하이브리드 근무 보호

온네트워크와 오프네트워크 환경 모두에서 모든 사용자의 위험을 줄이고 가시성을 높입니다

모든 사용자, 모든 장치, 모든 위치의 연결을 보호합니다

장소와 관계없이 일하는 미래: 글로벌 팬데믹이 시작된 지 몇 년이 흐른 지금, 다가올 경기 침체로 인해 하이브리드 근무는 계속될 것으로 보입니다. IT 팀과 보안 팀은 원격 근무든 사무실 근무든, 모든 사용자와 장치를 대상으로 일관된 보호와 경험을 제공해야 합니다. 그러나 기존의 위치 중심 도구(예: VPN 및 IP 기반 제어)로는 이러한 작업을 수행할 수 없습니다.

현대 인력을 위한 최신 보안: 따라서 많은 조직에서는 자체 IT 및 보안 아키텍처를 새롭게 구상하고, 분산된 인력의 필요 사항에 맞춰 규모를 조정하는 클라우드 제공 보안을 채택하며, Zero Trust의 모범 사례를 따릅니다.

Cloudflare에서는 모든 연결에 대한 보안을 간소화했습니다. 따라서 모든 장치나 위치에서 애플리케이션이나 인터넷에 액세스할 때 사용자는 보호를 받으며 생산성을 유지할 수 있습니다.

Gartner®의 견해:

> *2026년까지 직원의 75%가 계속해서 자택과 기존 사무실 위치에서 시간을 나눠 보낼 것입니다. 이 수치는 팬데믹이 절정이었던 2021년의 77%에서 약간 낮아졌습니다.[1]*

> *경계 보안 장비 모음을 기반으로 한 네트워크 보안 설계는 최신 디지털 비즈니스와 하이브리드 디지털 인력의 언제 어디서나 발생하는 가변적인 필요 사항을 처리하는 데는 적합하지 않습니다.[2]*

페이지별 목차

보안 최신화 기회

VPN 없이 애플리케이션 액세스를 보호

사용자가 널리 분산되어 있으므로 VPN과 같은 온프레미스 장비를 통한 트래픽 백홀은 성능이 저하되고 기업 네트워크 전반에 걸쳐 위협이 내부적으로 확산될 위험을 초래합니다.

대신 사용자에게 더 가까운 곳에서 ID 기반 제어를 시행하여 모든 요청에 대한 가시성을 다시 얻고 생산성을 유지하세요. 백홀이 필요하지 않습니다.

SaaS 보안 간소화

직원들은 그 어느 때보다 기존 기업 네트워크의 제어를 벗어난 장소에서 SaaS 애플리케이션에 더 많이 의존합니다.

따라서 조직은 더욱더 포괄적인 가시성과 SaaS 애플리케이션에 대한 제어가 필요합니다. 이를 통해 액세스 정책을 설정하고, 데이터 보호 제어를 적용하며, 섀도우 IT를 완화하고, 잘못된 구성이 있는지 앱을 스캔할 수 있습니다.

사용자와 데이터를 인터넷 위협으로부터 보호합니다

랜섬웨어, 피싱, 기타 인터넷 위협은 항상 존재하며 계속해서 정교해지고 있습니다.

아웃바운드 트래픽을 대상으로 클라우드 기반 검사 및 격리를 채택하면 사용자를 맬웨어로부터 안전하게 보호할 수 있습니다. 또한 관리자는 관리되지 않는 로컬 장치에 중요한 데이터가 도달하지 않도록 제어할 수 있습니다.

성숙한 기업의 하이브리드 근무

성숙한 기업을 위해 자신감 있게 하이브리드 근무의 보안을 최신화합니다

문제: 복잡한 레거시 환경

여러 조직에서는 사무실 내 근무 모델을 실험하고 있습니다. 그러나 보호 및 사용자 경험을 일관되게 유지하는 것은 이러한 하이브리드 시나리오 전반에 걸쳐 어려운 일입니다.

이러한 조직은 이미 존재하는(대체로 복잡한) 온프레미스 및 레거시에 더욱 큰 규모로 투자하여 변화를 추구하기가 더 어려운 경향이 있습니다. 경기 침체가 시작되는 상황에서 새로운 보안 프로젝트를 시작하는 것은 너무 위험하고 어렵게 느껴질 수 있습니다.

기회: 최신화를 지향하는 더 간편한 길

조직에서는 무한한 예산, 값비싼 '개념 증명', 복잡한 구현 단계, 데이지 체인 서비스 없이도 나름의 진행 속도로 디지털 변환을 추진할 수 있어야 합니다.

