의료 분야에서 지속될 랜섬웨어 및 SaaS 문제

-데이터센터부터 클라우드까지 차세대 방화벽으로 보호하라-

신봉현 차장
System Engineer

paloalto NETWORKS®

데이터 유출의 비용

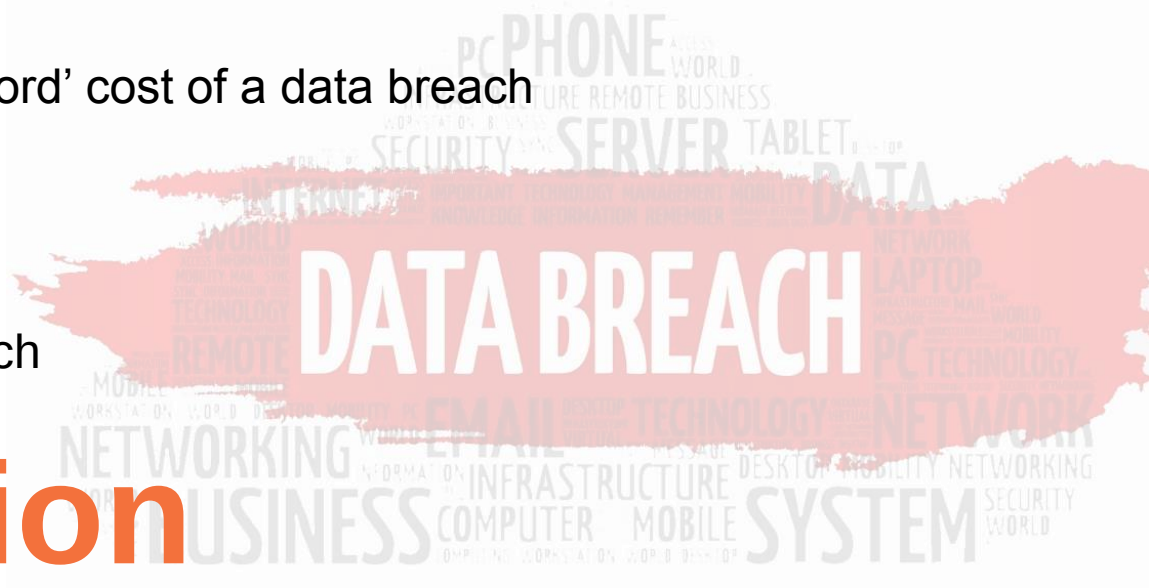
Source: *Ponemon's 2018 Cost of Data Breach Study: Global Overview*

$408

Average organizational 'per-record' cost of a data breach

103 days

Mean time to contain data breach



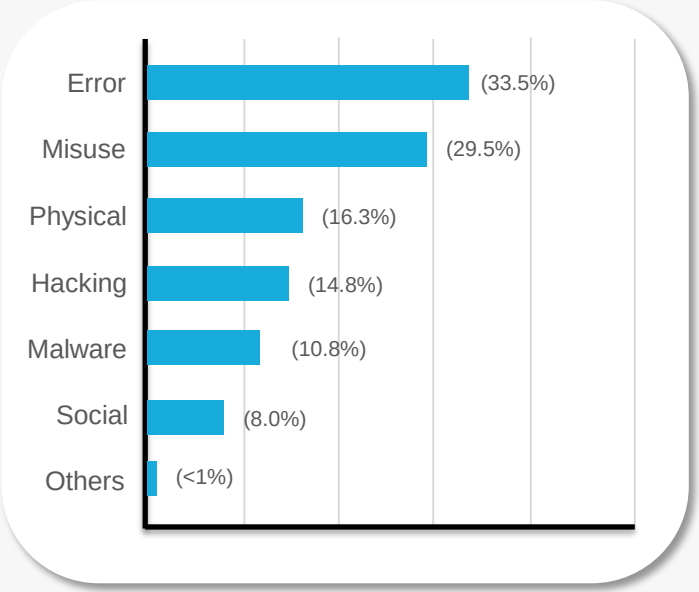
$3.86 million

Average total cost of a data breach (across all industries)

건강 관련 개인정보 유출 리포트 - 2018

Source: *Verizon PHI Data Breach Report 2018*

Verizon's 2018 PHI data breach report states that Healthcare is the only industry in which internal actors are the biggest threat to an organization



사이버 보안의 현재

Source: Fortified's *2018 Horizon Reports: The state of cybersecurity in healthcare*

100% of web application penetration tests result in demonstrating the ability to access ePHI

97% of web application penetration tests uncovered critical vulnerabilities

93% of network penetration tests demonstrated the ability to gain access to ePHI

68% of external penetration tests result in breaching the perimeter and gaining full access to the internal network

Over 40% of consumers would abandon or hesitate to use a healthcare organization if it had been hacked*

**Source: Top Health Industry issues of 2016: Thriving in the new health economy, PwC Research Institute*

72% of network penetration tests result in gaining domain admin privileges

25% of penetration tests involve compromise due to remote code execution vulnerabilities

54% of penetration tests involve compromise due to access control vulnerabilities

33% of penetration tests involve compromise due to insecure configuration of VDI and SSL VPN environment

국내 의료기관 보안 주요 뉴스

국내 대학병원 랜섬웨어 감염 의심…한국도 '빨간불'(종합2보)

송고시간 | 2017-05-13 15:59

세계 강타한 랜섬웨어, 인터넷 통해 급속도로 유포

주말 사이 국내에서도 대규모 확산 우려

[출처 : 연합뉴스]

[redacted]병원, 헬스케어 전용 클라우드 플랫폼 구축

입력 : 2017.05.11 14:33:20

[redacted]병원은 헬스케어 분야 전용 클라우드 플랫폼을 도입했다고 11일 밝혔다.

병원 측에 따르면 이 클라우드 서비스가 도입되면 환자의 의료 기록 데이터를 클라우드를 통해 수집하고, 해당 데이터를 실시간으로 분석해 빠르고 정확한 진단이 가능하다.

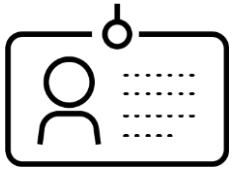
또 개인별 스마트기기를 이용해 질병 예방·식습관 관리·운동법 등의 맞춤형 관리 서비스(After Care)에 활용할 수 있고, 축적된 데이터를 분석해 새로운 의료정보를 예측하고 확보할 수 있게 된다.

