의료기관을 위한 진화형 랜섬웨어 보호 및 대응 방안

Fortinet ATP (Advanced Threat Protection)

2022. 05. 24

Fortinet Korea

Agenda

- ❑ 진화하는 사이버 위협
- ❑ 현재 대응 방법의 문제점
- ❑ 효과적인 방어를 위한 주요 기능
- ❑ 구축 사례
- ❑ Summary

진화하는 사이버 위협

Email을 이용한 타겟형 공격

사이버 위협의 증가

사이버 위협 환경은 그 어느 때 보다 악의적이고 정교해짐

"의료 및 공공 보건 부문을 대상으로 하는 랜섬웨어 활동"
- FBI Alert AA20-302A

SolarWinds는 해킹이 2개의 주요 정부 기관을 포함한 18,000명의 고객에게 영향을 미쳤다고 밝힘
-News week

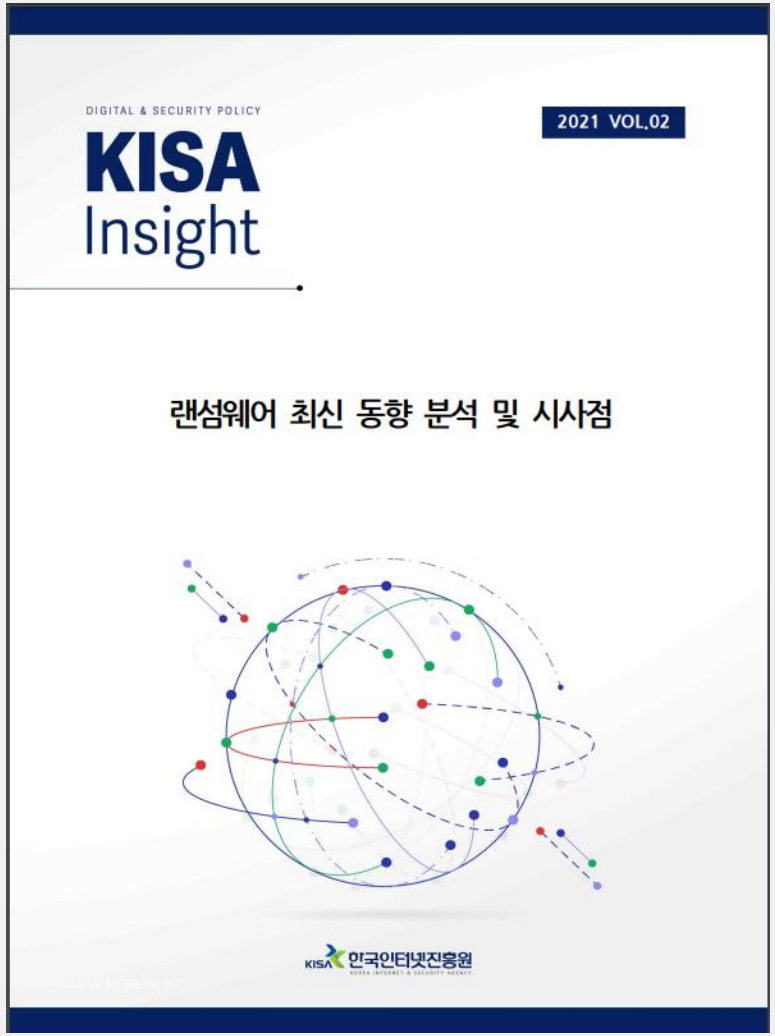
Sources:
CISA. Trends and Predictions in Ransomware. June 2020.

We have seen an explosion of ransomware in 2020… with demands in the millions of dollars

- Jonathon Holmes, FBI, Cyber Summit 2020

코로나 19 이후 사이버 침해사고 트랜드 변화

다양한 산업 분야로 랜섬웨어 공격이 매년 지속적으로 확대됨

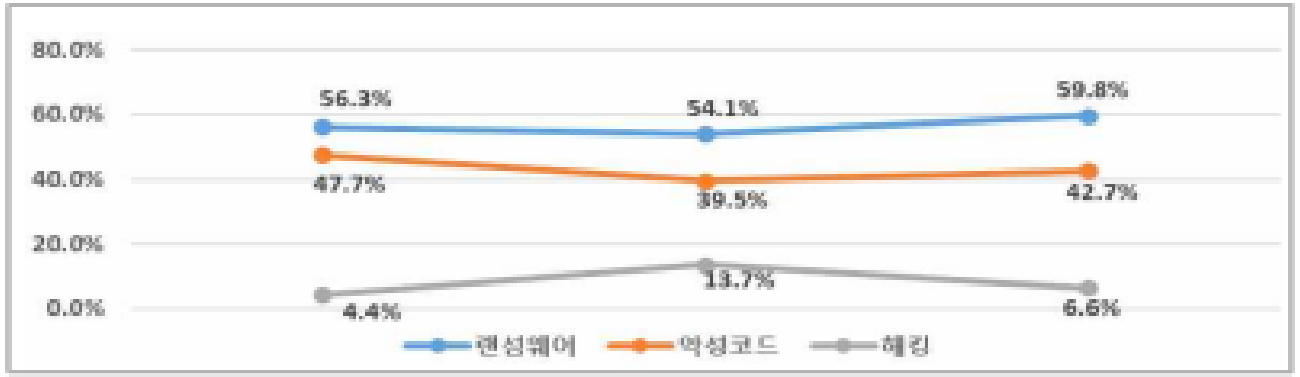


[참고] 20년 정보보호 실태조사 결과 분석

- (기업) 20년 정보보호 실태조사를 통해 조사된 국내 기업의 침해사고 경험률은 2%로 전년대비 0.8% 감소하였으나, 랜섬웨어(54.1%→59.8%), 악성코드(39.5%→42.7%)로 인한 피해는 증가

[표1] 기업 침해사고 경험 유형

구분	2018	2019	2020	증감률('19~'20)
침해사고 경험률	2.3%	2.8%	**2.0%**	-0.8%p
랜섬웨어	56.3%	54.1%	**59.8%**	**+5.7%p**
악성코드	47.7%	39.5%	**42.7%**	**+3.2%p**
해킹	4.4%	13.7%	**6.6%**	-7.1%p
애드웨어/스파이웨어	12.1%	6.6%	**4.0%**	-2.6%p
내부인력에 의한 중요정보유출	3.9%	1.1%	**1.6%**	+0.5%p
DoS/DDoS 공격	2.5%	0.8%	**4.1%**	+3.3%p



국내외 랜섬웨어 피해 사례

코로나 19 확산으로 인한 원격근무 시스템을 노린 이메일, 원격접속 등을 대상으로 공격 증가

- **한국(성형외과)** - 2021년 5월
  - 공격자는 랜섬웨어 공격 후 병원 고객연락처를 탈취
  - 고객들과 직접 연락을 취한 정황이 파악되는 등 2차 피해 발생

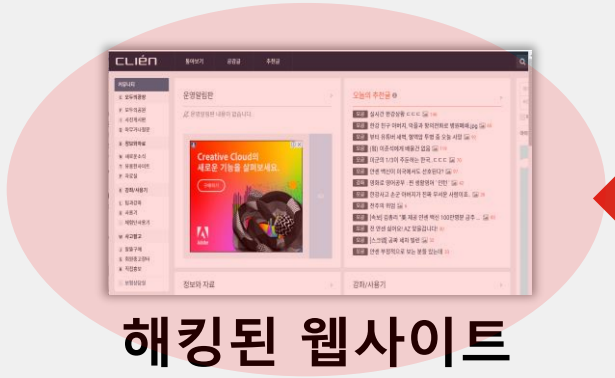
- **독일(뒤셀도르프대 병원)** - 2020년 9월
  - 병원 서버 30대가 랜섬웨어 공격으로 인해 마비
  - IT 서비스 운용이 불가능하게 되어, 응급환자를 받지 못하는 상황 발생

- **영국(국민건강서비스)** - 2017년 5월
  - 국민건강서비스(NHS)가 워너크라이 공격을 당해 16개 병원이 폐쇄
  - 최소 6,900건에 달하는 국민건강서비스 진료예약이 취소

- **스페인(정보 노동기관)** - 2021년 3월
  - 스페인 정보 노동기관 SEPE가 랜섬웨어 공격으로 네트워크 시스템이 암호화
  - 일부 서비스가 중지되는 피해 발생

