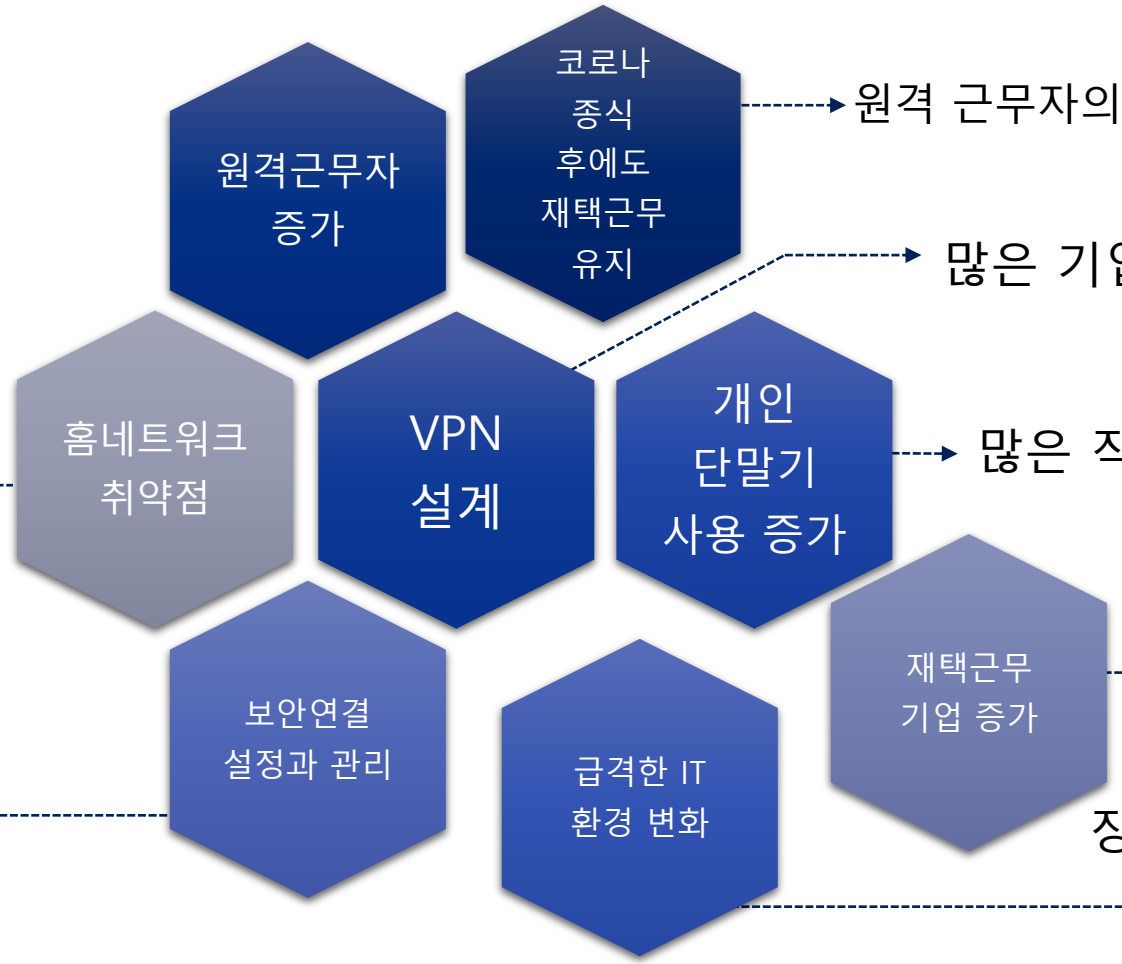
# 금융권 원격 근무 확대 실시에 따른 재택근무 보안 대응 방안

포티넷 코리아
박종석 이사, 김기덕 부장

# COVID19로 인한 IT 환경 변화

**패치가 되지 않은 홈네트워크**에 연결된 다른 장치들이 **공격자의 주요 표적**이 됨




원격 근무자의 50% 이상이 코로나 이후에도 재택근무를 할 것을 예상

많은 기업들이 **VPN 연결 볼륨**을 관리하도록 설계되지 않음

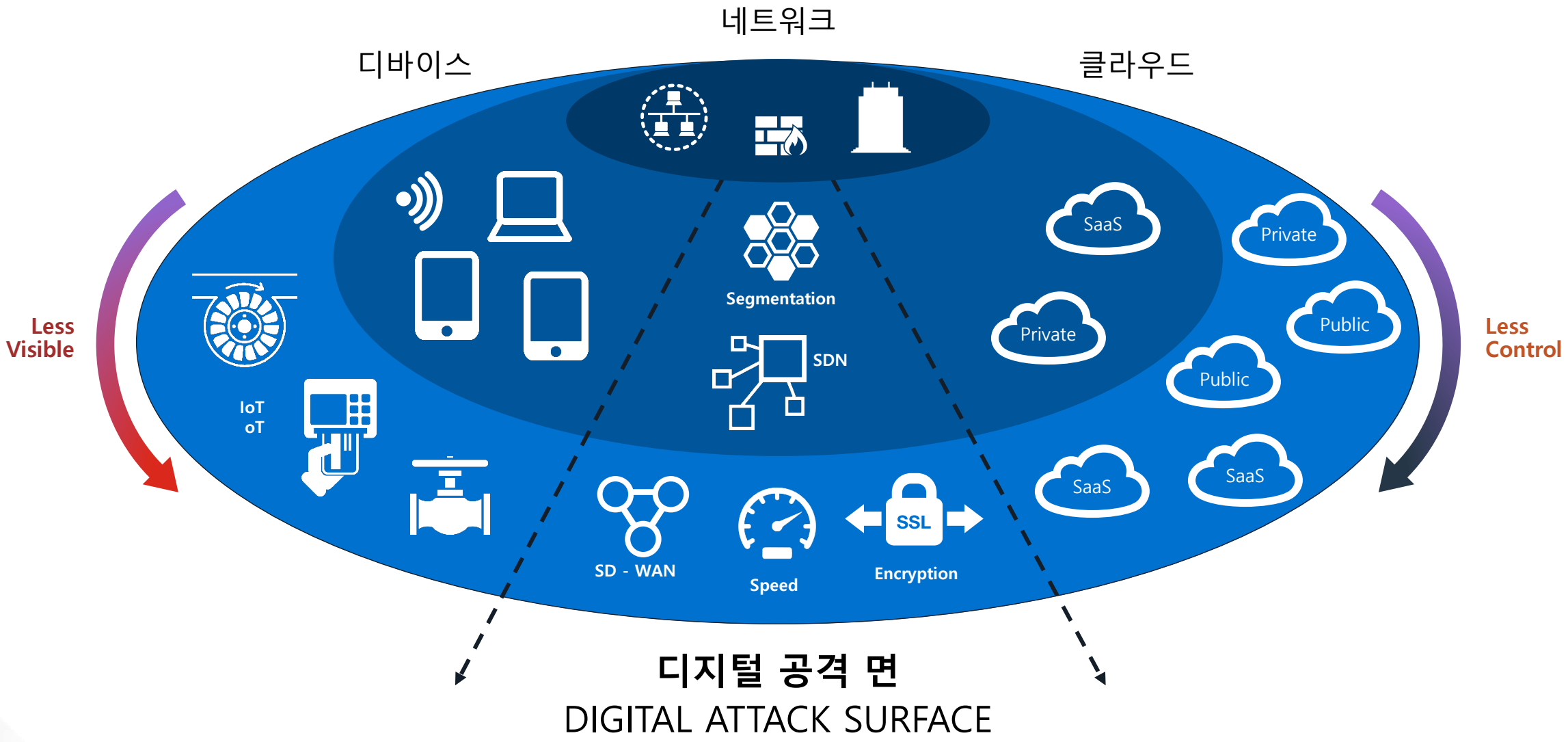
많은 직원이 **개인 단말기를 사용**하여 회사 네트워크에 접속

전세계 기업의 2/3 가량이 재택근무

장기적인 계획없이 **짧은 시간동안 IT 보안 환경이 변화**

포티넷 조사결과 응답자의 32%가 **보안연결 설정과 관리**가 재택근무 전환 시 가장 어렵다고 응답

# 2021년 디지털 공격 면의 급격한 증가 예상



# 금융권 원격 근무 규정 개정에 따른 보안 솔루션 구성 방안

# 전자 금융 감독 규정 시행 세칙 개정(2020.10)

금융생활에 필요한 모든 정보, 인터넷에서 「파인」 두 글자를 쳐보세요

