CLOUDFLARE

전자책

가동 중지 시간 방지: DDoS 방어 모델 가이드

내용

클릭하여 섹션으로 건너뛰기

소개: 하이브리드 근무 환경에서의 DDoS 방어

더 빠르고 우수한 애플리케이션과 고객 경험의 수요가 늘어나면서, 현재 기업에서는 별개의 클라우드 서비스를 평균 1,400개 이상 사용하고 있습니다 [1]. 하지만 클라우드로 전환되면서 공격 표면이 확장되고 있습니다. 디지털 서비스가 많아질 수록 공격자가 악용할 수 있는 '진입점'도 많아집니다. 또한 수년간의 글로벌 팬데믹으로 필수가 된 하이브리드 근무(사무실 근무와 원격 근무의 결합 형태)로도 공격 표면이 확장되었습니다.

이러한 모든 요인으로 인해 리소스가 부족한 기업에서는 압박을 더 많이 느끼고 있습니다. IT 및 보안 팀은 더 탄력적인 애플리케이션과 네트워크를 제공해야 하며 위치에 관계없이 진화하는 위협으로부터 사용자와 기기를 보호해야 합니다.

이러한 위협에는 더 빈번하고 길고 규모가 큰 분산 서비스 거부(DDoS) 공격이 포함됩니다. 2023년 2월, Cloudflare는 기록상 최대 규모의 HTTPS DDoS 공격(71Mrps)을 감지하고 완화했습니다. 데이터에 따르면 2022년에는 전 분기 대비 대규모 볼류메트릭 DDoS 공격(100Gbps 이상의 공격) 역시 증가했습니다.

오늘날의 경제 현실과 하이브리드 근무 환경에서 기업은 DDoS 방어 체계를 재평가해야 합니다.
가동 중지 시간, 데이터 도난, 네트워크 침입, 재정적 손실의 위험이 너무 큽니다.

연구에 따르면 중단의 60% 이상은 비용이 10만 달러 이상 발생하고, 중단의 15%에서는 비용이 100만 달러 이상 발생하는 것으로 나타났습니다 [2]. 한 예로, 한 기업에서는 일련의 DDoS 공격으로 가동 중지 시간이 초리되어 거의 1,200만 달러의 비용이 발생했습니다 [3].

현실이 이렇기 때문에 DDoS 방어는 모든 규모의 조직에서 매우 중요합니다. 과거의 수동적인 접근 방식은 이제 충분하지 않습니다. 공격은 사람이 시작할 수도 있지만, 봇에 의해 실행되며, 승리하려면 봇과 봇으로 싸워야 합니다. 감지 및 완화 기능은 최대한 자동화해야 합니다.

이 전자책에서는 다음 내용을 설명합니다.

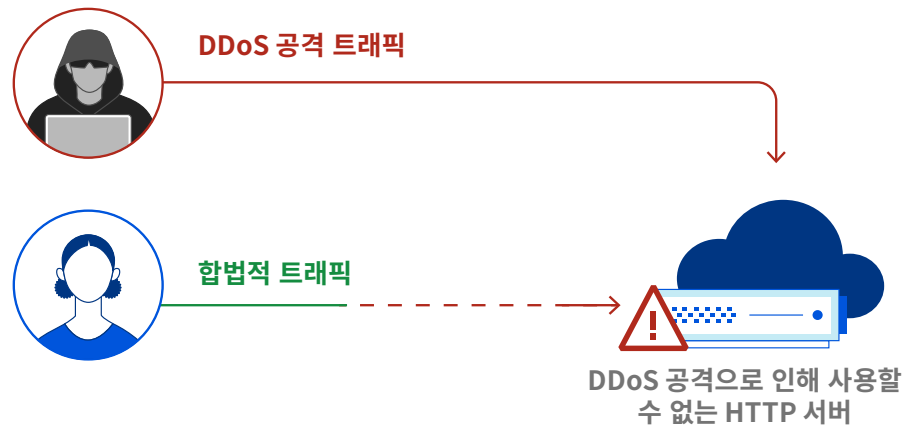
- 다양한 클라우드 기반 DDoS 방어 모델
- 상시 가동 클라우드 스크러빙의 한계 극복
- 글로벌 Fortune 500대 기업이 Cloudflare를 통해 랜섬 DDoS 공격을 저지한 방법

