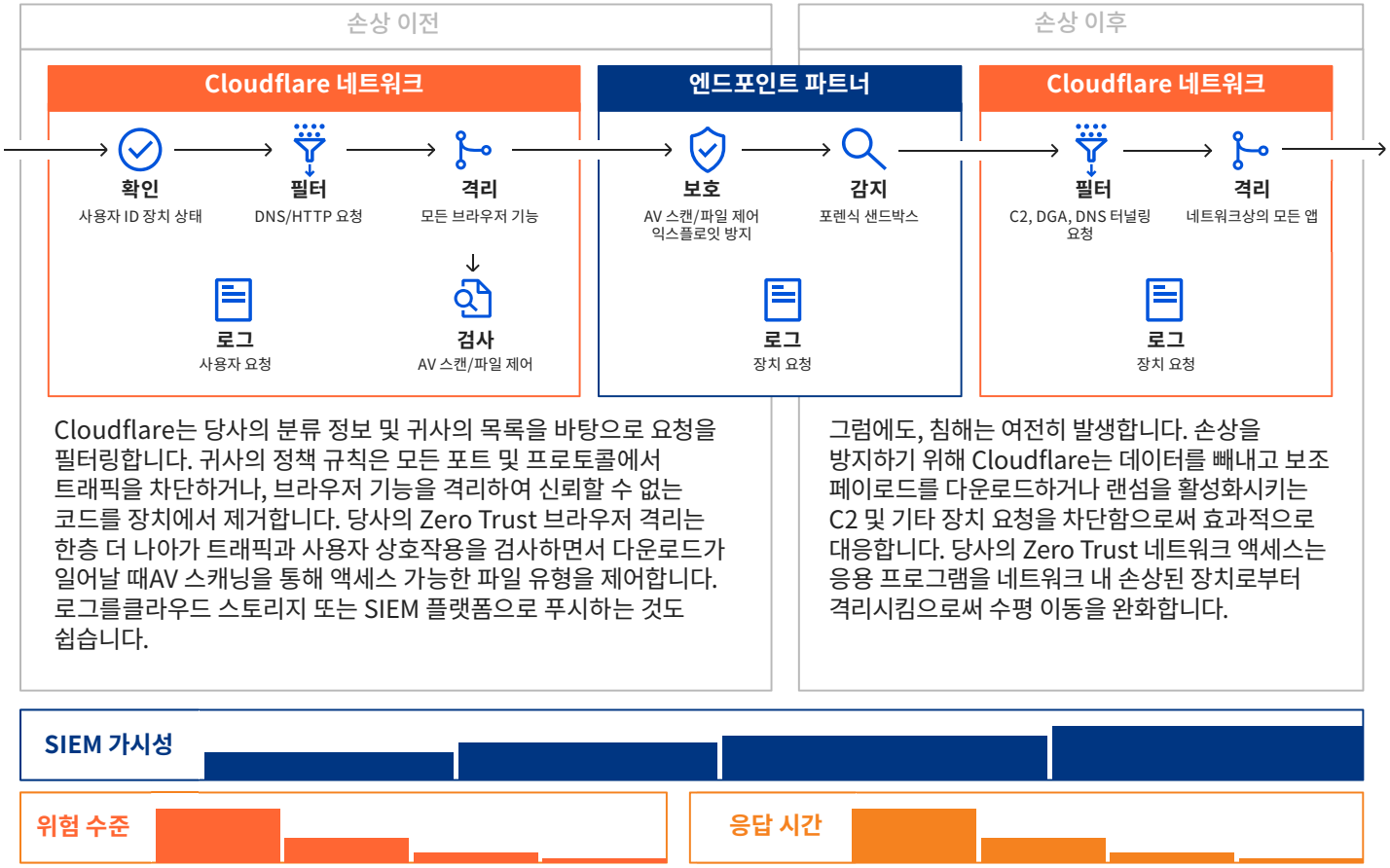
더 간단하고 더 효과적인 위협 방어

맬웨어, 피싱, 크립토마이닝 등의 공격은 충격이 상당합니다. 충격을 완화해 주세요.

끊임없이 변화하는 위협에 맞서려면 몇 겹에 걸친 방어막이 최선입니다. 하지만 보안을 강화한다는 취지로 너무 많은 도구를 사용하면 비용이 커지고 더 복잡해질 뿐만 아니라 성능까지 저하될 수 있죠. 규모가 작은 조직은 위험을 줄일 수 있는 더 간단한 방법을 원하고, 중간 규모 조직 역시 더 효과적인 대응 방법을 원하며, 규모가 큰 조직도 마찬가지로 한 곳에서 모든 것을 파악할 수 있는 가시성을 필요로 합니다.

Cloudflare는 이전에는 별개였던 여러 보안 서비스들을, 심지어 브라우저 내에서 이루어지는 모든 엔드포인트 컴퓨팅을 이동시키면서, 방대한 Anycast 에지 네트워크에서 구동되는 하나의 Zero Trust 플랫폼으로 통합합니다. 더 나은 위협 방어는 Zero Trust에서부터 시작됩니다. 장치를 기업 리소스에 연결시키기 전에 안전하게 관리되는 장치인지를 먼저 검증하죠.

