백서

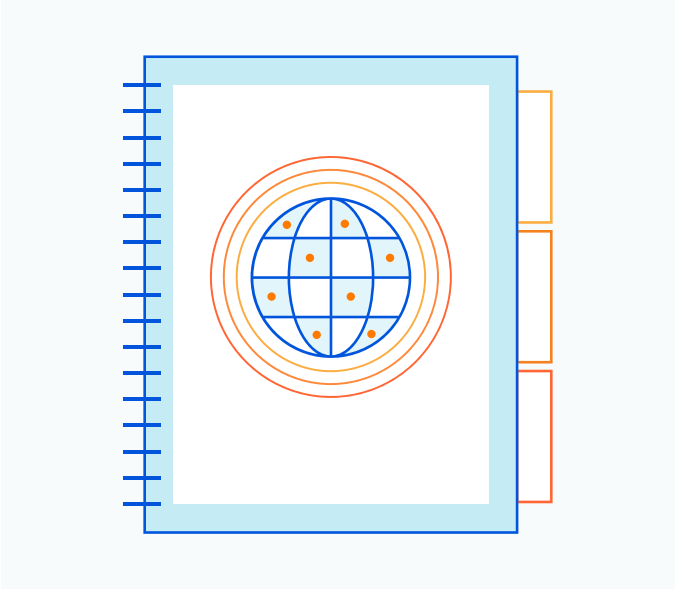
온라인 비즈니스의 보안, 성능, 안정성을 극대화하는 5가지 방법

인터넷은 급격히 변하고 있으며, 현대 기업의 본질도 변하고 있습니다. 글로벌 고객에게 뛰어난 온라인 환경을 제공하는 것은 이제 선택 사항이 아닙니다. 웹 기반 서비스와 응용 프로그램에 대한 수요가 증가함에 따라 기업은 웹 사이트와 응용 프로그램의 보안, 속도, 안정성을 최대로 유지하면서 고객 필요를 충족해야 합니다.

이와 같은 디지털 전환에 따라 기업은 성장을 위한 새로운 과제와 기회에 직면하고 있습니다. 고객의 디지털 요구 사항을 예측하고 충족하는 것부터 웹 기반 공격에 대해 강력한 방어를 구축하고, 대기 시간 문제를 극복하며, 사이트 가동 중단을 방지하고 네트워크 연결과 성능을 유지하는 것까지 다양한 과제와 기회가 있습니다.

온라인 고객 경험을 최적화하려는 기업은 사이트의 보안, 성능, 안정성을 탄탄하게 통합할 수 있는 전략을 채택해야 합니다. 이러한 전략에는 다양한 요소가 있지만, 고객의 요구 사항을 충족하고 안정적이며 원활한 사용자 경험을 제공하기 위해서는 다음의 5가지 핵심 요소를 고려해야 할 것입니다.

DNS 및 DNSSEC 지원을 활용하여 가용성과 가동 시간을 극대화하세요



흔히 인터넷 '전화번호부'라고 불리는 DNS(도메인 네임 시스템)는 도메인 이름을 숫자 IP 주소로 해석하여 브라우저가 인터넷 리소스를 로드할 수 있게 합니다. DNS는 모든 수신 주소를 수락하도록 설계됐기 때문에 올바른 DNS 보안 전략을 선택해야 합니다. 보안 전략이 없는 기업은 DNS 불법 탈취, 메시지 가로채기(man-in-the-middle attacks), 민감한 사용자 정보 노출 및 손실, 피싱, 기타 주요 위협을 비롯한 여러 가지 위험에 노출됩니다. DNS 공격이 더욱 보편화되면서, 기업들은 복원력이 있는 DNS가 없을 경우 전반적인 보안 전략에 약점이 생길 수 있다는 것을 인식하기 시작했습니다.

복원력 있는 DNS 전략을 배포하기 위해 기업에서 사용할 수 있는 접근법은 다양합니다. DNS 레코드를 모두 호스팅하고 전 세계 여러 노드에서 쿼리를 확인하며 통합 DNSSEC 지원을 제공하는 관리형 DNS 공급자를 사용할 수 있습니다. DNSSEC로는 기존 DNS 레코드에 암호화 서명을 추가하여 도메인 네임 시스템에 보안 계층을 더할 수 있습니다. 기업에서는 기본 DNS가 멈추더라도 보조 DNS가 응용 프로그램의 온라인 상태를 유지하게 해 주는 멀티 DNS 전략을 배포하여 추가 이중화를 구축할 수도 있습니다. 자체 DNS 인프라 유지를 선호하는 대기업은 보조 DNS와 연계하여 DNS 방화벽을 실행할 수 있습니다. 이와 같이 설정하면 온프레미스 DNS 인프라에 보안 계층을 더하고 전반적인 DNS 이중화를 보장하는 데 도움이 됩니다.