"금융은 튼튼하게, 소비자는 행복하게"

## 보 도 자 료

| 보도 | 2020. 9. 18.(금) 조간 | 배포 | 2020. 9. 17.(목) |
|---|---|---|---|
| 담당부서 | IT·핀테크전략국 | 장성옥 부국장(3145-7415), 변남주 선임(3145-7424) | |

**제 목 : 금융회사의 상시 재택근무가 가능해집니다.**

**(「전자금융감독규정시행세칙」 개정 예정 )**

◈ 금융회사가 **신속**하고 **안전**하게 **재택근무로 전환**할 수 있도록 **망분리 규제**를 **개선**합니다.

○ 금융회사의 **상시 재택근무**를 위한 **원격접속을 허용하였습니다.**

○ 다만, 재택근무로 인해 발생 가능한 **보안사고**를 **사전예방**하기 위하여 원격 접속 시 준수하여야 하는 **정보보호 통제사항**을 **강화**하였습니다.

### 1. 개 요

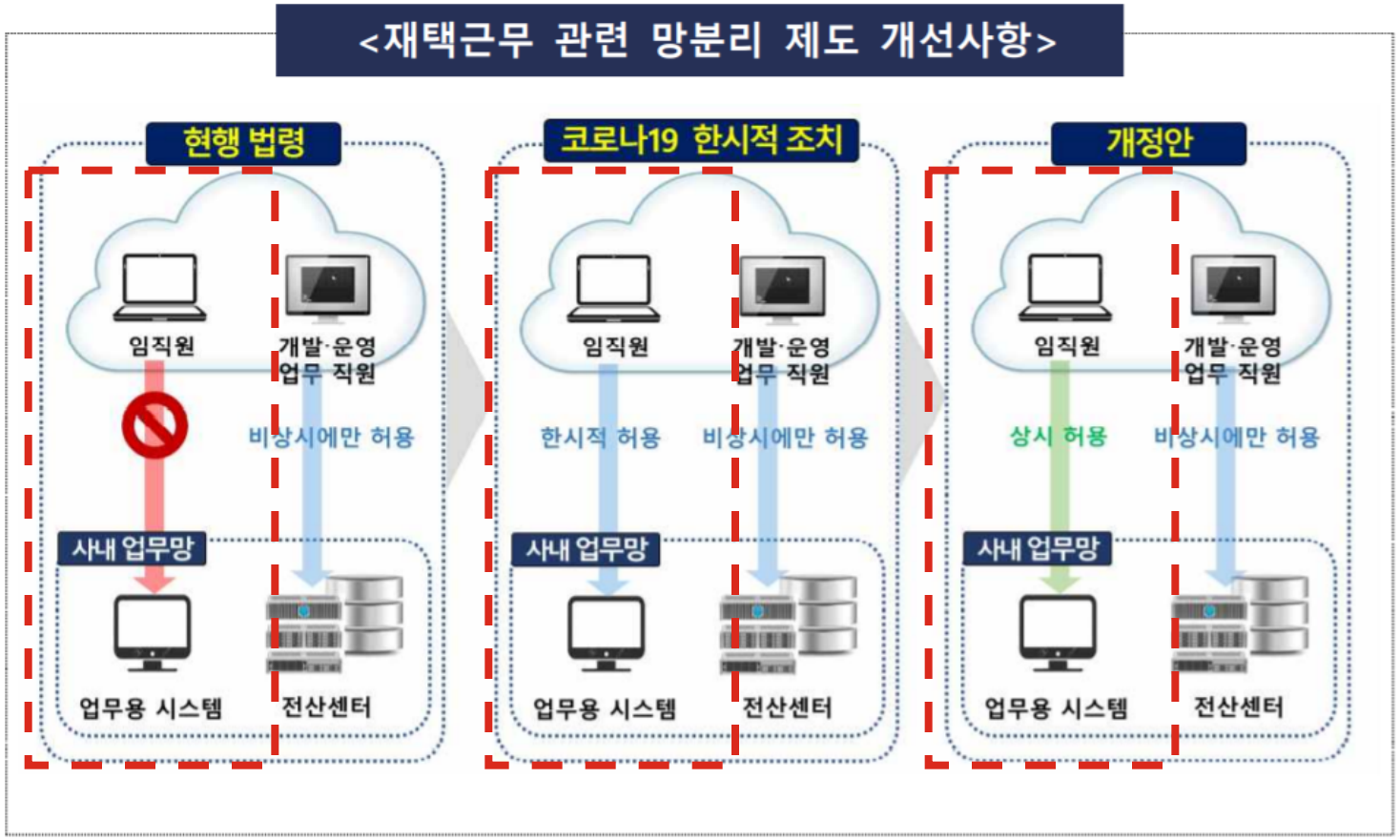
□ 금융회사는 전자금융거래법상 **망분리 규제**로 인하여 **재택근무**를 위한 **원격접속이 사실상 불가능**하였음

