

시큐리티 패브릭을 통한 엔드포인트 보안 전략

포티넷 코리아 이창운 이사

05 SEP 2018

공격의 대상인 된 엔드포인트



조사된 **44%**의 기업들이 지난 **24개월** 동안 하나 이상의 엔드포인트가 손상/감염되었다고 인정.¹



위반의 **30%**가 멀-웨어를 포함한 것이었으며, **16%**는 랜섬웨어와 같은 범죄행위를 하는 크라임웨어(**Crimeware**)에 의한 것.²





4%의 사람들이 특정 피싱(**phishing**) 캠페인을 클릭.²

Sources:

¹ SANS Institute Stage of Endpoint Security survey 2016



² Version DBIR 2018 – out of 53.308 incidents

엔드포인트 보안의 틈




63%, 기업이 네트워크 연결이 끊긴 엔드포인트 모니터링 할 수 없으며 절반 이상이 엔드포인트의 규정 준수 상태 (컴플라이언스)를 파악할 수 없음.

가시성 부족



99%, 2020년 말에는 악용되는 취약점의 99%가 보안 및 IT 전문가가 해당 시점에 이미 알고 있는 것.

취약점



87%, 대부분의 손상/감염 시간이 몇 분 이내에 불과

공격이 빠르게 변화

Sources:

1. Ponemon Institute The Cost of Insecure Endpoints, 2017
2. Gartner Endpoint Protection Platform Report, 2016
3. ESG Enterprise Adoption of Next-generation Endpoint Security, 2016

고객이 안고 있는 문제들

강력한 사이버 범죄 생태계에 의해
급속하게 진화하는 위협



최종 사용자는 항상 보호된
네트워크에 있지 않음

(즉, 시기 적절한 패치 관리 필요)



대응을 위해 소수의 직원에 의해
다양한 제품들에 다양한 정책 적용

(빠른 대응, 일관된 보안 정책 필요)



다운타임

위반

규제 처벌

브랜드 통합



엔드포인트 관리의 공통된 문제점

- 공격 표면 가시성
 - 기업 자산의 가시성 부족?
 - 즉각적인 주의가 필요한 것은 어떤 것?
- 안티 멀-웨어 방어
 - 대응에 오랜 시간이 걸리는지?
 - 너무 많은 품목/요소들의 변경으로 인한 협업 불가?
- 엔드포인트 ID
 - 너무 많은 로그로 인해 실시간 신원 확인의 어려움?
 - 누가 활성화 되어 있는지 파악 불가?
- 중앙관리
 - 취약점들을 어떻게 관리?
 - 내 자산들이 쉬운 먹이감이 되고 있나?

단순한 엔드포인트 보안 이상이 필요, 이러한 솔루션은 없을까?



Security Hygiene(보안 위생)의 기본을 유지

Gartner

This research note is restricted to the personal use of rdavis@fortinet.com.

Magic Quadrant for Endpoint Protection Platforms

Published: 30 January 2017 ID: G00301183

Analyst(s): Eric Ouellet, Ian McShane, Avivah Litan

The endpoint protection platform provides security capabilities to protect workstations, smartphones and tablets. Security and risk management leaders of endpoint protection should investigate malware detection effectiveness, performance impact on the host machines and administrative overhead.

Strategic Planning Assumption

By 2019, EPP and EDR capabilities will have merged into a single offering, eliminating the need to buy best-of-breed products for all but the most specialized environments.

Market Definition/Description

The enterprise endpoint protection platform (EPP) is an integrated solution that has the following capabilities:

- Anti-malware
- Personal firewall
- Port and device control

EPP solutions will also often include:

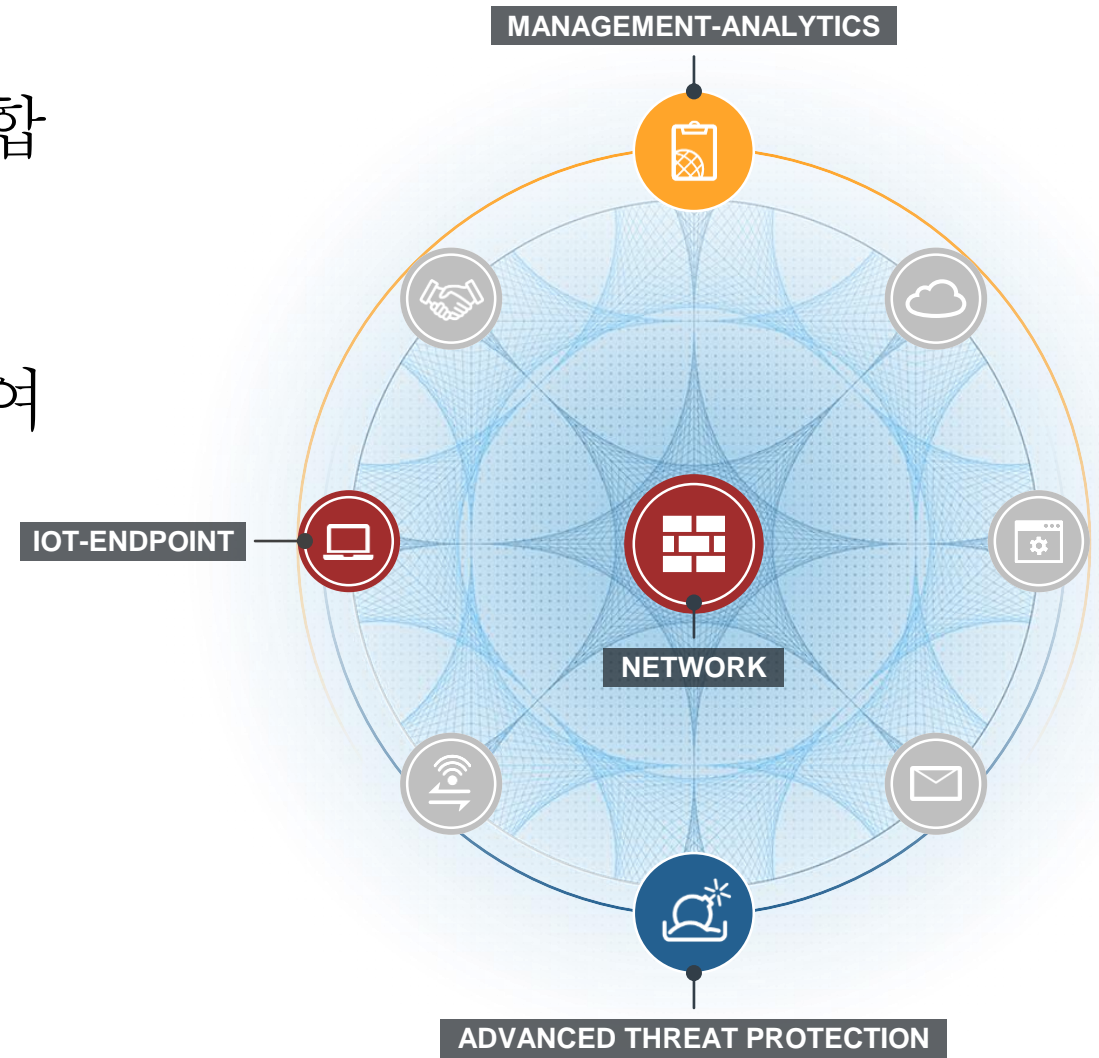
- Vulnerability assessment
- Application control (see Note 1) and application sandboxing
- Enterprise mobility management (EMM)
- Memory protection
- Endpoint detection and response (EDR) technology (see "Market Guide for Endpoint Detection and Response Solutions")
- Data protection such as full disk and file encryption

"대부분의 공격은 잘 알려지지 않은 취약점을 악용하고, 사회 공학을 사용하여 트로이 목마 악성 코드를 설치하거나 Java 또는 Visual Basic과 같은 해석 코드를 사용하여 악성 코드를 다운로드하고 설치합니다. 포괄적인 패치 프로그램과 응용 프로그램 제어는 세 가지 일반적인 멀-웨어 공격 기술을 모두 막을 수 있는 대단히 효과적인 방법이며, 주요 EPP 솔루션은 이를 예방 전략으로 추가하고 있습니다."

복잡하지 않은 공격에 쉽게 백도어(뒷문)로 악용될 수 있는 패치 되지 않은 엔드포인트의 위험성 강조

패브릭 기반의 엔드포인트

- 사내 전체의 네트워크 보안으로 기본 위생을 포함하여 엔드포인트 보안을 통합
- 알려지거나 알려지지 않은 위협에 대한 보호뿐만 아니라 패치 관리를 자동화하여 인시던트, 자원 및 공격 영역을 감소
- 독립적인 제3의 테스트를 기반으로 **최상위 등급** 획득



엔드포인트 및 관리 솔루션

패브릭 기반의 엔드포인트는 다음을 제공...

