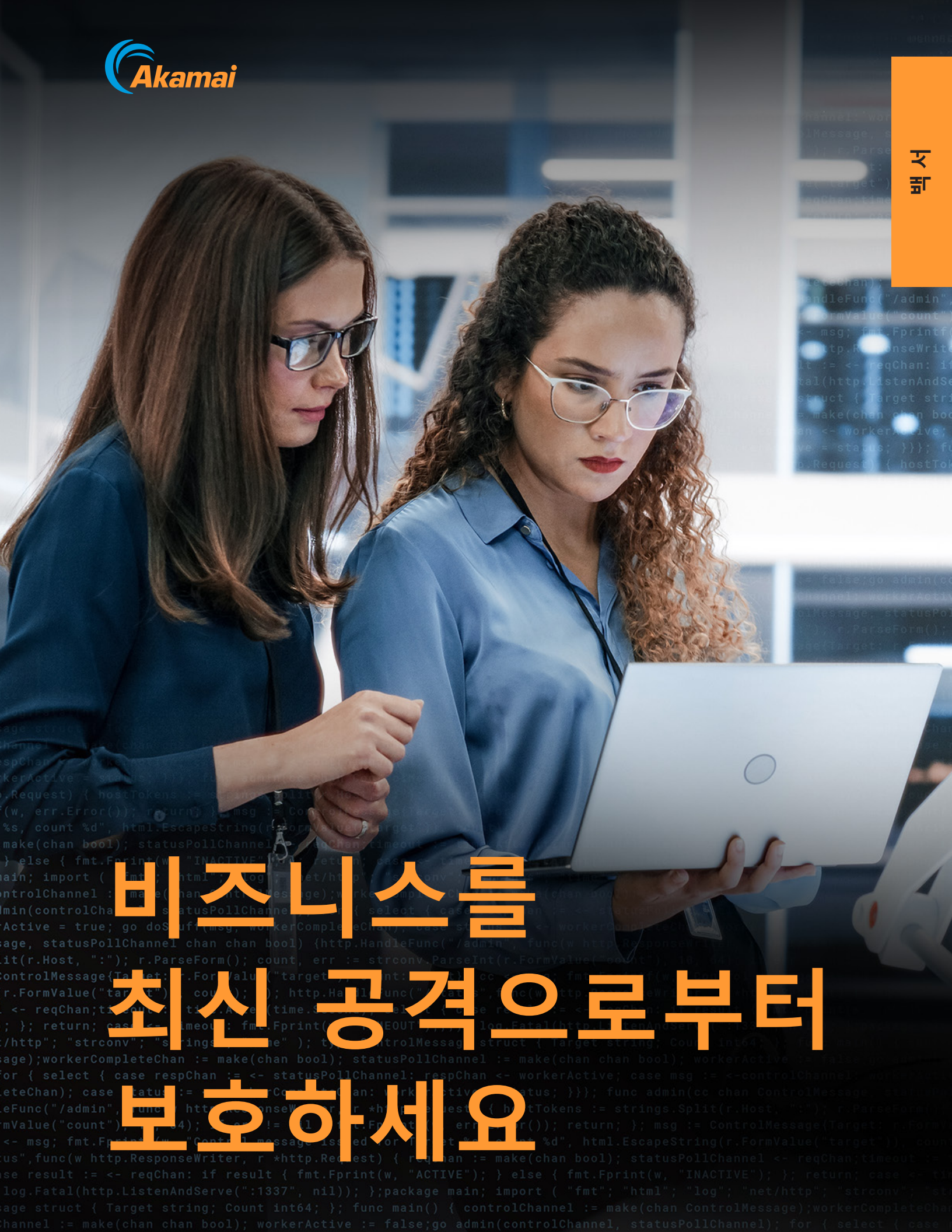
Akamai

백서



비즈니스를 최신 공격으로부터 보호하세요

IT 환경이 복잡해짐에 따라 사이버 공격도 새로운 취약한 지점을 이용하도록 변화했습니다. 애플리케이션, API, 마이크로서비스 및 구성요소는 지속적으로 확장되고 있으며 온라인 사업 운영 방식도 바뀌고 있습니다. 안타깝게도 이러한 변화로 공격자가 악용할 수 있는 새로운 취약점과 위협 표면이 생겨났습니다. 사이버 보안 솔루션은 내부에 존재하는 위협(자체 데이터 보안)과 외부에 존재하는 위협(랜섬웨어, DDoS, 리소스 고갈 및 기타 공격 차단)을 모두 해결해야 합니다.