고객 성공 사례

블록체인과 상호 작용하기 위한 오픈 소스 클라이언트측 도구를 공급하는 한 암호화폐 기업은, 모든 쿼리를 가짜 웹 사이트로 연결하는 정교한 DNS 공격을 받은 후 DNS 보안을 강화해야 했습니다. 해커들이 권한 있는 서버 중 하나를 속여 기업 웹 사이트의 모든 쿼리를 새로운 대상으로 연결하는 데 성공한 것입니다. 가짜 웹 사이트는 해당 기업의 웹 사이트와 똑같아 보였지만, 속임수를 써서 사용자의 개인 키를 해커에게 전송하도록 했기 때문에, 해커들은 대량의 암호화폐에 효과적으로 액세스할 수 있었습니다.

이 기업은 인터넷상의 많은 웹 사이트와 마찬가지로 인터넷 핵심 인프라의 주요 취약성 때문에 공격 대상이 됐고 그로 인해 고객의 신뢰를 잃었습니다. 이 회사는 이러한 사고가 다시 발생하지 않도록 하려고 Cloudflare DNS를 채택했습니다. 사용이 편리한 통합 대시보드에서 프로토콜을 제공하고 관리할 수 있기 때문에, Cloudflare로 전환하는 것이 DNSSEC를 실행하는 가장 수월한 방법이었습니다. 이 회사에서는 이 방법을 통해 보안 환경의 복원력을 개선했을 뿐만 아니라, 회사에 암호 자산의 보호를 맡긴 고객이 더욱 안전하고 효율적인 사용자 경험을 하도록 보장할 수 있었습니다.

DNS 및 DNSSEC 통합에 대한 자세한 정보는 Cloudflare DNS 를 참고하세요.

가장 덜 혼잡한 경로로 트래픽을 라우팅하여 콘텐츠 전달을 가속화하세요

Amazon과 Facebook 같은 주요 사이트의 트래픽을 비롯한 대부분의 웹 트래픽은 현재 CDN(콘텐츠 전송 네트워크)을 통해 처리됩니다. CDN은 지리적으로 분산된 서버 집단으로, 이를 통해 전 세계에 흩어진 사용자에게 인터넷 콘텐츠를 신속히 제공할 수 있으며 대역폭 비용도 줄일 수 있습니다.

CDN은 전 세계 여러 곳에 있는 서버를 통해 웹 사이트 방문자에게 더 가까운 곳에서 콘텐츠를 제공하여 내재된 네트워크 대기 시간을 줄이고 페이지 로드 시간을 개선할 수 있습니다. CDN은 네크워크 전역의 캐시에서 정적 자산을 처리하여 호스팅된 웹 서버에 대한 요청 개수를 줄이고 대역폭 및 호스팅 비용을 절감하기도 합니다.

고객 성공 사례

세계 최대의 주문형 음식 배달 서비스 업체가 겪은 문제에 대한 사례입니다. 미국 내 수천 개 도시에 협력업체가 있으며, 온라인 플랫폼과 스마트폰 앱을 통해 음식 배달 서비스를 제공하는 이 회사의 입장에서는 항상 빠르고 안정적인 사용자 경험을 보장하는 것이 매우 중요합니다. 그렇게 해야 성장하는 사용자 기반을 지원할 수도 있고, 지역 내 음식점 및 도소매업체와의 협력 관계도 견고해지기 때문입니다.

