INSEC security

Metadefender CORE

Metadefender E-mail

Metadefender Proxy

Metadefender KIOSK

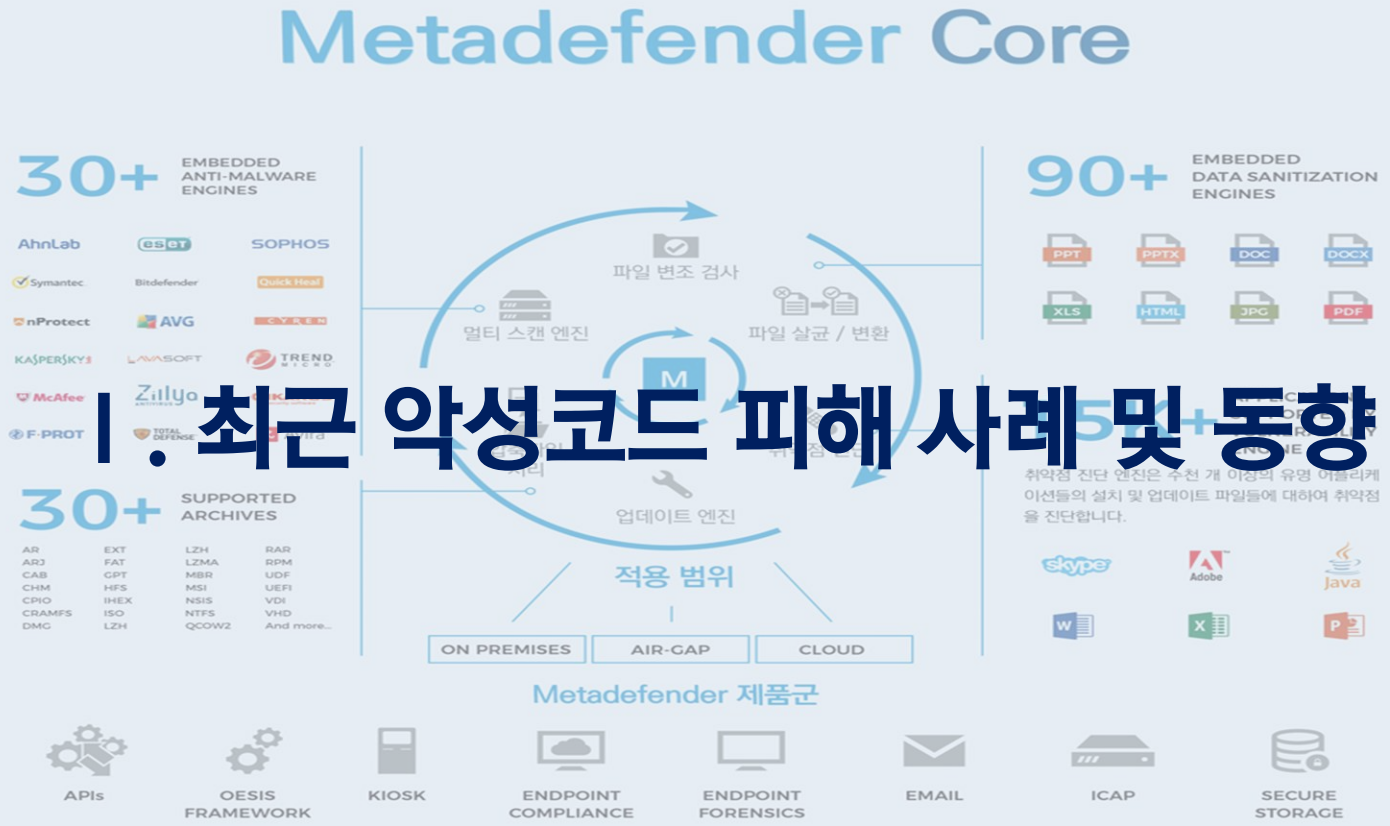
OPSWAT

Metadefender

글로벌 유명 멀티 안티바이러스 스캔 엔진

2017. 4

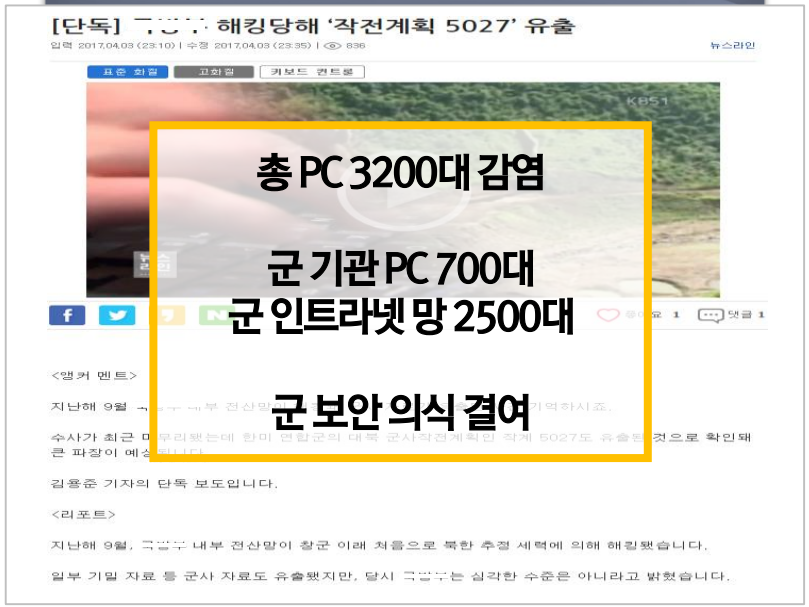
CONTENT



Ⅰ. 최근 악성코드 피해 사례 및 동향

최신 피해 사례 [국 내]

군 기관 해킹 사례



총 PC 3200대 감염

군 기관 PC 700대
군 인트라넷 망 2500대

군 보안 의식 결여

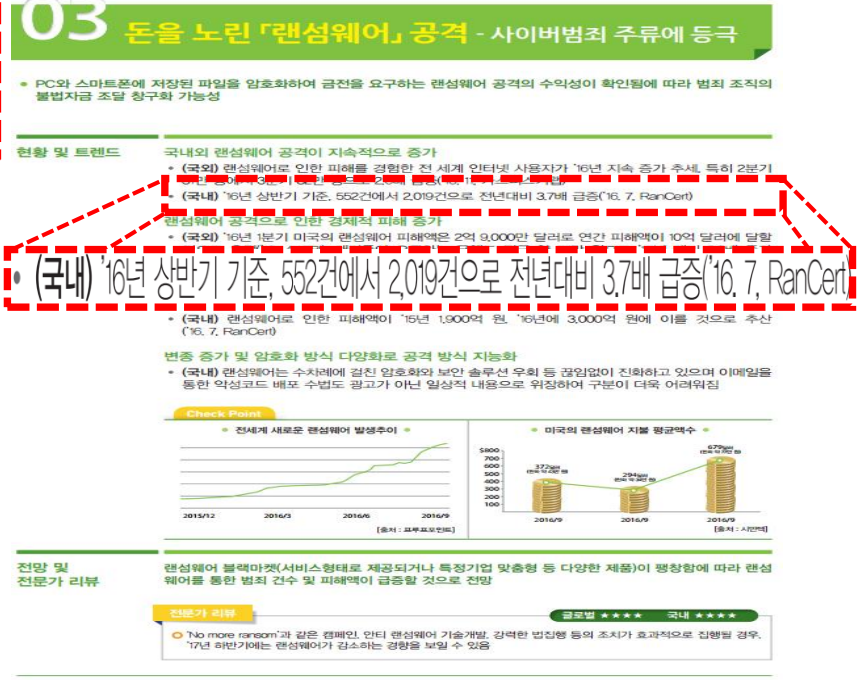
여기어때 해킹 사례

약 91만명 개인 정보 유출

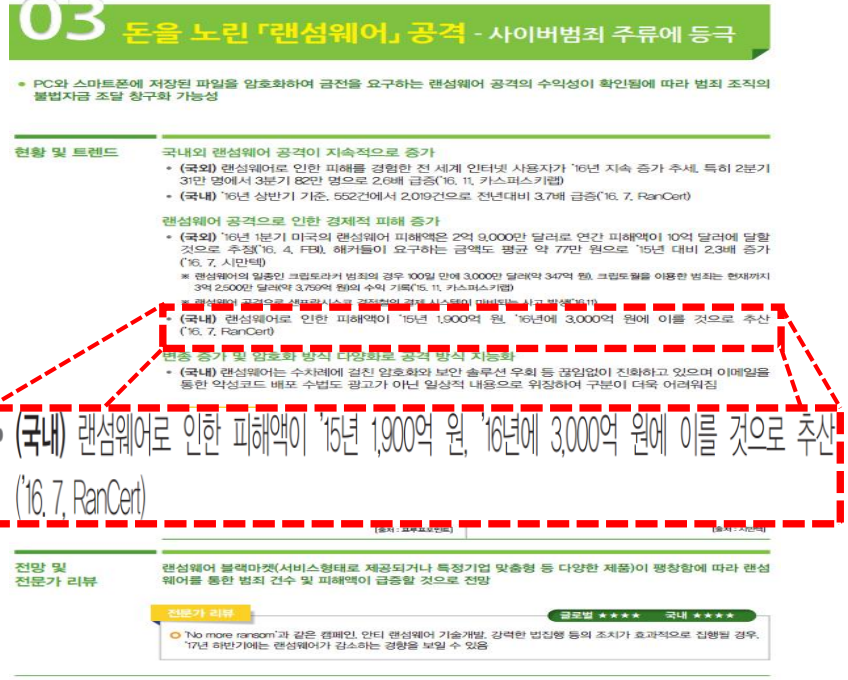
회원 정보 유출로 4000여명의 회원에게 협박 문자 및 보이스 피싱 시도

최신 피해 사례 [국 내]


1
강대국간 사이버 공방 심화
사이버 전면전 위험 고조
2
사이버위협정보 공유와 협력 확대
대응이 빨라진다
3
RANSOMWARE
돈을 노린 랜섬웨어 공격
사이버범죄 주류에 등극
4
빅데이터 AI 클라우드
패러다임이
5
분산저장기술
이론에서
8
활성화되는 커넥티드 카의 안전띠
사이버보안
YES!
NO!
잊힐 권리 보장
강화되는 개인정보 자기결정권
개인정보 가이드라인
개인정보 보호와 활용의 조화
4차 산업혁명을 좌우한다
3
RANSOMWARE
돈을 노린 랜섬웨어 공격
사이버범죄 주류에 등극
이슈
sed
Life
사물인터넷(IoT)
일상의 위험


03 돈을 노린 「랜섬웨어」 공격 - 사이버범죄 주류에 등극
• PC와 스마트폰에 저장된 파일을 암호화하여 금전을 요구하는 랜섬웨어 공격의 수익성이 확인됨에 따라 범죄 조직의 불법자금 조달 창구화 가능성
현황 및 트렌드
국내외 랜섬웨어 공격이 지속적으로 증가
• (국외) 랜섬웨어로 인한 피해를 경험한 전 세계 인터넷 사용자가 '16년 지속 증가 추세, 특히 2분기
• (국내) '16년 상반기 기준, 552건에서 2,019건으로 전년대비 3.7배 급증('16. 7, RanCert)
랜섬웨어 공격으로 인한 경제적 피해 증가
• (국외) '16년 1분기 미국의 랜섬웨어 피해액은 2억 9,000만 달러로 연간 피해액이 10억 달러에 달할
(국내) '16년 상반기 기준, 552건에서 2,019건으로 전년대비 3.7배 급증('16. 7, RanCert)
• (국내) 랜섬웨어로 인한 피해액이 '15년 1,900억 원, '16년에 3,000억 원에 이를 것으로 추산 ('16. 7, RanCert)
변종 증가 및 암호화 방식 다양화로 공격 방식 지능화
• (국내) 랜섬웨어는 수차례에 걸친 암호화와 보안 솔루션 우회 등 끊임없이 진화하고 있으며 이메일을 통한 악성코드 배포 수법도 광고가 아닌 일상적 내용으로 위장하여 구분이 더욱 어려워짐
Check Point
전세계 새로운 랜섬웨어 발생추이
2015/12
2016/3
2016/6
2016/9
[출처 : 프루프포인트]
미국의 랜섬웨어 지불 평균액수
$900
700
600
500
400
300
200
100
2016/9
2016/9
2016/9
[출처 : 사이버]
전망 및 전문가 리뷰
랜섬웨어 블랙마켓(서비스형태로 제공되거나 특정기업 맞춤형 등 다양한 제품)이 팽창함에 따라 랜섬웨어를 통한 범죄 건수 및 피해액이 급증할 것으로 전망
전문가 리뷰
글로벌 ★★★★ 국내 ★★★★
○ 'No more ransom'과 같은 캠페인, 안티 랜섬웨어 기술개발, 강력한 법집행 등의 조치가 효과적으로 집행될 경우, '17년 하반기에는 랜섬웨어가 감소하는 경향을 보일 수 있음

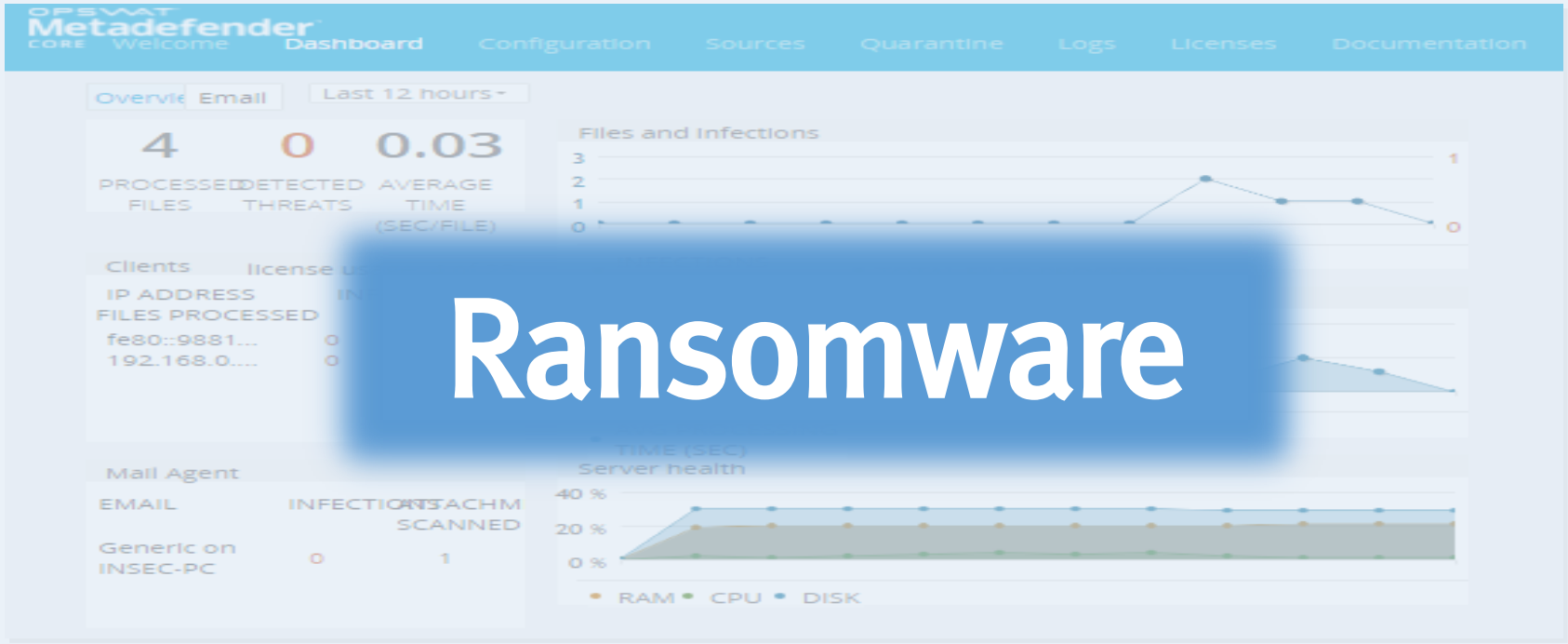
최신 피해 사례 [국 내]



• (국내) 랜섬웨어로 인한 피해액이 '15년 1,900억 원, '16년에 3,000억 원에 이를 것으로 추산 ('16. 7. RanCert)

최신 피해 사례 [국 내]


1
강대국간 사이버 공방 심화
사이버 전면전 위험 고조
2
사이버위협정보 공유와 협력 확대
대응이 빨라진다
3
돈을 노린 랜섬웨어 공격
사이버범죄 주류에 등극
4
빅데이터 AI 클라우드
패러다임이
5
분산저장기술
이론에서
8
활성화되는 커넥티드 카의 안전띠
사이버보안
YES!
NO!
잊힐 권리 보장
강화되는 개인정보 자기결정권
개인정보 가이드라인
개인정보 보호와 활용의 조화
4차 산업혁명을 좌우한다
3
RANSOMWARE
돈을 노린 랜섬웨어 공격
사이버범죄 주류에 등극
이슈
sed
Life
사물인터넷(IoT)
일상의 위험
03 돈을 노린 「랜섬웨어」 공격 - 사이버범죄 주류에 등극
• PC와 스마트폰에 저장된 파일을 암호화하여 금전을 요구하는 랜섬웨어 공격의 수익성이 확인됨에 따라 범죄 조직의 불법자금 조달 창구화 가능성
현황 및 트렌드
국내외 랜섬웨어 공격이 지속적으로 증가
• (국외) 랜섬웨어로 인한 피해를 경험한 전 세계 인터넷 사용자가 '16년 지속 증가 추세, 특히 2분기 31만 명에서 3분기 82만 명으로 2.6배 급증('16. 11. 카스퍼스키랩)
• (국내) '16년 상반기 기준, 552건에서 2,019건으로 전년대비 3.7배 급증('16. 7. RanCert)
랜섬웨어 공격으로 인한 경제적 피해 증가
• (국외) '16년 1분기 미국의 랜섬웨어 피해액은 2억 9,000만 달러로 연간 피해액이 10억 달러에 달할 것으로 추정('16. 4. FBI), 해커들이 요구하는 금액도 평균 약 77만 원으로 '15년 대비 2.3배 증가
랜섬웨어 블랙마켓(서비스형태로 제공되거나 특정기업 맞춤형 등 다양한 제품)이 팽창함에 따라 랜섬웨어를 통한 범죄 건수 및 피해액이 급증할 것으로 전망
Check Point
전세계 새로운 랜섬웨어 발생추이
2015/12
2016/3
2016/6
2016/9
[출처 : 체크포인트]
미국의 랜섬웨어 지불 평균액수
$800
700
600
500
400
300
200
100
372달러
294달러
679달러
2016/9
2016/9
2016/9
[출처 : 시만텍]
전망 및 전문가 리뷰
랜섬웨어 블랙마켓(서비스형태로 제공되거나 특정기업 맞춤형 등 다양한 제품)이 팽창함에 따라 랜섬웨어를 통한 범죄 건수 및 피해액이 급증할 것으로 전망
전문가 리뷰
글로벌 ★★★★ 국내 ★★★★
○ 'No more ransom'과 같은 캠페인, 안티 랜섬웨어 기술개발, 강력한 법집행 등의 조치가 효과적으로 집행될 경우, '17년 하반기에는 랜섬웨어가 감소하는 경향을 보일 수 있음


OPSWAT
Metadefender
CORE
Welcome
Dashboard
Configuration
Sources
Quarantine
Logs
Licenses
Documentation
Overvie
Email
Last 12 hours -
4
PROCESSED FILES
0
DETECTED THREATS
0.03
AVERAGE TIME (SEC/FILE)
Files and Infections
3
2
1
0
1
0
Clients
IP ADDRESS
FILES PROCESSED
fe80::9881...
0
192.168.0....
0
Ransomware
TIME (SEC)
Mail Agent
EMAIL
INFECTIONS
SCANNED
Generic on INSEC-PC
0
1
Server health
40 %
20 %
0 %
RAM
CPU
DISK

최신 피해 사례 [국 내]

페티야(PETYA) 랜섬웨어

MBR영역을 변조하는 'PETYA' 랜섬웨어 등장

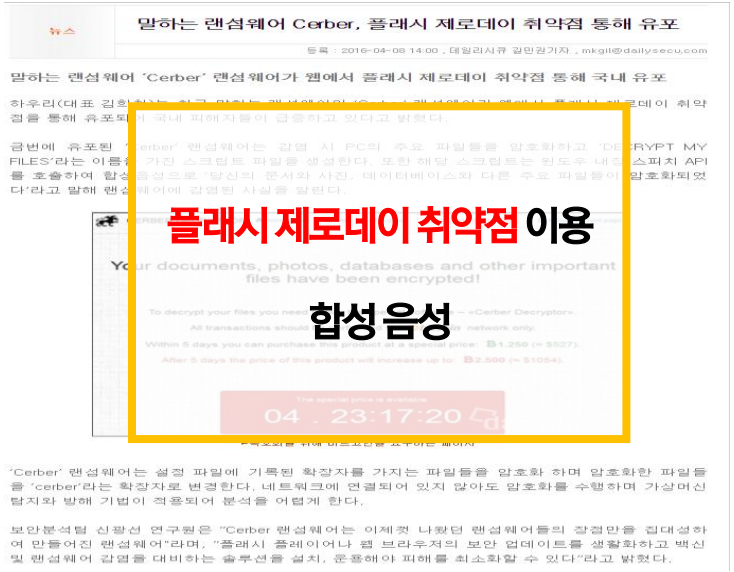
지난 금요일(3/25)부터 MBR(Master Boot Record)영역을 변조하여 아스키코드로 제작한 해골화면을 띄우고, 랜섬웨어에 감염되었다는 랜섬메시지를 띄우는 'PETYA' 랜섬웨어가 발견되어 주의가 필요합니다.