HIPAA 개인정보 보호 관행 안내서에 대한 이해

1996년에 제정된 건강보험 이전과 책임에 관한 법(Health Insurance Portability and Accountability Act, HIPAA)은 귀하의 의료 정보를 열람 및 수령할 수 있는 사람에 대한 규정을 명시한 연방법입니다. 이 법에 따라 귀하는 본인의 의료 정보 및 그 정보를 공유할 수 있는 시점과 관련된 권리를 갖게 됩니다. 또한 이 법에 따라 귀하의 담당 의사, 약사 및 기타 의료 서비스 제공자, 그리고 귀하의 건강보험제도는 귀하의 권리와 귀하의 의료 정보를 사용 또는 공유할 수 있는 방법에 대하여 설명해야 합니다. 다음 단계를 따라 본 공지서와 귀하의 권리를 명확하게 이해하도록 하십시오.

의료 기관 보안 고려 사항

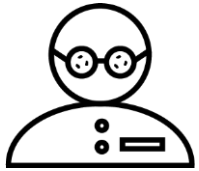
Ransomware



병원 관계자 정보 유출

개인 건강 정보 유출

Compliance

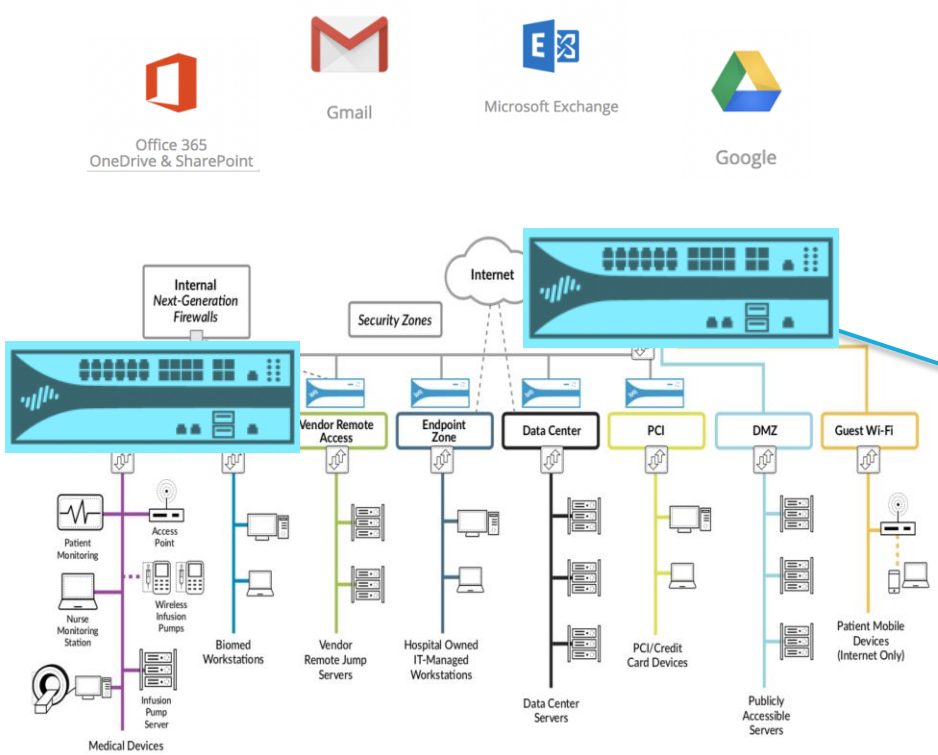


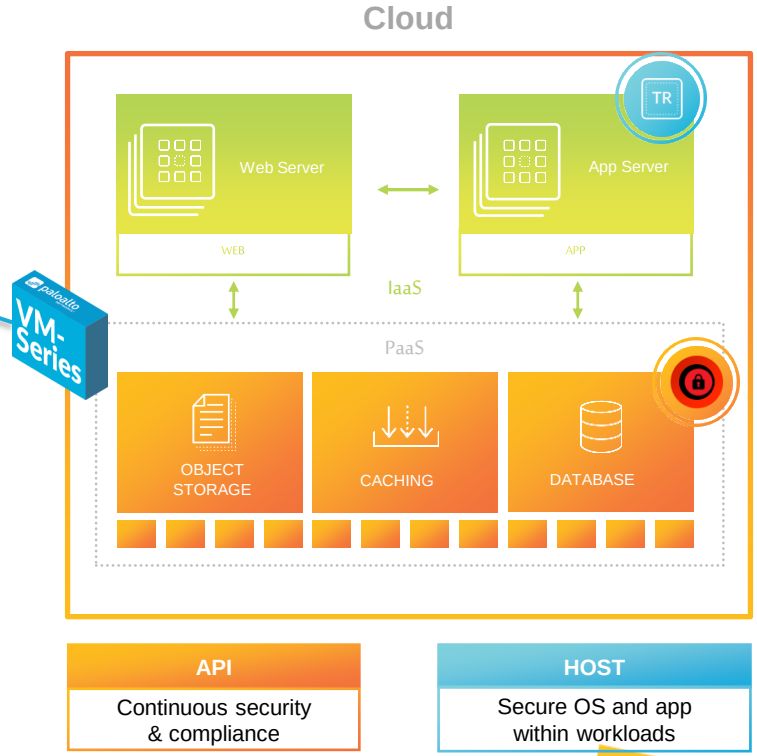
내부 관계자 위협

Cloud 보안

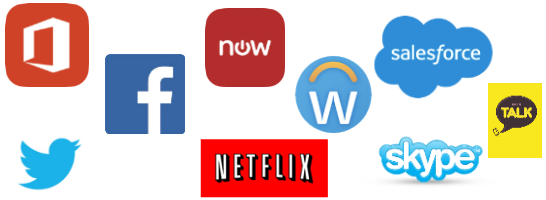
팔로알토 네트웍스
차세대 보안

팔로알토 네트웍스 in Healthcare





차세대 방화벽을 이용한 정보 보호



어플리케이션 제어

사용자/사용자 그룹 제어

컨텐츠 제어

차세대 방화벽

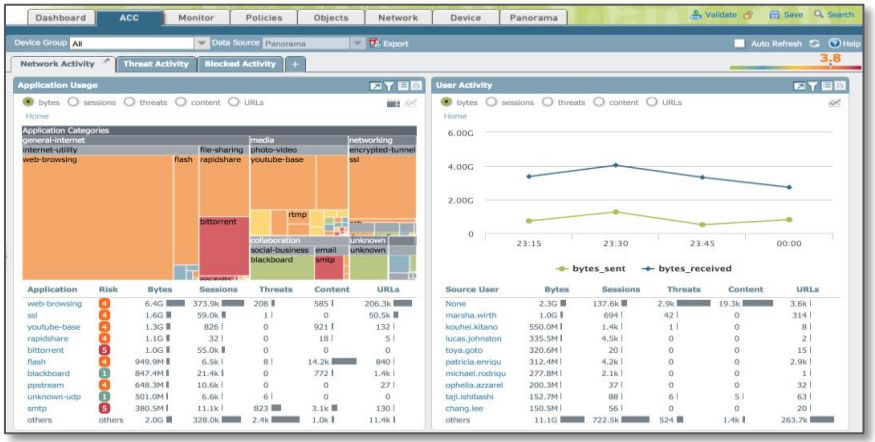
Wildfire Sandbox

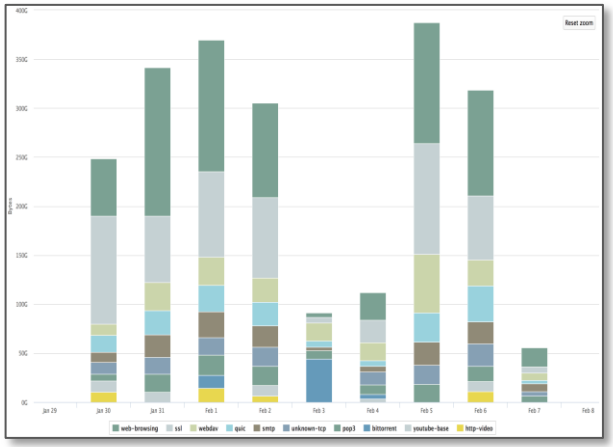
- L7 기반 차세대방화벽 : 기본 방화벽 + Application 제어 + 사용자 제어
- 외부 위협으로 부터의 보호 : Anti-Virus, IPS, WildFire 등 보안 기능
- 내부 Zone 별 트래픽 제어
- 사용자 그룹별 제어 : 업무별 보안 정책 적용
- 사용자 계정 도난 방지 시스템
- 다중 인증 방식 도입
- 패턴매치 방식 개인정보 유출 방지

