Akamai

하이브리드 클라우드 환경에서 DDoS 공격 방어하기

목차

지속적으로 발전하고 있는 DDoS

가장 오래된 사이버 위협 종류 중 하나인 분산 서비스 거부(DDoS)는 계속 발전하고 있으며, 이제는 사이버 범죄자와 이념적 동기를 가진 핵티비스트의 손에 고도로 정교한 툴이 되었습니다. 실제로 DDoS 공격은 대기업 및 중소기업뿐만 아니라 헬스케어, 에너지 및 유틸리티, 교육 등의 분야에서 중요한 공용 인프라에 보안상 리스크가 되고 있습니다.

또한, 공공 기관과 민간 기관 모두에서 클라우드 컴퓨팅 리소스를 점점 더 많이 도입하고 있어 이러한 상황이 더 복잡해지고 있습니다. 이들 조직이 기존 온프레미스 리소스와 클라우드를 결합하면 하이브리드 환경이 훨씬 복잡해집니다. 이에 따라 이제는 애플리케이션, 애플리케이션 프로그래밍 인터페이스(API), 데이터, 마이크로서비스 및 워크로드가 세분화된 환경을 거쳐 이동해야 하는 실정입니다. 이러한 환경의 다양한 아키텍처로 인해 새로운 취약점과 분열된 공격표면이 발생하며, 사이버 범죄자들은 이를 악용해 점점 더 정교하고 방어력을 약화시키는 DDoS 공격을 실행할 수 있습니다.

기업은 디지털 인프라를 보호하기 위해 고군분투하고 있습니다. 이들은 짧지만 예리한 DDoS 공격으로부터 온프레미스(프라이빗 클라우드) 인프라를 보호하는 동시에 대규모 증폭 DDoS 공격에 대비해 클라우드 스크러빙의 규모와 용량을 활용할 수 있는 통합형 하이브리드 DDoS 방어 플랫폼이 필요합니다.

트렌드를 보면 DDoS 공격이 더욱 강력해지고 자주 발생할 것이라는 점을 알 수 있습니다. 2023년 2월, Akamai는 아시아 태평양(APAC) 지역에 기반을 둔 Akamai Prolexic 고객을 대상으로 최고 시점에 초당 900.1기가비트, 초당 1억 5820만 패킷(Mpps)의 공격 트래픽을 기록한 사상 최대 규모의 DDoS 공격을 방어했습니다. 이는 유럽의 한 Akamai Prolexic 고객사에 대한 사상 최대 규모의 DDoS 공격이 발생한 지 불과 몇 달 만에 발생한 공격이었습니다. 당시 트래픽은 비즈니스 운영을 중단시키기 위해 704.8Mpps까지 급증하기도 하였습니다. 이러한 공격은 Akamai가 지금까지 방어한 공격 중 가장 큰 규모의 공격(초당 1.44테라비트[Tbps], 385Mpps로 두 시간 가까이 지속된 전 세계 분산 공격)에 이어 발생했습니다. 실제로 트래픽 및 공격 패턴에 대한 인사이트를 바탕으로 Akamai는 2023년에 DDoS 공격이 더 자주, 더 오래, 더 정교하게(여러 기법을 통해), 수평적 표적(동일한 공격 이벤트에서 여러 IP 대상을 공격)에 집중할 것으로 예상했습니다.

증가하는 위협

오늘날 대부분의 DDoS 공격은 멀티기법 공격이며, 10가지 이상의 공격 기법을 사용하여 기본적인 DDoS 방어 시스템과 플랫폼을 압도합니다. 실제로 Akamai의 내부 위협 인텔리전스에 따르면 멀티데스티네이션 또는 수평적 DDoS 공격이 2022년에서 2023년 사이 두 배로 증가했습니다. 한편, 2023년에 발생한 증폭 DDoS 공격의 전체적인 크기, 규모, 지속 기간은 역대 최고 수준으로 기록되었습니다.

공격자들이 기존의 증폭 공격과 함께 사용하는 다양한 기법의 발전은 기업의 보안 계획을 더욱 복잡하게 만들고 있습니다.

DDoS 공격자들은 다음과 같은 잠재적인 장애 지점을 노립니다.

- 웹사이트
- 웹 애플리케이션 및 기타 기업 서비스
- 기업 리소스 원격 접속을 위한 VPN 콘센트레이터
- SD-WAN 컨트롤러
- 애플리케이션 프로그래밍 인터페이스(API)
- 도메인 네임 시스템(DNS) 및 오리진 서버
- 데이터센터와 네트워크 인프라

DNS 인프라

기업의 DNS 인프라에 대한 DDoS 공격, 특히 NXDOMAIN 공격(유사 랜덤 하위 도메인 공격, DNS 물 고문 공격 또는 DNS 리소스 고갈 공격이라고도 함)이 점점 더 일반화되고 있습니다. 2023년 Akamai가 방어한 DDoS 공격의 60% 이상이 DNS 구성요소를 보유했으며, NXDOMAIN 공격은 DNS DDoS 공격의 절반 가량을 차지했습니다. 기업의 DNS가 다운되면 온라인에서 기업은 사라지는 것과 다름없기 때문에 이러한 공격은 기업의 수익과 평판에 심각한 리스크를 초래합니다.

