CLOUDFLARE®

뒤처지지 마십시오.

모바일 소비자를 위한 전자 상거래 사이트 성능 및 보안 향상

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

핵심 요약

현재 모바일은 전자 상거래 전략에서 가장 중요한 채널이 될 수 있는 전환점에 있습니다. 미국 소매업체의 상위 25%는 승자가 독식하는 경쟁에서 모바일 전환율을 높여 관련 시장에서 최대한의 점유율을 차지하는 방법을 이미 알아냈습니다. 이들은 빠르고 편리한 모바일 사이트 및 앱을 제공하여 사용자 재방문율을 높이고 제품 보기를 유도하고 있습니다. Cloudflare는 이처럼 중요한 요구 사항을 실현할 수 있도록 다음을 제공합니다.

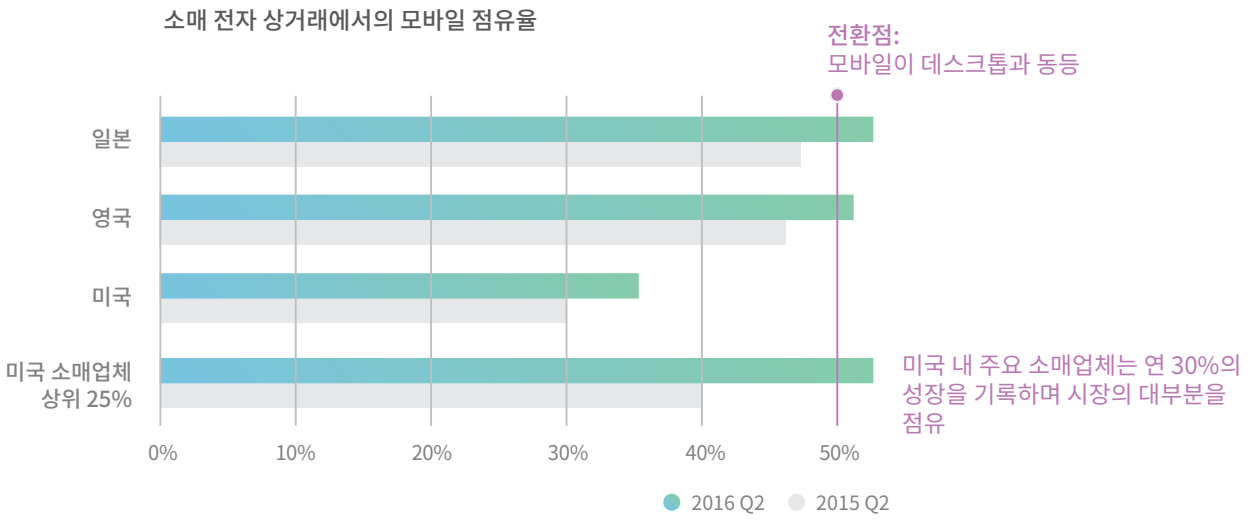
- Anycast(임의 캐스트) 라우팅 및 소비자와 물리적으로 가까운 위치에 콘텐츠를 캐시하는 기능을 기반으로 하여 대기 시간을 줄여 주는 가장 빠른 Content Delivery Network(콘텐츠 제공 네트워크) 중 하나
- 예측 가능한 정액 요금제
- 모바일 기기의 대기 시간을 줄여 주는 모바일 이미지 및 코드 최적화, IPv6 지원
- 계층 3, 4 및 7 DDoS 공격 및 계층 7 애플리케이션 취약성에 대한 보호로 가동 시간 증가
- 높은 성능을 바탕으로 즉시 암호화 수행

이러한 기능을 사용하도록 Cloudflare를 설정하는 것은 전자 상거래 공급업체가 사이트를 일 년 내내 능동적으로 신속하고 안전하게 보호할 수 있는 가장 좋은 방법입니다.

전환점에 다다른 모바일 상거래

전자 상거래는 무서운 성장세를 보이고 있습니다. 2015년의 연 성장 14.6%과 더불어, 2015년 미국 소매 판매에서는 36.2%라는 놀라운 성장을 기록했습니다. 이는 오프라인 소매를 크게 웃도는 수치입니다. 더욱 흥미로운 점은 모바일 상거래의 성장세는 이보다 더욱 빠르다는 것입니다. 모바일 상거래는 이제 전환점에 이르렀습니다. 일본과 영국에서는 2016년 2분기에 모바일 전자 상거래의 소매 거래 비율이 처음으로 50%를 넘으면서 데스크톱 거래를 앞질렀습니다. 미국에서는 전자 상거래의 모바일 점유율이 연 17%로 빠르게 증가하고 있습니다. 전자 상거래에서 미국의 모바일 점유율은 35%로 여전히 뒤떨어져 있지만 선도 국가를 곧 따라잡을 것으로 보입니다.