네트워크와 이메일을 통한 악성코드 유포

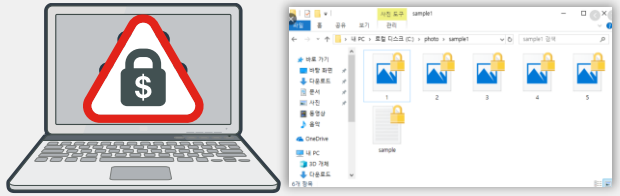
랜섬웨어 공격의 급격히 증가로 인해 기업의 중요 데이터들이 암호화 되어 큰 피해 발생



해킹된 웹사이트

접속

랜섬웨어 감염



사용자 시스템 데이터 암호화

해커

피싱 메일

악성메일 발송

가상화폐 지불

복호화 프로그램 구매 페이지

복호화를 위한 금전 요구

이메일은 가장 위협적인 공격 벡터

악성코드

✓ 사회공학기술을 이용하여 실행 유도
✓ 제로데이 악성코드
✓ 악성코드 유포 경로 중 80% 이상 차지*

피싱

✓ 사용자의 관심사, 역할에 맞춤형 컨텐츠
✓ 종종 C레벨을 대상으로 함
✓ 4%의 사용자가 악성파일 또는 링크를 클릭*

데이터 유출

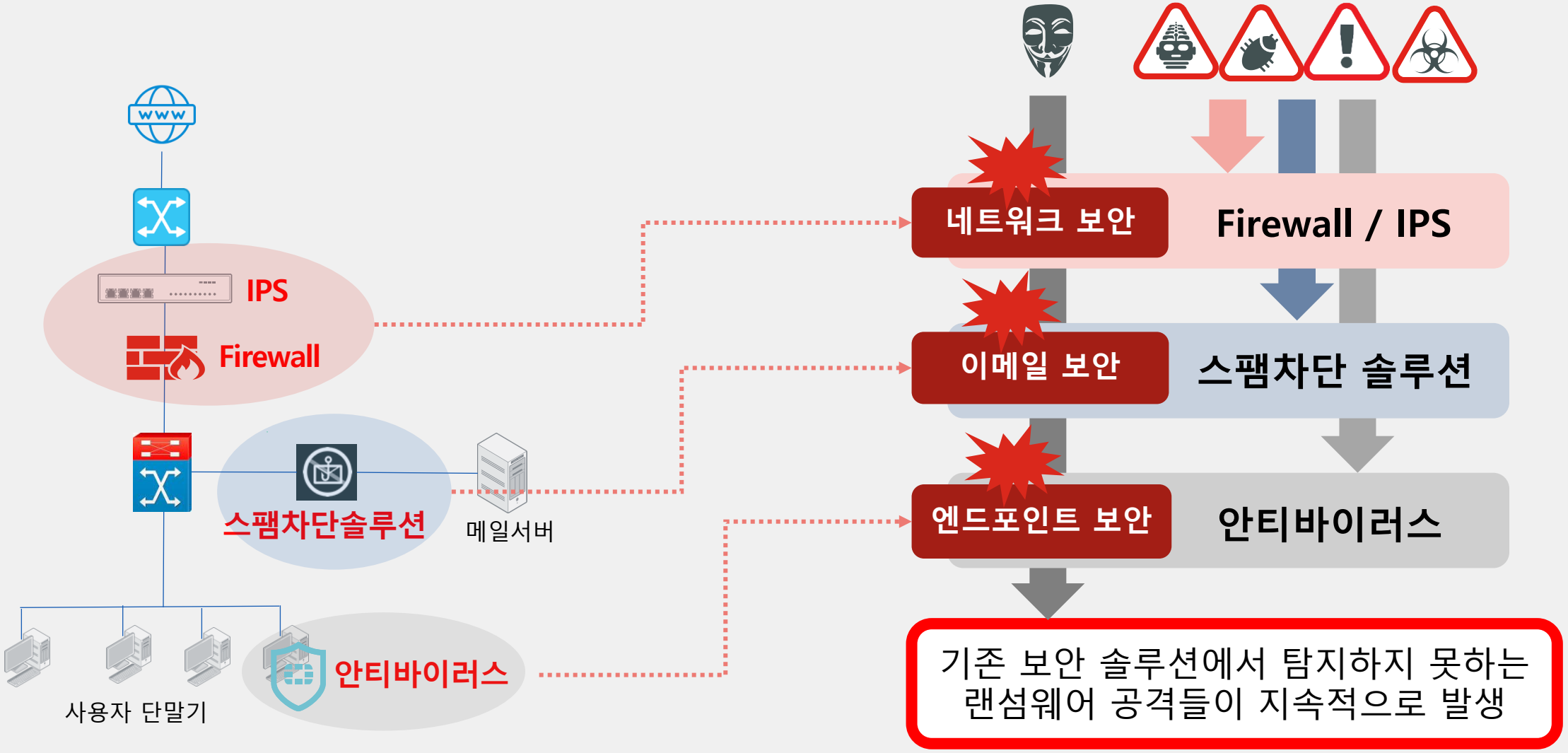
✓ 이메일을 통한 개인 식별 정보 전송
✓ 기업 기밀 정보를 외부로 전송
✓ 민감한 이메일 암호화 실패

* Source: Verizon 2018 Data Breach Investigations Report

현재 대응 방법의 문제점

기존 보안 솔루션으로 탐지하지 못하는 랜섬웨어 증가

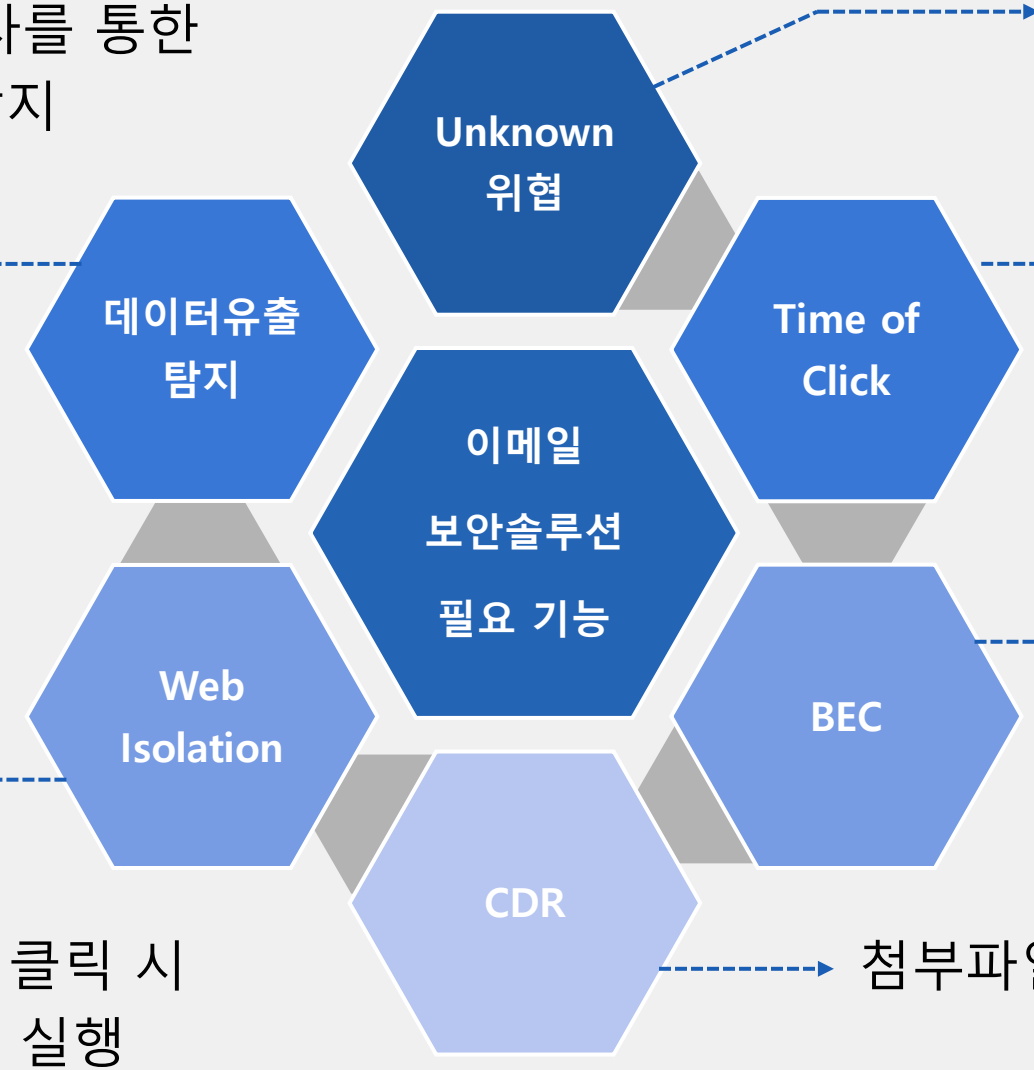
한계점 : 신종/변종 악성코드의 증가로 시그니쳐 기반의 제품의 대응 한계 발생