애플리케이션 레이어 공격

애플리케이션 레이어(레이어 7) DDoS 공격은 공격자들이 겉보기에 정상적으로 보이는 로직과 워크플로우를 악용하는 기법을 발전시키면서 더욱 정교해지고 있습니다. 2023년 발견된 HTTP/2 취약점은 역대 최대 규모의 레이어 7 DDoS 공격을 야기했습니다.

서비스로서의 DDoS

Anonymous Sudan이나 Killnet 같은 기업화된 사이버 범죄 그룹은 서비스로서의 DDoS를 제공하고 있습니다. 이 경우 범죄 그룹은 일반적으로 봇넷과 같은 서비스를 유료로 제공하고 클라이언트를 대신해 공격을 수행합니다. 이러한 DDoS 공격 대행 서비스는 동기부여가 된 그룹에게는 엄청난 수익을 가져다줄 수 있습니다.

랜섬웨어 + DDoS = RDDoS

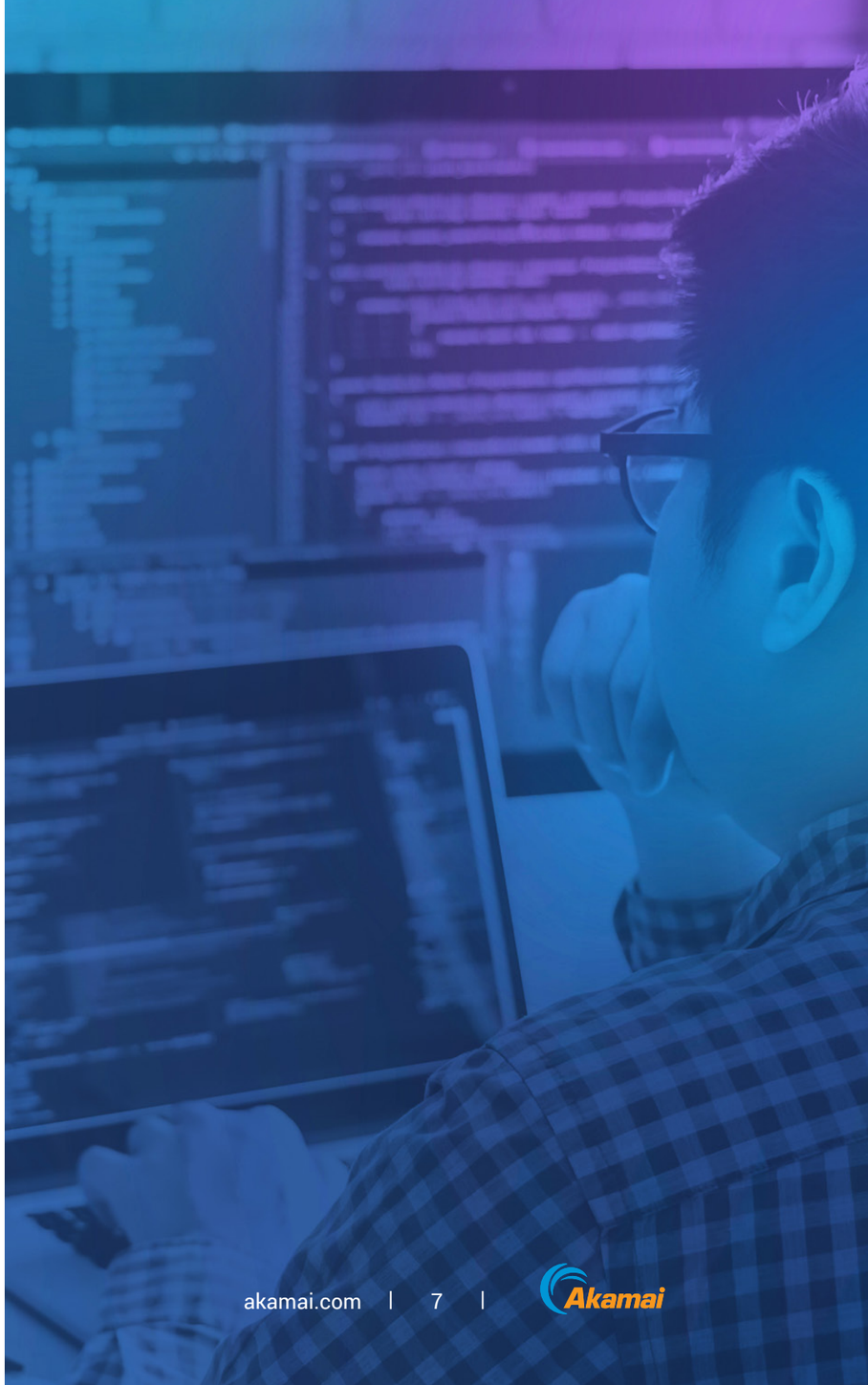
또한 공격자들은 서비스로서의 DDoS와 같은 기법을 사용할 수 있게 됨으로써 보안팀의 주의를 분산시키기 위한 연막작전으로 DDoS 공격을 더 쉽게 사용할 수 있게 되었습니다. 이들은 이와 동시에 랜섬웨어 공격 또는 삼중 갈취 공격을 시작합니다. 이러한 공격은 RDDoS(Ransom DDoS) 공격이라고 합니다.