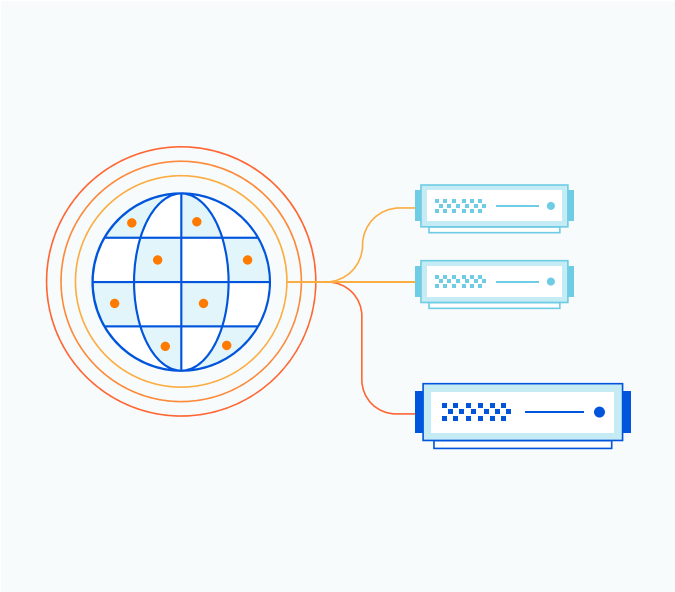
이 회사는 처음에 성능에 관해 여러 가지 문제가 있었습니다. 복원력 있는 CDN과 이미지 크기 조정 솔루션이 없었던 것입니다. 이미지 크기 조정 솔루션은 원활한 사용자 경험을 제공하기 위한 핵심적 요소였습니다. 회사 사이트의 방문자는 다양한 음식 메뉴의 고화질 이미지를 검색할 수 있어야 하는데, 회사가 성장하면서 메뉴의 수가 급격하게 증가한 것입니다. 고품질 이미지의 양이 늘어나게 되면서 이미지 전송을 최적화하고 대기 시간을 줄일 수 있는 솔루션을 찾는 일이 시급해졌습니다. 특히, 기존의 이미지 크기 조정 솔루션 비용이 매달 수천 달러에 달하면서 더욱 시급해졌습니다.

Cloudflare에서는 Cloudflare 콘텐츠 전송 네트워크(CDN)를 통해 이 음식 배달 서비스 공급자의 사용자 경험 가속화를 지원하고 있습니다. 수백만 개의 인터넷 자산이 포함된 전역 네트워크로 지원되는 Cloudflare CDN은 정적 콘텐츠를 최대한 최종 사용자와 가까운 곳에서 캐시하며 Argo Smart Routing과 함께 작동하면서 가장 빠른 경로를 통해 콘텐츠 요청을 라우팅합니다. 또한, Cloudflare Image Resizing을 통해 이미지를 캐시하고 대기 시간을 줄일 수 있으므로 이 회사의 CPU 가동률이 20% 감소했습니다.

CDN으로 기업 콘텐츠 제공을 가속화할 수 있는 방법을 알아보려면 Cloudflare CDN 을 방문하세요.

전 세계에 트래픽 부하를 분산하여 사이트 중단 위험을 최소화하세요

서버 리소스와 효율성을 극대화하려면 섬세한 균형이 필요할 수 있습니다. 대기 시간 증가와 서버 장애는 수익 손실, 고객 신뢰 상실, 브랜드 저하로 이어질 수 있기 때문에, 서버에 과부하가 걸리거나 서버가 최종 사용자로부터 지리적으로 너무 멀리 떨어지면 비즈니스에 악영향이 일어날 수 있습니다.



클라우드 기반 부하 분산 장치는 트래픽 급증을 처리하기 위해 요청을 여러 서버에 분산시킵니다. 부하 분산 결정은 사용자에게 가까운 네트워크 에지에서 일어나므로 기업이 이를 통해 서버 장애 위험을 최소화하면서 응답 시간을 개선하고 인프라를 효과적으로 최적화할 수 있습니다. 서버 하나가 멈추더라도 부하 분산 장치가 나머지 서버로 트래픽을 리디렉션하고 재분산할 수 있어 고객이 상당한 대기 기간이나 사이트 중단을 절대 경험하지 않게 됩니다. 또한, 부하 분산 장치가 능동적으로 상태 검사를 할 수 있어 기업은 성능이 떨어진 서버를 파악하여 실제 가동 중단이 발생하기 전에 선제적으로 조치를 취할 수 있습니다.

