# 공공정보자산 보호는 고성능방화벽으로

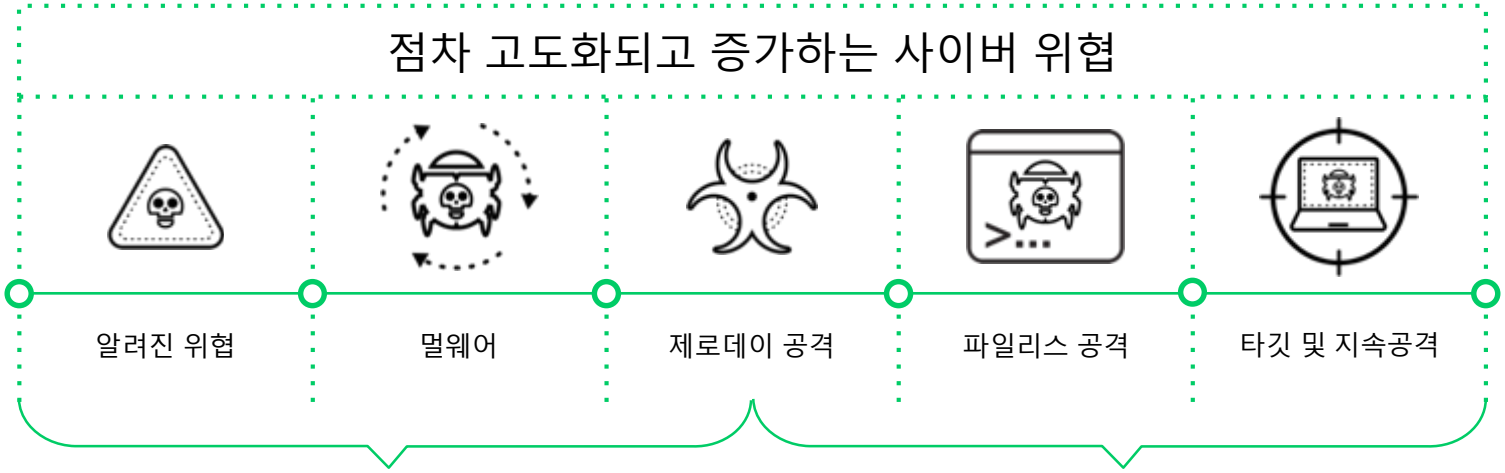
정교한 공격을 막아내는 가장 효율적이고 확실한 방법, 어플리케이션 제어

고재훈 이사 | 팔로알토네트웍스

27 January 2022

# 공공 보안의 환경 변화 및 과제

# 보안 환경의 변화




- 클라우드 서비스의 증가를 통한 공격 수준 향상
- 비트코인등을 통한 공격자의 수익 채널 증가를 통한 더욱 빈번한 국내 공격 증가

# 현재 공공기관의 보안 위협

공공기관, 보안 허점 방치…책임자가 없다

보안업계 "CISO 지정 의무화 필요"

컴퓨팅 | 입력 :2020/10/14 10:37 수정: 2020/10/14 13:24

김윤희 기자 | 기자 페이지 구독 기자의 다른기사 보기

정책 > 정치

[단독]정부 해킹 시도 한 해 10만건 넘는데… 최적 보안인력 갖춘 부처는 '0곳'

정부 해킹 시도, 최근 5년 평균 10만4759건
중국 13.9만으로 가장 많아… 미국·한국·러시아 순
정부, 정보보호 인력 최소 기준… 중앙부처 9명·지자체 12명

양범수 기자

공공 사이버위협 경보 '관심'으로 격상

류은주 기자

입력 2021.08.02 16:25

국가정보원 NATIONAL INTELLIGENCE SERVICE

국가정보원은 최근 발생하는 사이버 보안위협을 감안
. 또 경보체계가 보다 실효성 있게 운영될 수 있도록 지

[기자수첩] 구멍 숭숭 공공보안, 이래도 CISO 뒷짐질텐가

류은주 기자

입력 2021.06.23 06:00

5월 미국 최대 송유관 회사 콜로니얼 파이프라인이 랜섬웨어 해킹을 당했다. 사건은 세계를 당혹케 했다. 일반적인 민간 기업 해킹은 고객의 개인정보나 기업의 기밀 정보를 담보로 대가(몸값)를 요구하지만, 이번엔 달랐다. 산업계 전반에 영향을 미칠 수 있는 '석유' 공급이 달린 문제였다.

석유 공급 이슈는 기름값 폭등으로 이어질 수 있다. 해커는 500만달러(약 57억원)에 달하는 몸값을 요구했는데, 유류 공급 중단이 장기화될 경우 그 피해는 막대하다. 콜로니얼 측은 몰려 거자역기로 이에 응할 수밖에 없었다.