이러한 성숙한 기업에서 하이브리드 근무의 필요를 충족하는 데 도움을 주기 위해, Cloudflare는 Zscaler와 같은 다른 Zero Trust 서비스 공급자보다 더 쉽고 빠르게 배포할 수 있도록 설계되었습니다.

사용 사례 예시

통신

상황: 매년 200억 달러 이상의 수익을 올리며 100년 이상의 전통을 가진 유럽 통신 회사에서 인터넷 필터링을 배포하고 최근에 여러 클라우드 환경으로 마이그레이션한 레거시 앱에 대한 액세스를 인증해줄 벤더를 원했습니다.

솔루션: 이 회사에서는 서비스를 통합하고 10만여 명의 직원을 대상으로 애플리케이션과 인터넷 액세스를 모두 보호하기 위해 통합 플랫폼을 사용하려고 Cloudflare를 선택했습니다.

연방 정부

상황: 미국 국토안보부(DHS)에서는 연방 사무실, 위치, 인프라에 걸쳐 인터넷 위협 보호에 투자를 많이 합니다.

솔루션: DHS는 악의적이고 위험한 대상에 대하여 DNS 쿼리를 필터링할 공동 솔루션 개발을 위해 Cloudflare 및 Accenture Federal Services를 선정했습니다. 이 솔루션은 연방 기관 전반에 걸쳐 사용될 예정입니다.

미디어 및 광고

상황: 미디어 대기업(100억 달러 이상의 수익 및 십만 명 이상의 전 세계 직원)에서 랜섬 메모를 포함하여 내부 인프라에 대한 사이버 공격에 직면했습니다.

솔루션: Cloudflare에서 수백 개의 웹 및 비웹 앱을 ID 기반 Zero Trust 규칙으로 보호했습니다.
이 회사는 3개월 이내에 5만 명의 직원을 대상으로 보호 수단을 도입하며 9개월 이내에 전체 인력에 걸쳐 이를 확장할 계획입니다.

에너지

상황: Fortune 500 천연가스 공급자 하나가 해당 부문을 겨냥하여 커져가는 사이버 위협으로부터 자체의 분산된 데이터 센터 및 1,500여 명의 인력에 대한 보호를 강화하기를 원했습니다.

솔루션: 이 회사는 Zscaler를 대체하도록 Cloudflare를 선택했습니다. 그 이유로는 애플리케이션 및 인터넷 액세스를 보호하는 데 신뢰성과 일관성이 더 뛰어나다는 점을 꼽았습니다. 장기적으로도 원격 브라우저 격리를 통해 고급 제어를 채택하기가 더 쉽기 때문입니다.

고객의 의견

> *"Cloudflare는 우리의 Zero Trust 여정에서 천군만마와도 같습니다."*
>
> **John McLeod**
> **CISO, National Oilwell Varco**

> *"Cloudflare는 우리 Ziff Media Group의 내부 도구를 전 세계에 근무하는 직원들의 장치에 원활하고 안전하게 제공할 수 있도록 해주었습니다. 복잡하게 네트워크를 구성할 필요가 없었죠."*
>
> **Josh Butts**
> **SVP 제품 및 기술,**
> **Ziff Media Group**

> *"Cloudflare 덕분에 우리는 개발 환경을 위한 VPN 및 IP 허용 목록에 대한 의존을 줄일 수 있었습니다."*
>
> **Alexandre Papadopoulos,**
> **사이버 보안 담당 이사,**
> **INSEAD**

디지털 네이티브를 위한 원격 우선 인력

디지털 네이티브를 대상으로 신속한 보안을 우선시하여 원격 근무 유연성을 지원합니다

문제: 클라우드 보안 규모 조정 및 자동화

많은 조직에서는 원격 우선 채용을 채택하고 있습니다. 이러한 조직은 신생 기업이고, 초기에 클라우드를 채택했으며, 제한된 온프레미스 인프라 및 안전하고 빠르며 신뢰할 수 있는 디지털 서비스를 기반으로 한 비즈니스 모델을 갖추었습니다.

장소와 관계없이 일할 수 있도록 유연성을 제공하는 것은 차별화 요소가 될 수 있습니다. 그러나 사용자가 개인 장치로 이동하고 개인 장치에 의존함에 따라 똑같이 유연한 보안 도구가 필요합니다.

기회: 규모에 맞추어 구성 가능한 보안

사용을 중단할 레거시 IT의 수가 줄어들면서, 이러한 디지털 네이티브는 자체적인 보안 최신화 측면에서 민첩성을 유지하기 위해 Cloudflare의 인터넷 네이티브 아키텍처 및 배포 유연성을 활용할 수 있습니다.