클라우드 기반 DDoS 완화 접근 방식 이해

DDoS 공격은 인터넷 트래픽을 폭주시켜 대상 인프라나 주변 인프라를 압도하고 대상 서버, 서비스 또는 네트워크의 정상적인 트래픽을 방해하는 악의적인 시도입니다. 효과적인 DDoS 솔루션은 이러한 '트래픽 정체'가 언제, 어디서, 어떻게 발생하는지 정확히 알려주며 악성 트래픽을 흡수하고 경로를 다시 라우팅하여 합법적 트래픽을 방해하지 않도록 합니다. 보호되지 않는 인터넷 자산 및 네트워크와 더불어 대량의 트래픽이 발생하는 목적지는 모두 일반적인 목표물입니다.

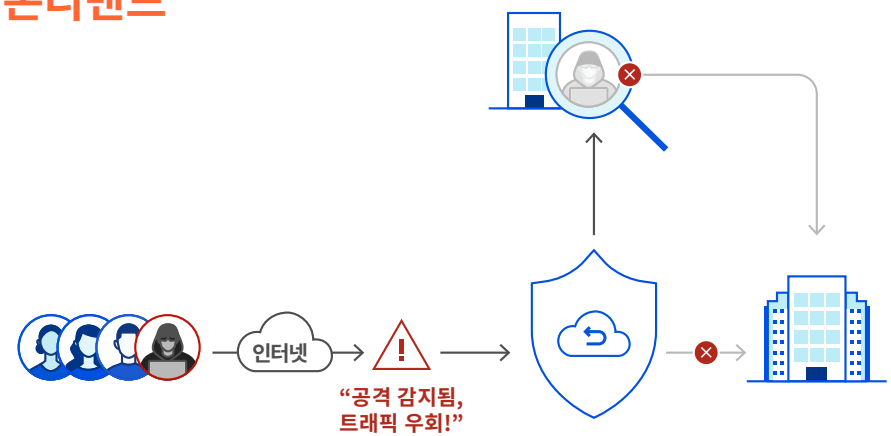
DDoS 공격은 새롭지 않지만, 막는 데는 새로운 접근 방식이 필요합니다. 애플리케이션이 클라우드로 마이그레이션되면서 온프레미스 DDoS 솔루션 시장도 줄었습니다[4]. 대신 DDoS 방어를 위해 클라우드로 전환하는 조직이 늘어나고 있습니다.

다양한 클라우드 기반 보호 기능을 갖춘 클라우드 공급자는 조직의 애플리케이션과 인프라 앞에 위치하여 모든 트래픽을 스크러빙 센터로 보낸 다음 '정화합니다'. 합법적인 트래픽만 고객에게 다시 전송합니다. '클라우드 스크러빙' 동작은 두 가지 방식, ***온디맨드*** 또는 ***상시 가동*** 방식으로 작동합니다.



