다 높은 API 도입률](#), 오픈 뱅킹, [PCI DSS v4.0](#) 등이 API 사용을 촉진해 보안 리스크를 초래하기 때문으로 보입니다. (API 관련 리스크에 대한 자세한 논의는 [API 위협 인텔리전스 진화](#) 섹션을 참조하세요.)

**2023년에 처음 관찰된** 트렌드가 지속되어, 24개월 동안 EMEA 지역에서 API를 표적으로 한 웹 공격이 가장 높은 집중도를 기록했습니다. EMEA 지역에서 발생한 총 1160억 건의 웹 공격 중 37%가 API를 표적으로 삼았습니다. 반면 북미 지역에서는 총 3270억 건의 웹 공격 중 29%가 API를 대상으로 했습니다. APJ 지역에서는 800억 건의 웹 공격 중 14%, LATAM에서는 30억 건 중 12%가 API를 노렸습니다.

EMEA는 API를 표적으로 삼은 레이어 7 DDoS 공격의 가장 높은 집중도를 기록했으며(20%), 이어 LATAM(18%), 북미(16%), APJ(6%) 순이었습니다. 일반적으로 각 지역에서 API를 표적으로 한 레이어 7 DDoS 공격 시도는 전체 웹 공격 중 비교적 비율이 작았습니다. Akamai는 더 진보된 봇 기반 공격과 API 취약점을 노린 AI 기반 공격의 급증을 비롯한 다양한 이유로 시간이 지나면서 이러한 비율이 증가할 것으로 예상합니다.

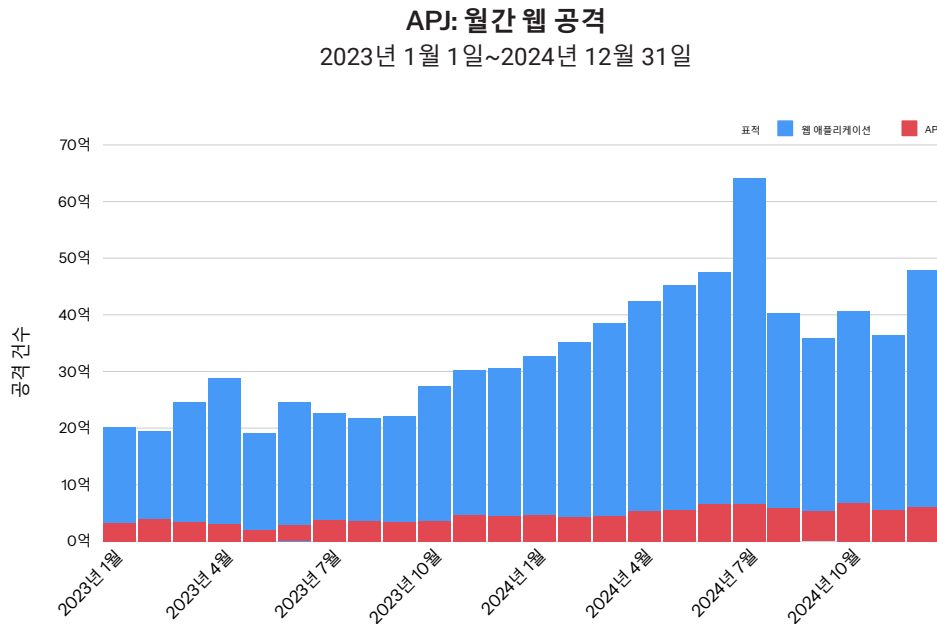
**공격 트렌드 2:** APJ는 전 세계 레이어 7 DDoS 공격에서 두 번째로 높은 수준인 7조 4000억 건(북미는 11조 9000억 건)을 기록했습니다. EMEA는 2조 6000억 건, LATAM은 2580억 건으로 뒤를 이었습니다. 이러한 트렌드는 Akamai의 [위협받는 디지털 요새 SOTI 보고서](#)에서 처음 관찰되었으며 APJ 지역에서 소셜 미디어를 표적으로 한 공격 시도의 집중도가 높은 것에 기인한다고 판단됩니다.

## APJ, EMEA, LATAM에 대한 심층 분석

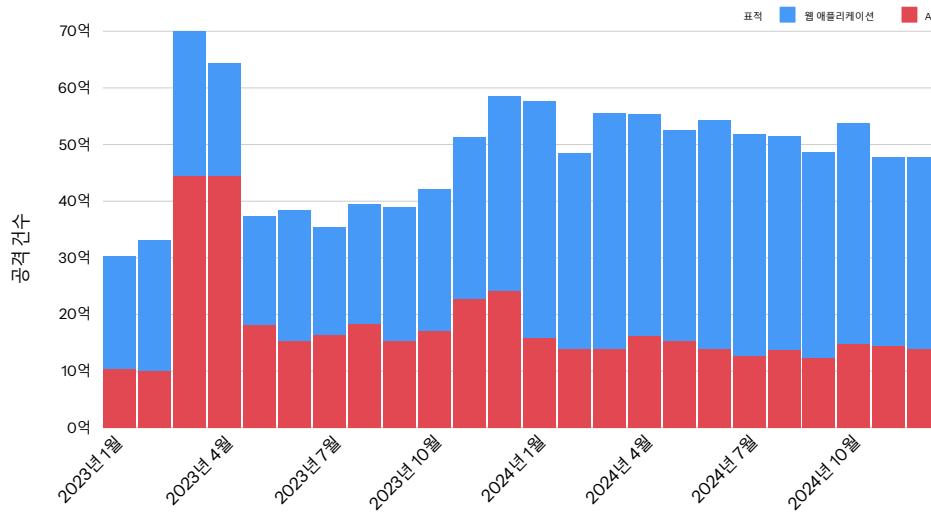
이 섹션에서는 APJ, EMEA, LATAM 내 주요 트렌드를 강조합니다. 또한 해당 지역 내 특정 지역에서 충분한 공격 이벤트 데이터를 확보해 통계적으로 유의미한 인사이트를 제공할 수 있는 데이터도 포함했습니다.

### 웹 애플리케이션 및 API 공격: 트래픽 분석

지역별 월별 웹 공격 트렌드 비교는 대조적인 결과를 보여줍니다(그림 12).



### EMEA: 월간 웹 공격 2023년 1월 1일~2024년 12월 31일



### LATAM: 월간 웹 공격 2023년 1월 1일~2024년 12월 31일

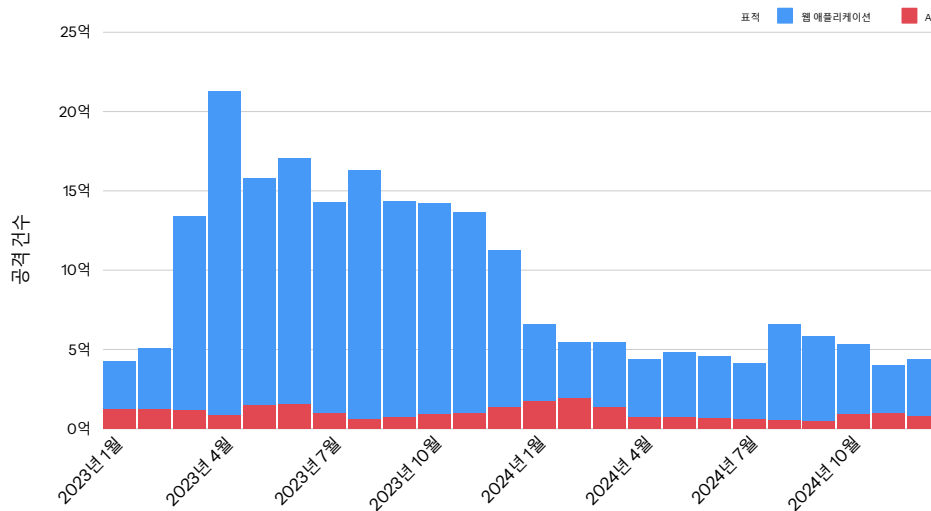


그림 12: 웹 애플리케이션 공격 활동이 APJ 및 EMEA 지역의 총 웹 공격 수 증가를 주도했으며 LATAM 지역에서는 공격이 급격히 감소했습니다.