주로 이메일 첨부파일을 통해 드롭박스를 경유하여 랜섬웨어가 유입되는 형태를 띄고 있으며, 일단 감염되면 MBR영역이 변조되기 때문에 재부팅 이후에도 정상적으로 윈도우OS 부팅이 불가능합니다. (감염되면 몇분 이내로 시스템이 강제 재부팅됨)

<그림1 PETYA 랜섬웨어가 MBR영역을 변조한 후 최초로 띄우는 해골 이미지 화면>

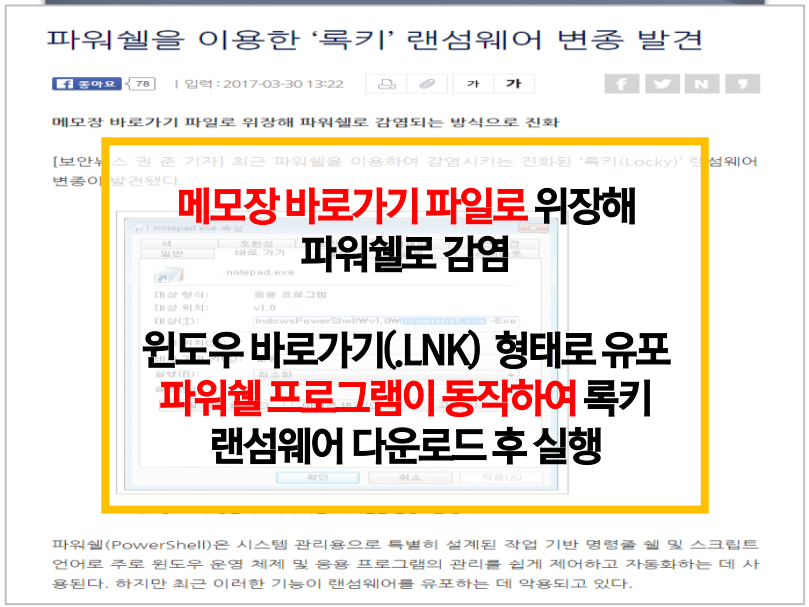
해골 이미지가 뜬 이후, 감염된 PC의 사용자가 아무키나 입력하면 아래의 랜섬 메시지가 뜨게 됩니다.

서버(Cerber) 랜섬웨어



최신 피해 사례 [국 내]

록키(Locky) 랜섬웨어



파워쉘을 이용한 '록키' 랜섬웨어 변종 발견

메모장 바로가기 파일로 위장해 파워쉘로 감염되는 방식으로 진화

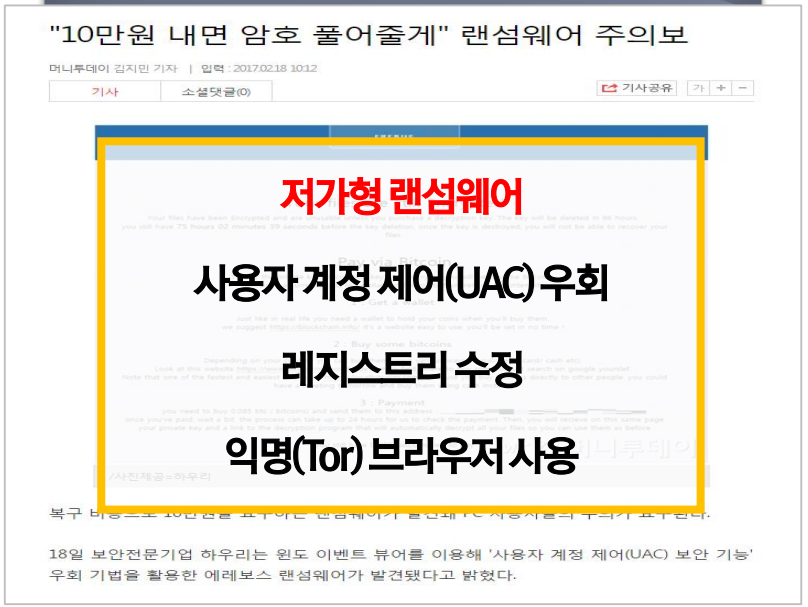
[보안뉴스 권 준 기자] 최근 파워쉘을 이용하여 감염시키는 진화된 '록키(Locky)' 랜섬웨어 변종이 발견됐다.

메모장 바로가기 파일로 위장해
파워쉘로 감염

윈도우 바로가기(.LNK) 형태로 유포
파워쉘 프로그램이 동작하여 록키
랜섬웨어 다운로드 후 실행

파워쉘(PowerShell)은 시스템 관리용으로 특별히 설계된 작업 기반 명령줄 쉘 및 스크립트 언어로 주로 윈도우 운영 체제 및 응용 프로그램의 관리를 쉽게 제어하고 자동화하는 데 사용된다. 하지만 최근 이러한 기능이 랜섬웨어를 유포하는 데 악용되고 있다.

에레보스(Erebus) 랜섬웨어



"10만원 내면 암호 풀어줄게" 랜섬웨어 주의보

머니투데이 김지민 기자 | 입력 : 2017.02.18 10:12

기사 | 소셜댓글(0) | 기사공유

저가형 랜섬웨어

사용자 계정 제어(UAC) 우회

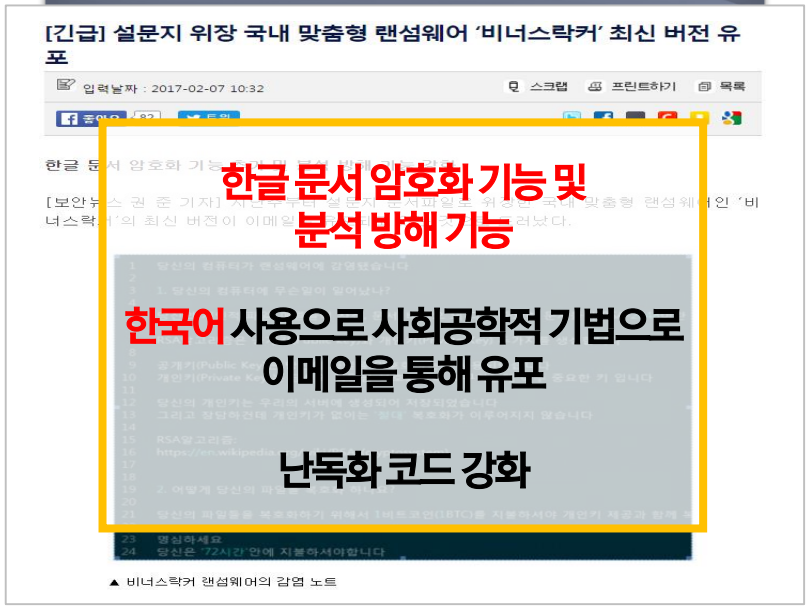
레지스트리 수정

익명(Tor) 브라우저 사용

18일 보안전문기업 하우리는 윈도 이벤트 뷰어를 이용해 '사용자 계정 제어(UAC) 보안 기능' 우회 기법을 활용한 에레보스 랜섬웨어가 발견됐다고 밝혔다.

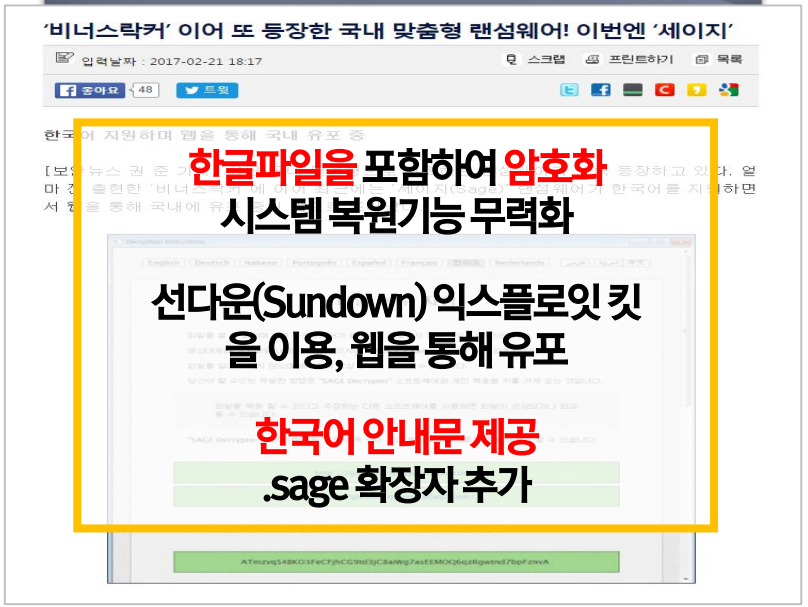
최신 피해 사례 [국 내]

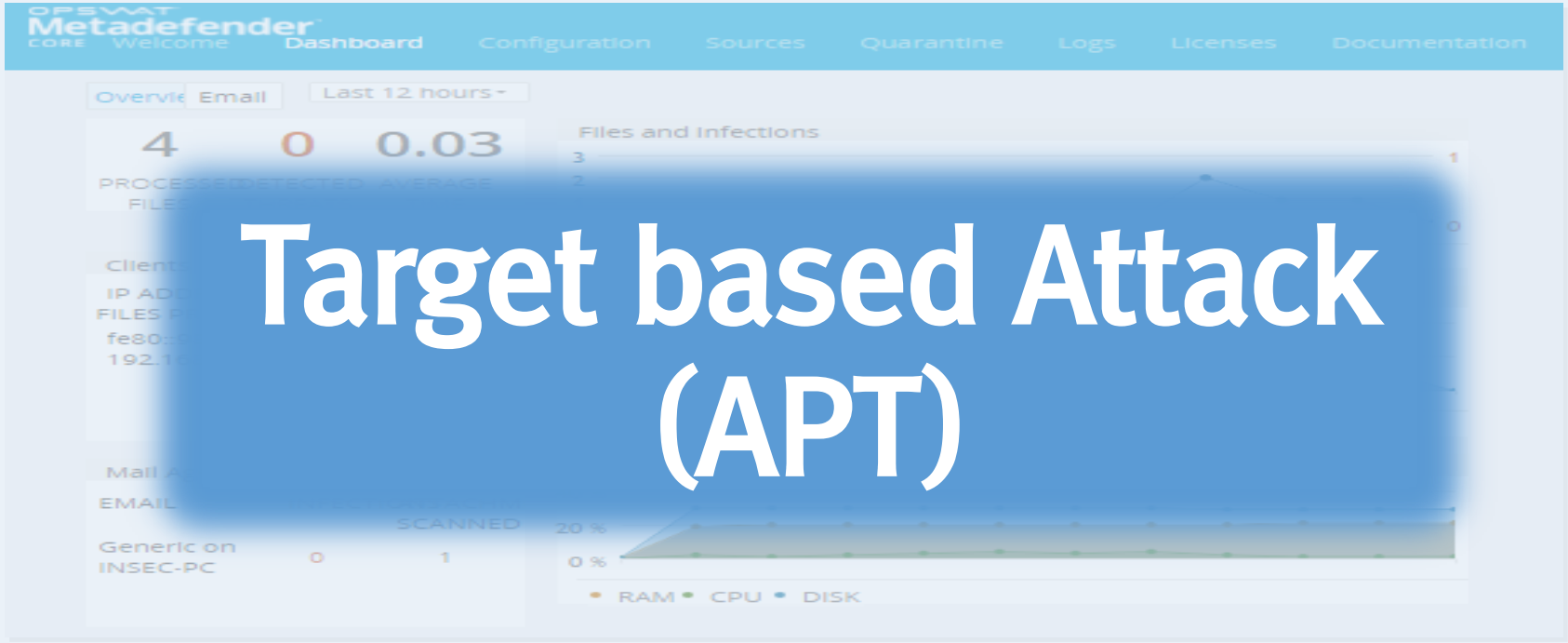
비너스락커(VenusLocker) 랜섬웨어



▲ 비너스락커 랜섬웨어의 감염 노트

세이지(sage) 랜섬웨어



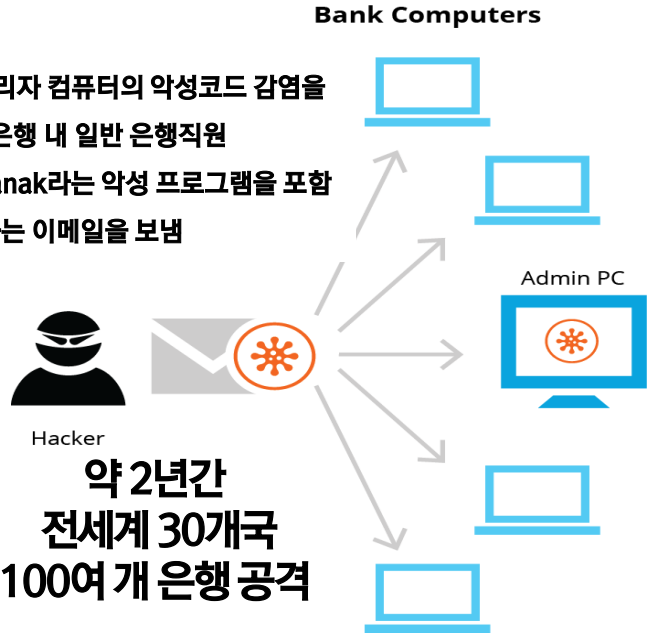


Target based Attack (APT)

최신 피해 사례 [국 외]

- **카바나크(Carbanak) APT**
  - ✓ 최초 악성코드가 감염된 이메일 첨부파일을 통해 전파
  - ✓ 악성코드는 내부 네트워크를 통해 빠르게 전염
  - ✓ 관리자 시스템에서 스크린샷 또는 키 스트로크 로그인 정보를 수집
  - ✓ ATM 현금 자동화 기기를 통해 현금 인출
  - ✓ 피해액이 10억 달러에 달함

해커는 은행 관리자 컴퓨터의 악성코드 감염을 위해 은행 내 일반 은행직원 컴퓨터에 Carbanak라는 악성 프로그램을 포함하는 이메일을 보냄



악성코드

탐지

어떻게 하고 계십니까?

최신 악성코드 동향

악성코드!

탐지?

제대로 하고 계신가요?

최신 악성코드 동향

엔드 포인트

사용자, 서버 시스템

보안 시스템?

최신 악성코드 동향

네트워크 포인트

Firewall, IPS, UTM

기타 보안 시스템?

최신 악성코드 동향

악성코드로 인한

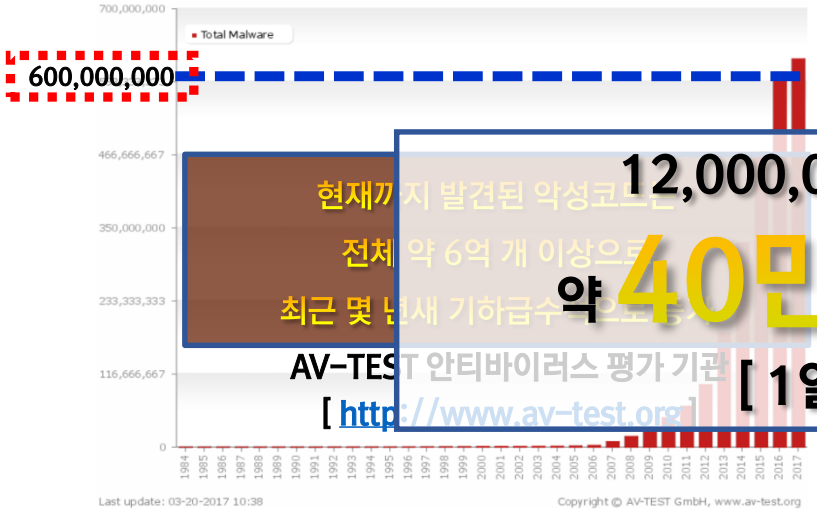
보안 사고가 계속해서

발생되는 원인?

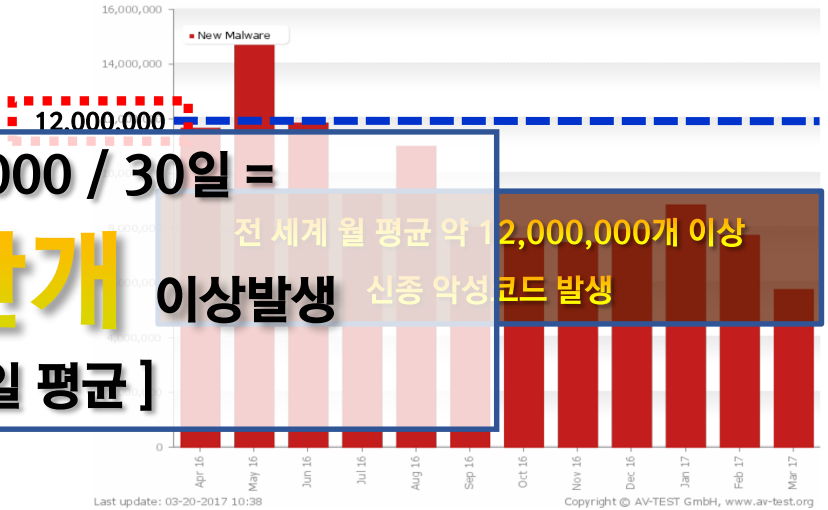
최신 악성코드 동향

✓ 현재까지 발생한 악성코드 총 합계는 약 6억 개에 달하며, 1일 평균 신종 악성코드의 발생 건 수는 약 40만개 이상 달한다.

Last update : 2017-03-20



Last update : 2017-03-20



12,000,000 / 30일 =

약 40만개 이상발생

[1일 평균]

AV-TEST 안티바이러스 평가 기관

[http://www.av-test.org]

최신 악성코드 동향

2017년 현재
일일 약 40만개 이상의
신종 및 변종
악성코드 발생

?

안티바이러스 스캐너

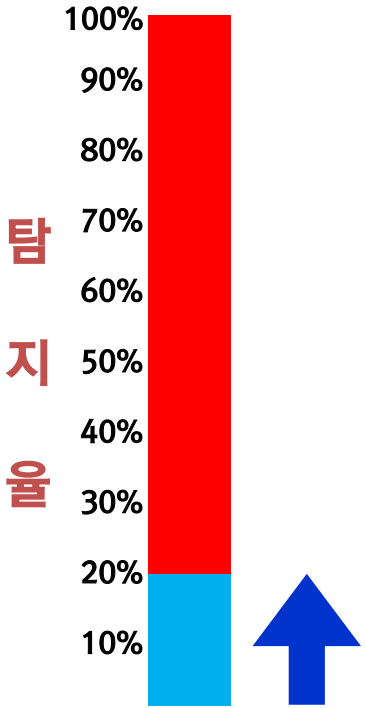
[A/V Scanner]

1일 패턴 DB 업데이트 개수?