효과적인 방어를 위한 주요 기능

Email ATP의 필요 기능

Outbound 메일 검사를 통한
중요 데이터 유출 탐지



Sandbox 연동을 통한 행위분석

메일 URL Rewrite 후,
사용자 클릭 시 실시간 분석

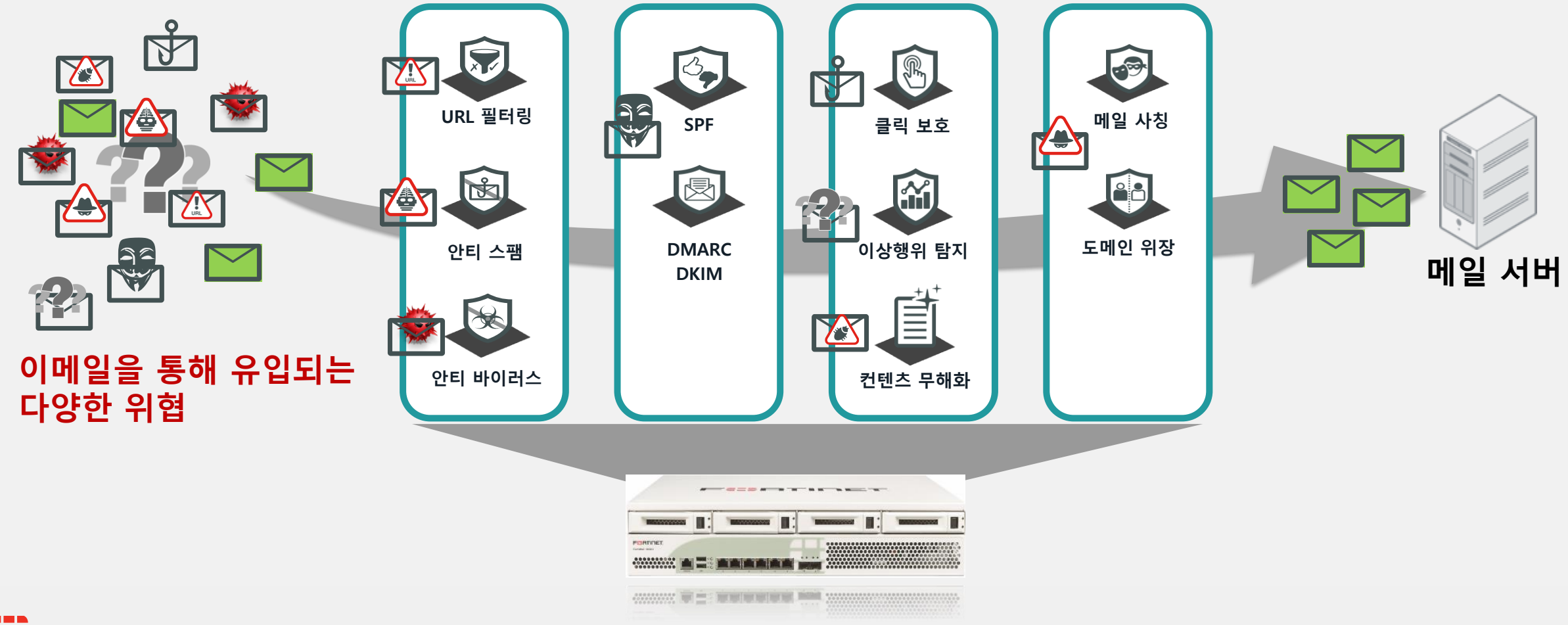
정상메일을 사칭한
악성메일 탐지

메일 본문의 URL을 클릭 시
격리된 공간에서 웹 실행

첨부파일에 포함된 유해 컨텐츠 제거

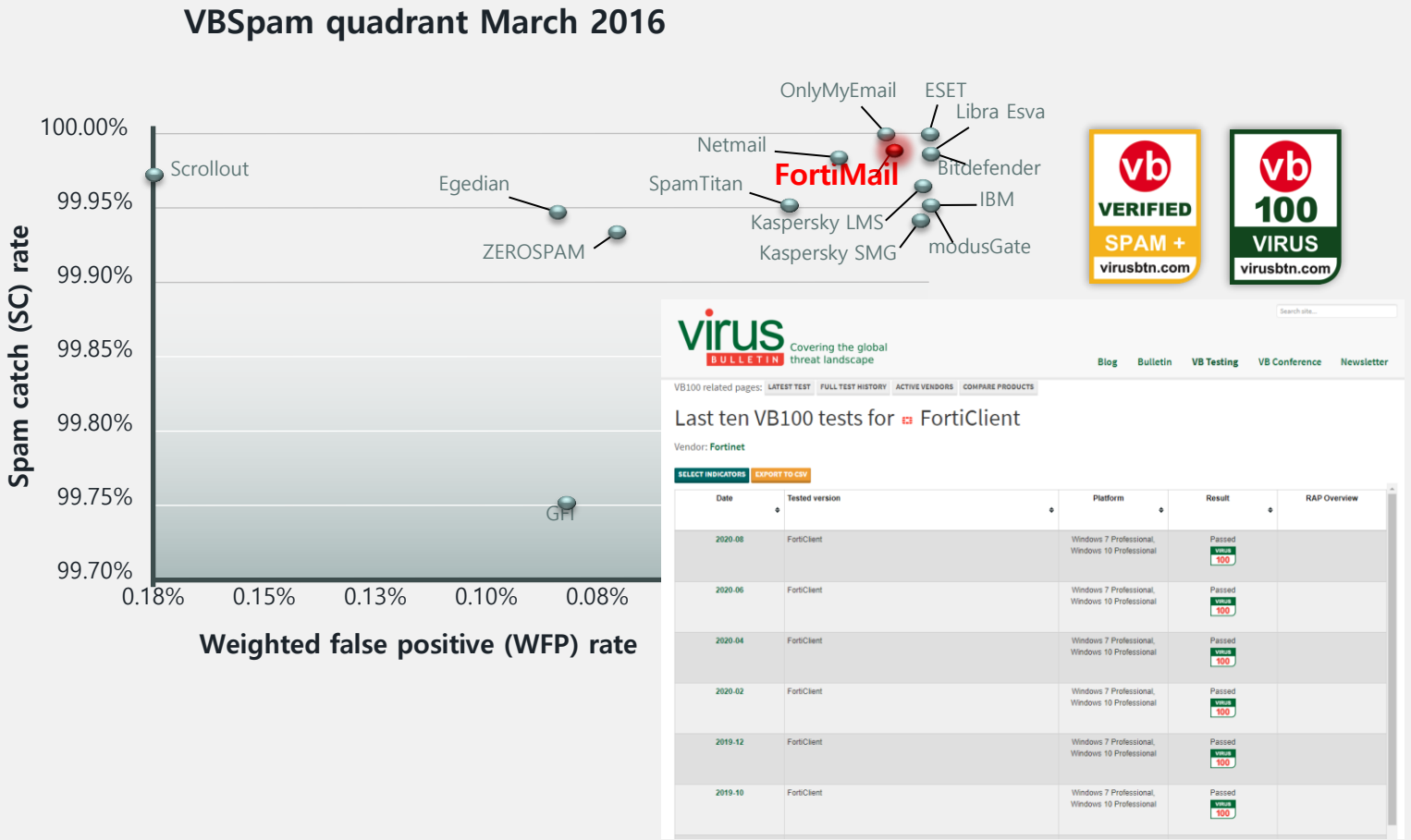
Fortinet Email ATP – 통합 이메일 보안 게이트웨이

단일 솔루션을 통해 이메일로 유입되는 다양한 형태의 위협을 제거



Fortinet Email ATP 주요 기능 – Anti Spam, Anti Virus

공인 기관으로부터 높은 탐지력을 인정받은 Anti-Spam과 Anti-Virus 엔진

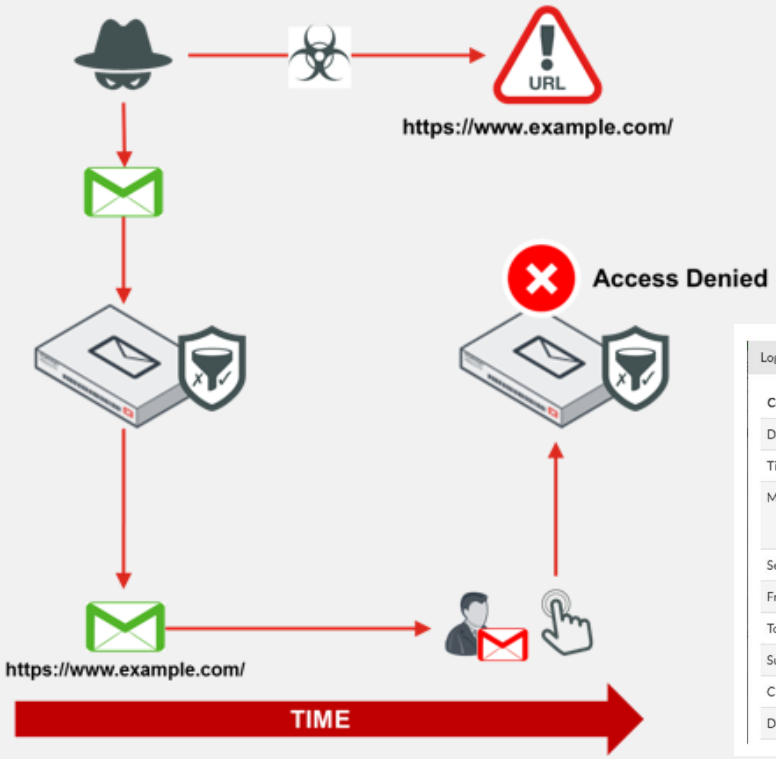


주요 특징

- Anti-Spam 엔진은 지속적으로 공인된 기관으로부터 높은 탐지력을 인정받음
- 강력한 Anti-Virus 엔진은 지속적으로 VB100 테스트 통과

Fortinet Email ATP 주요 기능 – URL Click Protection