고객 성공 사례

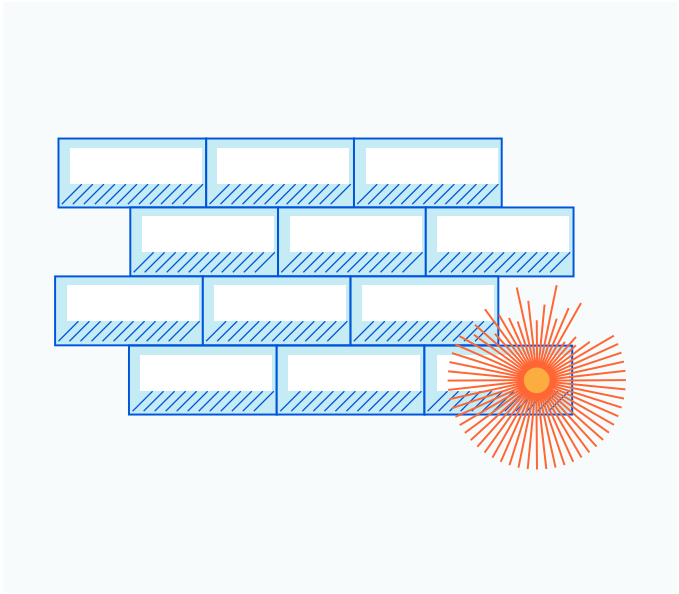
캐나다에 본사가 있으며 전 세계 175개 국가에서 운영 중인 한 전자상거래 회사는 통합 성능 및 보안 솔루션이 필요하게 되자 쉽게 실행할 수 있으며 인프라 비용을 줄일 수 있는 공급자를 찾기 시작했습니다. 이 회사는 Cloudflare로 마이그레이션 하는 과정에서 회사의 플랫폼에 의존하는 100여 만 개 사업체의 사업을 중단시키지 않으면서 마이그레이션을 원만하게 추진해야 했습니다. 이 전자상거래 회사가 모든 사이트를 Cloudflare의 전역 네트워크로 옮기면서 이를 이용하는 소매업체들은 고객에게 신속한 경험을 제공하게 되어 이 플랫폼을 통한 매출이 증가했습니다.

이러한 성능 향상의 중심에는 Cloudflare Load Balancing이 있습니다. 부하 분산을 통해 동적인 조정이 가능해진 것입니다. 즉, 가장 빠른 원본 서버 풀로 특정 사용자의 트래픽을 보냄으로써 대기 시간을 줄여 트래픽 속도를 더욱 높이게 되었습니다. 이 회사는 현재 원본 서버 간의 트래픽 분산을 세밀하게 제어하고 있으며 네트워크 에지에서 내리는 의사결정을 통해 추가적인 성능 및 정확성 향상 효과도 누리고 있습니다.

Cloudflare Load Balancing 으로 애플리케이션 성능과 가용성을 개선하는 방법을 알아보세요.

악의적인 공격으로부터 웹 응용 프로그램을 보호하세요

인터넷을 이용하는 웹 기반 기업은 다양한 위치에서 시작된, 다양한 복잡성을 지닌 광범위한 공격에 노출됩니다. 웹 응용 프로그램과 기타 중요 비즈니스용 자산을 보호할 때는 계층화된 보안 전략을 이용하여 수많은 유형의 위협으로부터 보호할 수 있습니다.



A. 웹 애플리케이션 방화벽 보호

WAF(웹 애플리케이션 방화벽)는 HTTP 트래픽을 필터링하고 모니터링하여 웹 응용 프로그램을 보호합니다. WAF를 배치하면 제로데이 공격을 차단하는 것은 물론, 서버를 손상시키고 데이터 도난이나 변조를 일으킬 수 있는 CSRF(교차 사이트 요청 사기), XSS(교차 사이트 스크립팅), SQL 삽입 공격 등의 일반적인 위협으로부터 응용 프로그램을 보호할 수 있습니다.

또한 WAF로 응용 프로그램의 취약성을 보호하고 새로운 위협을 방어할 수 있는 장벽을 설치함으로써 보안 정책을 세밀하게 관리할 수 있습니다. 클라우드 기반 WAF는 일관되게 업데이트되므로, 상당한 추가 작업이나 사용자측 비용을 발생시키지 않으면서 새로운 위협으로부터 보호하기 때문에, 일반적으로 실행이 가장 유연하고 비용 효과적인 솔루션입니다.

고객 성공 사례

Fortune 500대 기업인 한 다국적 금융 기업은 지리적 위치별로 추가 마케팅 웹 사이트를 구축하는 데 어려움을 겪었습니다. 글로벌 온라인 서비스를 구축해야 했지만, 복잡한 구성을 아웃소싱하거나, 값비싼 전문 서비스에 대해 기존 공급자에 큰 비용을 지불해야 했으며, 이 과정에 엄청나게 많은 시간과 비용이 들었습니다. 이 기업은 웹 자산을 더욱 세밀히 제어할 수 있으면서, 온프레미스 데이터 센터와 클라우드 기반 애플리케이션 간 멀티 클라우드 접근법의 균형을 맞출 수 있는 현대적인 아키텍처 솔루션이 필요했습니다.