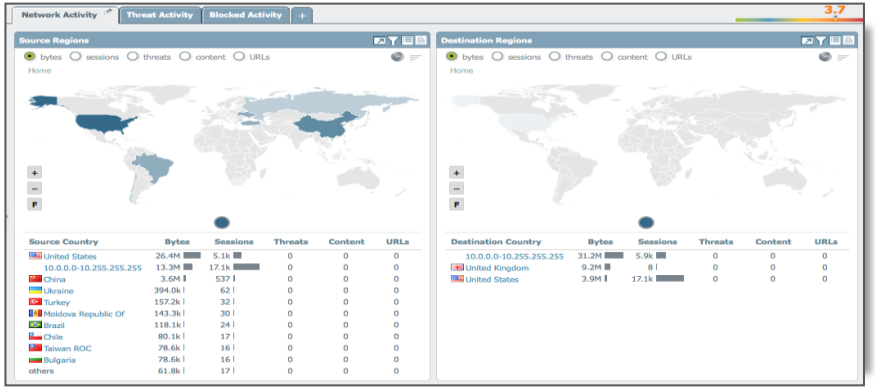
Credential Theft Prevention

MFA

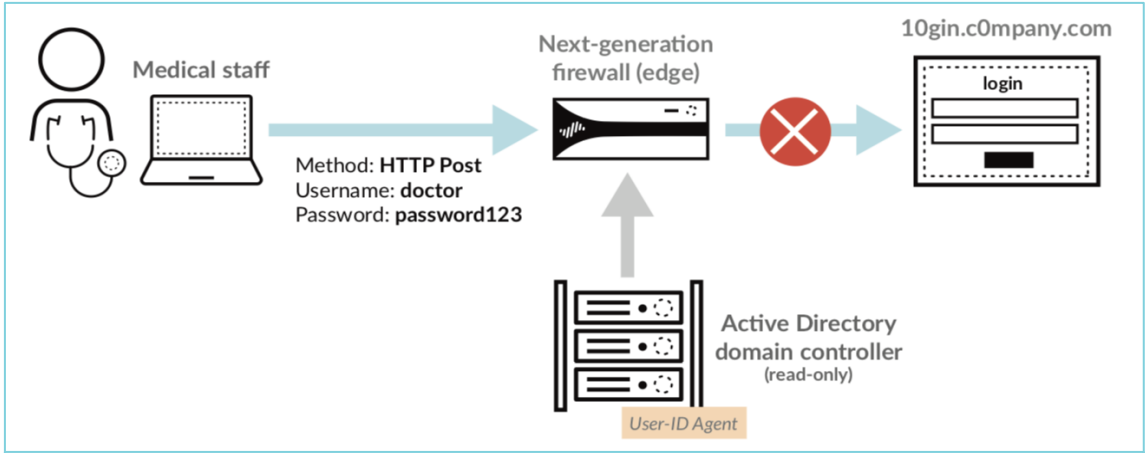
트래픽 가시성 확보

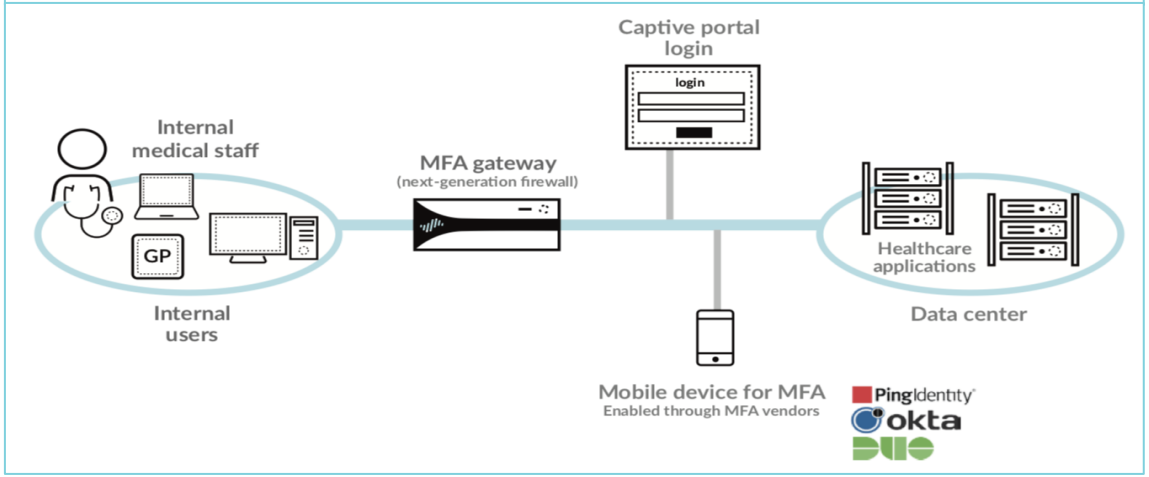






차세대 방화벽을 활용한 내부 정보 유출 방지





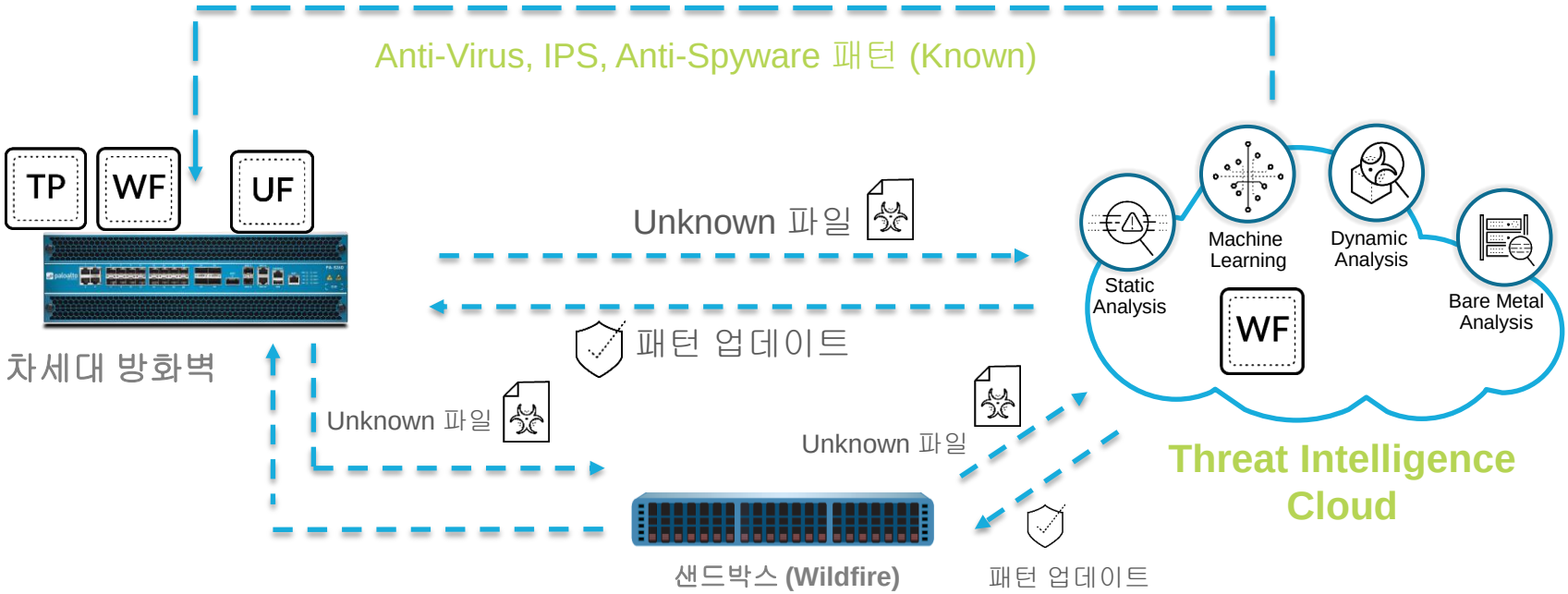
Credential Theft Prevention

- 피싱사이트에 정보 유출 방지
- AD 서버와 연동하여 내부 계정 외부유출 방지

다중 인증 방식

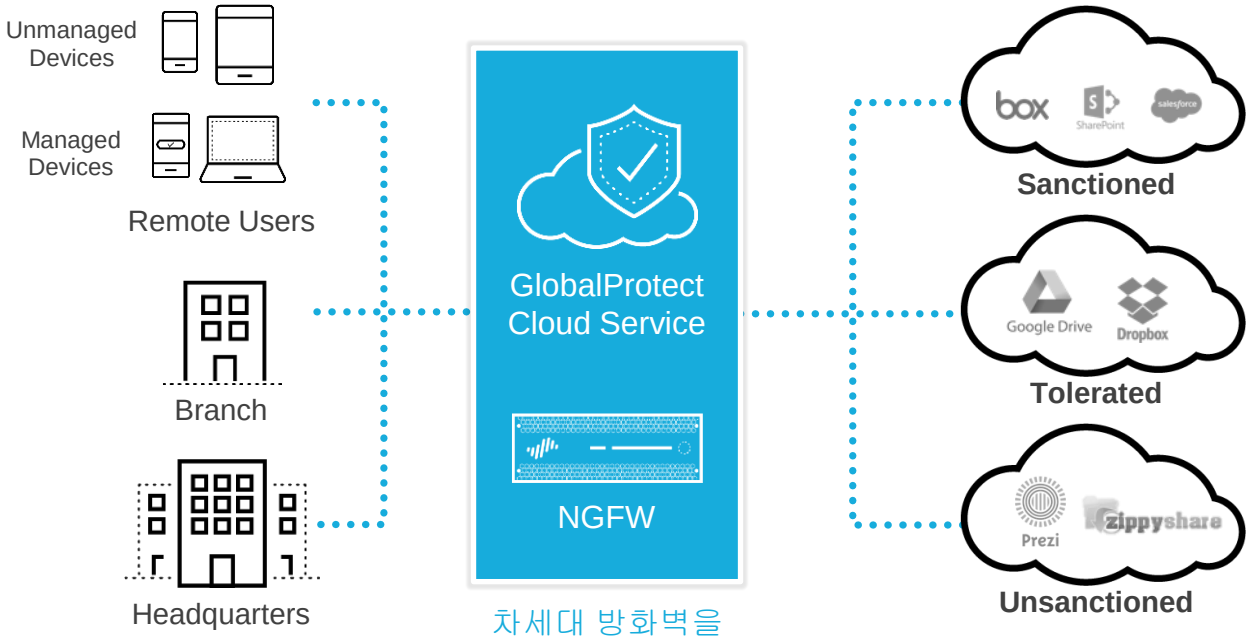
- 유출된 계정을 이용한 내부 접근 제어
- 외부 유출된 계정을 이용하여 접근하더라도 다중 인증 방식을 이용하여 보안 강화

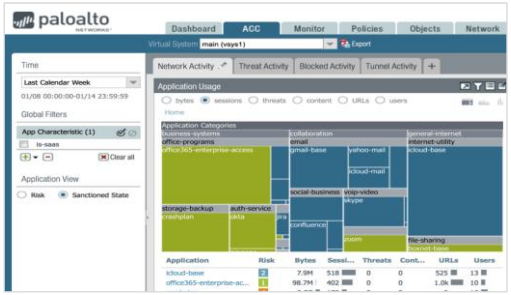
알려진/알려지지 않은 멀웨어 탐지 및 차단



Threat Intelligence Cloud – Global WF, 3rd Party, CTA 등 에서 수집된 Threat 정보

어플리케이션 형 클라우드 대응 (SAAS)





차세대 방화벽을 이용하여 SaaS 어플리케이션 접근 트래픽에 대한 보안 검사

HIPAA 컴플라이언스

- HIPAA 는 건강정보 관리에 대하여 최소한의 보안 요구사항을 정리.
  많은 HIPAA 보안 요구 사항 중 일부 내용 소개:
  - Access control: User identification at the firewall restricts user access to applications or zones.
  - Integrity controls: Advanced threat prevention features maintain the integrity of PHI by preventing malware and exploits.
  - Audit controls: Audit logging with native user identification provides access reports for systems with poor reporting capabilities that contain PHI.
  - Transmission encryption: Application detection at the firewall directs security teams to systems using unsecure protocols, such as FTP and HTTP, to transfer PHI.