세계 최고 사이버 보안 기술력을 자랑하는 미국도 당했다. 우리나라도 안전하지

Home > 전체기사

공공기관 350개 중 90%, 316개 59만건 계정정보 다크웹에 유출됐다

좋아요 50개 | 입력 :2021-06-03 15:11

#공공기관 #350개 #계정정보 #다크웹 #인텔리전스 플랫폼 #다크트레이서

2021년도 지정 공공기관 350개 분석... 10개 기관은 1만 건 이상 계정정보 유출돼
다크웹 인텔리전스 플랫폼 다크트레이서(DarkTracer)로 다크웹 유출자료 조사 결과 발표

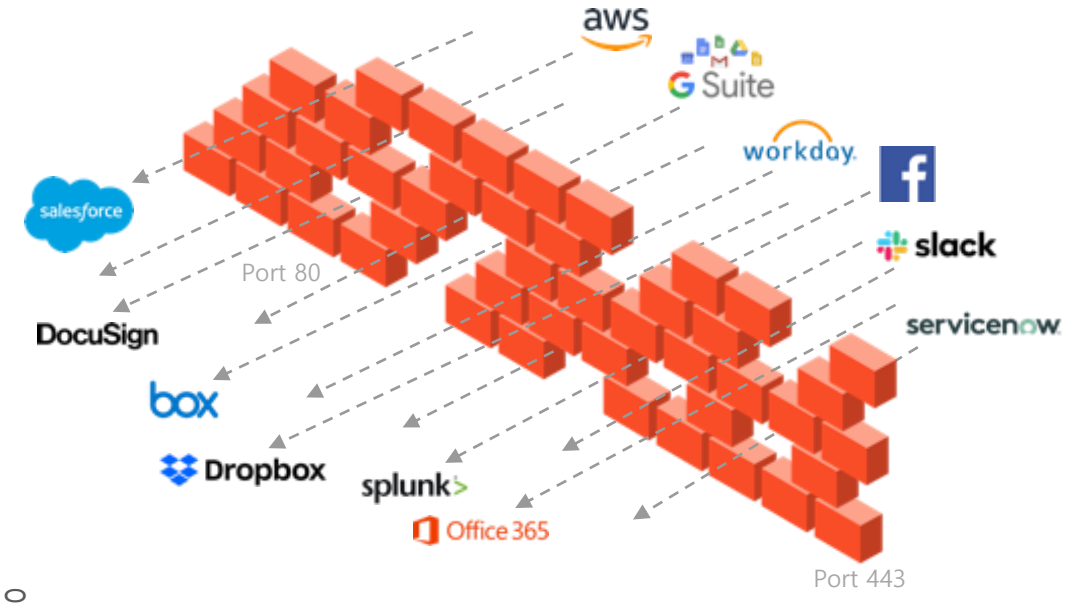
# 네트워크 보안 도전과제

## 애플리케이션 변화

- 포트 ≠ 애플리케이션
- IP 주소 ≠ 사용자
- 패킷 ≠ 콘텐츠
- IP 주소 ≠ 신뢰할 수 있는 디바이스

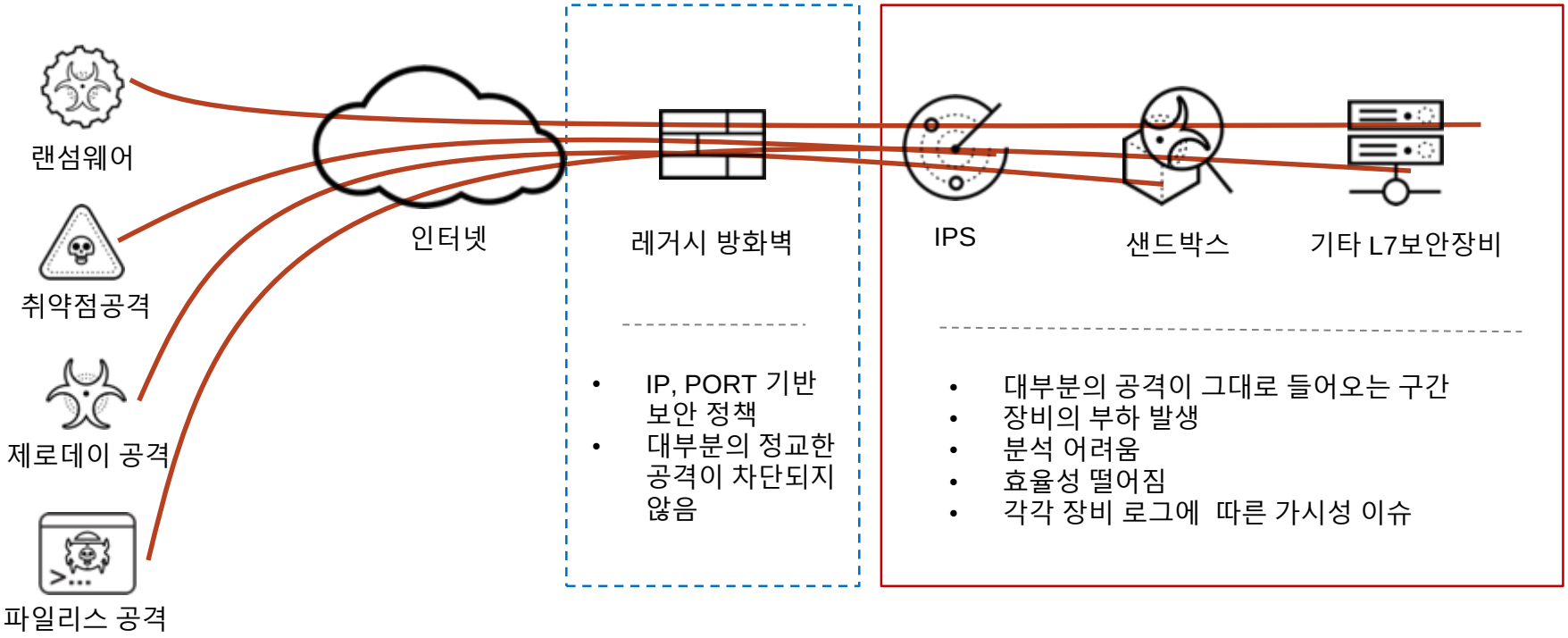
## 새로운 접근 방식 필요

- 모든 포트/프로토콜에 대한 가시성
- 항상 모든 보안 기능 활성화
- 애플리케이션, 사용자, 콘텐츠, 디바이스 식별
- 알려지거나 알려지지 않은 위협에 대한 인라인 보호
- 모든 구성 요소간의 위협 인텔리전스 공유