최신 악성코드 동향

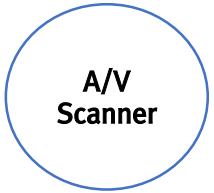

Updates in the last 24 hours
300
A/V 스캐너의
DB 업데이트
제작 / 패치 속도 한계!
1일 300개 미만 !
일일 약 40만개 이상의
신종 및 변종 악성코드에 대한
업데이트 / 패치 제작 및 대응 불가능!
400,000 – 300
= 3##,###개
150
0
Avira
Avast
AVG
Bitdefender
Total Defense
ClamAV
ESET NOD32
F-Prot
Fortinet
G Data
Ikarus
Kaspersky
McAfee
McAfee GW Edition
McAfee (Beta)
Microsoft
Panda Security
QuickHeal
Rising
Sophos
ThreatTrack
Symantec
Symantec (Beta)
Trend Micro
Trend Micro (Beta)
VBA32
Agnitum
Copyright © AV-TEST GmbH, www.av-test.org

최신 악성코드 동향



※ 안티바이러스의 한계점

약 6억 개
[600,000,000]
2017년 4월 현재



안티바이러스
엔진 1개

최신 악성코드 동향

전세계적으로

100% 악성코드를 차단할 수 있는

완벽한 안티바이러스(A/V)

제품은 단 한 개도

존재하지 않습니다.

최신 악성코드 동향

우선! 먼저!

탐지해야만

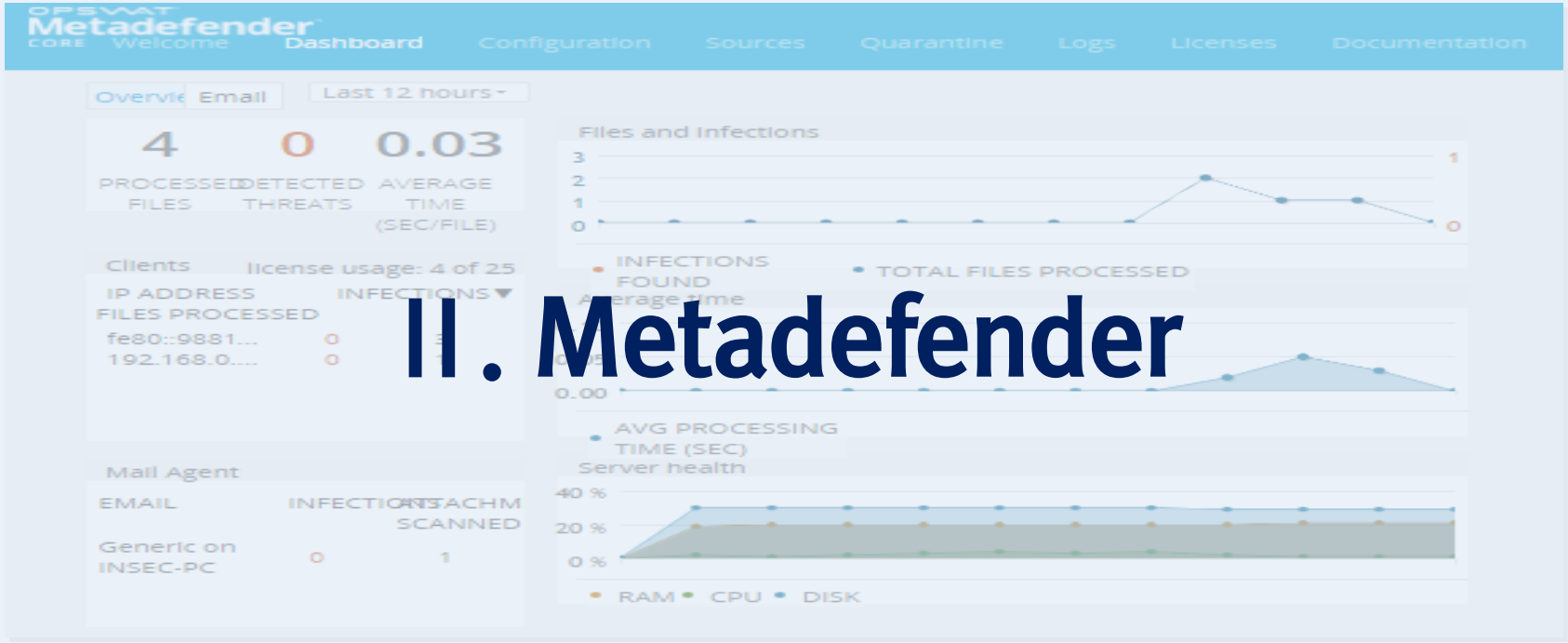
차단할 수 있습니다!

최신 악성코드 동향

어떻게

악성코드 탐지를 할 것인가?

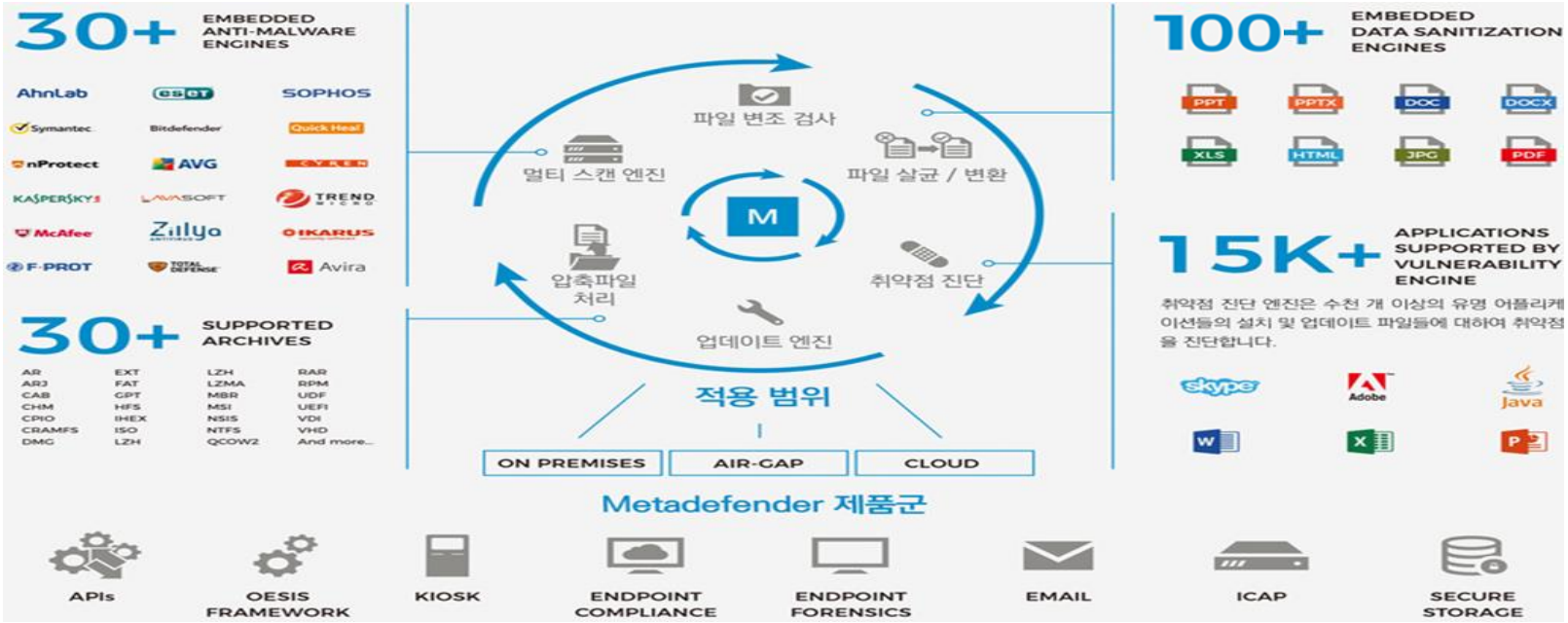
How ?



II. Metadefender

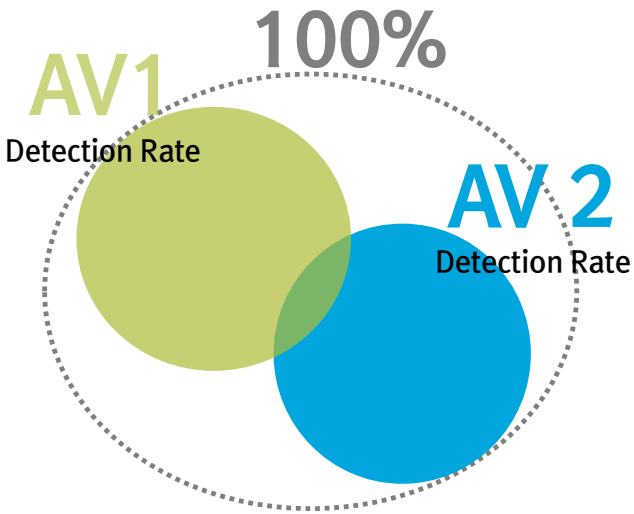
Metadefender 장점

- ✓ **글로벌 유명 Anti-Virus 30여개를 물리적으로 통합하여 Multi scanning 및 Data sanitization에 의한 악성코드 원천 유입 방지**

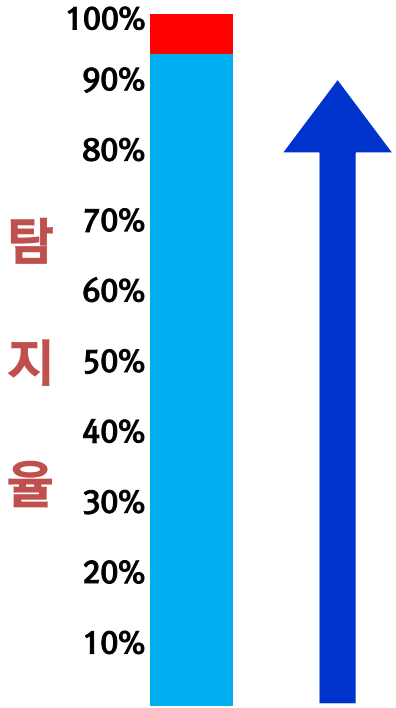


멀티스캐닝 장점

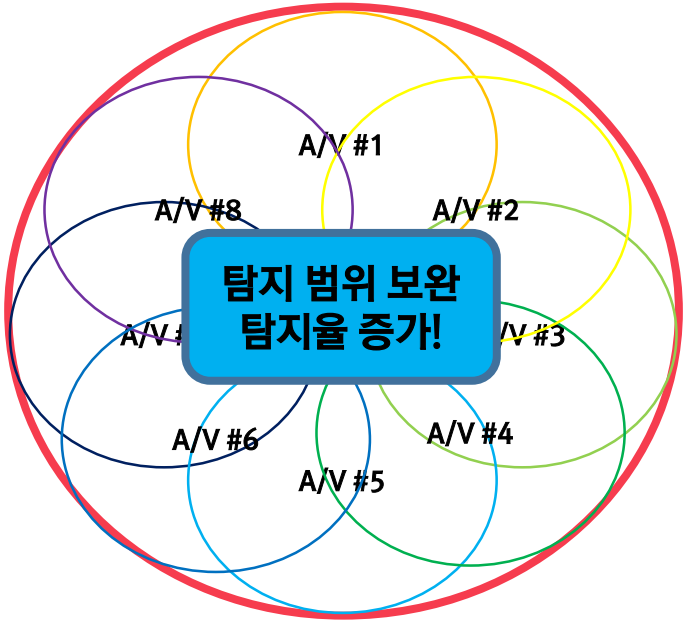
- ✓ 단일 안티바이러스 엔진은 완벽하지 않음
- ✓ 각 엔진 별 강점과 약점을 가지고 있어, 복수의 엔진을 사용하면 보완효과
- ✓ 복수의 엔진을 사용하여 탐지율을 향상



멀티스캐닝 장점



※ 탐지율 증가!



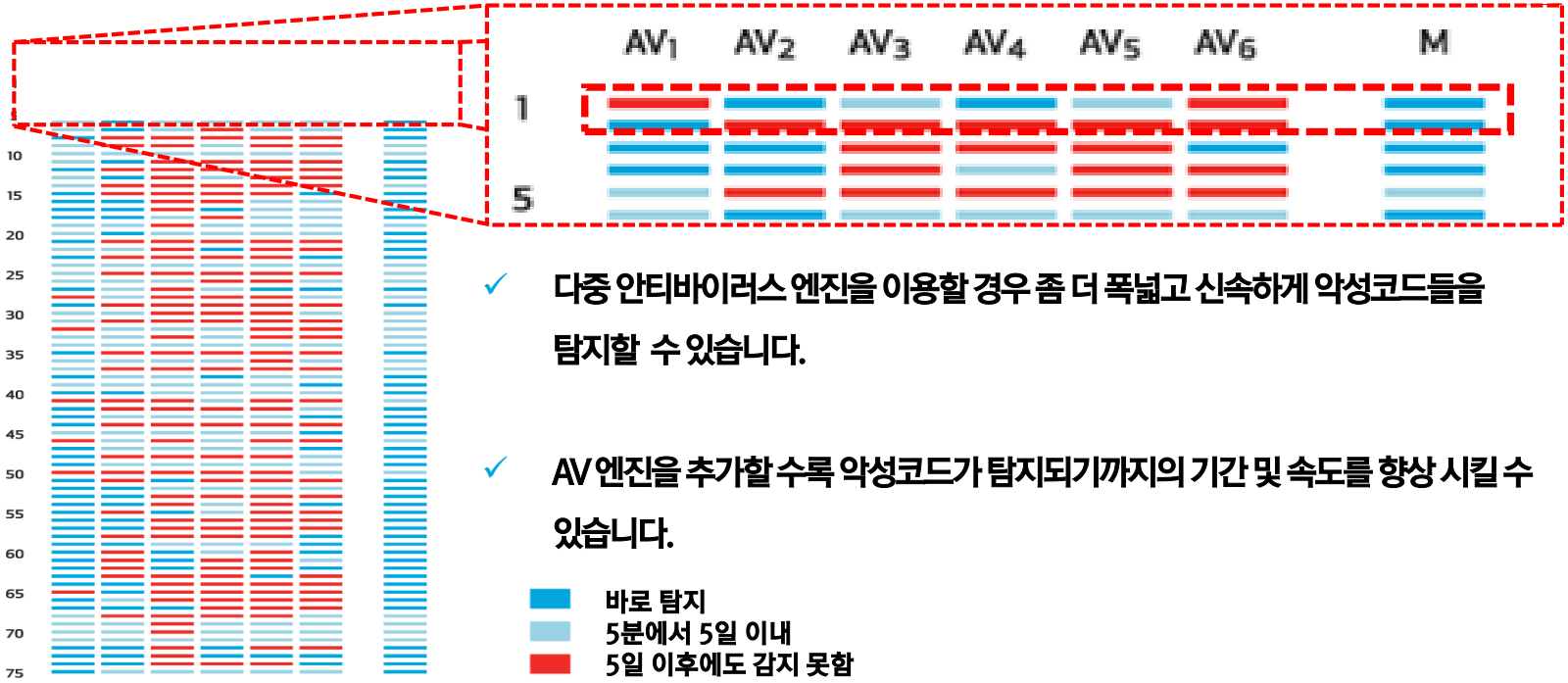
기업에
위협적인
악성코드들

약 6억 개
[600,000,000]
2017년 4월 현재

A/V
Scanner

안티바이러스
엔진

멀티스캐닝 장점



✓ 다중 안티바이러스 엔진을 이용할 경우 좀 더 폭넓고 신속하게 악성코드들을 탐지할 수 있습니다.

✓ AV 엔진을 추가할 수록 악성코드가 탐지되기까지의 기간 및 속도를 향상 시킬 수 있습니다.

바로 탐지
5분에서 5일 이내
5일 이후에도 감지 못함

멀티스캐닝 장점

SHARE THESE RESULTS:

xwU6h1MX.exe=

Rescan | Scan new file

First uploaded	2017-02-25 05:46:44 GMT
Last scanned	2017-02-25 05:46:45 GMT
Filetype	Win32 Executable MS Visual C++ (generic)
File size	238 KB
MD5	D6A6AECA00C684FCDD7B292AA39F5339
SHA1	8F6AA8A6CA6580CBED9AA1CDF4DBD46602EA885B
SHA256	5B07C04DE17A4D91C0037F551BBB760F25F409DFDCC037446DE880C5A5CE8CB8

MULTISCANNING | PE INFO | APPLICATIONS LIST | NETWORK CONNECTIONS | LOADED COMPONENTS

KNOWN VULNERABILITIES | FILE NAMES | SCAN HISTORY

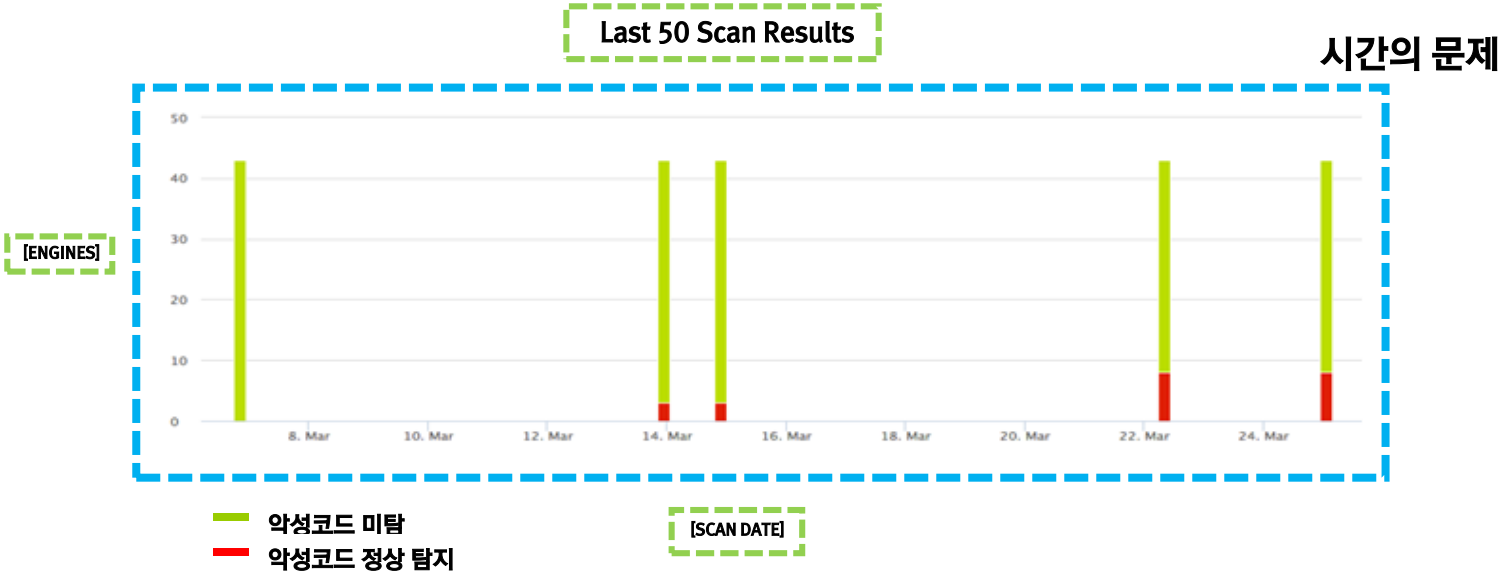
We leverage both signature and heuristic scanning from up to 30 scan engines on-premises and more than 40 scan engines in the cloud to increase malware detection rates. Please contact our sales team to have a deeper discussion about Metadefender Core, the packages and deployments options.