합법적인 사용자를 대상으로 서비스를 거부하는 애플리케이션 계층 DDoS 공격 다이어그램

온디맨드

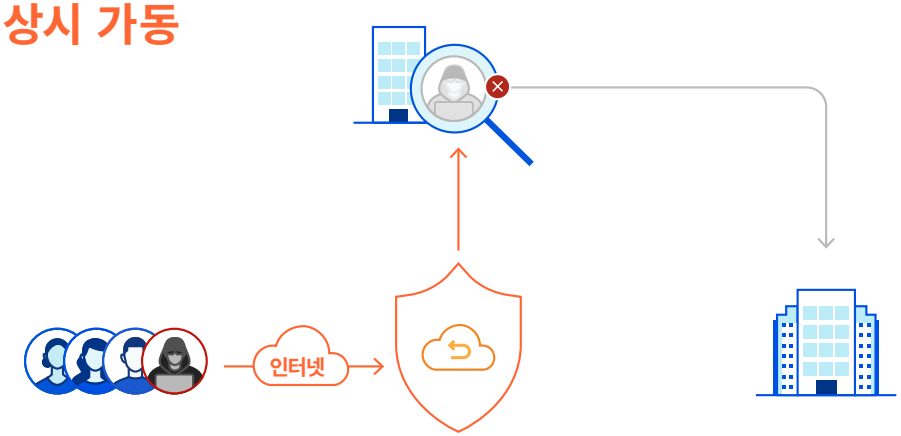


온디맨드 클라우드 스크러빙은 '평상시'에 리디렉션 없이 모든 트래픽을 애플리케이션과 인프라에 도달시킵니다. DDoS 공격 상황이 진행 중인 트래픽만 클라우드 스크러빙 공급자로 우회됩니다.

인바운드 트래픽이 사전 구성된 임계값(예: 링크 용량의 70%)을 초과하거나 대규모 공격이 감지된 경우, 온디맨드 클라우드 완화 모드가 활성화되어 가장 가까운 스크러빙 센터로 트래픽을 우회해 처리합니다.

비교

상시 가동



본질적으로, 클라우드 스크러빙에 자율적으로 접근하는 방식은 평시에도 항상 위협을 검사하기 위해 클라우드 공급자의 데이터 센터를 통해 트래픽을 라우팅합니다.

상시 가동 모델은 서비스 중단 없이 감지부터 완화까지 걸리는 시간을 최소화하는 데 유용합니다.

온디맨드 및 상시 가동 기술은 이점이 다르지만 다음 섹션의 설명처럼 서로 다른 상황에서 각각 한계가 있을 수 있습니다.

클라우드 스크러빙 방법의 일반적인 한계

온디맨드 클라우드 스크러빙의 과제

공격 대응 지연:

- 온디맨드에서는 DDoS 공격 발생 시 클라우드 공급자로 트래픽을 다시 라우팅해야 합니다. 이렇게 위치를 바꾸려면 공격에 수동으로 대응하는 데 걸리는 시간(예: 공급자에게 서비스를 켜 달라는 요청) 이외에도 몇 분 정도 시간이 더 걸릴 수 있습니다. 온디맨드 보호 기능을 제때 켜지 않으면 큰 영향을 미칠 수 있습니다.

장기적인 비용 증가:

- 온디맨드 클라우드 공급자는 공격 트래픽 요금을 바이트 단위로 부과하는 경우가 많습니다. 사용한 만큼만 비용을 지불하면 되지만 조직이 DDoS 공격을 당하는 빈도가 잦을 수록 더 많은 비용이 발생할 수 있습니다.

공격 누락 가능성:

- 사용률 임계값을 넘지 않은 DDoS 공격은 감지할 수 없으므로 네트워크 링크가 혼잡하면 합법적인 트래픽에 영향을 줄 수 있습니다.
- 또한 네트워크 링크는 SSL과 애플리케이션 수준에서 상위 계층 프로토콜 공격을 모니터링하지 않습니다.

상시 가동 클라우드 스크러빙의 과제

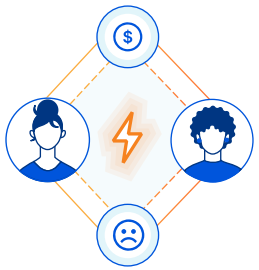
부정적인 사용자 경험으로 이어지는 대기 시간 문제:

