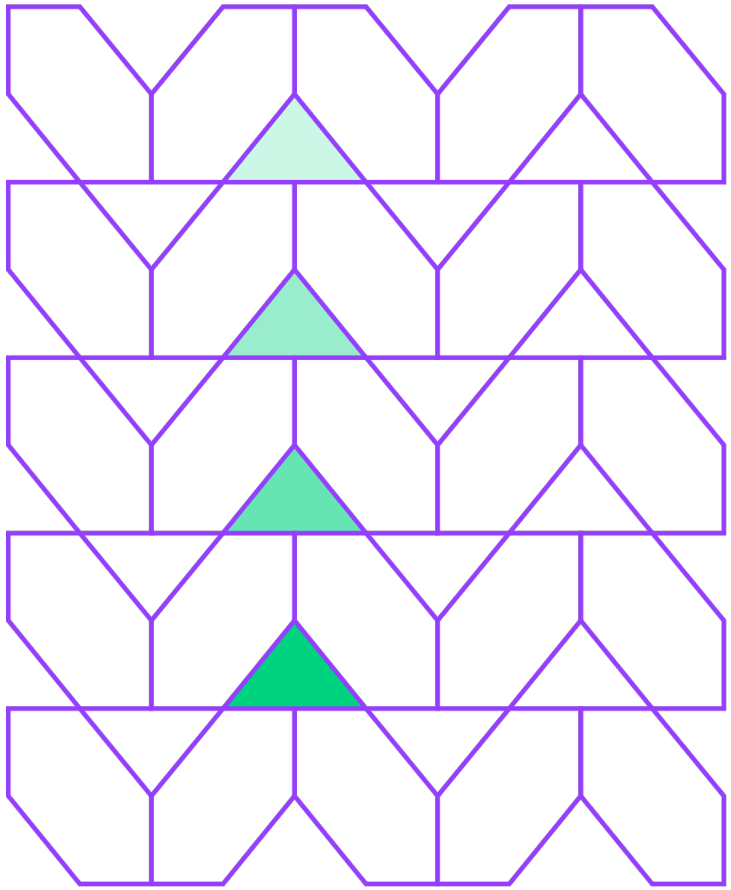
MENLO SECURITY

이메일 격리 솔루션 제안

지능적인 이메일 공격으로부터 사용자 완벽 보호

멘로시큐리티 코리아

Agenda



- 제안 배경
- 제안 목표
- 이메일 격리 주요 기능
- 도입 효과

제안 배경

이메일을 이용한 사이버 공격증가 - 2022 ver. 리포트

- 모든 데이터 유출의 36%가 피싱과 관련 (예, 국내 기업 대상 Labsus$ 공격)
- 전송된 이메일의 거의 1.2%가 본질적으로 악성 이메일

1. 타깃 공격에 효과적 - 각종 사회 관계망 서비스를 이용하여 손쉽게 타겟 확인

- 특정 공격 대상자 지정 후, 목적에 따라 손쉽게 공격 가능
- 계정 탈취를 위한 Phishing 공격, 악성코드 전달/감염을 위한 URL 링크 전달에 효과적

2. 이메일을 이용한 공격 방어 어려움 - 비지니스 애플리케이션

- 대부분의 대외 업무는 이메일 이용 - 관계사(Supply Chain)로 위장 시, 손쉽게 보안 우회
- 본문의 각종 링크 및 컨텐츠들에 대한 심층 분석/대응 솔루션 부재
  - 제로데이 악성 URL 이용시 손쉽게 보안 우회

3. 재택/원격 근무 증가로 개인 대상 공격 후, 회사 공격

- 재택 또는 원격 근무가 증가 - 보호되지 않은 개인 이메일 대상 선 공격 후, 계정 탈취 & PC 감염 실시
- 이후 VPN 이용 회사 네트워크 접속 시, 회사 정보 유출

