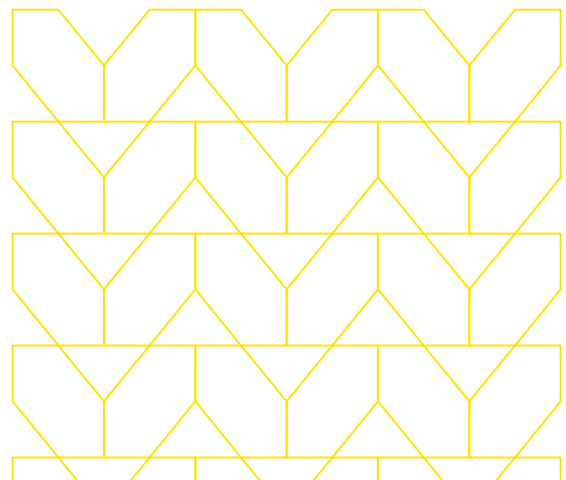




# Menlo Security 이메일 격리 솔루션과 피싱 공격에 대응하는 Fortune Magazine 50대 글로벌 투자 회사

이메일 보안 인프라의 격차를 해소하는

Menlo Security 이메일 격리



## 회사

전 세계 수백만 명 고객을 대상으로 연간 수백억 달러 규모의 거래를 하는 유명 투자 은행입니다.

---

## 과제

기존 이메일 보안 솔루션이 표적형 스피어 피싱 공격을 차단하지 못했습니다.

결과적으로 자격 증명 도용 및 멀웨어 익스플로잇이 발생했습니다.

사이버 범죄자들이 단말 액세스와 함께 정교한 네트워크 공격을 실행할 수 있습니다.

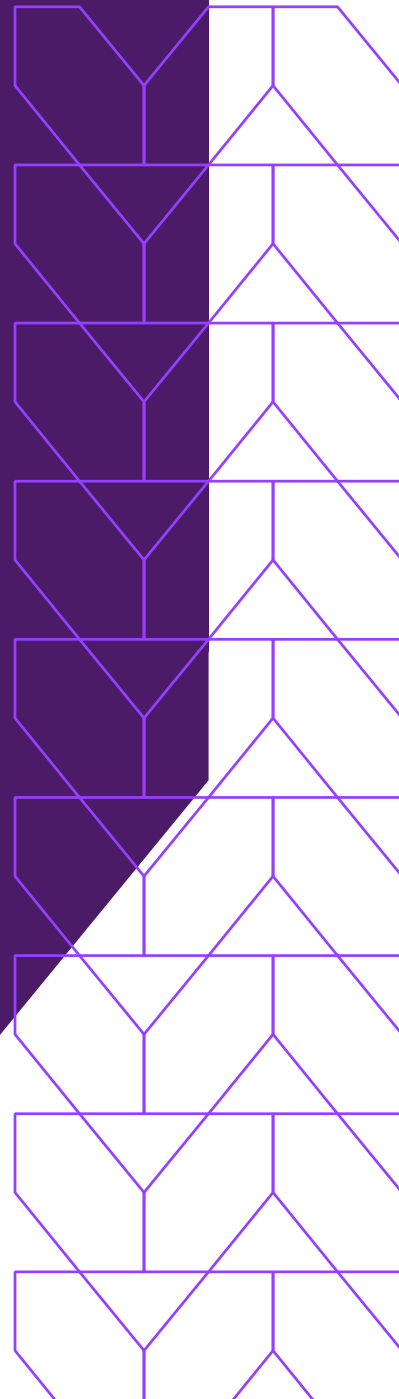
---

## 해결책

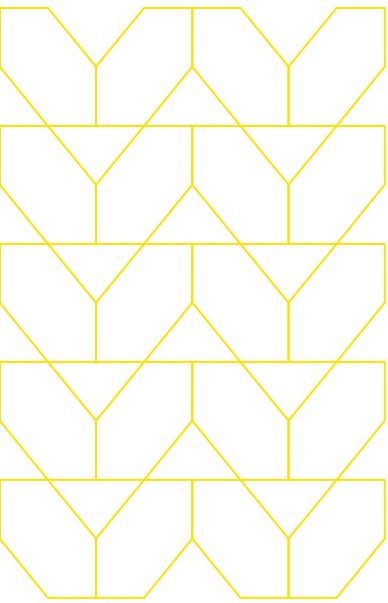
Menlo Security Internet Isolation Gateway를 구현했습니다.