DDoS 공격의 결과

네트워크(레이어 3) 및 전송(레이어 4) 레이어 DDoS 공격의 경우, 증폭 및 프로토콜 기반 공격은 인터넷 파이프를 막히게 하고, 서버를 과부하시키고, 상태 테이블 항목을 고갈시켜 네트워크와 서비스를 사용할 수 없게 만들려고 시도합니다. 레이어 7 공격의 경우, 공격자는 로우 및 슬로우 공격, HTTP 플러드와 같은 기법을 통해 웹 성능과 사용자 경험을 방해하여 수익에 영향을 미치는 다운타임을 유발하는 것을 목표로 합니다. DNS에 대한 DDoS 공격은 다소 복잡할 수 있습니다. 공격 종류에 따라 기업 네트워크의 다른 레이어에 영향을 미칠 수 있기 때문입니다. 예를 들어, DNS 반사 및 증폭 DDoS 공격은 기업 네트워크의 레이어 3과 4에서 트래픽을 생성하는 반면, NXDOMAIN 또는 DNS 플러드 종류의 DDoS는 네트워크의 애플리케이션 레이어를 공격하는 경우가 많습니다.

다운타임은 단순히 표적이 된 서비스의 비용과 애플리케이션을 사용할 수 없게 되는 것 이상의 파급력을 미칩니다. Ponemon Institute에 따르면 기술 지원 확대, 인시던트 대응 리소스 사용, 내부 에스컬레이션, 법률 비용, 운영 혼란, 직원 생산성 손실 등 기업이 DDoS 공격으로 인해 입는 평균 피해 규모는 연간 170만 달러에 달합니다. 또한 금융 서비스 기관, 게임 및 미디어 기업, 이커머스 기업과 같은 소비자 대면 비즈니스의 경우 오프라인 상태가 되면 금전적 손해뿐만 아니라 더 중요한 것은 회복할 수 없는 평판 손상을 입을 수 있다는 점입니다.

하이브리드 클라우드 인프라로 전환하는 비율이 높아짐에 따라 위험 또한 높아지고 있는 것은 분명합니다.

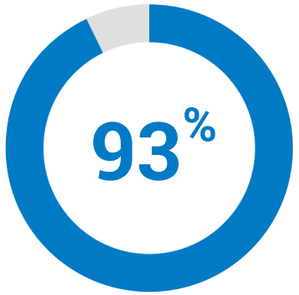


보안을 끊임없이 복잡하게 만드는 하이브리드 및 멀티클라우드

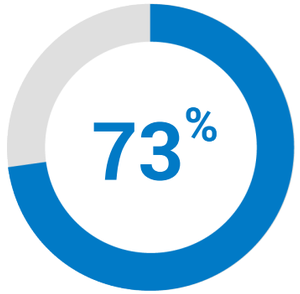
기업이 일부 워크로드는 온프레미스 데이터센터 또는 프라이빗 클라우드에 유지하고 다른 애플리케이션은 퍼블릭 클라우드 호스팅 환경으로 이전하는 하이브리드 인프라 접근 방식에서 강력한 보안을 보장하는 일은 매우 복잡합니다. 마찬가지로 기업들은 권한 DNS 영역 중 일부는 클라우드에서 관리하고 나머지 영역은 온프레미스 네임서버와 글로벌 서버 부하 분산(GSLB)에서 관리하는 하이브리드 DNS 인프라를 사용하는 경우가 많습니다. 기업이 일부 온프레미스 DNS 인프라를 계속 유지하고자 하는 이유가 있습니다. 예를 들어, 컴플라이언스 요구사항을 충족하기 위해 온프레미스 인프라를 구축하는 데 이미 상당한 자본을 투자했을 수 있습니다. 모든 DNS를 클라우드로 전환하는 것은 그 복잡성으로 인해 재정적으로 실현할 수 없을 수도 있습니다.

공격자들은 이러한 세분화된 환경에서 발생하는 취약점을 잘 알고 있습니다. 이들은 일관성 없는 보안 정책과 요구사항으로 인해 발생하는 기업의 보안 아키텍처 및 보안 체계의 약점을 악용합니다. 또한 분산되고 세분화된 클라우드 호스팅 인프라에서 문제 해결이 어렵다는 점을 유리하게 활용하곤 합니다.

