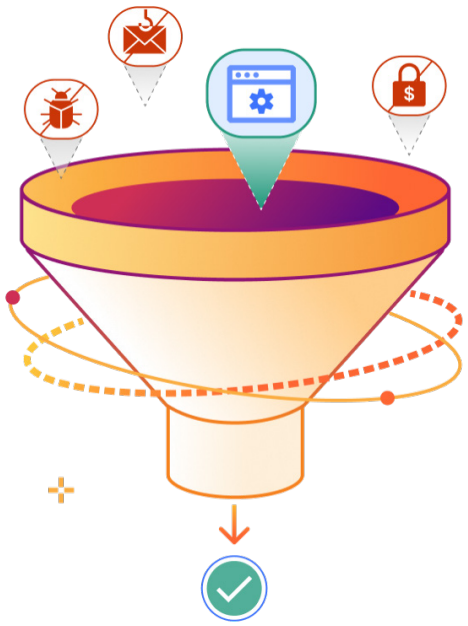
보안 웹 게이트웨이(SWG)

Cloudflare One에서 제공되는 구성 가능 서비스인 Cloudflare Gateway는 ID 인식 인터넷 필터링을 사용하여 사이버 위협으로부터 사용자와 데이터를 보호합니다.



간단한 최신 위협 방어

복잡한 레거시 웹 보안 대체

사이버 위협은 모든 곳에 있으며, 늘어나는 조직 공격면의 격차를 계속 악용하고 있습니다. 여러 포인트 솔루션(예: DNS 확인자, 웹 게이트웨이, 네트워크 방화벽)을 사용한다면 비용, 복잡성, 위험이 늘어나기만 합니다.

Cloudflare Gateway는 인터넷 및 내부 리소스 액세스를 일관적으로 보호하고 가시성을 제거하여 보안을 간소화합니다. 조직에 유용한 ID 인식 정책으로 사이버 위험을 줄이세요.

- **인터넷 위협 차단:** 랜섬웨어, 피싱, 명령 및 제어 등
- **L4-L7 트래픽 제어 및 모니터링:** DNS, HTTP, 네트워크, 브라우저 격리 규칙 이용
- **허용 가능한 사용 정책 시행:** 원격 근무자, 사무실 근무자 모두에게 적용

싱글 패스 아키텍처로 모든 트래픽을 확인하고 필터링하며 검사하고 위협에서 격리합니다.

현재의 SWG, 미래의 보안 서비스 에지(SSE)

SSE 아키텍처로 보안을 통합하고 Zero Trust 모범 사례를 수용하기 위해 일반적으로 SWG 제어 최신화 단계를 거칩니다.

Cloudflare와 이 여정을 함께한다면 어떨지 알아보세요.

왜 Cloudflare를 사용해야 할까요?

통합 보안

네트워크 1개

및 보안 서비스 에지(SSE), 웹 앱 및 API 보호(WAAP), 이메일 보안, 기타 도메인에 걸쳐 모든 서비스를 위한 제어판을 갖추고 있습니다.

방대한 위협 인텔리전스

2조 개

DNS 쿼리를 매일 처리합니다. 새롭고, 새로 확인되었으며, 위험한 도메인 전체에 실시간 가시성을 제공하여 AI/ML 기반 위협 사냥 모델을 강화합니다.

확장성이 뛰어난 설계

310개 이상의

네트워크 위치(120여 개국)를 갖추고 있습니다. 고객이 모든 SWG 및 Zero Trust/SSE 기능을 모든 위치에서 실행할 수 있으므로 언제나 빠르고 일관되게 적용됩니다.