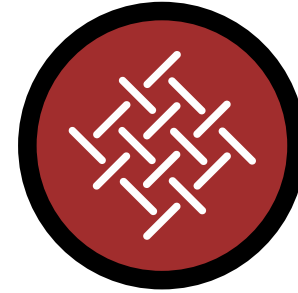
- 통합된 엔드포인트 가시성, 제어 및 컴플라이언스.
- 능동적인 엔드포인트 방어.
- 자동 위협 차단 및 확산 통제.
- 안전한 원격 액세스



Sandbox Agent



Anti-Malware Protection



Fabric Agent



Vulnerability Management



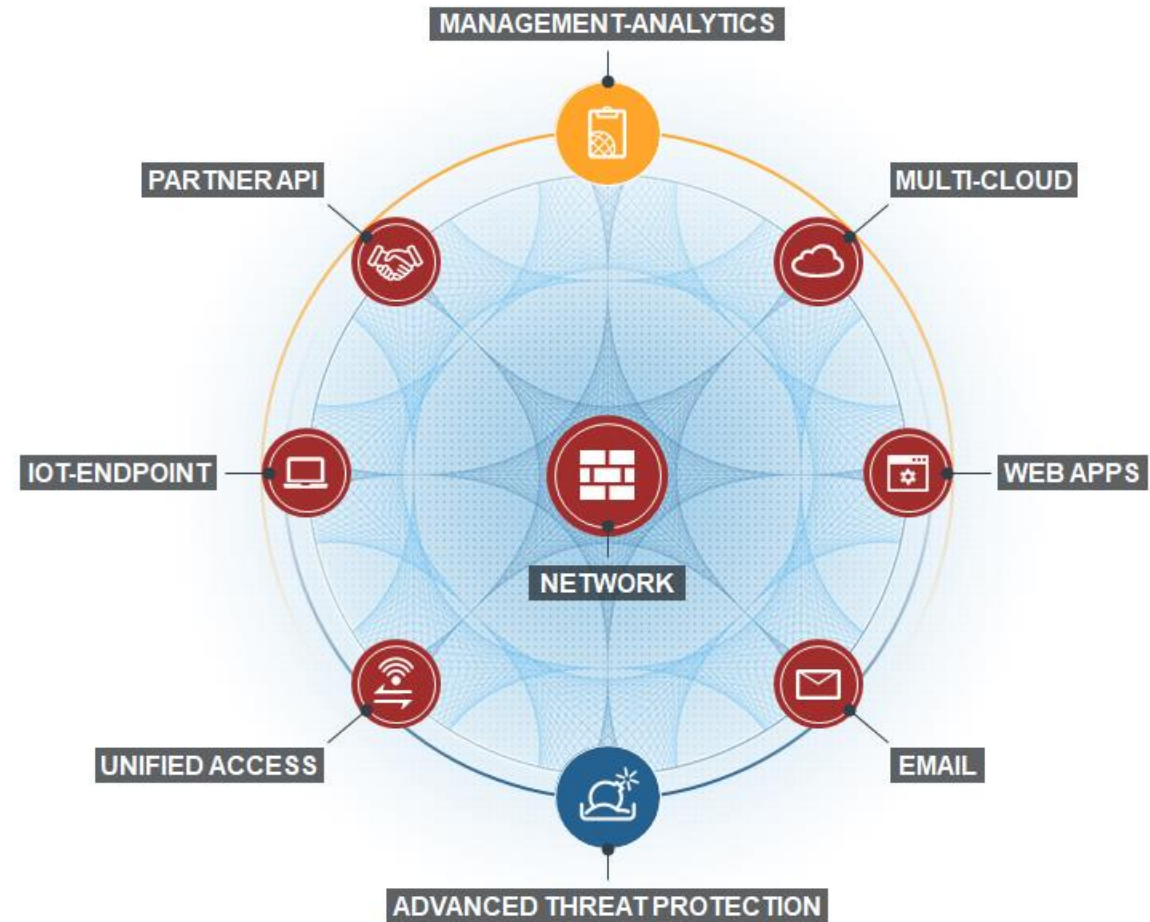
Software Inventory



Remote Access

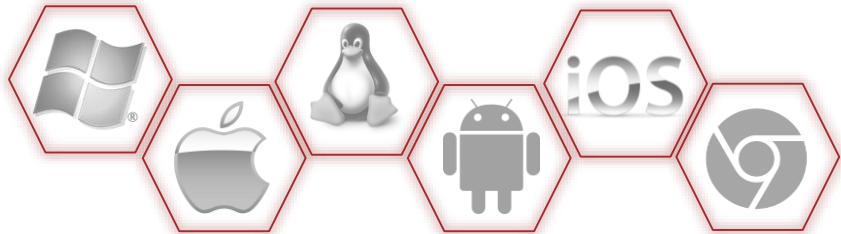
시큐리티 패브릭 기반의 엔드포인트 차별화

- **효율성** : 최상위 보안 패브릭 보호 및 엔드포인트 탐지 강화
- **통합** : 엔드포인트 및 네트워크 가시성 및 대응을 통합
- **상호 연동** : UTM/NGFW 및 샌드박스와 연동하고, 기존 EPP와 호환



차세대 엔드포인트 구성요소

- 4 **엔드포인트 보호(NG EPP 에이전트)**
어플리케이션 방화벽, 안티 멀-웨어, 안티 익스플로잇, 웹-필터링
- 3 **지능형 공격 위협(ATP 에이전트)**
샌드박스 통합
- 2 **안전한 원격 액세스(VPN 에이전트)**
SSL & IPSec VPN, SSO(Single Sign On)
- 1 **패브릭 에이전트**
텔레메트리, 격리, 취약점, 소프트웨어 인벤토리



시큐리티 패브릭 통합 UTM/NGFW, 샌드박스, 어날라이저, 인증서버		
글로벌 위협 분석 DB CPRL ¹ AV, 웹-필터링, 어플리케이션 방화벽, 취약점 관리		
엔드포인트/IoT 가시성, 제어 및 컴플라이언스	안전한 원격 액세스	첨단 엔드포인트 보호
엔드포인트, UTM/NGFW, Fabric Partners	엔드포인트, UTM/NGFW, 인증서버	엔드포인트, 샌드박스, 글로벌 위협 분석 DB

1. 일반적으로 지능형 지속 위협 공격자가 생성하는 침투 기술은 탐지 엔진을 우회할 수 있도록 하는데, 이러한 우회 공격을 탐지하고 차단하기 위해서 독창적인 특허 기술로 특정 시나리오 상의 단일 시그니처로 5만개 이상의 다양한 바이러스를 탐지

엔드포인트 보호의 진화

- AV 엔진과 함께 실시간 보호
 - 멀-웨어 기능에 기반한 식별 (CPRL)
 - 실시간 멀-웨어 에뮬레이션
- 안티-익스플로잇 탐지
 - 메모리 기반의 위협에 대한 보호
- 웹-필터 및 어플리케이션 방화벽
- 샌드박스 통합
 - 행위 기반의 탐지



포티넷 엔드포인트의 주요 기능

엔드포인트 가시성

- ✓ 시큐리티 패브릭의 엔드포인트 텔레메트리 실시간 공유
- ✓ 보안 등급에 위험 점수 부여
- ✓ 텔레메트리에 사용자 ID, 장치 유형, OS, 보호 상태, 보안 등급, 취약성 등 포함.

이점들

- ✓ 네트워크 컨텍스트 내에서 엔드포인트 인식 제공
- ✓ 엔드포인트 위험의 시각화

능동적 방어

- ✓ 유연한 패치로 취약성 검색.
- ✓ 안티 익스플로잇.
- ✓ 패턴 기반(CPRL) 멀-웨어 방지 엔진
- ✓ 샌드박스 통합.
- ✓ 응용 프로그램 방화벽 및 웹 필터링.

이점들

- ✓ 패치되지 않은 취약점 완화
- ✓ 알려지지 않은, 지능적인 멀-웨어 차단

통합과 자동화

- ✓ 자동회피
- ✓ 엔드포인트 컴플라이언스 수행
- ✓ 샌드박스에 파일 전달
- ✓ 의심되거나 손상된 엔드포인트 격리
- ✓ 위협과 인시던트 방지

이점들

- ✓ 보안 컴플라이언스 수행
- ✓ 위협과 인시던트 방지
- ✓ 확산 방지

단순한 엔드포인트 보안 이상

- 패브릭 에이전트
- 취약점 관리
- 안티 멀-웨어 보호(CPRL)
 - AV 엔진
 - 샌드박스 통합
 - 안티 익스플로잇(메모리 기반 위협 대응)
- 웹 보안
- 어플리케이션 방화벽
- 원격 액세스(VPN)
- 소프트웨어 인벤토리
- 지원 OS
 - WINDOWS
 - MAC
 - LINUX
 - iOS
 - ANDROID
 - CROMEBOOK 등등
- 그외 다양한 3rd party AV와 협업

엔드포인트 보호 그 이상, 포티클라이언트

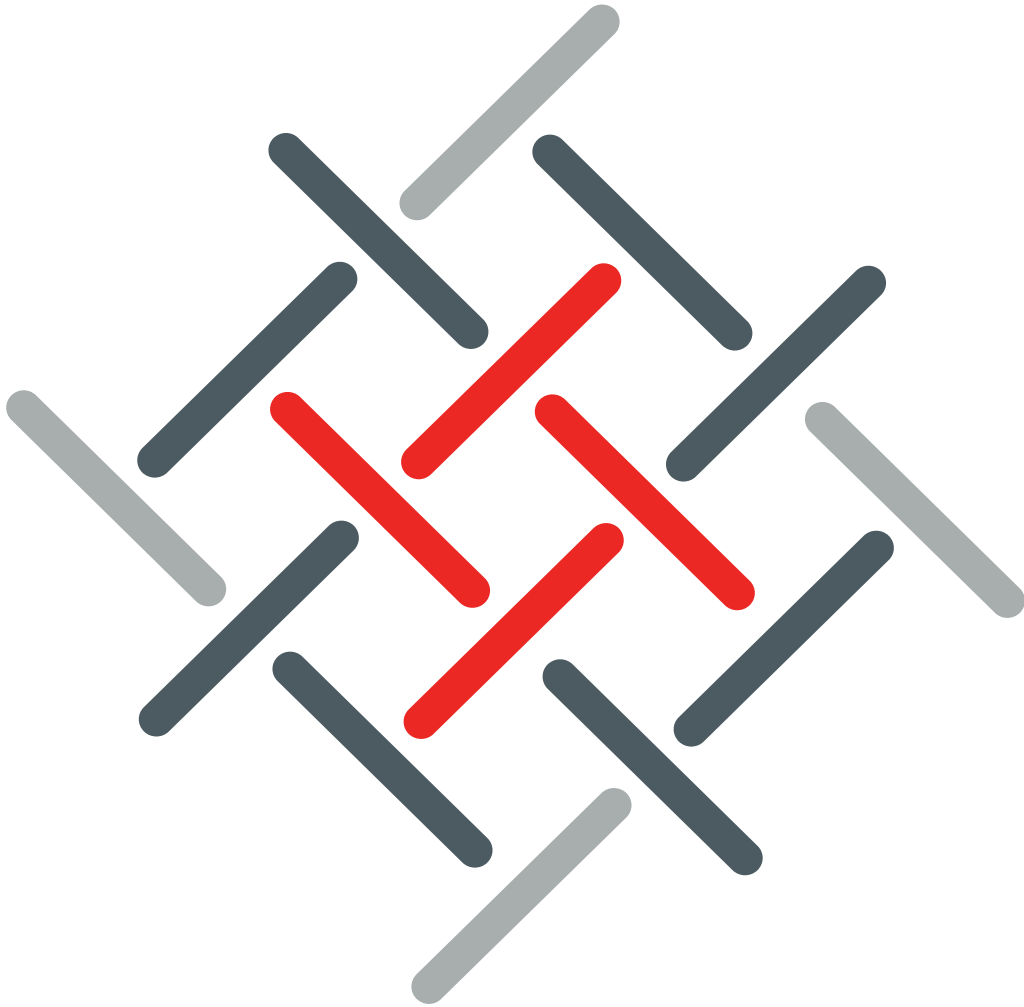
- 4 엔드포인트 보호(NG EPP 에이전트)
어플리케이션 방화벽, 안티 멀-웨어, 안티 익스플로잇, 웹-필터링
- 3 지능형 공격 위협(ATP 에이전트)
샌드박스 통합
- 2 안전한 원격 액세스(VPN 에이전트)
SSL & IPSec VPN, SSO
- 1 패브릭 에이전트
텔레메트리, 격리, 취약점, 소프트웨어 인벤토리