○ 장애·재해 발생 등 **비상상황 시** 신속한 조치를 위하여 **전산센터**에 대해서만 **예외적**으로 **허용**하고 **일반 임직원의 경우는 불가**

**<망분리 제도>**

* 외부 사이버공격, 정보유출 등을 방지하기 위하여 **금융회사의 통신회선을 업무용(내부망), 인터넷용(외부망)으로 분리**하여 운영토록 하는 제도 ('13.12.3)

- **(물리적 망분리)** 통신망을 물리적으로 업무용과 인터넷용으로 분리하고 **별도 PC 사용**하는 것으로 **전산센터에 적용**
- **(논리적 망분리)** 통신망을 소프트웨어적으로 업무용과 인터넷용으로 분리하고 **논리적으로 분리된 PC**를 사용하는 것으로 전산센터 외 **일반업무 환경에 적용**



# 전자 금융 감독 규정 시행 세칙 개정(2020.10)

## 망분리 대체 정보보호통제

- 공통 통제 사항
  - 외부 → 내부 **전송 자료에 대한 악성 코드** 검사(지능형 해킹(APT))
  - 전산 자료의 외부 전송에 대한 정보 유출 탐지/차단/사후 모니터링
- 메일 시스템
  - 메일 **본문/첨부파일에 대한 악성코드** 검사
  - 메일을 통한 정보 유출 탐지/차단/사후 모니터링
- 업무용 단말기
  - 관리 권한, 프로그램, 저장 자료 암호화 관리
- 원격 접속
  - **암호화된 통신** 회선
  - 간접/직접 접근 내부망 접속 시, **인터넷 접근 통제**
  - **이중 인증**을 통한 사용자 접근 통제
  - 파일 접근 관리 외, 다수

**보안팀의 고려 사항은 증가!**

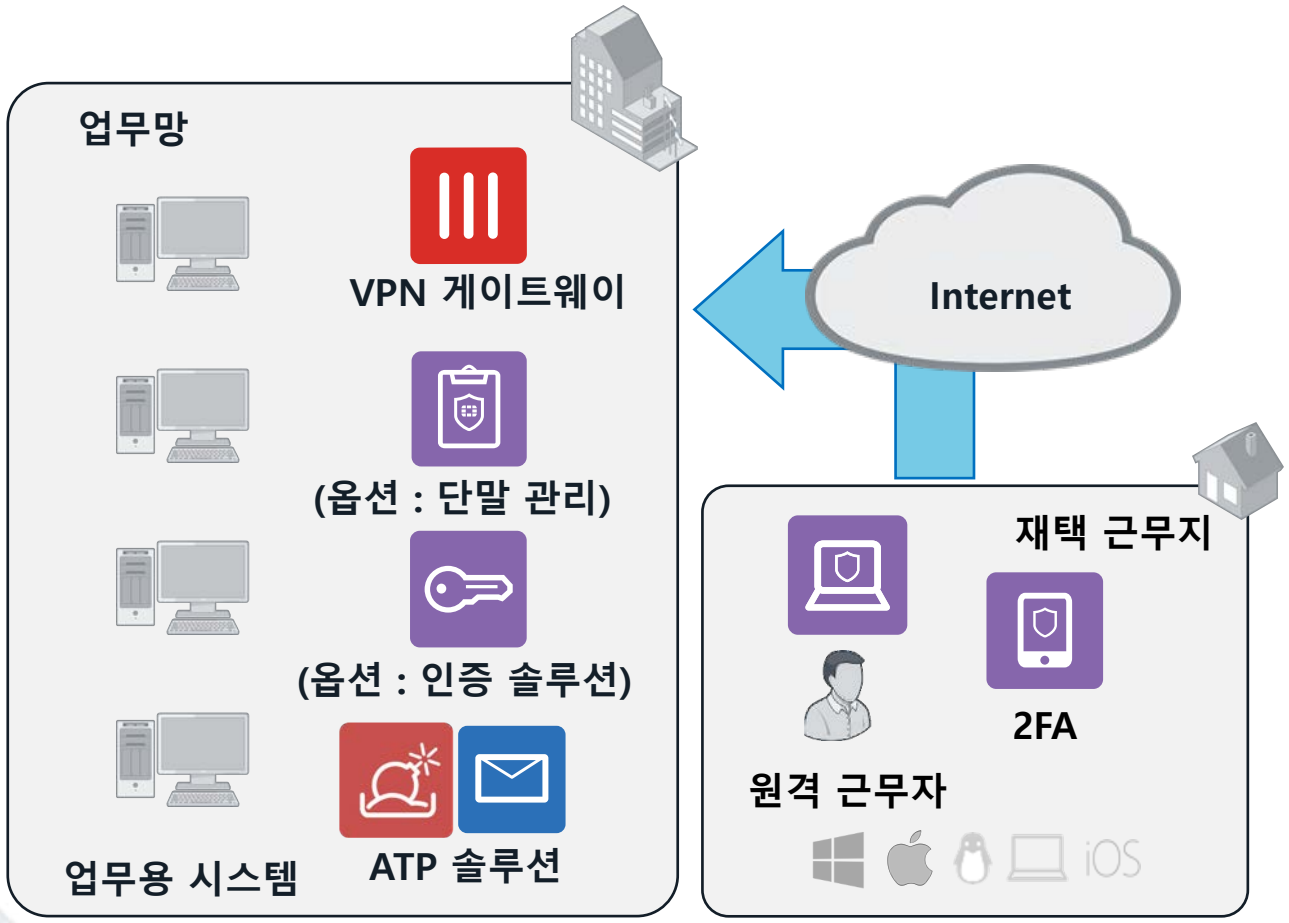
# 전자 금융 감독 규정 시행 세칙 개정(2020.10)

