개발 6개월 / 훔치는데 6시간 / 판매 6분

포티넷이 알려주는
‘진화하는 이메일 위협 방어를 위한 솔루션 가이드’

2020년 12월 03일(목) 15:00~16:00

포티넷코리아 박종석 이사

진화하는 사이버 위협

Email을 이용한 타겟형 공격

이메일 보안 위협 동향

BBC NEWS | 코리아

뉴스 비디오 다운로드 TOP 뉴스

이메일 위조: 세계적으로 30조원이 넘는 피해를 안긴 해킹 수법

조이 타이디
사이버보안 전문기자

2019년 10월 2일

여느 이메일처럼, 회사의 CEO가 보낸 메

"거래가 성사됐으니 800만 달러를 이 계
해. 고맙네."

CNBC HOME U.S. NEWS MARKETS INVESTING TECH MAKE IT VIDEO SHOWS MORE

CRIME

LIFE | TRAVEL | ENTERTAINMENT | SPORTS | WEATHER | CRIME | ART & CULTURE

Xoom says $30.8 mln transferred fraudulently to overseas accounts

REUTERS

news1 뉴스 KOREA 포토 | 이슈 | 카드뉴스

정치 북한 사회 경제 IT/과학 금융/증권 산업 지방 국제 생활

재계 | 전기전자 | 자동차산업 | 에너지·중공업 | 유통 | 생활경제 | 중기·창업 | 패션 | 뷰티 | 호텔·관광 | 의료 | 식음료 | 헬스케어

홈 > 산업 >

랜섬웨어 스팸메일 주의...스팸메일 발송량 2.5배 이상 증가

개인 및 기업 보안 비상...면밀한 주의와 전문적 관리 필요

(서울=뉴스1) 전민기 기자 | 2016-04-27 14:35 송고

기사보기 | 네티즌의견 | 좋아요 0개 | 공유하기 | 트윗

© News1

기업메일 전문기업 '메일플러그'에서 조사한 자료에 따르면, 2016
일 발송량이 직전분기 대비 약 2.5 배 이상 증가한 것으로 파악됐다
메일을 통한 랜섬웨어 감염에 각별한 주의가 요구되고 있다.

CNBC CRIME

Xoom says $30.8 mln transferred fraudulently to overseas accounts

REUTERS

15 COMMENTS Join the Discussion

CSO

CEO fired after 'fake CEO' email scam cost firm $47m

COMPUTERWORLDUK FROM IDG

Home > News > IT Business News

Surrey County Council hit with £120,000 fine for misdirected emails

The Information Commissioner's Office (ICO) has imposed a fine on Surrey County Council after the local authority repeatedly sent unencrypted, personal information to the wrong email addresses.

보안뉴스 SECURITY

#전체기사 #시큐리티월드 #사건사고 #2020년 보안시장 #코로나19

Home > Security

BEC 공격자들, 아무리 체포해도 줄어들지 않는 이유

좋아요 6개 | 입력 : 2020-08-28 09:50

#정보보호 #정보보안 #IT보안 #사이버보안

서부 아프리카 지역에서 주로 활동하는 BEC 공격자들...나이지리아서 가나로
사이버 범죄, 사회적으로 수용되지 못한 청년들이 선택하는 경우가 많아

[보안뉴스 문가용 기자] 최근 미국 사법부는 가나에서 체포된 데보라 멘사(Deborah Mensah)라는 인물을 인도받았다. 멘사는 기업 이메일 침해 공격(BEC 공격)을 통해 수억 달러의 피해를 여러 조직들에게 입히는 데 일조했다고 알려져 있다. 현재 수많은 해킹 범죄 전담 조직들은 전 세계적인 공조를 통해 BEC 공격을 하는 일당들을 잡는 데 힘을 다하고 있다.

이메일은 가장 위협적인 공격 벡터

악성코드

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

피싱

- ✓ 사용자의 관심사, 역할에 맞춤형 콘텐츠
- ✓ 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

Security Email Gateway

이메일 보안 솔루션 개요

Email Security 솔루션 주요 벤더

SOPHOS

CYREN

Symantec

Microsoft

SECU LETTER

FORTINET®

proofpoint.

Armorblox

TREND MICRO™

지란지교시큐리티

Forcepoint

KIWONTECH

FIREEYE™

SONICWALL

Email Security 솔루션 핵심 기능

Email security refers collectively to the prediction, prevention, detection and response framework used to provide attack protection and access protection for email. Email security spans gateways, email systems, user behavior, and various supporting processes, services and adjacent security architecture**. Key capabilities** of the market include Network Sandbox, Content Disarm and Reconstruction, URL Rewriting, Time-of-Click Analysis, Web Isolation Services, Display Name Spoof Detection, Domain-Based Message Authentication, Reporting and Conformance on Inbound Email, Lookalike Domain Detection, and Anomaly Detection. The growing problem of phishing and impersonation can be reduced through education, social graph impersonation filtering, improved indicators of identity in email and suspicious email workflow along with email security solutions ***- Gartner peerinsights.***