Cloudflare의 구성 가능한 서비스, API 우선 설계, 단일 제어판 관리를 이용하면 쉽게 보안을 시작하고 조정할 수 있습니다. Cloudflare 전역 네트워크의 속도, 규모, 신뢰성은 원격 근무만 하는 인력의 필요 사항을 충족합니다.

사용 사례 예시

B2B SaaS

상황: 호주 그래픽 디자인 플랫폼인 Canva(2021년 기업 가치, 400억 달러)는 팬데믹 이전에 Cloudflare를 배포하여 타사 사용자의 액세스를 간소화하고 VPN 구현의 번거로움을 없앴습니다.

솔루션: 시간이 지남에 따라 Canva는 늘어나는 전체 인력을 대상으로 Zero Trust 애플리케이션 액세스 정책을 도입하였고, 인터넷 필터링 및 검사를 확대했습니다.

핀테크 및 블록체인

상황: BlockFi는 시리즈 D 자산 관리 플랫폼으로, 블록체인 기술로 구동됩니다. 이 플랫폼에서는 늘어나는 관리 자산과 원격 근무 우선 직원을 대상으로 발생하는 사이버 위협에 직면하여 보안을 업그레이드해야 했습니다.

솔루션: Cloudflare에서는 BlockFi가 시간이 많이 소요되는 IP 기반 제어에서 애플리케이션 액세스를 위한 ID 기반 인증으로 전환할 수 있도록 했습니다.

소셜 미디어

상황: 글로벌 소셜 미디어 플랫폼에서 내부 애플리케이션 액세스 및 VPN 구성을 악용하여 세간의 이목을 끌었던 유출을 경험했습니다.

솔루션: 이에 대응하여 이 회사에서는 13,000명의 직원 및 계약자를 대상으로 Cloudflare의 Zero Trust Network Access(ZTNA) 솔루션을 채택하고 자체 VPN 배포를 퇴출시켜 원격 액세스 접근 방식을 개편하기로 결정했습니다.

전자 상거래

상황: 글로벌 전자 상거래 플랫폼(40억 달러 이상의 수익 및 15,000명 이상의 직원)에서 오프네트워크 상태에서 인터넷을 이용하면서 중요한 SaaS 앱에 액세스하는 원격 사용자를 더 강력하게 보호할 수 있기를 원했습니다.

솔루션: 이 회사에서는 DNS 필터링과 같은 계층 위협 보호 기능에 Cloudflare를 배포합니다. 동시에 SaaS 애플리케이션 사용량에 대한 향상된 가시성을 제공합니다.

고객의 의견

"Delivery Hero에서는 언제나 고객에게 멋진 경험을 제공하려고 노력합니다. Cloudflare 덕분에 우리 내부 직원도 역시 멋진 경험을 하고 있어요. 세계 모든 곳에서 안전한 작업 환경과 빠르고 신뢰할 수 있으며 개인정보를 중요하게 여기는 애플리케이션을 쉽게 구축할 수 있거든요."