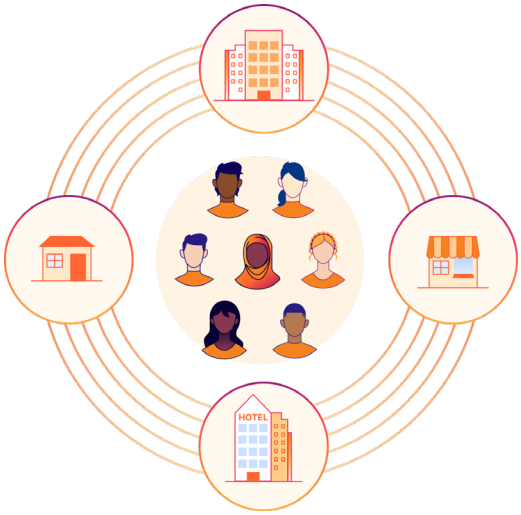
사용 사례: 원격 근무자 및 사무실 위치에 대한 위협 방어

문제

하이브리드 근무로 공격면이 확대되었으며 서로 다른 도구를 관리해야 하는 보안 격차가 생겼습니다. 이에 따라 랜섬웨어, 피싱, 기타 사이버 위협으로 인해 큰 비용이 발생하고 브랜드 평판에 손상을 입게 되기 쉬워졌습니다.

솔루션

Cloudflare의 SWG는 원격 및 사무실 근무자에게 일관적인 웹 보안을 제공합니다. 가치 창출 시간을 빠르게 만들기 위해 DNS 필터링을 시작한 다음, 모든 인터넷 활동에 좀 더 포괄적인 검사와 제어를 계층화하는 조직이 대부분입니다.



시작하기

Cloudflare 네트워크로 트래픽을 먼저 전송하여 DNS를 확인(이후 전체 HTTP 검사가 이어짐)

DNS 필터링 시행: 원격 근무자일 경우 ID / 장치 기반, 사무실 근무자일 경우 위치 기반

더욱 세분화된 제어 계층화: HTTP, 네트워크, 브라우저 격리 규칙 등

인라인으로 클라우드 이메일 보안 배포: MX로, API를 통해, 또는 두 방식 모두(멀티 모드)

먼저, 네트워크 안팎에서 사용자 웹 브라우징 보호

다음 단계, 이메일 보안 계층화

위험을 줄이면서도 팀 생산성을 높이세요

단순하고 유연한 배포

DNS 확인을 위한 네트워크 라우터를 사용합니다. GRE/IPsec 터널, WAN 커넥터 또는 기존 SD-WAN을 통해 L3 트래픽을 전송합니다.

또는, Cloudflare의 장치 클라이언트를 배포해 프록시 트래픽을 전달합니다.

빠르고 일관적인 보호

네트워크 전체에서 단일 경로 검사를 수행해 모든 곳에서 빠르고 일관적으로 정책을 적용합니다.

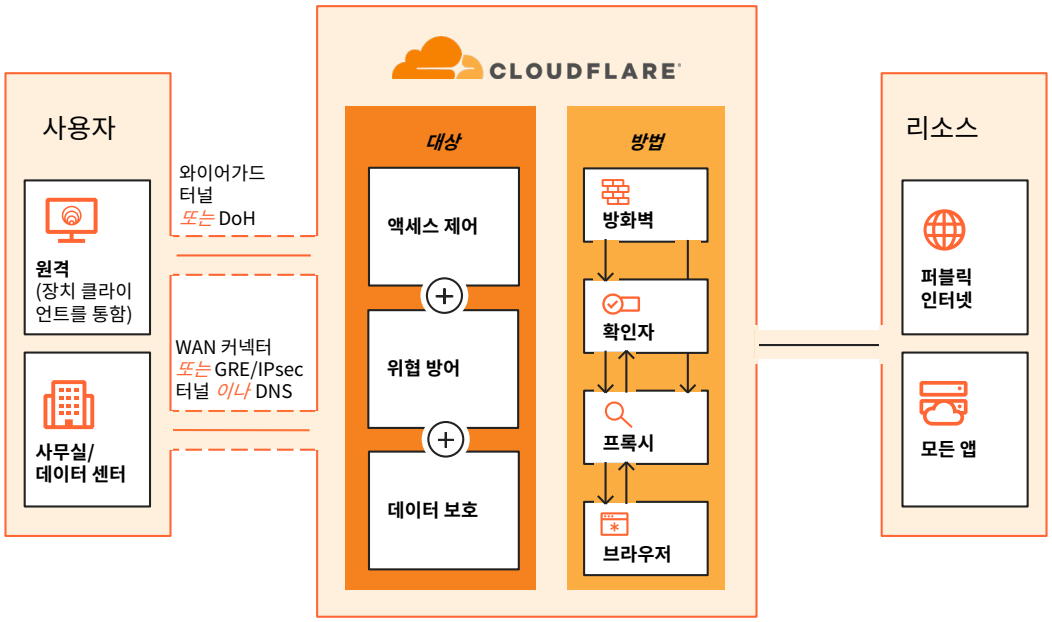
다른 벤더보다 성능이 빠른 것으로 입증되었습니다(예: Zscaler, Netskope, Palo Alto Networks).

