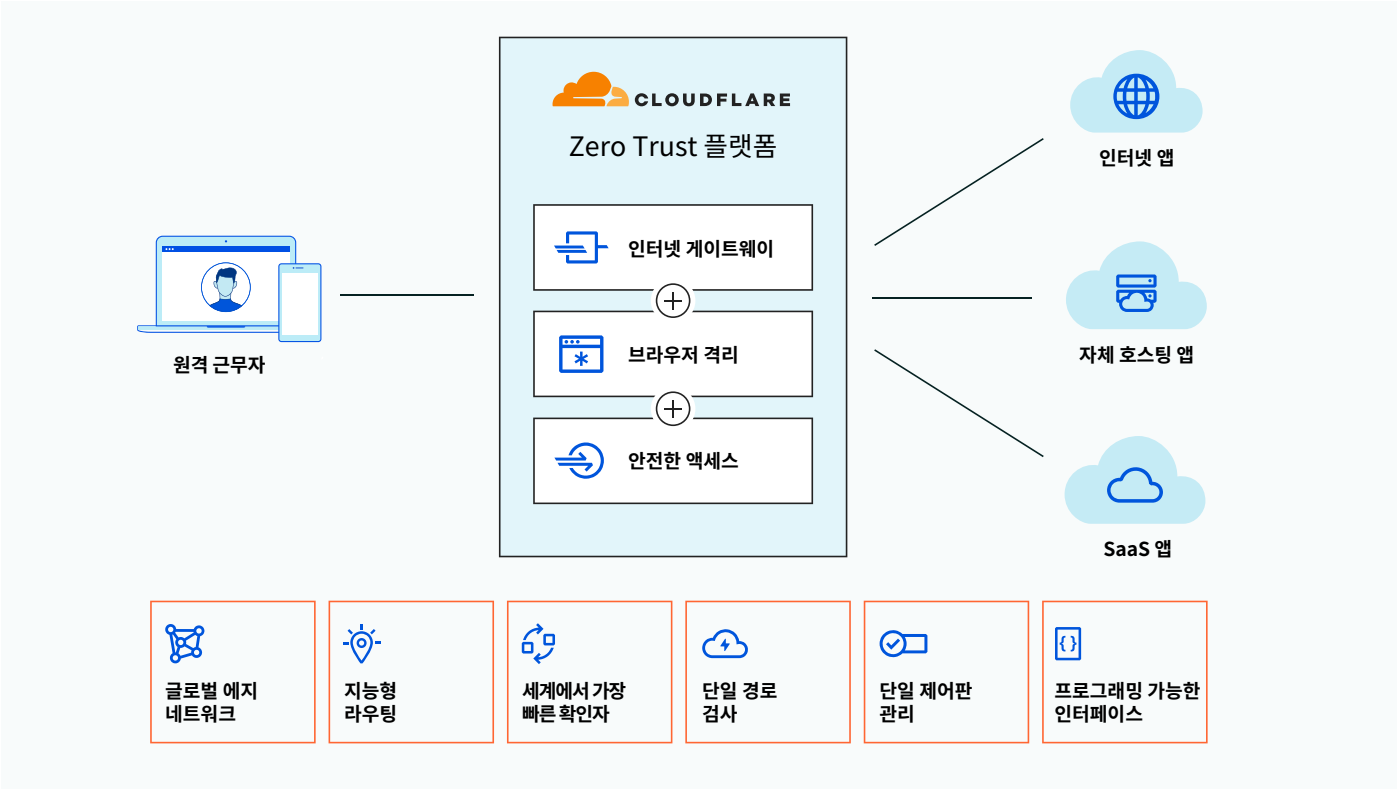
Cloudflare로 장시간에 걸친 원격 근무자 연결성 확보

코로나19로 하루아침에 원격 근무로 전환하게 되자, 기업들은 직원들의 계속적 연결을 위해 발빠르게 움직였습니다. 전략적인 솔루션도 있었지만, 그밖에 느리고 불안정한 VPN 사용을 늘리는 것, 인터넷 트래픽을 분할 터널링하는 것, 성급하게 원격 액세스 해킹을 적용하는 것 등 전술적 응급처치에 불과한 것도 있었습니다. 그런데 가시성, 보안, 복잡성 등의 익숙한 문제들이 지속됨에 따라, 이러한 접근 방식의 결함이 나타나고 있습니다.

원격 근무 보안 결함을 고치는 것은 수개월이나 수주가 걸리는 일이 아닙니다. Cloudflare Zero Trust를 사용하는 관리자는 30분 만에 20건 이상의 시급한 직원 보안 및 연결 사용 사례를 처리할 수 있습니다.