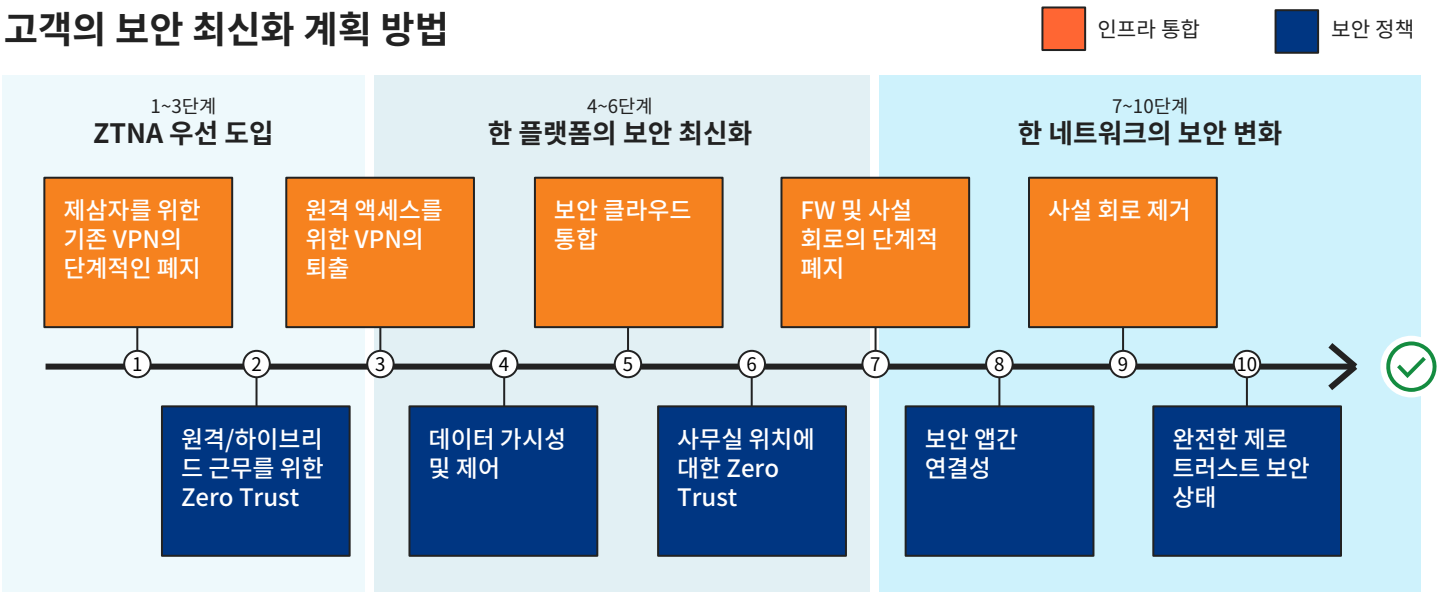
Christina von Hardenberg
CTO, Delivery Hero

"Cloudflare는 우리가 늘어나는 원격 근무 인력을 보호하는 데 중요한 역할을 합니다. 애플리케이션 액세스에 Zero Trust를 채택하면서 관리자의 가시성이 향상되었고 세부 제어가 가능해졌습니다. 이전 레거시 도구로는 절대 가능하지 않았던 일입니다."

Marccio Alcaide
IT 보안 책임자, Facily

하이브리드 근무를 설명하는 로드맵

고객의 보안 최신화 계획 방법



보안 최신화 로드맵

위 로드맵에서는 조직에서 하이브리드 근무에 적응하기 위해 자체 보안을 최신화할 때 사용하는 접근 방식을 설명합니다. 이 로드맵에는 2개의 핵심 목표가 있습니다.

1) **상단 행(오렌지색):** 연결성과 보안 인프라를 통합하여 포인트 제품과 하드웨어를 하나의 클라우드 네이티브 플랫폼으로 만듭니다.
2) **하단 행(파란색):** 가시성과 제어를 확보하여 모든 장치와 위치에서 사용자와 리소스 간에 Zero Trust 보안을 채택합니다.

1~5단계: 앱 및 인터넷 액세스 보호

많은 경우 하이브리드 근무로 변경하는 것은 우선 인력이 기업 리소스에 도달하는 방법을 최신화하는 것을 의미합니다.

1단계: 보통 첫 단계는 선택된 사용자(예: 계약자, 개발자, 파트너, 새로 인수한 팀)를 대상으로 VPN 트래픽 오프로드를 시작하고 인터넷 네이티브 제어로 전환하는 것입니다. Cloudflare는 특히 엔드포인트에서 어떠한 소프트웨어를 배포할 필요 없이 브라우저를 통해 액세스할 수 있는 자체 호스팅 앱을 보호하는 것을 간소화합니다.

2단계: 이 최신 도구로는 역할, MFA 및 하드 키 요구 사항, ID, 장치 상태를 기반으로 앱별 정책을 구축하는 데 필요한 가시성을 얻을 수 있습니다.

3단계: 팀은 이러한 접근 방식으로 자신감을 얻으며 자체 VPN을 모두 퇴출시키고 비웹 및 레거시 사설 네트워크를 Zero Trust로 보호합니다.

4단계: 그런 다음 초점이 SaaS 앱에 대한 가시성 및 제어를 개선하는 것으로 이동합니다. 여기에는 섀도우 IT 완화, 테넌트 관리, 데이터 유출 방지가 포함됩니다.

5단계: 내부 및 SaaS 앱을 이제 단일 플랫폼에서 관리할 수 있으므로 조직에서는 아웃바운드 인터넷 액세스를 대상으로 제어를 확대하고 DNS 필터 및 안전한 웹 게이트웨이와 같은 위협 방어 도구를 통합하려고 합니다.

6~10단계: 연결성을 클라우드로 전환

로드맵의 나머지 단계는 대부분의 조직에서 계획하고 있습니다. 그러나 이들 조직에서는 모든 네트워크 연결성 및 보안을 하나의 통합 클라우드 네트워크로 전환하려는 포부를 갖습니다.