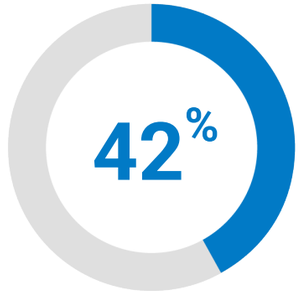
안타깝게도 퍼블릭 클라우드 환경 내 보안에 대한 책임은 공급업체마다 일관되지 않을 수 있으며, 많은 기업이 잘못된 생각을 하고 있어 리스크에 노출되기 십상입니다. 예를 들어, IBM 설문 조사에 참여한 기업 응답자 중 73%는 퍼블릭 클라우드 서비스 사업자(CSP)가 SaaS(Software as a Service)를 보호하는 주요 책임자라고 생각한 반면, 42%는 CSP가 클라우드 IaaS(Infrastructure as a Service)를 보호하는 주요 책임자라고 생각하고 있었습니다. 보안 관리 책임에 대한 지식의 결여로 인해 감염이 발생할 수 있으며, 이러한 리스크는 어떤 기업에서도 용납되기 어려운 것입니다.



멀티클라우드 전략을 사용하는 비율



퍼블릭 CSP가 SaaS 보안을 책임져야 한다고 믿는 비율



CSP가 클라우드 IaaS 보안을 책임져야 한다고 믿는 비율

기업들은 애플리케이션, API, DNS 및 이를 지원하는 기반 인프라를 보호할 수 있도록 확장성이 뛰어나고 포괄적인 통합 DDoS 방어 플랫폼을 제공하는 DDoS 보안 공급업체로 전환하고 있습니다.

다양한 DDoS 방어 기능

기업들이 클라우드 인프라에 계속 투자하는 가운데, 하이브리드 환경에서 일관적인 관리를 유지하는 일은 보안팀에 새로운 도전 과제가 될 것입니다. 또한 여러 백엔드 클라우드 인프라에 배포된 애플리케이션을 보호하는 것이 더욱 어려워짐에 따라 많은 기업에서 방어 체계를 조율하기 위한 단일 제어 지점을 찾고 있습니다.

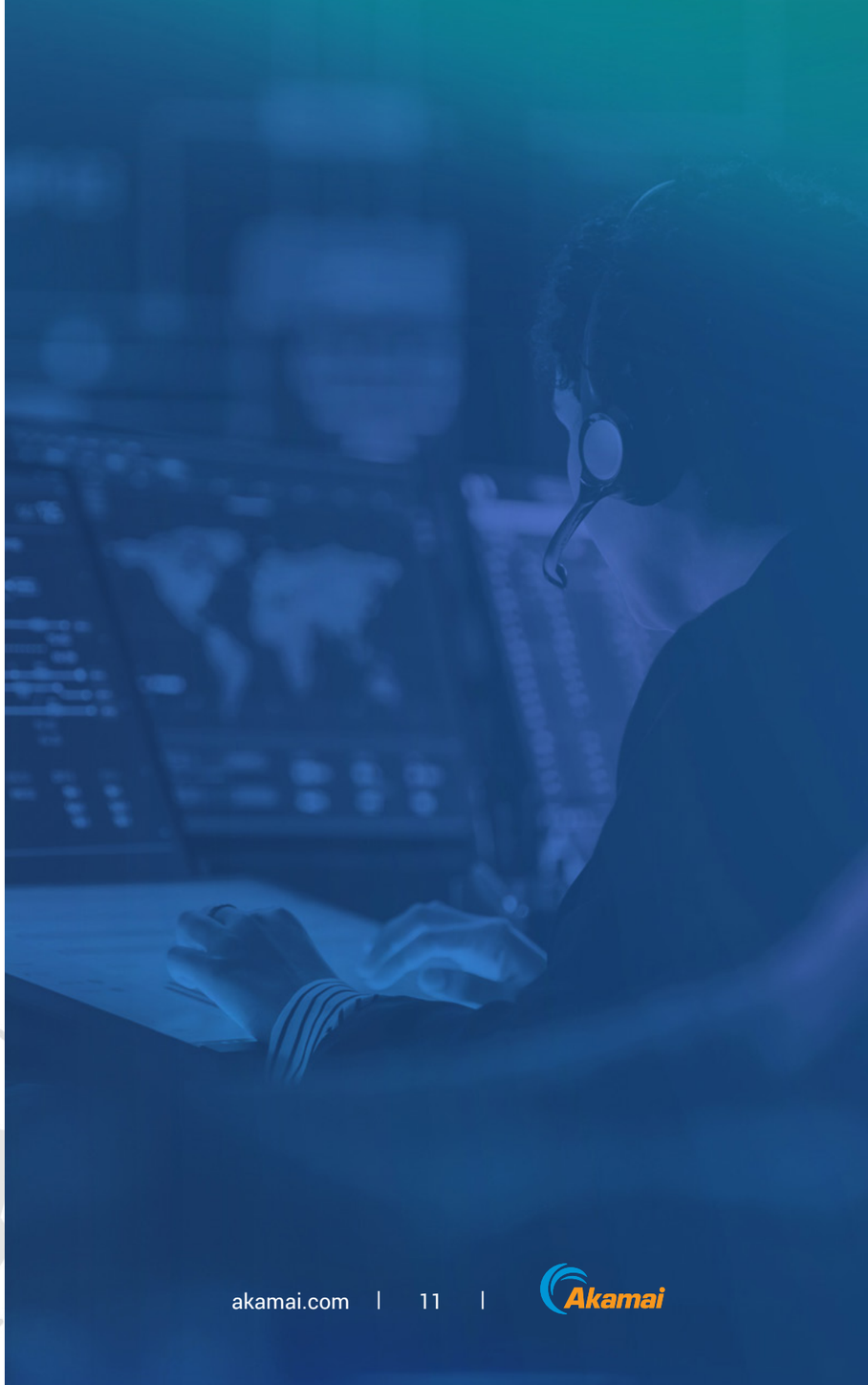
보안 기술 스택이 점점 복잡해질수록 많은 기업이 환경에 대한 통합적인 시각을 원합니다. 이는 최적화된 가시성을 위해서 뿐만 아니라 API를 통해 이벤트 데이터 상관 관계 시스템에 제공될 수 있는 효율적인 보고를 위해서이기도 합니다.