Zero Trust 채택 가속화

구성 가능한 SSE/SASE 서비스를 망라하여 한 명의 정책 관리자가 이용하는 하나의 통합 제어판.

웹 및 이메일 보안에서 시작하고 원하는 속도로 다른 Zero Trust 제어를 계층화합니다.

SWG의 작동 방식



보안을 간소화하세요.

인터넷으로 향하는 트래픽과 내부 리소스 트래픽 모두에 방화벽, 확인자, 프록시, 브라우저 제어를 적용합니다.

하나의 정책 관리자로 정책을 구축합니다.

SWG 기반에서 SSE 제어를 계층화하세요

조직에서는 Cloudflare의 SWG를 통해 프록시 트래픽을 전달하여, 기본적으로 통합되어 있으며 구성 가능한 Cloudflare의 SSE 서비스 전반을 활용하여 보안 제어와 가시성을 넓힐 수 있습니다.

RBI를 통한 웹 활동 및 앱 활동 보호

- Cloudflare의 전역 네트워크에서 모든 브라우저 코드를 실행하여 로컬 장치 보호 - 대기 시간 짧음
- 장치 클라이언트 유무와 관계없이 DLP 스캔과 브라우저 제어(예: 복사-붙여넣기 차단, 업로드/다운로드 제한, 인쇄)로 앱을 격리하여 데이터 보호

멀티 모드 DLP 및 CASB로 데이터 보호

- HTTP(S) 트래픽과 사전에 정의된 파일(예: 금융/상태 데이터) 또는 사용자 지정 프로필(예: 정확한 데이터 일치)에 있는 중요한 데이터를 감지하고 차단하여 데이터 유출을 방지합니다
- 중요한 데이터에 통합 DLP 감지를 사용하여 잘못된 구성이 있는지 SaaS 제품군을 스캔하고 수정할 수 있도록 규범 조치를 취합니다

ZTNA로 ID 인식 액세스 정책 확장

- 셀프 호스팅 기업 앱, SaaS 앱, 사설 네트워크 IP, 호스트 이름에 대한 액세스를 제한하는 Zero Trust 규칙을 시행합니다
- ID 및 엔드포인트 보호 공급자를 한 번에 통합하고 동일한 규칙 빌더를 사용하여 인터넷 및 앱 액세스 규칙 전체에 상태 검사를 적용합니다

가시성 향상

- 관리되는 장치와 관리되지 않는 장치 전체에 자세한 감사 로그를 유지합니다(계약 요금제에서는 DNS 로그를 6개월 동안, HTTP 및 네트워크 로그를 30일 동안 저장함)
- 상관 관계 및 추가 분석을 위해 선호하는 SIEM으로 로그를 푸시합니다