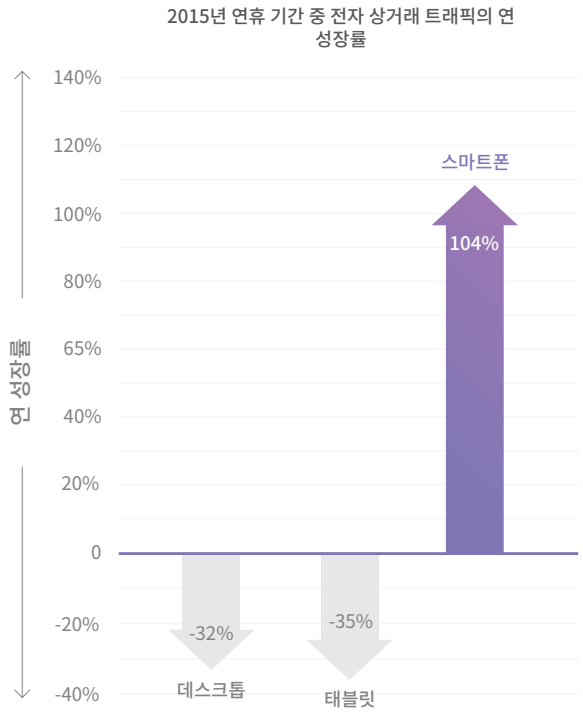
미국 소매업체 중 상위 25%는 최상의 모바일 사이트와 앱을 제공하면서 이러한 추세를 이미 활용하고 있습니다. 사용자 재방문율을 높이고 제품 보기를 유도하며, 일반적인 신규 소매업체에 비해 전환율이 최대 90% 높습니다. 그 결과 전자 상거래 매출의 52%를 모바일을 통해 창출하여 높은 점유율을 차지하면서 연 30%의 엄청난 비율로 성장하고 있습니다.

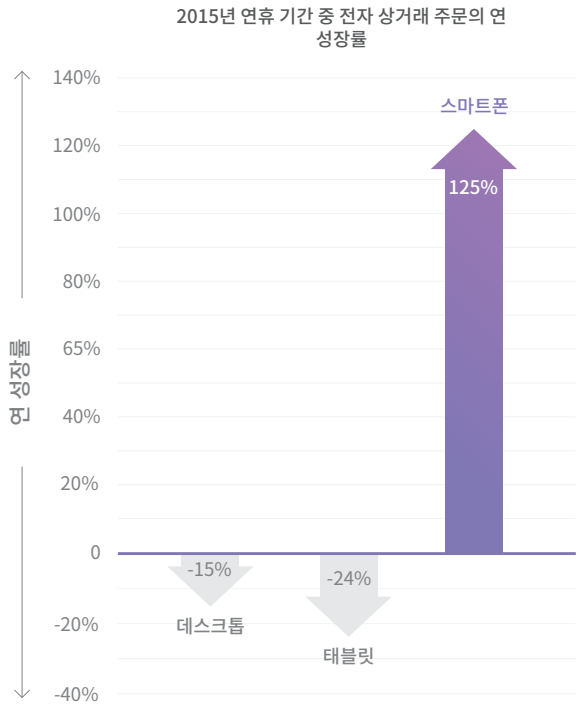


모바일 상거래가 주요 판매 및 마케팅 채널로 발전했음은 의심의 여지가 없습니다. 최고의 모바일 경험을 제공하는 소매업체는 승자가 되어 유효한 시장에서 우세한 점유율을 유지할 것입니다.

모바일은 연휴 쇼핑 시즌의 핵심

Cyber Monday가 미국 역사상 온라인에서 가장 많은 지출이 발생한 날로 기록되면서 연휴 온라인 쇼핑(Cyber 5)이 2015년에 새로운 기록을 수립했습니다. 스마트폰은 트래픽의 49%와 주문의 27%를 차지하면서 대단히 중요한 역할을 수행했습니다. 스마트폰에서 발생하는 트래픽 및 주문은 놀라운 속도로 증가하고 있으며, 이에 따라 데스크톱 및 태블릿의 트래픽/주문 액수는 줄어들고 있습니다.