ENGINE	SCAN TIME	LAST UPDATED	RESULT
Agnitum	375 ms	Feb 22 2017 (5 days ago)	Trojan.SageCrypt! ✖
Ahnlab	406 ms	Feb 24 2017 (3 days ago)	Trojan/Win32.SageCrypt ✖
AVG	578 ms	Feb 24 2017 (3 days ago)	Ransom_r.BOB ✖
Avira	625 ms	Feb 24 2017 (3 days ago)	TR/AD.Cerber.sgmbb ✖


OPSWAT
Metadefender
CORE
Welcome
Dashboard
Configuration
Sources
Quarantine
Logs
Licenses
Documentation
Email
Last 12 hours
4
PROCESSED FILES
0
DETECTED THREATS
0.03
AVERAGE TIME
Files and Infections
Clients
IP ADDRESS
FILES PROCE
fe80::9881
192.168.0
Mail Agent
EMAIL
INFECTIONS
ATTACHM
SCANNED
Generic on
INSEC-PC
0
1
40 %
20 %
0 %
RAM
CPU
DISK

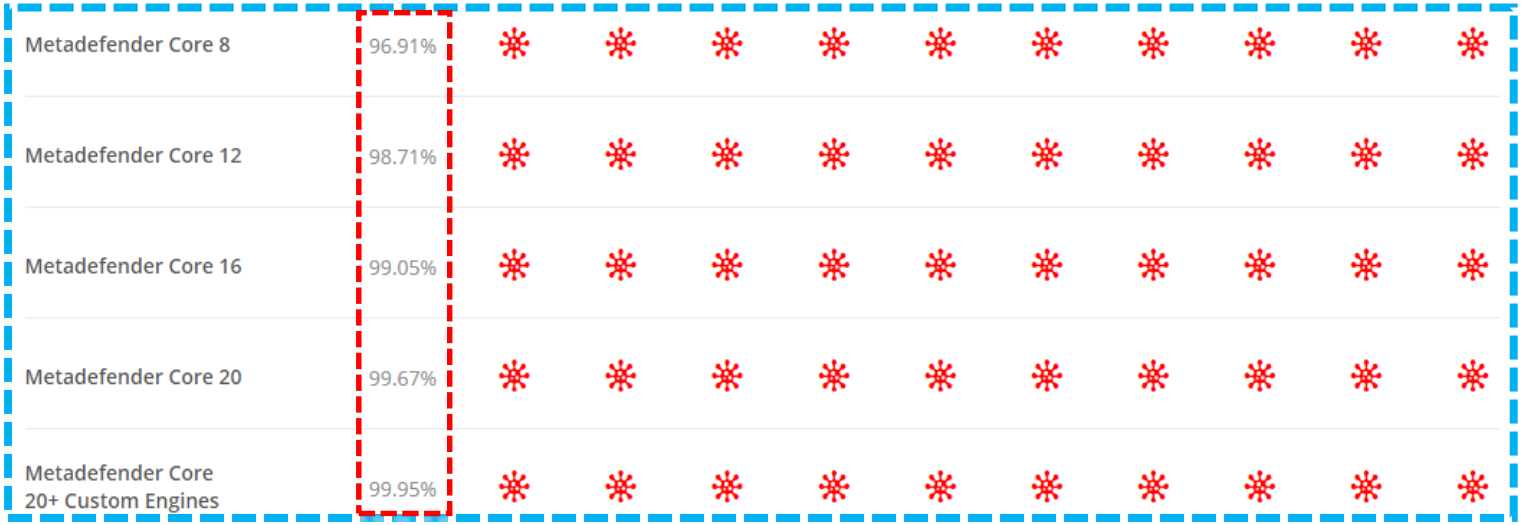
알려지지 않은 위협

알려지지 않은 위협



- ✓ 분석이 필요하며, 백신에 탐지 되지 않는 위협들
- ✓ 일부 엔진은 학습하는데 시간이 오래 걸림

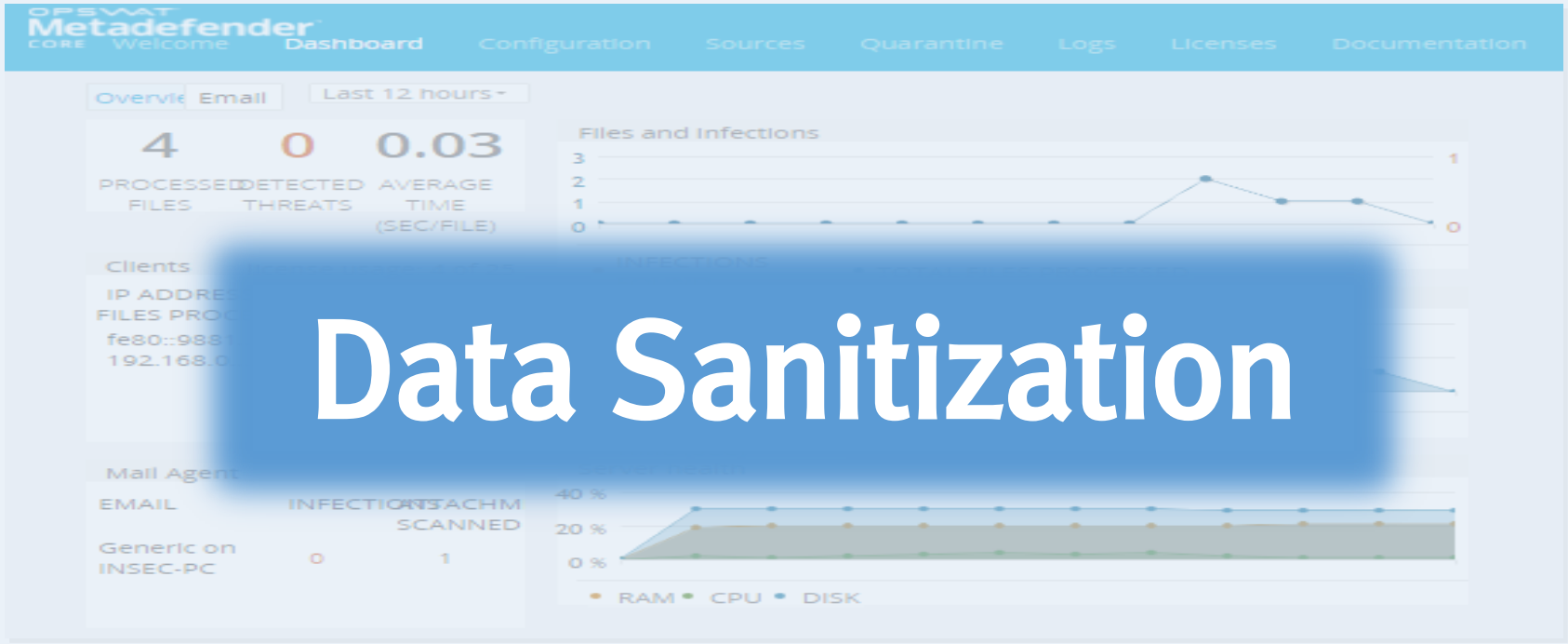
알려지지 않은 위협



(위 탐지율은 2017년 3월 2일부터 2017년 4월 1일까지 www.metadefender.com 에서 수집된 TOP 악성코드를 사용하여 계산되었습니다.)

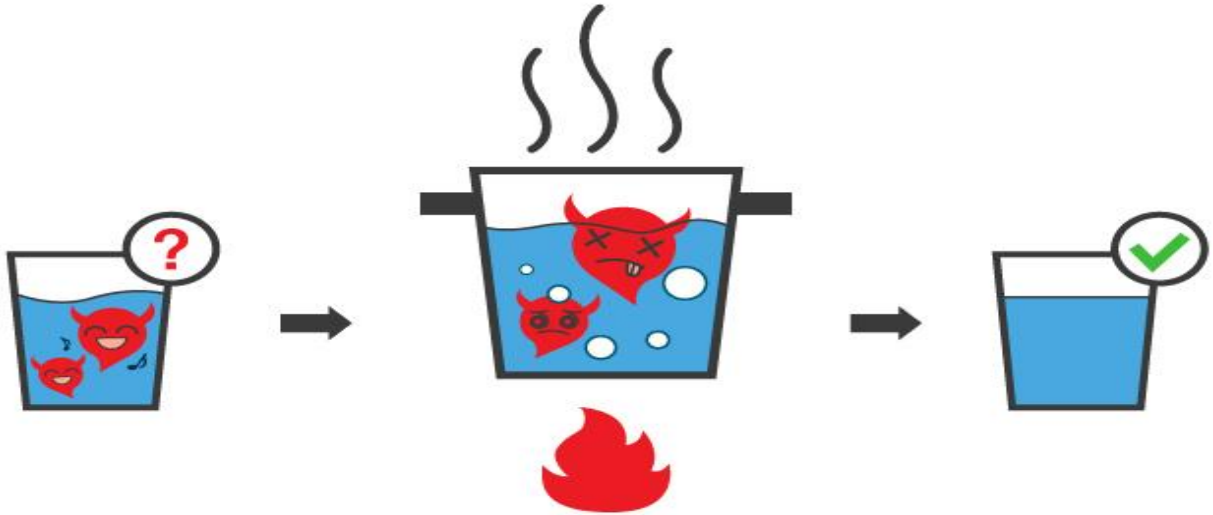
- ✓ 적은 엔진일 수록 알려지지 않은 위협들이 더 존재함
- ✓ 20 엔진을 가지고도 알려지지 않은 위협

100% – 99.67% = 0.33%



Data Sanitization

데이터 살균



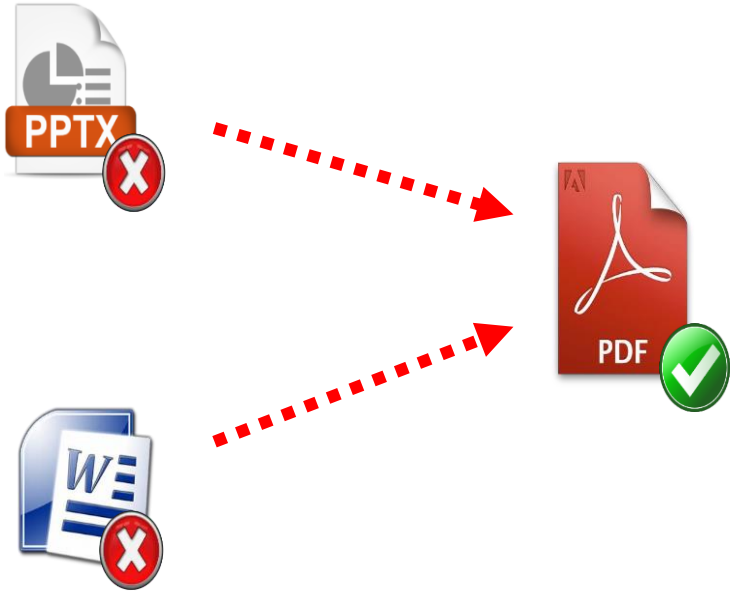
✓ 물(데이터)을 끓여(살균,sanitization) 잠재적 위협인 세균(위협가능성)을 제거하는 기술

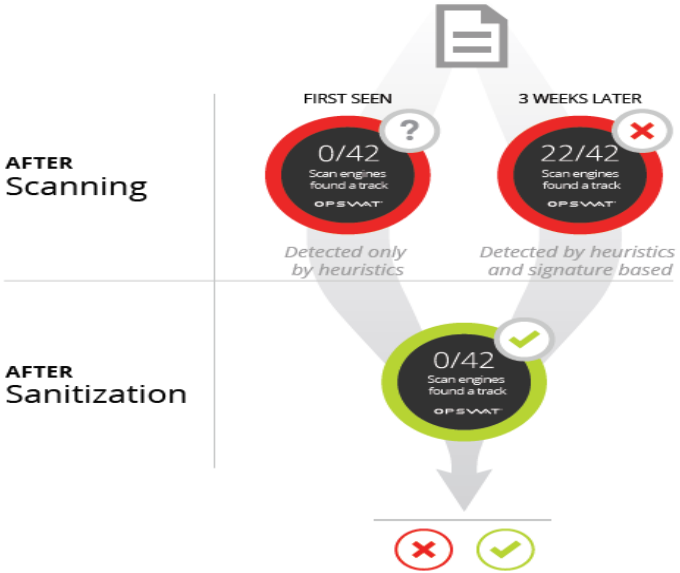
데이터 살균

✓ 악성코드가 실려지거나 공격코드가 실행되는 위협 요소를 사전에 제거.

✓ 안전한 콘텐츠만 파일 형식 변환을 통해 제공.

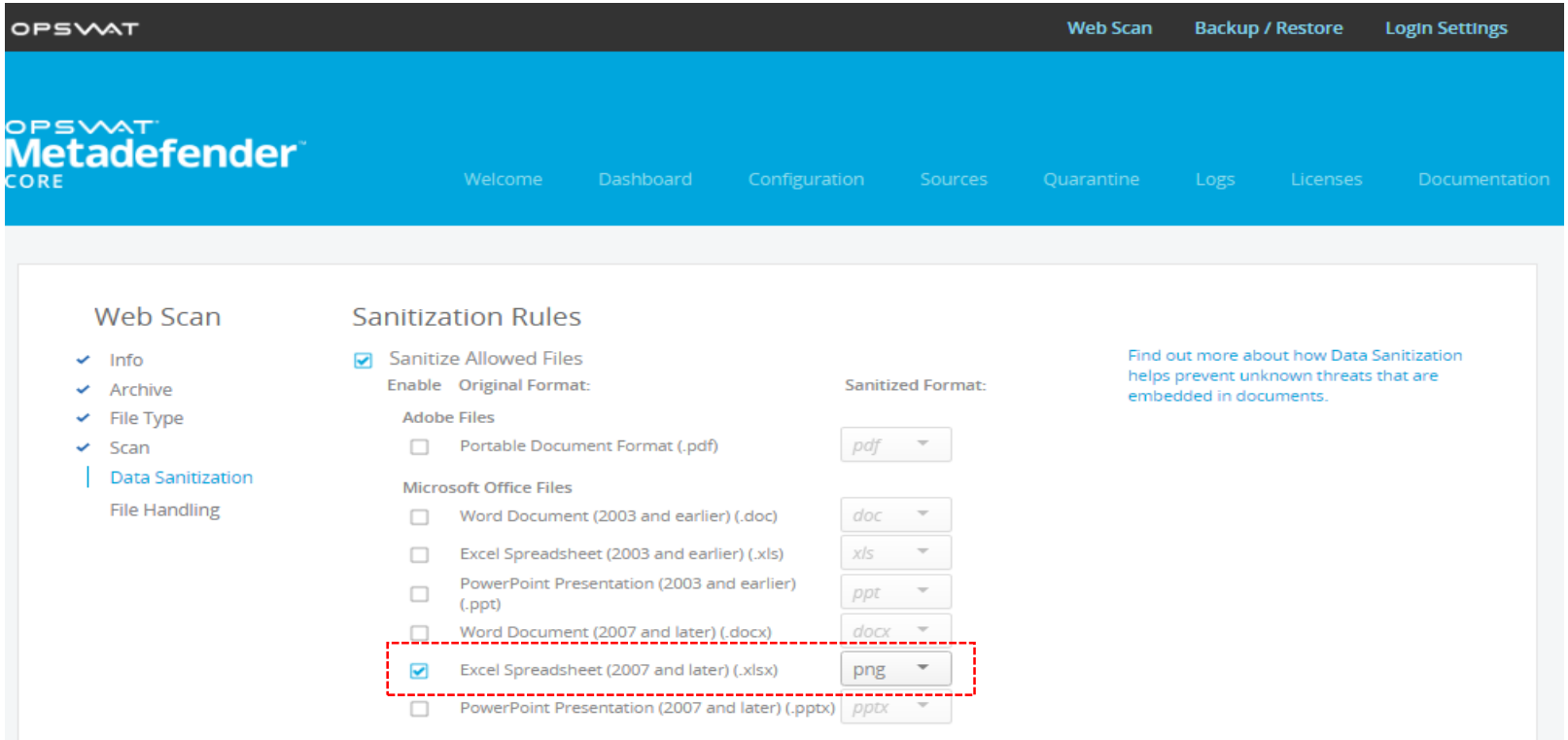
데이터 살균





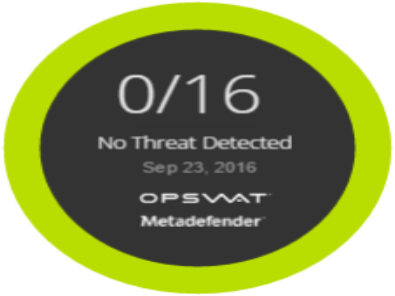
- ✓ 파일 형식(File Type) 변환
- ✓ 파일 형식을 다른 안전한 파일 형식으로 변환

데이터 살균


OPSWAT
Web Scan
Backup / Restore
Login Settings
OPSWAT
Metadefender
CORE
Welcome
Dashboard
Configuration
Sources
Quarantine
Logs
Licenses
Documentation
Web Scan
Info
Archive
File Type
Scan
Data Sanitization
File Handling
Sanitization Rules
Sanitize Allowed Files
Enable
Original Format:
Sanitized Format:
Adobe Files
Portable Document Format (.pdf)
pdf
Microsoft Office Files
Word Document (2003 and earlier) (.doc)
doc
Excel Spreadsheet (2003 and earlier) (.xls)
xls
PowerPoint Presentation (2003 and earlier) (.ppt)
ppt
Word Document (2007 and later) (.docx)
docx
Excel Spreadsheet (2007 and later) (.xlsx)
png
PowerPoint Presentation (2007 and later) (.pptx)
pptx
Find out more about how Data Sanitization helps prevent unknown threats that are embedded in documents.

데이터 살균

EXTRACTED FILES | ORIGINAL FILE



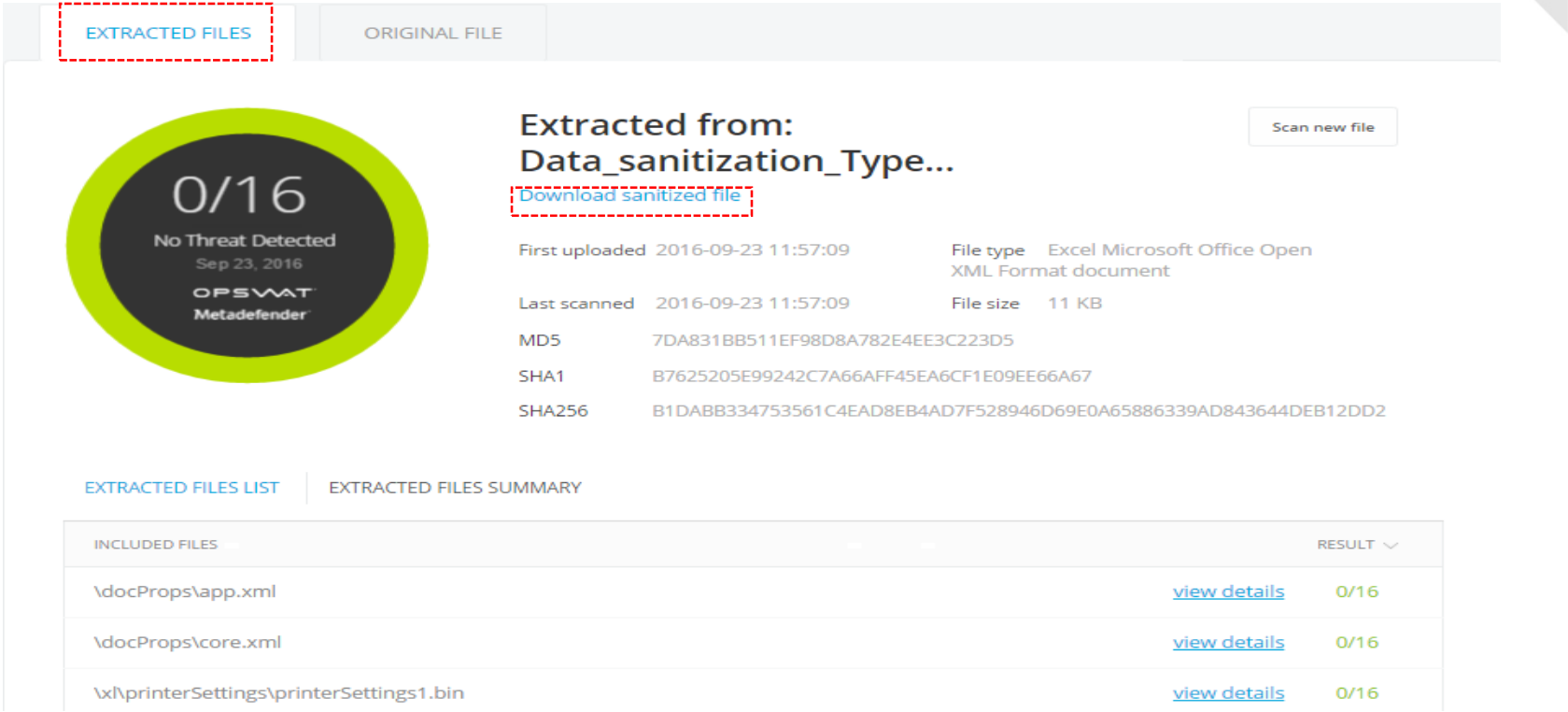
Data_sanitization_Type...

