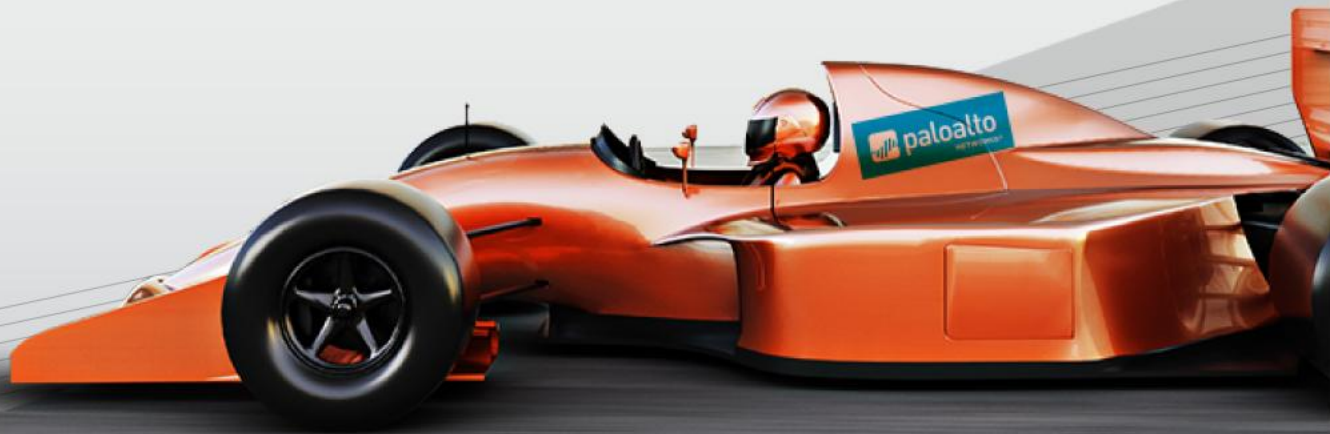


“금융권 클라우드 보안”

이제부터가 시작입니다!



PALO ALTO NETWORKS KOREA

김민석 이사, Cloud Security Specialist, 팔로알토 네트워크스
(stkim@paloaltonetworks.com)



클라우드 환경 보안을 위한 도전과제



리스크 없이 좀 더 빨리..



은행



투자



회계



신용판매



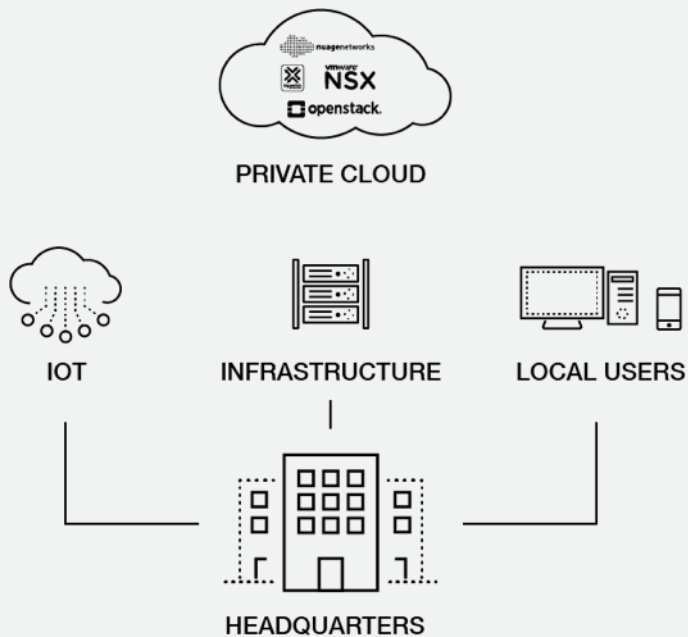
보험



경제학



보안장비의 전통적인 위치는..



보안장비의 전통적인 위치는..