솔루션: Cloudflare Zero Trust



Cloudflare의 Zero Trust 보안 플랫폼으로 원격 근무자들의 응용 프로그램 및 인터넷 연결에 대한 가시성을 높이고 복잡성을 제거하며 위험을 줄일 수 있습니다. 세계에서 가장 빠른 에지 네트워크에서 실행되므로 다른 공급자에 비해 배포가 신속하고 성능이 우수합니다.

Zero Trust 플랫폼이 원격 근무자 보안을 강화하는 세 가지 방식

위험 감소

VPN 의존도는 장애 조치 위험을 만들고 기업 인프라에 공격자가 악용할 수 있는 구멍을 남겼습니다. 공격자가 일단 액세스 권한을 얻으면, 여러 리소스로 수평 이동하면서 데이터를 탈취할 수 있습니다. 위협에 맞서고 그것을 차단하려는 최선에 노력에도 불구하고, 엔드포인트는 여전히 미발견 맬웨어에 의해 손상됩니다.

Zero Trust 보안 플랫폼은 기업 앱에 대한 모든 요청에 대해 ID 및 컨텍스트 기반 인증을 시행함으로써 수평 이동의 여지를 최소화하고 원격 근무의 위험을 경감합니다. 브라우저 격리는 브라우징 활동으로부터 엔드포인트를 격리시켜, 알려지거나 알려지지 않은 위협을 완화합니다.

가시성 향상

이전에 사용자들이 사무실에 있을 때는 활동 로그를 유지하는 것이 간단했지만, 직원들이 지리적으로 흩어져 있고 새로운 장치로 근무하는 상황에서는 감사 추적을 유지하는 것이 훨씬 어렵습니다. SaaS 응용 프로그램에서의 로깅 기능은 일관성이 없고 VPN 로그는 분석하기 어려울 수 있습니다.

Zero Trust 플랫폼은 손상되지 않은 장치 포함, 모든 원격 장치의 요청에 대한 인터셉션 및 로깅을 통해 가시성을 복원합니다. 관리자는 내부 호스팅 및 SaaS 앱에서 감사 추적을 통해 사안을 조사하면서 원격 근무자의 활동을 모니터링할 수 있습니다. 로그는 하나의 대시보드에 중앙 집중되어 있으며, 선택한 SIEM에 자동으로 보내집니다.

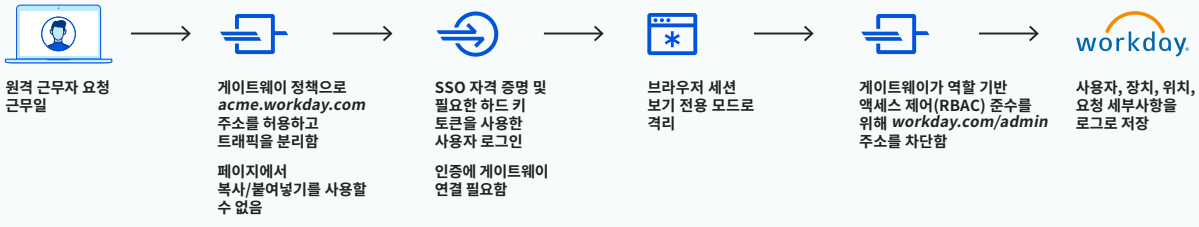
복잡성 제거

응급처치 솔루션이 원격 근무자 연결을 위해 실행되었지만 이는 장기적으로 매우 취약한 것으로 나타나고 있습니다. 호환되지 않는 여러 툴을 가지고 트래픽 필터링 정책을 관리해야 하는 것은 오롯이 관리자의 몫이며, 사용자들은 느린 속도에 좌절하게 됩니다.

Zero Trust 플랫폼은 사용자 연결 방식과 관리자의 업무 방식을 간소화합니다. 레거시 VPN에 대한 의존도를 줄임으로써 관리자는 그 연결이 어떻게 시작되는지 또는 트래픽이 네트워크 스택 어디에 존재하는지에 상관없이 모든 트래픽에 표준 보안 컨트롤을 적용할 수 있습니다. 모든 정책은 하나의 대시보드에서 관리될 수 있습니다.

Zero Trust 보안의 실제

사용 사례: SaaS 응용 프로그램에서 데이터 손실 방지하기



단일 경로 아키텍처 내에서, 원격 근무자 트래픽은 검사되고 격리되고 로깅되고 인터넷 위협으로부터 보호됩니다. 이때 사용자는 가까운 데이터 센터에 짧은 홉만으로 연결되기 때문에 성능이 전혀 저하되지 않습니다.