솔루션: 네트워크 전반에 걸친 통합 위협 방어 및 엔드포인트 보안



Cloudflare는 당사의 분류 정보 및 귀사의 목록을 바탕으로 요청을 필터링합니다. 귀사의 정책 규칙은 모든 포트 및 프로토콜에서 트래픽을 차단하거나, 브라우저 기능을 격리하여 신뢰할 수 없는 코드를 장치에서 제거합니다. 당사의 Zero Trust 브라우저 격리는 한층 더 나아가 트래픽과 사용자 상호작용을 검사하면서 다운로드가 일어날 때AV 스캐닝을 통해 액세스 가능한 파일 유형을 제어합니다. 로그를클라우드 스토리지 또는 SIEM 플랫폼으로 푸시하는 것도 쉽습니다.

그럼에도, 침해는 여전히 발생합니다. 손상을 방지하기 위해 Cloudflare는 데이터를 빼내고 보조 페이로드를 다운로드하거나 랜섬을 활성화시키는 C2 및 기타 장치 요청을 차단함으로써 효과적으로 대응합니다. 당사의 Zero Trust 네트워크 액세스는 응용 프로그램을 네트워크 내 손상된 장치로부터 격리시킴으로써 수평 이동을 완화합니다.

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

Cloudflare One Intel 플랫폼

정책 규칙에 따라 차단, 격리, 또는 SIEM으로 로그푸시할 보안 위험 범주

맬웨어	새로 보이는 도메인	DGA 도메인	스파이웨어
피싱	새 도메인	DNS 터널링	스팸
크립토마이닝	접근할 수 없는 도메인	C2 및 봇넷	익명성 도구

Cloudflare Intel은 당사의 네트워크 데이터 및 생태계로 인해 알려진 위협 및 새로운 위협을 효과적으로 차단합니다. 하지만…

- 벤더가 얼마나 많은 위협 사냥 프로그램 또는 위협 피드를 갖고 있든,
- 얼마나 많은 데이터나 머신 러닝을 사용하든,
- 인텔리전스가 얼마나 자주 업데이트되든, 얼마나 빠르게 실행되든,

… 필터와 검사만으로 위협을 100% 차단하지는 못합니다.

그리고 귀사의 보안 팀이 직원들의 업무를 방해하지 않으면서 조직에 대한 위험을 내포하고 있는 모든 사이트를 차단할 수는 없습니다. 결국엔 위협으로 인한 손해보다 생산성 손실과 IT 티켓 처리에 들어가는 비용이 더 커질 수도 있는 것이죠.

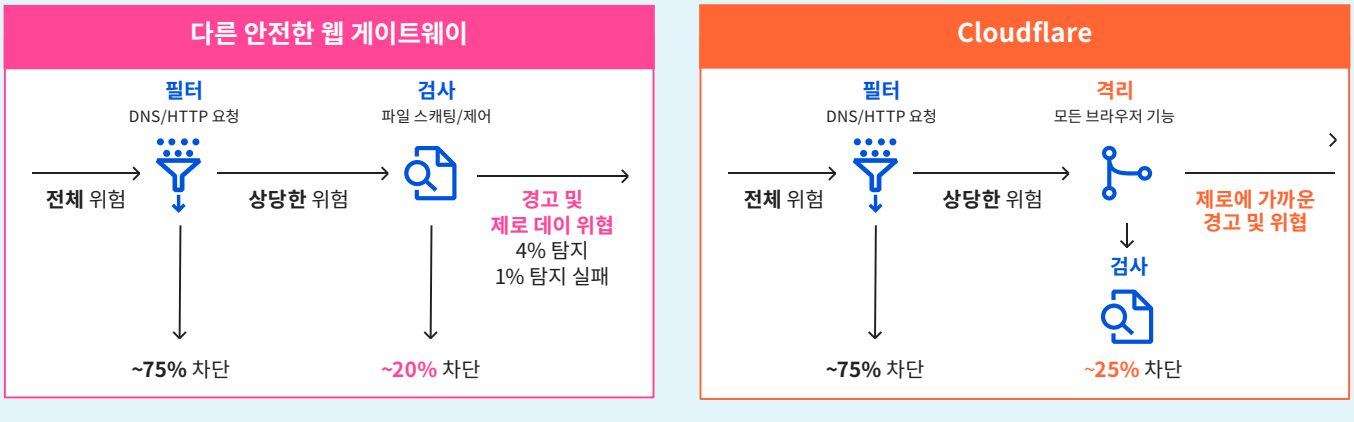
인터넷 브라우징에 대한 Zero Trust 접근법이 필요한 이유가 이것입니다. Cloudflare 브라우저 격리는…

- 매끄러운 사용자 경험을 번개처럼 빠르게 제공하고,
- 차단 해제된 모든 사이트에 대해 비용 효율적으로 사용할 수 있습니다.

미분류	위험	저위험

곧 제공될 기능:

- 전송 중인 데이터뿐 아니라 사용 중인 데이터까지 검사하고 제어.
- 다운로드한 파일을 저장할 위치를 지정.
- 자격 증명이 양식에 입력되지 않도록 방지.



오늘 문의해서 Cloudflare Zero Trust의 Enterprise 요금제 계정 액세스를 요청하세요.