CLOUDFLARE®

클라우드에서 애플리케이션 보안 유지

DDoS, 데이터 손상 및 악성 봇에 대한 빠르고 배포하기 쉬우며 확장성 있는 계층적 방어

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

클라우드에서 애플리케이션 보안 유지

DDoS, 데이터 손상 및 악성 봇으로부터 보호하기 위한 빠르고 배포하기 쉬운 계층화된 방어

기업은 보안 태세를 더 강화해야 한다는 압력을 받고 있습니다. 이러한 압력을 가중시키는 세 가지 요인은 다음과 같습니다.

- 공격자는 더 강력하고 교묘해졌으며 더 큰 동기가 있습니다.
- 애플리케이션의 공용 API 노출, 더 높은 SaaS 채택률, 타사 애플리케이션과의 통합이 증가함에 따라 공격 노출 영역도 커지고 있습니다.
- 데이터, 개인 정보 보호 및 보안에 대한 공공 및 정부 기관의 정밀 조사가 강화되었습니다.

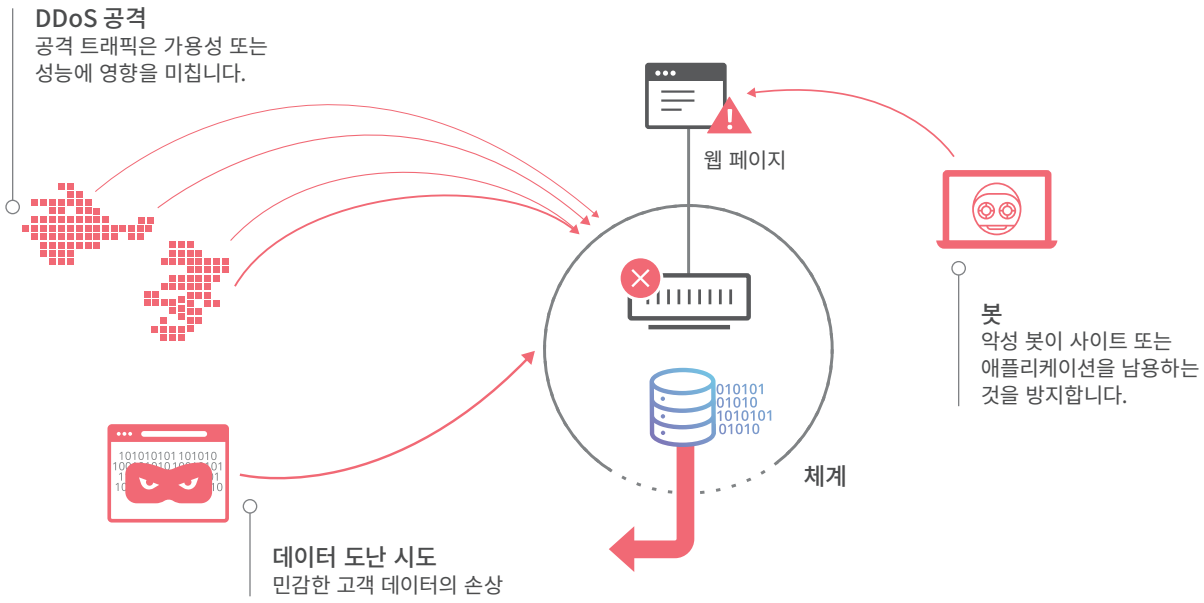
공격자는 DDoS(분산 서비스 거부) 공격의 빈도와 양을 늘리고 있습니다. 온라인상에서 봇넷과 수백만 개의 IoT(사물 인터넷) 기기를 활용하여 고도로 분산된 볼류메트릭 공격을 더 쉽고 효과적으로 수행할 수 있게 되었습니다.

전송할 수 있는 양이 많아졌을 뿐만 아니라 공격자는 네트워크 계층에서 애플리케이션 계층으로 초점을 이동하고 있습니다. 애플리케이션 계층 또는 "계층 7" 공격은 탐지하기 어렵고, 대개 더 적은 자원으로도 웹 사이트나 애플리케이션을 중단시키고 작동을 방해할 수 있습니다.