APJ 지역은 2023년 290억 건에서 2024년 510억 건으로 73%의 큰 증가율을 기록했습니다. EMEA 지역에서는 전년 대비 16% 증가(540억 건에서 620억 건)를 기록했지만 이렇게 증가율이 작은 것은 데이터에 기록된 이상치 사건이 영향을 준 결과이며 해당 사건을 제외하면 증가율은 약 33%에 가깝습니다. LATAM 지역에서는 웹 공격이 2023년 160억 건에서 2024년 600만 건으로 61% 감소했습니다.

특히 APJ와 LATAM 지역에서 API 공격이 낮은 수준을 유지하면서 웹 애플리케이션 공격의 증가가 총 웹 공격 건수 증가를 주도한 것으로 보입니다.

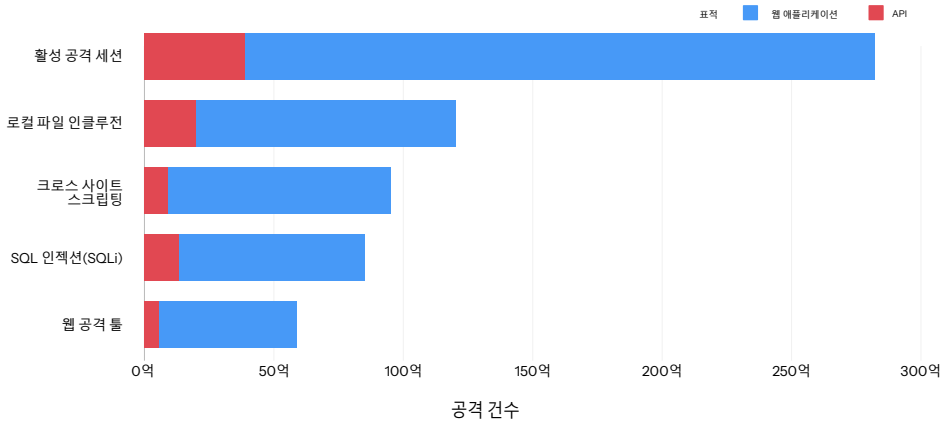
EMEA 지역에서는 2023년 상반기([스페인 커머스 부문을 표적으로 한 대규모 집중 공격과 관련됨](#))의 급증 이후 API 공격 수준이 감소했으며 2024년 내내 다른 지역에 비해 낮은 수준을 유지했습니다.

LATAM에서는 공격자가 커머스 부문을 제약 및 비즈니스 서비스를 포함한 다른 업계와 [랜섬웨어](#) 같은 다른 종류의 공격으로 초점을 전환함에 따라 웹 공격이 감소했습니다.

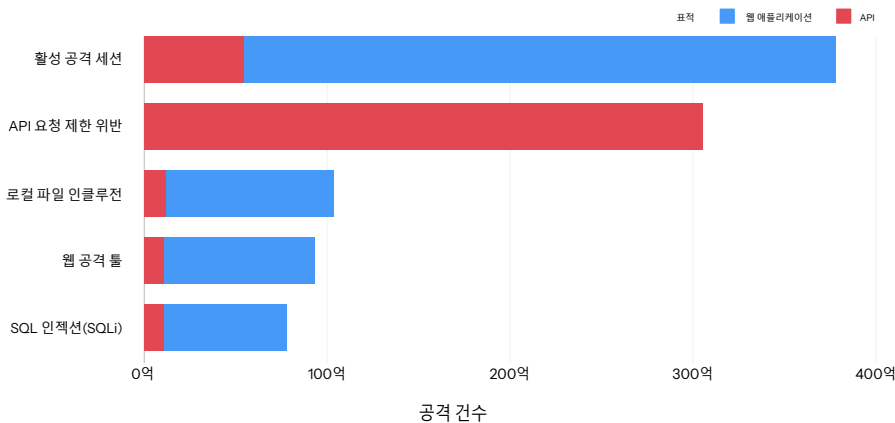
## 웹 애플리케이션 및 API 공격: 주요 공격 기법

지난 2년간 공격자는 기존 검증된 방법을 계속 사용했지만 최신 행동 기반 웹 공격 기법의 사용률도 높았습니다(그림 13).

**APJ: 기법별 웹 공격**  
2023년 1월 1일~2024년 12월 31일



**EMEA: 기법별 웹 공격**  
2023년 1월 1일~2024년 12월 31일





## LATAM: 기법별 웹 공격

2023년 1월 1일~2024년 12월 31일

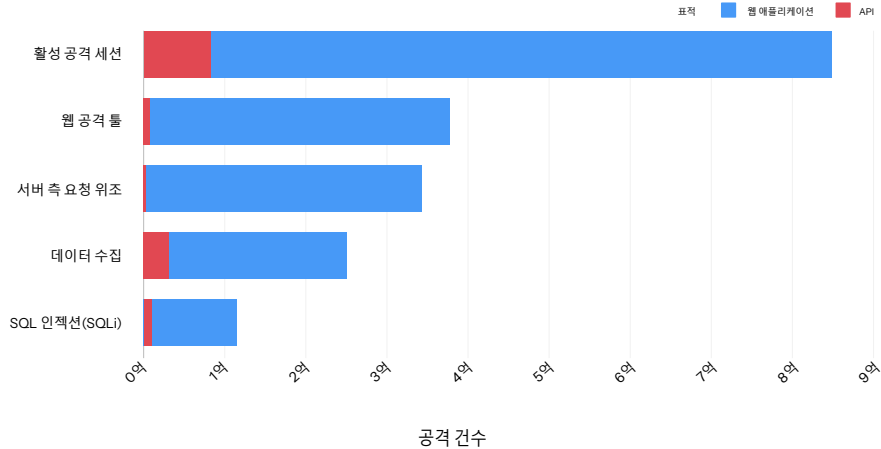


그림 13: 지역별 상위 공격 기법에는 기존 방법과 API 악용을 특정 목표로 삼은 최신 행동 기반 방법이 포함되었습니다.

지역별 공격 기법은 전 세계 트렌드와 마찬가지로 기존 공격 기법(LFI, SQLi, XSS)이 지속되었으며 LATAM 지역에서는 SSRF도 관찰되었습니다. Akamai는 [2025년 보안팀 가이드](#)에서 기존 웹 취약점을 보호하기 위한 XSS의 지속적인 영향력과 관련성을 강조했습니다.

해당 기간 동안 공격자가 API 악용에 집중함에 따라 최신 행동 기반 공격 기법과 관련된 문제가 증가했습니다. 공격자는 해당 기법을 사용해 취약점을 발견하고 악용합니다. Akamai 연구진은 지역별로 기법을 추적해 다음과 같은 결과를 관찰했습니다.

- 각 지역에서 가장 활발한 공격 기법은 활성 공격 세션으로, 이에 대해 Akamai 지능형 제어 기능이 알려진 공격자로부터의 요청을 일정 기간 동안 사전 차단하는 데 사용됩니다.
- EMEA 지역에서 API 요청 제약 조건 위반이 두 번째로 가장 널리 퍼졌으며 API 중심 공격의 집중도가 가장 높았습니다. 공격자는 속도 제한이나 데이터 입력 요구사항을 회피하는 방식으로 API를 악용하려고 시도합니다.
- 각 지역에서 웹 공격 툴은 상위 5위 안에 포함되었습니다. 공격자는 이러한 기법을 활용해 표적의 보안 및 설정에 대한 정보나 악용 가능한 취약점을 탐색합니다.