하루

34

억 개 이상

피싱 이메일 발생

MENLO SECURITY

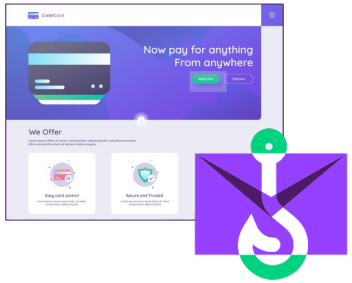
제안 배경 - 제로데이 악성 URL 대응 어려움

감염 벡터 및 대응

악성 / 피싱메일

URL 링크

- 자동 혹은 수동 신규 URL 링크 생성
- 모든 보안 솔루션 탐지 회피



정보 유출

- Credential 피싱
- 내부 정보 유출

악성코드 다운로드 & 감염

- HTML Smuggling 링크
- Data URI 링크
- 패스워드 설정
  압축 파일 다운로드

AV/Sandbox

첨부 파일

- 단순 악성 첨부파일은
  기존 보안 솔루션에서
  이미 대부분 차단

차단

제안 목표

이메일을 이용한 각종 공격 완벽 방어

이메일 본문 내 URL 링크에 대한 웹 격리 기술 적용

1) 이메일 본문 내, URL 링크에 웹 격리 기술 적용

- 사용자 감염 방지
- 클라우드 웹 격리 기술 적용
- 원본 HTML 소스 포함
- 사용자에게 컨텐츠 전달 방지

2) 피싱 공격 대응

- 피싱 공격 의심시, 해당 링크에 Read-only 모드 적용
- 사용자 입력 차단

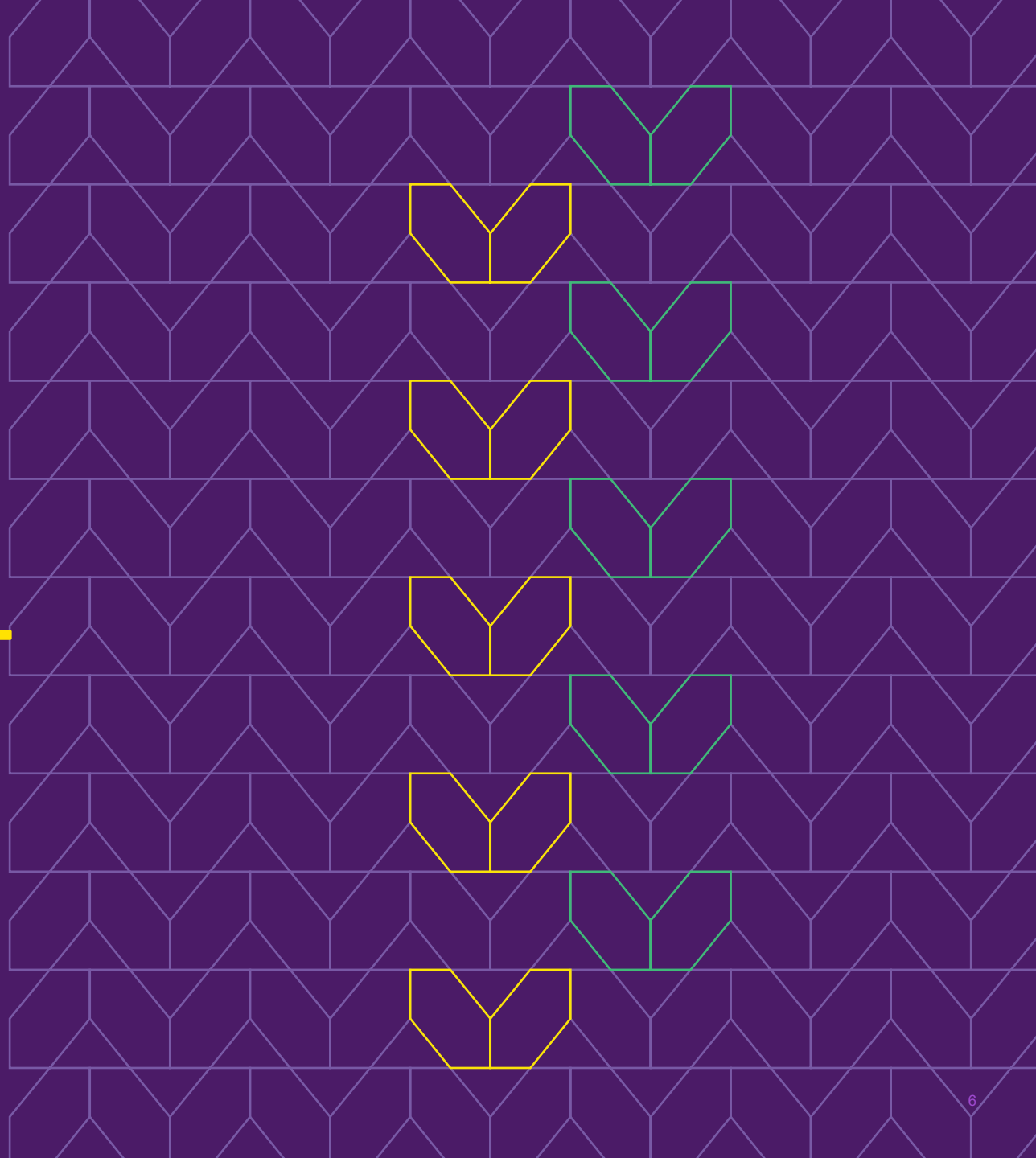
3) 클라우드 및 자체 이메일 서비스 모두 적용

- 클라우드 이메일 서비스 (O365, G-suite) 쉽게 연동
- 자체 이메일 서버를 위한 On-prem 솔루션 지원

기존 레거시 방식이 아닌, 혁신적인 기술 사용 사용자 완벽 보호

MENLO SECURITY

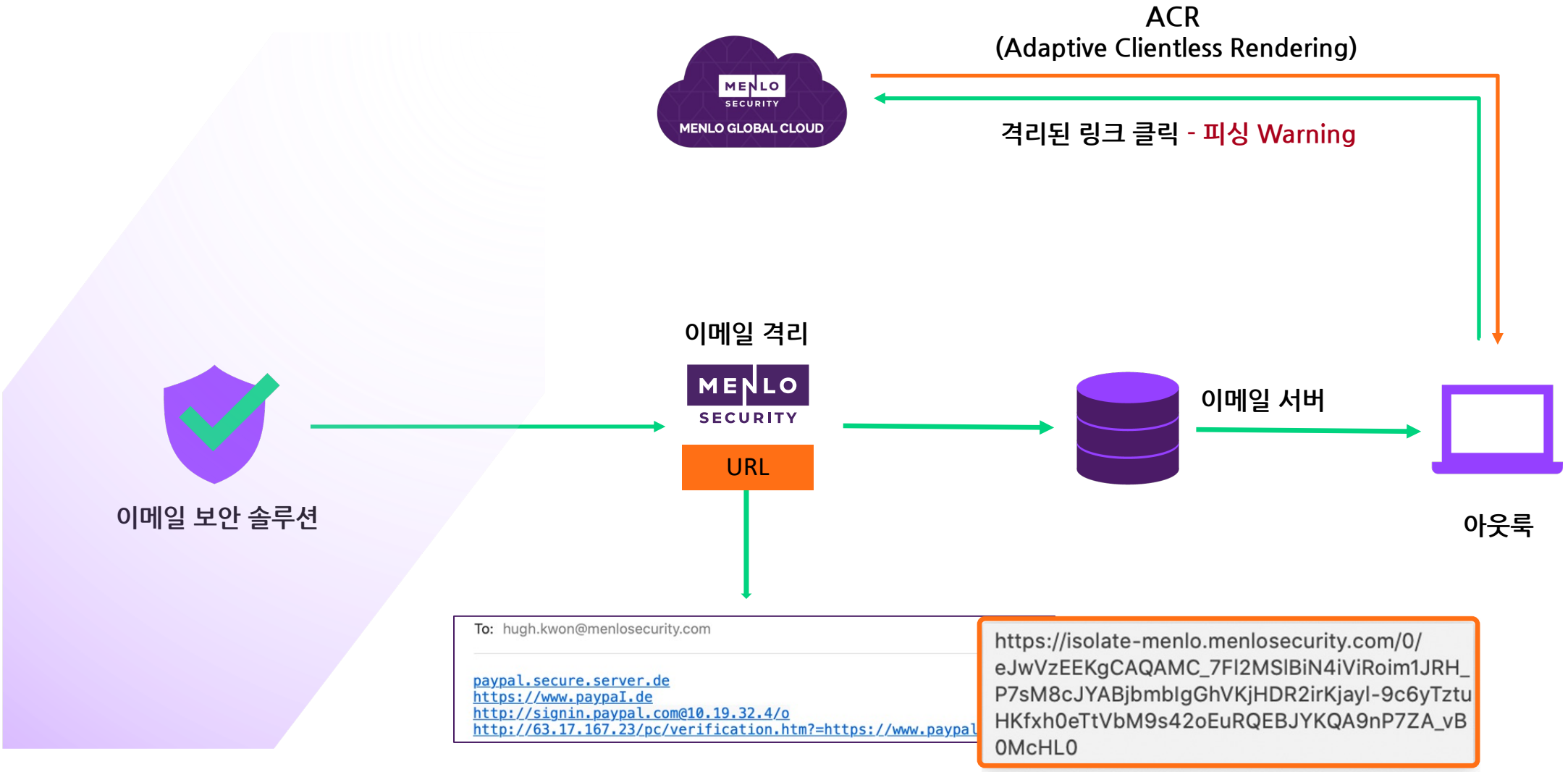
이메일 격리 주요 기능



MENLO SECURITY