Scan new file

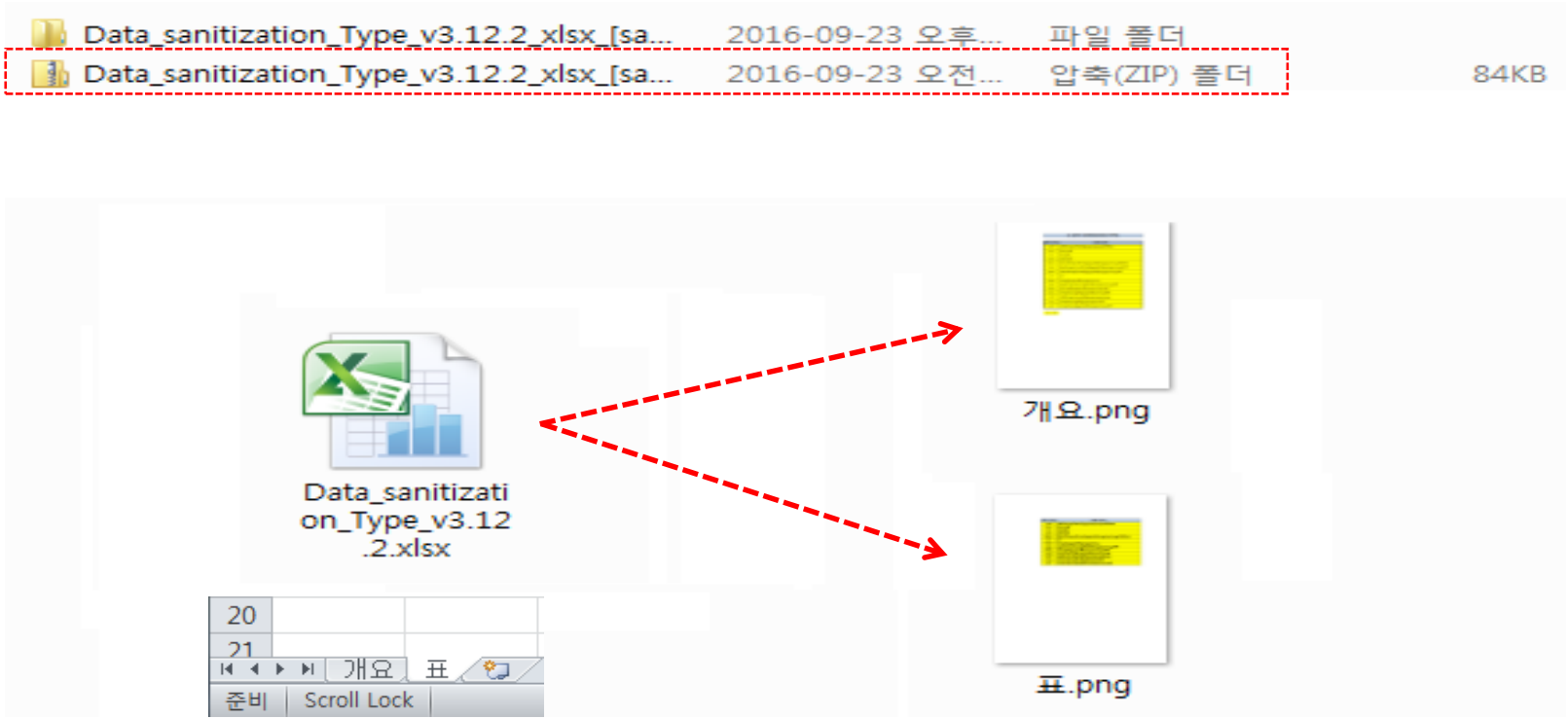
First uploaded 2016-09-23 11:57:09
File type Excel Microsoft Office Open XML Format document
Last scanned 2016-09-23 11:57:09
File size 11 KB
MD5 7DA831BB511EF98D8A782E4EE3C223D5
SHA1 B7625205E99242C7A66AFF45EA6CF1E09EE66A67
SHA256 B1DABB334753561C4EAD8EB4AD7F528946D69E0A65886339AD843644DEB12DD2

ENGINE	SCAN TIME	DEFINITION DATE	RESULT
F-prot	16 ms	2016-09-21	✓
Zillya!	1 ms	2016-09-22	✓
TotalDefense	16 ms	2016-09-20	✓
QuickHeal	16 ms	2016-09-21	✓

데이터 살균


EXTRACTED FILES
ORIGINAL FILE
0/16
No Threat Detected
Sep 23, 2016
OPSWAT
Metadefender
Extracted from:
Data_sanitization_Type...
Scan new file
Download sanitized file
First uploaded 2016-09-23 11:57:09
File type Excel Microsoft Office Open XML Format document
Last scanned 2016-09-23 11:57:09
File size 11 KB
MD5 7DA831BB511EF98D8A782E4EE3C223D5
SHA1 B7625205E99242C7A66AFF45EA6CF1E09EE66A67
SHA256 B1DABB334753561C4EAD8EB4AD7F528946D69E0A65886339AD843644DEB12DD2
EXTRACTED FILES LIST
EXTRACTED FILES SUMMARY
INCLUDED FILES
RESULT
\docProps\app.xml
view details
0/16
\docProps\core.xml
view details
0/16
\xl\printerSettings\printerSettings1.bin
view details
0/16

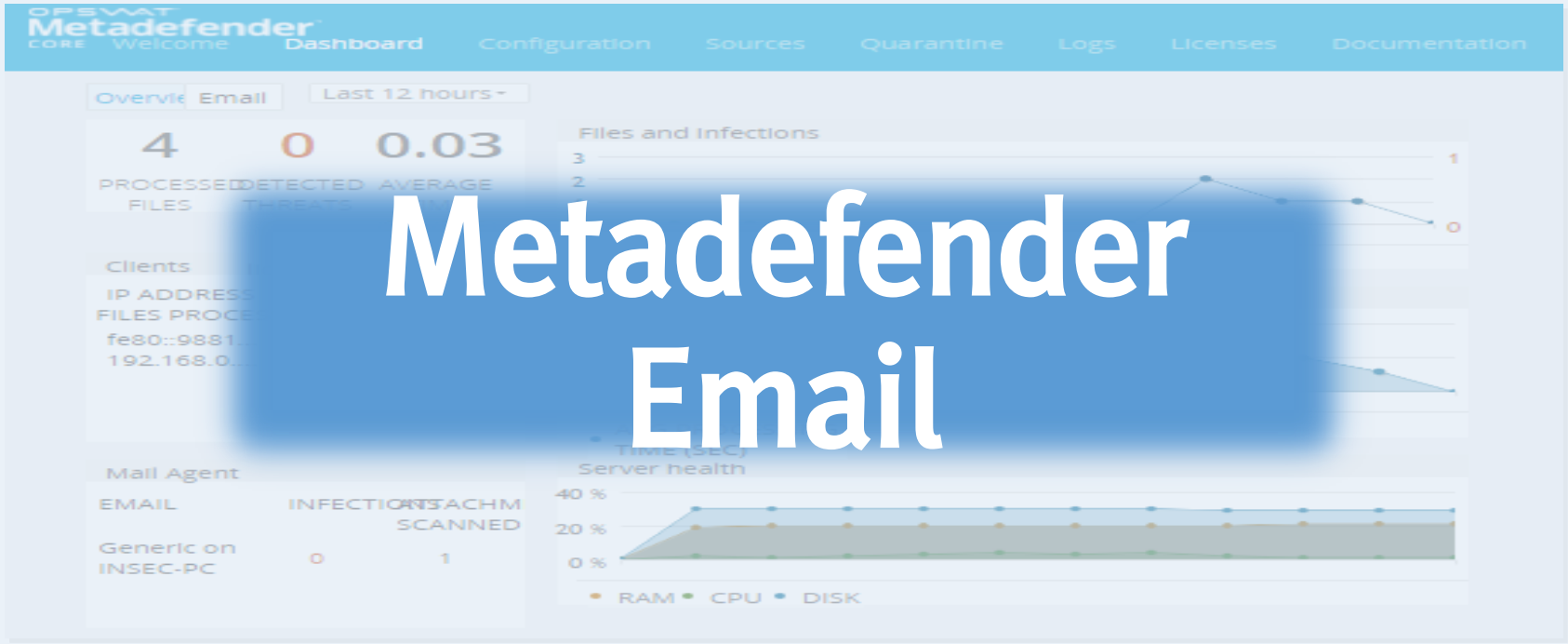
데이터 살균


Data_sanitization_Type_v3.12.2_xlsx_[sa... 2016-09-23 오후... 파일 폴더
Data_sanitization_Type_v3.12.2_xlsx_[sa... 2016-09-23 오전... 압축(ZIP) 폴더 84KB
Data_sanitization_Type_v3.12.2.xlsx
개요.png
표.png
20
21
개요
표
준비
Scroll Lock

데이터 살균

원본 형식	변환 형식
pdf	pdf/bmp/html/jpg/png/svg/tiff/txt
doc	doc/pdf
xls	xls/pdf
ppt	ppt/pdf
docx	docx/bmp/html/jpg/pdf/png/ps/svg/tiff/txt
xlsx	xlsx/bmp/csv/html/jpg/pdf/png/ps/svg/tiff
pptx	pptx/bmp/html/jpg/pdf/png/ps/svg/tiff
rtf	rtf
jtd	jtd
hwp	hwp
html	html/bmp/jpg/pdf/png/ps/svg
jpg	jpg/bmp/eps/gif/pdf/png/ps/svg/tiff
bmp	bmp/eps/gif/jpg/pdf/png/ps/svg/tiff
png	png/bmp/eps/gif/jpg/pdf/ps/svg/tiff
tiff	tiff/bmp/eps/gif/jpg/png/ps/svg
svg	bmp/eps/gif/jpg/png/ps/tiff
gif	bmp/eps/jpg/pdf/png/ps/svg/tiff

- ✓ 여러 파일 형식을 지원 (17 → 102개)
- ✓ 문서 파일 뿐 아니라 이미지 파일 형식까지도 지원


OPSWAT
Metadefender
CORE
Welcome
Dashboard
Configuration
Sources
Quarantine
Logs
Licenses
Documentation
Email
Last 12 hours
4
PROCESSED FILES
0
DETECTED THREATS
0.03
AVERAGE
Files and Infections
Clients
IP ADDRESS
FILES PROCE
fe80::9881
192.168.0
Mail Agent
EMAIL
INFECTIONS
SCANNED
Generic on INSEC-PC
0
1
Server health
40 %
20 %
0 %
RAM
CPU
DISK
Metadefender
Email

Metadefender Email

Multi-scanning

높은 악성코드 탐지율 제공

over 30+ anti-malware engines

AhnLab, eset, SOPHOS, McAfee, Symantec, Bitdefender, Quick Heal, nProtect, AVG, CYREN, Zillya!, KASPERSKY, LAVASOFT, TREND MICRO, TOTAL DEFENSE, IKARUS, Avira, F-PROT, AND MORE...

Data Sanitization

데이터 살균 [**파일에 삽입된 악성코드 제거**]

100+ data sanitization

PDF, DOC, DOCX, XLS, XLSX, PPT, PPTX, RTF, HTML, JPEG, BMP, PNG, RIFF, SVG, GIF

Metadefender Email

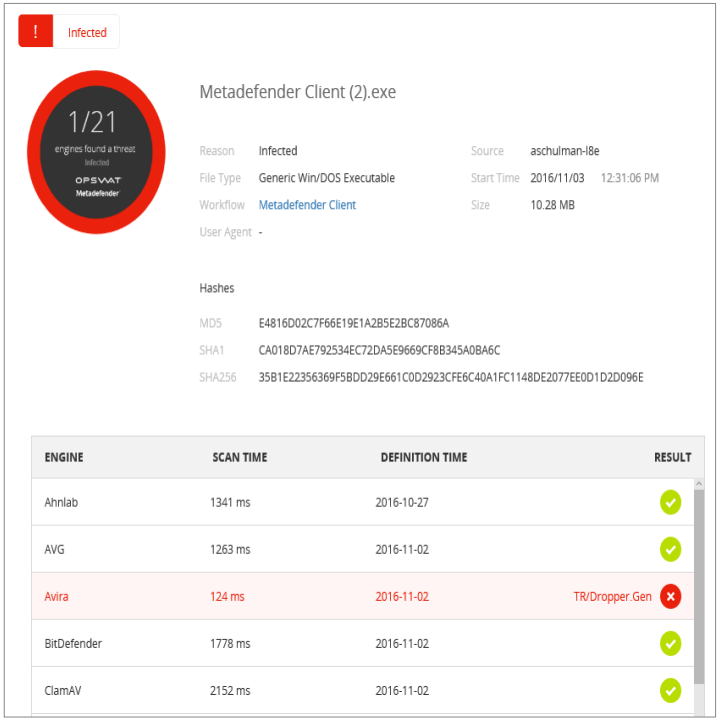
Metadefender Core notification: Email infected

AS aschulman@opswat.com

To: www@caffeine.andymillar.co.uk; Demo DU. User;

Metadefender Core has detected an infection in the following email:

Date : 11/08/2016 01:33:09
From : "Apache, andymillar.co.uk" <andy@andymillar.co.uk>
To : "demouser@napswitch.com" <demouser@napswitch.com>
Subject: EICAR Virus Test Email
Result : EICAR_Test_File

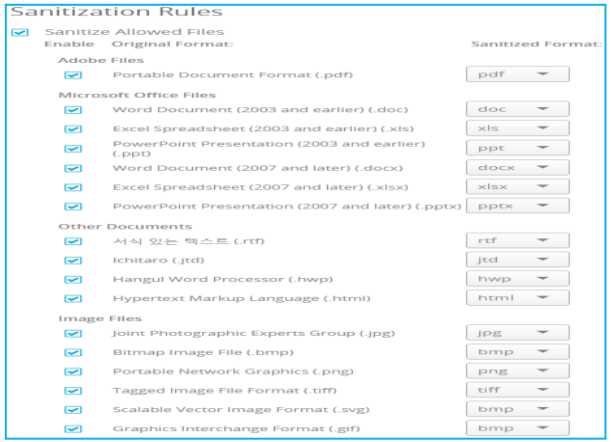


Metadefender Email

문서 파일 기반의
악성코드 위협 증가

문서파일 내 잠재된 위협 제거 (
e.g. scripts and macros)

문서 재구성



Unknown Malware
Ransomeware 차단

17종류 원본형식을 100개 이상의 변환형식으로 변경 (.hwp 지원)

Metadefender Email

proofpoint

Email Protection

CISCO

Email Security Appliance

FireEye

Ex Series

FORCEPOINT

POWERED BY Raytheon

Triton AP-Email

Symantec

Messaging Gateway

Barracuda

Email Security Gateway

SOPHOS

Email Appliance

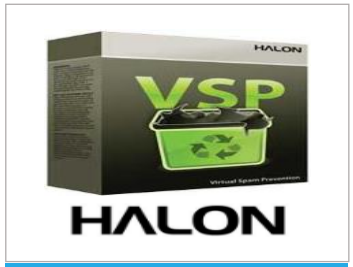
clearswift

Secure Email Gateway

Metadefender Email

Terrace Mail Suite

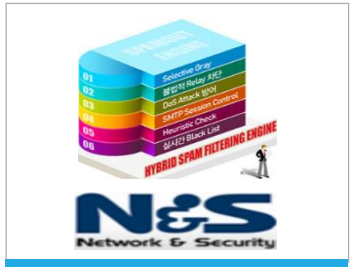
Spam Email Gateway



Spam Email Gateway

Secure Email Gateway

McAfee Email Gateway



Spam Email Gateway

Spam Email Gateway

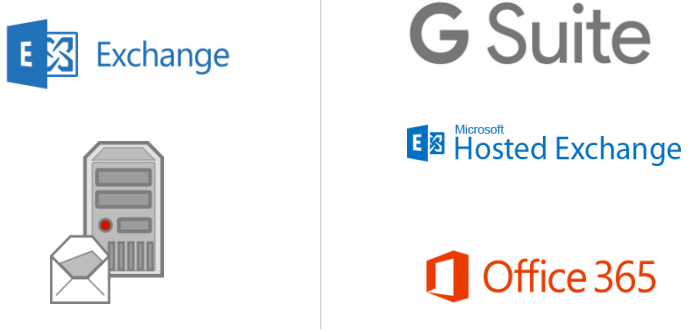
Secure Email Gateway

Metadefender Email

Brand	Product
Proofpoint	Email Protection
Cisco	Email Security Appliance
FireEye	EX Series
Microsoft	Exchange Online Protection
Symantec	Messaging Gateway
Intel Security	McAfee Email Gateway
Trend Micro	InterScan Messaging Security
Mimecast	Secure Email Gateway
Forcepoint	TRITON AP-EMAIL
BAE Systems	Email Security (AV/AS)
Barracude Networks	Email Security Gateway
SOPHOS	Email Appliance
Clearswift	SECURE Email Gateway
Fortinet	FortiMail
Dell SonicWall	Email Security Appliances
Trustwave	Secure Email Gateway
WatchGuard Technologies	Extensible Content Security (XCS)