공격자는 사이트를 중단시키거나 중요한 데이터를 훔치려는 시도를 통해 사이트를 담보로 금전을 요구하는 등의 방식으로 수익을 얻을 수 있습니다. 결국 목표 기업은 금전을 지불하고 공격자는 더 큰 동기를 받아 조직화되며 만연하게 됩니다.

더 많이 노출됨에 따라 회사는 다음과 같은 세 가지 주요 문제와 위험에 대비하여 방어를 강화해야 합니다.

- 가용성이나 성능을 저하시켜 매출 감소, 운영 비용 증가 및 브랜드 평판 악화로 이어지는 애플리케이션, 웹 사이트 및 API에 대한 DDoS 공격
- PII(개인 식별 정보) 또는 지적 재산과 같은 중요한 고객 및 비즈니스 데이터의 손상과 그로 인한 고객 및 신뢰 상실
- 콘텐츠 스크래핑, 계정 탈취 및 사기성 결제를 통해 고객 애플리케이션을 남용하는 악성 봇



DDoS, 데이터 유출 또는 악성 봇에 대한 달러 피해는 회사의 규모나 업종에 따라 다를 수 있지만 비즈니스에 미치는 영향의 심각도는 모든 비즈니스에서 커지고 있습니다.

2015년 IDC 보고서에 따르면 인프라 중단 시간의 평균 피해액은 시간당 10만 달러입니다.[1]

데이터 손상으로 인해 사용자 정보가 유출될 수도 있고 애플리케이션의 데이터 저장소에서 신용 카드 및 암호와 같은 중요한 고객 데이터가 반출될 수도 있습니다. 2017년 분실 또는 도난 기록당 데이터 침해 비용은 전 세계 평균 141달러였고 데이터 침해로 인한 평균 총 비용은 362만 달러였습니다.[2] 정부와 언론의 감시가 강화됨에 따라 회사는 재정적으로 손해를 볼 뿐 아니라 대중의 신뢰를 잃게 되어 아주 작은 데이터 손상만으로도 큰 손실을 보고 있습니다.

악성 봇은 사용자 계정을 탈취할 수 있을 뿐 아니라 사기성 결제 및 콘텐츠 스크래핑을 수행할 수 있습니다. 제한적으로 공급되는 재고를 반복적으로 자동 구매하는 봇의 결제 사기는 매장 브랜드에 해를 끼치고 미래의 고객 창출을 막아 향후 매출 감소를 초래할 뿐 아니라 공급 업체와의 관계도 훼손할 수 있습니다. 특히 광고 중심 비즈니스에서 콘텐츠 스크래핑이 발생하는 경우, SEO 순위가 낮아지거나 CPM(웹 페이지 광고 노출률)이 줄거나 광고주를 잃음으로써 수익 감소의 직접적인 원인이 될 수 있습니다.

장점

늘어나는 노출과 비즈니스 영향의 증가 모두에 맞서려면 기업은 구체적인 전략적 문제를 해결할 뿐 아니라 끊임없이 진화하는 위협 환경에서 불량 행위자보다 앞서 있는 강점을 찾아내야 합니다.

세 가지 중요한 차이점은 **규모, 성능 및 사용 편의성**입니다.

규모의 중요성

Cloudflare는 데이터 분석과 관련해 네트워크 규모 및 트래픽의 가변성이라는 이점을 제공합니다. Cloudflare는 600만 개가 넘는 고객 웹 사이트를 보호해온 경험을 바탕으로 신종 글로벌 위협에 대한 통찰력을 보유하고 있습니다. 그로 인해 Cloudflare의 DDoS 보호 및 웹 애플리케이션 방화벽은 가동 중지 시간과 수익 손실을 유발하는 공격으로부터 고객을 능동적으로 보호합니다.

규모에 맞게 설계된 Cloudflare의 네트워크는 속도와 복원력을 모두 제공합니다. 하루 3,000억 건이 넘는 요청에 대해 모든 서비스를 제공하기 위해 모든 데이터 센터의 각 서버에서 실행되는 DNS, 암호화 및 WAF와 같은 서비스는 대기 시간이 짧고 신뢰성이 높은 막대한 트래픽 부하를 처리할 수있습니다.

DDoS 공격의 규모가 커짐에 따라 네트워크의 규모와 복원력은 고객에게 이점이 됩니다. 116개가 넘는 Cloudflare의 데이터 센터 규모는 Anycast 네트워크와 결합하여 Cloudflare가 최대 규모의 분산 공격에도 저항할 수 있게 해줍니다.