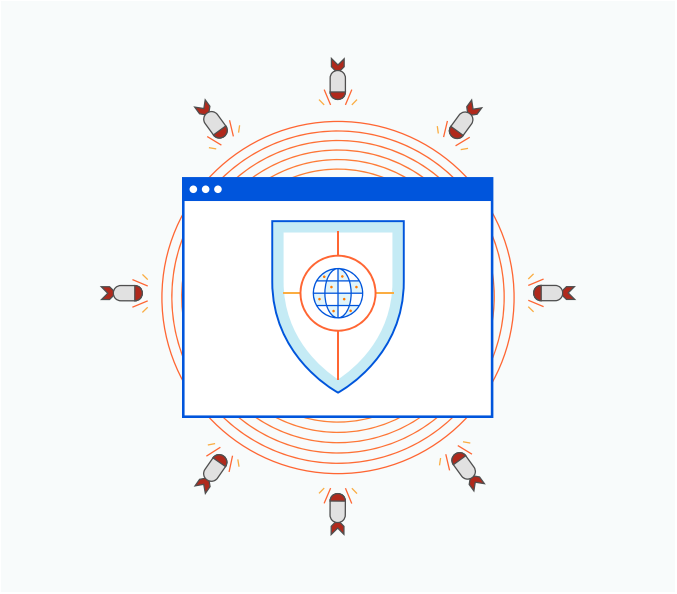
이 기업은 Cloudflare로 전환한 후 추가 비용 없이 700여 개 웹 자산을 수분 내에 보호할 수 있었습니다. 이제 이 기업은 더욱 유연하고 자율적으로 작동하는 환경의 이점을 활용하여 시간과 귀중한 내부 자원을 모두 절약할 수 있습니다.

이 기업의 많은 웹사이트를 통해 은행들이 디지털 카드 서비스를 액세스하고 기타 민감한 데이터를 처리하기 때문에 계층화된 보안 전략을 시급히 채택해야 했습니다. 공격이 한 번만이라도 성공하면 브랜드 평판이 손상되고 업체 및 고객과의 신뢰가 무너질 수 있었습니다. 이 기업은 Cloudflare WAF(웹 애플리케이션 방화벽)와 고급 DDoS 방어를 배치하여 공격과 악의적 위협으로부터 모든 사이트를 보호했습니다.

Cloudflare 웹 애플리케이션 방화벽으로 중요 비즈니스 웹 애플리케이션을 악의적인 공격으로부터 보호하는 방법을 알아보세요.

B. DDoS 공격 방어

대부분의 웹 사이트에서 대량 웹 트래픽은 좋은 일이 될 수 있습니다. 전환 증가, 고객 증가, 매출 증가로 이어질 수 있기 때문입니다. 하지만, 네트워크 연결을 교란하고 서버를 손상시키며 합법적인 사용자의 사이트 액세스를 막으려는 사이버 공격으로 인해 웹 트래픽이 증가하기도 합니다.



DDoS 공격은 불법적인 인터넷 트래픽을 이용해 서버, 장치, 네트워크 또는 주변 인프라에 과부하를 주는 악의적인 시도입니다. DDoS 공격은 대상 장치와 인터넷 사이의 가용한 대역폭을 모두 소비하여 서비스 장애를 일으킬 뿐만 아니라, 기업 자원에 대한 고객의 액세스를 막아, 기업에 상당한 부정적인 영향을 끼칩니다.

고객 성공 사례

고객이 6천만 명이 넘는 한 인도 최대의 티켓 발매 회사는 매월 화면 조회가 약 50억 건에 달하며, 연간 티켓 발매 수는 2억 매 이상입니다. 이러한 서비스에는 빠르고 안전한 사용자 경험을 제공하는 것이 매우 중요합니다. 부정적인 경험을 한 고객이 경쟁업체로 옮겨갈 것이기 때문입니다. 이 회사가 대규모의 DDoS 공격을 받게 되자, 회사의 플랫폼은 큰 위험에 처하게 됐습니다.