사용자가 이메일 본문의 URL을 클릭하는 시점에 실시간 검사하여 위협 탐지



- 세부 리스트 확인과 탐지사유에 대한 확인 가능

Log Details: 0300002026

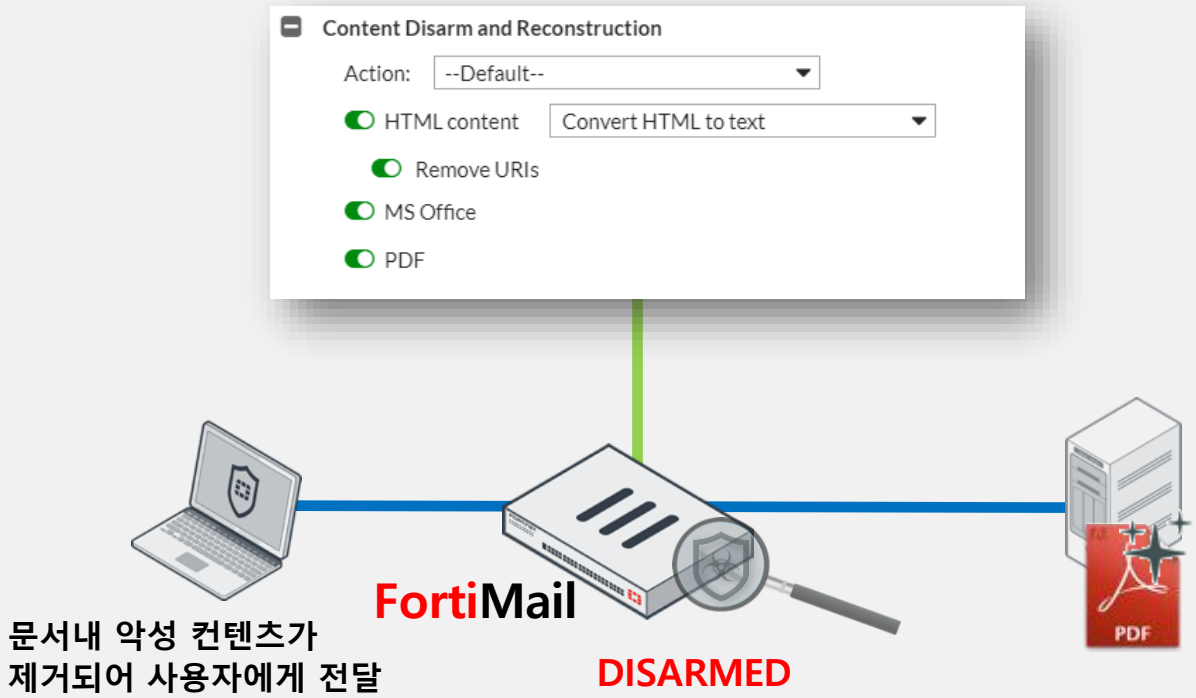
Column	Content
Date	2020-05-13
Time	00:43:14.460
Message	File name: [삼성화재]환급금 수령.xls(checksum:d8fe50c065415e9764bca3e7f3a5df088967bc78ce4433079cf2a33b4d258585), scanned by Antivirus Scanner(detected)
Session ID	04CFhDKw002025-04CFhDL0002025
From	mit258@naver.com
To	robinkim@mail.fortinet.co.kr
Subject	바이러스1
Client IP	192.168.14.74
Destination IP	192.168.14.75

주요 특징

- 메일 검사 시 URL에 대한 위험이 탐지되지 않더라도 사용자가 메일의 URL을 클릭하는 순간 다시한번 URL에 대한 위협검사 결과 반영하여 차단이 가능