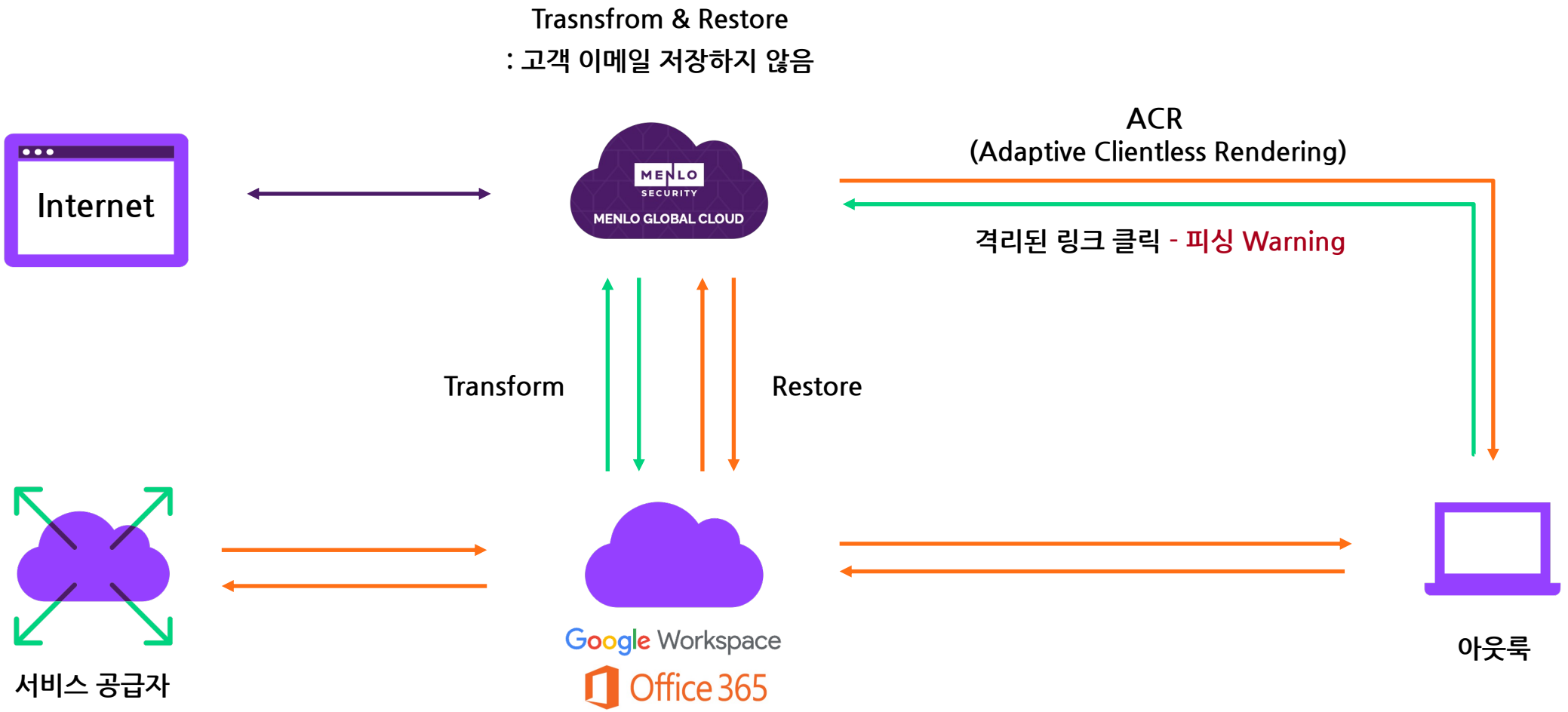
이메일 격리 - 자체 이메일 서버 보유 시

#1 URL 변환



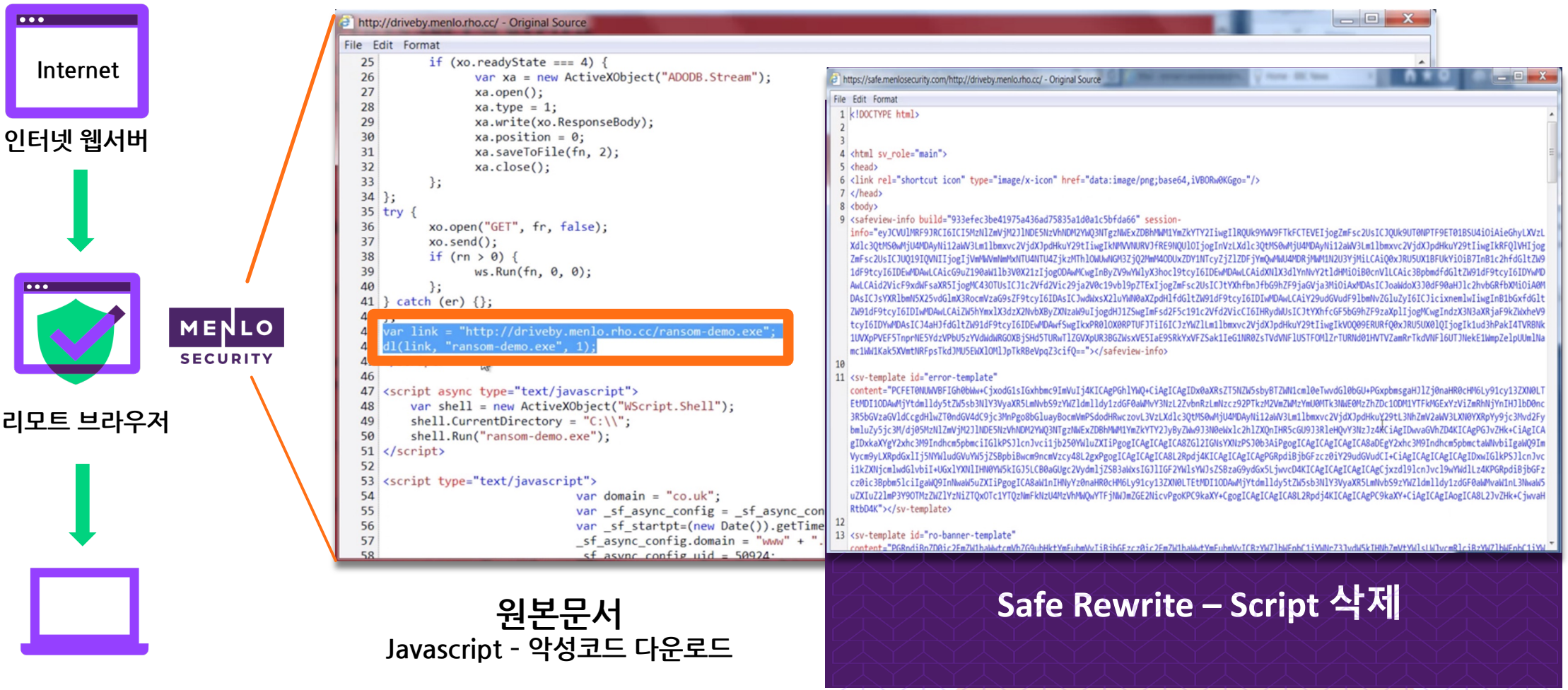
이메일 격리 - O365/Google Workspace 연동 시

#1 URL 변환



이메일 격리

#2 URL 격리: 악성코드 다운로드 방지 + 피싱 방지



이메일 격리

2 URL 격리: **악성코드 다운로드 방지** + 피싱 방지

URL 링크를 통한 모든 웹 페이지는 격리 실시 - 따라서 악성코드 다운로드 위험 없음

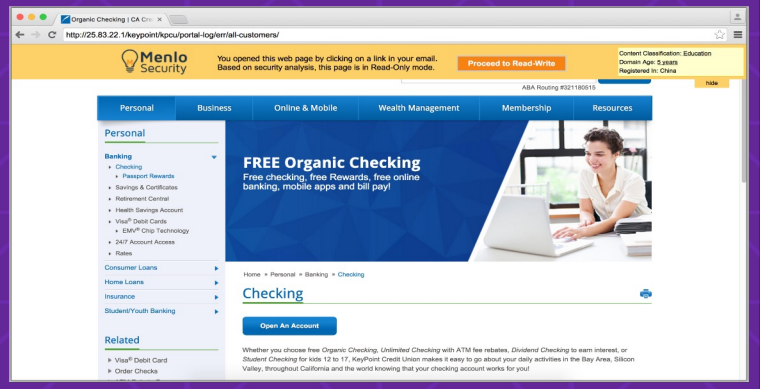
이메일 격리

#2 URL 격리: 악성코드 다운로드 방지 + 피싱 방지

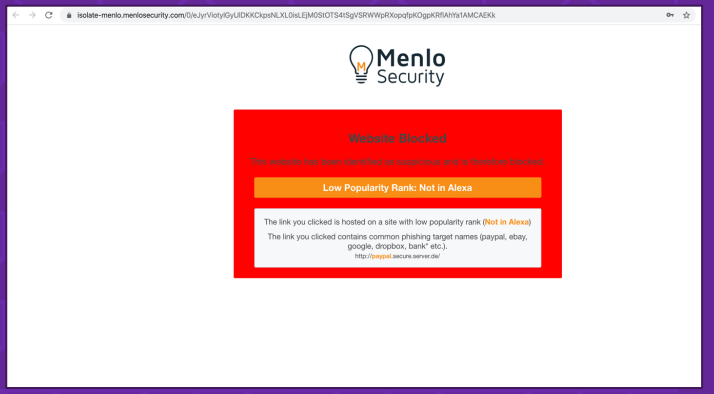
