장비는 이제 안녕

레거시 장비를 버리고 민첩하고 확장 가능한 서비스형 애플리케이션 보안을 이용하세요

보안 장비의 문제점

하드웨어 보안 장비는 정교한 최신 애플리케이션 공격에 대응하는 데는 적합하지 않습니다. 장비는 유지하고 관리하는 데 비용이 많이 들고 다운타임이 발생하며 공격이나 높은 수요에 따른 트래픽 급증을 처리할 설비를 갖추고 있지 않습니다. 기술이 발전하고 기업 규모가 늘어나므로 조직에서는 처리량에 맞추어 3~7년마다 새로운 하드웨어를 구매해야 합니다. 또한 하드웨어를 업그레이드하거나 유지 보수를 진행 중일 때 보안 서비스는 오프라인 상태가 되므로 보호 격차가 생길 수 있습니다. 게다가 장비는 최대 예상 수요를 처리할 만큼 적절한 크기여야 하며, 크기가 적절하지 않으면 활용도가 낮아지거나 예상되는 수준 이상의 트래픽을 처리할 수 없어 애플리케이션은 무방비 상태가 됩니다.

클라우드 기반 보안으로 전환하면 조직이 인프라와 운영을 간소화할 수 있을 뿐만 아니라 하드웨어 교체가 불필요하고, 무분별한 벤더 확장이 줄어들며, 데이터 센터 간접비를 절감하여 상당한 비용을 절감할 수 있습니다.

Cloudflare의 차별성

에지 서버의 Cloudflare 전역 네트워크는 대기 시간을 줄이고 웹 사이트 성능과 보안을 개선합니다. Cloudflare는 DDoS 방어, 웹 애플리케이션 방화벽(WAF), 봇 보호 등 다양한 웹 기반 공격으로부터 보호하는 데 유용한 보안 기능을 폭넓게 제공합니다. 클라우드 네이티브 아키텍처는 새롭게 떠오르는 위협에 대응하기 충분합니다. 예를 들어 Cloudflare의 엔지니어 팀이 관리형 규칙에 적용될 새로운 WAF 규칙을 릴리스하면, Cloudflare 사용자는 프로덕션에서 10~15초 내에 곧바로 보호 받을 수 있습니다. Cloudflare는 통합 보안 및 성능 올인원 솔루션입니다. 성능과 보안을 다루는 하나의 제어판 솔루션은 보안 팀에서 인시던트를 신속하게 인지하고 대응하는 데 유용합니다.

확장 가능하고 사용하기 쉬움

Cloudflare를 이용하는 조직은 필요에 따라 리소스를 사용할 수 있으며 성능에 영향을 주지 않으면서도 대규모 DDoS 공격을 흡수할 수 있습니다.

Cloudflare를 이용하면 수동 구성 및 관리를 최소화하는 동시에 자동 위협 조사 및 인시던트 대응이 더 빨라집니다.

새로운 공격 신속 방어

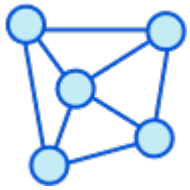
Cloudflare의 클라우드 네이티브 보안 스택은 방대한 전역 네트워크에서 가져오는 위협 인텔리전스를 이용하여 조직에서 새로운 보안 패치 또는 장비 업데이트를 기다릴 필요 없이 이러한 공격에 정면으로 대응하는 것을 돕습니다.

비용 효과성

Cloudflare는 구성 및 관리에 소요되는 귀중한 엔지니어링 시간을 줄여주므로 우선순위가 가장 높은 이니셔티브에 집중할 수 있습니다.

하드웨어 비용을 미리 지불하는 대신 필요할 때 리소스 필요량에만 비용을 지불할 수 있어 효율적으로 확장할 수 있습니다.

보안에 확장성이 매우 중요한 이유는 무엇인가요?



Cloudflare를 통해 사용자는 DDoS 공격이나 수요가 높은 제품 출시와 같은 피크 시간에 필요에 따라 리소스를 활용하여 트래픽 급증에 대응할 수 있습니다. 게다가 무제한 DDoS 및 레이트 리미팅 솔루션도 제공하므로 비용이 치솟을까 우려하거나 애플리케이션을 방어할 리소스를 할당하는 데 어려움을 겪지 않아도 됩니다.

Cloudflare의 네트워크는 최대 규모의 DDoS 공격도 흡수할 수 있어 비즈니스가 온라인 상태를 유지할 수 있습니다.

보안 장비 벤더와 Cloudflare를 비교해 확인하세요

	레거시 보안 장비	Cloudflare 애플리케이션 보안
하드웨어 비용	업데이트 비용 및 데이터 센터 간접비 등의 하드웨어 비용.	하드웨어 비용이 들지 않음.
엔지니어링 시간	하드웨어 및 소프트웨어 수명 주기 관리를 포함해 복잡한 스크립팅 및 유지 관리 오버헤드에 많은 시간이 소요되므로 엔지니어링 비용이 많이 들 수 있음.	사용하기 쉬운 제품 덕분에 한 곳의 벤더를 관리하는 데 소요되는 엔지니어링 시간이 단축되고, 엔지니어는 더 영향력 있는 프로젝트를 진행할 수 있음.
보안	장비 벤더의 애플리케이션 보안: • 강력하고 사용자 지정이 가능하지만 그다지 민첩하지 않음 • 유지 보수 시 다운타임이 있으므로 애플리케이션은 보호되지 않은 채로 방치됨 • 인터넷에서 최대 규모의 DDoS 공격을 흡수 또는 대응할 수 없거나 피크 트래픽 수요를 처리할 수 없음	장비 벤더와 비교한 Cloudflare 보안의 이점: • 평균 공격 감지 시간 50% 이상 단축 • Cloudflare의 규모와 전역 네트워크를 통해 위협에 신속하게 대응하고 공격 시도를 30~40% 더 많이 감지할 수 있음 • 일반적으로, 이러한 평균 공격 복원 시간 90% 이상 단축
회계상의 영향	장비는 자본 비용임: • 선불 취득 비용이 필요하며 여러 해에 걸쳐 가치가 떨어질 수 있음 • 기업은 피크 요구 사항을 뒷받침하기 위해 하드웨어를 구입해야 하지만, 그 외 시간에는 하드웨어를 충분히 활용하지 못함	운영 비용에서 자본 지출, 감가 제외됨: • Cloudflare의 회계상의 이점은 더욱 즉각적 • 고객은 Cloudflare의 운영 지출 모델로 초기 비용 없이 특정 요구 사항을 충족하도록 환경을 쉽게 확장할 수 있음
구현 시간	• 하드웨어 리드 타임(공급망 문제로 늘어남) • 장황한 설정 프로세스 • 모든 장치에 구성이 일관되게 배포되도록 중앙 관리 스크립트를 작성해야 하는 경우가 많음	• 모든 도메인에서 보안을 중앙에서 쉽게 관리할 수 있음 • 하드웨어를 제공 받아 마련한 이후라 해도, Cloudflare는 애플리케이션 벤더와 비교해 가치 창출 시간을 최소 10배 더 빠르게 제공함