Fortinet Email ATP 주요 기능 – 악성 컨텐츠 무해화 기술

CDR(Content Disarm and Reconstruction)을 통한 악성 컨텐츠를 선택적으로 제거

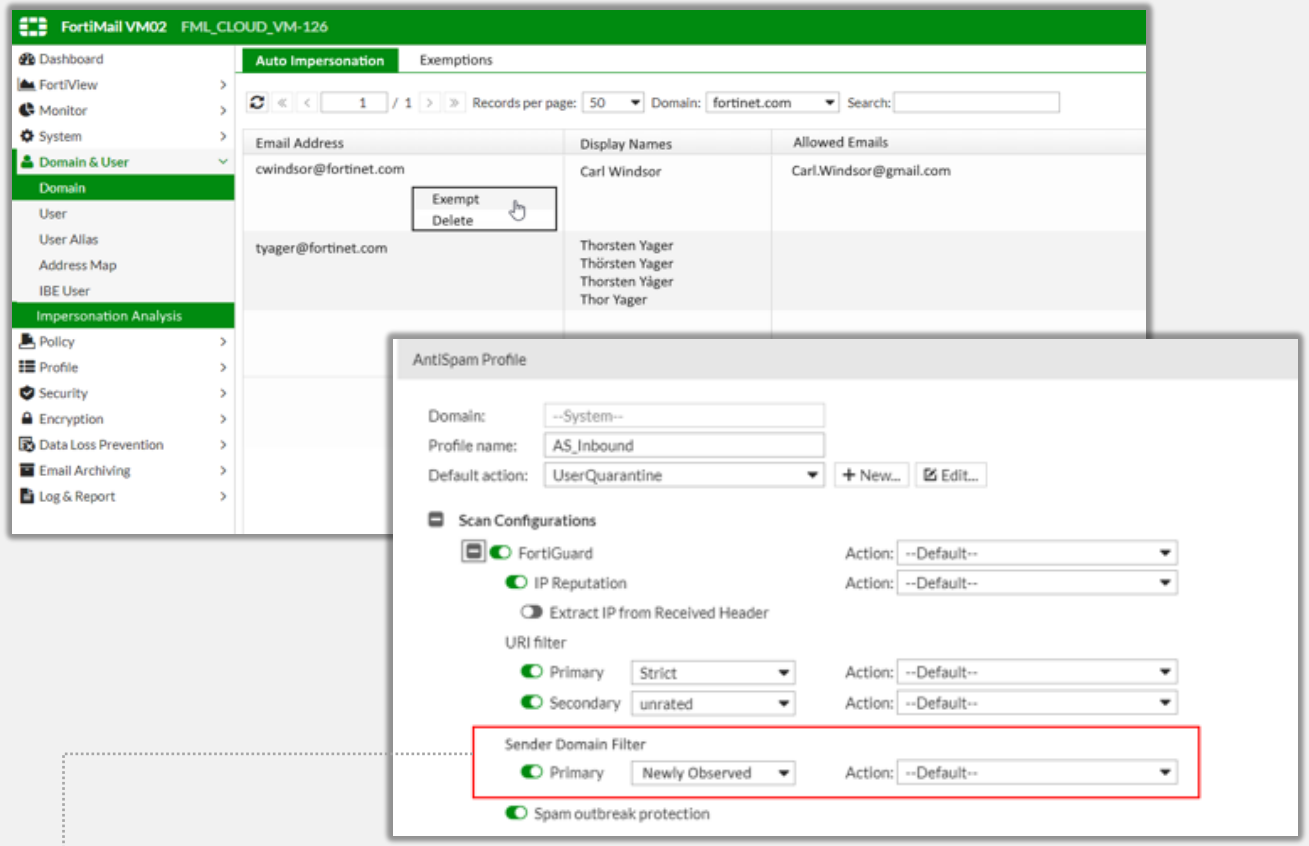


주요 특징

- 엔드포인트에서 문서가 실행되기 전 문서 내부의 액티브 컨텐츠를 제거
  - 매크로
  - 하이퍼링크
  - 임베디드 오브젝트
- 사용자 실수로 악성 컨텐츠가 포함된 문서가 시스템에서 실행되는 것을 방지

Fortinet Email ATP 주요 기능 – 비지니스 이메일 위협 차단

Impersonation Analysis를 통해 위장 메일에 대한 탐지 기능을 제공



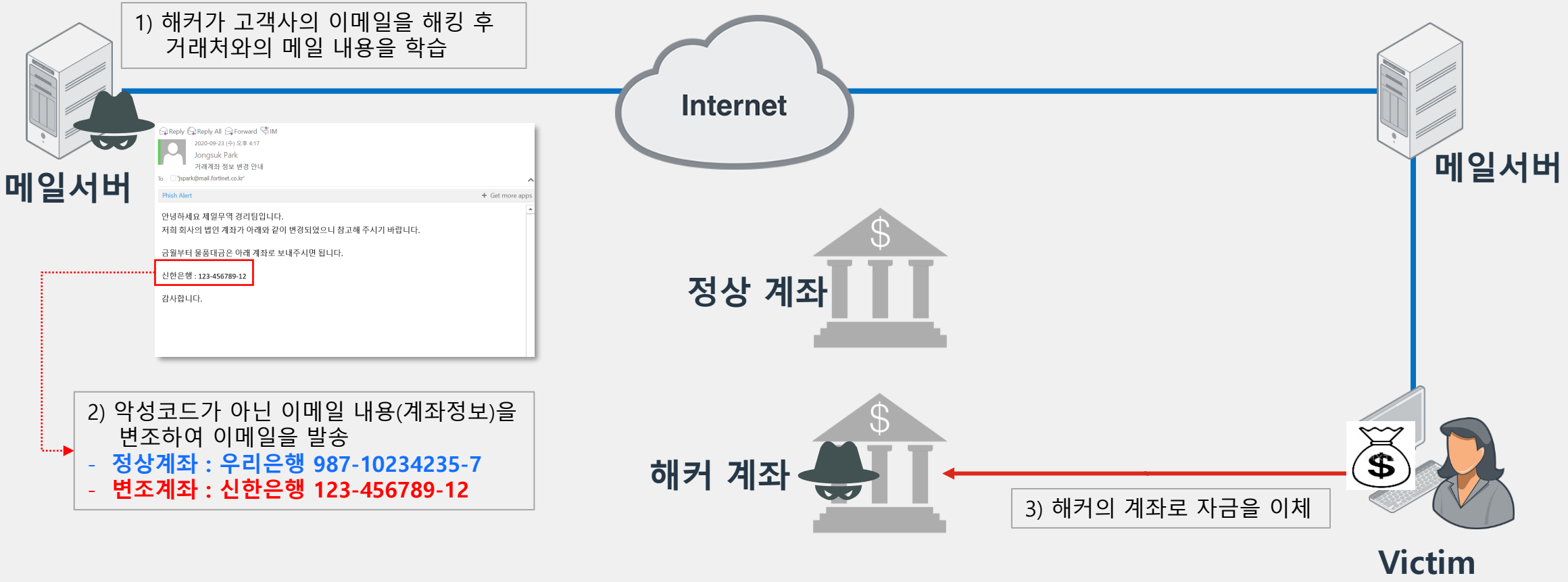
BEC(Business Email Compromise) 위협 탐지를 위해 다양한 설정 기능을 제공

주요 특징

- BEC 공격 탐지를 위한 기능을 제공
  - VIP 사용자의 스푸핑 탐지
- 발신자 도메인 필터
  - 새로 등록되거나 평가되지 않은 도메인 차단

Fortinet Email ATP 주요 기능 – 비지니스 이메일 위협 차단

이메일 계정을 사칭하여 거래은행 변경 메일을 Victim User에게 발송



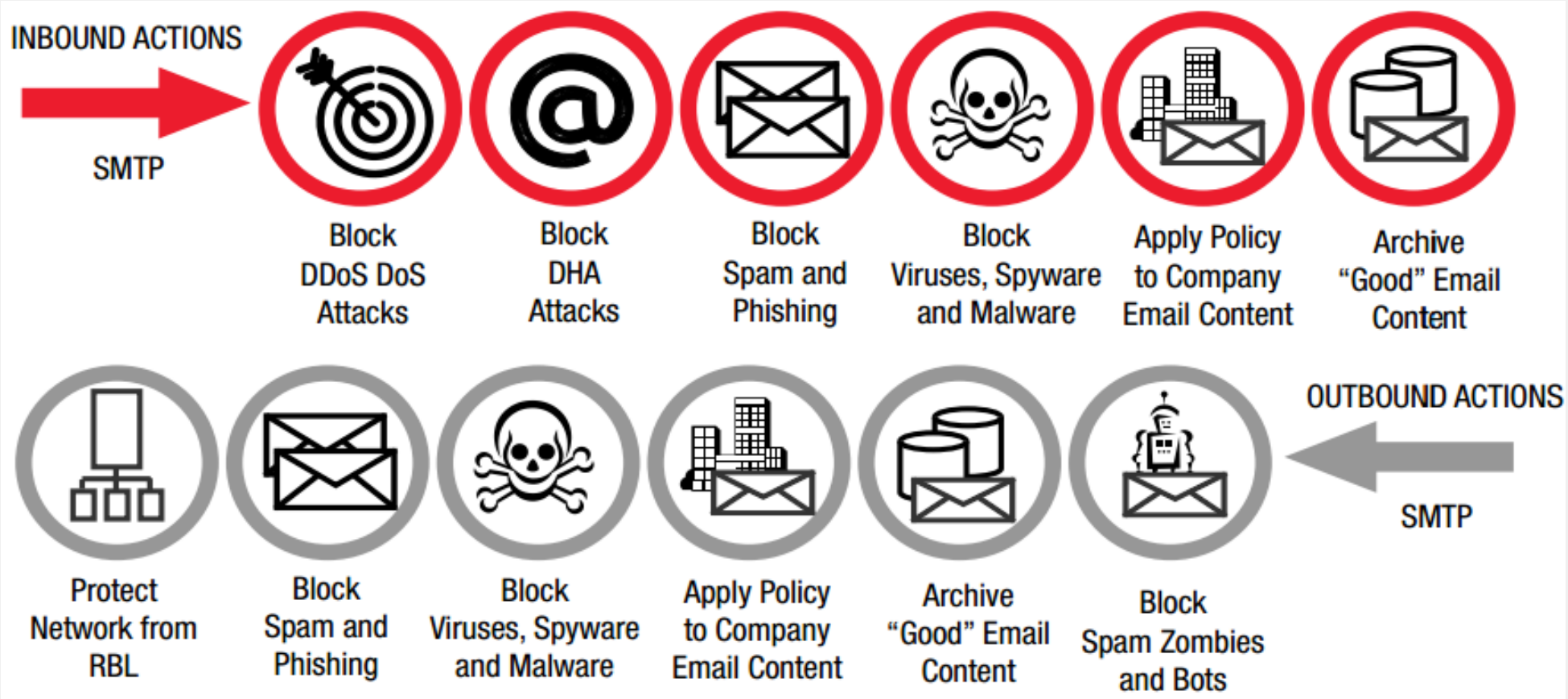
Fortinet Email ATP 주요 기능 – 비지니스 이메일 위협 차단