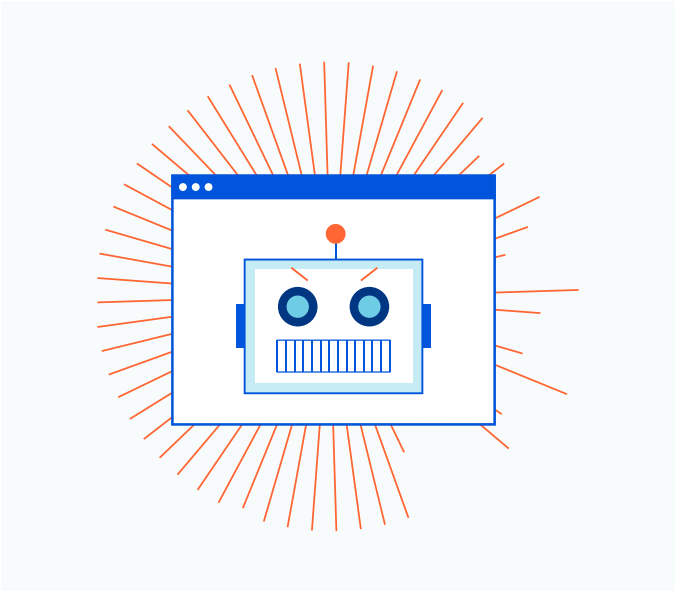
이 회사는 Cloudflare 고급 DDoS 보호 기능에 힘입어 '공황 상태'에 빠지지 않고 공격을 완화할 수 있었습니다. 121Tbps 이상의 네트워크 용량을 제공하는 Cloudflare DDoS 방어는 사용 및 관리가 용이하도록 설계되었으며, 네트워크 에지에서 공격을 차단하여 온프레미스, 하이브리드, 멀티 클라우드 여부와 무관하게 원본 서버의 가동과 가용성을 유지합니다.

Cloudflare는 초당 50기가바이트에 달하는 악의적 트래픽을 즉시 차단하기 시작했고, DDoS 공격으로 인해 사이트의 운영이 중단되거나 속도가 저하되지 않도록 효과적으로 방어했습니다. 이를 통해 이 티켓 발매 회사는 보안 상태가 개선되었을 뿐 아니라, 더욱 발전하기 위한 완벽한 안정성 및 운영 효율도 보장할 수 있게 되었습니다.

계층화된 보안 접근법의 채택에 대한 자세한 내용은 Cloudflare 고급 DDoS 방어를 참조하시기 바랍니다.

C. 악의적인 봇 완화

사이버 위협에 대응하여 고객 데이터와 웹 응용 프로그램을 완벽하게 보호하려면 계층화된 접근법이 필요합니다. 사이트는 다른 일반적인 사이버보안 위협은 물론, 악의적인 봇 활동의 대상이 될 경우에도 손상될 수 있습니다. 웹 서버에 과부하가 걸리고, 분석이 왜곡되며, 사용자가 웹페이지에 액세스할 수 없게 되고, 중요 비즈니스 기능이 손상될 수 있기 때문입니다.



좋은 봇은 웹 페이지의 콘텐츠 스캔부터 웹 사이트의 고객 문의 대응까지의 유용한 작업을 수행하도록 프로그래밍된 소프트웨어 애플리케이션을 말합니다. 하지만 해커에게 손상된 봇은 자격 증명 스터핑 및 민감한 데이터 침해부터 SEO 콘텐츠 도난 및 비즈니스 운영 방해까지 악의적인 활동을 수행하는 데 사용될 수도 있습니다. 기업은 봇 관리 솔루션을 실행함으로써, 유용한 봇 활동과 유해한 봇 활동을 구분하여 악의적인 행동이 사용자 경험에 영향을 주지 못하게 막을 수 있습니다.

고객 성공 사례

마케팅 자동화 소프트웨어 업계의 한 선두업체 웹 양식에 스팸 봇 활동이 폭주하면서 문제가 발생했습니다. 봇이 해당 양식을 목표로 하는 일이 잦아 정당한 사용자가 페이지에 쉽고 빠르게 액세스할 수 없게 되고 원활한 고객 경험을 제공하는 회사의 역량에 타격을 받은 것입니다.