## 원격 접속 : 직접 연결 방식과 간접 연결 방식

<직접 연결 방식 예시>


<간접 연결 방식 예시>

# 원격 근무자를 위한 포티넷 대응 솔루션




**VPN**

- **IPsec, SSL VPN 게이트웨이**
- 재택 근무자 접근 제어
- 추가 제안 : 외부 위협으로 부터 IPS / AV 보안 기능 수행

**단말기 에이전트**

- **단말기의 VPN 에이전트**
- 관리 서버 및 VPN 게이트웨이를 통한 접근 정책 배포
- 웹필터/AV등 보안 기능 제공(옵션)

**이중인증**

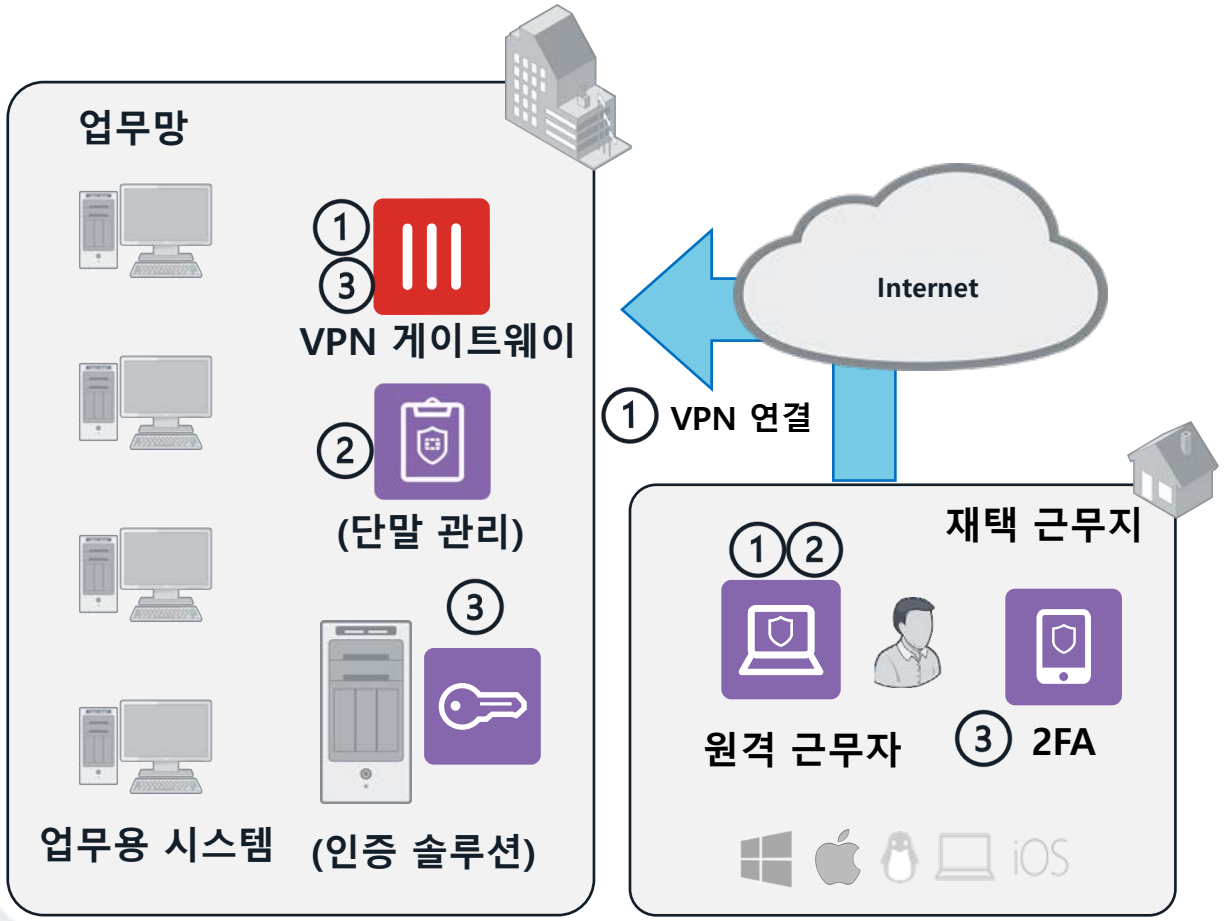
- 단말기 에이전트의 (VPN)접근 요청에 대한 **이중 인증** 수행
- 모바일 토큰, 하드웨어 토큰