- 네트워크 트래픽을 스크러빙하는 전용 데이터 센터가 멀리 위치한 클라우드 DDoS 완화 공급자가 많고, 이러한 데이터 센터는 공격 트래픽 발생 지점에서 멀리 떨어져 있습니다. 일반적으로 스크러빙 센터 수가 적을 수록 대기 시간이 길어집니다. 이 트래픽 백홀로 인해 대기 시간이 생기고 지연이 눈에 띄게 나타날 수 있습니다.
- DDoS 스크러빙 전용 데이터 센터에서 네트워크 계층만 검사하는 경우도 많습니다. 웹 애플리케이션 방화벽이나 콘텐츠 캐싱 등 다른 계층에 있는 기능의 경우, 보통 대체 데이터 센터에서 이 트래픽을 처리하므로 대기 시간이 더 길어집니다.

총 소유 비용 증가:

- 네트워크 용량이 부족한 상시 가동 클라우드 스크러빙 솔루션에서는 대역폭 제한을 높은 비용의 형태로 고객에게 전가할 수 있습니다. 전문 서비스 수수료가 부과될 수도 있습니다.

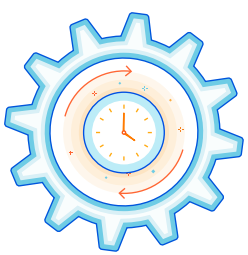
시간이 돈일 때: 가동 중단 시간과 대기 시간이 비즈니스에 미치는 영향



91%의 조직은 비즈니스 손실, 생산성 중단, 문제 해결 노력으로 인해 **시간당 가동 중단 시간 비용이 최대 30만 달러에 달한다고 밝혔습니다** [5]

게이머의 44%는 대기 시간이 발생하면 **플레이하던 게임을 종료하고** 나중에 다시 시도하지만 **24%는 이 게임을 종료하고 다른 게임을 플레이합니다** [8]

유명 전자 상거래 에 가동 중단 시간이 발생하면 분당 최대 **220,000달러**의 비용이 발생할 수 있습니다 [6]



IT 의사 결정권자의 64%는 더 빠르고 간편한 고객 경험을 제공해야 하므로 **"기술 인프라에 상당하고 중대한 부담을 느낀다"고 합니다** [9]

쇼핑객의 90%가 '적절한 시간 내에' 사이트가 로딩되지 않을 때 사이트를 이탈하며 **57%는 사이트에서 나가거나 비슷한 소매업체에서 구매합니다** [7]

클라우드 기반 DDoS 방어의 모든 가능성을 실현하고 중단으로 인한 매출 손실을 방지하세요

지능형 전역 네트워크를 사용하는 Cloudflare의 통합 클라우드 플랫폼을 통해 DDoS 위협으로부터 보호하는 방법은 다음과 같습니다.

온디맨드 클라우드 스크러빙은 사람의 개입에 의존하므로 완화 대응에 시간이 더 걸립니다. 반면 상시 가동 클라우드 DDoS 방어 기능은 더 포괄적이지만, 사용자 경험 시 대기 시간이 더 소요되는 원거리 스크러빙 센터에 의존하는 상시 가동 클라우드 벤더가 많습니다.

Cloudflare는 DDoS 방어(3, 4, 7 계층)의 3계층과 온프레미스, 클라우드 호스팅, 하이브리드 네트워크의 트래픽 가속이 포함된 하나의 보안 플랫폼으로 이러한 제한을 해결합니다. 공격 트래픽이 출발지와 가까운 곳에서 완화되므로 최종 사용자는 원활하고 뛰어난 성능을 경험할 수 있습니다.

네트워크 기반 보안

Cloudflare는 **285개 이상의 도시에 데이터 센터를 두고 있으며, 네트워크 용량은 197Tbps**입니다(반면, 잘 알려진 상시 가동 DDoS 완화 서비스 한 곳은 스크러빙 센터가 40개 미만이며 네트워크 용량이 20Tbps에 불과합니다).

공격이 고객 네트워크에 도달하기 전에 Cloudflare 네트워크에서 자동으로 흡수하며, 악의적인 트래픽은 **3초 이내에** 대부분 차단됩니다. 백홀이 필요하지 않습니다.