시큐리티 오퍼레이팅 플랫폼과 HIPAA 보안 룰

HIPAA Standard	Requirement	팔로알토 네트웍스의 기술 지원
§ 164.312(a)(1)	**Access control:** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4) [Information Access Management].	차세대 방화벽을 이용하여 사용자를 인지하여 사용자 기반의 보안정책 마련. 전체 존 혹은 건강 정보를 가지고 있는 특정 어플리케이션에 대하여 정책 적용.
§ 164.312(a)(2)(i)	**Unique user identification:** Assign a unique name and/or number for identifying and tracking user identity.	개별적인 사용자 이름을 로그로 남기기 때문에 어떠한 행동을 했는지 확인 가능
§ 164.312(a)(2)(iv)	**Encryption and decryption:** Implement a mechanism to encrypt and decrypt electronic protected health information.	암호화 되지 않은 프로토콜, 즉 FTP등과 같은 프로토콜을 이용할 경우 별도로 로깅할 수 있음.
§ 164.312(b)	**Audit controls:** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	사용자 기반으로 Audit logging 을 지원

		팔로알토 네트웍스의 기술 지원
§ 164.312(d)	**Person or entity authentication:** Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	MFA 인증을 이용하여 복합 인증 시도
§ 164.312(e)(1)	**Transmission security:** Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	비암호화된 프로토콜을 이용할 경우 확인 가능하며, 통제 및 로깅 가능함
§ 164.312(e)(2)(ii)	**Encryption:** Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	
§ 164.312(c)(1)	**Integrity:** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Anti-malware, anti-exploit, TI 를 제공하여 건강 정보가 malware 등에 의해 변형되거나 감염되는 것을 보호
§ 164.312(c)(1)	**Integrity controls:** Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	
164.308(a)(5)(ii)(B)	**Protection from malicious software:** Implement procedures for guarding against, detecting, and reporting malicious software.	

팔로알토 네트웍스 APT 진단/분석 SLR

▣ 팔로알토 네트웍스 SLR(Security Lifecycle Review) 개요

- **개요** : 내부 인터넷 트래픽 분석을 통해 보안위협 및 사용중인 애플리케이션/웹 등에 대한 종합 정보 제공하여 강력한 보안 정책을 구축하기 위함

- **상세 목적**
  - 사용중인 애플리케이션/웹 및 취약점 노출에 대한 위협의 가시성 제공
  - 애플리케이션 사용 통계를 이용하여 관측된 위협 노출 정보 제공
  - 이미 알려진 멀웨어 혹은 알려지지 않은 멀웨어 탐지 (Zero-day 공격 탐지)
  - 악의적인 혹은 업무상 불필요한 웹 접속 내용 제공

- **탐지 항목** : 안티 바이러스, 안티 스파이웨어, 취약점 공격 차단, 웹 필터링, 파일 전송 제어, 제로데이 공격(알려지지 않은 공격)

- **SLR 구축 방안** : 탭 구성 – 미러링을 이용하여 트래픽을 차세대 방화벽으로 전달하는 방식으로 내부 구성 및 트래픽에 영향 없이 보안위협 및 트래픽 정보 제공

- **결과 리포트 제공** : 결과 요약 제공, 애플리케이션 사용 현황 제공, 탐지된 멀웨어/취약점 공격 내용 제공, 잠재적인 위협 분석 내용 제공

팔로알토 네트웍스 APT 진단/분석 SLR

▣ 팔로알토 네트웍스 SLR 결과 항목 서머리

- **사용중인 애플리케이션**
  - 업무용 / 비업무용 포함 총 275개 탐지
- **고위험 애플리케이션**
  - 네트워크 외부로 파일을 전송하는 등의 보안 취약점을가지고 있는 애플리케이션 총 75개 탐지
- **네트워크 상에서 발견된 Threat**
  - Vulnerability Exploits, 알려진/알려지지 않은 멀웨어, 외부와의 C&C(command and control) 통신 등을 포함하여 총 455,796 건 탐지