거래처의 이메일을 사칭하여 발송된 BEC 위협 탐지

BEC 위협 탐지 시 메일을 격리하거나 경고 문구를 삽입하여 사용자에게 위협 경고

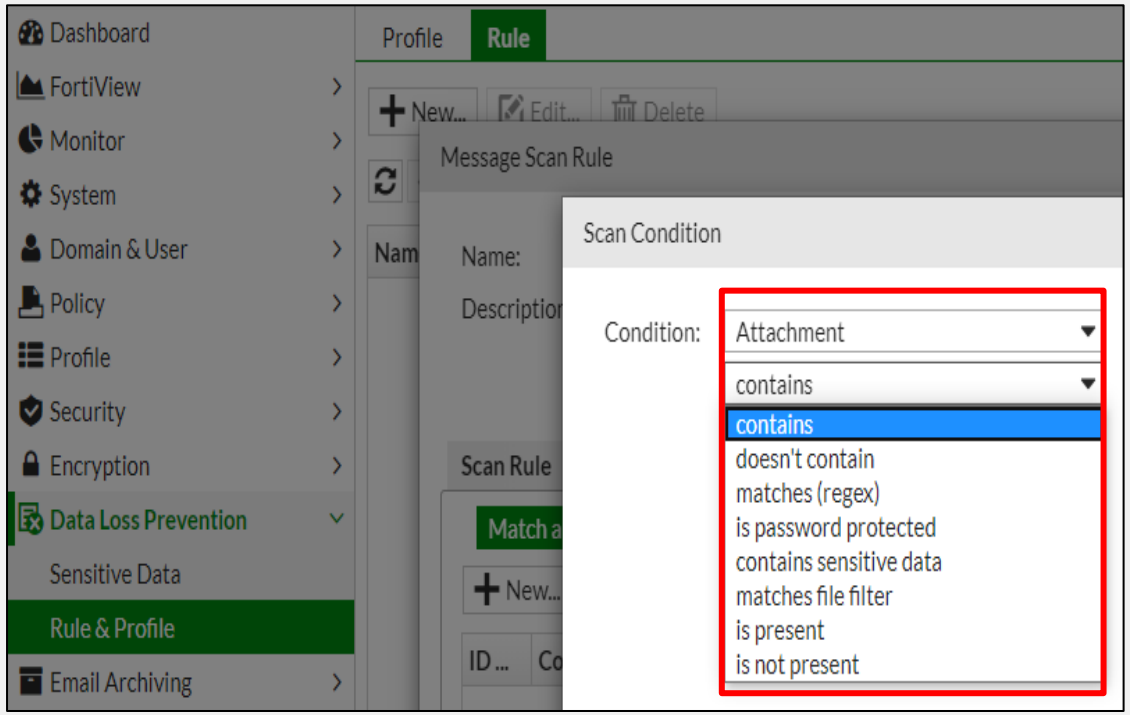
Fortinet Email ATP 주요 기능 – 아웃바운드 메일 검사

조직 내부에서 외부로 전달되는 이메일에 대해 다양한 위협 검사 수행

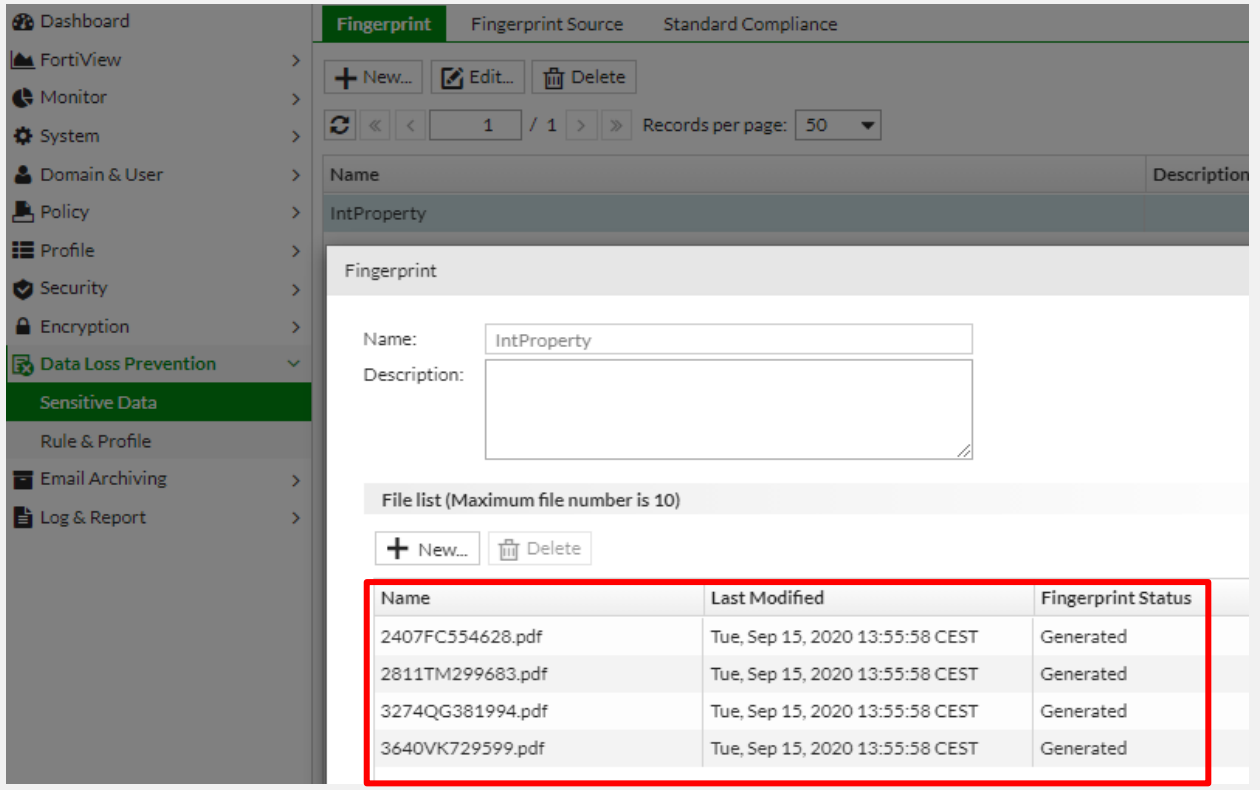


Fortinet Email ATP 주요 기능 – 데이터 유출 방지

DLP(Data Loss Prevention) 설정을 통한 조직의 중요 데이터 유출 방지



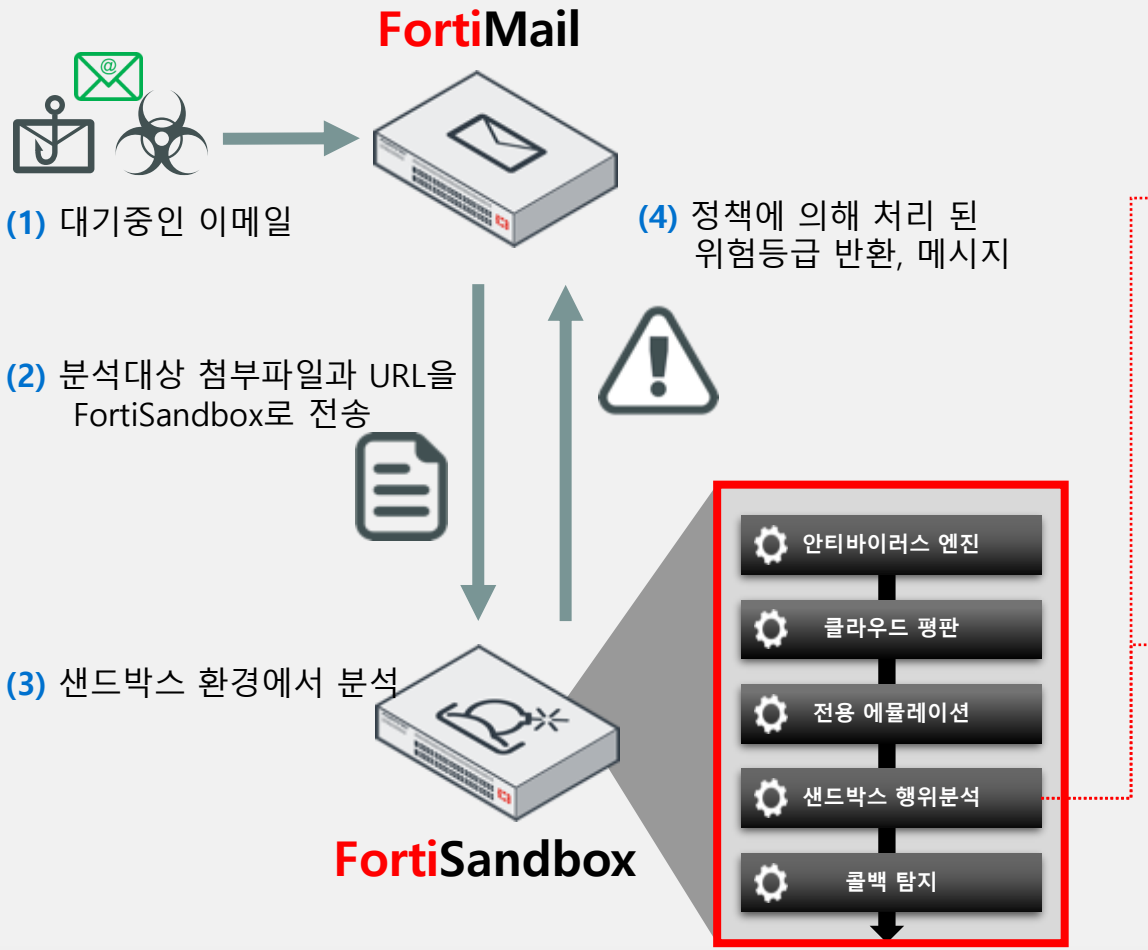
DLP 검사조건

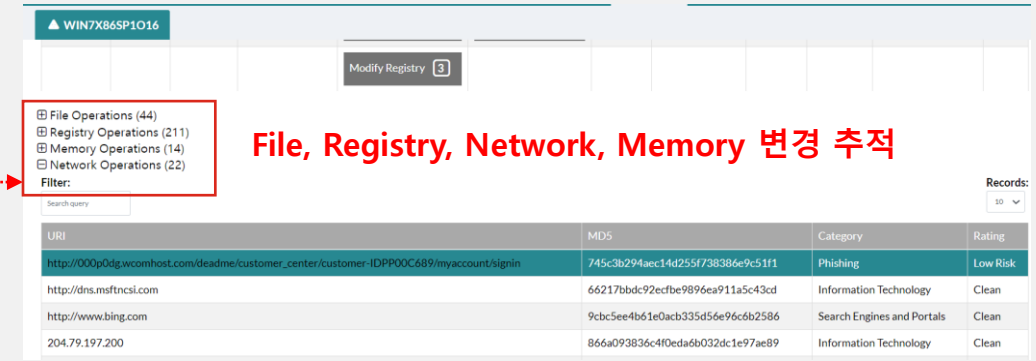


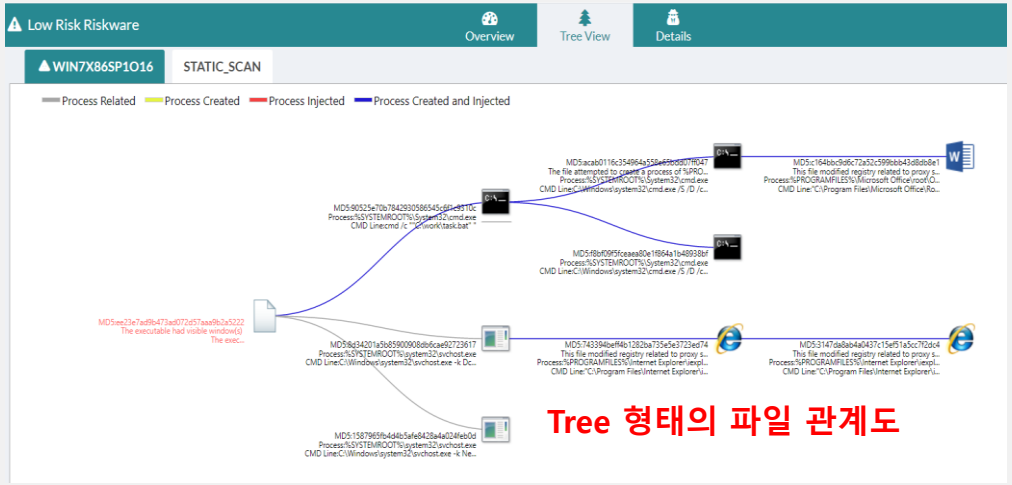
Fingerprint 등록을 통한 중요 문서유출 탐지

Fortinet Email ATP 주요 기능 – FortiSandbox 연동