성능 향상과 동시에 애플리케이션 보안 유지

전통적으로 고객은 보안과 성능 사이에서 절충해야 했습니다. TLS 및 WAF 솔루션으로 인해 사이트의 성능이 저하되는 경우가 많습니다. 예를 들어, 연결을 암호화하는 프로토콜인 TLS는 보안 세션을 1회 시작하는 데만 해도 최대 네 번의 왕복이 포함합니다. 이러한 추가 왕복은 대기 시간을 증가시킬 수 있습니다. 마찬가지로 WAF는 각 요청을 인라인으로 검사하기 때문에 추가 지연이 발생합니다.

[1] IDC, 개발 운영 및 중단 시간 비용: 포춘지 선정 1000대 모범 사례 수량화 지표, 스티븐 엘리엇, 2015년 3월
[2] Ponemon Institute, 2017년 데이터 침해 비용 조사, 2017년 6월

Cloudflare를 사용하면 보안을 위해 성능을 희생할 필요가 없습니다. 성능을 저하시키는 대신 Cloudflare의 보안 기능은 트래픽 가속화와 통합된 짧은 대기 시간의 보안 서비스를 통해 애플리케이션 성능을 향상시킵니다. TLS 1.3 및 글로벌 세션 재개를 지원하기 때문에 왕복 횟수는 줄어들고, 다중 다운로드를 허용하는 HTTP/2로 인해 페이지 로드 시간이 단축됩니다. Cloudflare의 보안 서비스는 캐싱 및 스마트 라우팅과 같은 트래픽 가속화 서비스와 통합되어 애플리케이션을 Cloudflare 없이 안전하지 않은 상태로 실행할 때보다 더 빠른 성능을 경험할 수 있습니다.

캐싱을 통해 웹 사이트 방문자는 정적 콘텐츠에 더 쉽게 접근할 수 있습니다. 이로써 원본 서버에 부하가 줄어들 뿐 아니라 애플리케이션의 응답도 빨라집니다. 스마트 라우팅을 통해 Cloudflare에서 원본까지의 가장 빠른 경로가 결정되면 동적 및 정적 콘텐츠가 가속화됩니다.

규모
복원력을 위한
완전한 설계

사용 편의성
민첩한 구성 및 관리를 위한
직관적 UI 및 API

속도
트래픽 가속과 통합된
고성능 보안

사용 편의성으로 인한 보안 상태 개선

사용자 및 관리자를 위한 보안 솔루션의 사용 편의성은 보기 좋은 인터페이스 구현에 그치지 않고 회사의 보안 상태를 개선하는 데도 기여합니다. Gartner의 연구에 따르면 2020년까지 방화벽 침해의 99%가 결함이 아닌 단순 방화벽 구성 오류로 인해 발생할 것으로 예상됩니다.[3]

유용한 사용자 환경(UX)으로 인해 구성 오류로 인한 보안 위험은 줄어들고 끊임없이 변화하는 위협 환경에서 민첩성은 향상됩니다. Cloudflare 설정은 완료하는 데 5분도 걸리지 않습니다. 이러한 사용 편의성 덕분에 회사는 보안 전문가가 아닌 직원에게 더 많은 보안 정책 관리를 맡기고, 정책을 변경하고 새 정책을 배포하는 데 걸리는 시간을 줄이며, 복잡한 애플리케이션의 보안 상태를 더 시기적절하게 조정할 수 있습니다.

Cloudflare는 다음과 같은 세 가지 주요 문제로부터 고객을 보호하기 위해 이러한 이점을 활용합니다. 애플리케이션의 성능과 가용성을 저하시킬 수 있는 DDoS 공격, 다중 벡터 공격으로 인한 고객 데이터 손상 및 악성 봇의 웹 사이트 남용

DDoS로부터 애플리케이션 보호

DDoS 공격은 사이트 또는 서비스를 중단시키기 위해 대량의 트래픽을 전송합니다. 원본 서버에 과부하가 걸리면 이 악성 트래픽으로 인해 대상 애플리케이션이 느려지거나 최종 사용자가 애플리케이션을 사용할 수 없게 됩니다. Cloudflare는 다중 계층 방어 기능을 제공합니다.