275 APPLICATIONS IN USE

75 HIGH RISK APPLICATIONS

455,796 TOTAL THREATS

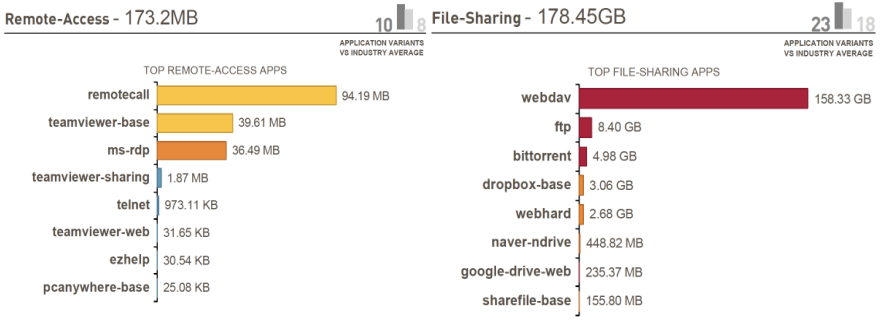
300,965 VULNERABILITY EXPLOITS

868 KNOWN MALWARE

346 UNKNOWN MALWARE

Report Period: 8 Days
Start: Wed, Jan 31, 2018
End: Wed, Feb 07, 2018

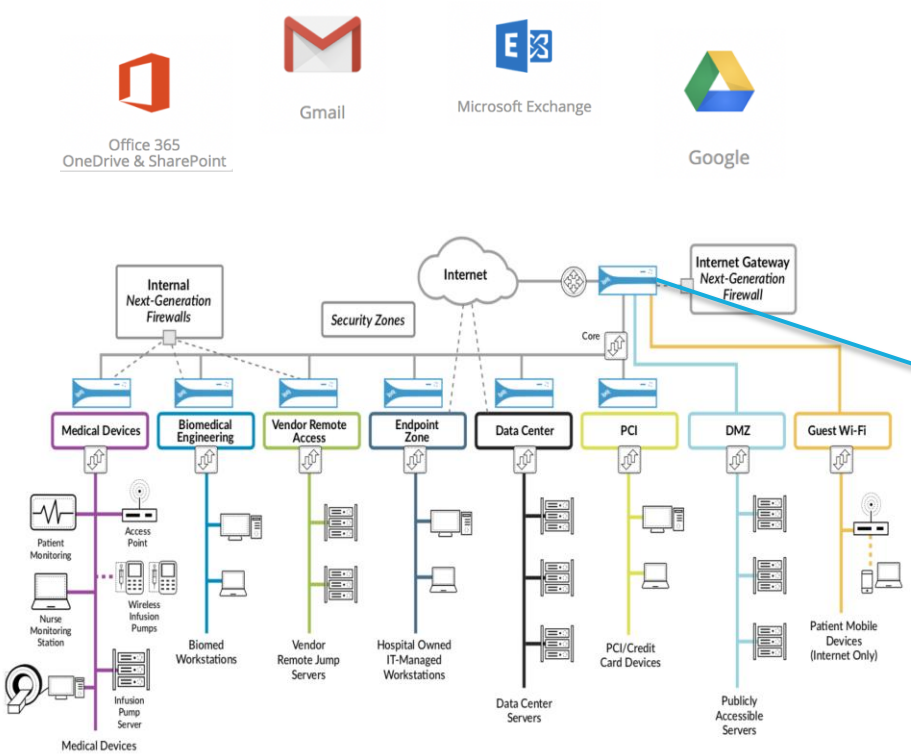
[SLR 결과 요약 제공]

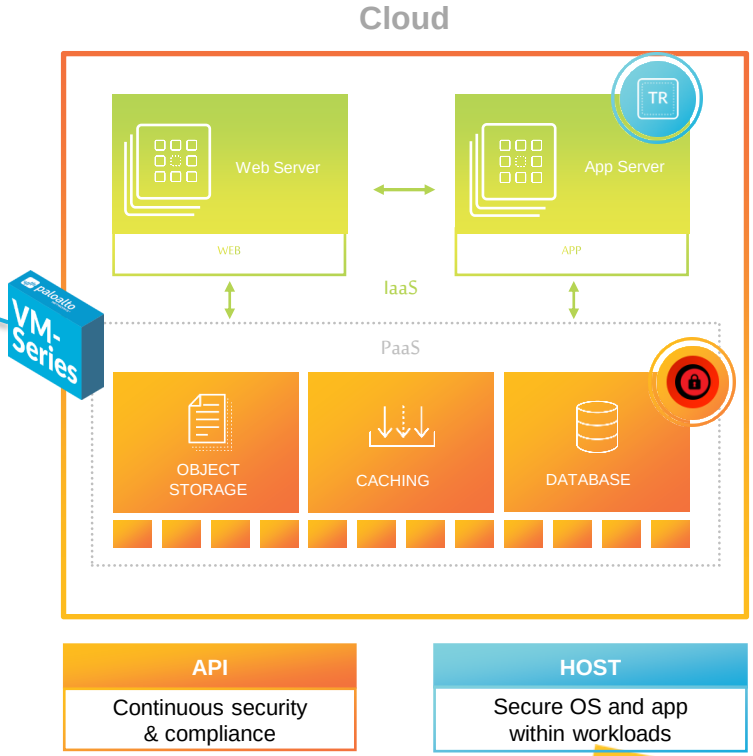


[애플리케이션별 트래픽 사용량 제공]

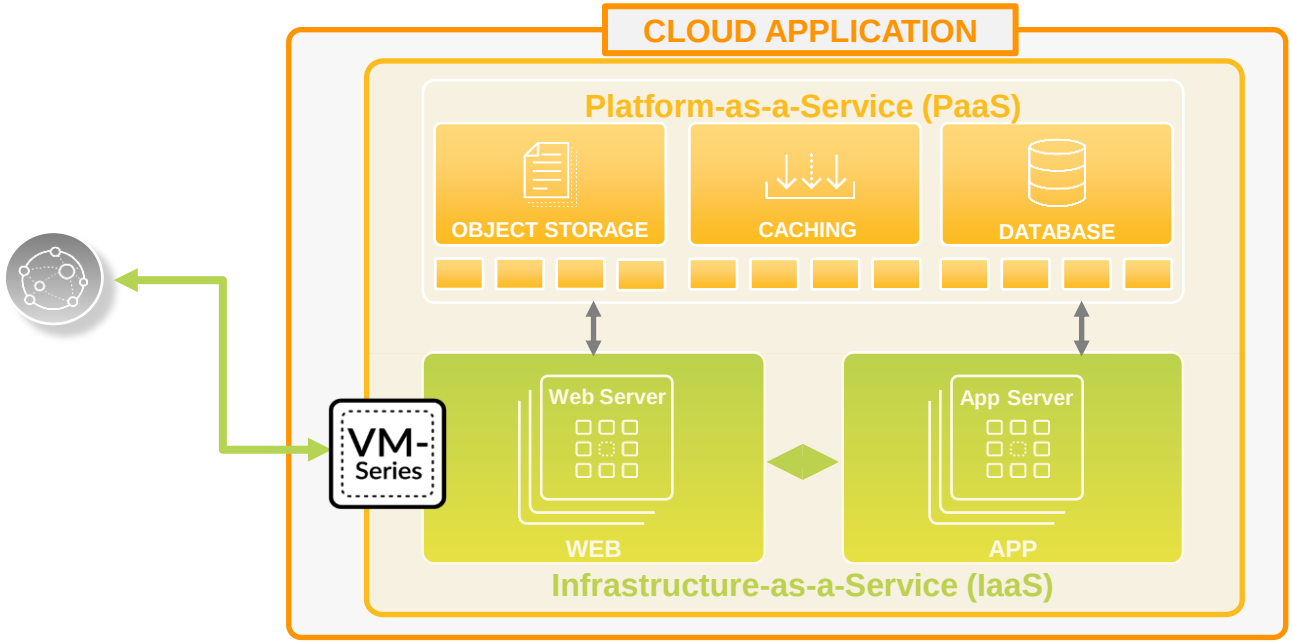
[애플리케이션별 발견된 취약점 분석 제공]

팔로알토 네트웍스 in Healthcare





클라우드의 보안 by Palo Alto Networks



Prevent outbound and inbound attacks	Application visibility and workload segmentation	Centrally manage and automate deployments

