Menlo Security Email Isolation으로 이메일 기반 사이버 공격을 차단합니다.

이메일은 가장 일반적인 공격 벡터이지만 기업 입장에서는 가장 방어하기 어려운 자산이기도 합니다.

이점:

- 사용자가 중요한 사용자 자격 증명을 웹 양식에 입력하지 못하도록 보호합니다.
- 잠재적으로 위험한 링크를 클릭하여 조직에 가장 큰 위험을 초래하는 사용자를 식별합니다.
- 추가적인 기업 피싱 인식 교육을 제공하는 구성 가능한 실시간 경고 메시지를 전달합니다.
- 사용자가 안전한 문서 또는 원본 문서 첨부 파일을 다운로드할 수 있는 정책을 수립합니다.
- 클라우드 기반의 바이러스 방지 샌드박스 환경에서 허용되는 원본 문서(암호로 보호되는 ZIP 파일 포함)를 자동으로 검사합니다.
- 사용자 환경 또는 기존 워크플로에 영향을 주지 않고 기존 메일 서버 인프라와 통합됩니다.

전통적인 보안 솔루션의 한계

이메일은 현재까지 사이버 범죄자들이 멀웨어를 배포하는 가장 일반적이고 성공적인 공격 벡터입니다. 전통적인 이메일 보안 솔루션은 샌드박스만 활용하여 내부 및 제3자 위협 인텔리전스 피드를 기반으로 "안전한" 콘텐츠와 "안전하지 않은" 콘텐츠를 판별합니다. 그러나 오늘날 대부분의 이메일 공격은 소규모 그룹 또는 개인 한 명을 표적으로 삼는 만큼 나중에 탐지할 수 있는 눈에 띄는 흔적을 남기지 않습니다.

결과적으로 탐지 중심 접근 방식은 사용자와 조직을 이러한 유형의 공격으로부터 보호하지 못합니다.

Menlo Security Email Isolation

Menlo Security는 격리 방식을 사용하여 위협 행위자들이 악의적인 링크나 이메일 첨부 파일을 통해 사용자의 호스트에 멀웨어를 전달하지 못하도록 차단합니다. Menlo Security Email Isolation은 Menlo Cloud Isolation Gateway에 직접 통합되며, 알려진 악의적인 링크와 첨부 파일을 자동으로 차단하고, 안전하다고 간주되는 링크와 첨부 파일을 격리시키는 차단 또는 격리 접근 방식을 활용합니다. 이러한 제로 트러스트 전략은 이메일을 통해 전달되는 악의적인 콘텐츠가 사용자의 호스트에 액세스하는 것을 완벽하게 차단합니다.

이 솔루션은 기존 이메일 서버 인프라에 완벽하게 통합되므로 사용자에게 일관적이고 기존에 사용하던 이메일 경험을 그대로 제공할 수 있습니다. 새로운 이메일 시스템을 배우거나 소프트웨어를 설치할 필요가 없습니다. 모든 웹 콘텐츠와 이메일 첨부 파일은 Menlo Cloud Isolation Gateway(MCIG)를 라우팅하므로 멀웨어가 사용자 장치에 도달할 수 없습니다. 이러한 방식은 어떠한 이메일 보호 서비스에서도 제공한 적이 없는 업계 최초의 방식입니다.

이메일 링크

Menlo는 합법적인 이메일 링크와 그렇지 않은 이메일 링크를 판별하지 않고 격리 게이트웨이를 통해 모든 웹 콘텐츠를 격리시키므로 정확하지 않은 범주화에 따른 허용 또는 차단 판별을 수행할 필요가 없습니다. 가져오기 및 실행 명령이 사용자 브라우저와 멀리 떨어져 있는 격리된 환경에서 수행됩니다.

관리자는 Menlo를 통해 웹 페이지와 양식을 읽기 전용으로 렌더링하는 사용자 지정 정책을 수립하여 사용자가 실수로 자신의 자격 증명을 노출시키는 사고를 방지할 수 있습니다. 또한, 분석을 통해 피싱공격에 가장 취약한 사용자를 식별할 수 있는 통찰력을 제공하며, 실시간 메시지 구성을 통해 사용자에게 능동적으로 피싱 방지 교육을 수행할 수 있습니다.

이메일 첨부 파일

사용자가 받은 이메일을 열고 첨부 파일을 클릭하면 100% 안전하게 격리된 상태에서 문서를 즉시 볼 수 있습니다. Menlo는 기존 워크플로를 방해하거나 사용자 환경에 부정적인 영향을 주지 않습니다. 또한 관리자는 사용자에게 첨부 문서를 안전하고 매크로가 없는 PDF 버전으로 다운로드할 수 있는 옵션을 제공할 수 있습니다. 드문 경우지만 첨부 파일이 암호로 보호되고 있더라도 특정 사용자가 사전 바이러스 방지 검사와 샌드박스 검사를 통한 확인 과정을 거쳐 저장된 원본 문서를 다운로드할 수도 있습니다.

96%

이메일을 통해 실행된 사회 공학적 공격 비율

—Verizon 2018 Data Breach Report

Menlo의 제로 트러스트 접근 방식

조직은 스팸 방지, 바이러스 방지, 데이터 보안 및 암호화를 포함한 종합적인 이메일 보안 솔루션을 운영함에도 불구하고 이메일 기반 사이버 공격에 계속 희생되고 있습니다. 조직은 탐지 중심 접근 방식에만 의존하지 말고 SWG 솔루션에 직접 이메일 격리를 통합해야 합니다. 이메일 격리는 위험성 여부에 관계없이 이메일에서 비롯되는 모든 웹 콘텐츠와 문서를 사용자의 단말 장치로부터 먼 격리된 공간에서 실행합니다. 이러한 제로 트러스트 전략은 탐색과 이메일 경험에 영향을 미치지 않고 사용자와 조직을 웹 기반 공격으로부터 보호할 수 있는 유일한 방법입니다.

Menlo Security 솔루션이 어떻게 조직을 보호하는지 알아보려면 Korea@menlosecurity.com으로 문의하십시오.

Menlo Security 회사 소개

Menlo Security는 웹, 문서 및 이메일에서 멀웨어 위협을 제거하여 사이버 공격으로부터 조직을 보호합니다. Menlo Security의 클라우드 기반 격리 플랫폼은 사용자 단말에 소프트웨어가 필요하지 않으며 최종 사용자 환경에 영향을 주지 않고 기업 규모에 관계없이 확장 가능한 포괄적인 보호 성능을 제공합니다. Menlo Security는 포춘지 선정 500대 기업과 금융 서비스 기관을 비롯한 세계 주요 기업을 지원하고 있습니다.

문의
menlosecurity.com
Korea@menlosecurity.com