Akamai는 이를 잘 알고 있습니다. Akamai 연구원은 매일 평균 788TB의 데이터를 분석하고, 습득한 지식을 바탕으로 제품을 계속 혁신해 공격이 진화하는 상황에서도 가장 위험한 공격자와 진화하는 캠페인으로부터 고객과 고객의 사용자를 보호해야 하기 때문입니다.

기업이 직면할 수 있는 가장 위험한 공격은 무엇이며, 이에 대비하려면 어떻게 해야 할까요?

랜섬웨어의 증가

고객과 고객 사용자의 데이터에 대한 접속 손실은 기업에 가장 큰 위협입니다. Akamai의 멈추지 않는 랜섬웨어 보고서에 따르면, 2022년 1분기와 2023년 1분기 사이에 랜섬웨어 공격 건수는 전 세계적으로 143%, 공격자는 제로데이 및 원데이 취약점을 악용합니다. 최신 공격의 가능성과 영향은 세그멘테이션을 통해 줄일 수 있습니다.

세그멘테이션은 성능 및 보안 강화를 위해 네트워크를 더 작은 세그먼트로 나누는 아키텍처 접근 방식입니다. 한편, 마이크로세그멘테이션은 네트워크를 개별 워크로드 수준까지 구분된 보안 세그먼트로 논리적으로 분할할 수 있는 보안 기술입니다. 그리고 고유한 각 세그먼트에 대해 보안 제어 및 서비스 전송을 정의할 수 있습니다.

Akamai Guardicore Segmentation은 제로 트러스트를 위한 Akamai Guardicore Platform의 일부로, 모든 중요 시스템에 대한 공격을 차단해 자산에서의 확산(동서 방향 이동)을 차단하고 대응과 복구를 강화합니다. 이를 통해 유출로 인한 평판 손상, 데이터 손실, 매출 손실을 방지할 수 있습니다.

Akamai Guardicore Platform은 마이크로세그멘테이션을 위한 에이전트리스 솔루션으로 네트워크를 물리적으로 변경하거나 서버와 디바이스가 어디에 있는지 걱정하지 않고 빠르고 쉽게 배포할 수 있습니다. 네트워크의 모든 연결에 대해 인터랙티브한 시각 정보를 생성해 배포의 주요 장애물 중 하나인 가시성 부족 문제를 해결할 수 있습니다. 또한, Akamai는 잠재적인 성능 병목 현상과 컴플라이언스 요구사항을 해결하는 능동적인 방법과 다양한 종류의 인프라를 포괄할 수 있는 정책 적용을 구축했습니다. 이로써 단일 플랫폼을 통해 여러 환경에 대한 다양한 가시성을 제공하고 세분화된 제어를 지원할 수 있습니다.

Akamai는 대규모로 분산된 글로벌 네트워크 전반의 온라인 트래픽에 대한 탁월한 가시성을 제공합니다. Akamai Guardicore Platform은 이를 활용해 자체 환경, 자산, 접속 및 네트워크 흐름에 대한 심층적인 가시성을 제공합니다. 이러한 실시간 정보를 바탕으로 고객은 비즈니스 중단에 대한 걱정 없이 운영을 지속할 수 있습니다.

공격받는 앱과 API

기업에서 현재 몇 개의 애플리케이션을 사용 중이신가요? 현재 알고 계신 것보다 분명 더 많을 것입니다. 기업은 평균적으로 1000개가 넘는 앱을 사용합니다. 거의 모든 온라인 트랜잭션은 API에 대한 의존도가 높고, 마이크로서비스 기반 아키텍처의 도입이 증가함에 따라 앱은 점점 더 복잡해질 것입니다. 하지만 혁신을 통해 빠르게 성장해야 한다는 부담 때문에 기업은 잠재적인 보안 문제에 대한 엄격한 테스트를 진행하기도 전에 앱을 출시해야 하며, 이로 인해 전체 애플리케이션 생태계에 더 많은 리스크가 발생합니다.