FortiSandbox 연동을 통해 알려지지 않은 위협에 대해 대응







Fortinet ATP 연동을 통한 제로데이 위협의 실시간 차단

탐지된 위협 정보를 로컬 DB에 저장 후 동일한 공격에 대해 자동으로 차단

실시간 인텔리전스 업데이트 및 공유

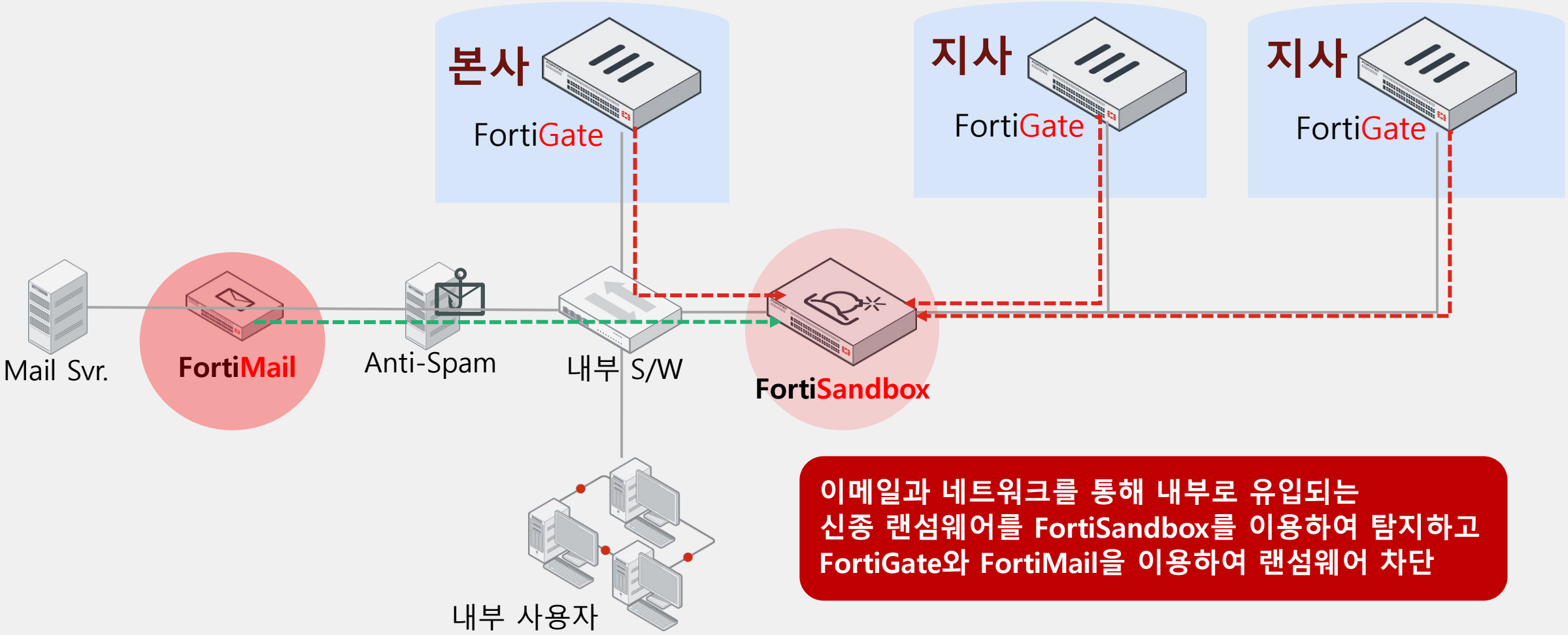
Fortinet Security Fabric & FortiGuard Threat Intelligence

국내 위협 포함, 광범위한 글로벌 위협 인텔리전스

구축 사례

A사 ATP 구축 사례

랜섬웨어 감염 사고로 인해 랜섬웨어 유입 구간에 대한 사전 대응 솔루션 구축



이메일과 네트워크를 통해 내부로 유입되는 신종 랜섬웨어를 FortiSandbox를 이용하여 탐지하고 FortiGate와 FortiMail을 이용하여 랜섬웨어 차단

Summary

랜섬웨어 공격은 지속적으로 증가

랜섬웨어 공격은 2022년에도 많은 기업들을 대상으로 증가가 될거라 예상되고 있으며,
단 한번의 감염으로도 기업의 중요 데이터들이 한순간에 모두 사라질 수 있습니다!