게이트웨이 기능

위협 방어 및 보안 액세스	
보안 및 앱 카테고리	포괄적 범위(랜섬웨어, 피싱, DGA 도메인, DNS 터널링, 신규 및 새로 발견된 도메인, C2 및 봇넷, 기타 보안 위험)를 다룹니다. 인라인 CASB 범위는 AI를 포함하여 25가지 앱 범주에 달합니다.
재귀 DNS 필터링	도메인 및 IP 주소를 허용/차단/재정의하며 보안 또는 콘텐츠 범주를 기준으로 합니다. Tenant API를 통해 DNS 필터링을 관리하여 상위-하위 구조 구성이 가능합니다.
HTTP(S) 필터링 및 검사	트래픽 제어는 소스, 대상, 도메인, HTTP 메소드, URL 등에 따릅니다. HTTP1/2/3 검사로 AV 및 DLP 스캔, 파일 제어, 장치 상태, 테넌트, RBI 등을 사용할 수 있습니다.
무제한 TLS 1.3 검사	기본적으로 TLS 1.3 검사가 무제한입니다. 모든 HTTPS 트래픽을 해독하고, 정책을 적용하며, 요청은 Cloudflare 인증서 또는 사용자 지정 인증서 로 다시 암호화됩니다. 어느 경우든 시장을 선도할 만큼 대기 시간이 짧습니다. TLS를 통한 DNS(DoT) 및 HTTP를 통한 DNS(DoH) 표준을 지원합니다. FIPS 140-2를 준수하는 암호 제품군만 활성화합니다.
L4 FWaaS	L4 네트워크 정책이 모든 퍼블릭/프라이빗 TCP/UDP 패킷에 적용되어 감지된 프로토콜, 지리적 위치, SNI 도메인 등에 따라 HTTP 이외의 리소스에 대한 액세스를 제어합니다. 포트 22를 통해 SSH 트래픽을 감사합니다. (L3 FWaaS 기능은 WAN 네트워킹 서비스에서 기본 제공됩니다.)
바이러스 검사	스캔: 다양한 유형(PDF, ZIP, RAR 등)의 업로드/다운로드된 파일을 스캔합니다.
ID 및 장치 상태 확인	모든 주요 엔터프라이즈 ID 공급자, 소셜 ID, SAML 및 OIDC 표준에 따라 정책을 설정합니다. 장치 클라이언트 또는 타사 엔드포인트 보호 공급자를 통해 장치 상태를 확인합니다.
통합된 위협 인텔리전스	봇 인텔리전스는 Cloudflare AI/ML 모델과 타사 피드를 기반으로 합니다. 권한 및 재귀 DNS 확인자 중 규모가 가장 큰 편에 속하는(매일 2조 건 이상의 쿼리) 글로벌 원격 측정으로 자사 정보를 도출합니다. 웹 크롤러 역시 몇 주에 한 번씩 전체 웹(80억 페이지 이상)을 색인화하여 새롭게 떠오르는 캠페인 인프라를 찾아냅니다. 사용자 정의 위협 피드 및 서명(IP, URL, 도메인 등)도 지원합니다.
온램프(on-ramp) 및 오프램프(off-ramp)	
장치 클라이언트 사용	Cloudflare의 디바이스 클라이언트(WARP)를 통해 전체 WireGuard 터널을 거치거나 DoH를 이용해 프록시 트래픽을 전달합니다. MDM을 통해 자체 등록 또는 배포합니다. 장치 상태 검사가 가능해집니다. 장치가 네트워크에 있는지 감지합니다.
클라이언트리스 옵션	옵션: 고객 위치에서의 네트워크 라우팅 DNS 쿼리. Anycast GRE/IPsec 터널. WAN 커넥터, PAC 파일을 통한 프록시 엔드포인트. 재작성된 URL을 통한 클라이언트리스 웹 격리.
IPv4 및 IPv6 지원	모든 기능은 IPv4 및 IPv6 연결(IP6 전용 또는 듀얼 스택)로 사용할 수 있습니다.
트래픽 라우팅	
전용 송신 IPS 및 송신 정책	전용 정적 IP(IPv4 or IPv6) 범위가 있어 소스 IP에 따라 트래픽을 허용 목록에 추가하는 데 사용할 수 있습니다. 송신 정책 을 이용해 ID, 지리적 위치 또는 장치 상태 등의 속성에 따라 사용할 송신 IP를 선택합니다. 각 송신 IP 는 개별 계정에 고유하며 다른 고객이 사용하지 않습니다.
확인자 정책	DNS 요청을 사용자 지정 DNS 확인자로 라우팅하여 사설 네트워크 서비스 및 내부 앱과 같이 공개적으로 라우팅할 수 없는 도메인에 전달합니다. (기본적으로 DNS 요청에는 Cloudflare의 자체 퍼블릭 DNS 확인자이자 세계에서 가장 빠르고 신뢰할 수 있는 1.1.1.1이 사용됩니다.)
분할 터널링	IP 주소 또는 도메인을 제외/포함하여 사설 네트워킹 또는 VPN과 함께 실행합니다.
가시성 및 확장성	
로깅	포괄적으로 로깅: 모든 포트에서 검사된한 모든 DNS 쿼리, L4 네트워크 패킷, HTTP 요청을 로그로 기록합니다. Logpush 또는 API를 사용하여 기존 SIEM, 오케스트레이션, 분석 도구와 통합합니다. 관리자는 수집된 개인 식별 정보(PII)를 사용자 전체적으로 제외하거나 삭제할 수 있습니다.
섀도우 IT 발견	추적, 검토, 승인: 고객의 최종 사용자가 인라인 CASB를 통해 방문하는 SaaS 및 사설 네트워크 원본을 추적, 검토, 승인합니다.
페이지 사용자 지정	브랜드에 맞게 사용자 지정 HTTP 차단 페이지를 업로드 하거나 사용자 경험을 개선할 지침을 전달할 수 있습니다.
자동화	직관적인 API와 Terraform 공급자가 제공되어 모든 SSE / Zero Trust 구현 측면을 프로그래밍 방식으로 관리할 수 있습니다. 자동화된 서비스에 유저리스 서비스 토큰 지원도 제공합니다.