Anti-Phishing

Threat Intel

UBA

Forensics



IOT

Orchestration

MFA



PRIVATE CLOUD



INFRASTRUCTURE



HEADQUARTERS

IPS

AV

Sandbox

URL/IP



LOCAL USERS

Endpoint AV

EDR

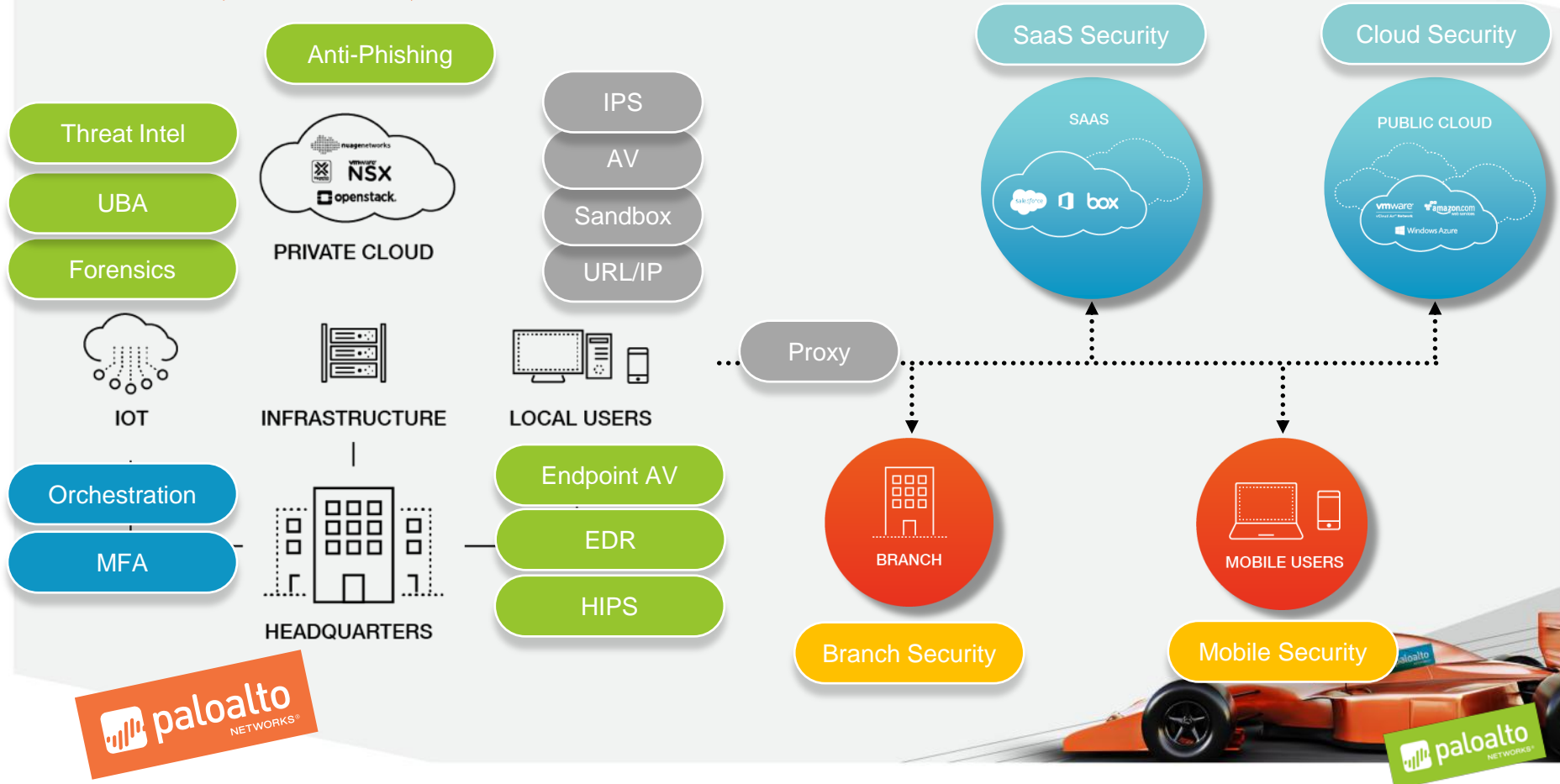
HIPS

 paloalto
NETWORKS®