[3] Gartner, Inc., 대부분의 기업에서 모범 사례가 된 방화벽 브랜드, 애덤 힐스 및 라이프릿 카울, 2017년 6월 5일,

전역 Anycast 네트워크

116개가 넘는 데이터 센터로 이루어진 Anycast 네트워크로 인해 Cloudflare가 DDoS 공격을 분산시킬 수 있는 영역이 늘어납니다. Anycast를 통해 여러 컴퓨터가 동일한 IP 주소를 공유합니다. Anycast IP 주소로 요청이 전송되면 라우터는 네트워크에서 가장 가까운 컴퓨터로 요청을 보냅니다. 이를 통해 DDoS 트래픽의 일부가 단일 지점에 집중되는 대신 각 데이터 센터에 흡수되기 때문에 봇넷에 의한 고도로 분산된 공격이 완화됩니다.

에지에서 이루어지는 지능형 및 자동 완화

Cloudflare는 600만 개 사이트 전체에서 가시성을 보유하고 있으므로 DDoS 보호 서비스에서는 한 사이트에 대한 공격을 기반으로 둔 경험적 접근을 발전시켜 다수의 다른 사이트를 보호할 수 있습니다.

네트워크 흐름 및 HTTP 공격 트래픽의 핑거프린팅을 통한 자동 완화 기능으로 공격 트래픽이 고객 사이트를 손상시키기 전에 미리 식별하여 중지시킵니다.

이러한 대용량 공격을 네트워크 에지에서 삭제함으로써 고객의 원본 서버를 보호하여 온라인 상태로 유지합니다.

DNS, 네트워크 및 계층 7 보호의 통합 스택

각 에지 서버에는 DNS, 방화벽, Rate Limiting 및 WAF와 같은 보안 서비스 통합 스택이 있으므로 Cloudflare는 분산 보호뿐 아니라 특히 DNS, 네트워크 및 애플리케이션 계층 DDoS와 같은 다양한 유형의 DDoS 공격에 맞선 계층적 방어를 제공할 수 있습니다.

Cloudflare의 분산 DNS 서비스는 도메인 이름 서버에 대한 공격을 막아낼 수 있습니다. 계층 3 및 4와 같은 네트워크 공격을 자동으로 차단할 뿐 아니라, 고객은 IP 방화벽을 통해 IP, 출처 국가 또는 ASN별로 악성 소스를 차단하도록 이 서비스를 구성할 수 있습니다. 보안 설정을 통해 600만 개 웹 사이트의 모든 IP 주소에 대한 Cloudflare의 가시성을 활용함으로써, 식별된 불량 트래픽을 사전에 차단할 수 있습니다.

> 당사는 Cloudflare를 설치하면 따로 신경을 쓰지 않아도 어떠한 종류의 악성 DDoS 공격에도 영향을 받지 않을 것이라는 믿음을 통해 얻게 되는 마음의 평화를 사랑합니다.

BUYCRAFT | 리 맥닐 CTO

구성 가능한 속도 기반 완화

Cloudflare의 DDoS 솔루션이 볼류메트릭 네트워크 및 애플리케이션 공격으로부터 고객을 자동으로 보호하지만 소량의 악성 트래픽으로부터 자신을 보호할 수 있는 구성 가능 제어 장치가 필요한 고객도 있습니다.

고객은 요청 속도 임계값, 대상 URI, 메서드 및 응답 코드와 같은 요청 특성을 사용자 지정할 수 있어 자신의 애플리케이션 및 트래픽 프로필을 기반으로 하여 방어력을 유연하게 조정할 수 있습니다.

계층적 방어를 통한 데이터 손상 위험 감소

공격자는 고객 데이터를 손상하려 할 때 여러 가지 공격 벡터를 사용하는 경우가 많습니다. 자신을 보호하려면 회사에 계층적 방어가 필요합니다.