# 보안 환경의 변화에 따른 보안 과제



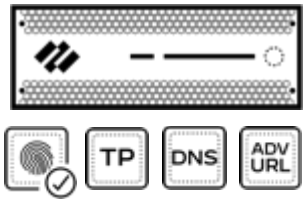

**“방화벽이 선제 제어를 하지 않으면 현재의 위협에 대응하기 위한 체계를 세울수가 없다”**

고성능 방화벽 ≠ 높은 패킷처리 성능(throughput)

고성능 방화벽 **= 성능저하 없이 L7 기반 어플리케이션 제어**

# 고성능 방화벽 기능을 통한 Hierarchical 방어체계 구축

고성능 방화벽 Hierarchical 방어체계




어플리케이션 및 알려진 위협차단

APP-ID + USER ID

L7 기반 여러가지 보안 서비스를 통한 랜섬웨어 등 효과적인 대응

라이선스추가로 손쉬운 기능 추가


샌드박싱및 L7을 통한 알려지지 않은 악성코드 분석

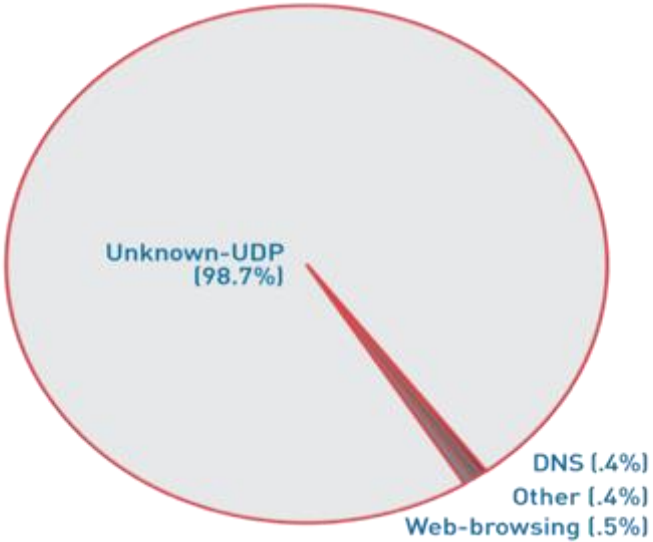
샌드박스 등 기존의 APT 제품

고성능 방화벽의 사전 차단을 통한 기존 장비 효율성 증대

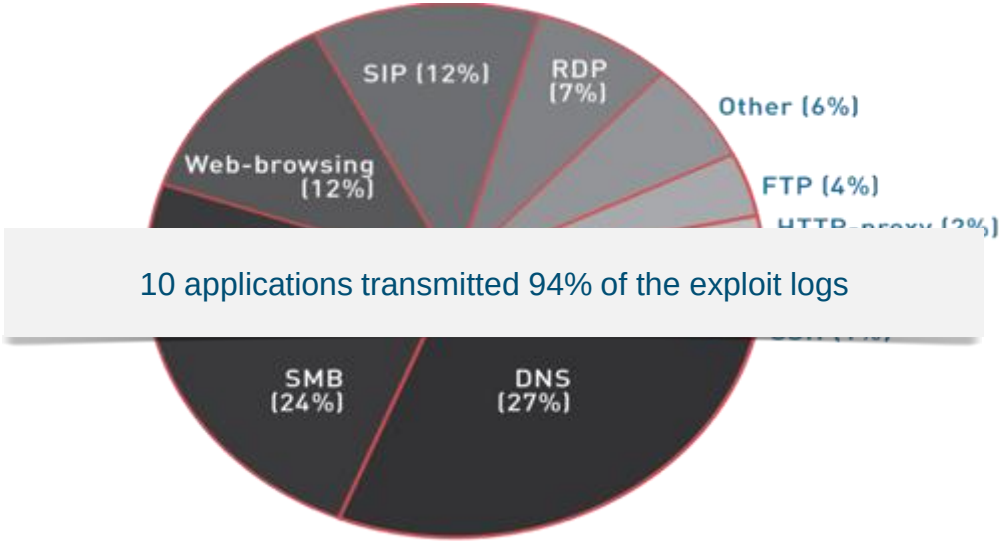
효율적인 랜섬웨어 방어 구조

# APP-ID (어플리케이션 제어) 소개

# 공격의 통로로 사용되는 애플리케이션 현황




Applications with Most Malware activity

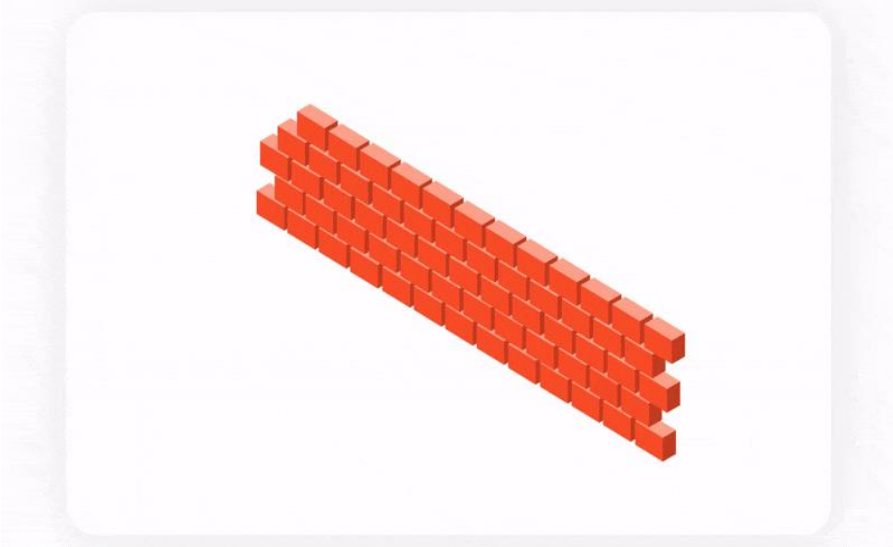



10 applications transmitted 94% of the exploit logs

Top Applications with Exploit activity

Source: Palo Alto Networks Application Usage and Threat Report (AUTR) – survey of >**5,500 networks**

# 전통적인 Port-Based Rules 와 Application-based 제어의 차이

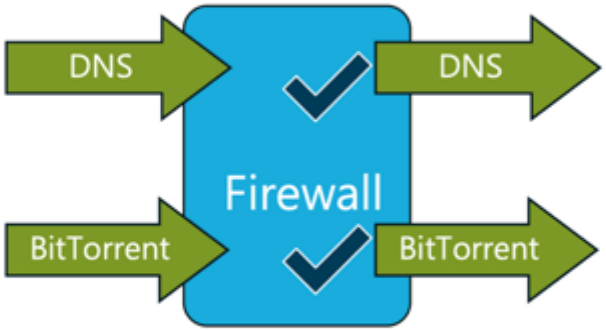


애플리케이션 기반 제어를 통해 특정 애플리케이션에만 문을 열 수 있습니다.