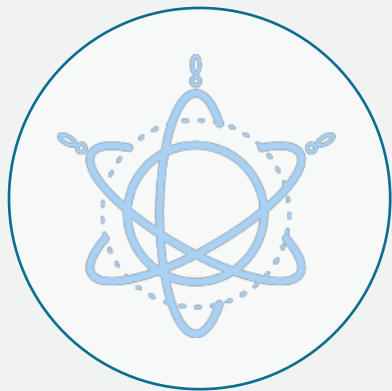
 paloalto
NETWORKS®



사용자, 데이터, 애플리케이션은 다양한 위치에 있습니다..



직면한 보안과제



가시성의 한계



과도한 경보
및
로그 처리



수동대응
및
자동화 부족



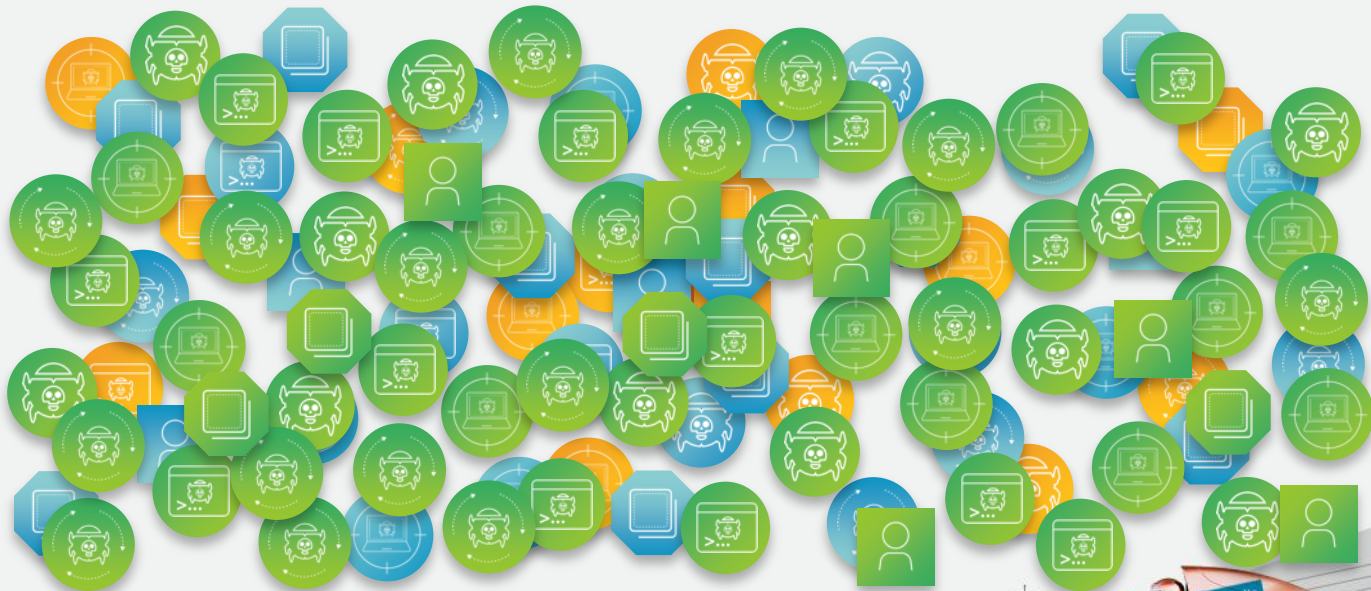
사이버 공격을 성공적으로 사전 차단하려면..

네트워크

엔드포인트

클라우드

가시성 확보



사이버 공격을 성공적으로 사전 차단하려면..