Menlo Risk Score	User Experience	Entry Action	Exit Action
Low	Educate	Read-Write	Connect Direct
Medium	Educate	Read-Only	Read-Write
High	Coach	Block	

피싱 이메일 판단 시 Read-only 모드 적용

Low Risk



Medium Risk



High Risk

MENLO SECURITY

도입효과

이메일을 공격 수단으로 한 각종
사이버 공격 완벽 방어

- 악성 URL에 대해 단순 허용/차단이 아닌 모든 컨텐츠에 대한 격리 실시
- 악성 URL에 의한 Drive-by Download 익스플로잇 공격 방지(제거) 하는 유일한 솔루션
- 최첨단 피싱 탐지 엔진을 활용하여 로그인 정보 유출 피싱으로부터 완벽 보호
- 피싱 위험정도에 따라 다양한 정책 적용
- 사용자 교육 메세지 전달 & 인식 강화
- 엔드 포인트 소프트웨어 또는 어플라이언스가 필요하지 않으며 보안 인프라를 단순화
- Office 365와 손쉽게 통합

MENLO SECURITY

멘로시큐리티와 함께하는 많은 기업들

MENLO SECURITY

ANZ

JPMorgan Chase & Co.

VISA

HSBC

citi

Government and defense

Critical infrastructure and transportation

4 out 5 largest credit card companies

8 out 10 largest banks

Global-2000 customers

Frost & Sullivan's Leader in the Frost Radar: Secure Web Gateways Report

menlosecurity.com