6단계: 이 단계에서 조직에서는 일관된 Zero Trust를 모든 네트워크 위치로 확장하려고 합니다. 여기에는 하이브리드 근무를 지원하기 위한 본사, 지점, 데이터 센터, 지사가 포함됩니다.

7단계: 사무실 트래픽이 보안을 위해 점점 더 많이 Cloudflare로 전송됨에 따라 조직에서는 기존 온프레미스 방화벽 및 기타 사설 네트워크 장비를 단계적으로 퇴출시킬 수 있습니다.

8단계: 이러한 첨단 사용 사례에서는 앱 연결성을 하이브리드 다중 클라우드 환경 전반에 걸쳐 보호하는 데 초점을 맞춥니다. 이는 따라 네트워크 인프라 팀은 **9단계**에서 통신회사 MPLS 계약을 종료하도록 준비할 수 있습니다.

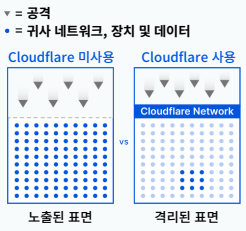
10단계: 최신화는 절대 영원히 끝날 수 없지만 포부는 Zero Trust를 이제 모든 사용자, 장치, 데이터, 애플리케이션, 환경으로 확대 적용하는 것입니다.

비즈니스 및 보안 결과

Zero Trust를 통해 비즈니스의 시간과 돈을 절약하는 5가지 방법

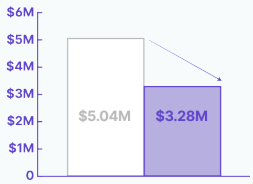
공격 표면 감소

91%↓



침해 비용 감소

35%↓



직원 온보딩 가속화

60%↑

IT 티켓 부담 감소

80%↓

사용자 대기 시간 감소

39%↓

기타 사업 동력

인력 생산성 활용

관리자의 경우

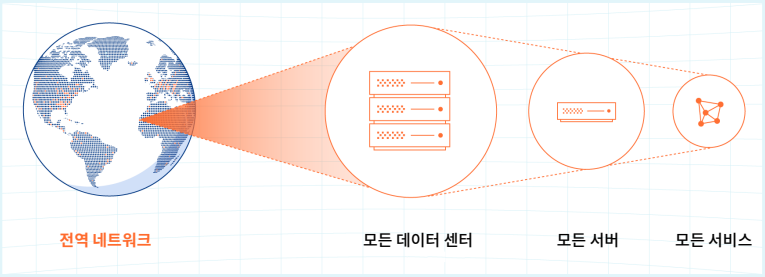
- ■정책을 애플리케이션 및 인터넷 액세스 전반에 걸쳐 설정하기 위해 단일 관리 인터페이스로 구성 간소화
- ■동일한 관리 인터페이스에서 ID 공급자, 엔드포인트 보호, 클라우드 공급자, 네트워크 온램프로 모든 통합 구성

최종 사용자의 경우

- ■방해가 되지 않는 보안으로 원활한 인증 및 기본 브라우징 경험

레거시 서비스 비용 절감

- ■가상 사설 네트워크(VPN) 장비를 대체하거나 보강하고 대신 다음을 채택: Zero Trust Network Access(ZTNA)
- ■온프레미스 웹 프록시 또는 방화벽에서 다음으로 전환: 클라우드 네이티브 L3-L7 보안 서비스
- ■다음을 사용하여 가상 데스크톱 인프라에서 사용 사례를 오프로드: Remote Browser Isolation (RBI)
- ■기존 보안 이메일 게이트웨이를 다음으로 교체: 최신 클라우드 이메일 보안



모든 원격 및 사무실 사용자를 보호하기 위한 일관된 속도 및 규모

모든 보안, 성능, 안정성 기능이 현재 275개 이상의 도시에 걸쳐 있는 당사 네트워크의 모든 Cloudflare 데이터 센터 내 모든 서버에서 실행되도록 설계되었습니다.

Zero Trust 로드맵을 가속화하세요

지금 사용해 보세요 | 문의

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

REV: PMM-2022JUL

[1] *하이브리드 작업을 지원하기 위한 최고의 네트워크 사례,* Gartner, Karen Brown, Andrew Lerner, Mike Toussaint, 04/08/2022
[2] *2022년 SASE 컨버전스를 위한 전략적 로드맵,* Gartner, Neil MacDonald, Andrew Lerner, John Watts 06/24/2022