기존 이메일 인프라에 통합했습니다.

모든 이메일 링크가 클라우드에서 격리되므로 피싱 공격이 감소합니다.

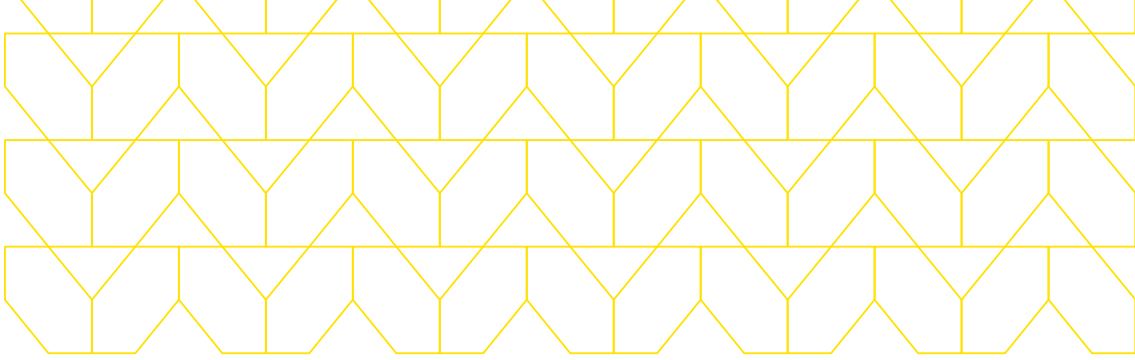


# 다수의 보안 방어 계층과 엔드 유저 교육에 많은 시간과 비용을 지출함에도 불구하고 피싱은 사이버 범죄 중 가장 위협적인 공격 벡터 중 하나로 자리 잡았습니다.



한 포춘지(Fortune) 50대 글로벌 투자 회사는 이메일 위협에 맞서기 위해 각각 이메일 보안 문제의 특정 부분을 처리하는 여러 보안 계층을 배포했습니다. 아키텍처는 다른 많은 대기업에서 사용하는 아키텍처와 유사했습니다. 즉 스팸 방지, 바이러스 백신, 데이터 보안, 암호화 및 샌드박스 솔루션의 클라우드 버전과 온프레미스 버전이 결합된 아키텍처였습니다. 이러한 솔루션은 다양한 위협을 방어할 수 있지만 가장 은밀한 공격을 대표하는 스피어 피싱과 드라이브 바이 멀웨어(drive-by malware) 익스플로잇에 매우 취약하다는 약점은 전혀 변하지 않았습니다.

이 대형 투자 회사의 보안 팀은 조직 내 특정 개인을 표적으로 하는 스피어피싱 공격이 증가하는 상황을 인지했지만 유감스럽게도 기존 이메일 보안 솔루션으로는 이러한 공격을 차단할 수 없었습니다. 기존 솔루션이 이메일 링크의 "안전성" 또는 "유해성" 평가를 주로 사용했기 때문입니다.



## Menlo는 사용자의 기본 이메일 환경에 영향을 주지 않고 스피어피싱, 자격 증명 도용 공격을 비롯한 링크와 첨부 파일에 포함된 이메일 기반 멀웨어를 방어합니다.

각각의 이메일 링크가 고유했으므로 정확하게 판별하도록 내부적으로 감지 또는 분석할 수 있는 위협 인텔리전스의 평판 데이터가 소용이 없었습니다. 한 번 판단이 잘못되면 자격 증명 도용을 시도하거나 멀웨어가 단말에 다운로드되는 사이트로 사용자가 직접 연결되었습니다. 단 한 번의 오류로도 수십억 달러의 손실을 야기하는 전면적인 공격이 발생할 수 있으므로 그 위험은 너무나 컸습니다.