고객이 SWG를 사용하는 방법

미국 사이버보안 및 인프라 보안국(CISA)을 위한 Cloudflare 및 Accenture 보안 인터넷 액세스

100+ **미국 민간 기관**
Cloudflare의 DNS 필터링으로 사무실 보안을 구축

자세한 정보

스칸디나비아의 IT 및 디지털 커뮤니케이션 컨설팅 회사

"우리는 Cloudflare를 통해 포트를 보호하고, 위협을 필터링하며, 트래픽을 검사해 공격면을 줄입니다."

— Victor Persson, 보안 운영 책임자
사례 연구 읽어보기

일본의 클라우드 통합업체 및 컨설팅 회사

4,000건의 **요청을 주마다 차단**
직원 수백 명에게서 유해하고 원치 않는 인터넷 콘텐츠를 차단합니다

사례 연구 읽어보기

Zscaler와의 비교 샘플

기준	Cloudflare Gateway	Zscaler Internet Access
아키텍처	✓ 하나의 클라우드 플랫폼, 하나의 제어판	✗ 다수로 분편화된 클라우드, 제어판 다수
관리 인터페이스	✓ 모든 SSE에 하나의 인터페이스	✗ SWG 및 ZTNA용으로 분리되어 있음
단일 경로 검사	✓ 모든 SSE 서비스에 가능함	✗ 아니요
IPv6 전용 지원	✓ 예	✗ 아니요
가동 시간 SLA	✓ 모든 서비스에 100%	✗ 대부분의 서비스에 99.999% DNS 확인자에 99.9%