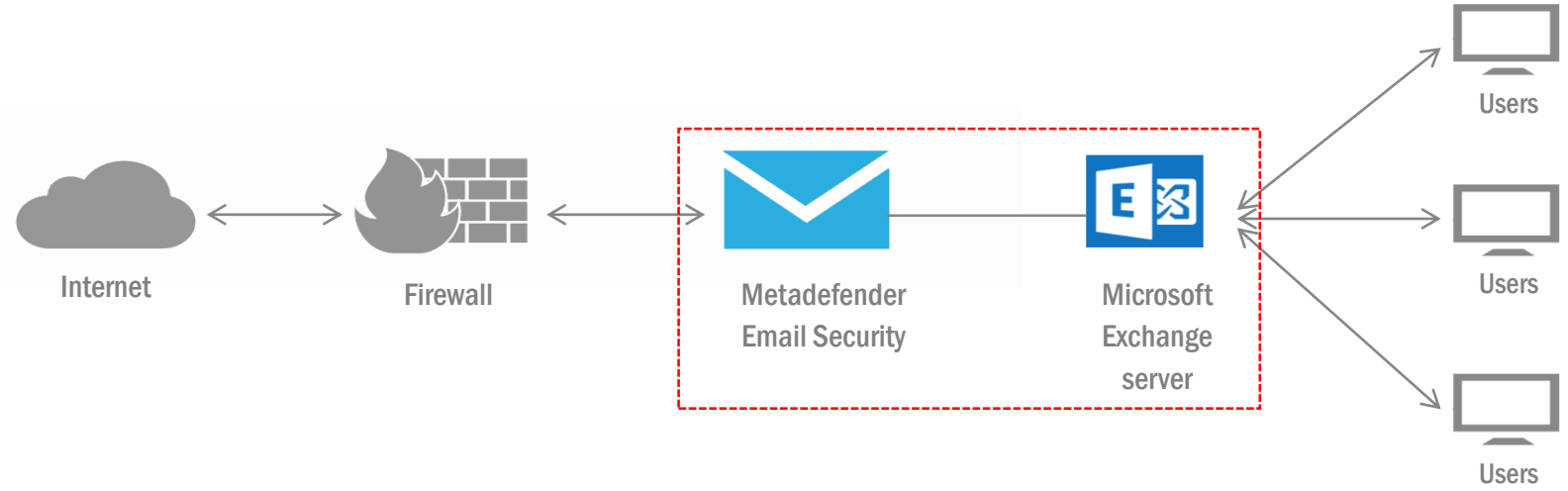
On-Premises

Cloud & Hosted

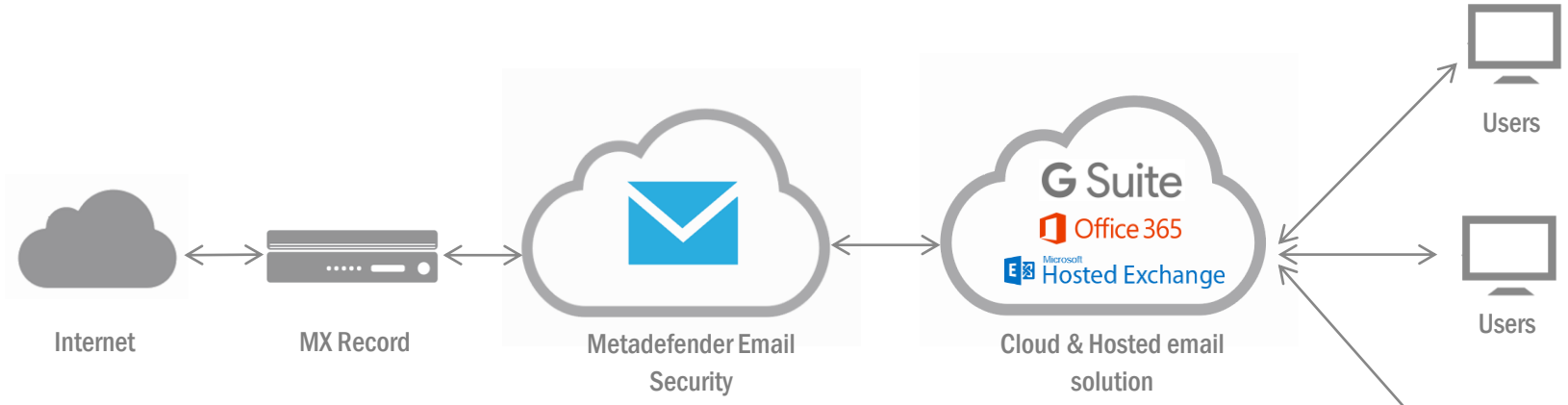


Metadefender Email

Metadefender Email

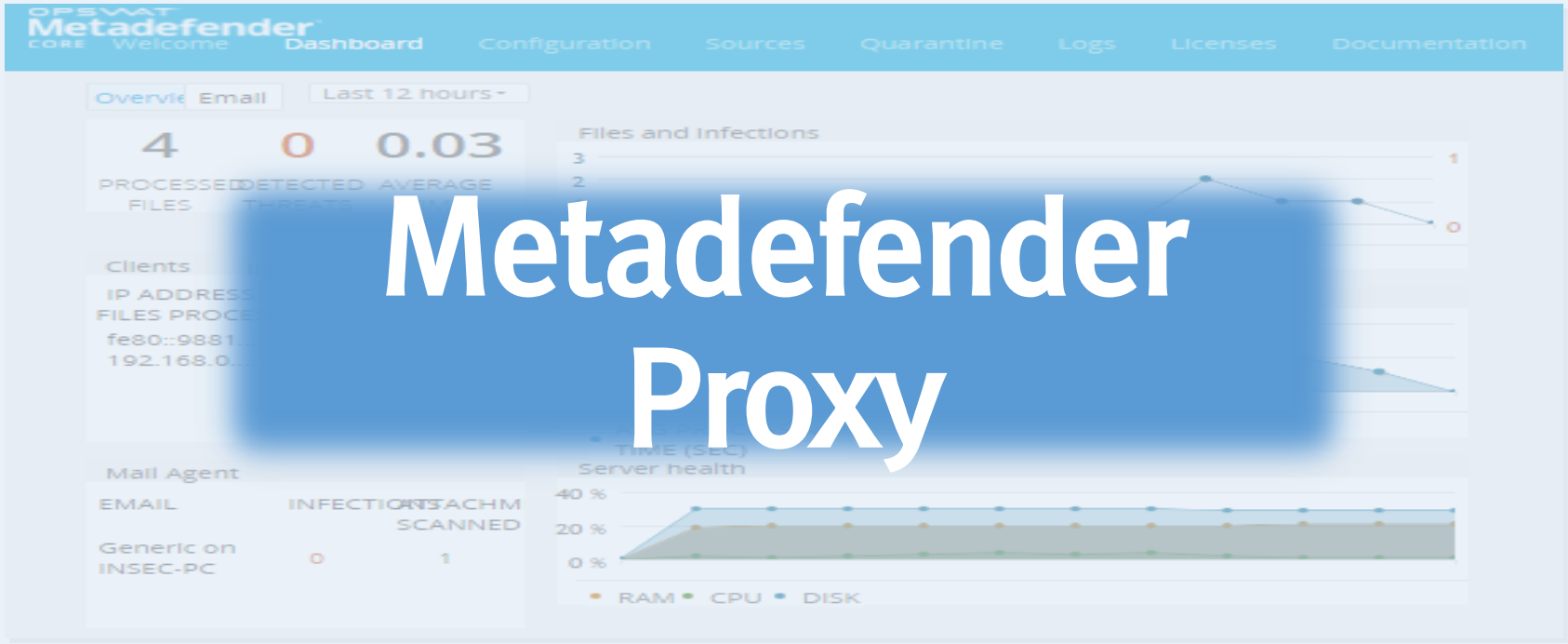


Metadefender Email



Hosting options:

- Amazon Web Services
- Your Data Center
- Hosting Service Provider



Metadefender Proxy

Metadefender Proxy

ICAP 프로토콜이란?

- ICAP(Internet Content Adaptation Protocol)

- ICAP 프로토콜은 원격에서 HTTP 메시지를 전송하여 원격 프로시저를 호출하기 위해 개발 된 프로토콜로 최근 보안 솔루션들이 웹 보안을 위해 ICAP 프로토콜을 지향하고 있음

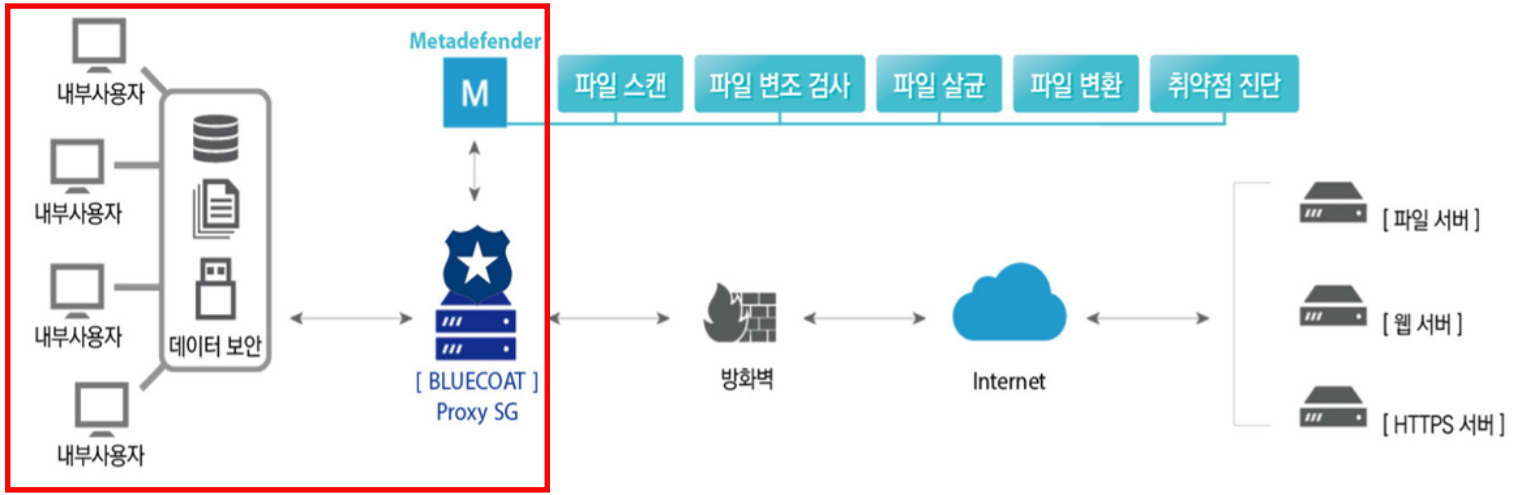
- 최근 다양한 벤더 사의 웹 프록시 제품들이 ICAP 프로토콜을 기본적으로 지원

Metadefender Proxy

- **웹 프록시 연동** : 웹 프록시를 이용하는 모든 사용자의 다운로드 행위를 검사하고 위협이 발견 된 다운로드를 차단하여 회사 네트워크 내 악성코드가 유입되는 것을 차단합니다.

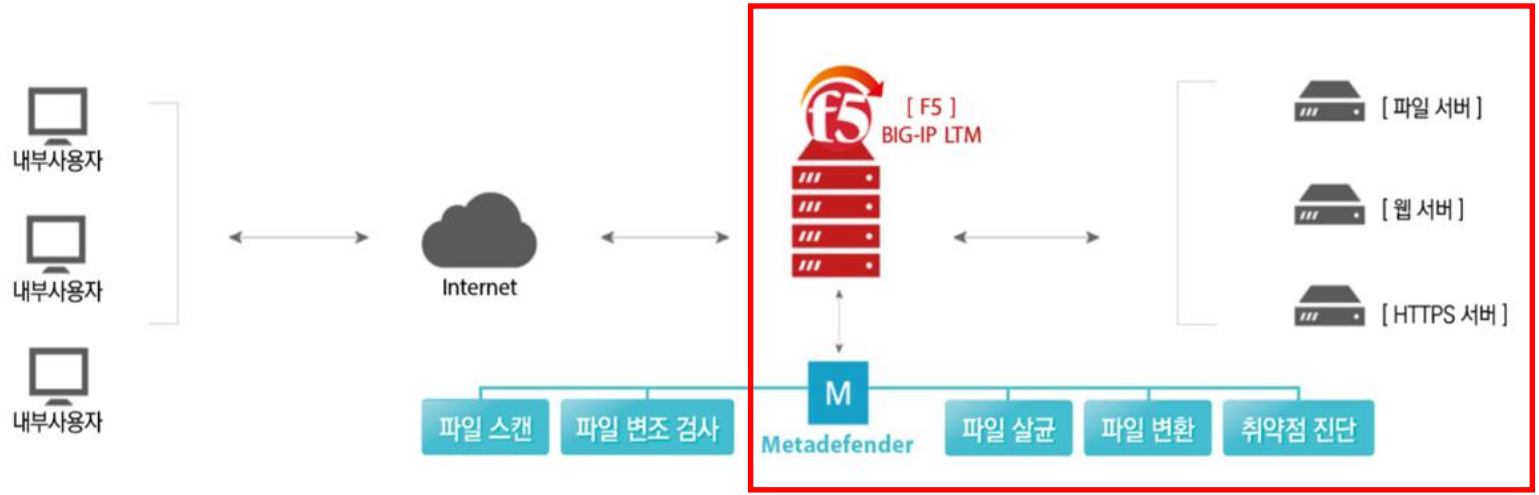
- **역방향 프록시 연동** : 악성코드가 기업 내 웹 서버에 업로드 되는 것을 차단합니다.

Metadefender Proxy



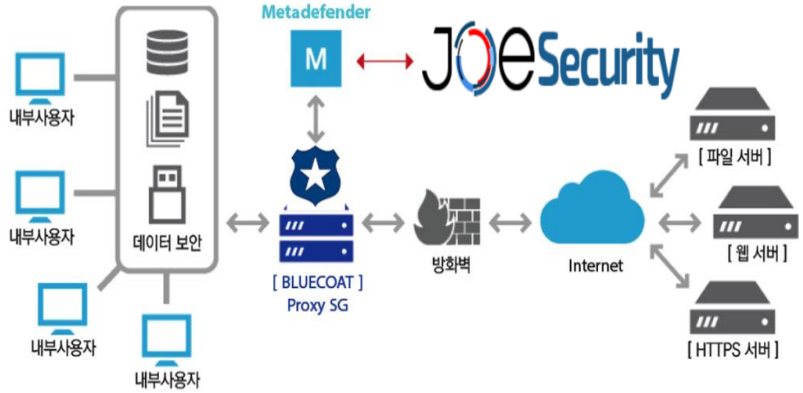
[사용자 웹 보안]

Metadefender Proxy

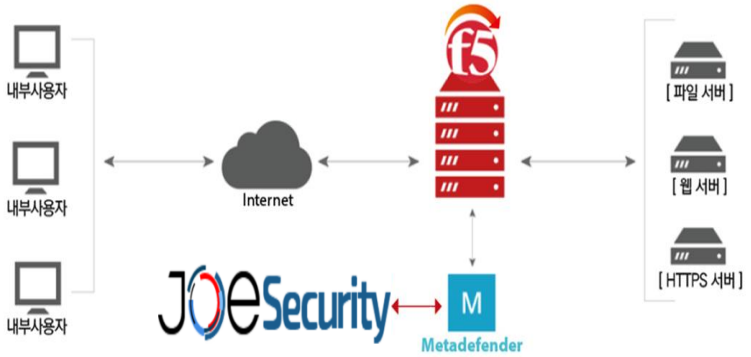


[웹 서버 보안]

Metadefender Proxy

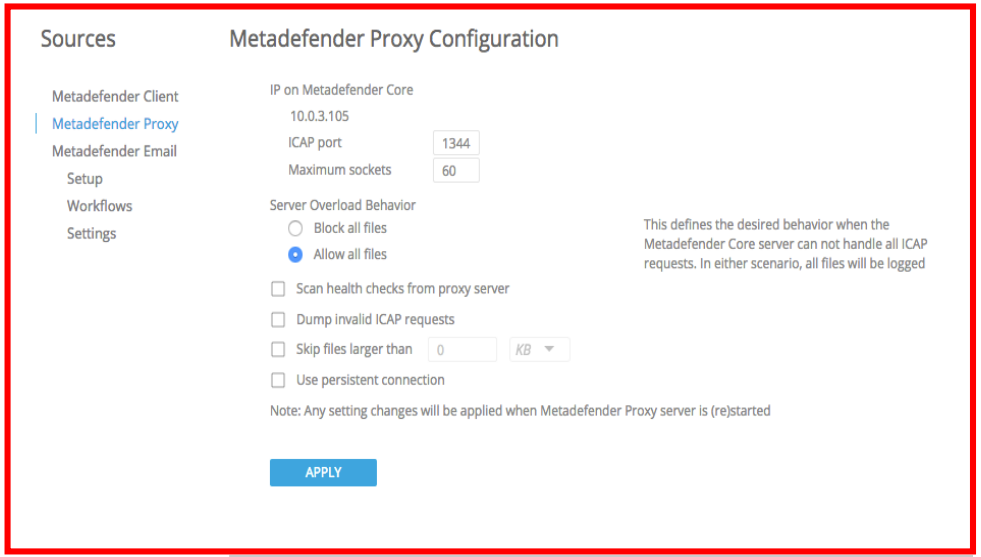


BlueCoat Proxy SG + Joe Sandbox

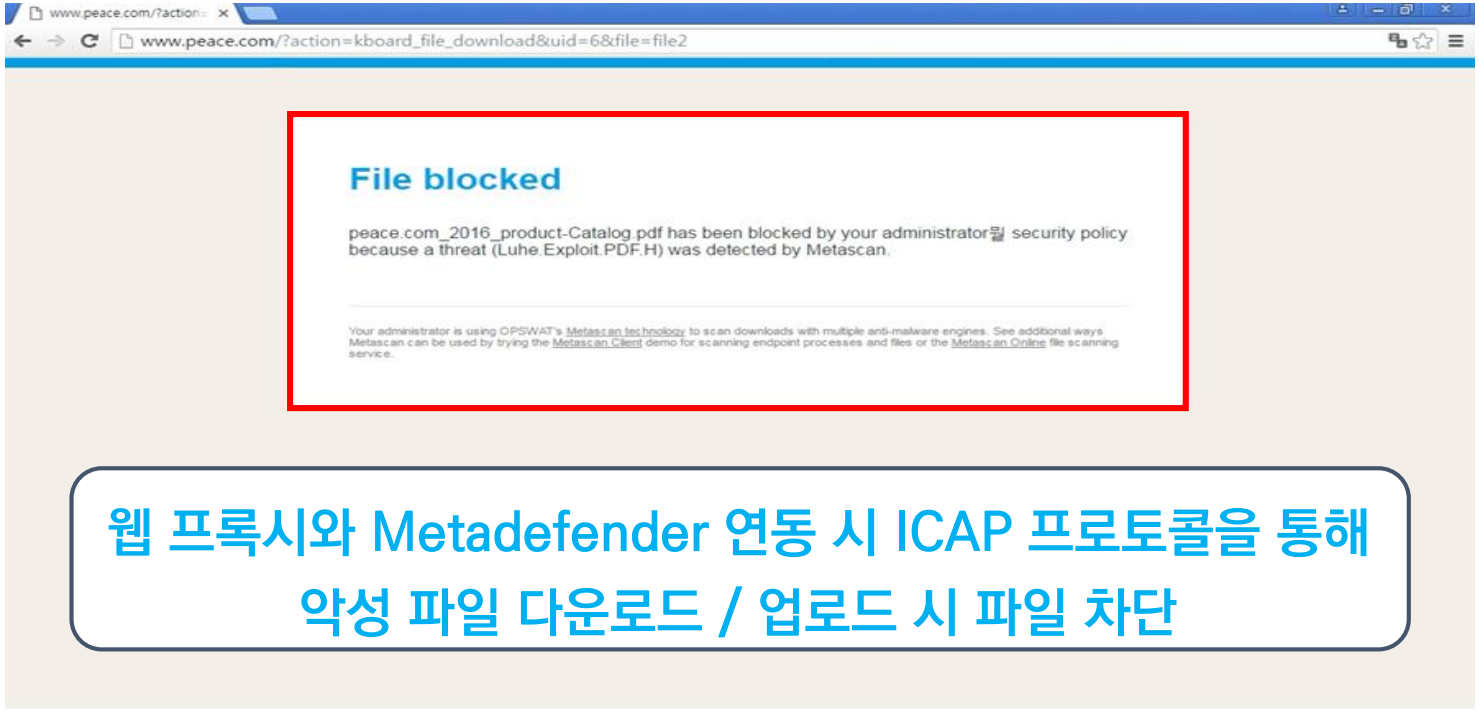


연동 F5 BIG-IP + Joe Sandbox 연동

Metadefender Proxy



Metadefender Proxy



웹 프록시와 Metadefender 연동 시 ICAP 프로토콜을 통해
악성 파일 다운로드 / 업로드 시 파일 차단

Metadefender Proxy

ICAP 프로토콜을 지원하는 웹 프록시 제품들은 전부 연동이 가능합니다

Squid Proxy

BlueCoat ProxySG

F5 BIG IP

ARA network JAGUAR5000

McAfee Web Gateway

Metadefender Kiosk

Metadefender KIOSK

▪ Metadefender Kiosk

☞ 기업 내 직원 또는 방문객의 휴대용 미디어 내에 포함된 위협을 탐지 및 식별하여 금지된 파일 차단 및 허용된 파일만 유입 되도록 통제하는 솔루션 입니다.