주요 기법에 대한 자세한 내용은 [웹 공격](#) 섹션을 참조하세요.

## 웹 애플리케이션 및 API 공격: 주요 표적

각 지역 내에서 공격자가 집중한 지역을 구체적으로 살펴보면, APJ 지역에서는 호주(203억), 인도(173억), 싱가포르(159억)가 웹 애플리케이션 및 API 공격의 가장 큰 타격을 받았으며 일본(63억), 중국(62억), 한국(49억), 뉴질랜드(29억), 홍콩 SAR(22억)이 뒤를 이었습니다.

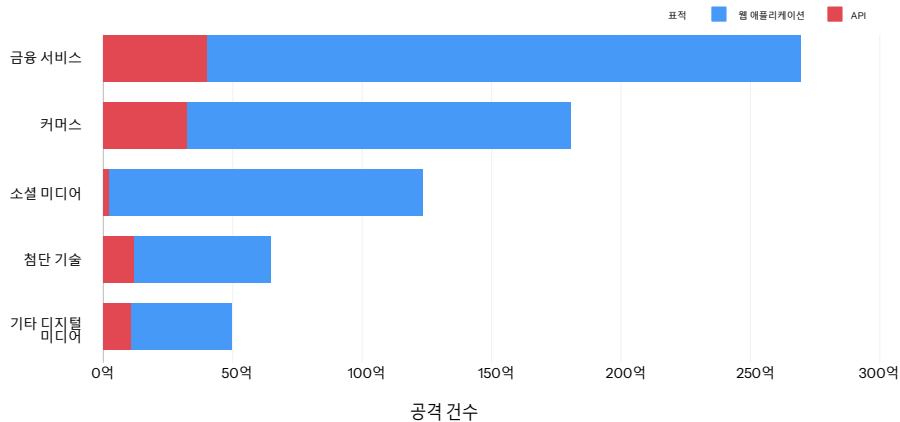
EMEA 지역에서는 웹 애플리케이션 및 API 공격으로 가장 큰 영향을 받은 국가로 영국(303억), 네덜란드(195억), 스페인(142억), 독일(128억)이 꼽혔습니다. 오스트리아(82억)가 그 뒤를 이었으며 프랑스(75억), 이탈리아(41억), 스위스(37억), 벨기에(35억), 이스라엘(33억)이 포함되었습니다.

LATAM 지역에서는 웹 애플리케이션 및 API 공격이 브라질(193억)에 집중되었으며 다음으로 멕시코(20억)와 칠레(4억)가 해당 지역 공격의 일부만 겪었습니다.

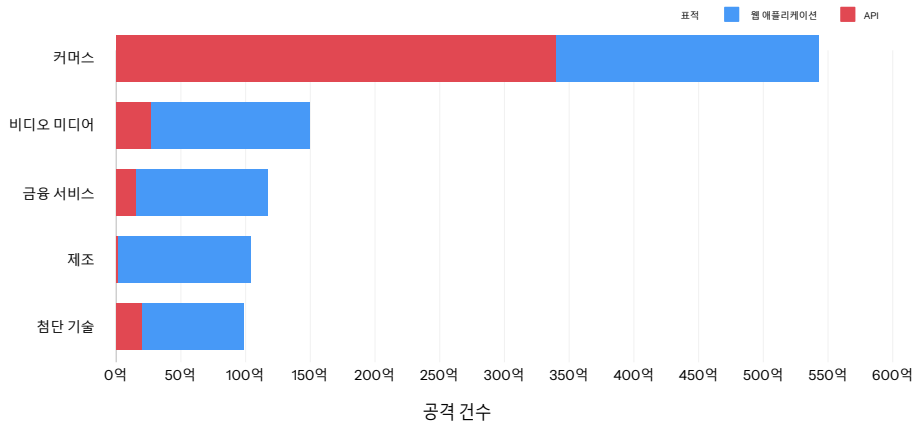
## 업계별 표적

업계별 트렌드 분석 결과, APJ, EMEA, LATAM 지역에서 커머스 및 금융 서비스 업계가 웹 공격의 주요 표적 업계 상위 3위 안에 꾸준히 포함되었습니다(그림 14).

**APJ: 업계별 웹 공격**  
2023년 1월 1일~2024년 12월 31일



**EMEA: 업계별 웹 공격**  
2023년 1월 1일~2024년 12월 31일



## LATAM: 업계별 웹 공격

2023년 1월 1일~2024년 12월 31일

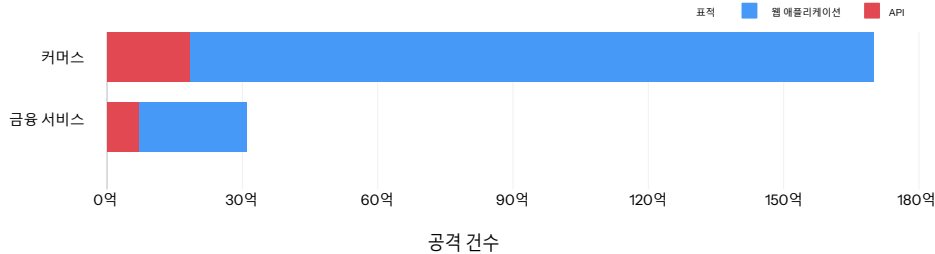


그림 14: APJ, EMEA, LATAM 지역에서 커머스 및 금융 서비스가 웹 공격의 주요 표적 업계 상위 3위에 포함되었습니다.

APJ 지역에서 금융 서비스 업계는 총 웹 공격 건수에서 270억 건으로 가장 많았으며 커머스는 180억 건으로 두 번째였습니다. 이는 전년 대비 각각 52%와 161% 성장한 결과입니다. API 공격에서 가장 많은 표적이 된 업계는 디지털 미디어(22%)였으며 커머스(18%)와 금융 서비스(15%)가 뒤를 이었습니다.

EMEA 지역에서는 커머스 업계가 웹 공격으로 가장 큰 영향을 받았으며 540억 건으로 2위 업계보다 3배 더 많은 수치를 기록했습니다. 높은 집중도에도 불구하고, 2023년의 급증으로 인해 지역 데이터가 왜곡되면서 커머스 부문을 표적으로 한 총 웹 공격은 전년 대비 10% 감소했습니다. 그러나 EMEA 지역은 금융 서비스(152%)와 제조업(96%)을 포함한 다른 업계를 표적으로 한 공격의 증가로 인해 총 웹 공격이 전년 대비 16% 증가했습니다. 지역 내 API를 표적으로 한 공격을 자세히 살펴보면 커머스를 표적으로 한 전체 웹 공격의 63%가 API를 표적으로 삼았습니다.