Network Sandbox

Content Disarm and Reconstruction

URL Rewriting

Time-of-Click Analysis

Web Isolation

Phishing

DLP

Impersonation

Security Email 솔루션 배포형태 및 고려사항

어플라이언스 형태

- 이메일 처리량
- 주요 보안 기능
- 라이선스 정책

클라우드 환경

- 설치 모드
- 호환성 유무
- 라이선스 정책

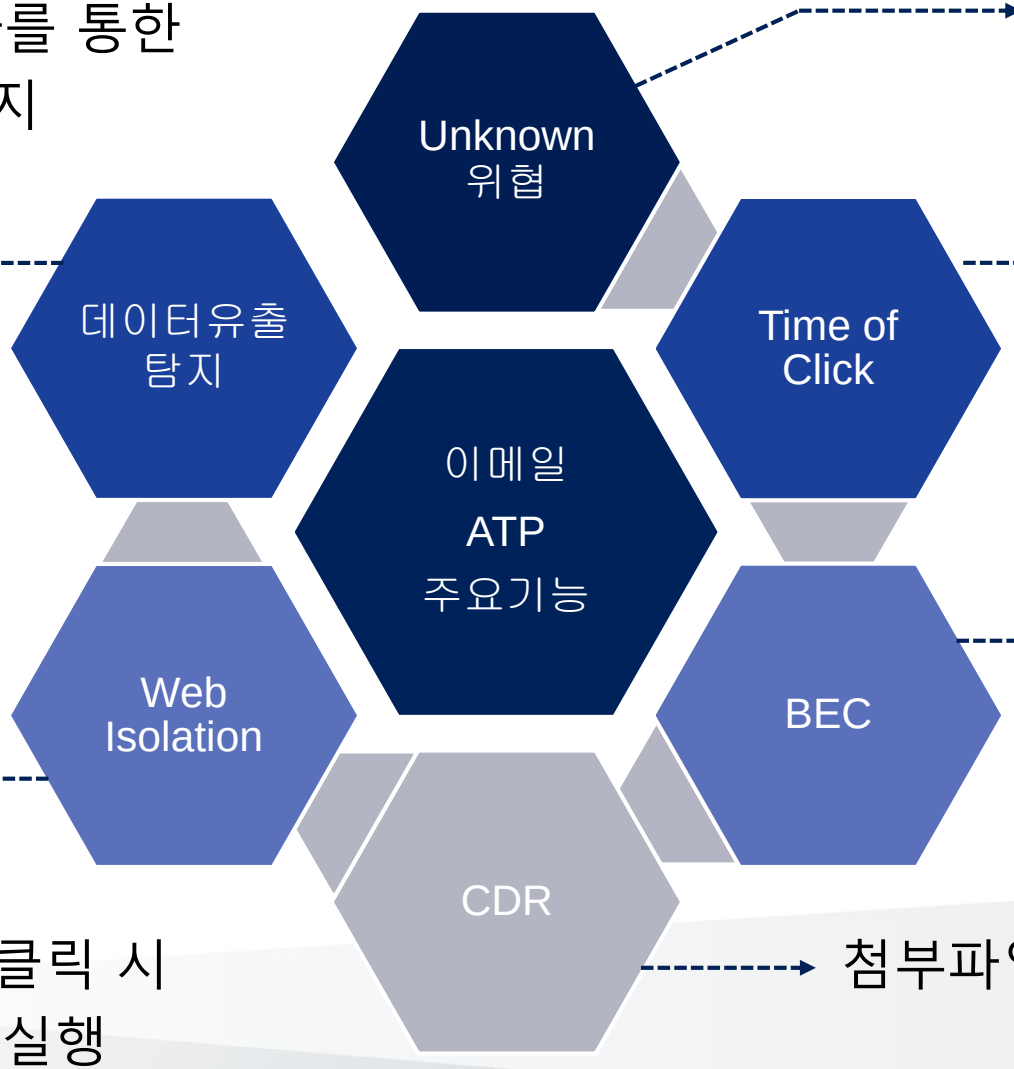
SaaS

- 서비스별 과금 형태
- 컴플라이언스
- 데이터센터 물리적 위치
- SLA

Email ATP 솔루션 기능

최신 위협 방어를 위한 핵심 기능

Outbound 메일 검사를 통한
중요 데이터 유출 탐지



Sandbox 연동을 통한 행위분석

메일 URL Rewrite 후,
사용자 클릭 시 실시간 분석

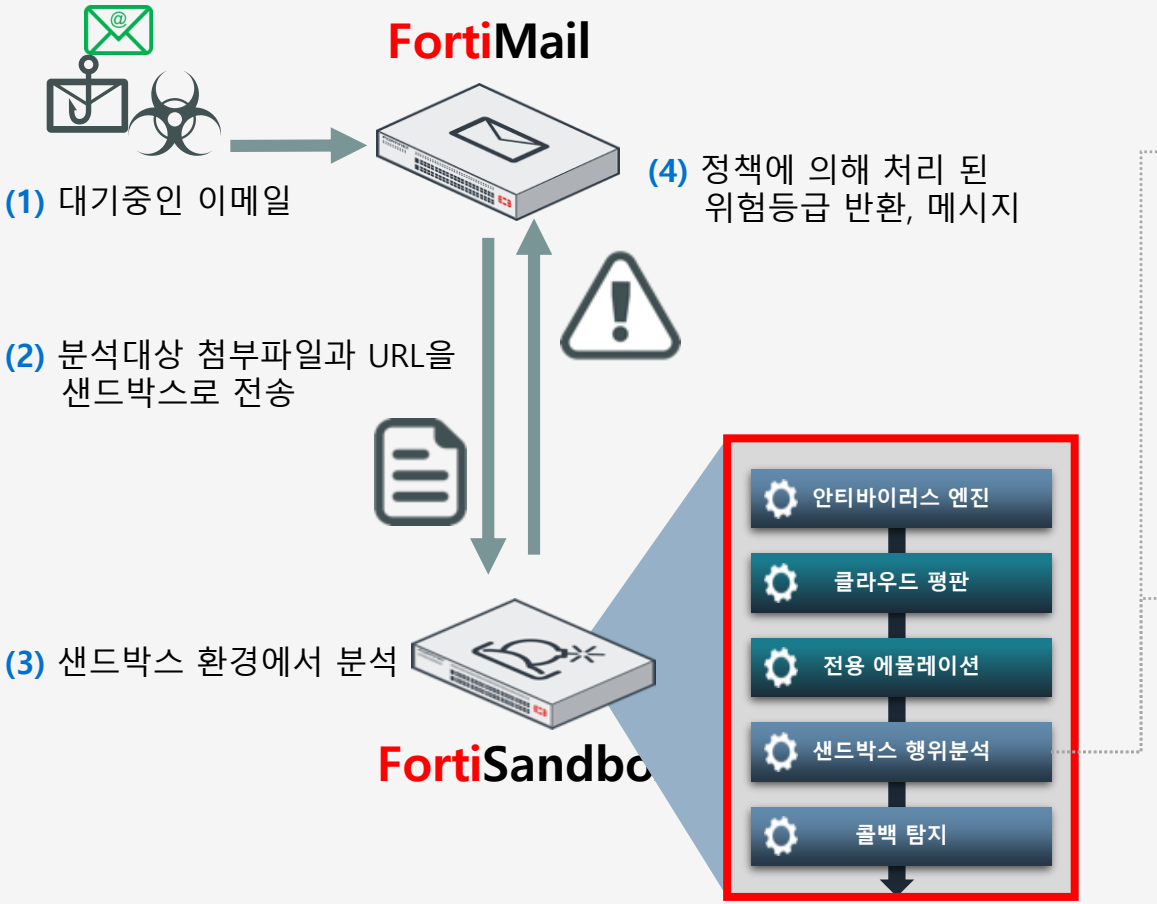
정상메일을 사칭한
악성메일 탐지

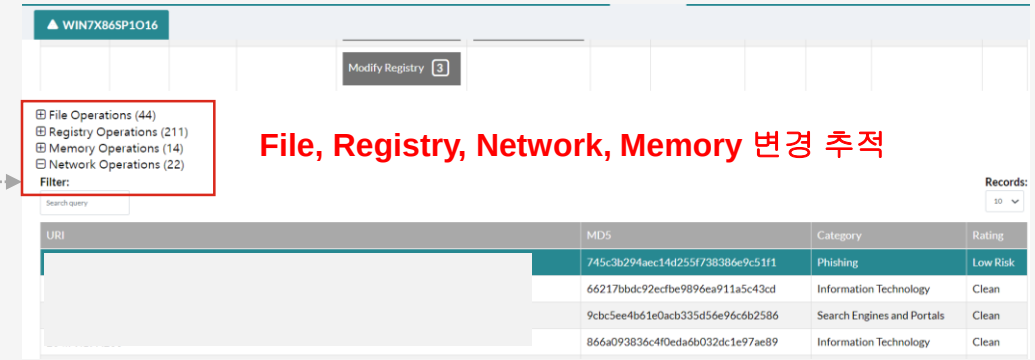
메일 본문의 URL을 클릭 시
격리된 공간에서 웹 실행

첨부파일에 포함된 유해 콘텐츠 제거

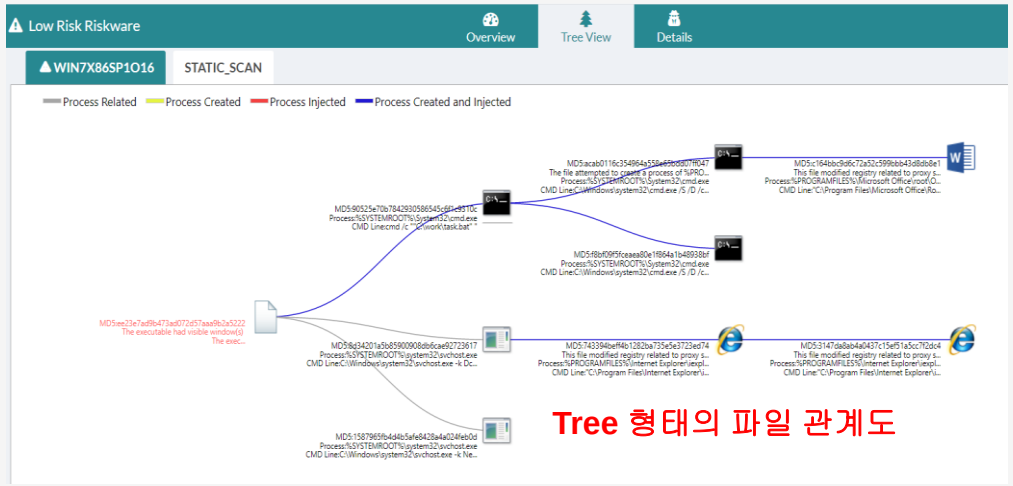
Fortinet Email ATP 주요 기능 – 1) Unknown 위협 탐지