- 엔드 포인트 가시성
- 시큐리티 패브릭의 엔드포인트 텔레메트릭 공유
- 엔드포인트 컴플라이언스 시행
- 패치 옵션으로 취약점 검사
- 엔드포인트 위협 점수 - 보안 등급의 일부
- 소프트웨어 인벤토리
- Windows, Mac 및 Linux 지원

- 리눅스용 패브릭 에이전트
- 소프트웨어 인벤토리
- 자동화

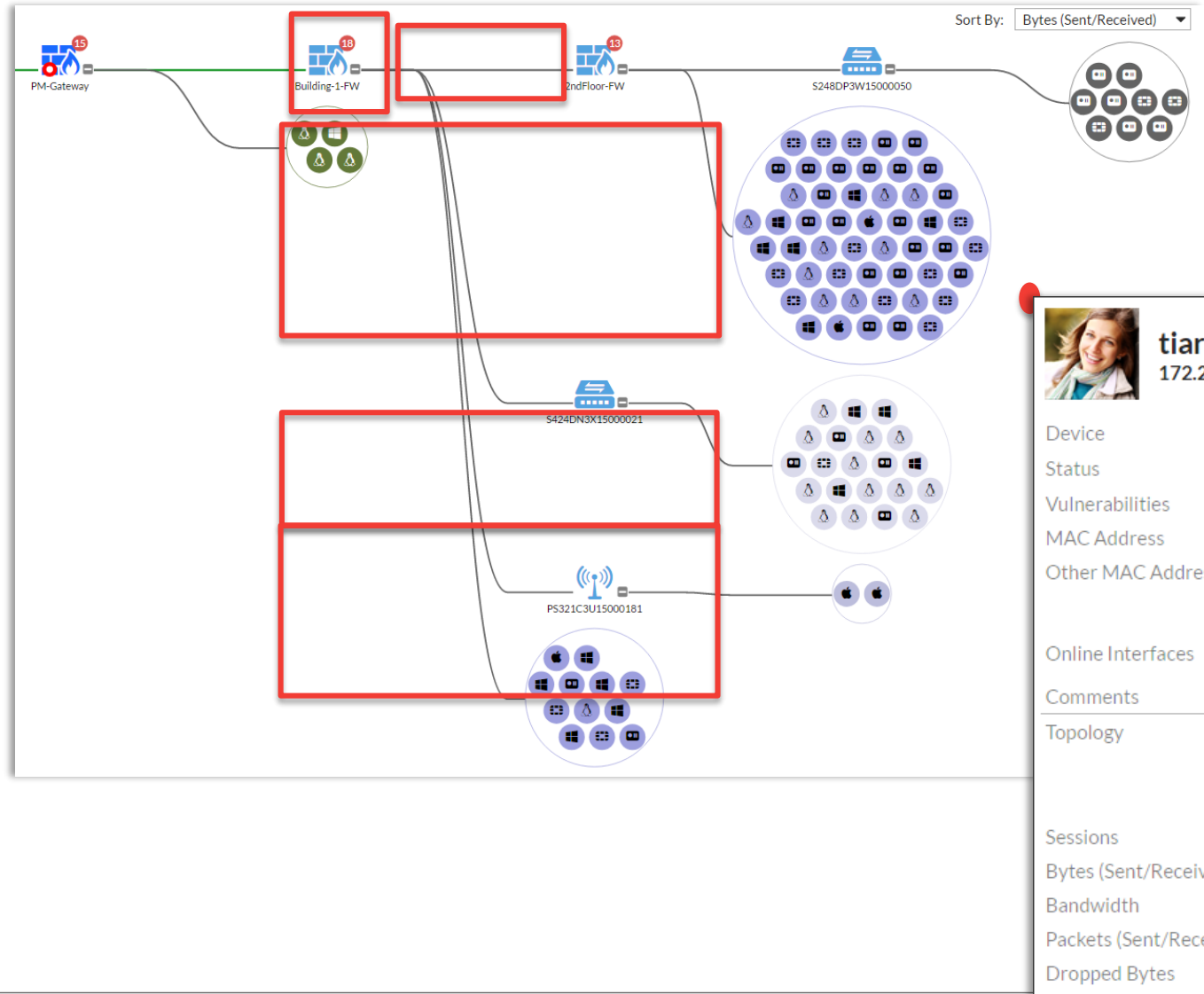
- 보안 등급에 기여
- 로그 분석을 위한 엔드포인트 이벤트

패브릭 에이전트란? 왜 필요한가?



포티뷰를 통한 엔드포인트 가시성

- 네트워크에 대한 심층적인 가시성
 - 엔드포인트 위치에 대한 가시성
 - 트래픽 발생량, 세션 수 등등 실시간 모니터링
- 정확한 엔드포인트 정보
 - OS
 - 로그인한 사용자
 - 사용자 아바타
 - 엔드포인트 에이전트 상태
 - 엔드포인트 취약성
 - 여러 개의 MAC 주소를 상호 연관
 - 사회 보장 번호
 - 온라인/오프라인
 - 설치된 응용 프로그램들 파악



소프트웨어 인벤토리

FortiClient Enterprise Management Server admin

178 Total Applications
 38 Total Vendors
 0 New Detections

Display by Application

Name	Vendor	Version	First Detected	Last Installed	Install Count
172.16.0.10.app		13.4	2018-07-22		0
172.16.14.10.app		13.4	2018-07-22		0
아이나비 매니저	아이나비	3.05.0000	2018-06-20		0
한컴오피스 뷰어	Hancom	9.6.1.0	2018-06-20	2016-11-05	1
Activity Monitor.app	Apple	10.13	2018-06-21		0
Adobe Acrobat Reader DC - Korean	Adobe Systems Incorporated	18.011.20040	2018-06-20		0
Adobe Acrobat Reader DC - Korean	Adobe Systems Incorporated	18.011.20055	2018-07-22		0
Adobe Flash Player Install Manager.app	Adobe Systems, Inc.	25.0.0.163	2018-07-31		0
Adobe Refresh Manager	Adobe Systems Incorporated	1.8.0	2018-06-20		0
AirPort Utility.app	Apple	6.3.8	2018-06-21		0
AnySign4PC.app		1.1.0.7	2018-07-31		0
App Store.app	Apple	2.4	2018-06-21		0
AppCleaner.app	Julien Ramseier	3.4	2018-06-21		0
Apple Configurator 2.app	Apple Mac OS Application Signing	2.7	2018-06-21		0
Apple Configurator 2.app	Apple Mac OS Application Signing	2.7.1	2018-07-31		0

- ✓ 어플리케이션 인지
- ✓ 라이선스 관리
- ✓ 엔드포인트 보안 위생 향상

자동화 기능

- 파일 격리
- 샌드박스 분석을 위한 파일 전달
- 자동 패치
- 컴플라이언스 수행
- 엔드포인트 격리

Dashboard > Security Fabric > Automation > New Automation Stitch

Name: Quarantine-IOC-Detected
Status: Enabled
FortiGate: All FortiGates

Trigger

- Compromised Host
- Event Log
- Reboot
- Conserve Mode
- High CPU
- License Expiry
- HA Failover
- Configuration Change

IOC level threshold: Medium High

Action

- Email
- FortiExplorer Notification
- Access Layer Quarantine
- Quarantine FortiClient via EMS
- IP Ban
- AWS Lambda
- Webhook