이러한 문제를 해결하기 위해 기업들은 애플리케이션, API, DNS 및 이를 지원하는 기반 인프라를 보호할 수 있도록 확장성이 뛰어나고 포괄적인 통합 DDoS 방어 플랫폼을 제공하는 DDoS 보안 공급업체로 전환하고 있습니다. 이들은 기업 서비스가 어디에 위치하든 상관없이 온프레미스, 클라우드 또는 하이브리드 환경에서 확장 가능하고 응답성이 뛰어난 방어 체계를 원합니다. 이는 CSP 고유의 환경 내에서 DDoS 방어를 통합, 배포 및 관리하는 데 필요한 운영 복잡성이 증가함에 따르는 직접적인 대응 방식입니다. 또한 여러 프라이빗 및 퍼블릭 클라우드에 걸쳐 많은 인터넷 기반 자산이 분산됨에 따라 상황은 쉽게 복잡해집니다.

게다가 많은 CSP의 자체 DDoS 방어 솔루션은 오늘날 기업 보안팀의 역량을 강화하는 데 중요한 가시성, 서비스 수준 협약(SLA), 보고 등 핵심 영역에서 부족한 점이 많습니다.

보안팀에게는 가시성과 실행 가능한 인사이트를 확보해 인시던트 대응 및 대비를 최적화하는 것이 무엇보다 중요합니다. 어떤 CSP DDoS 솔루션은 보고, 가시성, 공격 후 분석 측면에서 투명성이 거의 또는 전혀 제공되지 않기 때문에 많은 팀이 CSP를 애널리틱스 및 보고의 블랙박스라고 부르는 것도 당연합니다. 일부 CSP는 기업의 보안팀이 클라이언트별 환경에 대한 제어 권한을 설정하고 주권을 유지할 수 있도록 허용합니다. 그러나 일반적으로는 DDoS 트래픽에 대한 책임을 거부하고 애플리케이션 레이어 공격, 네트워크 레이어 공격, DNS DDoS 공격 등 어떤 공격이든 상관없이 DDoS 공격에 따른 천문학적인 양의 악성 트래픽에 대해 고객에게 요금을 청구합니다.

또한 일부 CSP와 보안 벤더사는 명확한 TTM(Time-To-Mitigate) SLA를 제공하지 않고 영향을 받은 기업에 서비스 크레딧을 제공하는 경우도 있습니다. 따라서 TTM 조항에 공격을 탐지하는 데까지 걸리는 시간이 포함되어 있는지 확인하는 것이 중요합니다. 플랫폼이 방어 프로토콜이 작동하기 전에 DDoS 공격을 탐지하는 데에만 몇 분 또는 몇 시간을 소요하면 피해 기업은 오랜 시간 동안 오프라인 상태에 놓일 수밖에 없습니다. 몇 초가 중요한 상황에서 기업은 공급업체가 성능 저하 없이 업타임과 가용성을 유지하기 위해 최선을 다한다는 확신이 필요합니다.



또한, 보안팀 또는 구매 기업에서 DDoS 보안 벤더사 및 CSP가 **전용 DDoS 방어 용량**을 제공하는지, 아니면 방어 용량이 CDN 네트워크와 공유되는지 파악하는 것의 중요성도 결코 낮지 않습니다. DDoS 방어 전담팀은 콘텐츠 전송과 같은 비즈니스의 다른 측면에 리소스나 인프라를 공유하지 않고 오로지 DDoS 공격 방어에만 집중하는 SWAT팀과 같아서 기록적인 DDoS 공격이 발생하더라도 영향을 최소화할 수 있습니다. DDoS 방어를 평가하는 기업은 벤더사 자체도 때때로 DDoS 공격을 받을 수 있다는 점을 이해하고 벤더사가 업타임/가용성 SLA를 제공하는지 여부를 중요하게 고려해야 합니다.