회사는 사용자 경험을 저하시키지 않으면서 악의적인 요청을 차단할 수 있는 봇 완화 솔루션을 위해 Cloudflare로 전환했습니다. Cloudflare Bot Management는 기계 학습을 이용해 웹 트래픽 패턴의 특이점을 찾아내며, 좋은 봇과 합법적 트래픽은 통과시키면서 봇의 공격은 차단합니다. 현재, 이 회사는 Cloudflare를 통해 매일 100만 회 이상의 악의적인 봇 요청을 완화하고 있으며, 사용자들은 서비스 중단이나 중요한 데이터를 잃을 우려 없이 이 회사의 마케팅 소프트웨어를 활용하고 있습니다.

Cloudflare 봇 관리를 이용해 실시간으로 봇 공격을 완화하고 좋은 봇과 나쁜 봇을 관리하세요.

네트워크의 가동 상태 유지

A. 네트워크 인프라 보호

웹 서버 보호만으로는 충분하지 않습니다. 기업의 온프레미스 네트워크 인프라가 공용 또는 사설 데이터 센터에 호스트된 경우가 많은데, 이 인프라도 DDoS 공격으로부터 보호를 받아야 합니다. 많은 DDoS 완화 공급자는 스크러빙 센터 또는 하드웨어를 통한 온프레미스 스캐닝 및 필터링의 두 가지 방법 중 하나를 이용하여 공격을 차단합니다. 그런데 이 두 가지 접근법은 사업에 악영향을 줄 수 있는 대기 시간을 초래한다는 문제점이 있습니다.

스크러빙을 하려면 악의적이지 않은 트래픽으로부터 악의적인 트래픽을 필터 또는 '스크러빙' 하기 위해, 지정된 지리적 위치의 중앙 집중식 스크러빙 서버로 네트워크 트래픽의 경로를 바꾸어야 합니다. 지리적으로 떨어진 스크리빙 센터로 모든 트래픽의 경로를 변경하면, 대기 시간이 상당히 증가하기 때문에 대부분의 애플리케이션에서는 이를 사용할 수 없습니다.

또 다른 DDoS 완화 기법은 온프레미스 하드웨어를 이용하여 트래픽을 스캔하고 악의적인 요청을 필터링하는 것입니다. 스크러빙과 마찬가지로 스캐닝 하드웨어로 인해 네트워크 대기 시간이 발생할 수 있으며, 하드웨어를 통해 네트워크 트래픽 경로를 변경하고 스캐닝 프로세스를 완료할 때 병목이 발생하는 현상으로 인해 성능이 제한됩니다. 온프레미스 DDoS 방지 장비에는 기본적으로 대역폭 제한이 있는 경우가 많으며, 이러한 대역폭 제한은 조직의 네트워크 용량과 하드웨어 용량의 조합에 따라 결정됩니다.

DDoS 공격을 감지하고 완화하는 더 나은 방법은 소스와 가까운 곳, 즉 네트워크 에지에서 처리하는 것입니다. 전 세계에 분산된 네트워크 중 가장 가까운 데이터 센터에서 트래픽을 스캐닝하므로, 강력한 DDoS 공격 도중에도 높은 서비스 가용성이 보장됩니다. 이러한 접근법을 이용하면, 지리적으로 멀리 떨어진 스크러빙 센터로 의심스러운 트래픽을 연결할 때 발생하는 대기 시간이 줄어듭니다. 또한, 공격 대응 시간도 단축됩니다.

고객 성공 사례

Alexa에서 선정한 상위 10대 웹 사이트 중 하나를 운영하는 한 비영리기관은 심각한 대기 시간 및 사이트 중단 문제를 겪게 되어, 네트워크 계층에서 공격을 완화하면서 신속히 온라인 상태로 복구할 수 있는 솔루션이 필요해졌습니다.

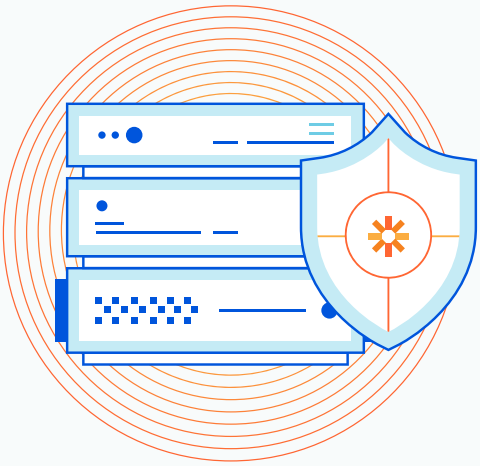
기업 서버에 과부하를 가해 모든 운영을 중단시키려는 악의적 '테이크다운 공격'으로 인해 불법적인 네트워크 계층 및 HTTP 트래픽이 서버를 압도한 것입니다. 이 회사에서는 Cloudflare에 공격 완화와 사이트 액세스 복구를 요청했으며, 미래의 공격을 방지하고자 네트워크 계층 DDoS 방어를 실행했습니다.