사용성, 가시성, 셀프 서비스

Cloudflare DDoS 방어는 서비스형으로 제공되므로 자본 지출 투자나 하드웨어 수명 주기 관리가 필요하지 않습니다.

또한, **단일 대시보드**에 맞춤형 구성 기능을 갖춘 **셀프 서비스**입니다.

대규모 위협 인텔리전스

더 많이 확인하고, 더 많이 보호합니다. 웹의 거의 20%가 Cloudflare에서 실행됩니다. Cloudflare 고객은 **매일 1,120억 건 이상의 사이버 위협을 차단하는** 전역 네트워크의 규모와 인텔리전스를 활용할 수 있습니다.

고급 머신 러닝 모델이 지속적으로 방어를 개선하여 고객 대신 새로운 위협에 한 발 앞서 대비합니다.

업계에서 인정받은 DDoS 방어

Cloudflare는 **2022년 GigaOm Radar의 DDoS 방어 부문 보고서**의 '리더'로 인정받았습니다. 이 보고서는 9개의 서로 다른 공급업체를 평가했고 전반적으로 Cloudflare의 순위가 가장 높았습니다. Cloudflare는 **The Forrester Wave™: 2021년 1분기 DDoS 완화 솔루션 보고서에서도 '리더'**로 선정되었습니다.

Cloudflare는 보안 운영 센터, 응답 자동화, 성능 등을 포함한 15가지 평가 기준에서 최고 점수를 받았습니다.

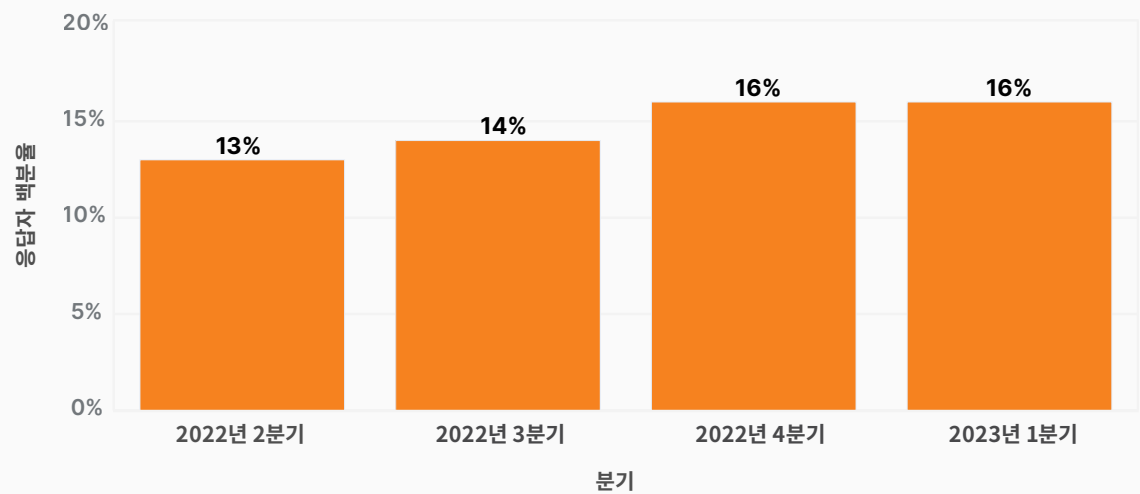
사례 연구: 랜섬 DDoS 공격의 표적이 된 글로벌 Fortune 500대 기업

랜섬 강탈로도 알려진 랜섬 DDoS(RDDoS) 공격은 악의적인 당사자가 DDoS 공격으로 개인이나 조직을 위협하여 금품을 갈취하려는 시도입니다. 랜섬 DDoS 공격 시도는 2022년 내내 꾸준히 증가했고 2023년 1분기에는 Cloudflare 고객의 16% 이상이 DDoS 공격의 일부로 위협을 당하거나 랜섬 관련 요구를 받았습니다.