샌드박싱을 통해 이메일 본문에 포함된 URL과 악성 첨부파일 탐지





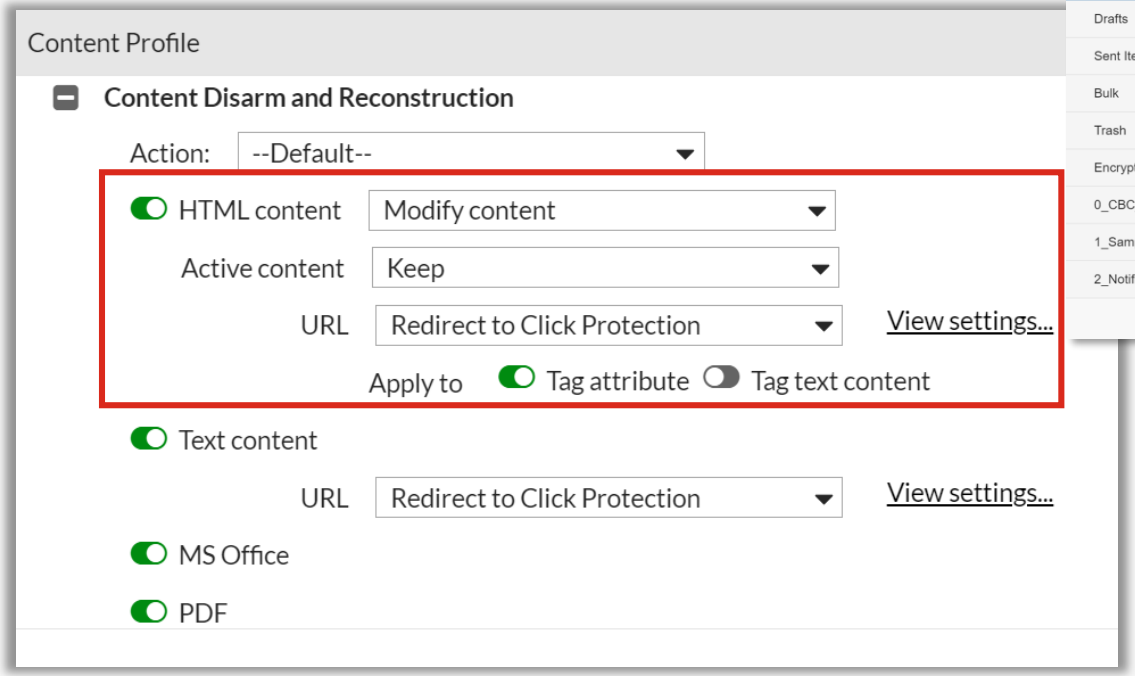
File, Registry, Network, Memory 변경 추적

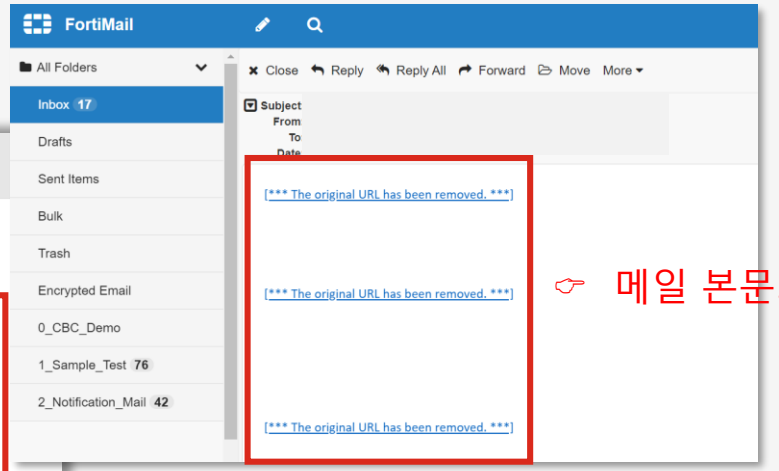


Tree 형태의 파일 관계도

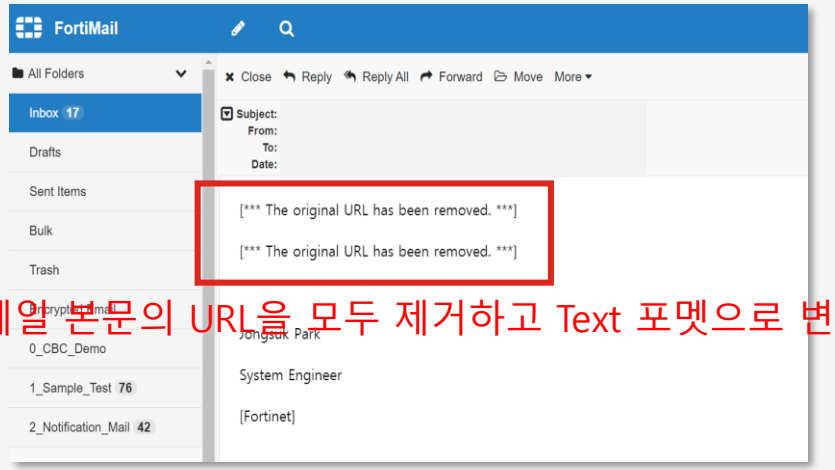
Fortinet Email ATP 주요 기능 – 2) URL Click Protection

이메일 본문에 포함된 URL을 제거 또는 텍스트로 변환하여 메일 발송





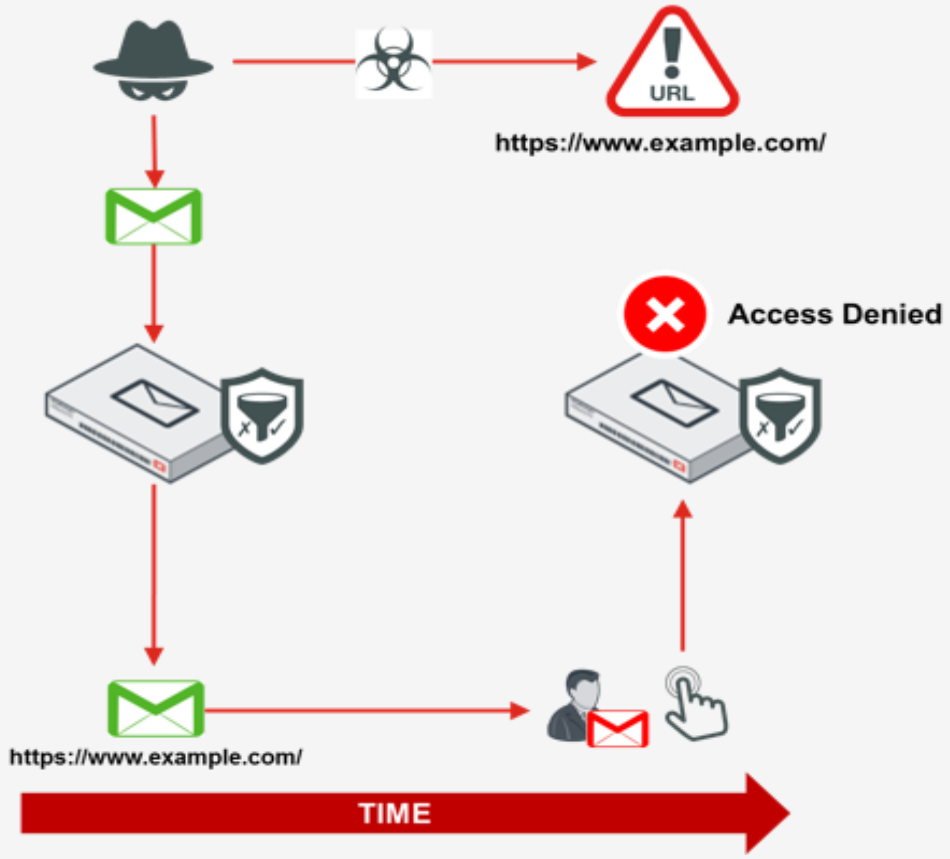
☞ 메일 본문의 URL을 모두 제거하여 메일 전달



☞ 메일 본문의 URL을 모두 제거하고 Text 포멧으로 변환하여 메일 전달

Fortinet Email ATP 주요 기능 – 2) Time of Click

메일 전달 시와 사용자가 본문의 URL을 클릭하는 시점의 시간차를 이용한 공격

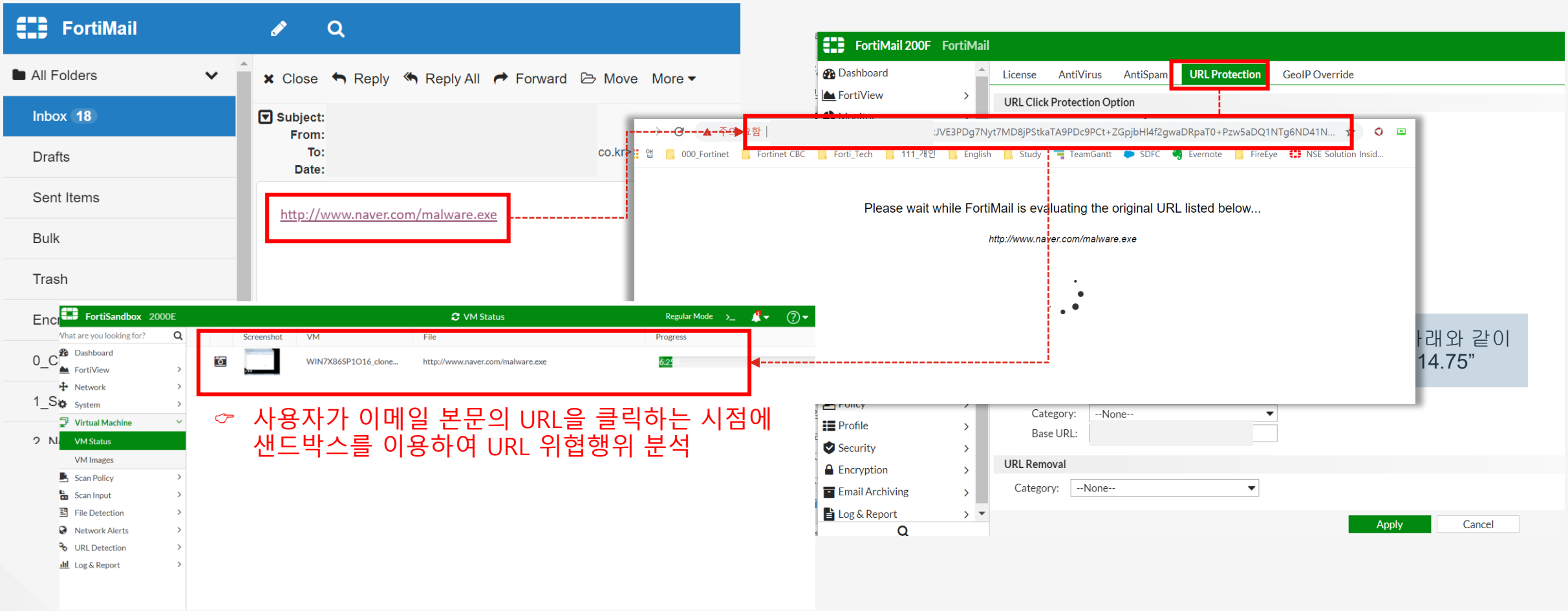


공격 특징

- 메일 발송 시 정상파일 or 유효하지 않은 URL을 이메일의 본문에 삽입
- 이메일 보안솔루션에서 검사 시 악성으로 확인되지 않아 정상적으로 메일 전달
- 특정 시간 후 파일 교체 or 악성파일을 업로드 하여 사용자 클릭 시점에 악성파일을 다운로드