# 어플리케이션 제어에 대한 예시

## 레거시 방화벽

Firewall Rule: ALLOW Port 53



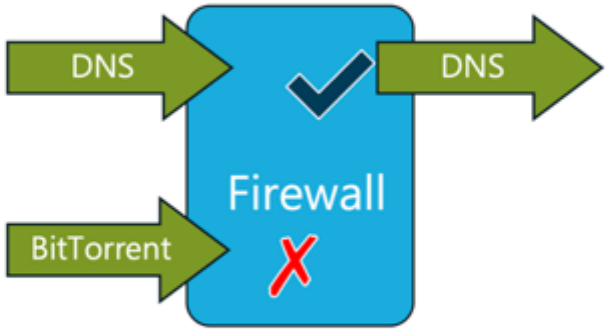

Packet on Port 53: Allow

Packet on Port 53: Allow

Visibility: Port 53 allowed

## 팔로알토네트웍스 고성능 방화벽

Firewall Rule: ALLOW DNS




DNS = DNS: Allow

BitTorrent ≠ DNS: Deny

Visibility: BitTorrent detected and blocked

# 레거시 방화벽으로 제어가 불가능한 어플리케이션 트래픽

| Order | Prot | SrcIP | SrcPort | DestIP | DestPort | Action |
|---|---|---|---|---|---|---|
| 1 | tcp | 140.192.37.2 | * | 161.120.33.* | 1433 | ACCEPT |
| 2 | tcp | 140.192.37.1 | * | 161.120.33.41 | 22 | DENY |
| 3 | tcp | 140.192.37.* | * | 161.120.33.41 | 22 | ACCEPT |
| 4 | tcp | 140.192.37.4 | * | 161.120.33.44 | 1433 | ACCEPT |
| 5 | tcp | 140.192.37.5 | * | 161.120.33.44 | 1433 | ACCEPT |
| 6 | tcp | 140.192.37.* | * | 161.120.33.44 | 1433 | DENY |
| 7 | tcp | 140.192.38.3 | * | 161.120.33.44 | 22 | DENY |
| 8 | tcp | 140.192.38.8 | * | 161.120.33.44 | 22 | DENY |
| 9 | tcp | 140.192.38.* | * | 161.120.33.44 | 22 | ACCEPT |
| 10 | tcp | 140.192.36.2 | * | 161.120.34.46 | 22 | DENY |
| 11 | tcp | 140.192.36.* | * | 161.120.34.46 | 22 | ACCEPT |
| 12 | tcp | 141.192.36.* | * | 161.121.33.* | 23 | DENY |
| 13 | tcp | 141.192.*.* | * | 161.121.33.* | 23 | ACCEPT |
| 14 | tcp | 141.192.37.3 | * | 161.121.34.3 | 80 | DENY |
| 15 | tcp | 141.192.37.5 | * | 161.121.34.3 | 80 | DENY |
| 16 | tcp | 141.192.37.* | * | 161.121.34.3 | 80 | ACCEPT |
| 17 | tcp | 141.193.38.* | * | 161.121.34.3 | 21 | ACCEPT |
| 18 | tcp | 141.193.39.* | * | 161.121.34.3 | 21 | ACCEPT |
| 19 | tcp | 141.192.*.* | * | 161.121.34.4 | 21 | ACCEPT |
| 20 | tcp | 141.*.*.* | * | 161.121.34.5 | 25 | ACCEPT |
| 21 | udp | 142.192.*.* | * | 161.122.33.43 | 69 | ACCEPT |
| 22 | udp | 143.192.*.* | * | 161.122.33.43 | 69 | DENY |
| 23 | udp | 144.*.*.* | * | 161.122.33.43 | 69 | ACCEPT |
| 24 | udp | 145.*.*.* | * | 161.122.33.43 | 69 | ACCEPT |
| 8 | tcp | 140.192.38.8 | * | 161.120.33.44 | 22 | DENY |
| 9 | tcp | 140.192.38.* | * | 161.120.33.44 | 22 | ACCEPT |
| 10 | tcp | 140.192.36.2 | * | 161.120.34.46 | 22 | DENY |
| 11 | tcp | 140.192.36.* | * | 161.120.34.46 | 22 | ACCEPT |
| 12 | tcp | 141.192.36.* | * | 161.121.33.* | 23 | DENY |
| 13 | tcp | 141.192.*.* | * | 161.121.33.* | 23 | ACCEPT |
| 14 | tcp | 141.192.37.3 | * | 161.121.34.3 | 80 | DENY |
| 15 | tcp | 141.192.37.5 | * | 161.121.34.3 | 80 | DENY |
| 16 | tcp | 141.192.37.* | * | 161.121.34.3 | 80 | ACCEPT |
| 17 | tcp | 141.193.38.* | * | 161.121.34.3 | 21 | ACCEPT |
| 18 | tcp | 141.193.39.* | * | 161.121.34.3 | 21 | ACCEPT |
| 19 | tcp | 141.192.*.* | * | 161.121.34.4 | 21 | ACCEPT |
| 20 | tcp | 141.*.*.* | * | 161.121.34.5 | 25 | ACCEPT |