마지막으로, 많은 CSP 및 보안 벤더사에서 공격 전, 공격 중, 공격 후 지원 외에도 연중무휴 24시간 글로벌 보안관제센터(SOC) 지원에 대한 온디맨드 접속을 제공하지 않는 경우가 많습니다. 만약 제공한다 하더라도 동급 최고의 공급업체가 제공하는 전문 하이브리드 DDoS 방어 솔루션보다 더 비싼 프리미엄 비용을 지불해야 하는 경우가 태반입니다. 완전 관리형 하이브리드 DDoS 방어 솔루션을 사용하면 서비스 공급업체는 기업의 인시던트 대응팀이 하나 더 있는 것과 같은 역할을 하며 DDoS 이벤트에 신속하게 대응할 수 있는 전문 지식을 제공할 수도 있습니다.

오늘날의 위협 환경에서 기업들이 하이브리드 환경 전반에서 매끄러운 보안 경험을 지원하고 공격표면의 복잡성을 줄여주는 DDoS 방어 파트너에게 의존하고 있는 것은 명확한 사실입니다. DDoS 방어 파트너는 고객의 하이브리드 또는 멀티클라우드 전략을 방해하는 것이 아닌, 실현시키는 파트너가 되어야 하며 비즈니스 목표에 알맞아야 합니다.