REDUCE MANUAL EFFORT WITH ANALYTICS

● 가시성 확보

● 공격가능영역
줄이기



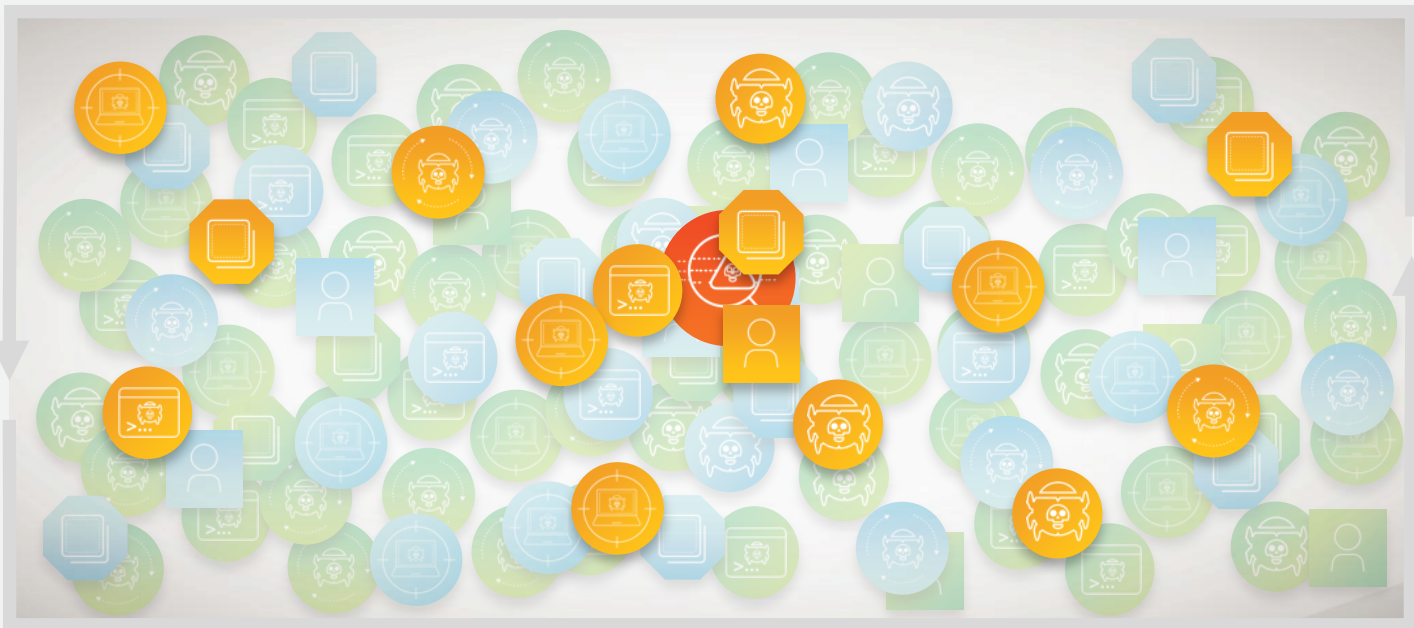
AUTOMATION OF ENFORCEMENT



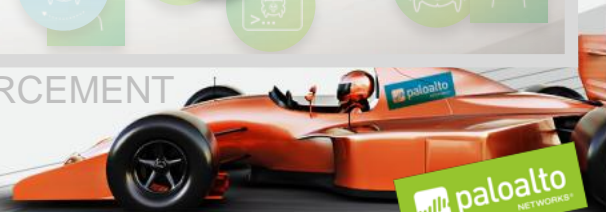
사이버 공격을 성공적으로 사전 차단하려면..