랜섬 DDoS 공격은 랜섬웨어 공격과 혼동되는 경우가 많지만, 작동 방식이 다르고 더 수행하기 쉽습니다. 랜섬 DDoS 공격은 피해자가 이메일을 열거나 링크를 클릭하도록 속일 필요가 없으며, 네트워크 침입이나 기업 자산에 접근할 수단이 필요하지도 않습니다. 또한 서비스형 랜섬웨어의 가용성이 증가함에 따라 공격자는 적은 노력과 낮은 위험도로 랜섬 DDoS 공격을 수행할 수 있습니다.

분기별 Ransom DDoS 공격 및 위협

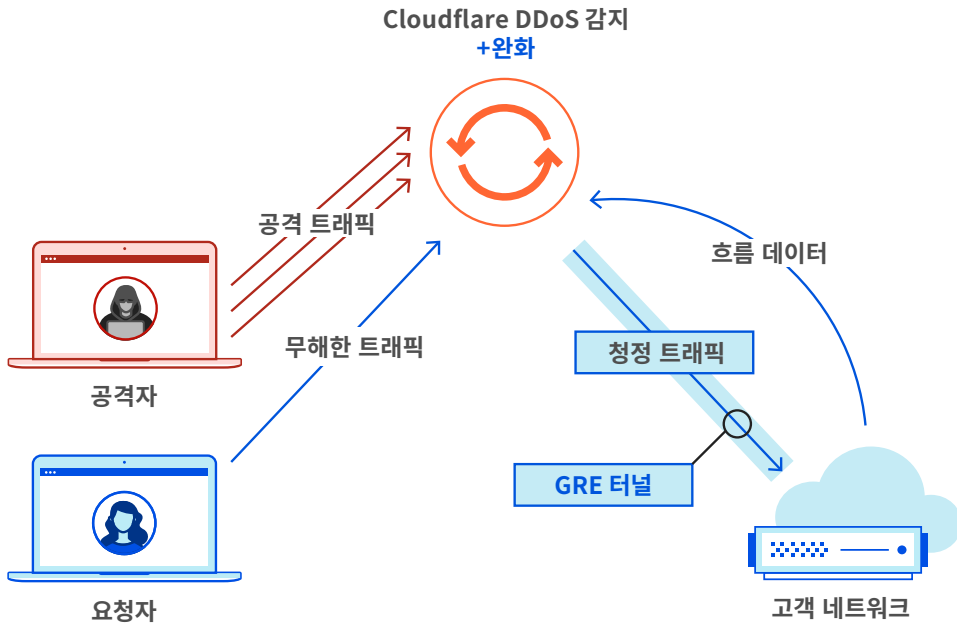
랜섬 DDoS 공격의 대상이 되었거나 위협을 받았다고 답한 응답자의 비율



2020년 말, 글로벌 Fortune 500대 기업 중 한 곳이 Cloudflare를 사용하여 DDoS를 완화하기 전에 Lazarus Group이라고 주장하는 자들로부터 RDDoS 공격의 대상이 되었습니다. 이 그룹은 북한 정부가 운영하는 것으로 추정되는 사이버 범죄 집단입니다. 공격자는 처음에 비트코인을 요구하는 이메일을 보내 일주일 안에 '지불하지' 않으면 두 번째 대규모 공격을 감행하고 몸값이 올라갈 것이라고 협박했습니다.

이 기업은 랜섬 메모를 받고 글로벌 데이터 센터 중 한 곳으로 향하는 트래픽이 크게 늘어난 것을 확인한 후, 온디맨드 스크러빙 센터 서비스에 연락했습니다. 벤더 서비스를 활성화하고 스크러빙 센터로 트래픽을 리디렉션하는 데 30분이 넘게 걸렸습니다. 또한 온디맨드 서비스를 활성화한 후 네트워킹 장애와
여러 인시던트가 발생했습니다.