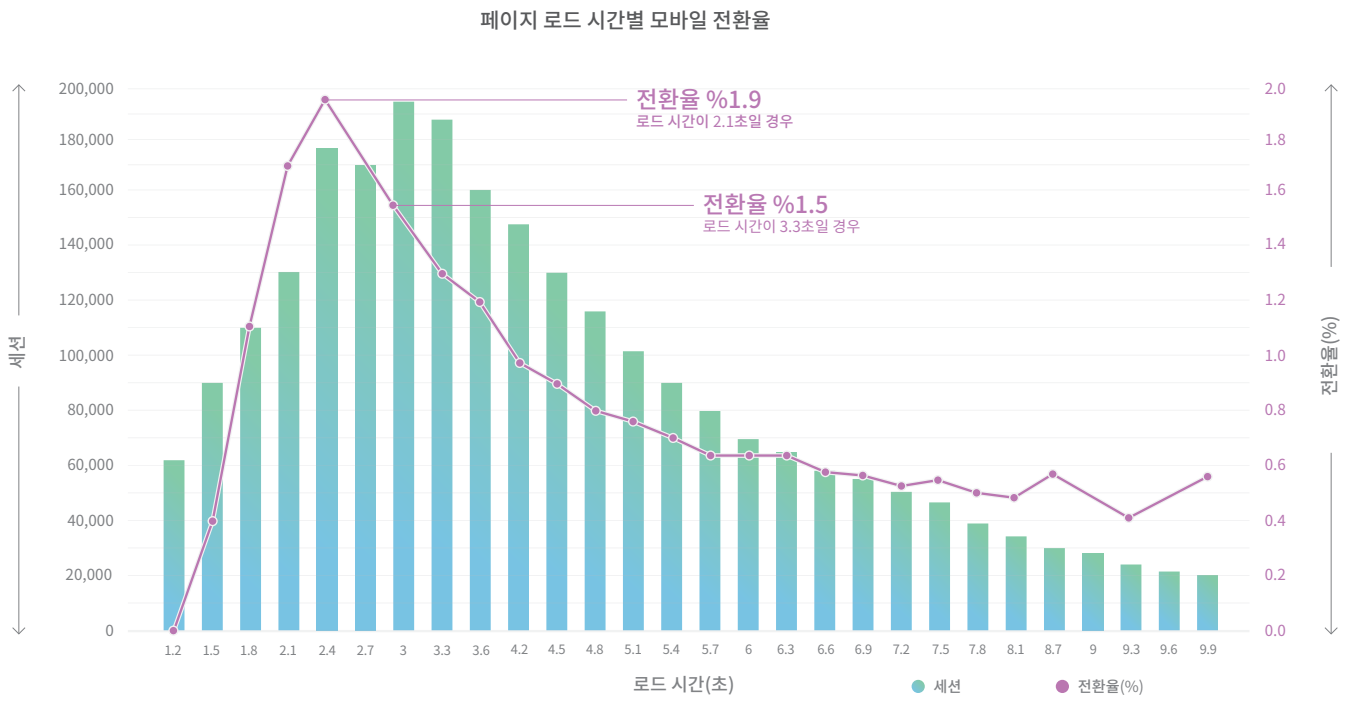




Cyber5 2015 쇼핑 기간은 최고의 모바일 환경을 갖춘 소매업체가 시장을 석권할 수 있음을 다시금 증명했습니다. 그 예로 2015년에 Amazon은 2014년 Cyber 5 기간에 비해 24.1%의 성장세를 보였습니다. 다가오는 연휴 기간에 오프라인 소매업체들은 매장 내 트래픽보다 더 많은 온라인 트래픽을 경험할 것이고, 모바일 쇼핑 환경을 성장의 핵심 요소로 삼을 것입니다.

대기 시간 및 가용성이 전환율에 미치는 영향

그룹의 리더를 차별화해 주는 요소는 무엇일까요? 주요 전자 상거래 소매업체는 전환율을 높이기 위해 최고의 모바일 사이트와 앱을 제공합니다. 여전히 낮은 모바일 전환율은 모바일 사이트/앱의 성능 및 가용성과 직접적인 연관이 있습니다. 예를 들어, 어느 주요 온라인 소매업체의 전환율은 최대 1.9%이며 평균 페이지 로드 시간은 2.4초였습니다. 페이지 로드 시간이 평균 3.3초로 1초만 느려져도 전환율이 27% 감소했습니다.