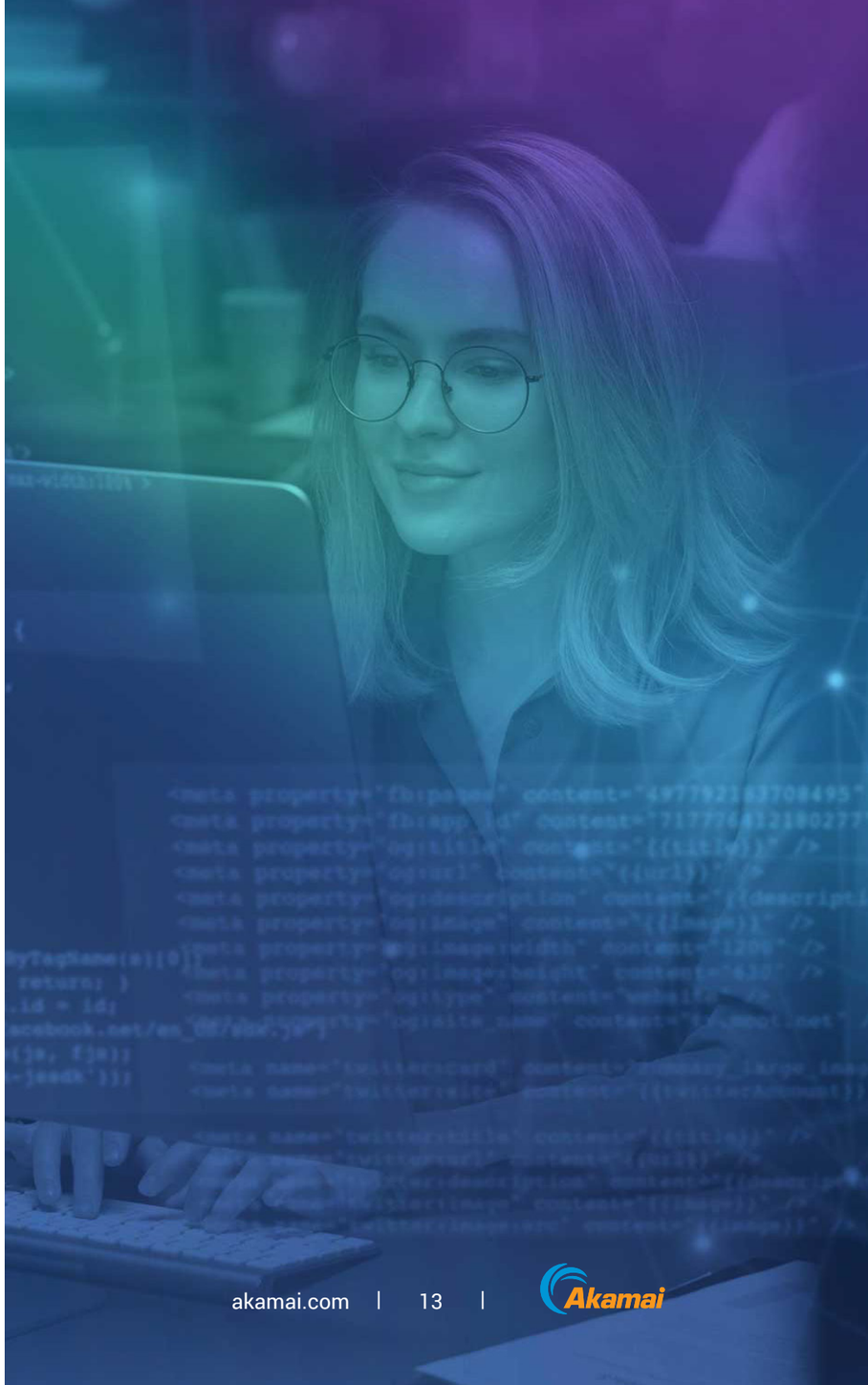
특수 목적으로 설계된 Akamai의 DDoS 방어

기업들은 하이브리드 및 멀티클라우드 환경을 포함하는 엔드투엔드 디지털 인프라 전략이 필요하지만, 엔드투엔드 DDoS 방어도 함께 고려해야 합니다. Akamai는 부수적 피해와 단일 장애 지점을 방지하기 위해 설계된 전용 엣지, 분산형 DNS 및 하이브리드 방어 전략을 통해 보안 기능을 제공하는 포괄적인 접근 방식을 기반으로 1차 방어선 역할을 합니다. 올인원 솔루션으로 구축된 다른 CSP 아키텍처와 달리, Akamai의 맞춤형 DDoS 솔루션은 향상된 안정성, 전용 DDoS 방어 용량, 웹 애플리케이션 또는 인터넷 기반 서비스의 특정 요구사항에 맞춰 미세 조정된 보다 높은 수준의 방어 품질을 제공합니다. Akamai는 고객에게 필요한 곳, 즉 온프레미스, 클라우드, 하이브리드 등 다양한 환경에서 언제든지 상시가동형(always-on) 또는 온디맨드 방식으로 DDoS 방어 기능을 제공합니다. 이 포괄적인 보호 기능은 세 가지 핵심 제품에 걸쳐 이루어집니다.

전용 DDoS 방어 용량

분산형 DNS

하이브리드 방어



Akamai Prolexic, 기업의 사전 예방적 및 적극적 보안 체계에 맞춰진 세계 최고의 DDoS 방어 체계

확장 가능한 최신 아키텍처

Akamai Prolexic은 엣지 컴퓨팅, 5G/6G 및 네트워크 가상화로 이동하는 네트워크 트렌드에 적응할 수 있도록 완벽한 소프트웨어 정의 아키텍처를 사용합니다. Prolexic은 가상화된 소프트웨어 환경으로의 전환과 함께 특수 하드웨어에 대한 모든 의존성을 제거했습니다. 이러한 배포 표준화를 통해 Akamai는 변화하는 고객의 요구사항에 더욱 빠르게 부응하고, 용량 확장을 위한 모듈식 배포를 촉진하며, 지연 시간이 짧은 링크를 통해 지역 적용 범위를 개선하고, 플랫폼의 이중화를 개선할 수 있습니다. 또한 이 아키텍처는 공격 시그니처에서 학습하고, 새로운 위협 기법에 적응하며, 고객을 위해 선제적으로 DDoS 방어 체계를 구축할 수 있는 Prolexic의 고급 행동 학습 기능을 더욱 가속화합니다. Prolexic Cloud는 **전 세계 32개 대도시 지역의 여러 스크러빙 센터와 총 20Tbps 이상의 전용 방어 용량으로** 구동됩니다. Prolexic의 방어 역량을 살펴보면, 알려진 가장 큰 규모의 레이어 3 및 레이어 4 DDoS 공격도 Prolexic 고객이 사용 가능한 용량의 10%에도 못 미칩니다.

포괄적이고 유연하며 안정적인 DDoS 방어

Akamai Prolexic은 Prolexic Cloud, Prolexic On-Prem 및 Prolexic Hybrid로 제공됩니다.

Prolexic Cloud는 클라우드 기반 DDoS 방어 업계를 선도하는 제품으로, 고객에게 0초 방어와 100% 플랫폼 가용성을 보장하는 SLA를 제공합니다. IPv4 및 IPv6 트래픽 플로우 전반에 걸쳐 공격을 막기 위해 방어 컨트롤 기능이 동적으로 용량을 확장합니다. 확장이 필요한 모든 방어 컨트롤 기능에 컴퓨팅 리소스를 동적으로 할당할 수 있습니다.

Prolexic On-Prem은 엣지 라우터와 기본적으로 통합되어 트래픽 백홀 없이도 고객 네트워크 엣지에서 98% 이상의 공격을 자동으로 차단하는 상시가동형, 물리적 또는 논리적, 인라인, 데이터 경로 DDoS 방어 기능을 제공합니다. 이는 대부분의 소규모 고속 공격과 초저지연 DDoS 방어가 필요한 비즈니스에 이상적입니다.