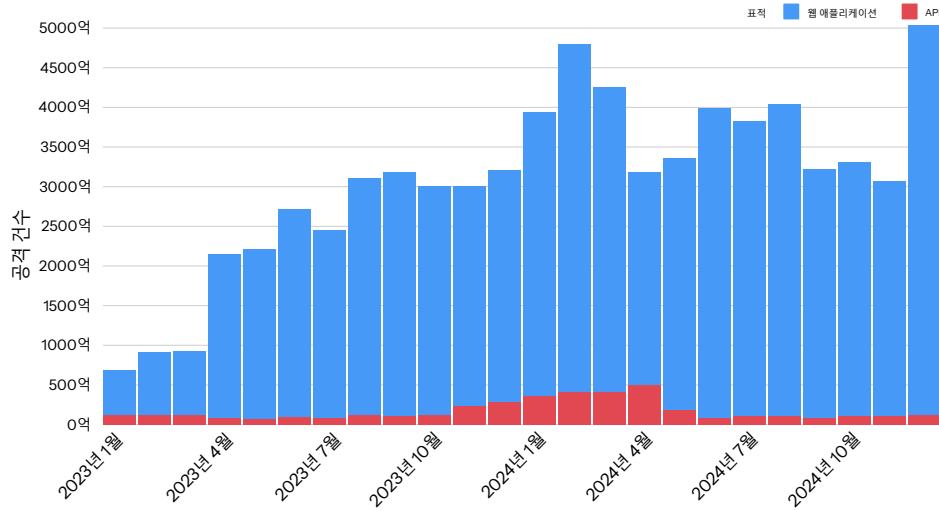
LATAM 지역에서도 유사한 트렌드가 관찰되었습니다. 커머스를 표적으로 한 총 웹 공격 건수는 170억에 달해 다른 업계를 압도했지만 전년 대비 커머스 부문 공격은 76% 감소했습니다. 한편, 제약 업계와 비즈니스 서비스 업계는 각각 전년 대비 107%와 129%의 증가율을 기록했습니다. 또한 커머스를 표적으로 한 공격의 11%가 API를 표적으로 삼았으며 금융 서비스는 API를 표적으로 한 공격의 집중도가 23%로 더 높았습니다.

금융 서비스와 커머스 업계는 웹 애플리케이션 및 API 공격의 표적으로 매력적인 특성을 공유합니다. 두 업계 모두 복잡한 생태계 내에서 운영되며 API에 대한 의존도가 높고, 가치 있는 데이터를 보유하고 있습니다. 공격자는 목표를 달성하기 위해 기존 공격 기술과 새로운 공격 기술을 결합해 사용합니다.

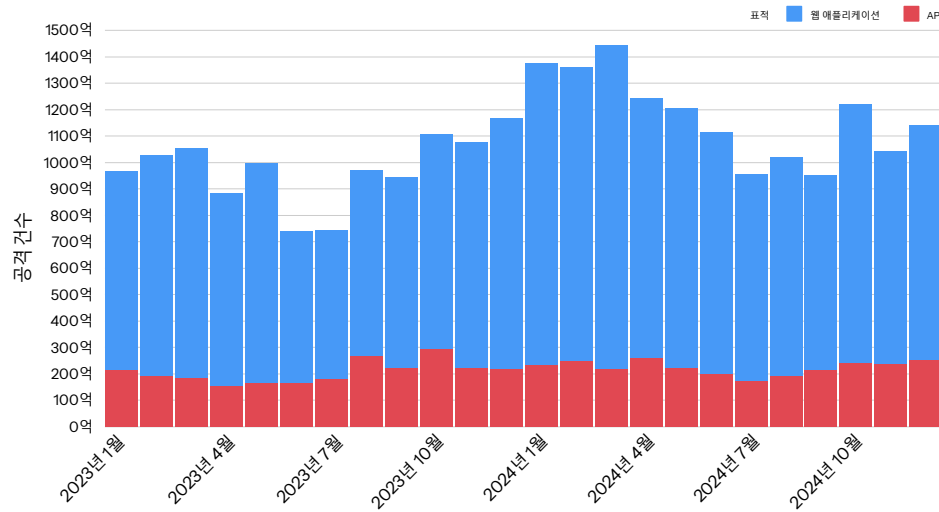
## 레이어 7 DDoS 공격: 트래픽 분석

지역별 월별 레이어 7 DDoS 공격 트렌드를 비교한 결과, APJ가 공격의 중심지였으며 EMEA와 LATAM은 공격이 증가와 감소가 반복되는 양상을 보였습니다(그림 15).

**APJ: 월간 레이어 7 DDoS 공격**  
2023년 1월 1일~2024년 12월 31일



**EMEA: 월간 레이어 7 DDoS 공격**  
2023년 1월 1일~2024년 12월 31일



## LATAM: 월간 레이어 7 DDoS 공격 2023년 1월 1일~2024년 12월 31일

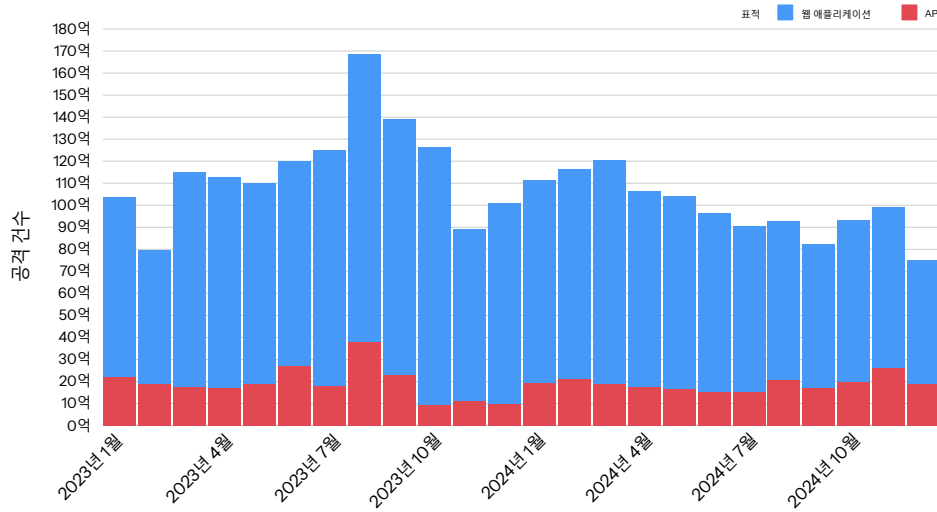


그림 15: 2024년에 레이어 7 DDoS 공격이 APJ와 EMEA에서 증가한 반면, LATAM에서는 감소했습니다.

APJ에서는 레이어 7 DDoS 공격이 전년 대비 66% 증가했으며 2024년 12월에 5040억 건으로 24개월 만에 최고치를 기록했습니다. 이 성장은 주로 소셜 미디어 업계를 표적으로 한 공격에 의해 주도되었습니다.

EMEA에서는 레이어 7 DDoS 공격이 2024년 3월에 약 1450억 건으로 정점을 찍은 후 감소세를 보이다가 다시 증가해 전년 대비 20% 성장했습니다. 이는 지정학 및 기술적 요인의 복합적 영향으로 설명됩니다. 지역 내 지속되는 긴장은 해티비스트의 활동을 촉진했습니다. 이러한 트렌드는 사이버 범죄자의 진입 장벽을 낮추는 AI 강화 툴과 서비스로써 DDoS 플랫폼의 등장으로 악화되었습니다.

LATAM 지역은 보고 기간 초반에 레이어 7 DDoS 공격 시도가 급증했으며 이는 API 리소스를 과부하를 유발하기 위한 [HTTP 플러드 공격](#)의 증가와 일치했습니다(이 공격 기법은 [레이어 7 DDoS 공격: 연간 비교 및 트렌드](#) 섹션에서 자세히 논의했습니다. 활동은 2023년 8월에 168억 건으로 정점을 찍은 후 기간 나머지 기간 동안 전년 대비 15% 감소해 75억 건으로 최저점을 기록했습니다.

## 레이어 7 DDoS 공격: 주요 표적

각 지역에서 공격자가 표적으로 삼은 지역 및 업계는 [이전 레이어 7 DDoS 공격 분석](#)과 비교했을 때 거의 변화가 없었습니다.