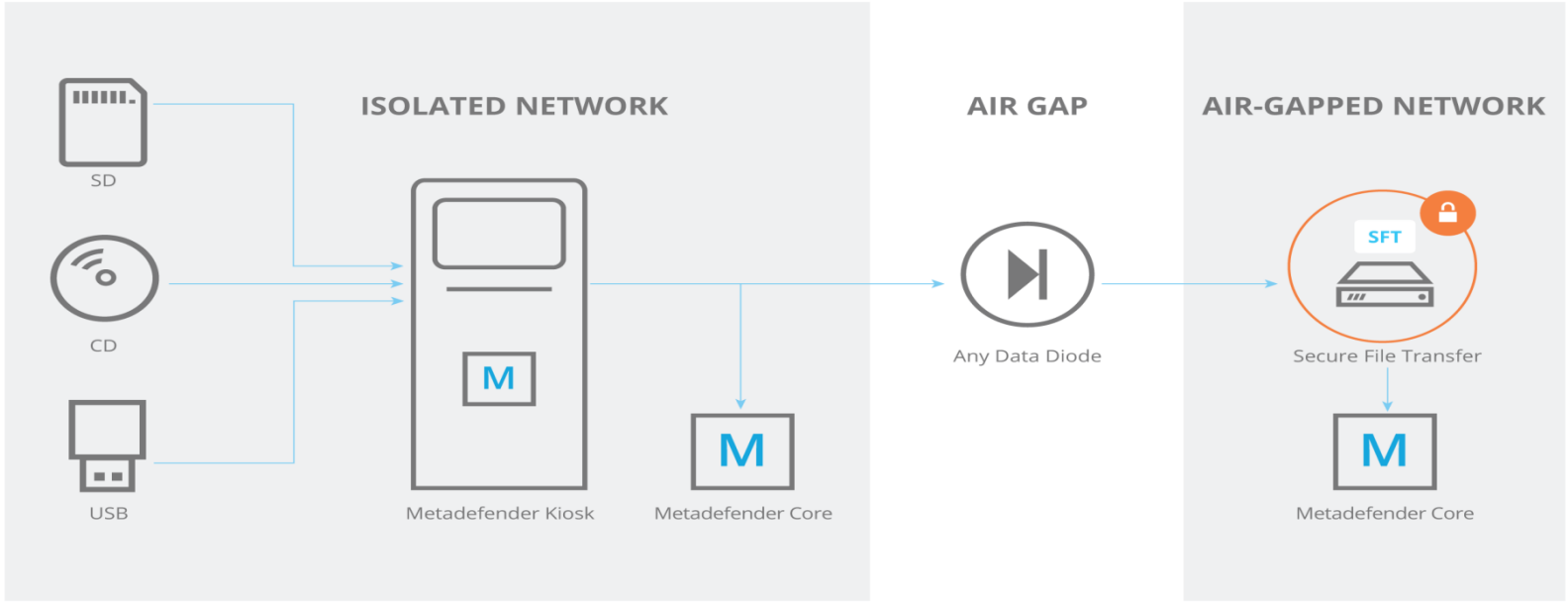
▪ 특징

☞ Metadefender Core 연동 (저장 매체 내 악성코드 검사)
☞ 데이터 살균 [Data Sanitization (CDR)]
☞ 아카이브 파일 검사
☞ 설치 파일, 업데이트 파일 설치 전 사전 스캔
☞ Data Diode와 연동 지원
☞ SFT와의 연동 지원

Metadefender Kiosk

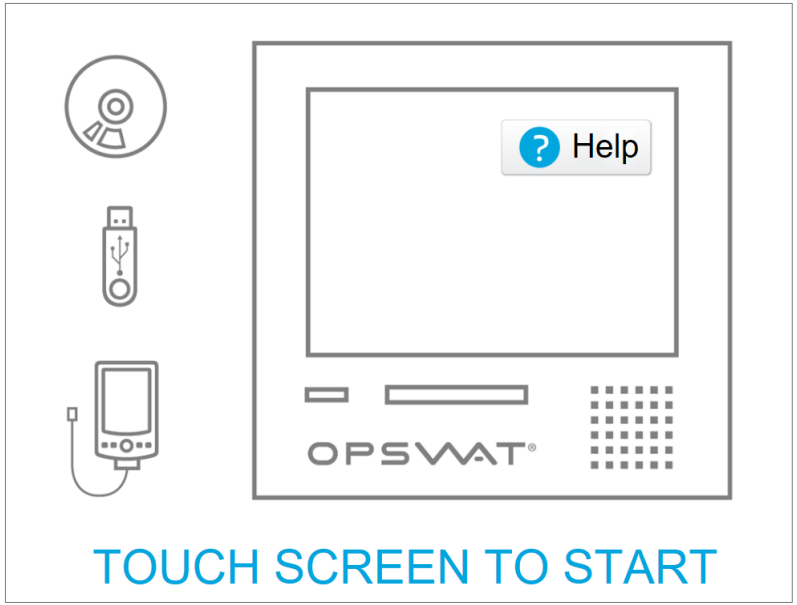
Metadefender KIOSK

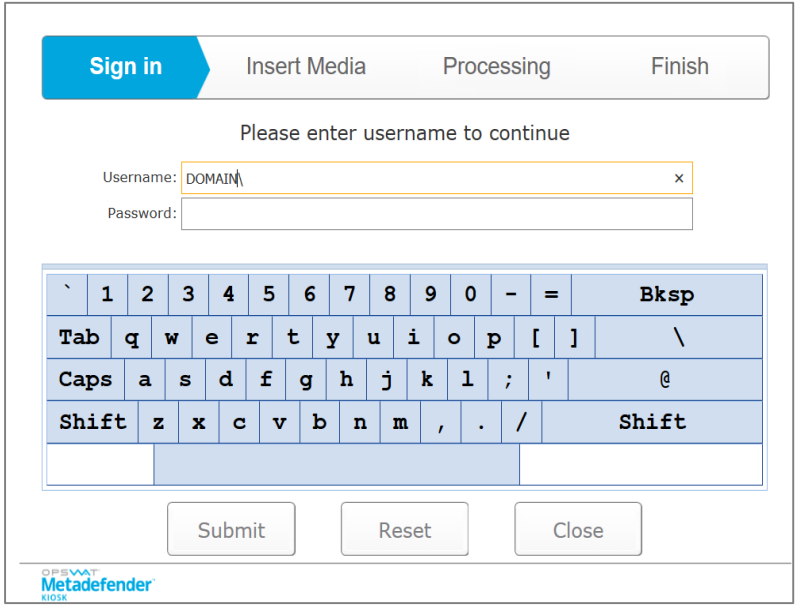
- **Metadefender Kiosk + Data Diode + SFT 통합 구성도**



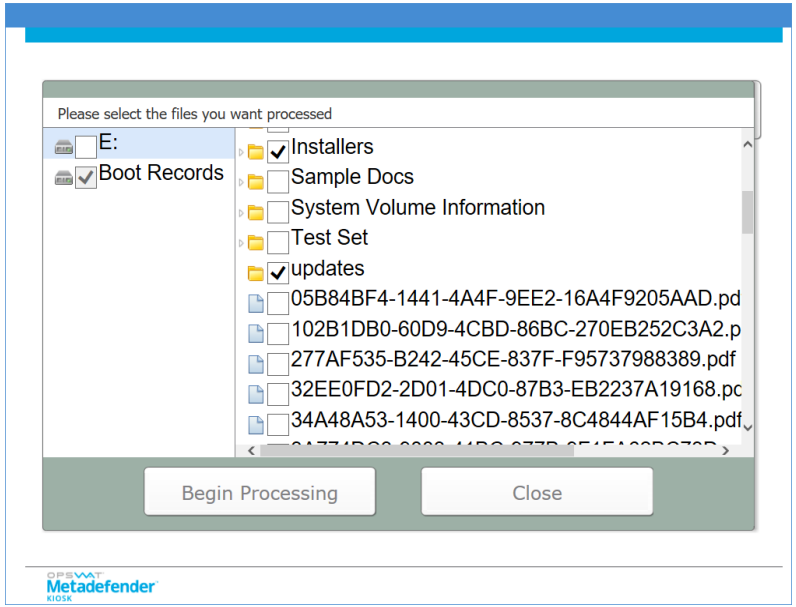
Metadefender can be located inside the isolated network as well as in the air-gapped network alongside SFT.

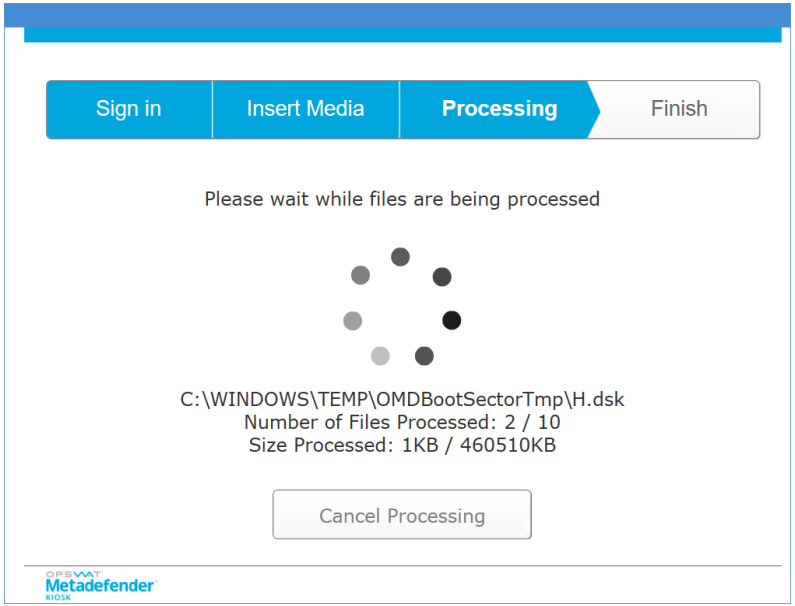
Metadefender KIOSK



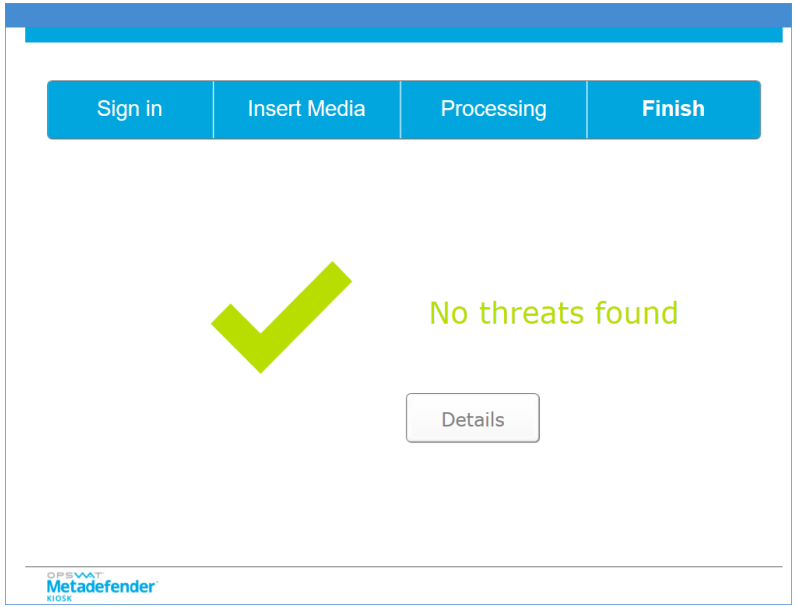


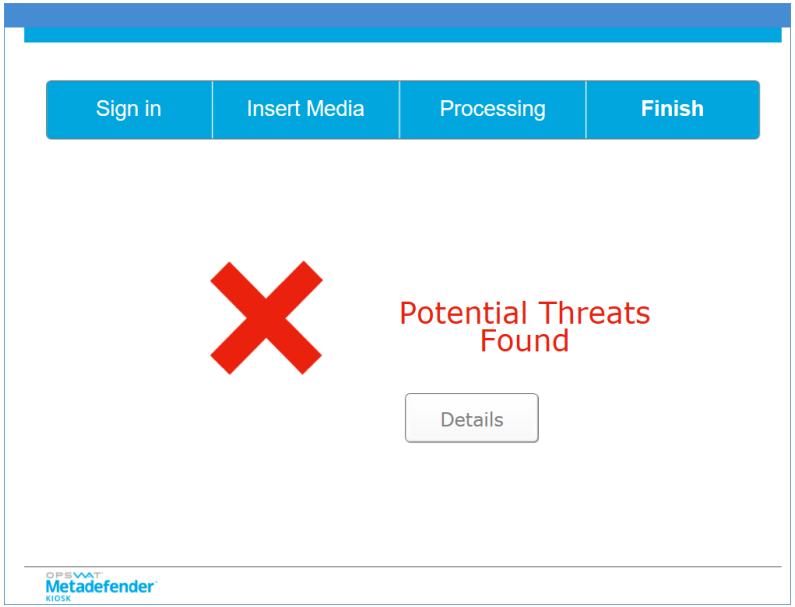
Metadefender KIOSK



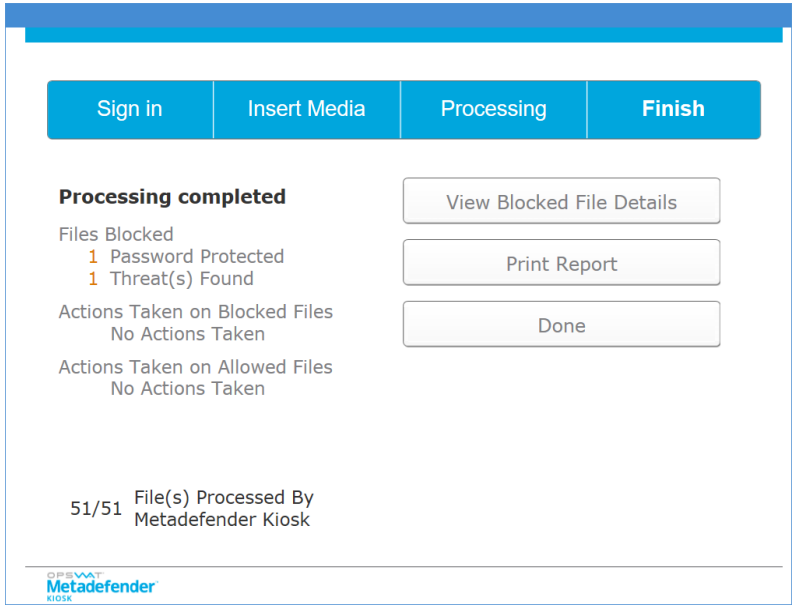


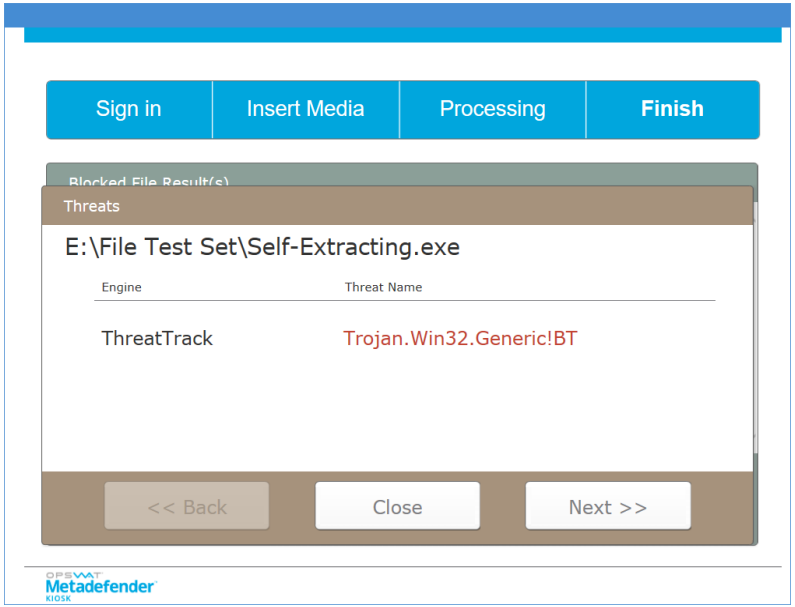
Metadefender KIOSK





Metadefender KIOSK





Metadefender KIOSK

Metadefender KIOSK

▪ Data Diode

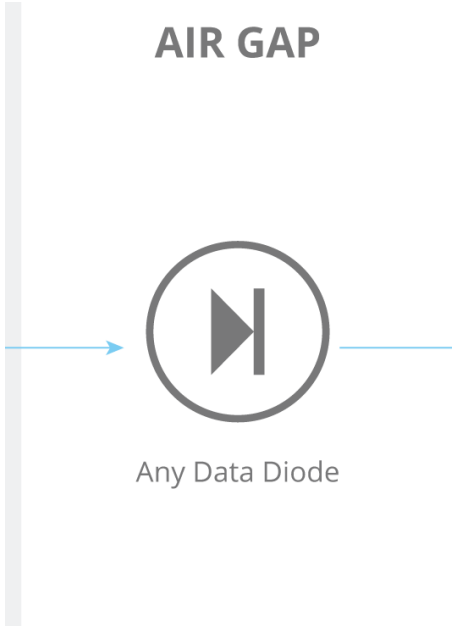
☞ Cross Domain Solution(CDS)라고도 불리는 데이터 다이오드는 낮은 보안 네트워크(예:인터넷 망)와 높은 보안 네트워크(예:내부 업무망)간에 안전한 데이터 전송을 제공하는데 사용

▪ 특징

☞ 네트워크에 단방향(Simplex) 트래픽 제공

☞ 종류에 따라 특정 신뢰할 수 있는 통신 허용

☞ 안티바이러스와 연동을 통해 전송 전 트래픽 내 악성컨텐츠 식별 가능



Metadefender KIOSK

▪ Air-Gap

☞ 공극, 공기 벽 등의 뜻을 가지며, 서로 분리된 비보안 네트워크에서 보안네트워크로 데이터를 물리적으로 이동 될 때의 간극

▪ Air-Gap + Data Diode

☞ 효율성이 낮은 Air-Gap 네트워크에서 Data Diode를 통한 효율적인 데이터 전송 지원

☞ Metadefender Core와의 연동을 통해 데이터 보안 네트워크로 전송되는 트래픽 내 악성 컨텐츠 식별

☞ OPSWAT SFT(Secure File Transfer)와의 연동 지원

Metadefender KIOSK

SFT(Secure File Transfer)

☞ Metadefender의 SFT는 보안 네트워크와 안전하게 데이터를 주고받는 일종의 Secure File Storage를 제공한다.

특징

☞ Data Diode를 통해 데이터 송신 지원

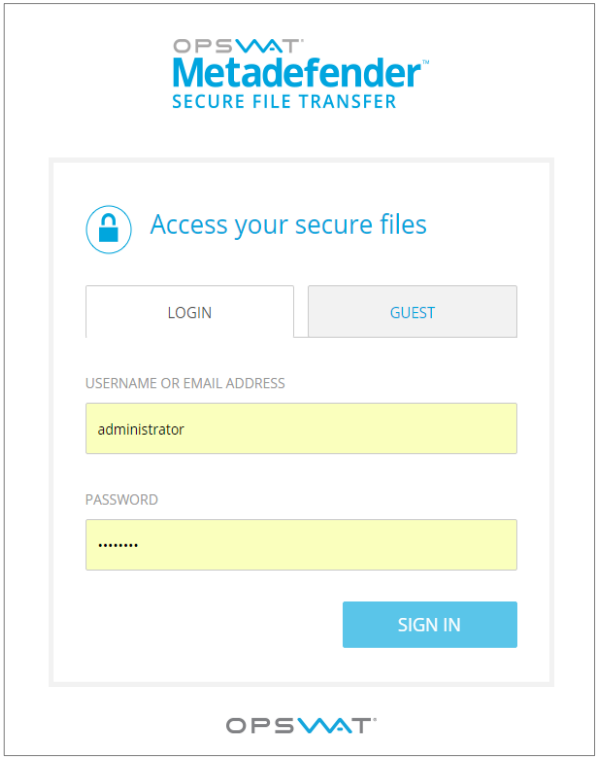
☞ KIOSK와의 계정 연동 기능 제공

☞ 조직 내 직원 및 Guest 계정 생성 제공

☞ Metadefender Core와 연동 기능 제공

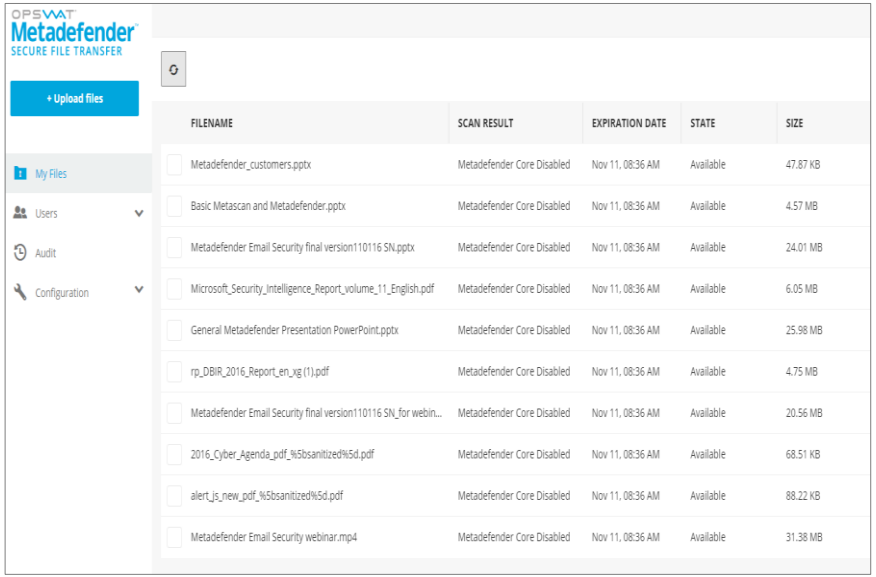
☞ Secure File Storage 내 Workflow Profile 사용 지원

☞ 데이터 살균 기능 지원



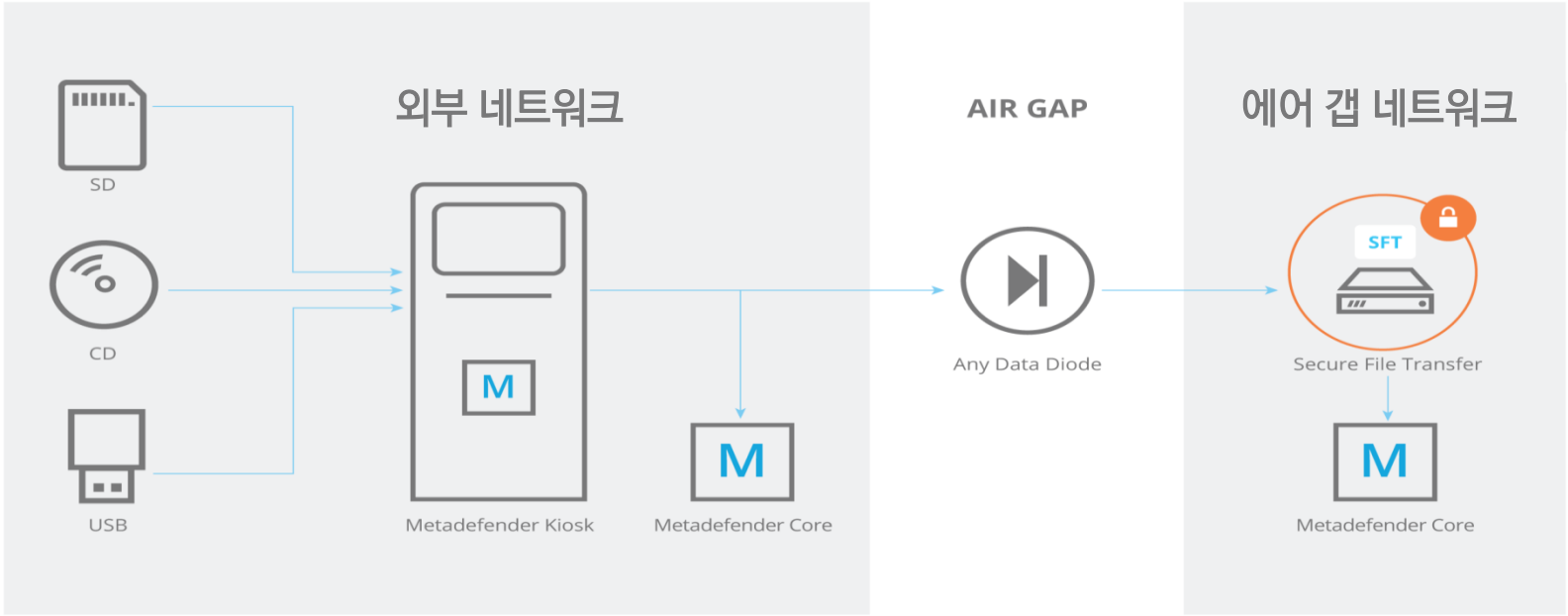
Metadefender KIOSK

- Data Diode에서 안전한 데이터 수신
- 스캔 파일들에 대한 로그 관리
- SFT 내 Workflow 적용



Metadefender KIOSK

- **Air-Gap + Data Diode와 연동을 통한 Kiosk 구성**



Metadefender can be located inside the isolated network as well as in the air-gapped network alongside SFT.