공격		CLOUDFLARE 솔루션
1. 양식 및 API를 통한 악성 페이로드 삽입	→	WAF를 통한 상위 OWASP 및 신종 애플리케이션 수준 공격을 차단
2. 고객이 입력한 암호화되지 않은 중요 데이터를 스누핑	→	SSL/TLS 블록 스누핑을 통한 암호화
3. 로그인 페이지에 대한 무차별 암호 대입 공격	→	Rate Limiting을 통한 로그인 보호
4. 공격자는 DNS 응답을 위조하여 고객 자격 증명을 가로채려고 함	→	복원력이 있는 DNS 및 DNSSEC를 통해 위조된 응답을 방지

안전한 DNS를 통한 스푸핑 감소

캐시 중독 또는 '스푸핑'의 경우, 의심 없이 사이트를 방문하는 사용자를 속여 공격 대상 사이트에 신용 카드 번호 등 중요 데이터를 입력하도록 합니다. 이러한 유형의 공격은 공격자가 잘못된 레코드가 있는 DNS 이름 서버의 캐시를 감염시킨 경우에 발생합니다. 캐시 항목이 만료될 때까지 해당 이름 서버는 가짜 DNS 레코드를 반환합니다. 방문자는 올바른 사이트로 이동하는 대신 공격자의 사이트로 연결되어 상습범이 중요한 데이터를 도용하도록 허용할 수 있습니다.

DNSSEC은 암호화 서명을 사용하여 DNS 레코드를 확인합니다. DNS 확인자는 레코드와 관련된 서명을 점검하여 요청한 정보가 메시지 가로채기(man-in-the-middle) 공격자가 아닌 권한이 있는 이름 서버에서 온 것인지 확인할 수 있습니다.

암호화를 통한 스푸핑 감소

공격자는 고객 세션을 가로채거나 '스누핑'하여 암호나 신용 카드 번호와 같은 자격 증명을 비롯한 중요 고객 데이터를 훔칠 수 있습니다. 메시지 가로채기(man-in-the-middle) 공격의 경우 브라우저는 암호화된 채널에서 서버와 통신하고 있다고 생각하고 서버는 브라우저와 대화하고 있다고 생각하지만 사실은 둘 다 중간에 있는 공격자와 교신하고 있는 것입니다. 모든 트래픽은 어떤 데이터라도 읽고 수정할 수 있는 이 중재자를 거칩니다.

빠른 암호화/해지, 간편한 인증서 관리 및 최신 보안 표준 지원을 통해 고객은 안전하게 사용자 데이터를 전송할 수 있습니다.

자동 업데이트를 지원하고 확장성 있는 WAF를 통한 악성 페이로드 차단

공격자는 데이터베이스나 사용자 브라우저에서 중요한 데이터를 빼낼 수 있는 악성 페이로드를 제출하거나 대상 시스템을 손상할 수 있는 맬웨어를 주입하여 애플리케이션 취약점을 남용합니다.

WAF(웹 애플리케이션 방화벽)는 의심스러운 트래픽을 찾는 웹 트래픽을 검사합니다. 그런 다음 적용하도록 요청한 규칙 집합을 기반으로 하여 부적절한 요청을 자동 필터링할 수 있습니다. WAF는 GET 및 POST 기반 HTTP 요청을 모두 확인하고 OWASP의 상위 10개 취약점을 다루는 ModSecurity 핵심 규칙 집합과 같은 규칙 집합을 적용하여 차단, 시도 또는 전달할 트래픽을 결정합니다. 또한 댓글 스팸, 교차 사이트 스크립팅 공격 및 SQL 삽입을 차단할 수 있습니다.

Cloudflare WAF는 600만 고객이 식별한 위협을 기반으로 하여 규칙을 업데이트하고, 대기 시간이 짧은 검사 및 트래픽 가속화와의 통합으로 인해 애플리케이션 성능에 영향을 미치지 않으면서도 고객을 보호할 수 있습니다.

로그인 보호를 통한 계정 탈취 방어

공격자는 폐기된 자격 증명으로 로그인을 자동화함으로써 '사전 공격'을 수행하여 '무차별 암호 대입'을 통해 로그인 보호 페이지에 로그인할 수 있습니다. Cloudflare를 사용하면 Rate Limiting 규칙을 사용자 지정하여 이처럼 탐지하기 어려운 공격을 에지에서 식별하여 차단할 수 있습니다.

모니터링 및 점수 매기기를 통한 보호

Cloudflare의 타사 애플리케이션은 웹 사이트에서 취약성을 모니터링하고 회사의 보안 성숙도를 평가하며 개발 프로세스에 통합됨으로써 사전 예방적인 보호 계층을 추가로 제공합니다.