APJ 지역에서는 싱가포르가 4조 7000억 건으로 가장 많은 공격을 받았으며 인도(1조 1000억), 한국(6070억), 인도네시아(2830억), 중국(2460억), 일본(1110억), 호주(1080억), 대만(810억)이 뒤를 이었습니다.

EMEA 지역에서는 독일(5690억)과 영국(5060억)이 가장 많은 레이어 7 DDoS 공격을 기록했으며 이스라엘(2050억), 스웨덴(1930억), 몰타(1600억)가 뒤를 이었습니다. 이탈리아(1580억), 스위스(1470억), 프랑스(1290억), 네덜란드(1110억), 스페인(960억)이 상위 10위에 올랐습니다.

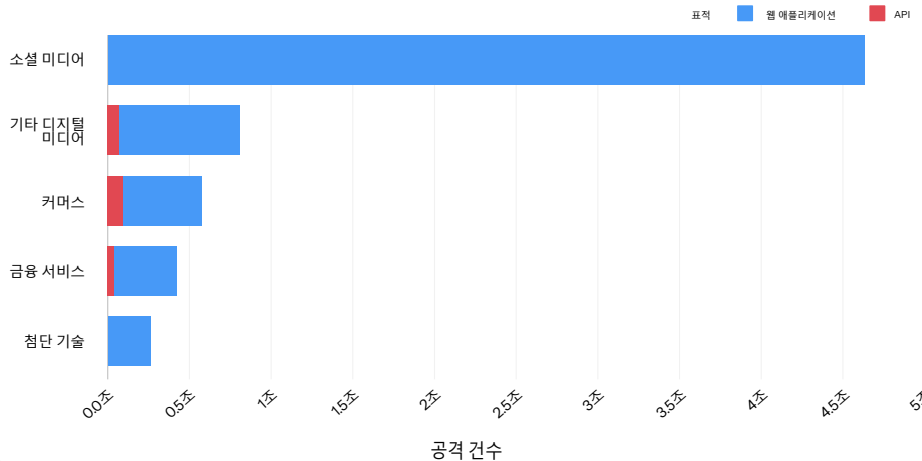
LATAM 지역에서는 브라질이 1750억 건으로 레이어 7 DDoS 공격이 가장 집중된 국가로 나타났으며 멕시코(390억)와 코스타리카(190억)가 그 뒤를 이었습니다.

## 업계별 표적

APJ 및 EMEA 지역에서 레이어 7 DDoS 공격으로 가장 큰 영향을 받은 업계(그림 16)는 [이전 보안 앱 SOTI 보고서](#)와 동일합니다. 이전 보고서에서 자세히 논의했듯이 APJ 지역의 소셜 미디어 플랫폼을 표적으로 한 레이어 7 DDoS 공격은 2023년 1월부터 2024년 6월까지 전 세계적인 군사 분쟁과 언론의 집중 보도를 받은 선거 이벤트와 연관되어 급증했습니다. 이는 지리적 정치적 혼란 시기에는 소셜 미디어 플랫폼이 대규모 트래픽을 처리해야 하기 때문에 예상된 결과입니다. 예상대로 2024년 나머지 기간 동안 APJ와 미국에서 선거가 진행되면서 이러한 트렌드는 더욱 강화되었습니다. 이러한 요인들은 해당 부문에 대한 공격이 전년 대비 130% 증가하는 데 기여했습니다.

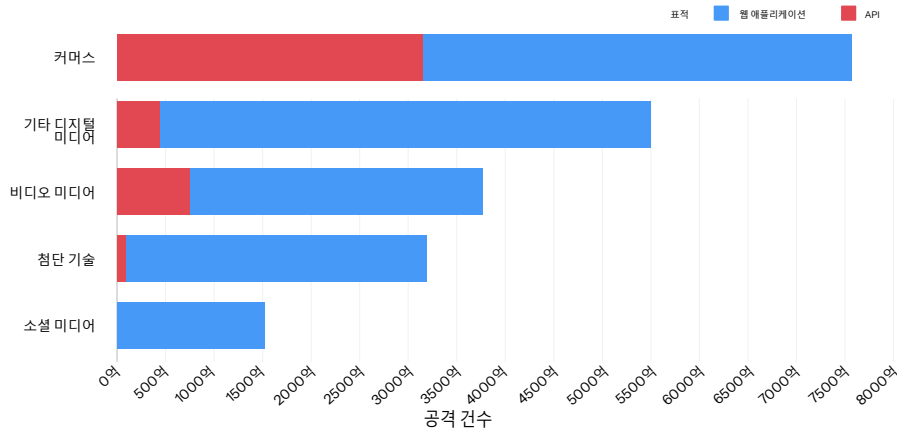
### APJ: 업계별 레이어 7 DDoS 공격

2023년 1월 1일~2024년 12월 31일





## EMEA: 업계별 레이어 7 DDoS 공격 2023년 1월 1일~2024년 12월 31일



## LATAM: 업계별 레이어 7 DDoS 공격 2023년 1월 1일~2024년 12월 31일

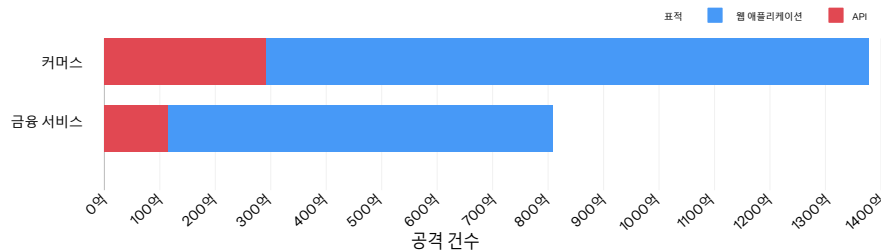


그림 16: 지역별 가장 큰 영향을 받은 업계는 과거 분석과 동일하게 유지되었습니다. 커머스는 레이어 7 DDoS 공격의 주요 표적이 된 업계로 꾸준히 가장 많이 공격을 받았습니다.

EMEA 지역에서는 커머스 업계가 변함없이 레이어 7 DDoS 공격의 영향을 가장 많이 받았으며 디지털 미디어와 비디오 미디어가 뒤를 이었습니다. 전년 대비 공격 성장률이 가장 컸던 업계는 첨단 기술(70%), 소셜 미디어(23%), 커머스(14%)였습니다. 이러한 변화는 공격자가 업계와 지역 사이에 초점을 얼마나 빠르게 전환할 수 있는지 보여주며 광범위한 트렌드를 추적해야 한다는 점을 강조합니다.

LATAM 지역에서도 커머스 업계가 레이어 7 DDoS 공격을 가장 많이 받았으며 금융 서비스가 그 뒤를 이었습니다. 보고 기간 동안 업계별 레이어 7 DDoS 공격 활동 수준은 전반적으로 안정세를 유지했습니다.

글로벌 트렌드를 살펴보면 레이어 7 DDoS 공격의 주요 표적이 된 업계 중 커머스는 각 지역에서 API에 대한 공격 집중도가 가장 높았습니다. EMEA 지역에서 커머스 업계를 표적으로 한 공격의 43%가 API를 표적으로 삼았으며 LATAM에서는 21%, APJ에서는 16%였습니다.

지정학적 혼란과 가시성이 높은 서비스 중단 of 잠재적 경제적 영향 등의 이유로, 커머스, 미디어, 금융 서비스 업계는 지난 2년간 EMEA와 LATAM에서 레이어 7 DDoS 공격의 주요 표적이 되었습니다. 커머스 및 금융 서비스 업계에 대한 높은 활동 수준의 배경과 방법에 대한 자세한 논의는 [업계 트렌드](#) 섹션을 참조하세요.