**ATP 솔루션**

- 외부 유입 파일 멀웨어 감염 여부 검사
- Zero Day Attack 탐지
- 이메일을 통한 외부 유입 파일/멀웨어 제어

# 포티넷 재택 근무 솔루션 구성 방안

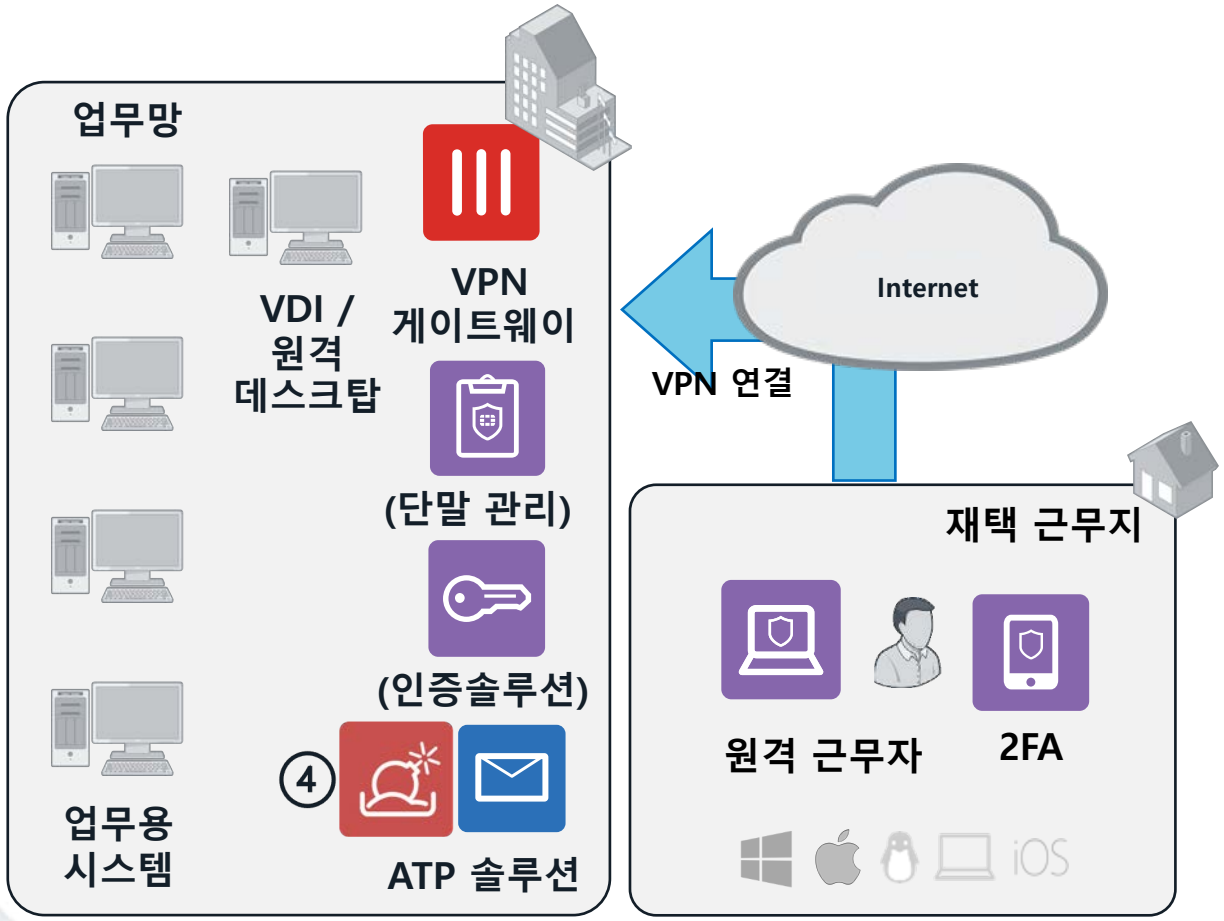
## 단계별 구성 방안




- 직접/간접 접근 방식 공통으로 암호화된 업무 채널 형성 필수
- **VPN 단말기 에이전트**를 사용하여 업무망 접근 시, **인터넷 엑세스 제어**
  - MS 윈도우, Mac OS, Linux등 여러 OS 지원
  - **사용자 ID와 비밀번호 인증**
  - 단말기 **에이전트 관리 서버**를 통한 접근 제어 정책 배포
- 이중 인증을 위해 포티넷의 인증 솔루션(옵션 : FortiAuthenticator)와 포티넷 **모바일 토큰을 통해 이중인증**(2FA) 지원(유료)

# 포티넷 재택 근무 솔루션 구성 방안

## ATP 위협 방어 구성




- 직접/간접 접근 방식에 활용
- 샌드 박스/이메일 게이트웨이를 통해 **알려지지 않은 위협**에 대한 업무 시스템 보호
- 전송되는 파일에 대한 지능형 공격 탐지/위협 정보 전파
- 2FA를 통한 사용자 인증
- 포티넷의 **단말기 에이전트를 통한 인터넷 접근 제어**