| 21 | udp | 142.192.*.* | * | 161.122.33.43 | 69 | ACCEPT |
| 22 | udp | 143.192.*.* | * | 161.122.33.43 | 69 | DENY |
| 23 | udp | 144.*.*.* | * | 161.122.33.43 | 69 | ACCEPT |
| 24 | udp | 145.*.*.* | * | 161.122.33.43 | 69 | ACCEPT |

| User | HIP Profile | Zone | Address | Application | Service | URL Category | Action |
|---|---|---|---|---|---|---|---|
| any | any | L3-Untrust | any | any | application-d... | blocked-sites | Deny |
| any | any | L3-Untrust | any | office365-consumer-access | application-d... | any | Allow |
| | | | | ssl | | | |
| | | | | stun | | | |
| | | | | web-browsing | | | |
| | | | | websocket | | | |
| | | | | windows-azure-base | | | |

예를 들어 Office365 서비스를 차단시

- 레거시 방화벽의 경우 수많은 차단 정책 필요
- 그로인한 관리자 업무량 증가, 낮은 가시성
- 팔로알토 방화벽은 단 두줄의 정책으로 완벽 방어

# 모니터링 비교


| Application | Risk | Bytes | Sessions | Threats | Content | URLs |
|---|---|---|---|---|---|---|
| web-browsing | 4 | 2.2G | 84.1k | 810 | 532 | 47.9k |
| ssl | 4 | 552.9M | 22.8k | 3 | 0 | 20.1k |
| rapidshare | 4 | 456.9M | 15 | 0 | 8 | 3 |
| youtube-base | 4 | 312.3M | 200 | 0 | 193 | 42 |
| bittorrent | 5 | 277.0M | 11.3k | 0 | 0 | 0 |
| smtp | 5 | 185.9M | 2.6k | 436 | 1.1k | 37 |
| flash | 4 | 175.6M | 1.7k | 7 | 2.8k | 293 |
| blackboard | 1 | 155.1M | 3.6k | 0 | 169 | 340 |
| gmail-base | 4 | 141.4M | 1.4k | 0 | 42 | 1.3k |
| pandora | 3 | 121.5M | 554 | 5 | 83 | 260 |
| others | others | 1.4G | 91.7k | 1.3k | 942 | 13.4k |



| | Column1 | Merged |
|---|---|---|
| 1 | 192.168.1.1 - 192.168.1.24 | 192.168.1.1 |
| 2 | 192.168.1.1 - 192.168.1.24 | 192.168.1.2 |
| 3 | 192.168.1.1 - 192.168.1.24 | 192.168.1.3 |
| 4 | 192.168.1.1 - 192.168.1.24 | 192.168.1.4 |
| 5 | 192.168.1.1 - 192.168.1.24 | 192.168.1.5 |
| 6 | 192.168.1.1 - 192.168.1.24 | 192.168.1.6 |
| 7 | 192.168.1.1 - 192.168.1.24 | 192.168.1.7 |
| 8 | 192.168.1.1 - 192.168.1.24 | 192.168.1.8 |
| 9 | 192.168.1.1 - 192.168.1.24 | 192.168.1.9 |
| 10 | 192.168.1.1 - 192.168.1.24 | 192.168.1.10 |
| 11 | 192.168.1.1 - 192.168.1.24 | 192.168.1.11 |
| 12 | 192.168.1.1 - 192.168.1.24 | 192.168.1.12 |
| 13 | 192.168.1.1 - 192.168.1.24 | 192.168.1.13 |
| 14 | 192.168.1.1 - 192.168.1.24 | 192.168.1.14 |
| 15 | 192.168.1.1 - 192.168.1.24 | 192.168.1.15 |
| 16 | 192.168.1.1 - 192.168.1.24 | 192.168.1.16 |
| 17 | 192.168.1.1 - 192.168.1.24 | 192.168.1.17 |
| 18 | 192.168.1.1 - 192.168.1.24 | 192.168.1.18 |
| 19 | 192.168.1.1 - 192.168.1.24 | 192.168.1.19 |
| 20 | 192.168.1.1 - 192.168.1.24 | 192.168.1.20 |
| 21 | 192.168.1.1 - 192.168.1.24 | 192.168.1.21 |
| 22 | 192.168.1.1 - 192.168.1.24 | 192.168.1.22 |
| 23 | 192.168.1.1 - 192.168.1.24 | 192.168.1.23 |
| 24 | 192.168.1.1 - 192.168.1.24 | 192.168.1.24 |