## 컴플라이언스

### 글로벌 및 북미 지역 관점

2025년 글로벌 사이버 보안 환경은 전례 없는 복잡성과 변동성이 특징입니다. 지정학적 긴장, 특히 우크라이나와 중동에서의 분쟁이 계속됨에 따라 사이버 위협과 국가 후원 공격이 강화됐습니다. 친러시아 그룹이 서방 국가를 표적으로 한 해킹이 확산되면서 위협 환경이 더욱 복잡해졌습니다. 경제적으로는 업계 전반에 걸쳐 디지털 전환이 가속화되면서 공격 표면이 확대됐으며 사이버 범죄자들이 핵심 인프라를 표적으로 삼고 AI와 같은 고급 기술을 활용해 능력을 강화하고 있습니다.

이러한 요인들이 글로벌 경제 압력과 주요 국가의 정치적 변화와 결합되어 완벽한 위기가 전 세계 사이버 보안 전문가를 뒤흔쳤습니다. 기업에게 웹 애플리케이션과 API를 보호하는 것이 필수 과제입니다. 이러한 엔트리 포인트를 보호하기 위한 윤리적 해커, 사이버 보안 전문가, Akamai와 같은 기업의 노력은 나날이 커지는 컴플라이언스 요구사항을 보완합니다.

전 세계 규제 기관은 애플리케이션에 대한 사이버 보안 컴플라이언스 요건을 강화하고 있습니다. 북미 지역에서는 포괄적인 리스크 관리 전략과 의무적 인시던트 보고로 초점이 이동했습니다. 미국에서는 2026년에 시행될 예정인 [핵심 인프라 사이버 인시던트 보고법](#)에 따라 핵심 인프라 기업은 정보 시스템을 목록화하고, 사이버 리스크를 분류하고, 연간 최소 한 번 이상 사이버 보안 체계를 평가해야 합니다. 해당 법은 특히 에너지, 화학 제조, 정보 기술 등 핵심 부문에서 사용되는 애플리케이션에 대한 강력한 보안 조치의 필요성을 강조합니다.

미국과 마찬가지로 캐나다와 멕시코도 국제 기준에 맞춰 규정을 조정하고 있으며 데이터 보호와 핵심 인프라 보안에 중점을 두고 있습니다. 구체적인 규정은 국가별로 다르지만 전 세계적인 트렌드는 강화된 입력 검증, 안전한 개발 관행, 정기적인 보안 감사 등을 포함하는 애플리케이션에 대한 보안 요구사항을 강화하는 방향으로 나아가고 있습니다.

API 보안 환경은 유사한 도전 과제에 직면하고 있습니다. API는 서비스 통합과 데이터 교환을 가능하게 하는 핵심 역할을 하기 때문에 사이버 범죄자들의 주요 표적이 되고 있습니다. 전 세계 규제 기관은 [보다 엄격한 규제](#)를 도입해 기업에 강력한 API 보안 조치를 구축하도록 하며 대응하고 있습니다.

여기에는 API의 지속적인 탐지, 모니터링, 진화하는 위협에 대한 보호 조치가 필수적으로 포함됩니다. 북미 지역에서는 API 생태계의 철저한 리스크 평가에 초점을 맞추고 있으며 안전한 개발 관행, 강력한 인증 메커니즘, 실시간 위협 탐지 능력을 강조하고 있습니다. 종종 API를 통해 통합되는 AI 기반 SaaS 툴의 빠른 확산으로 공격 표면이 크게 확대됨에 따라 규제 당국이 더 정교한 보안 접근 방식을 요구하고 있습니다.

특히 AI와 머신 러닝 애플리케이션의 확산으로 인해 API 환경의 복잡성이 증가함에 따라 데이터 유출, 무단 접속, 서비스 중단과 관련된 리스크를 방어하기 위해 컴플라이언스 요구사항이 진화하고 있습니다. APJ, LATAM, EMEA와 같은 지역은 자체 규정을 개발 중이지만 현대 디지털 아키텍처의 상호 연결성을 처리하기 위해 API 보안 표준을 조정하는 글로벌 트렌드가 강화되고 있습니다.

## APJ의 관점

APJ 지역은 다양한 부문의 기업에 영향을 미치는 새로운 컴플라이언스 의무가 도입되며 규제 환경의 큰 변화를 겪고 있습니다. 싱가포르의 최근 [사이버 보안법](#)을 개정하며 규제 범위를 물리 및 가상 핵심 정보 인프라 시스템으로 확대해 클라우드 플랫폼에 호스팅되고 [해외](#)에 위치한 시스템도 포함시켰습니다. 일본은 [사이버 보안 대응 및 전략 국가 센터 관련 법안](#)을 개정했으며 인도는 [디지털 개인 데이터 보호 법안](#)을 통과시켜 IT 법을 전면 개편했습니다. 호주는 2023-2030년 사이버 보안 전략을 발표하며 지역의 사이버 보안 강화에 대한 초점을 더욱 강조했습니다. 호주는 이러한 전략의 일환으로 2024년 말 중요 인프라 보안법을 개정하고 [2024년 사이버 보안법](#)을 제정해 IoT 디바이스, 애플리케이션, API 등 민감한 데이터를 처리하는 2차 자산도 관련 법의 적용을 받게 했습니다. 이러한 규제 변화는 특히 핵심 인프라와 민감한 데이터 보호에 중점을 두고 웹 애플리케이션 보안 관행을 재평가하고 강화할 것을 기업에 촉구하고 있습니다.

[PCI DSS v4.0.1](#)은 결제 카드 데이터를 처리하는 기업에 큰 영향을 미칠 것으로 예상되며 컴플라이언스 마감일은 2025년 3월 31일입니다. 새로운 버전은 소비자의 브라우저에서 실행되는 모든 결제 페이지 스크립트에 대한 제어 조치를 구축하고 웹 기반 공격을 지속적으로 탐지하고 방지하기 위한 자동화된 기술 솔루션을 사용하는 내용을 포함해 더 엄격한 웹 애플리케이션 요구사항을 도입했습니다. APJ 지역 내 기업은 웹 애플리케이션의 강화된 보안 기준을 충족하기 위해 철저한 격차 분석을 수행하고, 보안 정책을 업데이트하고, 필요한 기술적 변경을 구축해야 합니다.

APJ 지역에서는 API 측면에서 오픈 뱅킹 이니셔티브의 확산이 부분적인 원인이 되어 API 보안에 대한 관심이 증가하고 있습니다. APJ 지역은 EMEA 지역의 수준까지 오픈 뱅킹 규제를 완전히 도입하지는 않았지만 APJ 국가는 API **보안 우려**를 선제적으로 해결할 기회가 있습니다. 2024년 8월 APJ 지역에서 실시된 API 보안 인사이트 **조사** 결과, 내부 API가 가장 널리 사용되고 있으며 API 접속 제어와 관련하여 외부 사용자 접속이 여전히 우려되고 있습니다. 따라서 기업은 강력한 인증 및 권한 확인 프로토콜, 데이터 암호화, 지속적인 API 발견 및 모니터링을 포함한 강력한 API 보안 조치를 구축해야 합니다. APJ 지역이 **오픈 뱅킹** 규정을 도입함에 따라 기업은 진화하는 규제를 준수하고 새로운 위협으로부터 보호하기 위해 API 보안을 우선순위로 삼아야 합니다.