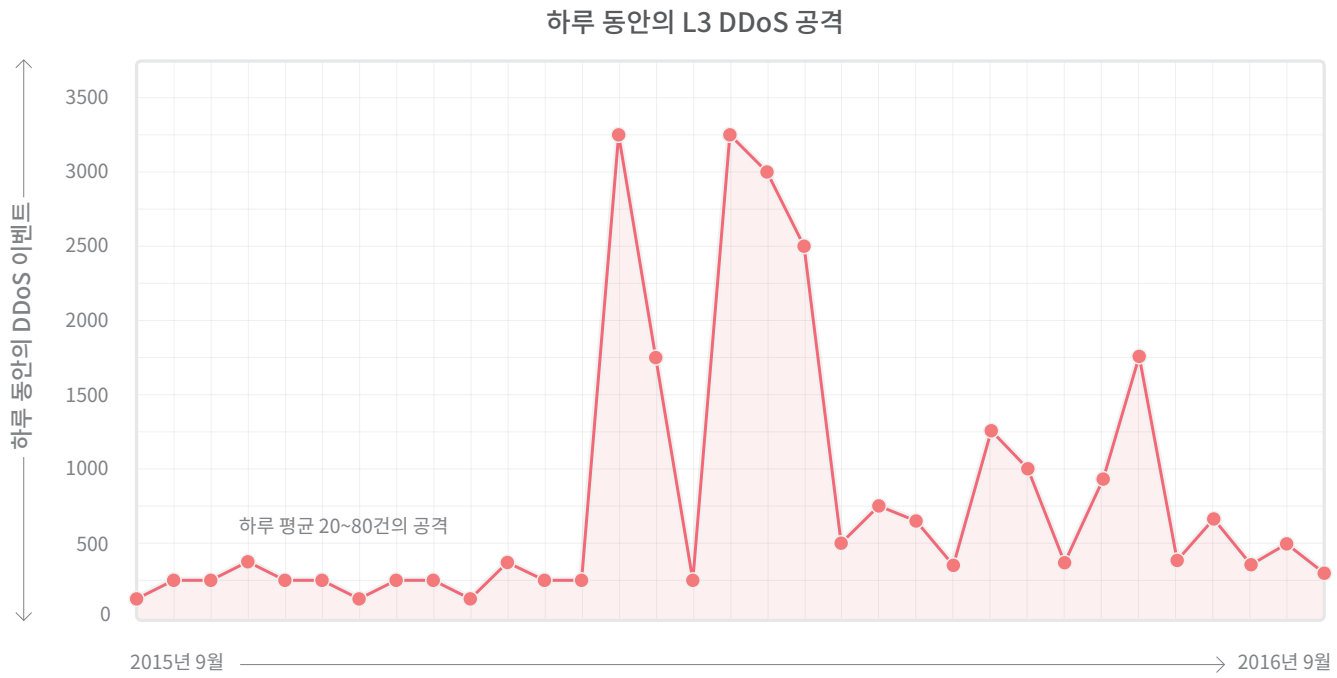


사이트 성능과 전환율 간의 연관성을 보여주는 업계 사례는 그 외에도 많습니다.

- Amazon에서는 사이트 대기 시간이 100ms 감소할 때마다 매출이 1% 증가
- Yahoo에서는 사이트 대기 시간이 400ms 감소할 때마다 트래픽이 9% 증가
- Walmart는 사이트 로드 시간이 평균 1초에서 4초로 증가하면서 전환율이 급격하게 감소

Google은 사이트 대기 시간이 100~400ms이면 소비자 행동에 유의미한 영향을 미치며, 경쟁 사이트보다 250밀리초 느린 사이트는 방문자 수가 더욱 줄어들 것이라고 밝혔습니다.

사이트/앱 자체에서 발생하는 대기 시간 외에도, DDoS(Distributed Denial-of-Service, 분산 서비스 거부) 공격을 받으면 사이트를 전혀 이용하지 못하게 될 수 있습니다. 전 세계 인터넷 트래픽의 약 10%를 담당하는 네트워크를 보유한 Cloudflare는 공격을 필터링하고 정확하게 평가할 수 있습니다. 지난해 Cloudflare는 더욱 빈번하고 강도 높은 공격을 받았습니다. 하루에 최대 1,400건의 DDoS 이벤트가 발생했고, 도합 400Gbps의 트래픽이 수신되었으며, 초당 200만 패킷의 공격이 발생했습니다.



공격은 대개 일회성으로 끝나지 않으며, 일반적으로 희생자는 1년에 수차례 공격 대상이 됩니다. Cloudflare의 경험에 따르면 조직의 규모에 상관없이 누구나 공격 대상이 될 수 있습니다. 사법권이 있는 많은 지역에서 DDoS 공격을 불법으로 규정하고 있지만, 서비스형 DDoS 구독을 제공하는 공급업체가 있으며 월 요금도 최저 $5~$10 수준으로 저렴합니다.

Amazon 웹 사이트(2015년 소매 매출액 990억 달러)도 과거에 알 수 없는 이유로 여러 차례 다운되었습니다. 예를 들어 2013년에 Amazon.com이 약 15~45분간 다운되었는데, 회사의 분당 평균 판매액 117,882달러를 기준으로 했을 때 매출 손실이 180만~530만 달러에 달했습니다. 계절의 영향을 받는 비즈니스 특성상(Amazon은 2015년 4분기에만 연 매출의 33%를 달성) 연휴 기간에는 전자 상거래 공급업체의 다운타임 비용이 더욱 커질 수 있습니다. 시스템 다운타임의 또 다른 부작용으로는 고객 만족도, 검색 엔진 순위 및 투자자 관계에 부정적인 영향 등이 있습니다.