> Cloudflare의 보안 기능 덕분에 개발자는 사이트를 온라인 상태로 유지하는 것에 대해 걱정할 필요 없이 다른 사이트를 개선하는 데 집중할 수 있었습니다.
>
> Gazeta Esportiva | 데이비드 버졸라, 기술 책임자

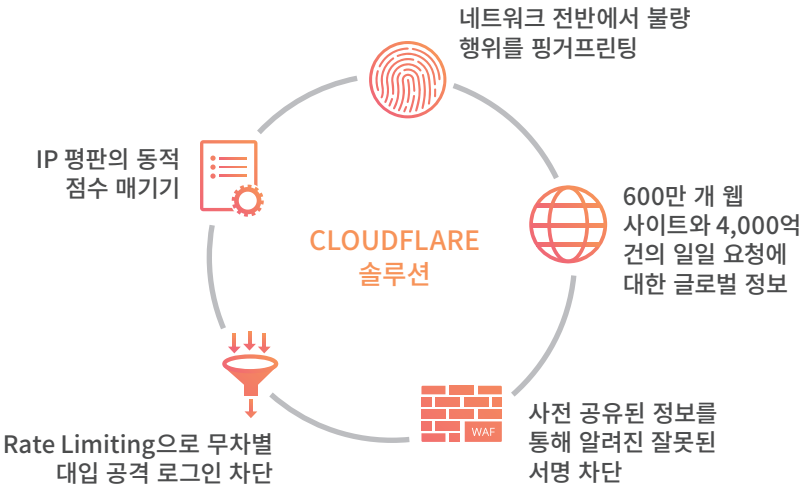
악성 봇 방지

세 가지 형태의 악성 봇은 빈도, 정교함 및 고객 영향이 증가 및 향상되고 있습니다. 결과적으로 봇 예방 솔루션이 다양한 잠재적 공격 프로필을 처리하려면 여러 가지 요소가 필요합니다.

가장 일반적인 공격은 계정 탈취, 콘텐츠 스크래핑 및 사기성 결제입니다. 세 가지 모두 서로 다른 봇 '스타일'을 사용할 수 있으며 각 스타일은 서로 다른 접근 방식으로 감지하여 완화할 수 있습니다.

공격

1. 계정 탈취
2. 콘텐츠 스크래핑
3. 사기성 결제



속도 기반 감지 및 완화

일부 봇은 자동화되어 있고 목표를 달성하기 위해 빠른 속도로 사이트를 공격해야 하므로 속도 기반 자동화는 이러한 공격을 감지하여 완화할 수 있습니다. 예를 들어, 무차별 암호 대입을 통한 로그인은 일반 사용자보다 단일 IP 주소에서 로그인 실패 비율이 더 높습니다. 속도 기반 임계값을 통해 이러한 유형의 계정 탈취 시도를 감지할 수 있습니다. 이와 마찬가지로 찾을 수 없는 페이지(404 오류)를 공격하는 콘텐츠 스크래퍼는 일반 사용자보다 더 빠른 속도로 이 페이지를 생성합니다.

알려진 잘못된 서명을 기반으로 한 차단

Cloudflare에서 보호를 받는 600만 개의 웹 사이트에서는 악성 봇에 대해 알려진 잘못된 서명이 한 사이트에서 감지되면 다른 모든 사이트에서도 차단됩니다.

결론

끊임없이 진화하는 위협 환경에서 기업이 상시적인 안전성과 '상시 온라인 상태'를 유지하려면 서비스 거부, 데이터 절도 및 악성 봇으로부터 보호할 수 있는 성능, 대규모 지능형 보안 및 계층형 방어가 필요합니다.

인간은 항상 전체 목표의 일부이므로 보안 정책을 배포, 구성 및 미세 조정할 때의 사용 편의성은 사용 중 오류를 줄이고 더 많은 직원이 위험이나 불필요한 마찰 없이 변경 사항에 대응할 수 있도록 함으로써 전반적인 보안 상태에 영향을 미칩니다.

Cloudflare의 클라우드 보안은 점점 더 정교해지는 DDoS 공격, 상습범과 악성 봇의 데이터 손상 시도를 방어합니다.

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

© 2017 Cloudflare Inc. All rights reserved.
Cloudflare 로고는 Cloudflare의 상표입니다. 기타 모든 회사 및 제품 이름은 연관된 각 회사의 상표일 수 있습니다.