초기 공격과 온디맨드 공급자와의 문제가 발생한 후, 이 기업은 Cloudflare Magic Transit을 온보딩하기로 결정했습니다. 이 기능은 상시 가동되어 네트워크 계층 DDoS 공격으로부터 보호해 줍니다. 공격자는 두 번째 대규모 공격을 수행할 것이라고 단언했지만 공격이 발생하지는 않았습니다.



네트워크 계층에서 DDoS 방어 기능을 제공하는 Cloudflare Magic Transit

"주요 차별화 요소 하나는 기존 공급자가 제공하지 못했던 공격 및 트래픽 분석입니다. 전혀 모르고 있었던 공격을 자동으로 완화하고 있습니다."

사고 대응 및 포렌식 팀
글로벌 Fortune 500대 기업

결론

팬데믹 이후 DDoS 공격의 빈도와 복잡도가 증가함에 따라 합법적인 트래픽을 유지하여 수익을 보호하는 것이 중요해졌습니다. Cloudflare를 사용하면 다른 공급자에서 흔히 발생하는 대기 시간 문제나 높은 비용 문제 없이 공격으로부터 빠르고 쉽게 보호할 수 있고 상시 가동 클라우드 전략을 쉽게 선택할 수 있습니다.

Cloudflare로 네트워크 DDoS 공격을 보호하는 방법을 자세히 알아보려면, 데모를 요청하세요.

기본 제공 Zero Trust 기능, DDoS 완화, 네트워크 방화벽, 트래픽 가속을 제공하는 하나의 전역 네트워크에 대해 자세히 알아보려면, 여기를 클릭하세요.

출처

1 Langrock, Sam. “The Cloud has Complicated Attack Surface Management.” Recorded Future, 2023년 4월 3일, https://www.recordedfuture.com/the-cloud-has-complicated-attack-surface-management

2 “Uptime Institute’s 2022 Outage Analysis Finds Downtime Costs and Consequences Worsening as Industry Efforts to Curb Outage Frequency Fall Short.” Uptime Institute, 2022년 6월 8일, https://uptimeinstitute.com/about-ui/press-releases/2022-outage-analysis-finds-downtime-costs-and-consequences-worsening

3 Cimpanu, Catalin. “Bandwidth.com expects to lose up to $12M following DDoS extortion attempt.” The Record, 2021년 11월 1일, https://therecord.media/bandwidth-com-expects-to-lose-up-to-12m-following-ddos-extortion-attempt

4 Holmes, David, Blankenship, Joseph 등, “The Forrester Wave™: DDoS Mitigation Solutions, Q1 2021,” Forrester, 2021년 3월 3일

5 Didio, Laura. “The Cost of Enterprise Downtime,” TechChannel, 2021년 9월 30일. https://techchannel.com/IT-Stratgy/09/2021/cost-enterprise-downtime

6 “The Cost of Downtime for the Top US Ecommerce Sites,” Gremlin, 2023년 5월 8일 액세스, https://www.gremlin.com/ecommerce-cost-of-downtime

7 Crets, Stephanie. “Most consumers abandon a slow-loading ecommerce site.” DigitalCommerce360, 2020년 8월 21일. https://www.digitalcommerce360.com/2020/08/21/most-consumers-abandon-a-slow-loading-ecommerce-site

8 Duperre, Mathieu. “44 percent of gamers respond to latency by quitting their games — what can we do to stop this?” PocketGamer.biz, 2022년 10월 24일, https://www.pocketgamer.biz/asia/comment-and-opinion/79974/44-per-cent-of-gamers-respond-to-latency-by-quitting-their-games-what-can-we-do-to-stop-this

9 “Infinity Data and the battle to conquer latency.” Hazelcast 및 Intel, 2019년 11월. https://hazelcast.com/resources/infinity-data-report

+82 70 4515 6893 | enterprise@cloudflare.com | www.cloudflare.com

CLOUDFLARE