Prolexic Hybrid는 Prolexic On-Prem의 강력한 기능, 자동화, 성능을 업계 최고의 규모와 용량을 갖춘 Prolexic 클라우드 온디맨드와 결합해 대규모의 증폭 DDoS 공격으로부터 고객 오리진을 보호합니다.

DDoS를 넘어 보안 강화

Akamai Prolexic은 Prolexic Network Cloud Firewall과 함께 제공됩니다. 이 기능은 완벽한 셀프서비스 및 사용자 설정이 가능하므로 ACL(Access Control List)은 물론 고객사가 네트워크 엣지에서 적용하고자 하는 룰을 손쉽게 정의, 배포, 관리할 수 있습니다. 이 방화벽은 다른 모든 방화벽보다 앞선 방화벽이기도 합니다. Network Cloud Firewall은 Akamai의 위협 인텔리전스 데이터를 기반으로 최상의 선제적 방어 체계를 위한 ACL을 추천하고 기존 룰에 대한 실행 가능한 애널리틱스도 제공합니다. 차세대 서비스형 방화벽인 Network Cloud Firewall은 고객이 다음을 수행할 수 있도록 지원합니다.

- 악성 트래픽을 즉시 차단하는 선제적 방어 정의
- 룰을 엣지로 이동해 로컬 인프라 부담 완화
- 새로운 사용자 인터페이스를 통해 네트워크 변화에 빠르게 적응

Akamai Edge DNS 및 **Akamai Shield NS53**, 중요한 DNS 인프라 보호 및 강화

Akamai Edge DNS는 온프레미스, 클라우드, 하이브리드 등 모든 환경에서 DNS 인프라에 대한 다양한 DNS 공격을 포괄적으로 방어합니다. 또한 이 솔루션은 높은 수준의 DNS 성능, 안정성 및 가용성을 제공합니다. 전 세계적으로 촘촘하게 분산된 애니캐스트(Anycast) 네트워크를 기반으로 한 Edge DNS는 1차 혹은 2차 DNS로 구축될 수 있으므로 기존의 DNS 인프라를 대체하거나 혹은 강화하는 역할을 하기도 합니다.

Akamai Shield NS53은 DNS 리소스 고갈 공격(일명 NXDOMAIN)으로부터 GSLB, 방화벽, 네임서버를 포함한 온프레미스 및 하이브리드 DNS 인프라를 보호하는 양방향 DNS 리버스 프록시 솔루션입니다. 고객은 자체 동적 보안 정책을 실시간으로 자체 설정, 관리, 운영, 적용할 수 있습니다. 비정상 DNS 쿼리와 DNS 공격 플러드는 Akamai 네트워크 엣지에서 차단되어 DNS DDoS 공격으로부터 중요한 DNS 인프라를 보호합니다.

Akamai App & API Protector, DDoS 공격으로부터 애플리케이션과 API 보호

시장을 선도하는 WAAP(Web Application and API Protection) 솔루션으로 인정받고 있는 App & API Protector는 (Akamai Connected Cloud에서 호스팅되는 자산의 경우) 네트워크 레이어 DDoS 공격을 엣지에서 즉시 차단하고 애플리케이션 레이어 DDoS 공격에 대한 철저한 방어 전략을 제공합니다.

Akamai를 선택해야 하는 이유

Akamai는 세계에서 가장 신뢰받는 글로벌 DDoS 방어 솔루션을 제공합니다. 개별 애플리케이션, 전체 데이터 센터, 중요 DNS 인프라 등 무엇을 보호하든 간에 Akamai는 최대 용량, 높은 안정성, 가장 빠른 방어를 염두에 두고 DDoS 방어를 구축했습니다.

Akamai는 세계 최대 규모의 DDoS 공격을 방어했습니다. 또한 선제적 방어 컨트롤을 사용해 0초 안에 방어하고 업계를 대표하는 SLA를 제공합니다. Akamai는 여러 클라이언트에 DDoS 방어 서비스를 제공하고 여러 DDoS 공격을 동시에 방어할 수 있습니다.

DDoS 공격 기법은 끊임없이 변화하고 그 공격 규모 또한 커지고 있으므로, 신뢰할 수 있는 DDoS 플랫폼은 지속적으로 혁신을 이루고, 개발하며, 기능을 배포해 위협을 사전에 탐지하고, 방어 전략을 조율하며, 영향을 최소화해야 합니다. Akamai는 공격이 시작되기 전에 공격을 방어함으로써 위협을 미리 대비하기 위해 최선을 다하고 있습니다.

DDoS 방어 전략은 하이브리드 및 멀티클라우드 전략을 강화해야 합니다. Akamai의 차세대 DDoS 솔루션은 온프레미스와 클라우드 환경 모두에서 디지털 네트워크 인프라, 애플리케이션, DNS를 보호하며, 머신과 인간 지능의 이점만을 결합한 솔루션입니다.

자세히 보기

 | 지원 | | 2024년 10월 발행