# 참고: 어플리케이션 방화벽과의 비교

192.168.1.10

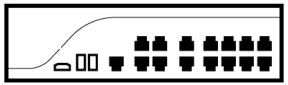
SSL, TCP/443

172.217.6.69

## 기존 레거시 방화벽

Apps Seen:
SSL to (?) Google servers

## 타사 어플리케이션 방화벽



Apps Seen:
Gmail-base

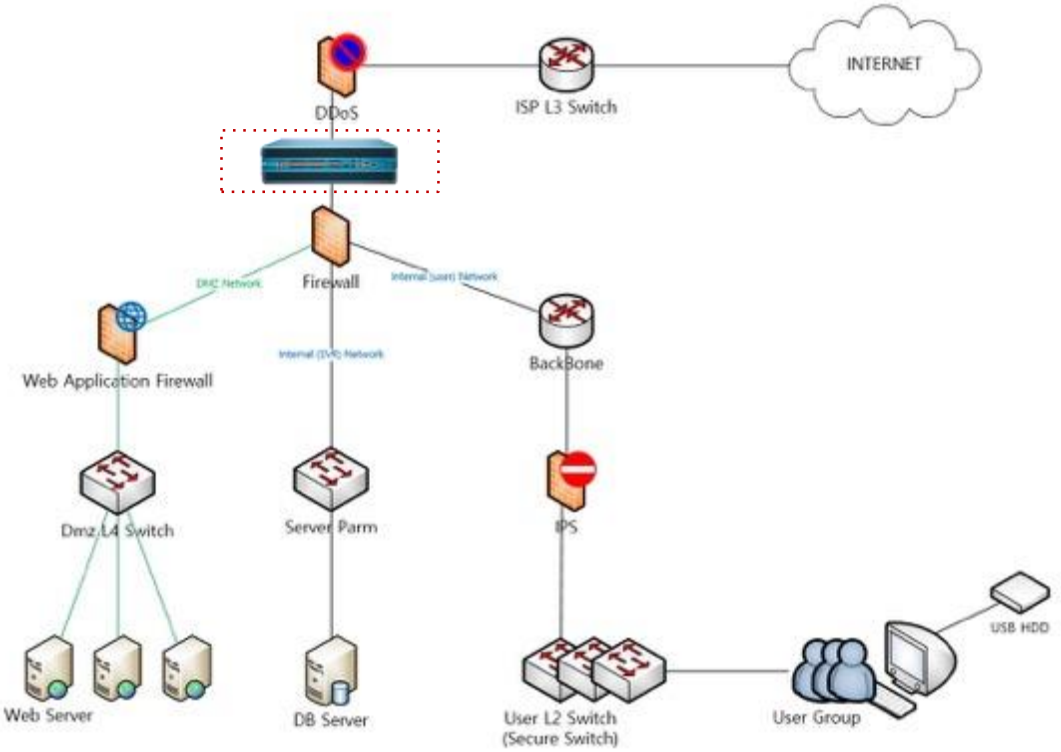
**IPS 시그니쳐 기반**

## 팔로알토 어플리케이션 방화벽


Apps Seen:
Gmail-base
Gmail-drive
Gmail-downloading
Gmail-uploading
Gmail-posting