Akamai의 최근 인터넷 보안 현황 보고서에 따르면, 글로벌 공격의 29%는 대체로 디지털 혁신의 핵심인 API(Application Programming Interface)를 표적으로 삼습니다. 유럽, 중동 및 아프리카 지역에서 이 비율은 47%가 조금 넘는 것으로 나타났습니다. 기존의 기술과 API 전용 기술을 모두 이용하는 API는 사이버 범죄자가 일반적으로 활용하는 기법이며 봇, DDoS(Distributed Denial of Service) 공격, 멀티 기법 공격을 모두 고려해야 합니다.

Akamai App & API Protector로 웹 애플리케이션을 보호하면 악성 활동과 사기로부터 워크플로우, 사용자, 기업을 보호할 수 있습니다. 이 솔루션은 API를 통해 시작된 공격을 비롯해 애플리케이션 레이어를 겨냥한 공격을 흡수할 수 있는 설정 가능한 방화벽 보안 기능을 제공합니다. 봇 트래픽에 대한 실시간 가시성을 통해 왜곡된 웹 애널리틱스를 조사하고, 오리진 부하 분산을 방지하며, 권한을 사용자 지정해 써드파티 및 파트너 봇에 아무런 방해 없이 접속할 수 있습니다.

하지만 원래 질문으로 돌아가서 앱과 API 모두에 대한 정보가 없다면 어떨까요? 이때도 가시성이 중요합니다. Akamai API Security는 모든 API를 식별하고, 리스크 수준을 평가하며, 공격에 대응합니다. 이를 통해 공격자가 사용자의 데이터에 접속하거나, 서버에 악성 파일을 로드하거나, 트래픽 폭주로 서버가 마비되는 것을 방지할 수 있습니다.

DDoS 및 리소스 고갈 방어

DDoS 공격은 가장 잘 알려진 대규모 온라인 위협입니다. 인터넷이 연결된 모든 곳에 DDoS 공격 가능성이 존재하며, 온라인에 있는 모든 것들이 공격의 영향을 받을 수 있습니다. DDoS 공격은 최근 몇 년 동안 규모가 커지고 지속 시간이 길어졌으며 여러 공격 기법과 목적지를 이용하면서 더 정교해졌습니다. 2021년에서 2023년 사이에 대규모 DDoS 공격 건수는 50% 증가했으며, 2023년 전체 DDoS 공격 중 DNS 구성요소를 이용한 건수는 60%가 넘습니다.

대기업도 이러한 적대적인 봇넷으로부터 안전하지 않습니다. 수백만 고객에게 제공되는 서비스와 사업 운영이 중단될 수 있습니다. 많은 리소스를 갖춘 사이버 범죄자, 국가 주도의 공격자, 지정학적 동기를 가진 핵티비스트는 대규모 분산형 봇넷을 이용해 대규모 기업은 물론, 학교, 병원에서 공항, 공공 서비스 공급업체에 이르는 핵심 공공 기관을 공격합니다. 파괴력이 큰 DDoS 및 리소스 고갈 공격은 모든 레이어, 포트, 프로토콜, 심지어 기업과 기관의 DNS까지 겨냥합니다.

알고 계셨나요?

2021년에서 2023년 사이에 DDoS 공격 50% 증가

2023년 전체 DDoS 공격의 60% 이상이 DNS 구성요소를 이용

DDoS 공격으로부터 인프라를 보호하려면 실시간 위협 인텔리전스가 필요합니다. 수집된 데이터는 DDoS 공격 차단 및 방어 솔루션인 Prolexic을 지원하는 데 사용됩니다. Prolexic은 기업의 디지털 애플리케이션과 경험을 뒷받침하는 기본 디지털 인프라를 보호할 수 있으며, 클라우드나 온프레미스 또는 양쪽 환경에서 모든 포트와 프로토콜에 걸친 공격이 기업에 영향을 미치기 전에 차단합니다.