# 원격 근무 환경 변화에 따른 추가 보안 고려 사항

# 증가하는 위협 대응의 어려움

## 분석 시간 지연


- Zero-Day 위협 증가
- 위협 탐지까지 시간 소요
- 샌드박스 분석 시간 소요

## 자동 차단 지연

- 미러링 구성 장비 증가
- 탐지룰 검증이 필요한 솔루션
- 탐지만 가능한 일부 보안솔루션

## 전문가 부족

- 악성코드분석 전문가 부족
- 침해사고대응 전문가 부족
- 보안 엔지니어 부족

# AI 기반 버츄얼 보안 분석가 - FortiAI

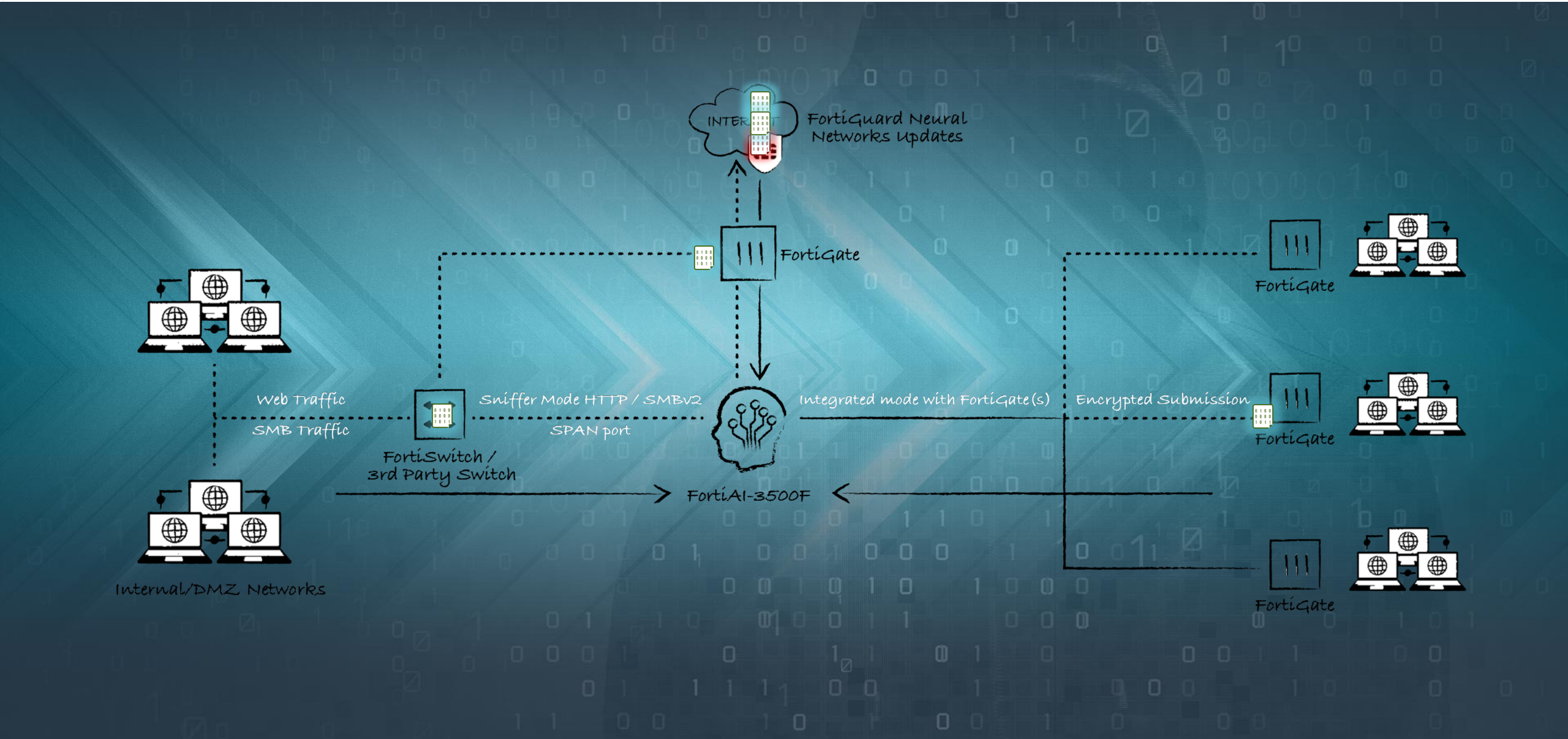
## 고도화된 학습

최고의 보안 전문가가 분석 하는 것처럼 악성코드를 탐지 및 차단 "AI" 기능을 사용함

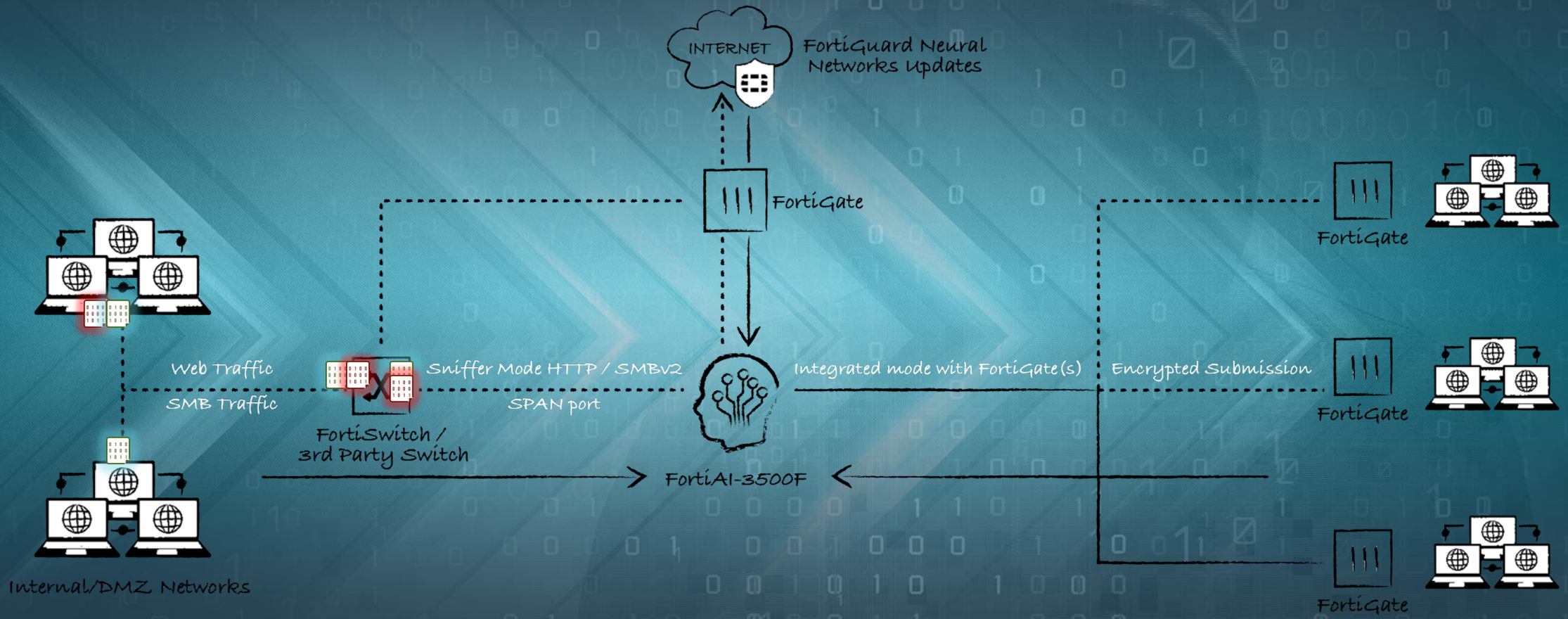