Minimum interval (seconds): 0

OK Cancel

이점들

- ✓ 위협 및 인시던트를 방지
- ✓ 확산 통제

로그 분석을 위한 엔드포인트 텔레메트리

■ 텔레메트리 데이터 수집

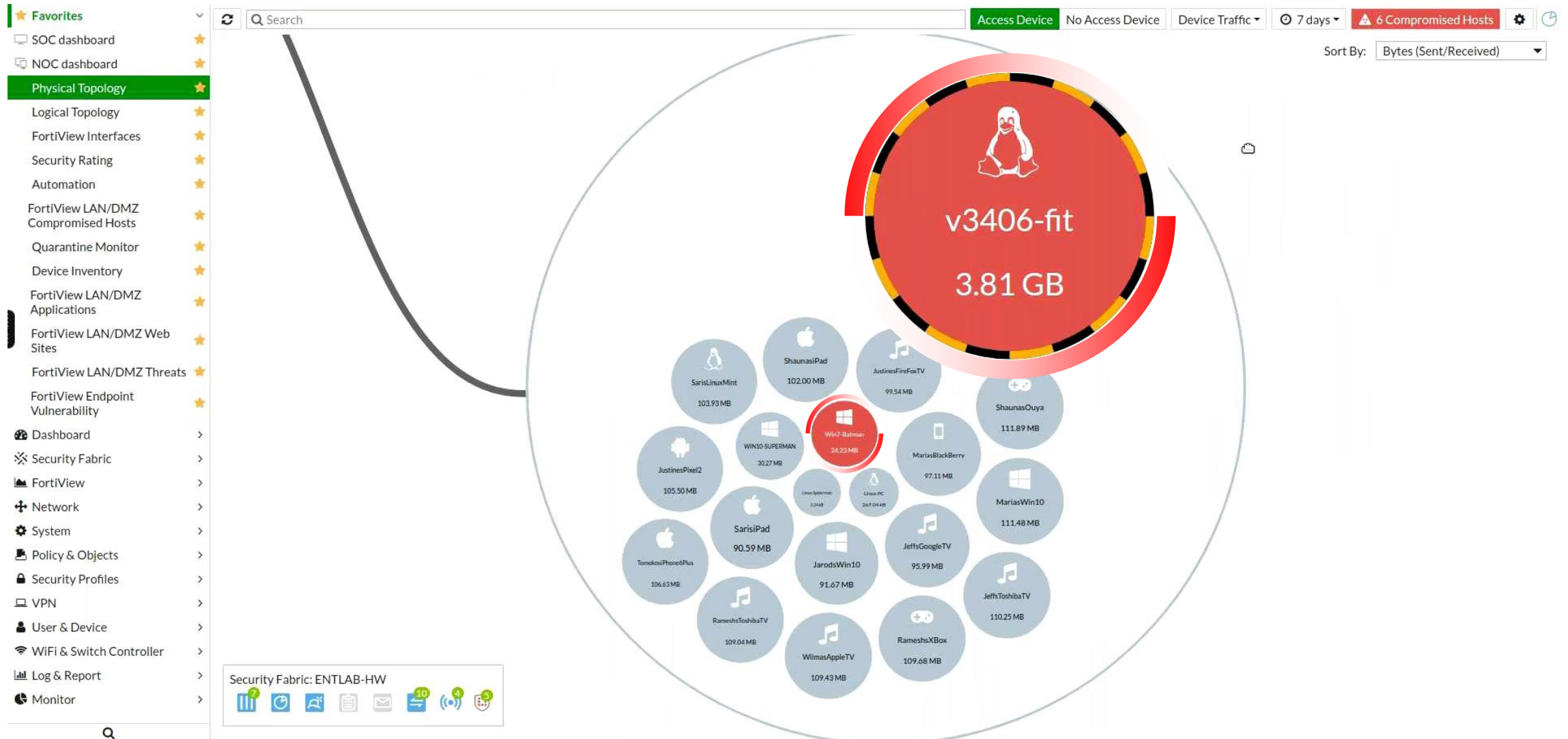
- 엔드포인트 이벤트
- 엔드포인트 취약성
- 사용자 이름
- 사용자 아바타

The screenshot displays the FortiView interface for endpoint telemetry. The top section shows a table of source IP addresses, groups, and the number of sites. The bottom section shows a grid of endpoint cards for various devices, each with details on OS, Source MAC, Offending Attempts, Verdict, and Possible Malware.

Source	Group	# Sites
172.172.2.204 (Jean-Pierre)	CSE Team	534
172.172.2.203 (rmay)	PM Team	971
172.172.1.200 (abirsfelder)	Video Team	98
172.172.2.201 (mxie)	PM Team	116

Endpoint Name	IP	OS	Source MAC	Offending Attempts	Verdict	Possible Malware
Steven-PC	172.16.69.206	Windows 7	28:f1:0e:03:25:b4	3	Infected 2	W32/Agent.QAHLtr...
Iwang-344Q	172.16.69.153	Linux 3.16.0	f0:df:1:41:82:d3	5	Infected 2	Dorkbot.Botnet...
Sandy.singh	172.18.4.151	Android 5.1	00:09:0f:09:00:16	3	Infected 1	Android/Agent.DLtr...
Linda-desktop	172.18.39.10	Windows 7	60:6d:c7:d5:bb:fd	4	Infected 1	Obfuscated.Flash.Exploit...
Shirley-PC	172.16.165.254	Windows 7	00:27:0e:31:d9:b3	5	High Suspicion 1	NetBus.Server.D...
Bing-433DR	172.16.179.20	Linux 3.X	f0:de:f1:c1:7f:56	2	Medium Suspicion 1	LSASS.139

네트워크에 무슨 일이 있는지..., 위험한 엔드포인트 식별



능동적 엔드포인트 방어

- 4 **엔드포인트 보호(NG EPP 에이전트)**
어플리케이션 방화벽, 안티 멀-웨어, 안티 익스플로잇, 웹-필터링
- 3 **지능형 공격 위협(ATP 에이전트)**
샌드박스 통합
- 2 **안전한 원격 액세스(VPN 에이전트)**
SSL & IPSec VPN, SSO
- 1 **패브릭 에이전트**
텔레메트리, 격리, 취약점, 소프트웨어 인벤토리

- 패턴기반(CPRL) 안티 멀-웨어
- 안티 익스플로잇
- 웹 필터링
- 어플리케이션 방화벽
- 샌드박스 통합

- FortiGuard Machine Learning & AI
- Anti-exploit UI

능동적 엔드포인트 방어

취약점 완화 및 악용 방지

- 취약점 검색
- 패칭
- 악용 방지

고급 멀-웨어 탐지 및 차단

- 안티 멀-웨어(CPRL 기반)
- 안티 익스플로잇
- 웹 필터
- 어플리케이션 방화벽
- 샌드박스 통합

통합 및 자동 대응

- 파일 및 엔드포인트 격리
- 자동 패칭
- 샌드박스 통합
- 3rd party EDR 통합
- SIEM 통합

가시성, 통합, 중앙관리

컴플라이언스를 이용한 네트워크 접근제어

```
aaa new-model
aaa authentication login console_auth line none
aaa authentication dot1x default group radius
aaa authorization network default group radius

aaa session-id common
dot1x system-authcontrol

interface FastEthernet1/0
switchport access vlan 10
dot1x pae authentication
dot1x port-control auto
dot1x auth-fail vlan 100
dot1x guest-vlan 99

interface FastEthernet1/1
switchport access vlan 10

interface Vlan1
no ip address
no ip route-cache

interface Vlan10
ip address 1.1.1.10 255.255.255.0

interface Vlan100
no ip address
ip access-group Restrict_VLANUser in

ip access-list extended Restrict_VLANUser
permit udp any host 255.255.255.255 eq bootps
permit icmp any host 1.1.1.254 echo-reply
deny ip any 1.0.0.0 0.255.255.255
permit ip any any

radius-server host 1.1.1.100 auth-port 1645
line con 0
```

Login: admin
Password:*****
> set ip address 192.168.72.7/24
> set gateway 192.168.72.254
> edit vlan 27
> set ip address 172.10.27.1/24
> set dhcp server enabled

> configure port1-10
> set vian native 27

```
aaa new-model
aaa authentication login console_auth line none
aaa authentication dot1x default group radius
aaa authorization network default group radius

aaa session-id common
dot1x system-authcontrol

interface FastEthernet1/0
switchport access vlan 10
dot1x pae authentication
dot1x port-control auto
dot1x auth-fail vlan 100
dot1x guest-vlan 99

interface FastEthernet1/1
switchport access vlan 10

interface Vlan1
no ip address
no ip route-cache

interface Vlan10
ip address 1.1.1.10 255.255.255.0

interface Vlan100
no ip address
ip access-group Restrict_VLANUser in

ip access-list extended Restrict_VLANUser
permit udp any host 255.255.255.255 eq bootps
permit icmp any host 1.1.1.254 echo-reply
deny ip any 1.0.0.0 0.255.255.255
permit ip any any

radius-server host 1.1.1.100 auth-port 1646 key aaa_auth
```

Login: admin
Password:*****
> set ip address 192.168.72.7/24
> set gateway 192.168.72.254
> edit vlan 27
> set ip address 172.10.27.1/24
> set dhcp server enabled

> configure port1-10
> set vian native 27

Login: admin
Password:*****
> set ip address 192.168.72.7/24
> set gateway 192.168.72.254
> edit vlan 27
> set ip address 172.10.27.1/24
> set dhcp server enabled

> configure port1-10
> set vian native 27

Login: admin
Password:*****
> set ip address 192.168.72.7/24
> set gateway 192.168.72.254
> edit vlan 27
> set ip address 172.10.27.1/24
> set dhcp server enabled

> configure port1-10
> set vian native 27



컴플라이언스를 이용한 네트워크 접근 제어

```
config endpoint-control profile
  edit "TeamViewerCompliance"
    config forticlient-winmac-settings
      set forticlient-system-compliance-action block
      config forticlient-own-file
        edit 1
          set file "C:\\Program Files (x86)\\TeamViewer\\Tea
        next
      end
      set forticlient-log-upload disable
      set forticlient-vuln-scan disable
    end
    config forticlient-android-settings
    end
    config forticlient-ios-settings
    end
    set device-groups "windows-pc"
  next
end
```

[응용 프로그램 유무 검사]

```
# config endpoint-control profile
(profile) # edit reg_check
(reg_check) # config forticlient-winmac-settings
(forticlient-winmac-settings) # config forticlient-registry-entry
(forticlient-registry-entry) # edit 1
(1) # set registry-entry HKEY_CURRENT_USER\\SOFTWARE\\MYCOMPANY\\
(1) # end
(forticlient-winmac-settings) # end
(reg_check) # end
```

[레지스트리 키-값 검사]

Edit FortiClient Compliance Profile

Profile Name: TeamViewerCompliance

Comments: Write a comment...