Fortinet Email ATP 주요 기능 – 2) Time of Click

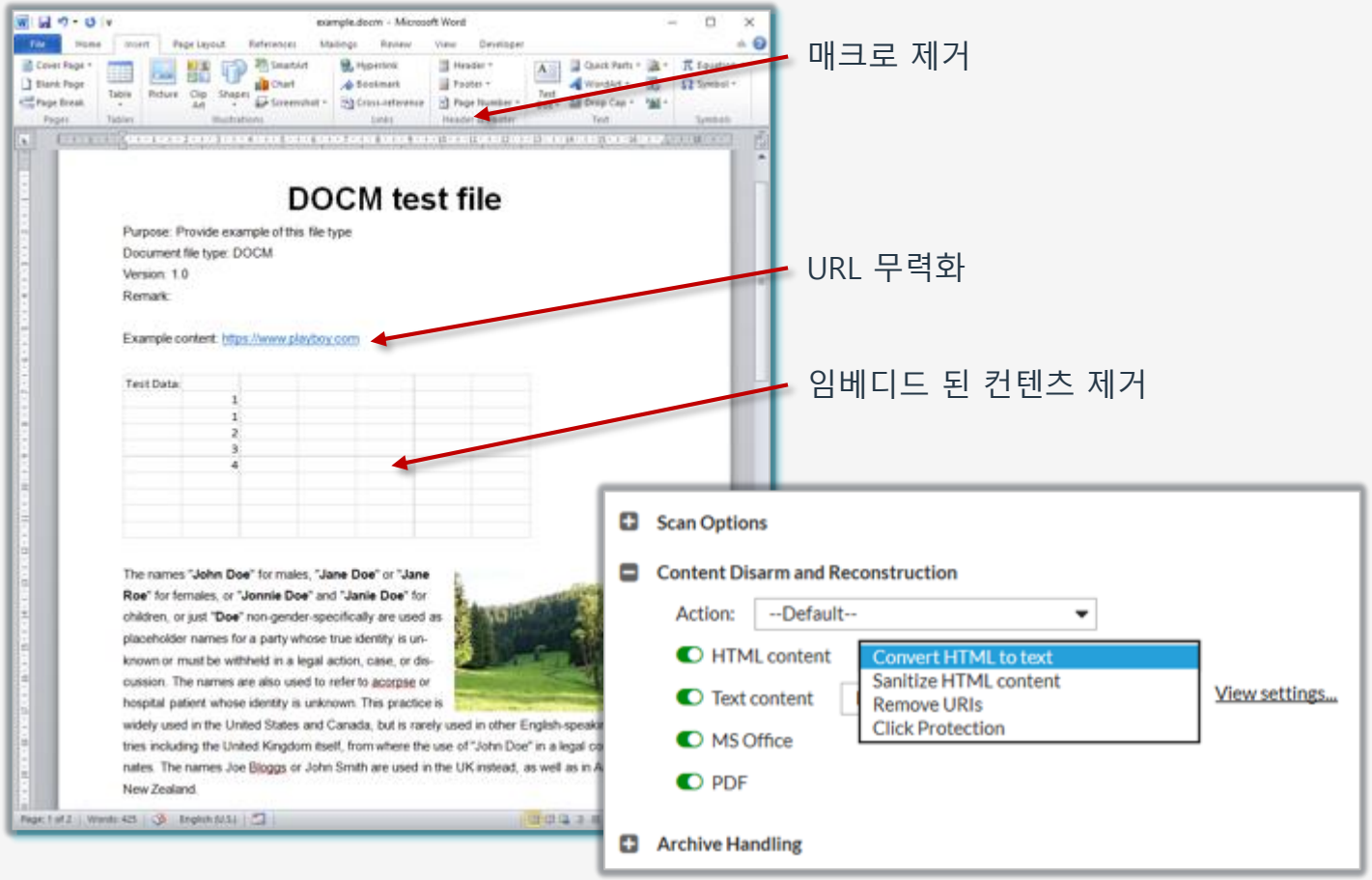
이메일 본문의 URL을 Rewrite한 후 사용자 클릭 시점에 샌드박스 분석



☞ 사용자가 이메일 본문의 URL을 클릭하는 시점에 샌드박스를 이용하여 URL 위협행위 분석

Fortinet Email ATP 주요 기능 – 3) 악성 콘텐츠 무해화 기술

CDR(Content Disarm and Reconstruction)

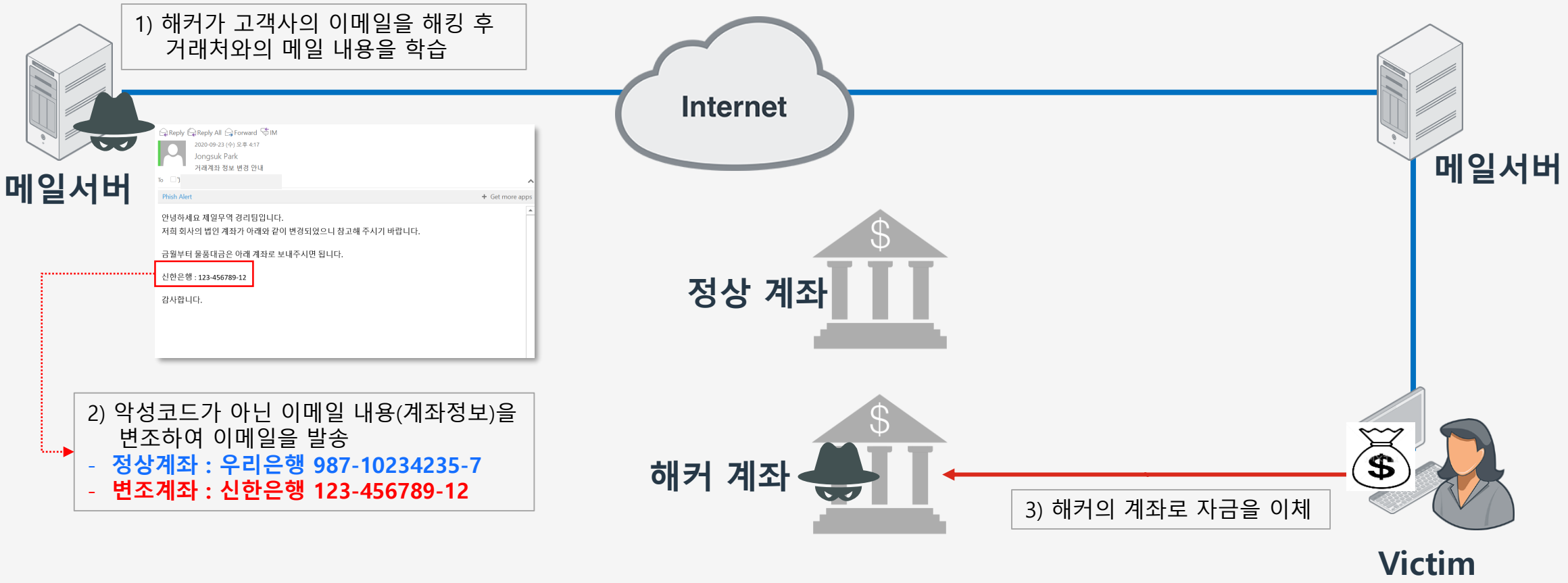


주요 특징

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

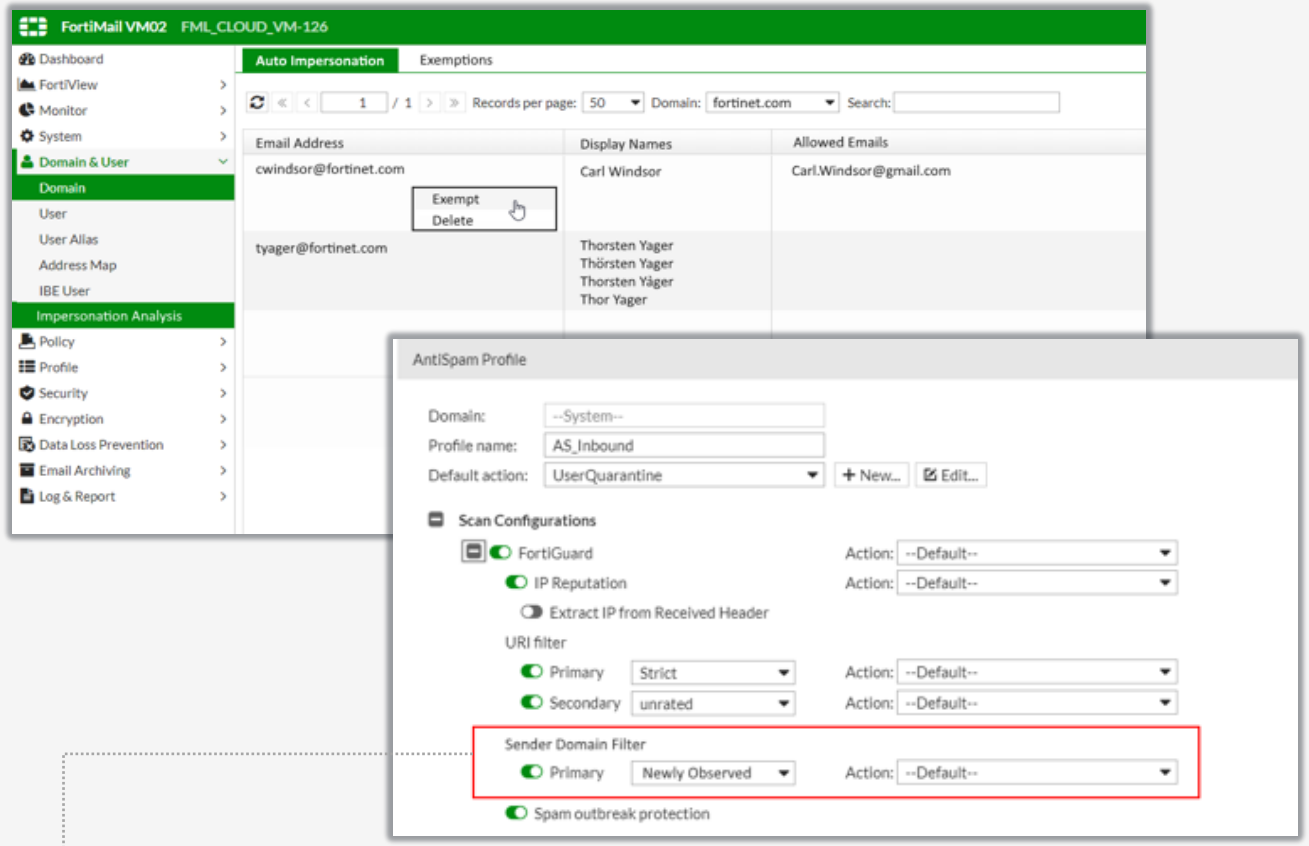
Fortinet Email ATP 주요 기능 – 4) 비즈니스 이메일 위협 차단