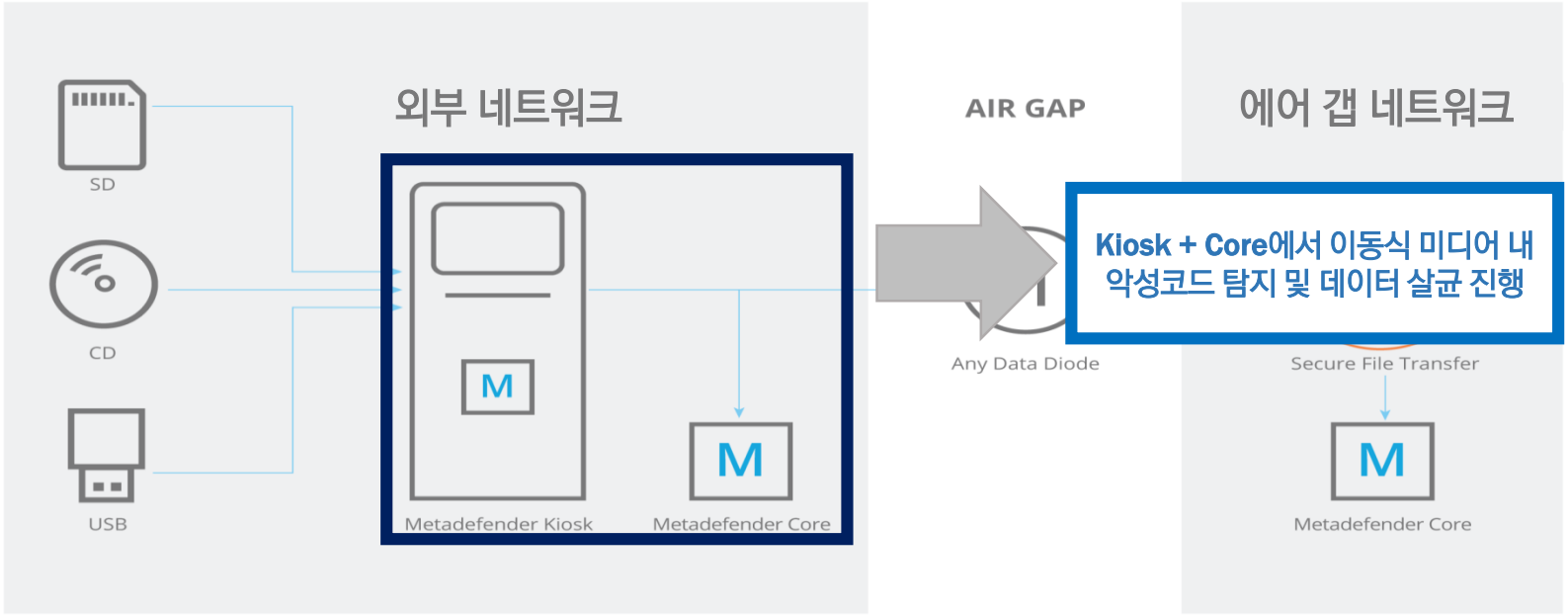
Metadefender KIOSK

- **Air-Gap + Data Diode와 연동을 통한 Kiosk 구성**

Metadefender can be located inside the isolated network as well as in the air-gapped network alongside SFT.

Metadefender KIOSK

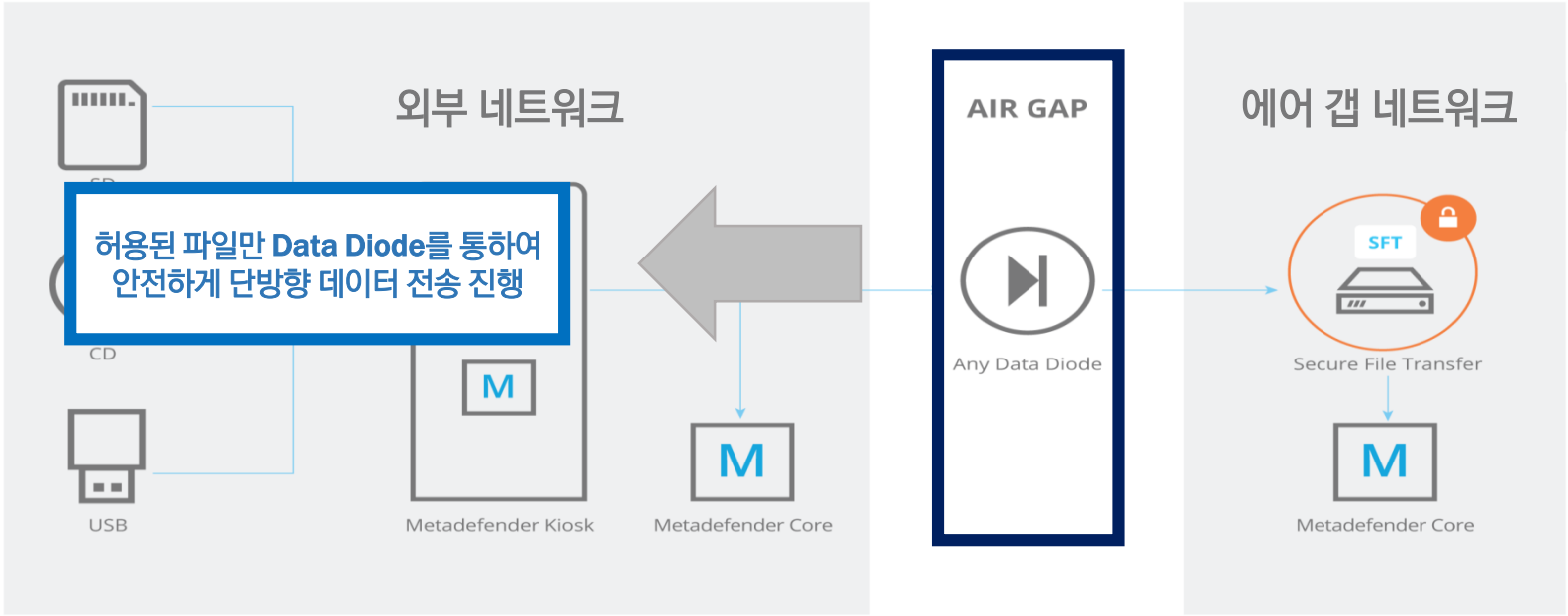
- **Air-Gap + Data Diode와 연동을 통한 Kiosk 구성**



Metadefender can be located inside the isolated network as well as in the air-gapped network alongside SFT.

Metadefender KIOSK

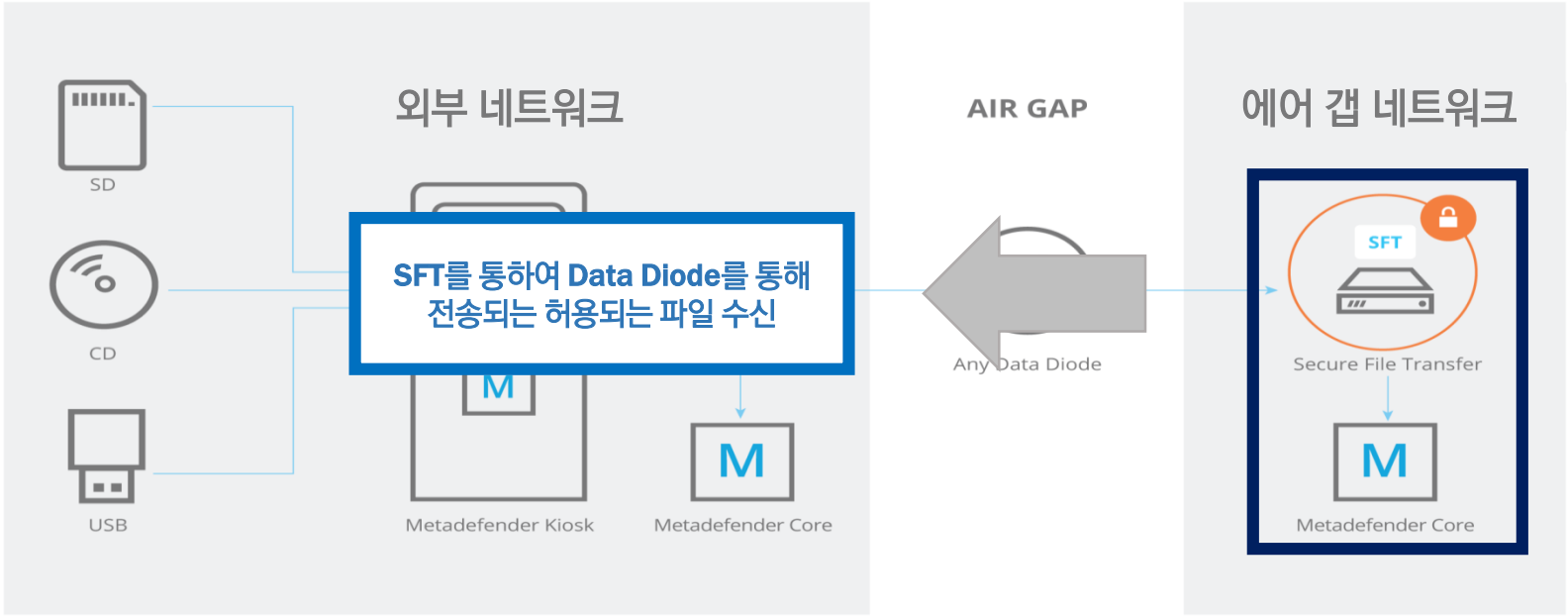
- **Air-Gap + Data Diode와 연동을 통한 Kiosk 구성**



Metadefender can be located inside the isolated network as well as in the air-gapped network alongside SFT.

Metadefender KIOSK

- **Air-Gap + Data Diode와 연동을 통한 Kiosk 구성**



Metadefender can be located inside the isolated network as well as in the air-gapped network alongside SFT.

Metadefender KIOSK

United States

Nuclear Industry

핵 발전소

Oil and Gas

정유시설

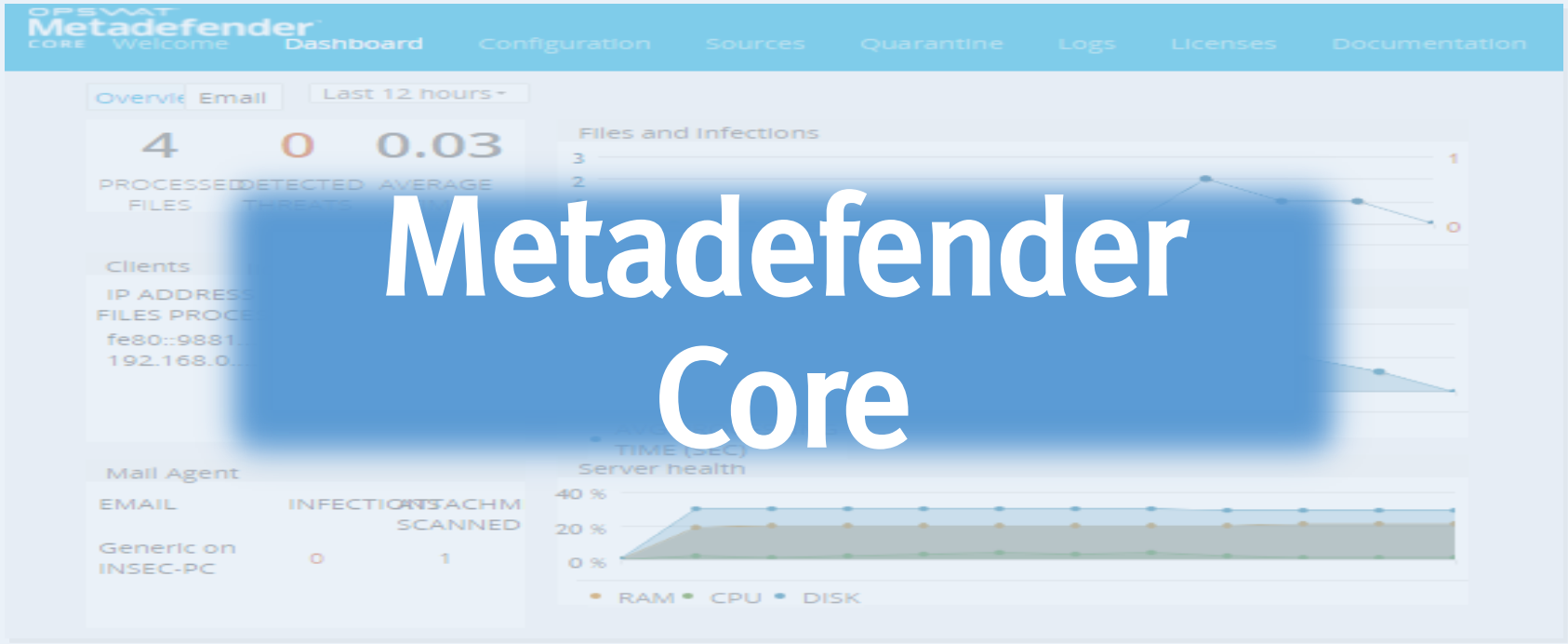
Government

정부기관

Manufacturing

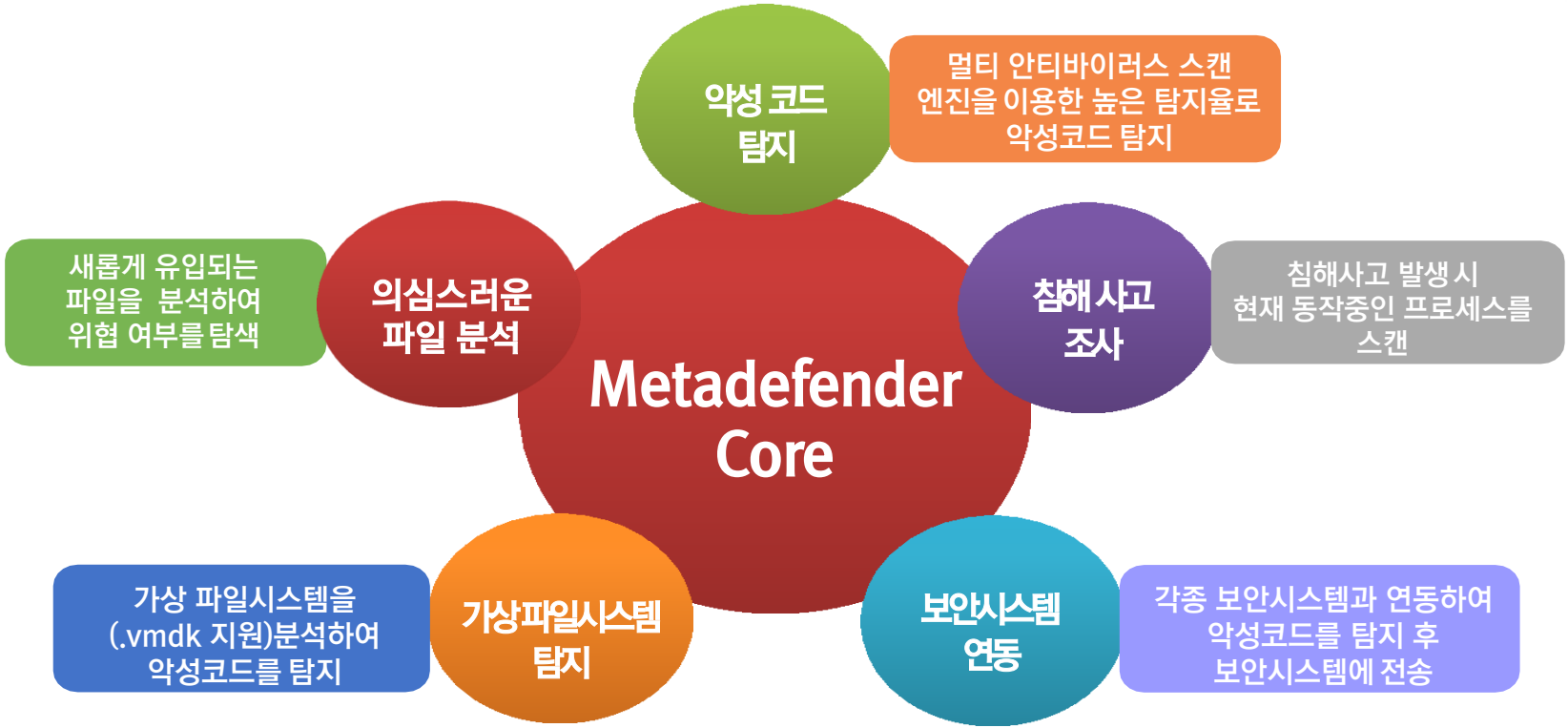
제조업

Metadefender KIOSK



Metadefender Core

Using Metadefender Core



Using Metadefender Core

외부 연계망

인터넷망

DMZ망

폐쇄망

내부 사설망

ICS & SCADA 망

Using Metadefender Core

ICS & SCADA 폐쇄망

Metadefender™

각종 발전소, 에너지 회사
철도, 교통, 정수, 항공, 은행
기타 금융 등 다수 기업 및
기관에서 사용 중 입니다.

정확한 고객사 정보는
별도로 요청하시기 바랍니다.

Using Metadefender Core

- ✓ 경찰청, 사이버테러대응센터, 검찰(대검찰청), KISA, 네이버, 군 특수기관 등 기타 주요 국가기관에 검증되어 운영 중

검찰 PROSECUTION SERVICE

사이버경찰청 NATIONAL POLICE AGENCY

KISA

NSRI 국가보안기술연구소 National Security Research Institute

ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute

NAVER

기타 주요 국가기관

Using Metadefender Core

✓ 옵스왓(OPSWAT) 제품 고객 및 사용 레퍼런스

Using Metadefender Core

- ✓ **Metadefender Core Package & Custom Engines**

For Windows

For Linux

Windows Custom Engines

OPSWAT Metadefender CORE

CONTACT US

INSEC Security

Email: insec@insec.co.kr

Phone: 02-863-5687

홈페이지 : www.insec.co.kr