즉, 특히 연휴 기간에 전환율을 높이려는 전자 상거래 공급업체라면 DDoS 공격으로부터 안전하며 재빠른 사이트/앱을 제공하여 가동 시간을 높이는 것이 매우 중요합니다.

빠르고 안전한 모바일 사이트를 위한 필수 기술

Cloudflare를 이용하면 하드웨어를 추가하거나, 소프트웨어를 설치하거나, 코드를 전혀 변경하지 않고도 모바일 상거래 사이트와 앱의 속도를 높이고 안전하게 보호할 수 있습니다.

첫 번째 단계는 매달 10조 건이 넘는 요청을 처리하는 세계 최대의 네트워크 중 하나인 Cloudflare의 CDN(콘텐츠 전송 네트워크)을 사용하는 것입니다. 이 숫자는 전 세계 25억 명 이상의 사람들로부터 발생하는 전체 인터넷 요청의 약 10%에 달합니다. Cedexis에 따르면 Cloudflare의 CDN은 중간 응답 시간이 34ms(미국 기준)로, 가장 빠른 CDN 중 하나로 꾸준히 인정받고 있습니다. 다음은 몇 가지 주요 기능입니다.

임의 캐스트 기반 라우팅

Cloudflare의 CDN은 임의 캐스트라는 라우팅 스키마를 사용하여 작동하지만, 오늘날 대부분의 인터넷은 여전히 Unicast(유니캐스트)라는 메커니즘을 사용해 작동합니다. 유니캐스트에서는 네트워크의 모든 노드에 고유 IP 주소가 할당됩니다. 라우터는 다양한 홉에서 최종 목적지에 도달하는 최단 경로를 유지하기 위해 전 세계의 IP 주소 맵을 유지합니다. 그러나 최종 목적지가 대륙 반대편 또는 세계의 다른 장소일 수 있으므로 추가 홉이 필요하지만, 홉을 추가할 때마다 대기 시간이 늘어납니다. Cloudflare에서 사용하는 라우팅 스키마인 임의 캐스트에서는 CDN 네트워크의 여러 시스템이 동일한 IP 주소를 공유하므로, 라우터가 물리적으로 가장 가까운 서버에 직접 요청을 보내어 대기 시간을 줄일 수 있습니다.

콘텐츠 캐싱

Cloudflare의 임의 캐스트 네트워크는 콘텐츠 캐싱과 함께 작동합니다. 임의 캐스트가 물리적으로 가장 가까운 서버로 요청을 라우팅하면, 이 서버에서 캐시된 콘텐츠의 사본에 액세스할 수 있습니다. 캐싱의 이점은 요청을 보낸 방문자 가까이로 콘텐츠를 이동하여 제공 속도를 높이고 원본 웹 서버의 부하를 줄일 수 있다는 것입니다. Cloudflare는 정적 콘텐츠를 자동으로 캐싱하는 기능을 제공하며, Railgun Cloudflare는 동적 콘텐츠를 캐싱하는 메커니즘을 제공합니다.

Cloudflare에서는 CDN의 서버를 통해 다시 전달되는 트래픽을 분석하여 원본 사이트의 정적 부분을 찾습니다. 그러면 정적 콘텐츠가 CDN에 잠시 캐싱됩니다. 일반적으로 "정적 콘텐츠의 자동 캐싱"을 사용해 웹 콘텐츠의 66%를 캐싱 가능하며, 나머지 34%는 캐싱할 수 없으므로 원본 웹 서버에서 가져와야 합니다. Railgun은 캐싱할 수 없는 콘텐츠의 전송 속도를 높이기 위해 설계되었으므로, 본질적으로는 전체 웹이 캐싱 가능하게 됩니다. 이는 캐싱할 수 없는 웹 페이지는 그리 자주는 변경되지 않는다는 사실을 바탕으로 작동하며, 웹 페이지 버전 간의 사소한 변경사항은 Cloudflare의 CDN 서버에서 확인할 수 있습니다. Cloudflare는 변경 사항을 최대 99.6%의 압축률로 압축하여 연결된 시스템 전체에 전송함으로써 최대 700%의 성능 향상을 달성합니다. Railgun의 경우, 원본 서버 측에 소프트웨어 구성 요소를 설치해야 합니다.

"대역폭 비용이 계속 상승하므로, Cloudflare처럼 에지에서 사용자에게 이미지를 제공하는 CDN을 사용하면 비용을 절감하고 모바일 고객의 대기 시간도 줄일 수 있습니다."