이메일 계정을 사칭하여 거래은행 변경 메일을 Victim User에게 발송



Fortinet Email ATP 주요 기능 – 4) 비즈니스 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

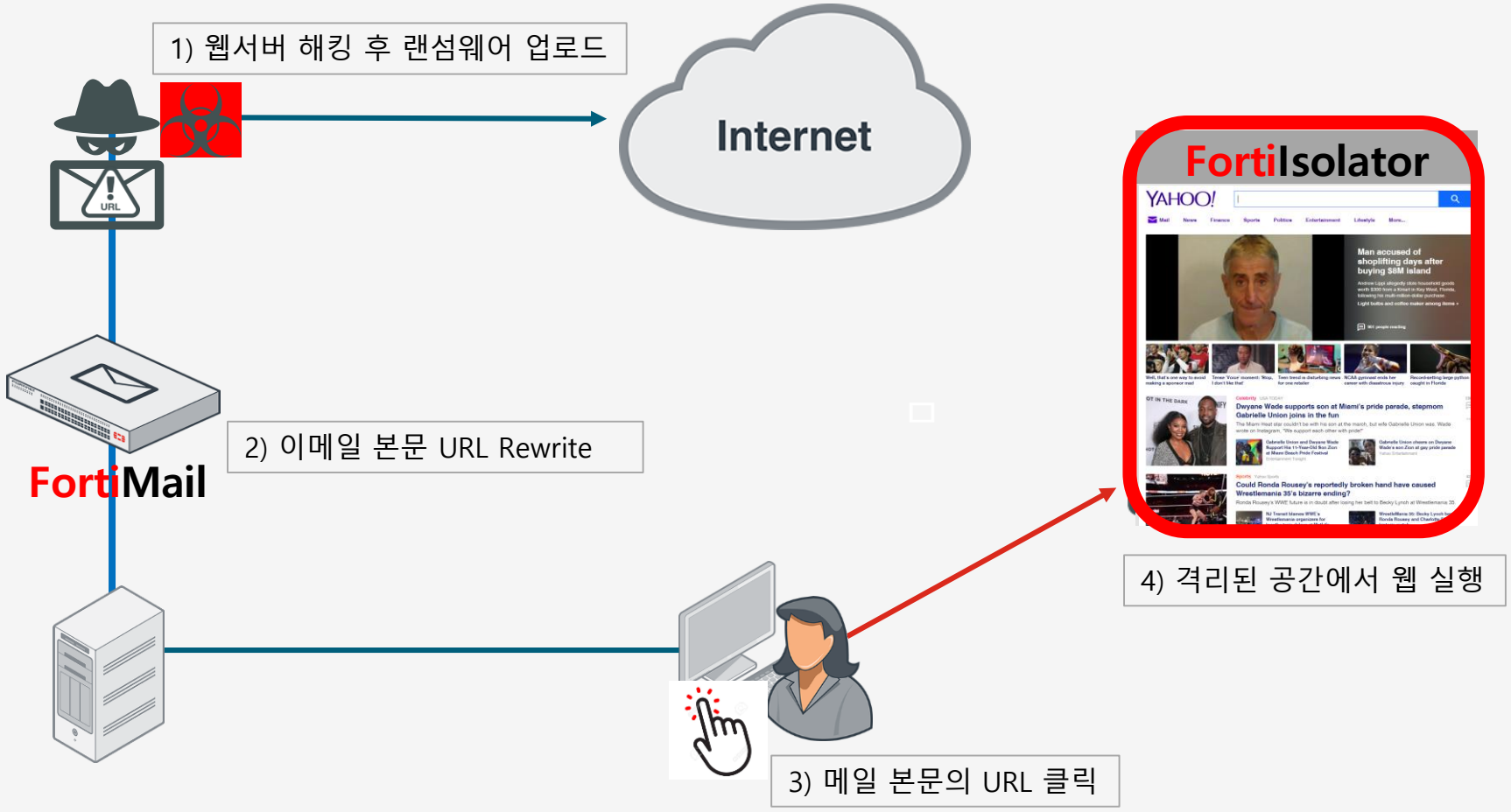
Fortinet Email ATP 주요 기능 – 4) 비즈니스 이메일 위협 차단

거래처의 이메일을 사칭하여 발송된 BEC 위협 탐지

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

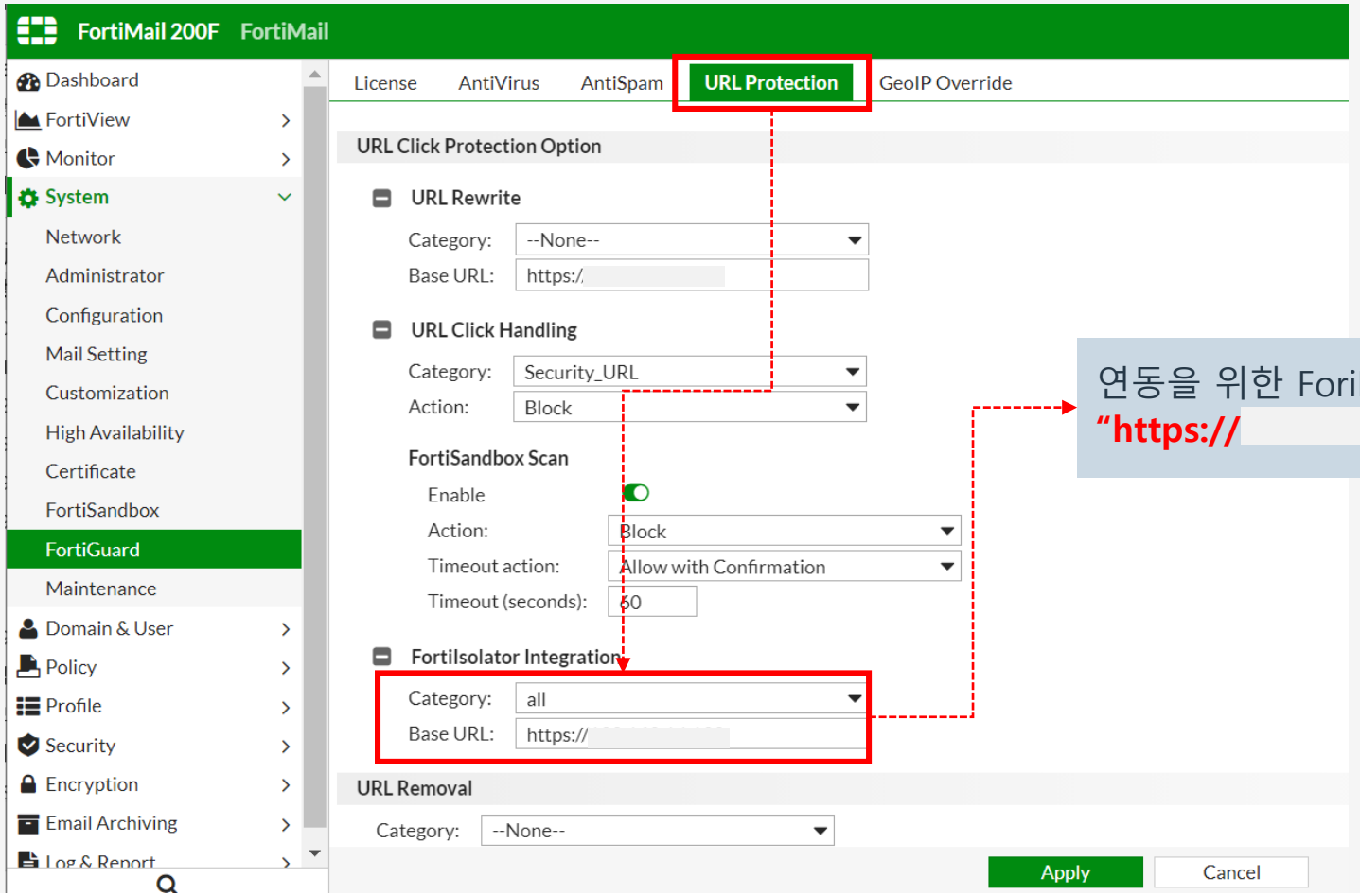
Fortinet Email ATP 주요 기능 – 5) Web Isolation