Assign Profile To: Windows PC

On-Net Detection By Address: +

Specify Compliance Criteria

Endpoint Compliance on: EMS FortiGate

Endpoint Vulnerability Scan on Client

System Compliance

Create FortiClient Running Application Rule

Application Name: []

Application Check Rule: Present Absent

Process Name 1: []

Application SHA256 Signature 1: []

Process Name 2: []

Application SHA256 Signature 2: []

Process Name 3: []

Application SHA256 Signature 3: []

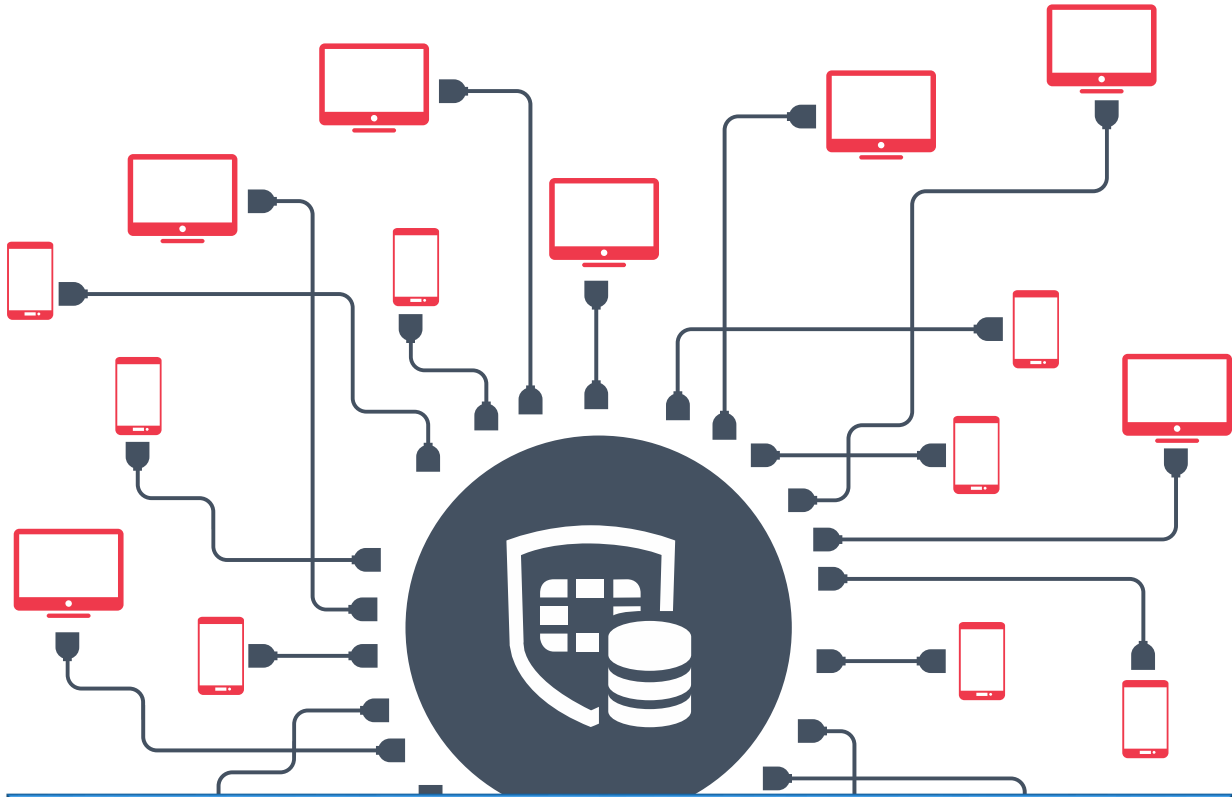
Process Name 4: []

Application SHA256 Signature 4: []

OK Cancel

[응용 프로그램 동작 유무 검사]

중앙 집중식 관리



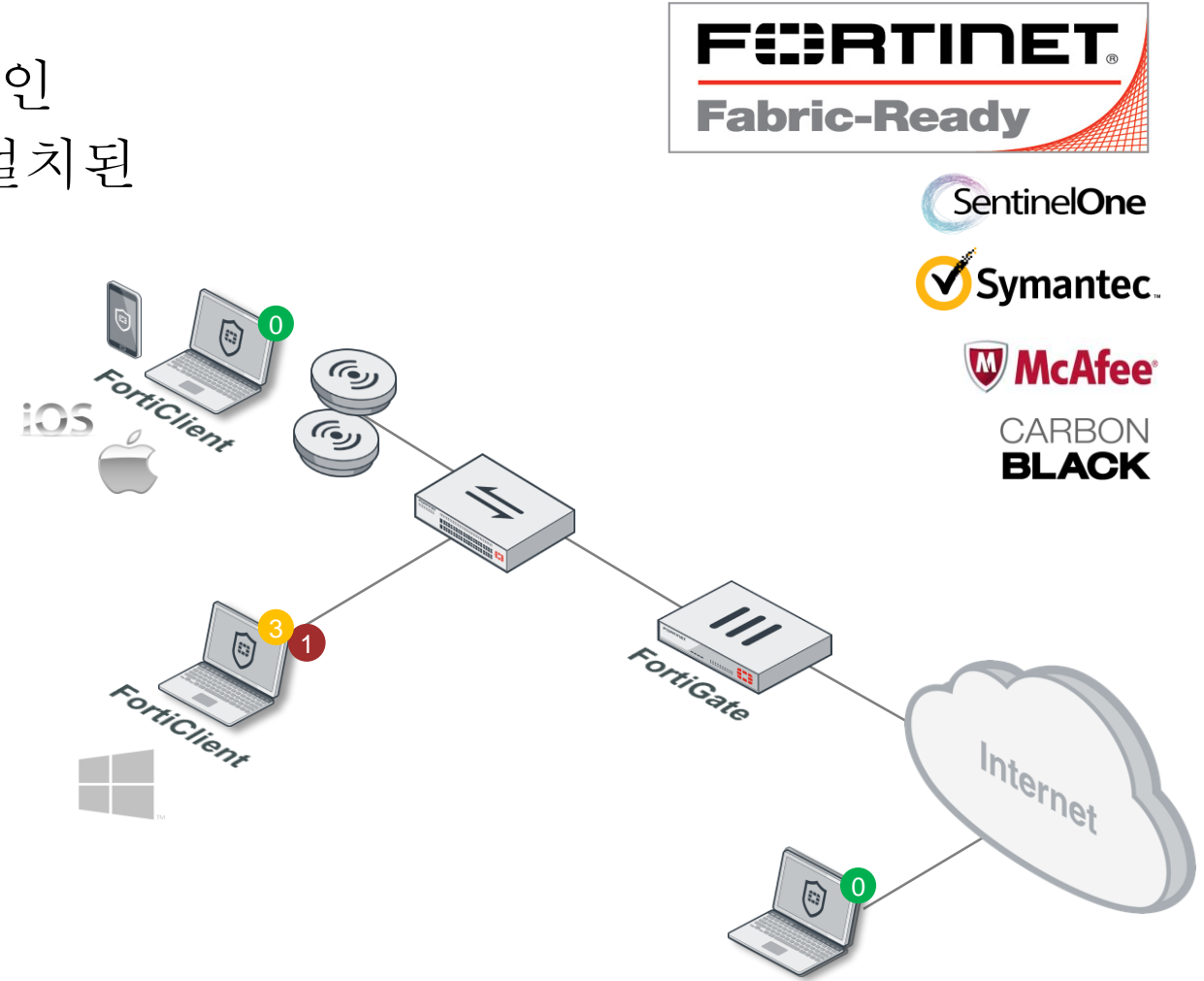
- 소프트웨어 인벤토리
- 크롬북을 통한 통합관리
- 안티-익스플로잇 구성
- 자동 그룹 할당을 위한 엔드포인트 태그
- 파일 격리 관리
- 자동화된 엔드포인트 격리

EMS(Enterprise Management System) 서버

- 엔드포인트 구성, 배포 및 관리
 - AD, LDAP 등 엔터프라이즈 시스템과 통합
- 실시간 엔드포인트 모니터링
- 위협 요약, 경고 및 알림
- 원격 제어
 - 안티 멀-웨어 검사
 - 취약점 검사
 - 엔드포인트 격리
- 소프트웨어 인벤토리
- 파일 격리 관리
- 높은 확장성

패브릭 에이전트 기능 요약

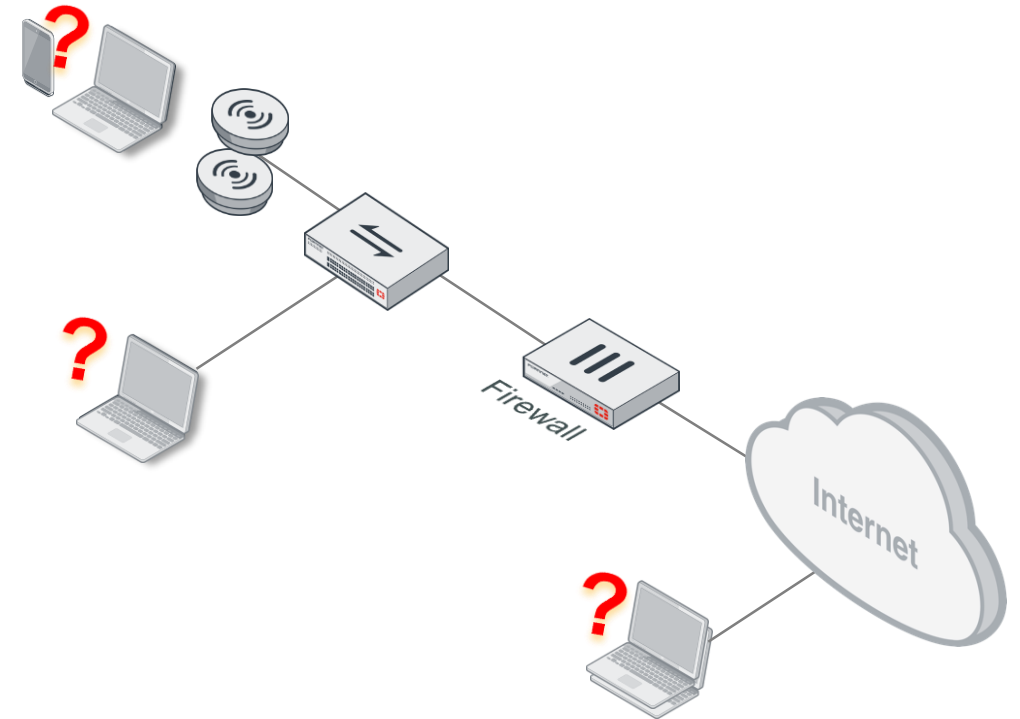
- 위험 기반 가시성
 - 패치 옵션으로 패치 되지 않은 취약점 확인
 - 소프트웨어 인벤토리에 의해 단말기에 설치된 응용프로그램 및 버전에 대한 가시성
- 엔드포인트 컴플라이언스 수행
- 통합 및 자동화
 - 시큐리티 패브릭과의 통합
 - 문제 확대 방지를 위한 자동 대응
- 기존 엔드포인트 투자 활용