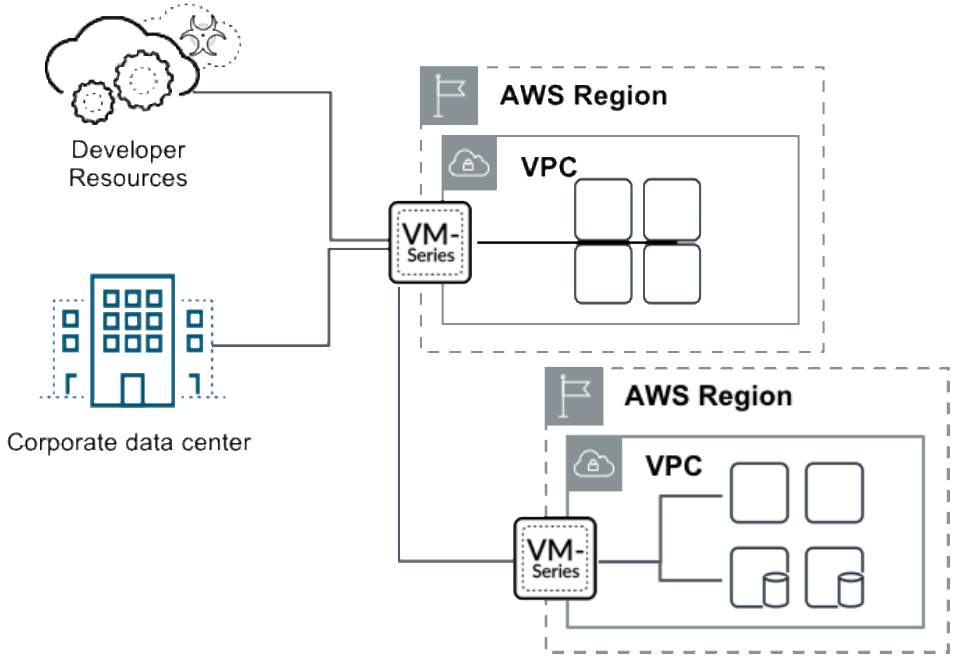
차세대 방화벽 in Cloud

내부 가상 서버의 보호

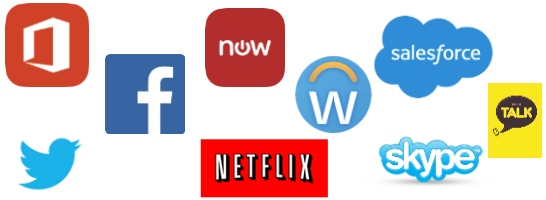
알려진/알려지지 않은 공격에 대한 보호

IPSEC VPN을 이용한 DataCenter 와 암호화된 통신

*기존 **DataCenter** 에서 통합 관리 - **Panorama***



차세대 방화벽 in Cloud



어플리케이션 제어

사용자/사용자 그룹 제어

컨텐츠 제어

차세대 방화벽 VM-Series

- L7 기반 차세대방화벽 : 기본 방화벽 + Application 제어 + 사용자 제어
- 외부 위협으로 부터의 보호 : Anti-Virus, IPS, WildFire 등 보안 기능
- South-North 및 East-West 간 트래픽 보호
- Dynamic Address Group 을 통한 정책 자동화 방안 지원
- 부트스트래핑을 통한 자동 확장 방안
- Panorama 를 통한 PA-Series 및 VM-Series 통합 관리