이메일 본문의 URL을 클릭 시 격리된 공간에 악성코드 Drive by Download



Fortinet Email ATP 주요 기능 – 5) Web Isolation

FortiIsolator의 Base URL 설정을 통해 격리된 공간에서 웹페이지를 실행

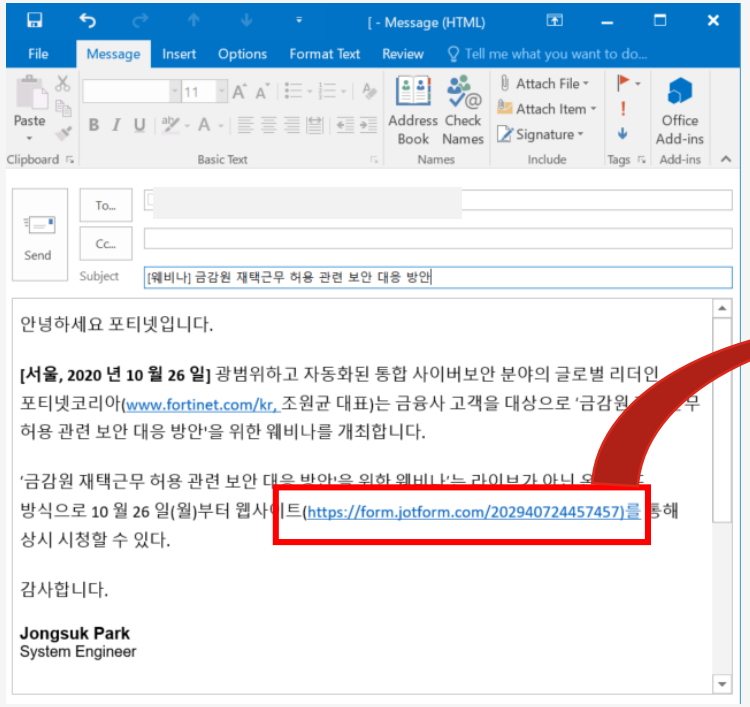


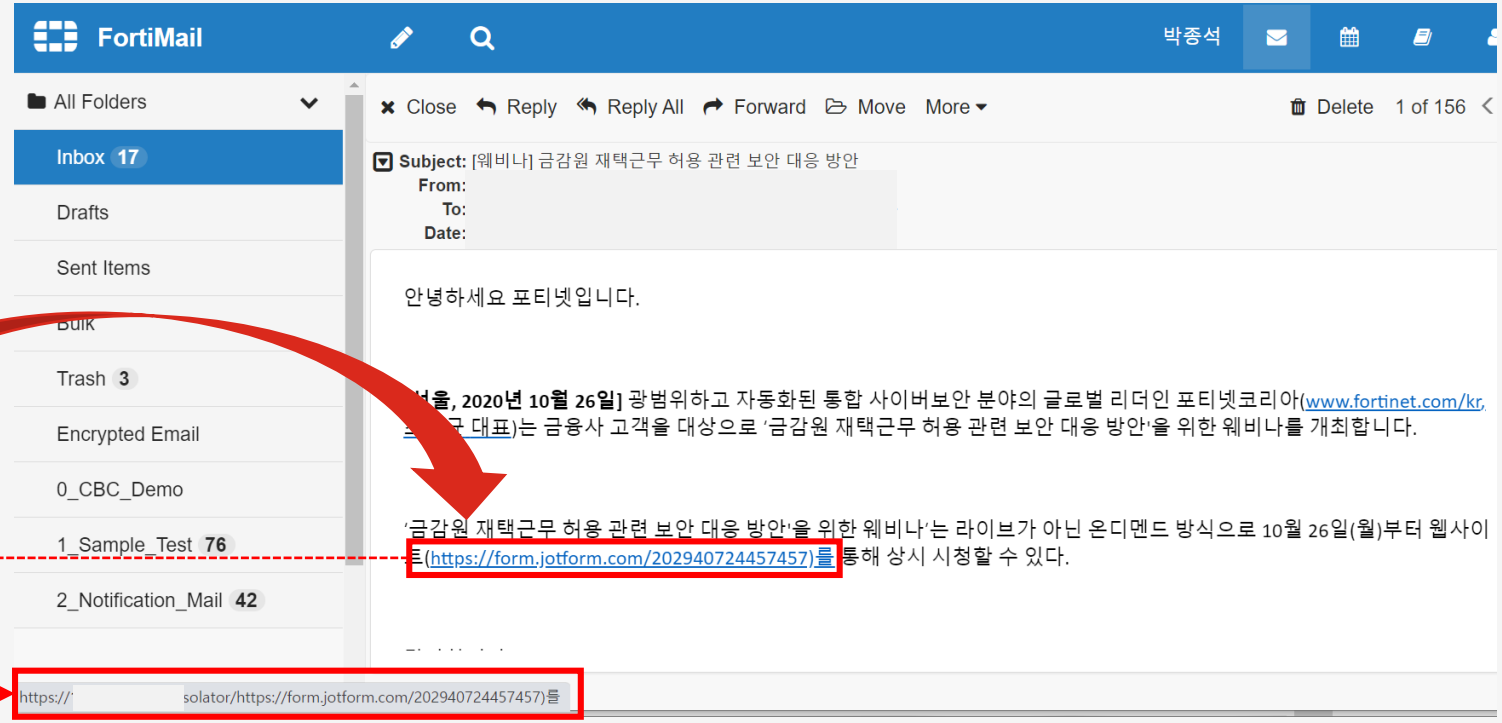
연동을 위한 FortiIsolator의 정보를 아래와 같이 Base URL로 입력

"https://"

Fortinet Email ATP 주요 기능 – 5) Web Isolation

이메일 본문의 의심 URL을 클릭 시 격리된 공간에서 웹페이지를 실행





- 공격자 발송 메일

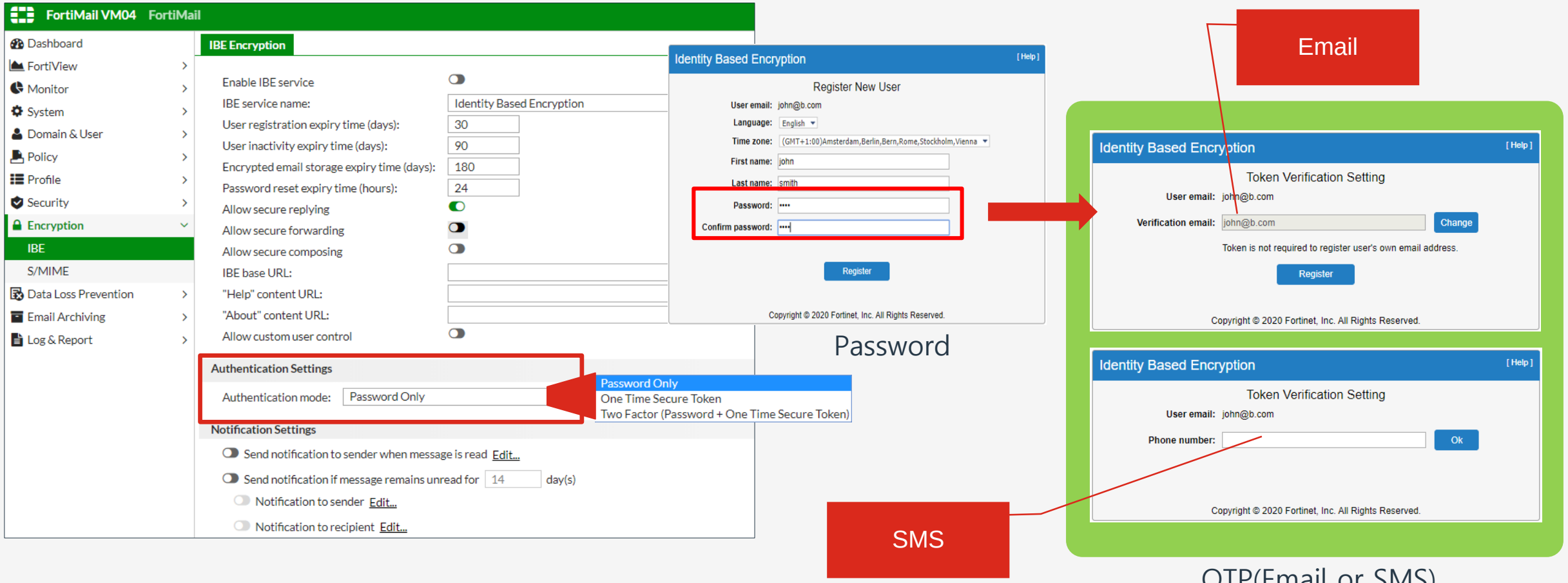
- 악성파일이 Drive by Download 되는 URL을 사용하여 이메일 발송

수신된 메일의 URL을 확인 시 아래와 같이 URL이 Rewrite 되어 있다.

"https:/ /isolator/https://cdn.jotfor.ms/202940724457457"