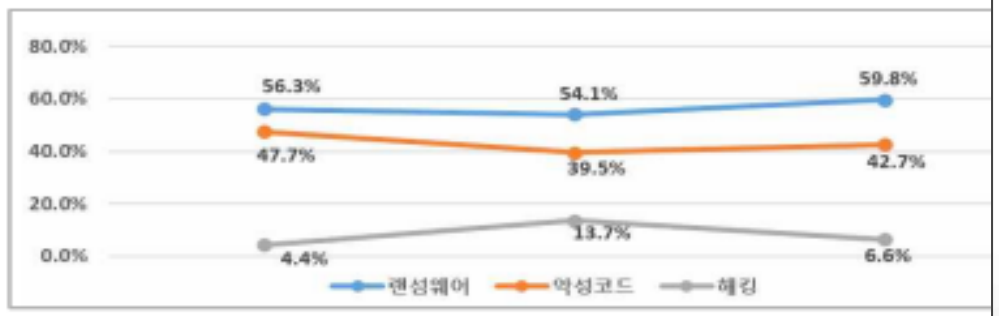
✓ KISA : 2022년 사이버위협 전망

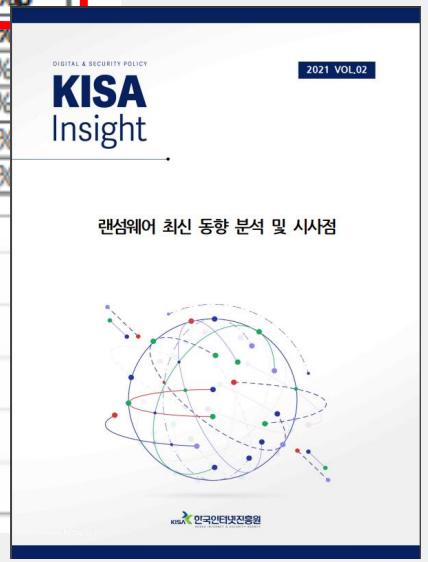
[참고] 20년 정보보호 실태조사 결과 분석

- **(기업)** 20년 정보보호 실태조사를 통해 조사된 국내 기업의 침해사고 경험률은 2%로 전년대비 0.8% 감소하였으나, 랜섬웨어(54.1%→59.8%), 악성코드(39.5%→42.7%)로 인한 피해는 증가

[표1] 기업 침해사고 경험 유형

구분	2018	2019	2020	증감률('19-'20)
침해사고 경험률	2.3%	2.8%	2.0%	-0.8%p
랜섬웨어	56.3%	54.1%	59.8%	+5.7%p
악성코드	47.7%	39.5%	42.7%	+3.2%
해킹	4.4%	13.7%	6.6%	-7.1%
애드웨어/스파이웨어	12.1%	6.6%	4.0%	-2.6%
내부인력에 의한 중요정보유출	3.9%	1.1%	1.6%	+0.5%
DoS/DDoS 공격	2.5%	0.8%	4.1%	+3.3%

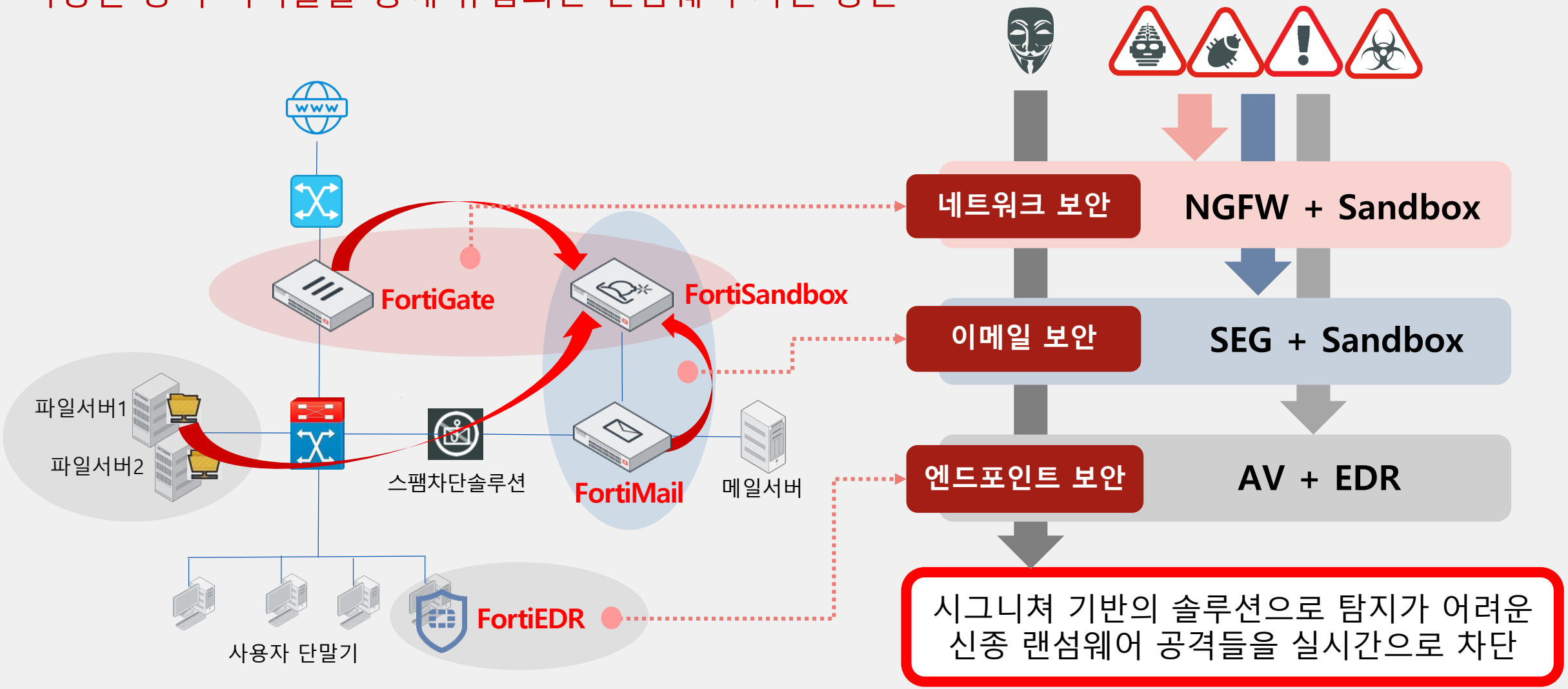




✓ KISA : 2021년 랜섬웨어 최신 동향 분석 및 시사점 내용 발췌

랜섬웨어 방어를 위한 다단계 방어전략

다양한 공격 벡터들을 통해 유입되는 랜섬웨어 차단 방안



FORTINET

Customer Briefing Center
포티넷 CBC 고객 솔루션 체험 센터

글로벌 탑 사이버 보안 벤더인 포티넷에서 국내 고객 분들을 위해 마련한 솔루션 체험 센터로 방문하시는 고객분들의 요구사항에 따라 맞춤화된 컨설팅을 제공합니다.

보안 중심 네트워크 | 다이나믹 클라우드 보안 | AI 기반 보안 관제 | 제로 트러스트 엑세스

☑ 포티넷CBC에 방문해야 하는 이유?

- 디지털 트랜스포메이션에 필요한 IT보안 요구 사항을 알아보고 최적의 해결 방안을 제시합니다.
- 고객의 비즈니스 목표에 맞추어 당사 기술 전문가와 1:1 맞춤 컨설팅이 가능합니다.
- 축적된 수많은 레퍼런스로 고객의 다양한 상황에 맞는 완벽한 보안 솔루션을 제공합니다.
- 보안 솔루션을 시각적으로 확인할 수 있는 라이브 데모를 직접 체험할 수 있습니다.

포티넷 CBC는 언제나 여러분께 열려있습니다. 지금 방문 신청해주세요!

www.fortinet-vcbc.com www.fortinet.com/kr/corporate/cbc

CBC 방문 신청하기

Virtual CBC 바로가기


FORTINET