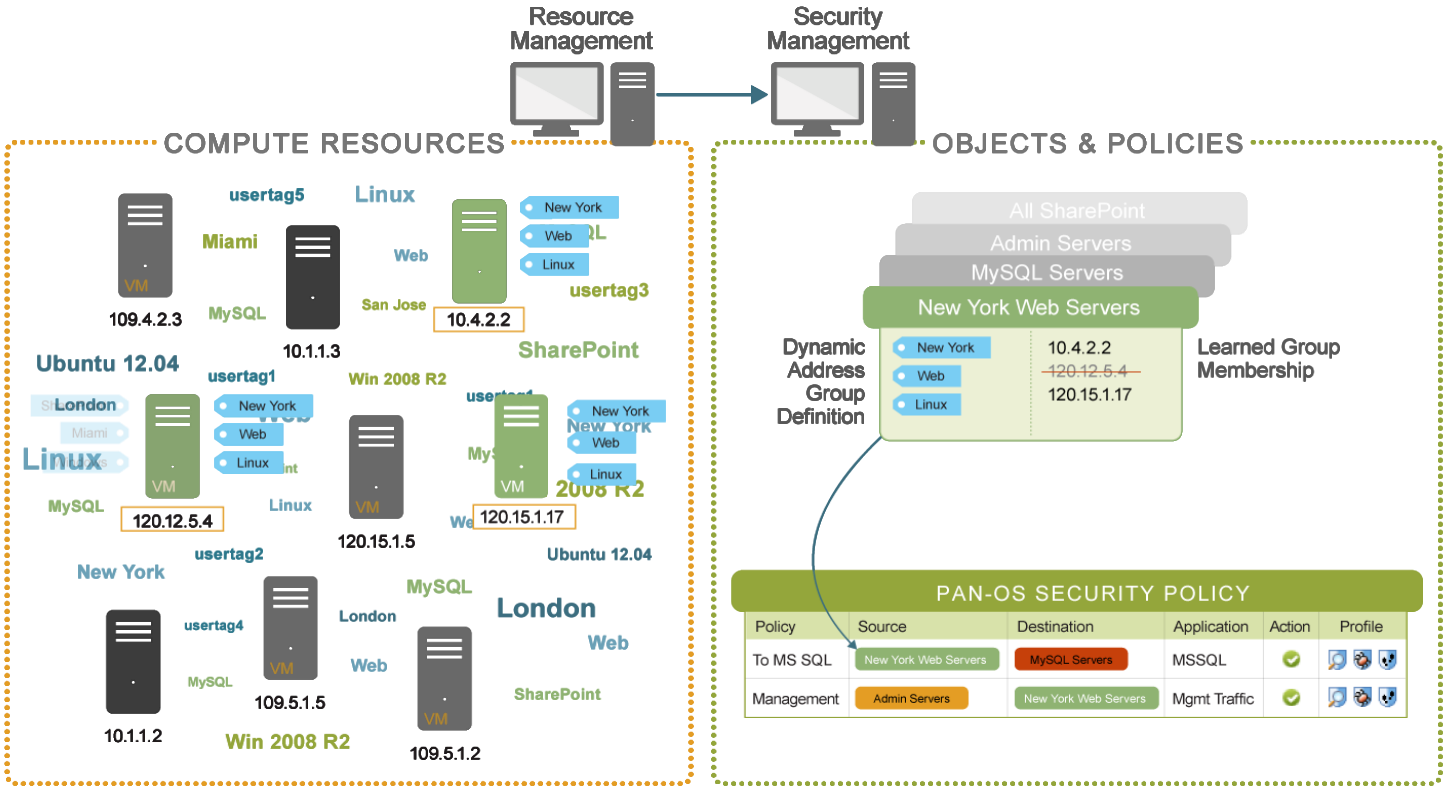
Wildfire Sandbox

Dynamic Address Group

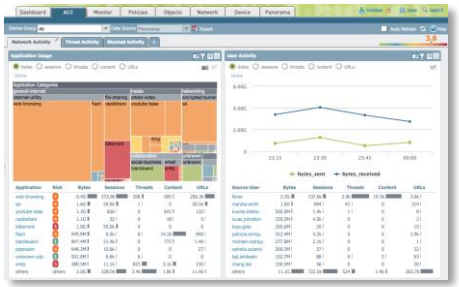
XML-Based Rest API

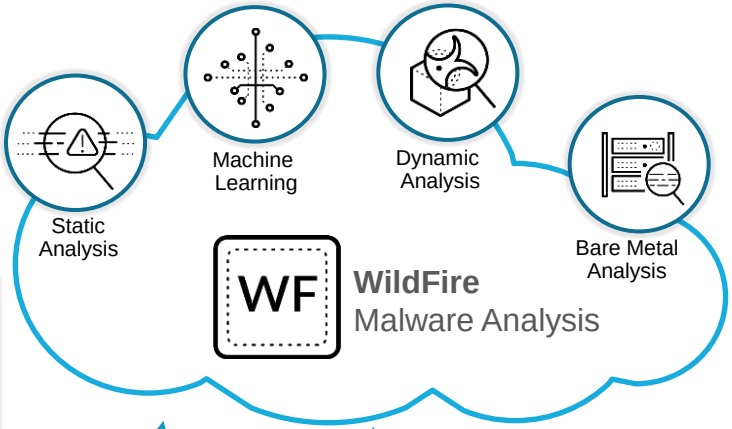
VM monitoring

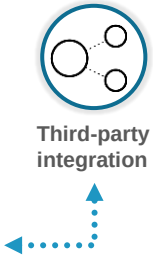
새로 생성된 서버의 방화벽 정책?

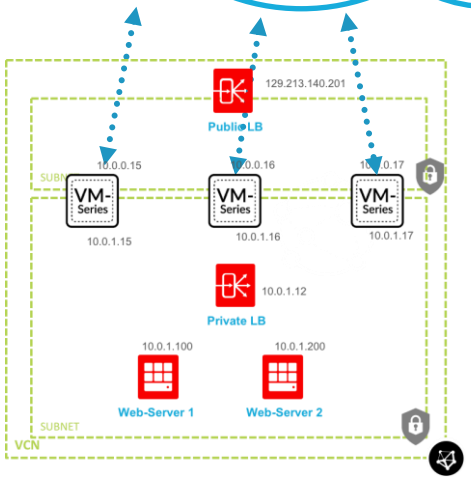


Cloud 환경의 유해 트래픽 차단









Threat Prevention
- Anti-Virus, IPS, Anti-Spyware

APT (SandBox)
- Cloud 기반 Sandbox

URL Filter
- 악성 및 유해 사이트, C&C 접근 통제

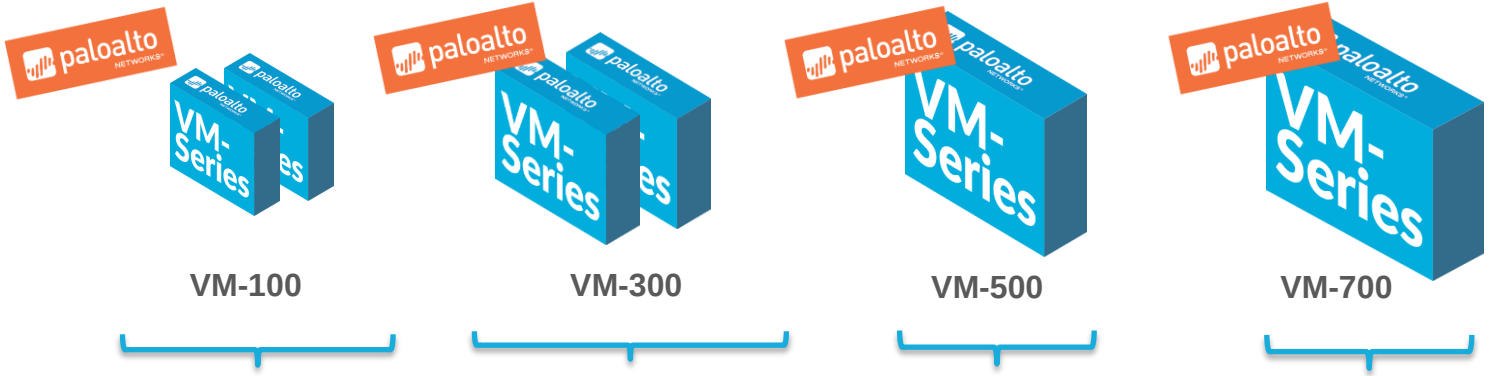
VM-Series 모델

aws

Google Cloud Platform

ORACLE Cloud

Alibaba Cloud



VM-100

VM-300

VM-500

VM-700

VM-100	VM-300	VM-500	VM-700
VCPU : 2 초당 신규 세션 : 9K 최대 세션 : 250K License : BYOL	VCPU : 2, 4 초당 신규 세션 : 9K 최대 세션 : 800K License : BYOL or Market place	VCPU : 2, 4, 8 초당 신규 세션 : 20K 최대 세션 : 2M License : BYOL	VCPU : 2, 4, 8, 16 초당 신규 세션 : 40K 최대 세션 : 10M License : BYOL

THE WORLD'S LEADING CYBERSECURITY COMPANY

85

of Fortune 100

rely on Palo Alto Networks

63% of the Global 2

are Palo Alto Networks custome

Figure 1. Magic Quadrant for Enterprise Network Firewalls

Source: Gartner (October 2018)

7년 연속 Leader

60,000+

customers

in 150+ countries

J.D.POWER 2018 CERTIFIED ASSISTED TECHNICAL SUPPORT

2018 tsia RATED OUTSTANDING ASSISTED SUPPORT GLOBAL | PALO ALTO NETWORKS

9.1/10

average CSAT score

Q4FY2018. Fiscal year ends July 31

Gartner, Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 1Q18, 14 June 2018

THANK YOU