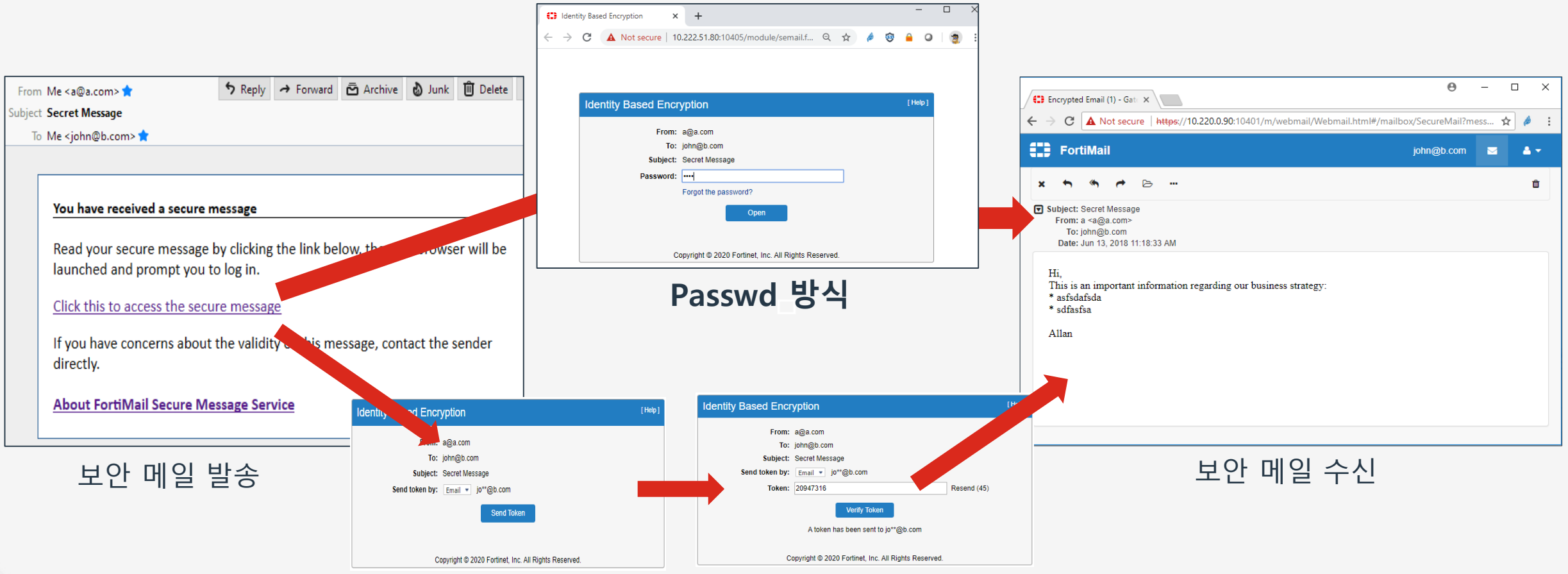
Fortinet Email ATP 주요 기능 – 6) 개인 보안 메일

IBE(Identity Based Encryption) Authentication 설정



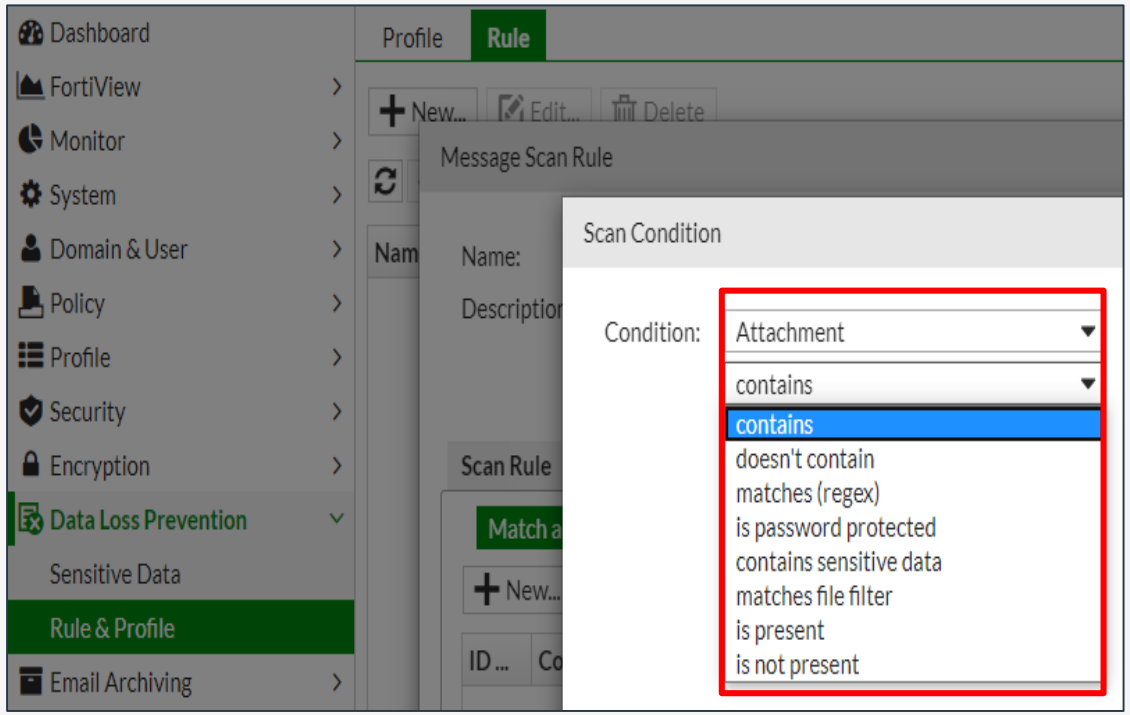
Fortinet Email ATP 주요 기능 – 6) 개인 보안 메일

IBE(Identity Based Encryption) 메일 수신

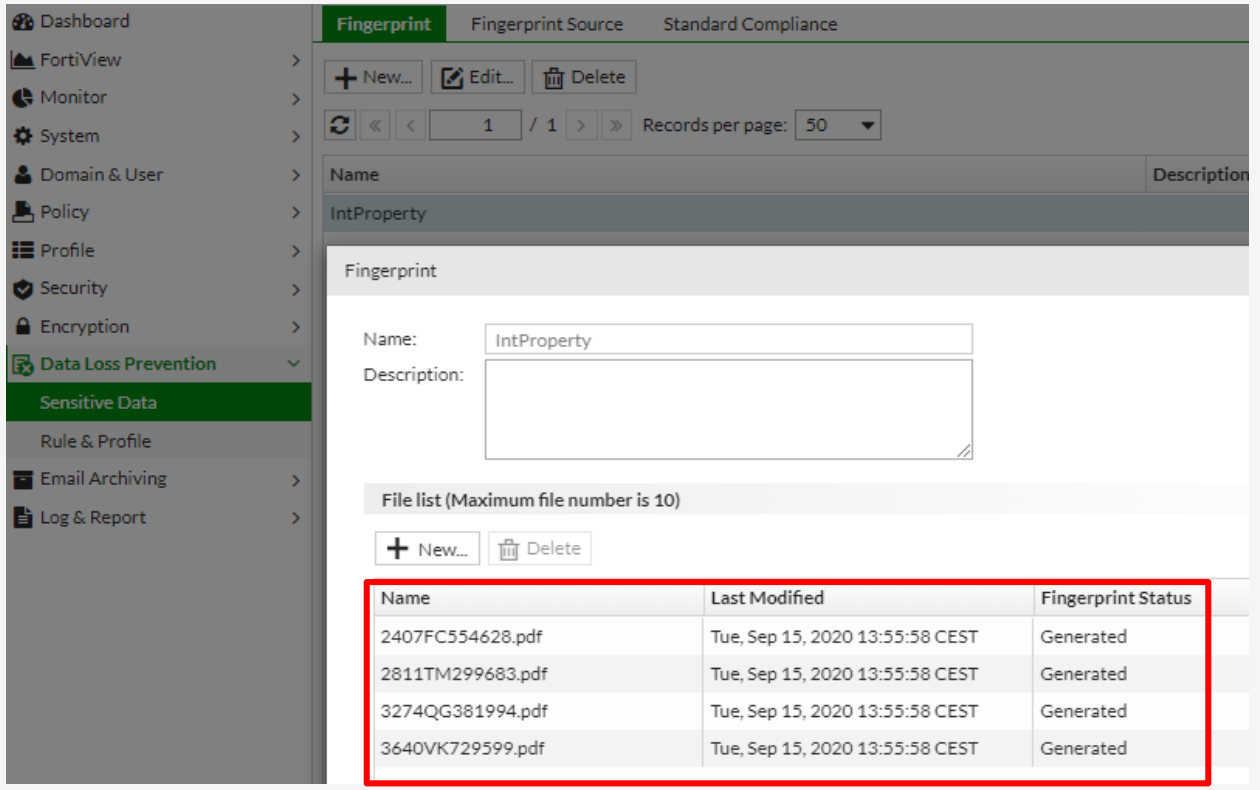


Fortinet Email ATP 주요 기능 – 7) 데이터 유출 방지

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



DLP 검사조건

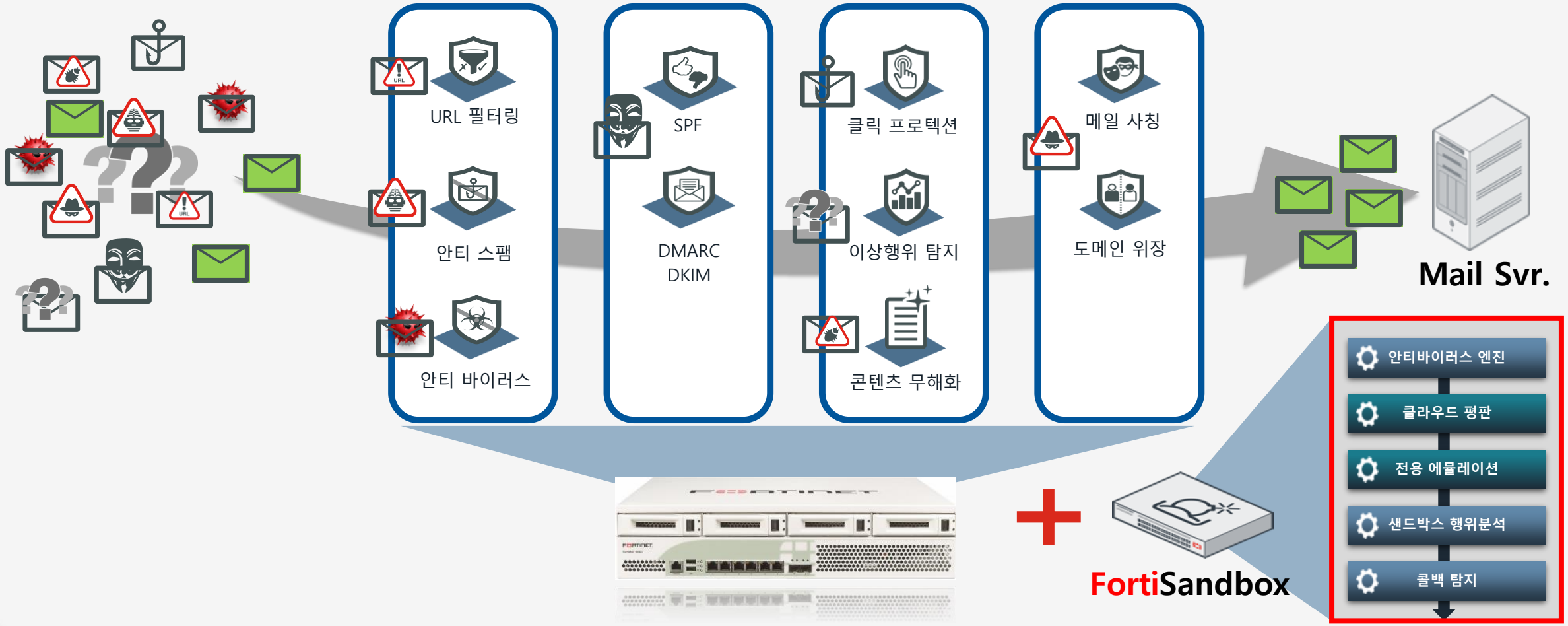


Fingerprint 등록을 통한 중요 문서유출 탐지

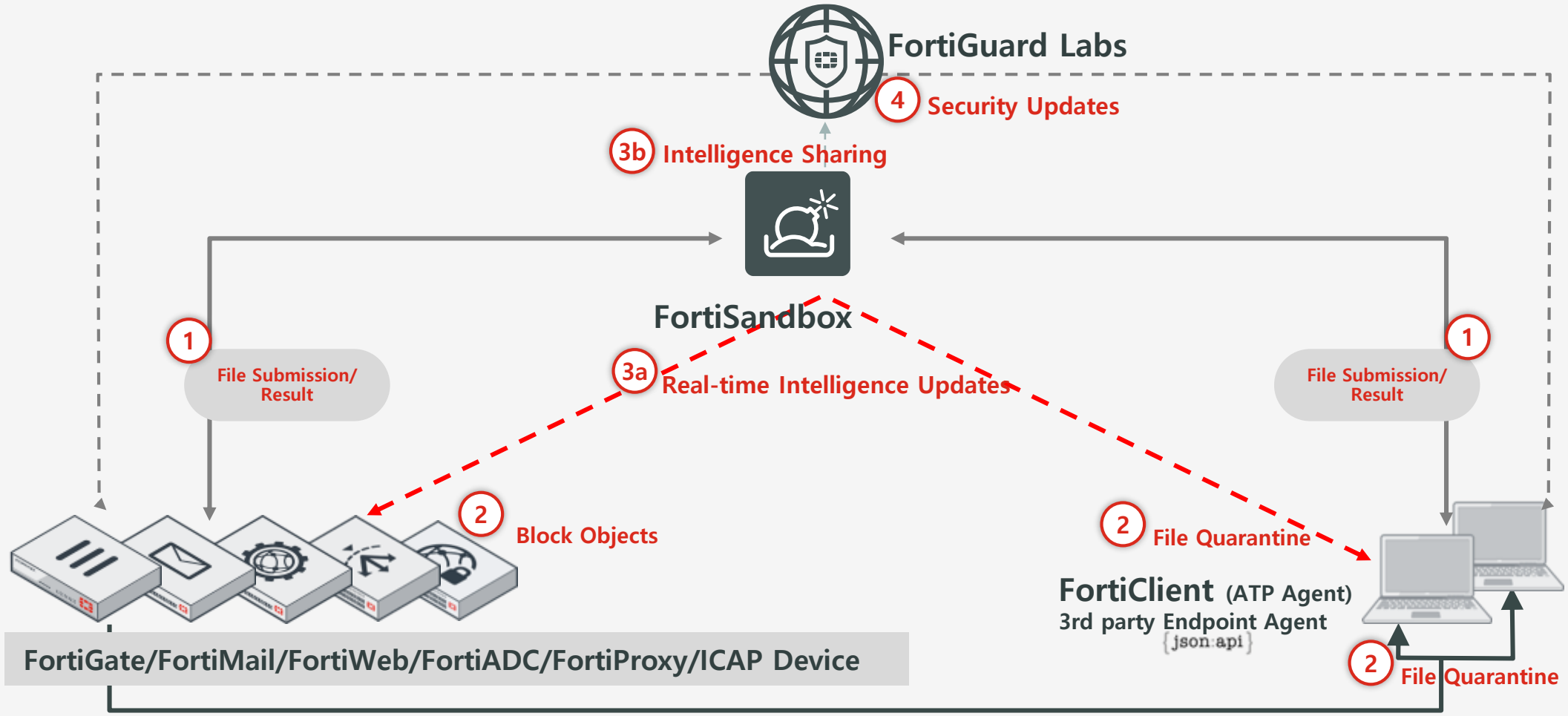
포티넷 이메일 ATP

FortiMail – 보안 이메일 게이트웨어

단일 솔루션으로 이메일로 유입되는 다양한 형태의 위협을 제거