엔드포인트/IoT 가시성, 제어 및 컴플라이언스

문제점

- 가시성 부족과 상관 관계 부족
- 일관성 없는 엔드포인트 보안 정책 및 보안 위생



엔드포인트/IoT 가시성, 제어 및 컴플라이언스

문제점

- 가시성 부족과 상관 관계 부족
- 일관성 없는 엔드포인트 보안 정책 및 보안 위생

솔루션

시큐리티 패브릭 기반의 엔드포인트

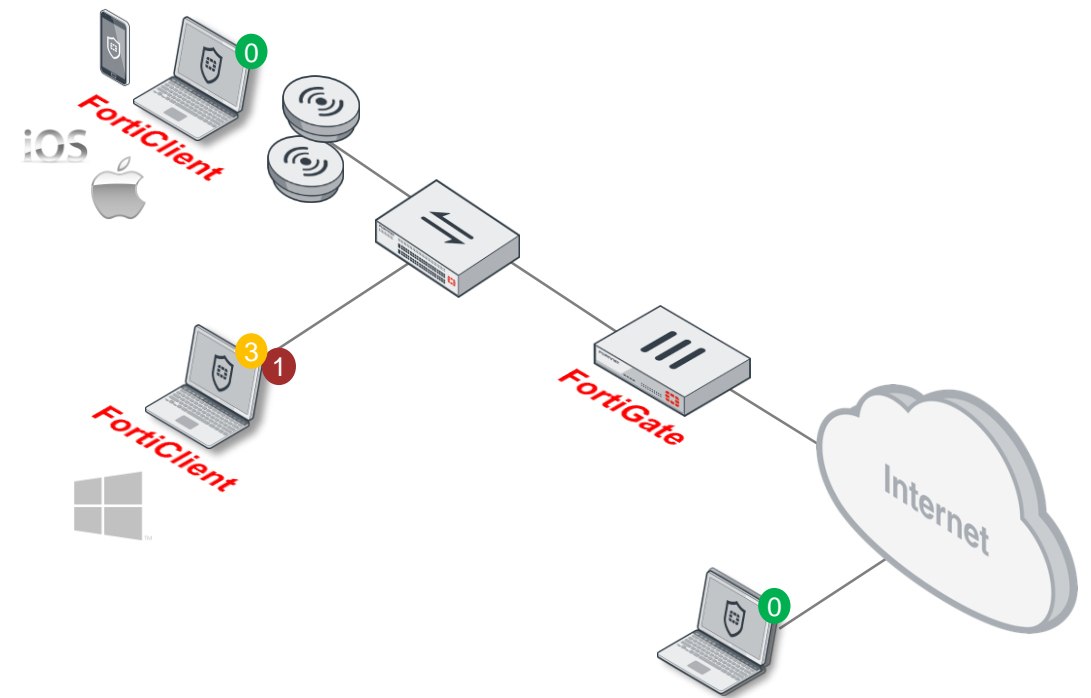
- 통합된 **End-to-end** 엔드포인트 가시성 및 정책 제어
- 엔드포인트 분리 및 검역하여 엔드포인트 미준수에 대해 조치
- 취약한 엔드포인트 파악 및 패치
- 기존 엔드포인트 투자를 활용

이점

- 단일 창 관리
- IT 및 사용자의 부담 경감
- 기존의 엔드포인트 보호

기능

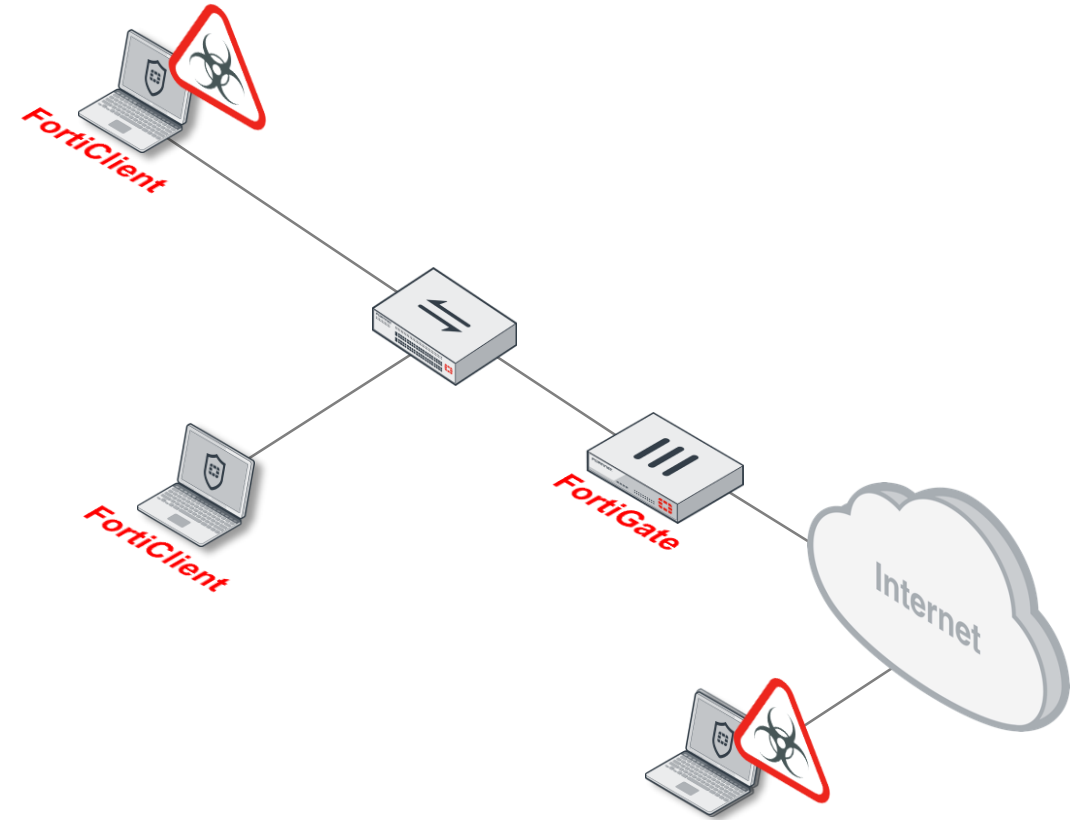
- IoT 관리
- 텔레메트리(OS, IP주소, 취약성 등등)
- 패치관리
- 격리



알려지거나 알려지지 않은 지능형 공격 위협 대응

문제점

- 급속하게 진화하는 위협
- 온/오프 환경에서 자산을 보호



알려지거나 알려지지 않은 지능형 공격 위협 대응

문제점

- 급속하게 진화하는 위협
- 온/오프 환경에서 자산을 보호

솔루션

글로벌 위협 분석 DB 및 샌드박스 활용

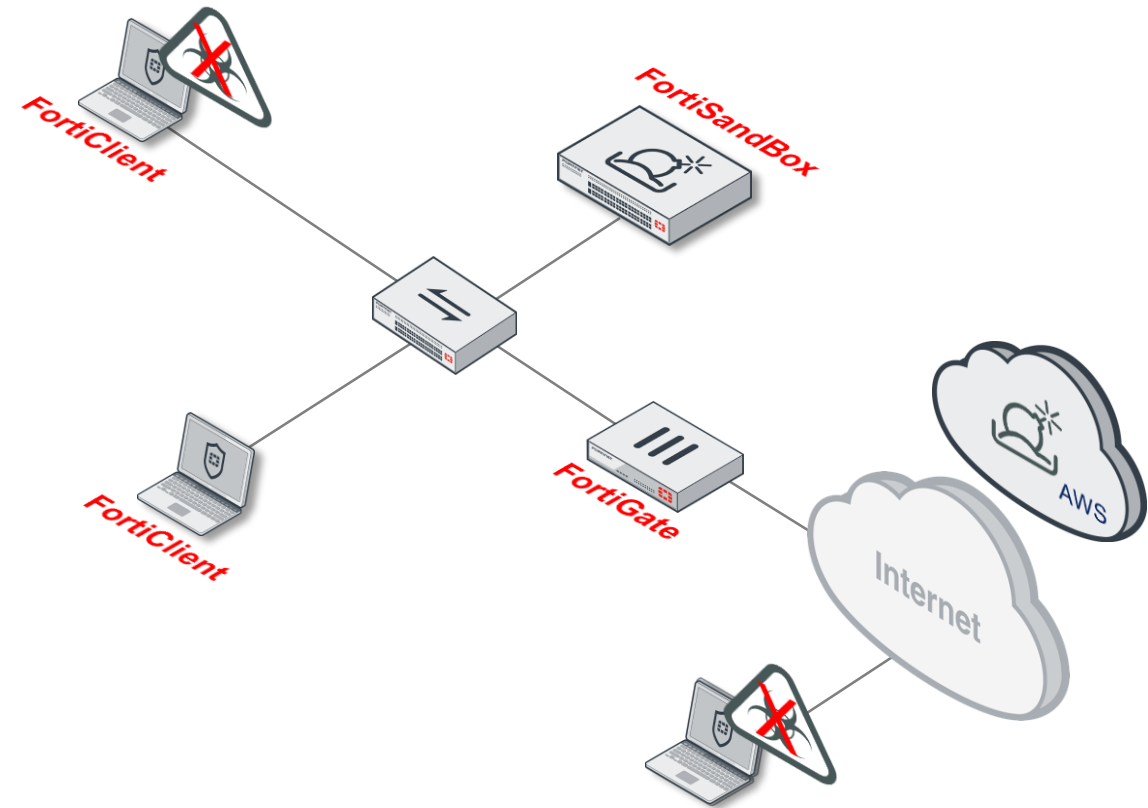
- 알려진 위협을 차단하기 위해 글로벌 인텔리전스를 기반으로 한 보안 스택 내장
- 제로데이 위협 방지