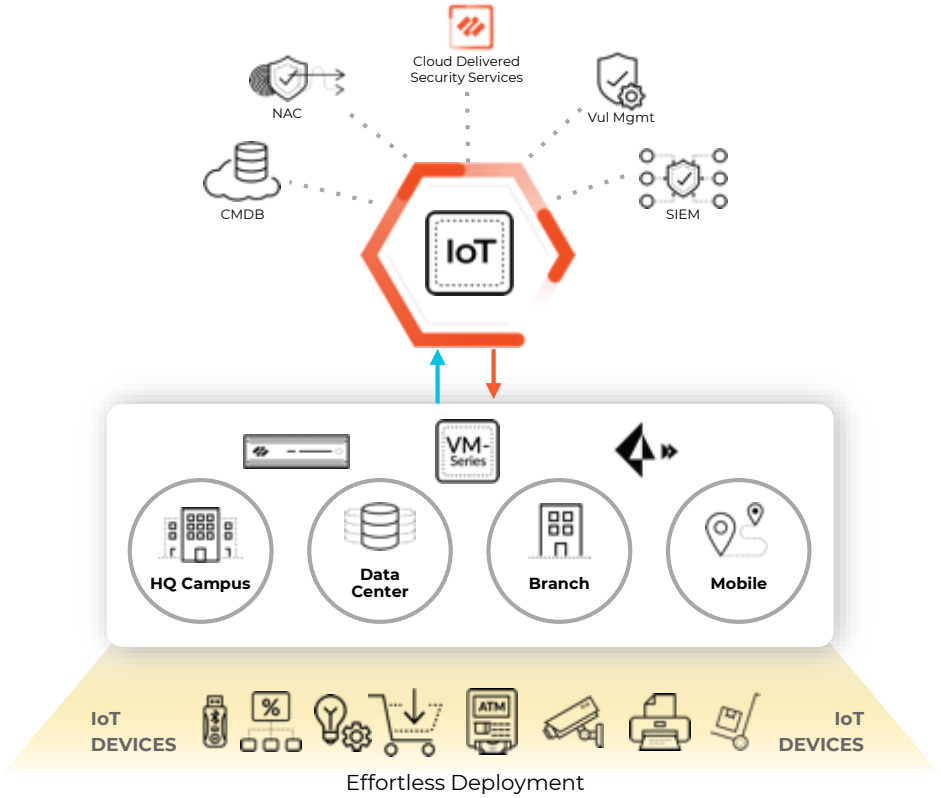
# 어플리케이션 제어 전용 보안장비로의 구성 – A 공공기관

- Vwire 모드를 통해 기존망 변경없이 구성 가능
- 방화벽 대체가 아닌 어플리케이션 전용 차단 분석 장비로 도입
- 기존 보안 정책 위에 어플리케이션 기반 보안 정책을 적용하여 보안성 및 가시승 증대 효과
- 이후 기존 방화벽을 대체함



