Cloudflare Area 1 이메일 보안

피싱, 비즈니스 이메일 손상 (BEC), 이메일 공급망 공격으로부터 사용자를 선제적으로 보호하세요.

피싱은 여러 조직에서 가장 자주 겪고 비용이 많이 드는 사이버 위협 중 하나입니다.

Cloudflare Area 1은 공격이 사용자의 받은메일함에 도달하기도 전에 공격을 식별하고 차단하는 클라우드 네이티브 이메일 보안 플랫폼이며, 스피어 피싱, BEC, 기타 기존 방어 방법을 회피하도록 진화된 위협에 대응하여 효과적으로 보호해줍니다.

Area 1을 이용하여 Microsoft와 Google의 환경 및 워크플로와 심층적으로 통합해서 클라우드 이메일 공급자가 기본으로 제공하는 보안을 강화할 수 있습니다.

Area 1은 Cloudflare Zero Trust 서비스의 일부입니다.

대상을 겨냥하는 피싱 위협을 차단하세요

Area 1은 대규모 캠페인부터 몇 달에 걸쳐 수행되며 흔하게 대상이 되는 이메일 공급망 손상 시도에 이르기까지, 광범위한 피싱 공격에 대한 보호를 제공합니다.

피싱

Verizon 2021 DBIR에서는 가장 흔한 침해 전술로 피싱이 언급됩니다. 대규모 웹 크롤링, 소규모 패턴 분석, 개선된 감지 기능을 조합하여 Area 1은 피싱 공격이 사용자의 받은메일함에 도달하기 며칠 전에 차단할 수 있습니다.

BEC 및 소셜 엔지니어링 위협

공격자는 BEC 수행 시 돈과 데이터를 훔치기 위해 신뢰할 수 있는 엔터티를 가장하거나 손상시킵니다. Area 1은 이메일 커뮤니케이션의 내용과 컨텍스트를 분석하여 "건초더미 속에 있는 바늘"과 같은 위협을 차단합니다

이메일 공급망 공격

공격자는 벤더의 이메일을 손상시키고 메일 패턴을 관찰하며 기존 스레드를 가로채 청구서 사기를 벌입니다. Area 1은 메일 스레드, 메시지의 기조, 소셜 그래프를 분석하여 이와 같은 정교한 공격을 차단합니다.

갈취 및 랜섬웨어 이메일

Gartner는 랜섬웨어 공격의 40%가 이메일을 통하여 시작된다고 추정합니다. Area 1은 랜섬웨어 이메일이 최종 사용자에게 전달되기 전에 사전 예방적으로 방어하고 악의적 메시지 역시 퍼지기 전에 제거하도록 도와줍니다.

기존 이메일 게이트웨이를 뛰어넘음

선제적

공격 초기 단계에 피싱을 차단할 수 있도록 미리 공격자의 인프라와 전달 메커니즘을 파악합니다.

컨텍스트 파악

고급 감지 기술(언어 분석, 컴퓨터 비전, 소셜 그래프 작성 등)을 활용해 BEC, 벤더 이메일 사기, 기타 무페이로드 위협을 잡아냅니다.

포괄적

이메일 공격 유형(URL, 페이로드, BEC), 벡터(이메일, 웹, 네트워크), 공격 채널(외부, 내부, 신뢰하는 파트너)의 전체 범위를 다룹니다.

연속적

받은메일함에 이메일이 전달되기 전, 전달되는 도중, 전달된 후에 위협 보호 계층을 이용해 심층 방어를 실행합니다.

이점

네이티브 이메일 보안 강화

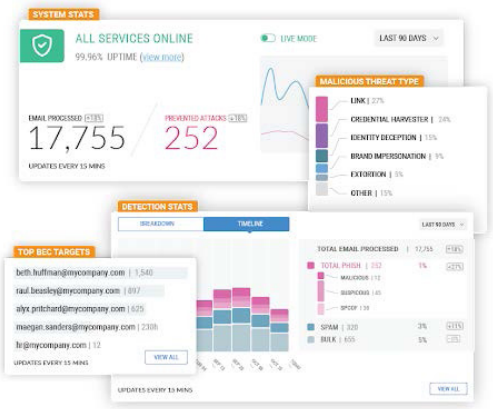
기본으로 제공된 보안 계층을 회피하도록 진화한 피싱 및 BEC 공격을 차단합니다. 이메일 생산성에는 거의 영향을 미치지 않으면서 클라우드 이메일 환경으로 심층 통합하는 방식을 활용합니다.

클라우드 우선적 아키텍처 채택

확장 가능한 최신 아키텍처를 위해 기존 이메일 게이트웨이의 과도한 작업이나 경직성을 방지합니다. 네이티브 이메일 보안 기능을 복제하는 보안 계층으로 인한 지출을 줄입니다.

SOC 팀의 시간 절약

하드웨어, 에이전트, 장비 없이 몇 분이면 배포됩니다. 정책을 작성하고 조정하는 데 들여야 할 시간이 절약됩니다. SIEM과 SOAR의 통합으로 SOC 조사 속도가 빨라집니다.



피싱 위험 평가 요청

라이브 이메일 프로덕션 트래픽에서 Area 1을 실행하도록 요청하고 기존 보안 제어를 통해서는 어떤 이메일 공격이 침투하는지 실시간으로 확인해보세요.

평가를 위하여 하드웨어나 소프트웨어를 설치할 필요가 없으며, 메일 흐름에는 영향이 미치지 않습니다.

평가를 이곳에서 요청하세요.

+82 70 4515 6893 | enterprise@cloudflare.com | www.cloudflare.com/ko-kr/