Chris Smith, Big 5 Sporting Goods 전자 상거래 담당 이사

정액 요금제

인터넷의 일부가 되기 위해 Cloudflare는 다양한 공급업체로부터 트랜짓(transit)이라는 대역폭을 구입합니다. Cloudflare에서는 지정된 달에 사용된 용량에 따라 트랜짓을 도매로 구매하여 일정 기간의 최대 사용량에 대한 비용을 지불합니다. Cloudflare에서 지불하는 요금은 전 세계의 지역에 따라 큰 차이가 있지만, Cloudflare에서는 요금 책정을 단순하게 유지하기 위해 트래픽이 전 세계 어디에서 제공되는지에 관계없이 고객에게 정해진 요금을 청구합니다. 네트워크를 통해 제공되는 개별 비트에 비용을 청구하는 일부 클라우드 서비스와 달리, Cloudflare는 월 청구 비용을 예측 가능하도록 하고 있습니다. Cloudflare는 가장 저렴한 가격으로 최고의 서비스를 제공하기 위해 트랜짓 요금을 낮추고 피어링을 늘리려는 노력을 멈추지 않고 있습니다.

이미지 및 코드 최적화

Cloudflare는 대기 시간을 줄이기 위해 Polish, Mirage 및 Auto-Minify 등의 단계별 솔루션을 제공합니다. 이러한 기능은 대역폭이 제한된 모바일 기기에 특히 중요합니다.

Polish는 메타데이터를 제거하고 이미지를 압축하여 크기를 줄입니다. Polish를 비손실 모드로 실행하여 이미지 데이터를 제거하지 않고도 이미지 헤더와 메타데이터에서 불필요한 확장을 제거할 수 있습니다. 따라서 평균 파일 크기가 21% 감소합니다. Polish를 손실 모드로 실행할 수도 있습니다. 이 경우 비손실 모드 외에도 압축 알고리즘을 적절한 이미지에 적용합니다. 이미지는 시각적으로 차이를 인지할 수 없을 만큼 이전과 똑같이 표시되지만, 평균 파일 크기는 48%까지 줄어듭니다. 일반적인 웹 사이트를 구성하는 데이터의 절반 이상이 이미지입니다.

Mirage는 이미지가 휴대기기에 로드되는 방식을 관리합니다. 사용자가 상호 작용할 수 있는 유용한 페이지 모양을 신속하게 생성하면서 사용자 경험을 방해하지 않고 페이지의 나머지 부분을 채웁니다.

- Mirage는 Lazy Loading(지연 로딩)을 사용하여 뷰포트에 있는 이미지, 즉 브라우저에 실제로 표시되는 이미지의 로딩 우선순위를 지정합니다. 그런 다음 필요에 따라 또는 사용할 수 있는 여분의 네트워크 리소스가 있을 때 브라우저에 표시되지 않은 다른 이미지를 페이지에 로드합니다.
- 휴대기기는 화면이 작기 때문에 이미지도 더 작아져야 합니다. Mirage는 서버에 있는 이미지를 원본 해상도의 1% 정도 크기로 조정하고 축소된 이미지를 먼저 전송합니다. 축소된 이미지를 사용해 페이지를 렌더링한 후 원본 해상도 버전으로 대체합니다. 이미지는 처음에 낮은 품질로 표시되지만 곧 초점이 선명하게 변합니다.
- Mirage는 각 이미지를 새로 요청하는 대신, Cloudflare의 네트워크에서 단일 요청으로 모든 이미지를 스트리밍합니다. 즉, 수백 개의 이미지가 있는 페이지라도 브라우저에서 적게는 두 번의 요청으로 렌더링을 시작할 수 있습니다. 느린 모바일 연결을 사용하는 사용자도 원본 해상도 이미지가 모두 로드될 때까지 기다리지 않고 즉시 페이지와 상호 작용할 수 있습니다.

Auto Minify는 HTML, JavaScript 및 CSS 파일에서 불필요한 모든 문자, 즉 "공백"을 즉석에서 제거하여, 기능 변경 없이 파일 크기를 20% 줄여줍니다. Cloudflare의 Auto Minify 구현은 가장 유사한 방식보다 100배나 빠릅니다.