이점

- 포괄적인 위협으로부터 보호
- 자동화를 통한 정보보안 자원 감소
- 입증된 보안 효과

기능

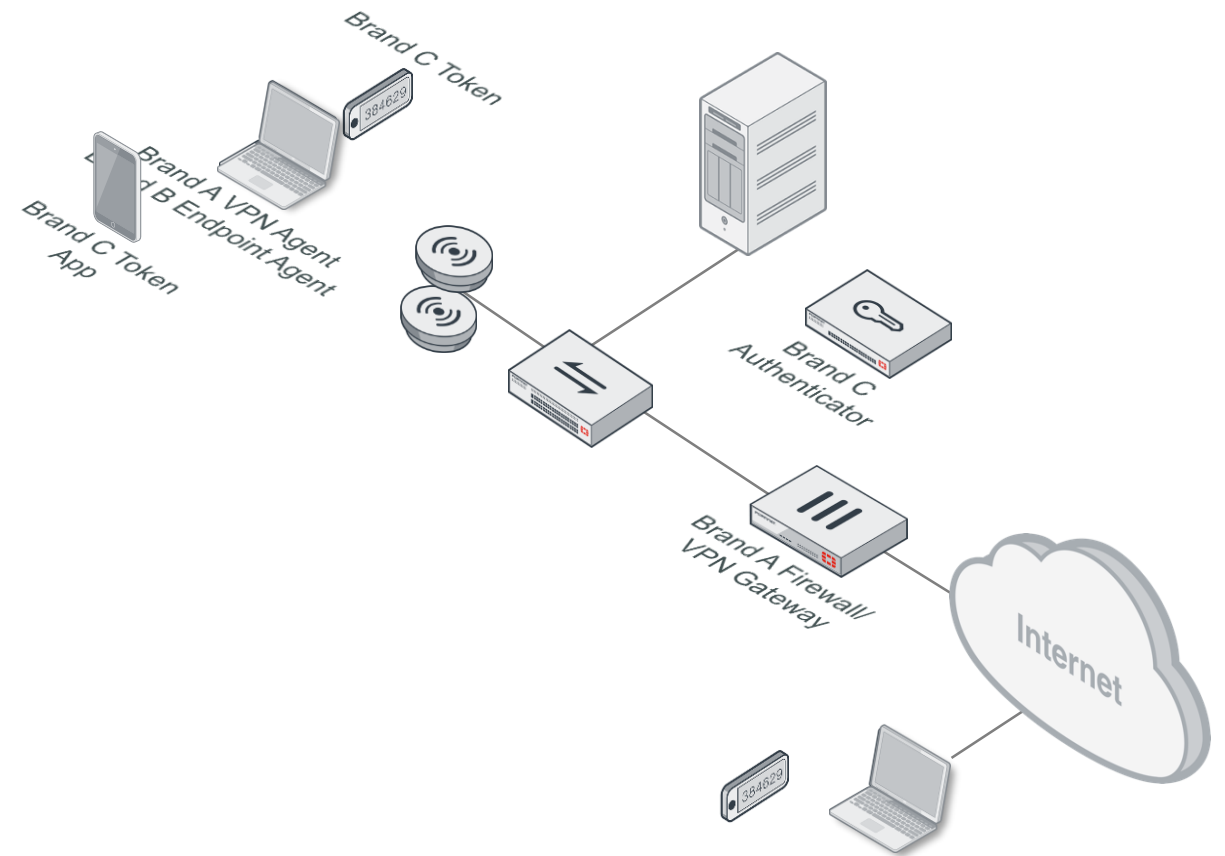
- AEE, CPRL AV, Web Filter, App FW



안전한 원격 액세스

문제점

- 다른 에이전트 및 제품 추가의 관리 복잡성
- 취약한 VPN 인증
- 민감한 리소스 제어가 부족



안전한 원격 액세스

문제점

- 다른 에이전트 및 제품 추가의 관리 복잡성
- 취약한 VPN 인증
- 민감한 리소스 제어가 부족

솔루션

사용자 인증 및 토큰을 통한 이중 인증

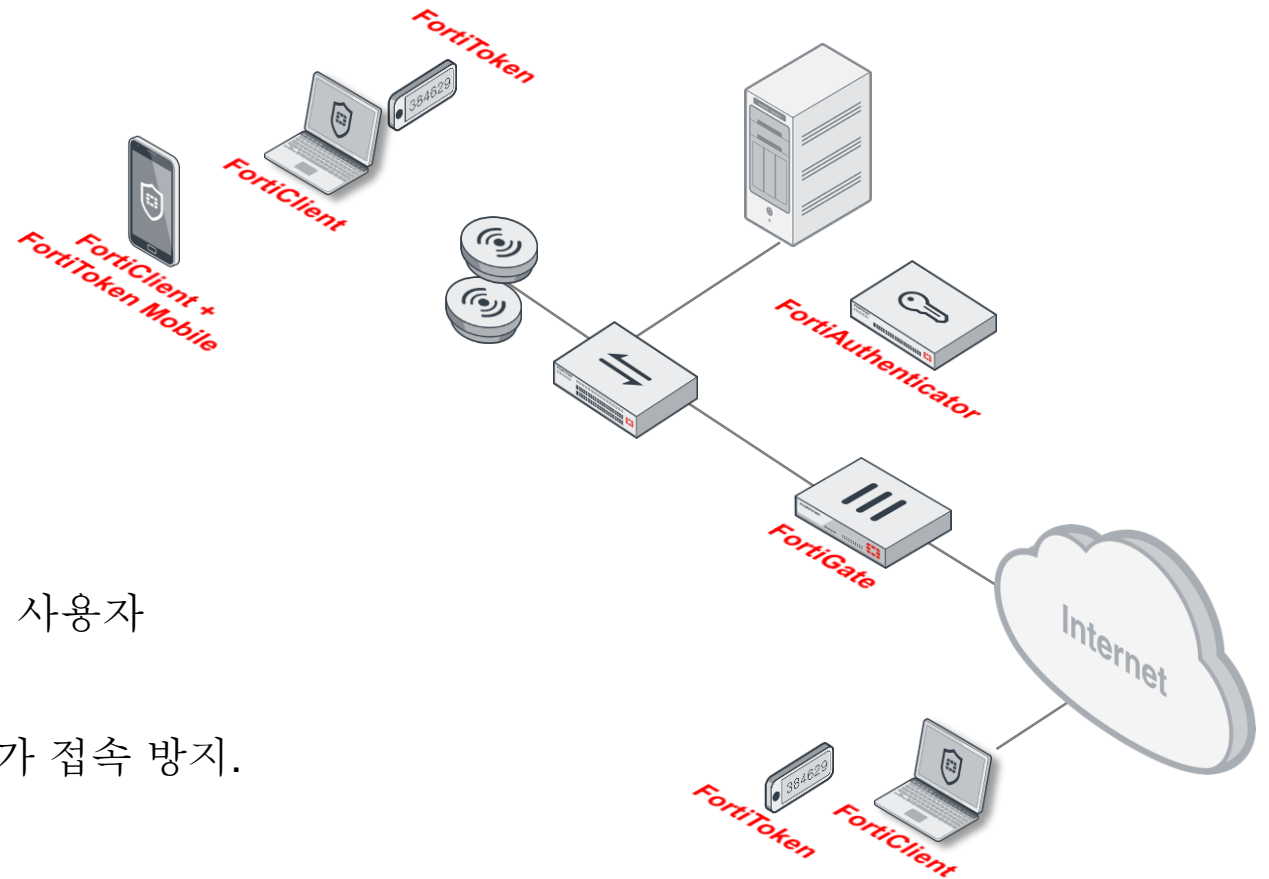
- 패키지형 VPN 솔루션 (IPSec/SSL)
- 통합 이중인증(2 Factor Auth) 및 SSO 기능 제공
- 통합 SSO 엔드포인트 에이전트
- 리소스 할당에 대한 사용자의 완벽한 제어