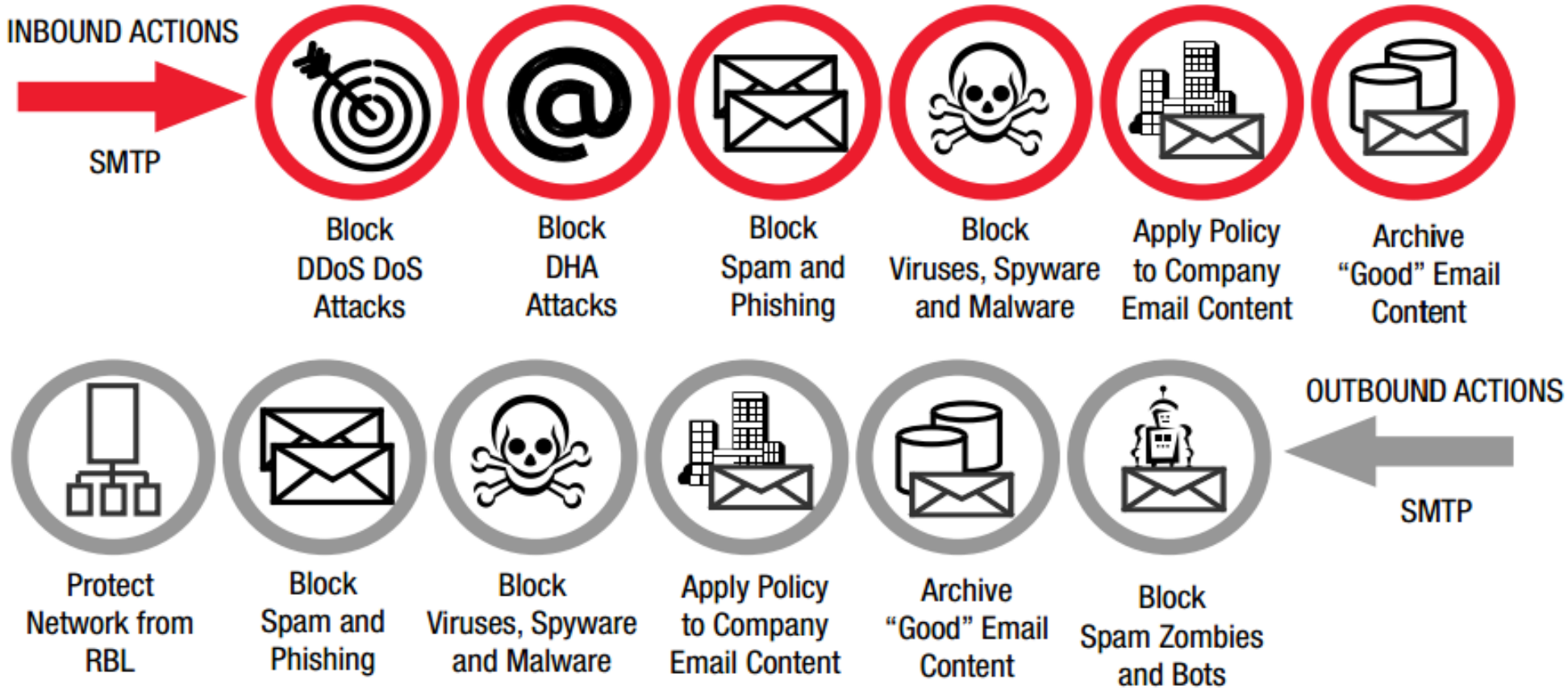


FortiSandbox 분석 정보 공유 및 자동 차단



Fortinet Email ATP 주요 기능

Inbound 이메일 뿐만 아니라 Outbound 이메일에 대한 검사 수행



Fortinet Email ATP

최신 위협을 대응하기 위한 Fortinet 이메일 ATP 제품의 특장점

- 단일 솔루션으로 이메일로 유입되는 다양한 위협들을 제거(AS, AV, CDR 등)
- Fortinet Security Fabric 연동을 통해 실시간 Intelligence 공유 및 차단
- 이메일을 통해 유입되는 URL 탐지(Rewrite, Remove, Time of Click)
- Inbound 뿐만 아니라 Outbound 메일에 대한 검사 수행
- BEC(Business Email Compromise) 위협 탐지
- IBE(Identify Based Encryption) 기능 제공
- 사용자별 라이선스 없이 하드웨어/소프트웨어 성능에 따른 라이선스 정책 적용

BMW i Motorsport
Official Partner