IPv6 지원

Facebook 및 Linkedin의 실제 사용자 모니터링 측정 결과에 따르면, IPv6를 통한 모바일 페이지 로드 시간은 미국의 상위 4개 모바일 네트워크의 IPv4보다 10% 이상 빠릅니다. IPv6는 출시까지 수십 년이 걸렸으며 느리다는 인식에 시달리고 있지만, 미국의 상위 4개 모바일 네트워크가 받은 Android 요청의 약 60% 및 iPhone 요청의 20% 이상이 듀얼 스택 사이트에서 IPv6을 사용했습니다(2016년 5월 4일 기준). Cloudflare에서는 2012년부터 완전한 IPv6 지원 외에도 IPv6-to-IPv4 게이트웨이를 제공할 뿐만 아니라, 고객이 "간단한 한 번의 클릭"으로 이 서비스를 사용할 수 있도록 하고 있습니다. 원본 서버가 IPv6를 지원할 경우, IPv6 연결을 통해 도착한 방문자는 프로토콜 엔드 투 엔드를 통해 전송됩니다. 원본 서버에서 IPv4만 지원할 경우, Cloudflare는 IPv6을 통해 방문자를 수락한 다음 IPv4를 통해 원활하게 서버에 요청합니다. 또한 원본 서버에서 실행되는 애플리케이션이 IPv4에서 실행되어야 하는 까다로운 요구 사항이 있을 경우, Cloudflare는 Pseudo IPv4를 제공합니다. 이 옵션은 IPv6을 통해 연결될 때마다 "모의" IPv4 주소가 있는 HTTP 헤더를 요청에 추가합니다.

계층 3 및 계층 4 DDoS 보호 - 자동 학습 플랫폼을 통한 임의 캐스트 네트워크 복원력

Cloudflare의 CDN(콘텐츠 전송 네트워크)을 사용하는 것 이외에도 다음 단계는 악성 공격으로부터 사이트/앱을 보호하여 가동 시간을 보장하는 것입니다. 네트워크 에지에 서비스로 프로비저닝된 Cloudflare의 고급 DDoS 방어는 위협의 정교함과 규모에 맞춰, 모든 형태와 크기의 DDoS 공격을 완화하는 데 사용할 수 있습니다. Cloudflare는 400Gbps 이상의 공격을 포함하여 최대 규모의 DDoS 공격을 차단한 바 있습니다.

계층 3 및 계층 4 DDoS 공격은 일반적으로 DDoS 증폭, DDoS 플러드 및 DDoS SYN 플러드 공격과 같은 볼류메트릭 공격입니다. 이러한 공격은 일반적인 유니캐스트 기반 네트워크를 압도할 수 있지만, Cloudflare의 임의 캐스트 기반 네트워크는 공격 트래픽을 100개 이상의 각 Cloudflare 데이터 센터 및 다른 네트워크와의 다양한 고대역폭 상호 연결에 분산하는 방식을 사용해 본질적으로 영역을 증가시켜 공격 트래픽을 간단하게 흡수합니다. 또한 Cloudflare는 네트워크 트래픽을 실시간으로 분석하여 비정상적이거나 악의적인 요청을 식별하는 자동 학습 플랫폼도 제공합니다. 새로운 공격이 확인되면 Cloudflare에서 특정 웹 사이트와 전체 커뮤니티에 대한 공격 유형을 자동으로 차단하기 시작합니다.

비용 면에서도 공격은 일반적으로 Cloudflare에 영향을 미치지 않습니다. Cloudflare에서는 상당한 양의 도매 대역폭을 구입하고 한 달 동안 평균으로 낸 수신(인바운드) 트래픽 또는 송신(아웃바운드) 트래픽 중 더 높은 트래픽에 대한 가격을 지불합니다. Cloudflare는 캐싱 프록시 역할을 하기 때문에 정상적인 환경에서는 항상 송신량이 수신량보다 일반적으로 4~5배 정도 많습니다. 공격을 받으면 두 라인의 전송량이 서로 비슷해지지만, Cloudflare가 전반적인 대역폭 비용을 추가할 만큼 큰 공격은 거의 없습니다. Cloudflare는 이러한 이점을 고객에게 드리기 위해, DDoS 공격으로 증가한 네트워크 트래픽 비용을 고객에게 청구하지 않습니다.

Cloudflare의 네트워크와 커뮤니티가 지속적으로 성장함에 따라, Cloudflare 사용자를 대상으로 효과적인 DDoS 공격을 시작하기는 갈수록 어려워질 것입니다.

계층 7 DDoS 방어 - IP 평판 데이터베이스를 사용하는 속도 제한기

계층 3 및 4 볼류메트릭 공격과 마찬가지로, 계층 7 서비스 거부 공격에서는 대량의 요청을 사용하여 실제 사용자가 웹 사이트에 액세스하지 못하도록 만듭니다. 계층 7 서비스 거부 공격에서는 하나의 IP 주소를 통해 악의가 없는 정상적인 트래픽 패턴과 유사한 요청을 다수 보내므로 공격을 방어하기가 어렵습니다.

Cloudflare의 Traffic Protector(현재 Early Access Program을 통해 사용 가능)는 각 IP 주소에서 사이트로 전송되는 요청 수를 추적하고 분당 요청 수가 너무 많은 사이트를 식별합니다. 의심스러운 IP 주소가 식별되면 이 IP 주소의 트래픽에 약 5초 동안 중간 페이지가 표시되어 일련의 수학적 인증을 수행합니다. 요청이 이 인증에 실패하면 Traffic Protector는 해당 IP의 평판을 다운그레이드하고 이 주소의 트래픽이 모든 액세스 시도와 함께 CAPTCHA 페이지로 보내집니다.