# 클라우드& IOT & 5G security

# IOT 보안



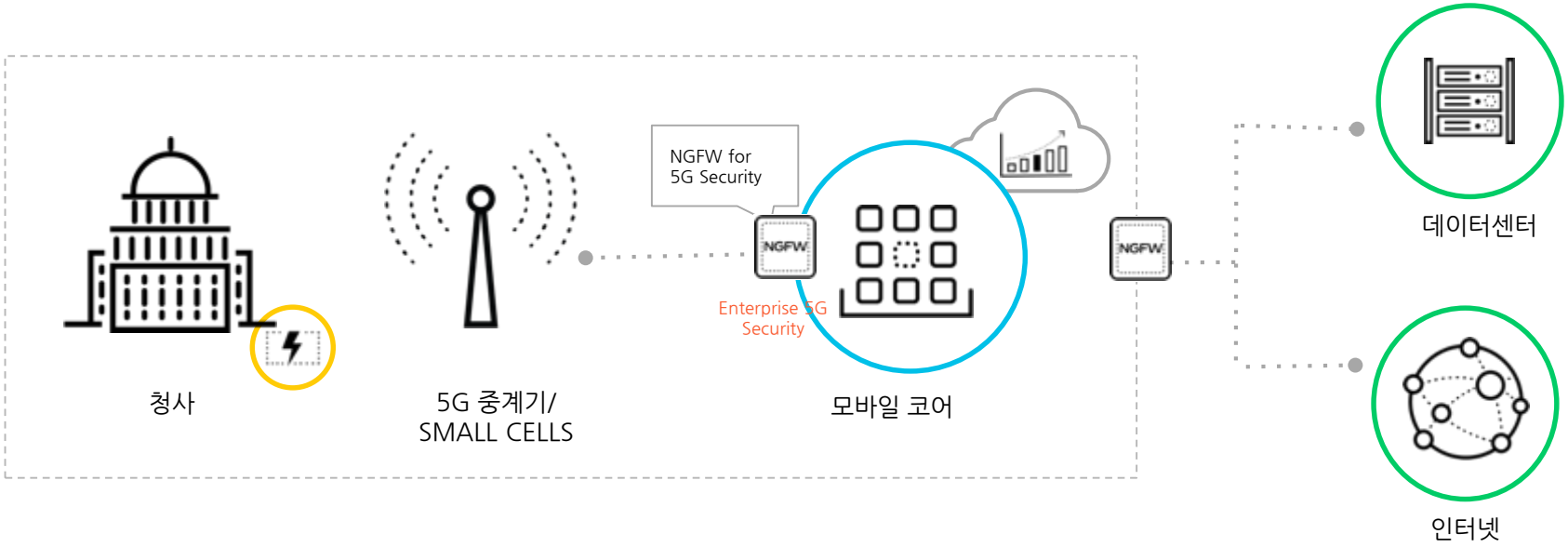

### 빠르고 정확한 Discovery
ML 및 크라우드소싱을 사용하여 이전에는 볼 수 없었던 모든 장치에 대한 가시성과 통찰력을 제공

### 동급 최고의 보호 기능을 제공
동작을 분석하여 장치 위험, 컴플라이언스 및 비정상적인 활동을 평가하고 알려진 위협과 알려지지 않은 위협을 방지

### 제로 트러스트 보안을 자동화
자동화된 최소 권한 액세스 정책 및 원클릭 적용으로 제로 트러스트 채택을 용이

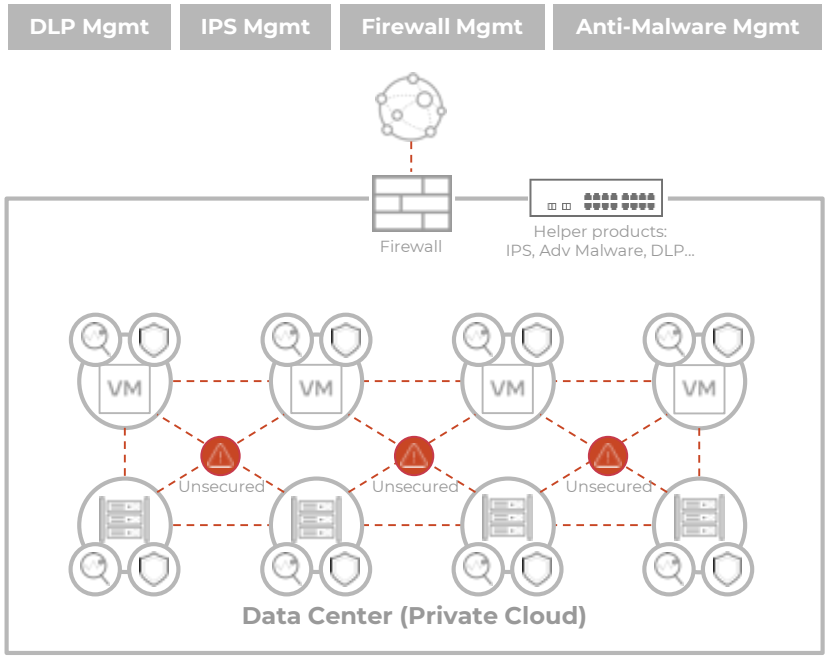
### Workflow 연동
기존 IT 및 보안 솔루션 전반에서 워크플로우를 자동화하여 IoT 사각지대 및 데이터 사일로를 제거

# 자가망 5G 보안



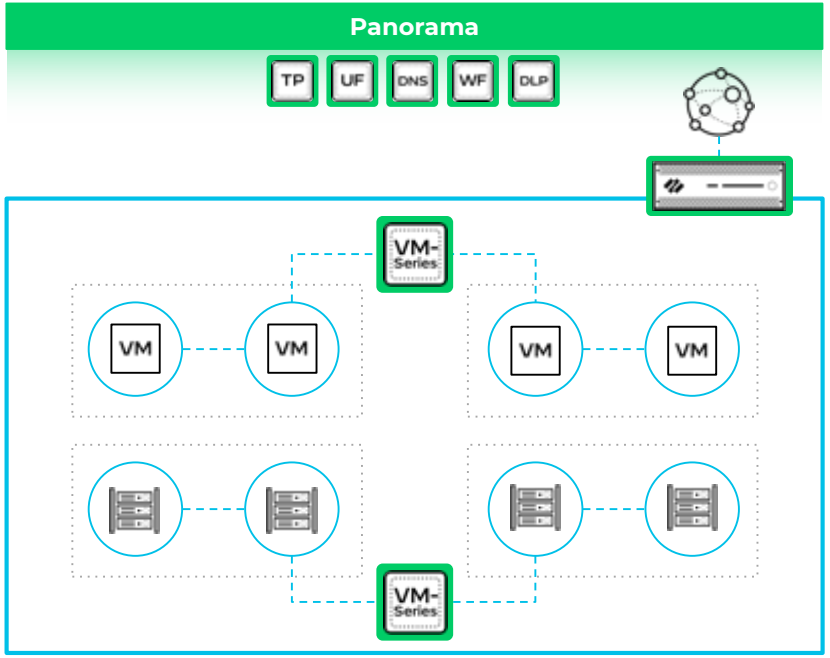

- 엔터프라이즈 5G 네트워크 트래픽의 가시성 및 제어
- 사용자 영역 내의 악성 프로그램, 바이러스, URL, C&C 및 기타 취약성 탐지 및 차단
- 감염된 장치에 대한 네트워크에서의 상관관계분석, 격리 및 검역
- 사용자/사용자 그룹별 전용 보안 정책 생성

# 공공 클라우드 인프라 보안: Private Cloud 센터용 VM, 컨테이너 방화벽




**Before**

연결이 끊어지고 무수한 보안 도구가 데이터 센터 경계를 보호하며 동서 트래픽은 보호되지 않습니다.



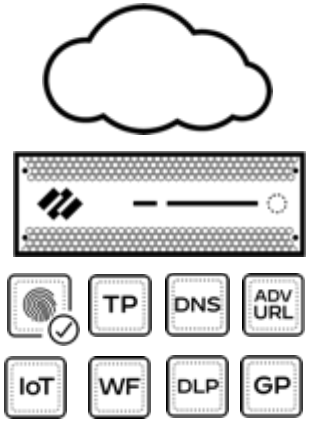

**After**

일관된 위협 보호 및 중앙 집중식 mgmt로 보안 및 보안 경계 및 East-West 트래픽 통합

# SUMMARY

# 고성능 방화벽을 통한 Hierarchical 방어체계 구축

향후 라이선스 추가만으로 기존 샌드박스등의 솔루션을 방화벽에서 통합 구성 가능




어플리케이션 제어로 Hierarchical 방어체계

어플리케이션 및 알려진 위협차단

APP-ID + TP

DGA 및 C2 차단을 통한 랜섬웨어 동작 무력화

DNS Security+
Advanced URL

샌드박싱및 L7을 통한 알려지지 않은 악성코드 분석

Wildfire
DLP

효율적인 랜섬웨어 방어 구조

# THANK YOU