Cloudflare Magic Transit은 온프레미스 네트워크 및 데이터 센터에 대한 DDoS 방어 기능을 제공하며, 상시 가동 모드 또는 온디맨드 배포 모드로 제공됩니다. Cloudflare 글로벌 네트워크를 이용해 공격의 출발지에서 가장 가까운 곳에 있는 Cloudflare 데이터 센터에서 DDoS 트래픽을 감지하고 완화합니다. 이 기관은 Cloudflare의 대규모 네트워크와 안정적인 DDoS 방어에 힘입어 공격의 영향에서 신속하게 벗어날 수 있었고, 최종 사용자 경험을 정상적인 수준으로 되돌릴 수 있었습니다.

Cloudflare Magic Transit 에서의 네트워크 DDoS 방어에 대해 자세히 알아보시기 바랍니다.

B. TCP/UDP 응용 프로그램 보호

공격자는 전송 계층에서 서버의 가용한 모든 포트에 과부하를 걸어 기업의 서버 리소스를 노리기도 합니다. 이러한 DDoS 공격으로 인해 서버는 합법적인 요청에 느리게 응답하거나 전혀 응답하지 못하게 될 수 있습니다. 전송 계층에서의 공격을 방지하려면 공격 패턴을 자동 감지하여 공격 트래픽을 차단할 수 있는 보안 솔루션이 필요합니다.



고객 성공 사례

전 세계 사용자가 2억 명을 상회하는 게임 업계의 선두업체이며 게임 제작업체인 한 회사가 어려움에 빠졌습니다. 다양한 DDoS 공격이 감지됐으며, 전 세계에 분산된 사용자들 중 회사의 TCP 기반 응용 프로그램에서 형편없는 사용자 경험을 하는 사용자들이 발생한 것입니다. 게임 업계에서 이는 심각한 문제입니다. 잠시라도 서비스가 중단되면, 상당한 고객이 빠져나가고 매출이 줄어들기 때문입니다.

이 게임업체의 인프라는 짧은 대기 시간을 요구하는 게이머들에 맞춰 설계된 회사 고유의 네트워크 프로토콜상에서 작동하고 있었는데, DDoS 공격을 받게 되면 기존의 보안 제품들은 이러한 사용자 지정 프로토콜을 방어할 수 없습니다.

회사는 성능을 높이고 전송 계층에서의 DDoS 공격을 완화하기 위해 Cloudflare에 도움을 요청했습니다. 회사는 모든 TCP/UDP 프로토콜에 대한 DDoS 방어 솔루션인 Cloudflare Spectrum을 활용해, 전체적인 성능의 저하 없이 핵심적인 사용자 지정 통신 프로토콜을 보호할 수 있게 되었고 서비스 속도를 저하하고 브랜드 명성을 훼손하려던 시도를 막을 수 있었습니다. 또한, Cloudflare Spectrum은 TCP 최적화 및 Argo Smart Routing을 이용해 Cloudflare 네트워크상에서 TCP 트래픽을 가속화할 수 있습니다.

Cloudflare Spectrum 으로 기업 TCP/UDP 응용 프로그램의 속도, 보안, 안정성을 개선하세요.

결론

탁월한 온라인 경험을 만들려면 올바른 보안 및 성능 전략이 필요하며, 기업은 이를 통해 콘텐츠 제공을 가속할 뿐만 아니라 네트워크 안정성을 보장하고 사이트 중단, 데이터 도난, 기타 중요 공격으로부터 웹 자산을 보호할 수 있습니다.

전 세계 100여 개국 250여 개 도시에 구축된 네트워크로 뒷받침되는 Cloudflare는 확장 가능한 통합 글로벌 클라우드 플랫폼을 제공하여, 기업이 온프레미스, 클라우드, SaaS 응용 프로그램에 보안, 성능, 안정성을 제공하는 데 도움을 줍니다. 온라인 비즈니스를 보호하고 지키는 방법에 대한 자세한 정보는 Cloudflare.com 을 방문하세요.