Cloudflare가 악성 요청을 하는 것으로 보이는 IP 주소를 식별하면 이를 Cloudflare IP 평판 데이터베이스에 저장합니다. 위협 점수에 따라 요청이 통과하거나 CAPTCHA로 보내집니다. CAPTCHA에 실패하고 IP 주소가 악의적인 것으로 확인되면 전체 네트워크의 Cloudflare 에지에서 요청이 차단되어 전체 Cloudflare 커뮤니티가 보호됩니다.

계층 7 non-DDOS 애플리케이션 취약성 공격 - 웹 애플리케이션 방화벽

계층 7 애플리케이션 계층 공격은 가장 복잡하고 정교한 공격 유형입니다. 애플리케이션의 정상적인 사용을 모방하여 대부분의 DDoS 완화 장비 및 취약성 보호 서비스를 통과할 수 있습니다. 일반적인 공격 유형에는 SQL 삽입 및 XSS(교차 사이트 스크립팅)가 포함되어 있어 공격자가 고객 또는 다른 종류의 애플리케이션 데이터에 액세스하고 이를 조작할 수 있습니다.

Cloudflare는 WAF(웹 애플리케이션 방화벽)를 통해 이러한 위협을 해결합니다. WAF는 OWASP 핵심 규칙 집합, Cloudflare에서 제공하는 기본 규칙 및 커뮤니티/고객이 만든 사용자 지정 규칙을 구현합니다. Cloudflare가 출시한 새로운 규칙은 30초 이내에 모든 Cloudflare 서버 노드에 전파되며, WAF 자체는 요청당 1ms 미만의 대기 시간을 추가하여 성능을 저하하지 않고 보안을 제공합니다. Cloudflare는 이러한 방법으로 Shellshock 취약점이나 Heartbleed 버그를 비롯한 주요 제로 데이 취약점으로부터 고객을 보호해 왔습니다.

"우리는 DDoS 공격의 영향을 매우 심각하게 받아들입니다. 도메인이 DDoS 공격에 직면했을 때 Cloudflare가 도메인을 신속하게 보호해 주어 고객에게 끊김 없는 경험을 제공할 수 있었습니다. Cloudflare가 제공하는 가장 큰 이점은 누군가가 네트워크를 모니터링하고 있으며 공격을 완화할 방법이 있다는 사실에 안심할 수 있다는 것입니다."

Chris Smith, Big 5 Sporting Goods 전자 상거래 담당 이사

서버 푸시가 지원되는 TLS 1.3 및 HTTP/2

신뢰할 수 있는 쇼핑 경험을 제공하려면 암호화가 필수이지만, 최신 SSL 개선 기능을 사용하면 암호화를 올바르게 수행하고 성능을 향상할 수 있습니다. TLS(전송 계층 보안) 1.3은 이전 TLS 버전의 안전하지 않은 기능을 제거할 뿐만 아니라 프로토콜 왕복을 절반으로 줄여 대기 시간을 단축해 줍니다. Cloudflare는 TLS 1.3을 처음으로 배포하여 표준에 크게 기여했으며, TLS에서만 작동하는 HTTP/2도 처음으로 배포했습니다. HTTP/2는 최종 사용자가 브라우저를 사용하면서 인지하는 성능, 특히 대기 시간을 개선해 줍니다. HTTP/2는 서버 푸시와 함께 작동합니다. 여기서 서버는 클라이언트가 아직 요청하지 않은 리소스를 보내어 인식되는 성능을 더욱 높일 수 있습니다. 서버 푸시 기능이 지원되는 TLS 1.3 및 HTTP/2는 새로운 기술을 네트워크에 지속적으로 통합하려는 Cloudflare의 노력 중 두 가지 예에 지나지 않습니다.

요점

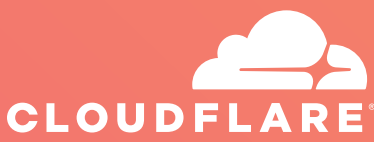
Cloudflare에 등록하여 모바일 사이트 및 앱의 성능을 높이고 DDoS 공격 및 애플리케이션 취약점으로부터 보호하십시오. 설정이 간편하므로 일반적으로 5분 이내에 완료하고 실행할 수 있습니다. www.cloudflare.com에서 Free부터 Enterprise에 이르는 다양한 플랜을 확인하십시오.

Cloudflare에 대해 자세히 알아보려면 다음으로 문의하십시오.

www.cloudflare.com

enterprise@cloudflare.com

1 888 99 FLARE



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com