이점

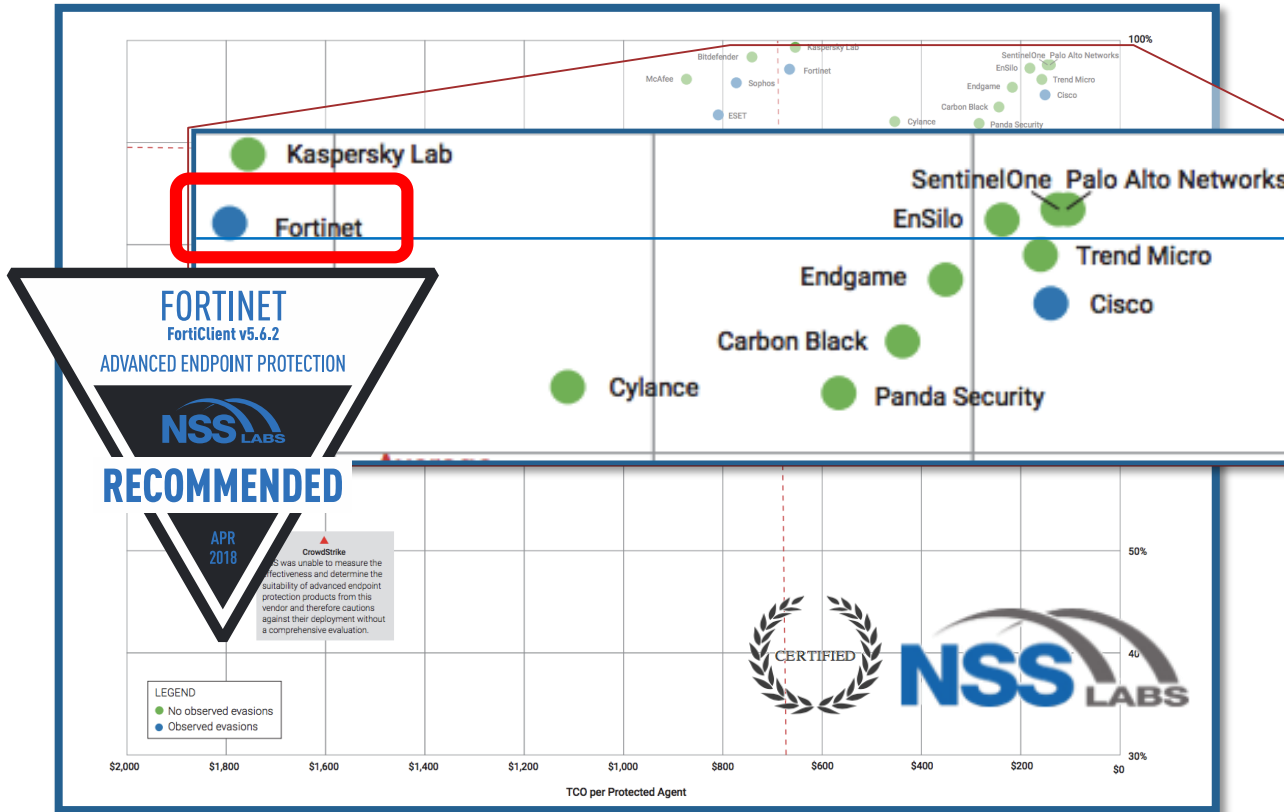
- 통합된 에이전트로 향상된 엔드포인트 자원 활용도 및 사용자
- 매우 안전한 VPN
- 네트워크에 민감한 어플리케이션 자원들에 대한 비인가 접속 방지.

기능

- VPN (IPSec/SSL)



검증된 엔드포인트 솔루션



NSS Labs 2018 Advanced Endpoint Protection (AED) Test

FortiClient is a top performer and "Recommended" by NSS labs in its 2018 Advanced Endpoint Protection (AEP) group test. NSS Labs expanded the scope of the AEP test and included malware, exploits, blended threats (combinations of threats), false positives, and evasions. FortiClient with integrated Sandbox blocked 100% exploits, 100% document and script-based attacks; 100% web and email attack, and offline threats with zero false positives.



Results tables

Certification tests	Windows 7				Windows 10				VB100
	FPs	FP rate	WildList misses	WildList catch rate	FPs	FP rate	WildList misses	WildList catch rate	
Faronics Anti-Virus	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
FireEye Endpoint Security	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Fortinet FortiClient	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
G DATA Antivirus	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Kaspersky Endpoint Security 10 for Windows	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
NANO Antivirus	2	0.0003%	0	100.00%	2	0.0003%	0	100.00%	
Panda Endpoint Protection Plus	1	0.0001%	0	100.00%	1	0.0001%	0	100.00%	
Panda Free Antivirus	0	0.00%	0	100.00%	1	0.0001%	0	100.00%	
Panazor CloudAntivirus	0	0.00%	0	100.00%	0	0.00%	0	100.00%	

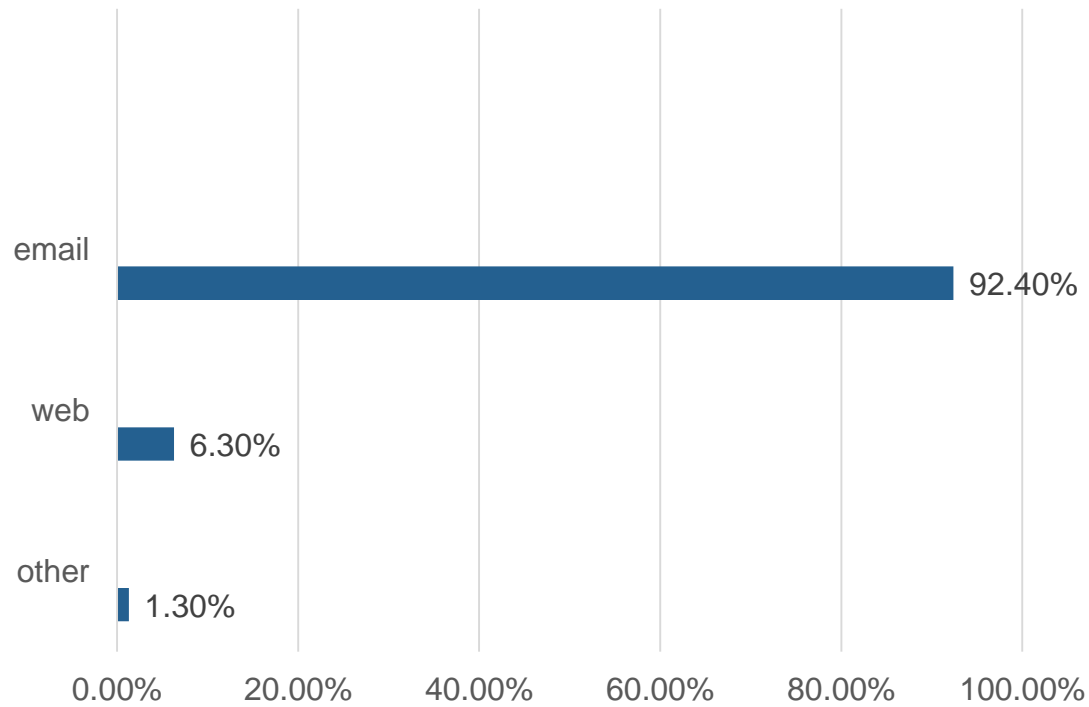
"Fortinet rarely misses a VB100 comparative, and a strong record of passes, complemented by a steady improvement in detection over the last couple of years, have put it well up with the leaders..."



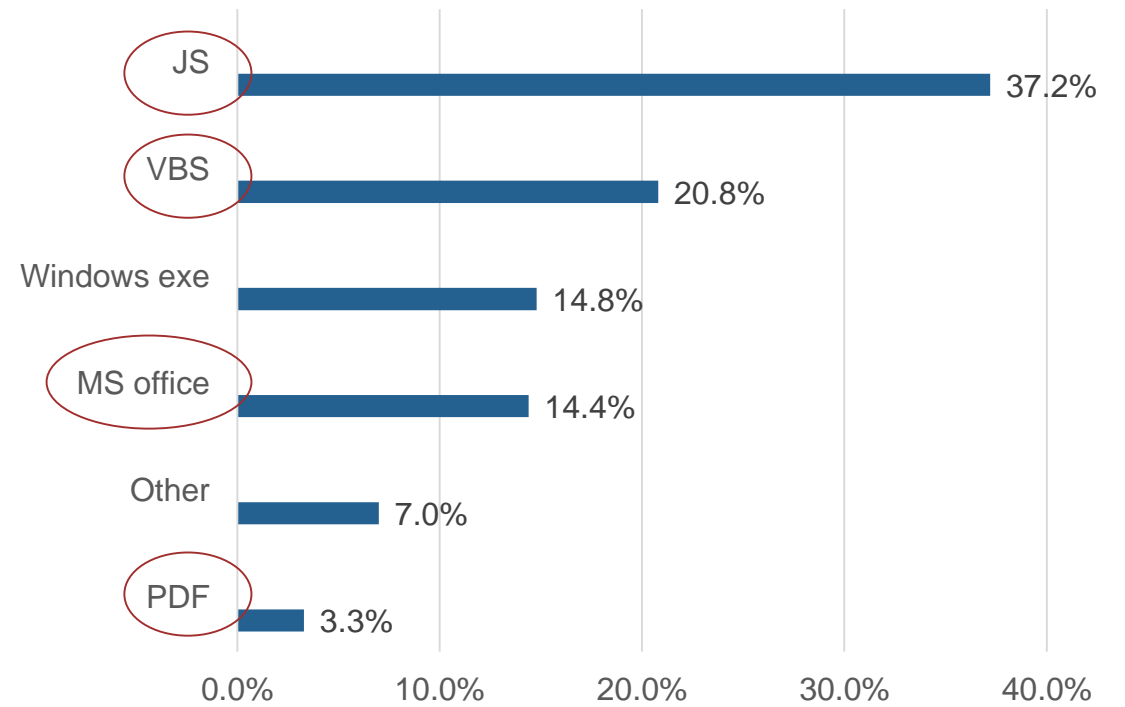
< Validated by NSS Labs and Virus Bulletin >

입증된 기능

Frequency of Malware Vectors



Frequency of Malware Type



FortiClient NSS Labs AEP test results:
Email: 100%
HTTP: 100%
Doc and Scripts: 100%

Source: Verizon DBIR 2018
NSS Labs AEP Test 2018

포티넷의 엔드포인트 및 관련 제품군



엔드포인트 지원 운영체제

- Windows
- macOS
- iOS
- Android
- ChromeOS
- Linux



엔드포인트 관리 서버

- 엔드포인트 관리
- 윈도우즈 서버에 설치되는 소프트웨어 기반
- 최대 100K까지 엔드포인트 지원



시큐리티 패브릭

- 엔드포인트 가시성 및 제어
- 컴플라이언스 제어
- UTM/NGFW 어플라이언스 또는 VMs
- 로그 관리 서버 어플라이언스 또는 VMs

요약정리



최고의 통합 네트워크 및
엔드포인트 보안



엔드포인트 가시성 및 제어



능동적인 엔드포인트 방어



자동화



낮은 TCO



The logo for FERTINET, featuring the word "FERTINET" in a bold, white, sans-serif font. The letter "E" is stylized with three horizontal bars. A registered trademark symbol (®) is located to the right of the word. The logo is centered horizontally on a blue background with a white geometric pattern of overlapping cubes and lines.

FERTINET®

Thank you.