최근 몇 년 동안 기업의 DNS 인프라를 겨냥한 리소스 고갈 공격이 다시 크게 증가했습니다. DNS는 온라인 사업 운영의 기본 구성요소입니다. DNS 시스템이 다운되면 기업의 온라인 보안이 무너집니다. Akamai Edge DNS 및 Shield NS53은 엣지에서 DNS 리소스 고갈 트래픽을 차단하고 정상적인 DNS 쿼리만 고객의 오리진에 도달하도록 허용합니다.

공격 규모가 2년마다 두 배로 증가하고 복잡성도 커지면서 DDoS 방어는 온라인 사업 운영에서 오랫동안 중요한 요소로 작용해 왔습니다. 매출과 고객의 신뢰를 잃지 않으려면 잠재적인 모든 장애 지점을 보호해야 합니다.

공격이 발생하면 어떻게 될까요?

디지털 보안을 구축했다면 언젠가 공격을 받을 수 있다고 가정하는 것이 안전합니다. 보안 전략의 한 가지 목적은 공격이 시작되기 전에 공격 대상을 보호하는 것입니다. 네트워크에 대한 가시성을 바탕으로 중요한 자산을 보호해 공격 대상을 줄이고, 이를 통해 현재 상황을 파악하여 공격이 시작될 때 이를 탐지할 수 있어야 합니다.

하지만 제로데이 공격과 같은 일이 발생하면 어떨까요? 이 경우 Akamai App & API Protector와 같은 솔루션의 핵심인 행동 분석이 중요한 역할을 합니다.

Akamai는 고도로 자동화된 솔루션과 머신 인텔리전스를 글로벌 SOCC(Security Operations Command Center)에서 근무하는 225명이 넘는 현장 대응 인력의 휴먼 인텔리전스와 결합해 고객의 데이터, 인프라, 최종 사용자의 디지털 경험을 보호합니다.

Akamai는 매일 13조 건이 넘는 DNS(도메인 네임 시스템) 쿼리를 검토하고 분기마다 120억 건이 넘는 WAF(웹 애플리케이션 방화벽) 공격을 방어합니다. Akamai는 현재 상황을 파악하고 고객사와 함께 다양한 경험을 쌓았으며 공격 분석을 바탕으로 솔루션을 강화해 왔습니다. Akamai는 위협 인텔리전스를 통해 솔루션의 대응 능력과 효율성을 높입니다.

Akamai의 보안 솔루션을 사용하고 있지 않더라도 공격을 받았다면 사이버 위협 핫라인을 통해 Akamai에 문의할 수 있습니다. 보안 전문가가 현재 공격을 방어하기 위한 다음 단계를 알려 드릴 것입니다.

비즈니스가 이루어지는 모든 곳을 안전하게 보호하세요

죽음과 세금 그리고 사이버 공격의 공통점은 아무도 피할 수 없다는 것입니다. 하지만 최신 위협 인텔리전스를 활용하고, 앱 및 네트워크에 대한 높은 가시성을 제공하며, 위협 환경과 함께 진화하는 보안 솔루션으로 기업과 고객을 보호할 수 있습니다.

Akamai는 어디에서 구축하고 제공하든지 생성하는 모든 것에 보안 기능을 내장하도록 지원함으로써 고객 경험, 시스템, 데이터를 보호합니다. Akamai의 광범위한 솔루션 포트폴리오는 글로벌 플랫폼의 위협 가시성을 활용해 업계 최고 수준의 안정성을 지원하기 때문에 기업은 위협에 대비하고 변화하는 보안 환경에 신속하게 적응할 수 있습니다.

추가 리소스

랜섬웨어 킬 체인 차단을 위해 취해야 할 5단계를 알아보세요

DDoS 공격을 차단하면서 하이브리드 클라우드 전략을 지원하세요

강력한 API 보안으로 비즈니스의 구성요소를 방어하세요

Akamai는 구축 및 전송되는 장소에 상관 없이 만들어지는 모든 것에 보안 기능을 내장하도록 지원함으로써 고객 경험, 직원, 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 있도록 지원합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관해 자세히 알아보려면 akamai.com와 akamai.com/blog를 확인하거나 X(기존의 Twitter), LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2024년 6월 발행.