## 분석 시간 단축

분석 시간을 몇 분에서 몇 초 단위 미만으로 단축

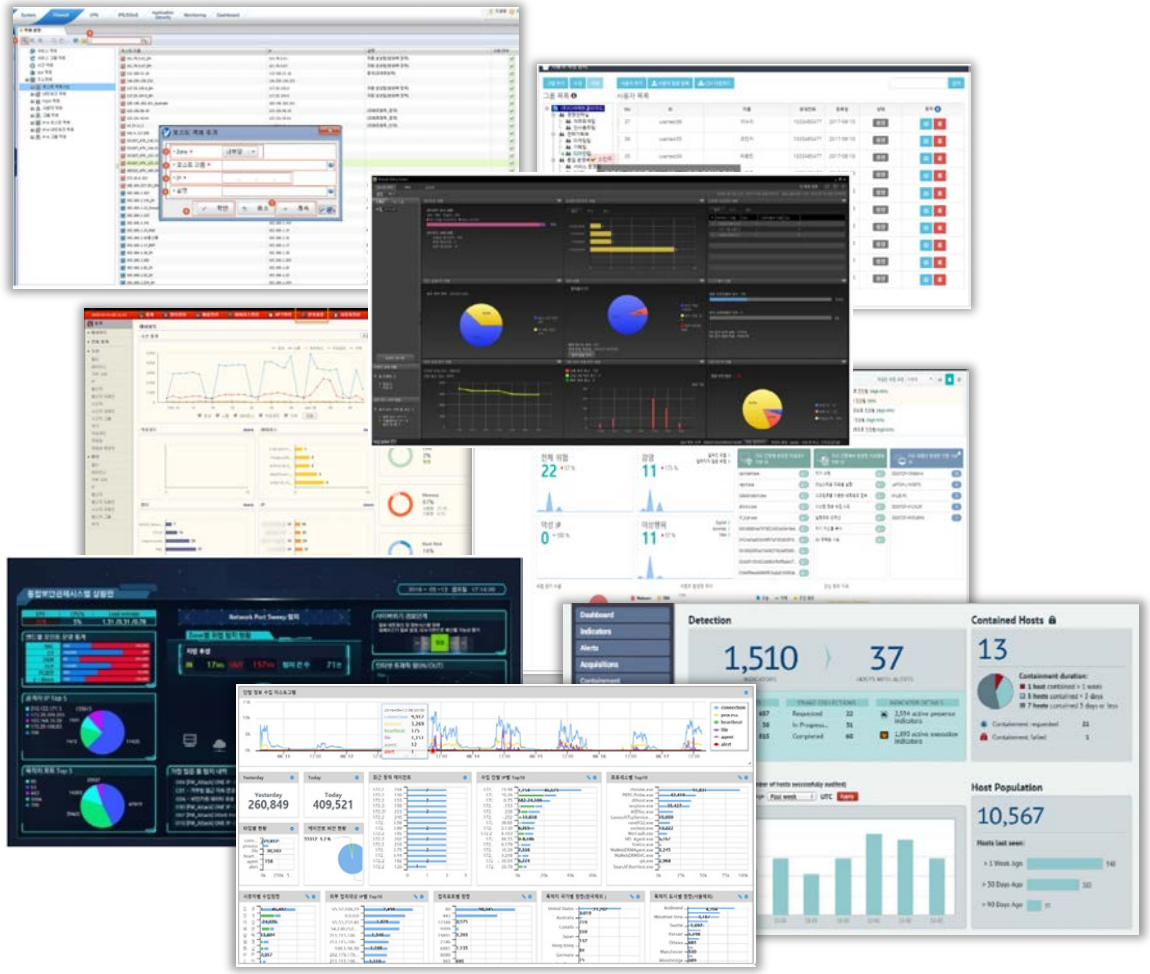
# VPN을 통해 내부 네트워크로 유입되는 악성파일 차단

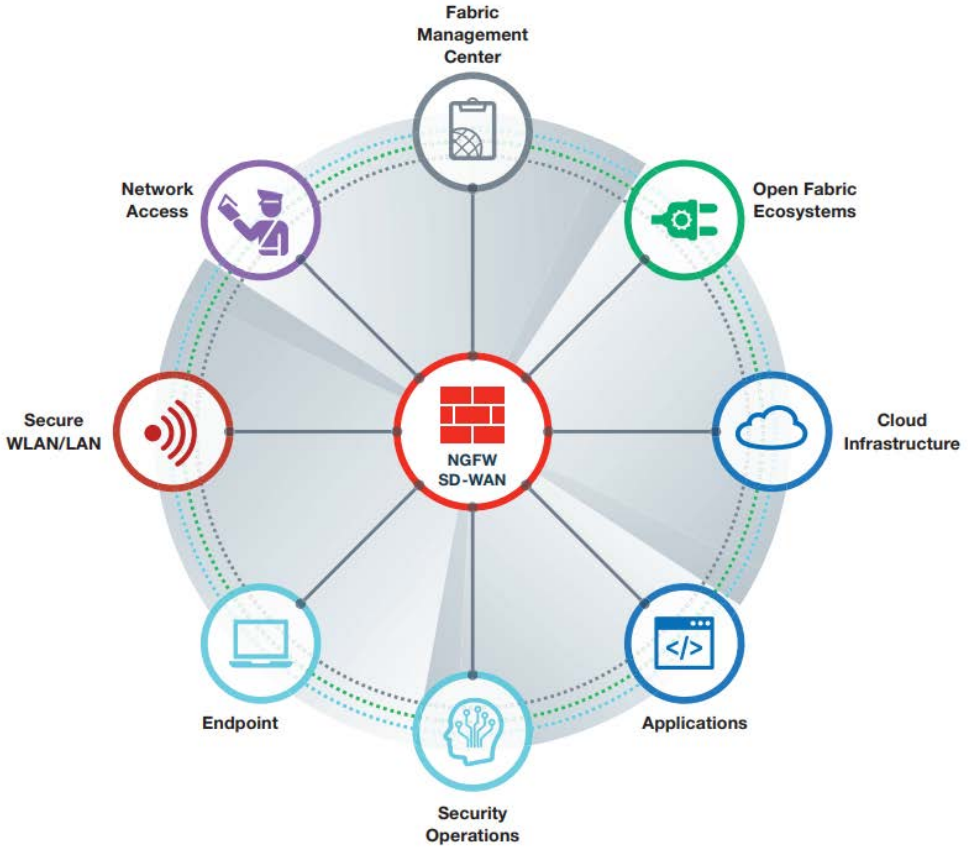


# 망 연계 또는 내부망을 통해 확산되는 악성파일 차단



# Fortinet Security Fabric – 가시성 확보 및 단일화된 관리

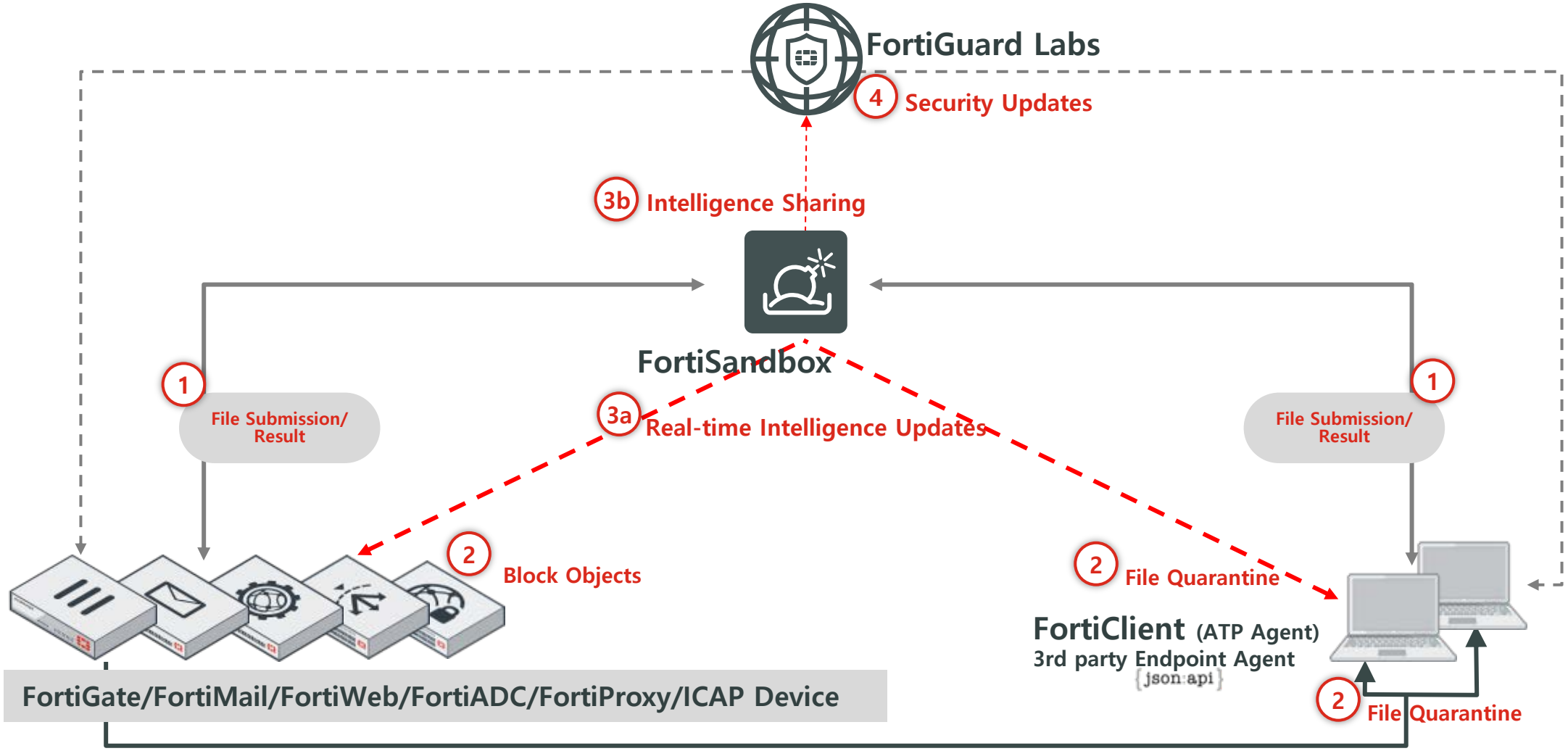



☞ Fortinet Security Fabric

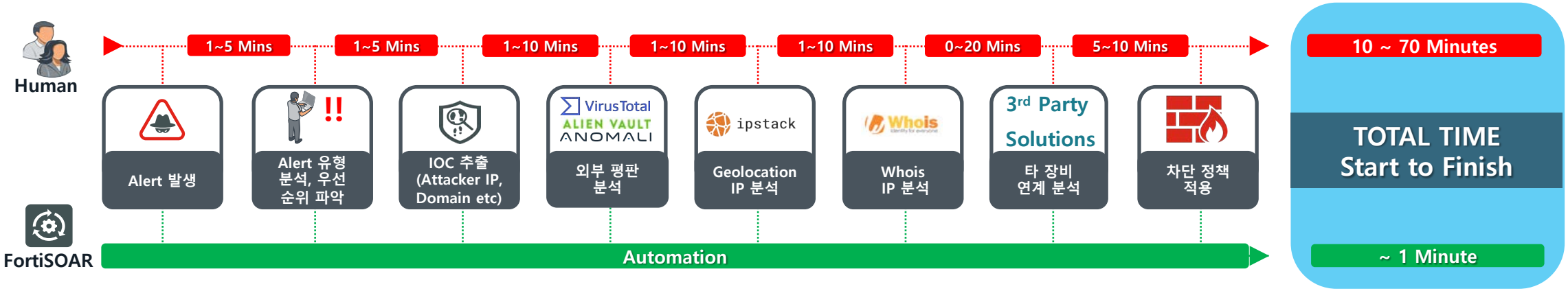
FORTINET

# Fortinet Security Fabric - 자동 정보 공유 및 차단

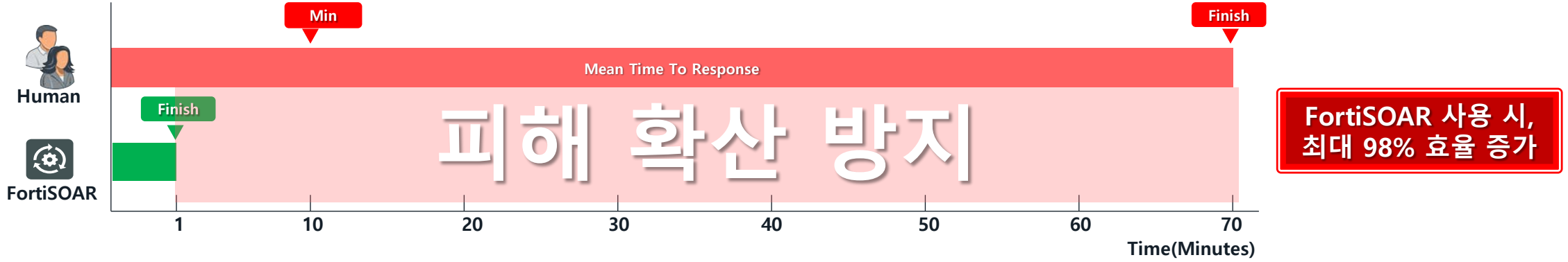


# FortiSOAR – 자동화된 운영과 대응

## ➢ SOC Incident Response Workflow#1 : 탐지된 침해정보 분석 업무(Network IOC Analysis)




## ➢ MTTR(Mean Time To Response) 소요 시간 비교






Icon made by Sherzod Mirzaakhmedov from www.flaticon.com

# 변종 랜섬웨어에 대한 대응 속도와 업무 효율

❑ 전통적 보안장비와 상용제품의 대응속도 비교


**Q. 랜섬웨어의 가장 큰 문제, 확산 피해란?**

**A. 감염 이후의 악성행위: 내부 네트워크 확산, 타 장치의 파일 암호화, 망간 이동, 서버 감염..**

FORTINET


FORTINET