## EMEA의 관점

EMEA 지역의 사이버 보안 환경은 지정학적 긴장, 기술적 진보, 규제 변화의 복잡한 상호작용으로 인해 급격한 변화를 겪고 있습니다. 우크라이나와 중동에서 지속적인 분쟁으로 인해 사이버 위협과 국가 후원 공격이 강화되는 등 독특한 도전 과제에 직면하고 있습니다. 또한, 특히 유럽 국가를 표적으로 삼는 친러시아 그룹의 해티비즘 확산으로 EMEA 지역은 정치적 동기의 사이버 작전의 주요 표적이 되었습니다.

EMEA 지역의 API 환경도 유사한 도전 과제에 직면하고 있습니다. API는 서비스 통합과 데이터 교환을 구현하는 데 핵심 역할을 맡고 있어 사이버 범죄자의 주요 표적이 되었습니다. 종종 API를 통해 통합되는 AI 기반 SaaS 툴의 급속한 도입으로 공격 표면이 크게 확대되었습니다.

유럽 연합은 이렇게 고조되는 위협에 대응해 포괄적인 사이버 보안 규정을 도입했습니다. 2025년 1월부터 시행되는 개정된 **NIS2(Network and Information Security) 지침**은 적용 범위를 18개 핵심 부문으로 확대하며 중견 및 대기업에 엄격한 사이버 보안 조치를 의무화합니다.

금융 부문에서는 2025년 1월 17일부터 시행되는 **DORA(Digital Operational Resilience Act)**가 NIS2를 대체하며 금융 서비스에 사용되는 애플리케이션에 대한 강력한 정보 및 통신 기술 리스크 관리 프레임워크, 인시던트 보고 메커니즘, 디지털 운영 안정성 테스트 프로그램을 요구합니다. 또한 2025년 3월 31일부터 의무화된 **PCI DSS v4.0.1**은 진화하는 보안 요구사항, 지속적인 보안 프로세스, 유연한 방법론, 강화된 검증 절차를 중심으로 새로운 컴플라이언스 요건을 도입합니다. 앞으로 도입될 **EU PSD3(Payment Services Directive)**는 PSD2의 부족한 점을 보완하기 위해 데이터 공유 메커니즘 강화, 보안 요건 강화, 금융 서비스 부문의 감독 강화 등을 목표로 합니다.

2024년 12월 10일에 발효된 [CRA\(Cyber Resilience Act\)](#)는 유럽 연합에서 판매되는 디지털 요소를 포함한 제품에 대한 필수 사이버 보안 기준을 도입했습니다. 이에 따라 제조사는 커넥티드 제품의 전체 수명 주기 동안 보안 조치를 구축해야 합니다. CRA에 따르면 애플리케이션 개발자와 사용자의 주요 리스크 기법에 스마트폰과 태블릿이 포함됩니다. 이에 따라 기업은 모바일 단말기를 전체 사이버 보안 전략의 핵심 구성요소로 간주하고 애플리케이션 라이프사이클 전반에 걸쳐 엄격한 보안 조치를 구축해야 합니다.

영국에서는 [사이버 보안 및 안정성 법안](#)을 곧 시행해 사이버 방어 체계를 강화하고 필수 공공 서비스를 보호할 것입니다. 이에 따라 레거시 규제 프레임워크가 대폭 개정돼 보호 대상 디지털 서비스 및 공급망의 범위가 확대되고, 집행력이 강화되며, 보고 요건이 늘어날 것입니다.

## LATAM 관점

LATAM의 사이버 보안 환경은 글로벌 기술 트렌드와 LATAM 지역만의 경제 및 정치적 도전 과제에 의해 빠르게 변화하고 있습니다. 이러한 맥락에서 시스템의 상호 연결이 증가함에 따라 취약점이 발생하고 LATAM 국가들이 급속히 디지털로 전환함에 따라 LATAM 지역은 사이버 범죄자와 국가 후원 공격자의 매력적인 표적이 되었습니다. 커머스 및 금융 서비스 부문은 사이버 공격의 주요 표적으로 부상했습니다. 온라인 리테일 기업, 결제 처리업체, बैं킹, 보험사, 핀테크 스타트업, 암호화폐 거래소는 디지털 인프라, 특히 웹 애플리케이션과 API를 겨냥한 위협에 특히 [취약](#)합니다.

LATAM 국가가 이러한 도전 과제를 인식하고 사이버 보안 규제의 개발 및 시행에서 중요한 진전을 이룸에 따라 웹 애플리케이션 및 API 보안에 대한 관심이 점점 더 높아지고 있습니다. 브라질은 데이터 보호 및 보안에 대한 엄격한 [요건](#)을 포함한 LGPD(Lei Geral de Proteção de Dados Pessoais)를 시행하며 선도적인 역할을 맡았습니다. LGPD는 웹 애플리케이션이나 API를 구체적으로 다루지 않지만 기업에 디지털 인터페이스의 보안을 포함해 전체 사이버 보안 체계를 강화할 것을 촉구했습니다.

칠레도 [사이버 보안 기본법](#)을 제정하고 2025년 1월 1일부터 시행했습니다. 사이버 보안 기본법은 국가 사이버 보안 기관의 설립을 명시하고, 웹 애플리케이션과 API에 크게 의존하는 부문을 포함해 다양한 부문에서 사이버 보안 인시던트를 예방하고, 보고하고, 해결하기 위한 포괄적인 조치를 규정합니다. 2025년 1월 아르헨티나도 [사이버 범죄 예방 및 사이버 보안 전략 관리 연방 계획\(2025-2027\)](#)을 발표했습니다.

API 관련 규제 부문에서 긍정적인 진전이 이루어지고 있습니다. 일례로 멕시코는 핀테크를 포함한 금융 부문에 초점을 둔 **법안**을 시행했으며 신용정보기관과 청산기관이 안전한 API를 개발하도록 상세한 요구사항을 규정했습니다. 이러한 접근 방식은 현대 디지털 생태계에서 API가 수행하는 핵심적인 역할과 맞춤형 보안 조치의 필요성에 대한 인식이 높아지고 있음을 반영합니다. 또한 멕시코의 **개인정보를 보유한 민간 기관의 개인정보 보호에 관한 연방법**은 개인이 보유한 개인정보의 처리 과정을 규제하며 기업 및 기관에 대한 의무를 규정하고 있습니다.

콜롬비아도 규제 **프레임워크**를 강화해 공공 기관에 대한 사이버 보안 공공 정책을 발표하고 다양한 수준의 인시던트 대응 보고 체계를 갖춘 디지털 보안 리스크 관리 시스템을 구축함으로써 법의 범위를 확대했습니다. API에 특화되지 않았지만 이러한 조치들은 기업 내 API 보안 관행에 불가피하게 영향을 미칠 것입니다.

지역 전반에서 업계별 **이니셔티브** 도입이 증가하는 트렌드에는 소비자 데이터를 보호하기 위해 API 보안 기준을 설정하는 오픈 파이낸스 프레임워크 등이 있습니다. 이러한 프레임워크는 금융 부문에 특히 중요합니다. API의 보안은 금융 거래의 무결성을 유지하고 민감한 고객 정보를 보호하는 데 필수적이기 때문입니다. LATAM 국가가 보안 강화에 우선순위를 두고 사이버 보안 규정을 국제 표준과 일치시킴에 따라 웹 애플리케이션 및 API 보안에 대한 더 포괄적이고 구체적인 지침이 등장할 것으로 예상됩니다.



## 방어

진화하는 위협 환경에서 더 정교한 공격 기술이 증가함에 따라 기업은 웹 애플리케이션과 API를 필수적으로 보호해야 합니다. 이에 따라 Akamai는 다음과 같은 보호 및 방어 기술을 추천합니다.