이 투자 회사는 이메일 기반 공격으로부터 사용자를 안전하게 보호하는 방법에 대한 사고의 전환이 필요하다는 사실을 알게 되었습니다

## 보안 격차를 해소하는 Menlo Security Internet Isolation Gateway

이 투자 회사는 이미 Menlo Security Internet Isolation Gateway를 사용하여 웹 기반 위협으로부터 사용자를 보호하고 있었으므로 Menlo에서 사용자 이메일의 링크와 첨부 파일도 격리시킬 수 있다는 사실을 알게 되었습니다. Menlo Security는 이 회사와 긴밀한 협력을 통해 전 세계 사용자 수십만 명을 지원할 수 있는 확장 가능한 아키텍처를 개발했습니다.

이제 이메일의 모든 링크가 Menlo 클라우드에서 격리 및 실행되므로 멀웨어의 사용자 브라우저 액세스가 차단됩니다. 동시에 의심스러운 웹 양식이 읽기 전용으로 렌더링되므로 사용자가 위조 로그인 페이지에 자신의 자격 증명을 입력하는 것을 방지할 수 있습니다. 사용자는 이 특별한 방식으로 입력 필드 제한 사항이 적용되는 사이트를 안전하게 볼 수 있으며 제공되는 정보로 사이트의 적법성을 판별할 수 있습니다. 이 정보는 기업 피싱 인식 교육을 추가로 실시할 수 있도록 구성 가능한 메시지를 통해 제공됩니다.

## 모든 이메일 링크 및 첨부 파일 기반 공격 완벽 방어

Menlo Security Isolation Gateway는 클라우드의 모든 이메일 링크를 사용자 장치로부터 격리함으로써 기존 솔루션의 감지 및 대응 방식의 한계에 따른 이메일 보안 격차를 해소합니다. Menlo는 사용자의 기본 이메일 및 인터넷 브라우징 환경에 영향을 미치지 않고 이메일 링크와 첨부 파일을 기반으로 하는 멀웨어, 스피어 피싱, 자격 증명 도용 및 랜섬웨어를 차단합니다. 사용자는 위험성 여부에 관계없이 어떤 이메일 링크를 클릭해도 바이러스에 감염되거나 자격 증명을 도용당하지 않는다는 확신을 가질 수 있습니다.

Menlo Security에서 어떻게 업무를 보호하는지 알아보려면 [menlosecurity.com](https://menlosecurity.com)에 방문하거나 [korea@menlosecurity.com](mailto:korea@menlosecurity.com)으로 문의하십시오.



자세한 내용은 다음 연락처로  
당사에 문의하십시오.

[menlosecurity.com](https://menlosecurity.com)

(650) 695-0695

[korea@menlosecurity.com](mailto:korea@menlosecurity.com)



### Menlo Security 회사 소개

Menlo Security는 조직에서 위협을 제거하고 생산성을 완전히 확보할 수 있는 격리 기반의 우수한 클라우드 보안 플랫폼을 제공합니다. 이 플랫폼은 클라우드 보안의 본질을 이행하는 유일한 솔루션으로, 악의적인 공격을 방어하기 위해 가장 안전한 제로 트러스트 방식을 제공하며 최종 사용자가 온라인 작업 과정에서 보안 기능이 실행되는 것을 인식하지 못하고 보안 팀의 업무 부담도 없애줍니다. 이제 조직은 조직 내 사용자에게 보안에 대한 걱정 없이 비즈니스 계속 수행할 수 있는 안전한 온라인 환경을 제공할 수 있습니다.

© 2021 Menlo Security, All Rights Reserved.