계속 비교: Cloudflare 대 Zscaler

더 빠른 보호

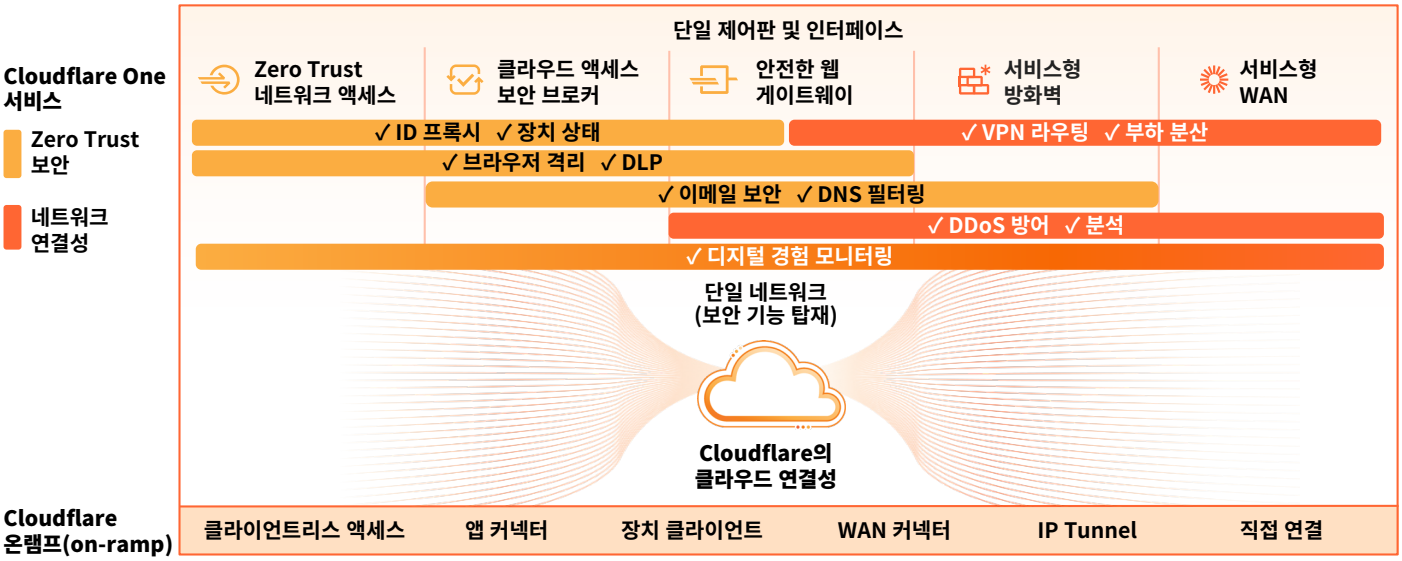
13~58%
더욱 빠른 보안 웹 게이트웨이(SWG)

45~64%
더욱 빠른 원격 브라우저 격리(RBI)

근거: 자사 테스트 및 타사 테스트

Cloudflare의 SSE 플랫폼으로 보안을 최신화하세요

Cloudflare Gateway는 Cloudflare의 SSE 플랫폼인 Cloudflare One 내에서 구성 가능한 서비스입니다. SWG를 기반으로 구축하고 Cloudflare One의 상호 운용 가능한 보안 기능을 사용하여 웹, SaaS, 비공개 앱 환경 전체에서 가시성과 제어를 확장하세요.



단일 통합 플랫폼

- **보안 액세스** 모든 사용자를 검증하고 모든 리소스로 세분화
- **위협 방어** 네트워크 기반 AI/ML 및 위협 인텔리전스로 모든 채널을 커버
- **데이터 보호**(전송 중, 저장 중, 사용 중인 데이터의 가시성과 제어 능력 강화)

프로그래밍 가능한 단일 네트워크

- **연결 및 정책 관리 간소화로** 더 효과적임
- **더 생산적**(모든 장소에서 빠르고, 안정적이며, 일관된 사용자 경험 보장)
- 변화하는 보안 요구 사항을 충족하기 위해 빠르게 혁신하므로 **더 민첩함**

아직 실시간 대화를 할 준비가 되지 않으셨나요?

SASE 참조 아키텍처에서 자세히 알아보거나 Cloudflare Zero Trust 플랫폼의 상호 작용형 투어에서 작동 방식을 살펴보세요.