- **포괄적인 API 보안 계획 수립:** API 설계부터 프로덕션 후 단계까지 보안을 통합하는 시프트 레프트 및 DevSecOps 접근 방식을 구축합니다. 숨겨진 API(새도, 레거시, 좀비 API)를 포함해 전체 공격 표면을 이해하기 위해 지속적인 [검색](#) 및 가시성을 확보합니다. 엄격한 인증 및 권한 확인(OAuth 2.0, mTLS, 역할 기반 접속 제어/속성 기반 접속 제어), 속도 제한, 봇 방어 조치를 통해 보안을 강화해 악용을 방지합니다. 실시간 위협 탐지, 비정상 모니터링, 런타임 보호 기능을 구축해 공격이 발생하면 즉시 탐지하고 차단합니다. DORA, GDPR, HIPAA, NIS2, PCI DSS 등의 규제를 준수하면서 API 거버넌스 정책을 적용해 대규모 환경에서도 보안을 유지합니다.
- **강력한 사이버 보안 조치 구축:** 실시간으로 위협을 모니터링하고 대응하며 위협 인텔리전스와 [런타임 보호](#)를 제공하는 [적응형 보안 엔진](#)을 사용합니다. 또한 DAST(Dynamic Application Security Testing)와 같은 [API 테스트 툴](#)을 사용해 안전한 접속, 암호화, 인증 등의 보안 요구사항이 충족되도록 지원합니다.
- **선제적 위협 방어:** [전문 DDoS 보호 툴](#) 사용, 속도 제한 및 CDN 캐싱 설정, 패치 관리, 접속 제어 정책, 네트워크 세그멘테이션 같은 조치를 구축합니다. 또한 DNS 인프라를 지속적인 트래픽 모니터링 및 하이브리드 플랫폼으로 보호합니다.
- **API 취약점 방어:** [OWASP](#)에서 제공하는 보안 지침과 같이 확립된 가이드라인을 준수해 강력한 API 보안을 확보하고, 해커가 무단 접속 권한을 얻거나 데이터를 조작하는 등의 악용할 수 있는 취약점을 형성할 가능성이 있는 API 아키텍처의 부적절한 코딩 관행 및 설정 오류 리스크를 해결합니다.

- **랜섬웨어 위협 방어:** 멀티레이어 접근 방식을 통해 랜섬웨어에 대응합니다. 제로 트러스트 솔루션을 구축해 악성 트래픽을 차단하고, 마이크로세그멘테이션을 통해 상세한 가시성과 정밀한 접속 제어를 구축하고, [MITRE ATT&CK 프레임워크](#)를 활용해 공격 패턴을 이해하고 대응 전략을 강화합니다.
- **AI 대비:** [봇 방어 솔루션](#), AI 기반 보안 툴, 전문 방화벽, 지속적인 평가 및 제로 트러스트 모델과 같은 사전 예방 조치를 포함한 포괄적인 방어 전략을 수립해 [AI의 사용 증가](#)로 인한 새로운 보안 리스크에 대응합니다. 다각적인 접근 방식으로 AI 시스템 보호: 모델과 데이터 세트에 대한 이해를 통해 프롬프트 인젝션과 데이터 포이즈닝 같은 특정 위협에 대응하고, 사전 취약점 테스트를 수행하고, 통합된 행동 모니터링, 콘텐츠 검증, 자동화된 공격 대응과 같은 강력한 방어 조치를 개발 및 런타임 환경 전반에 적용합니다.

## 방법론

### 웹 애플리케이션 및 레이어 7 DDoS 공격

이 데이터는 웹 애플리케이션 방화벽(WAF)을 통해 관측된 트래픽에 대한 애플리케이션 레이어 알림을 설명합니다. 애플리케이션 공격 알림은 보호하고 있는 웹사이트, 애플리케이션, API에 대한 요청에서 악성 페이로드를 탐지하면 트리거됩니다. 레이어 7 DDoS 알림은 보호하고 있는 웹사이트, 애플리케이션, API에 대한 요청 건수에서 대규모 비정상성을 탐지하면 트리거됩니다. 이러한 알림은 악성 요청과 정상 요청 모두에 의해 트리거될 수 있습니다. 일반적으로 요청 자체는 정상이지만 요청의 양이 많다는 것은 악의적인 의도가 있음을 시사합니다. 알림이 트리거됐다고 해서 공격이 성공한 것은 아닙니다. 이러한 제품은 높은 수준의 사용자 맞춤화가 가능하지만 Akamai가 여기에 제공한 데이터는 프로퍼티의 맞춤형 설정을 고려하지 않는 방식으로 수집했습니다.

이 데이터는 130여 개국 약 1300개 네트워크, 4000개 이상의 위치, 약 34만 대의 서버로 구성된 Akamai 클라우드에서 탐지된 보안 이벤트를 분석하는 내부 툴에서 추출한 것입니다. Akamai 보안 팀은 매달 페타바이트 규모의 데이터를 활용해 공격을 연구하고, 악성 행동을 식별하며, Akamai 솔루션에 인텔리전스를 추가합니다.

이 데이터는 2023년 1월 1일부터 2024년 12월 31일까지 24개월의 기간을 포괄합니다.

### API 보안 공격 데이터

Akamai는 Noname Security와의 통합을 통해 API 위협 리서치 및 보고 기능을 강화했습니다. 데이터 세트는 통합 및 분석의 초기 단계에 있습니다. 이 보고서를 위해 2025년 1분기 30일 데이터 샘플을 추출하고 API 보안 알림의 분포를 해당 보안 프레임워크 및 컴플라이언스 기준에 따라 분석했습니다. 데이터 세트를 계속 발전시켜 향후 API 보안 문제에 대한 확장된 관점을 제공할 것입니다.



## 크레딧

### 리서치 책임자

미치 메인(Mitch Mayne)

### 편집 및 작성

샬럿 펠리시아(Charlotte Pelliccia)

바데트 트리베이(Badette Tribbey)

랜스 로즈(Lance Rhodes)

마리아 블라삭(Maria Vlasak)

### 검토 및 주제별 기여

톰 에몬스(Tom Emmons)

스타스 네이만(Stas Neyman)

루벤 코(Reuben Koh)

스티브 윈터펠트(Steve Winterfeld)

리차드 메우스(Richard Meeus)

### 데이터 분석

첼시 터틀(Chelsea Tuttle)

### 홍보 자료

바니 벨(Barney Beal)

애슐리 리나레스(Ashley Linares)

### 마케팅 및 출판

조지나 모랄레스 햄프(Georgina Morales Hampe)

에밀리 스텍스(Emily Spinks)

## 인터넷/보안 현황 보고서

Akamai의 지난 인터넷 보안 현황 보고서를 읽고 다음 보고서를 확인하세요.

[akamai.com/soti](https://akamai.com/soti)

## Akamai 위협 연구팀

[akamai.com/security-research](https://akamai.com/security-research)에서 최신 위협 인텔리전스 분석, 보안 보고서, 사이버 보안 리서치 내용을 확인하세요.

## 이 보고서의 데이터 확인

이 보고서에 참조로 사용된 그래프와 차트의 고품질 버전을 확인하세요. Akamai가 제공한 소스라는 점이 정식으로 인정되고 Akamai 로고가 보존되는 경우 이러한 이미지를 무료로 사용 및 참조할 수 있습니다.

[akamai.com/sotidata](https://akamai.com/sotidata)

## Akamai 보안 리서치

Akamai 보안 리서치 블로그를 읽고 오늘날 가장 중요한 리서치에 대한 신속한 대응 관점을 확인하세요. [akamai.com/blog/security-research](https://akamai.com/blog/security-research)



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](https://akamai.com), [akamai.com/blog](https://akamai.com/blog)를 방문하거나 X(기존의 Twitter)와 LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 04월 25일 발행.