REDUCE MANUAL EFFORT WITH ANALYTICS

- 가시성 확보
- 공격가능영역 줄이기
- 알려진 위협 차단



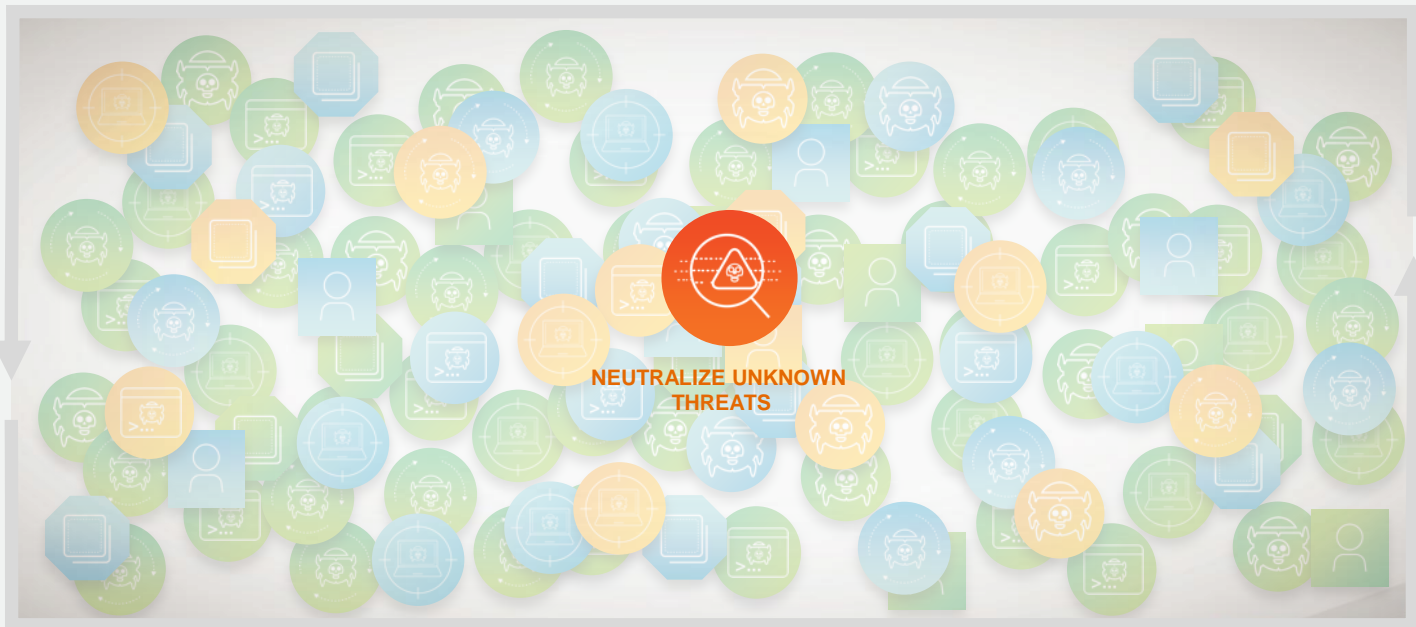
AUTOMATION OF ENFORCEMENT



사이버 공격을 성공적으로 사전 차단하려면..

REDUCE MANUAL EFFORT WITH ANALYTICS

- 가시성 확보
- 공격가능영역 줄이기
- 알려진 위협 차단
- 알려지지 않은 위협 차단



AUTOMATION OF ENFORCEMENT



보안목표 및 전략

1

사전차단능력 극대화
수동대응최소화

2

빠른대응
(threats software
cannot prevent)

3

일관된 보안정책
(for all users, data, and
applications)

4



금융권 클라우드 보안?

HOW?

팔로알토 네트워크스 가상 방화벽



팔로알토 네트워크 플랫폼



Threat Prevention



URL Filtering



WildFire



AutoFocus



Logging Service



LightCyber



MineMeld



CLOUD-DELIVERED SECURITY SERVICES



NETWORK SECURITY



ADVANCED ENDPOINT PROTECTION



CLOUD SECURITY



팔로알토 네트워크스 플랫폼: 개방 & 확장

PALO ALTO NETWORKS APPS



3RD PARTY PARTNER APPS



CUSTOMER APPS



CLOUD-DELIVERED SECURITY SERVICES

APPLICATION FRAMEWORK & LOGGING SERVICE



NETWORK SECURITY



ADVANCED ENDPOINT PROTECTION



CLOUD SECURITY



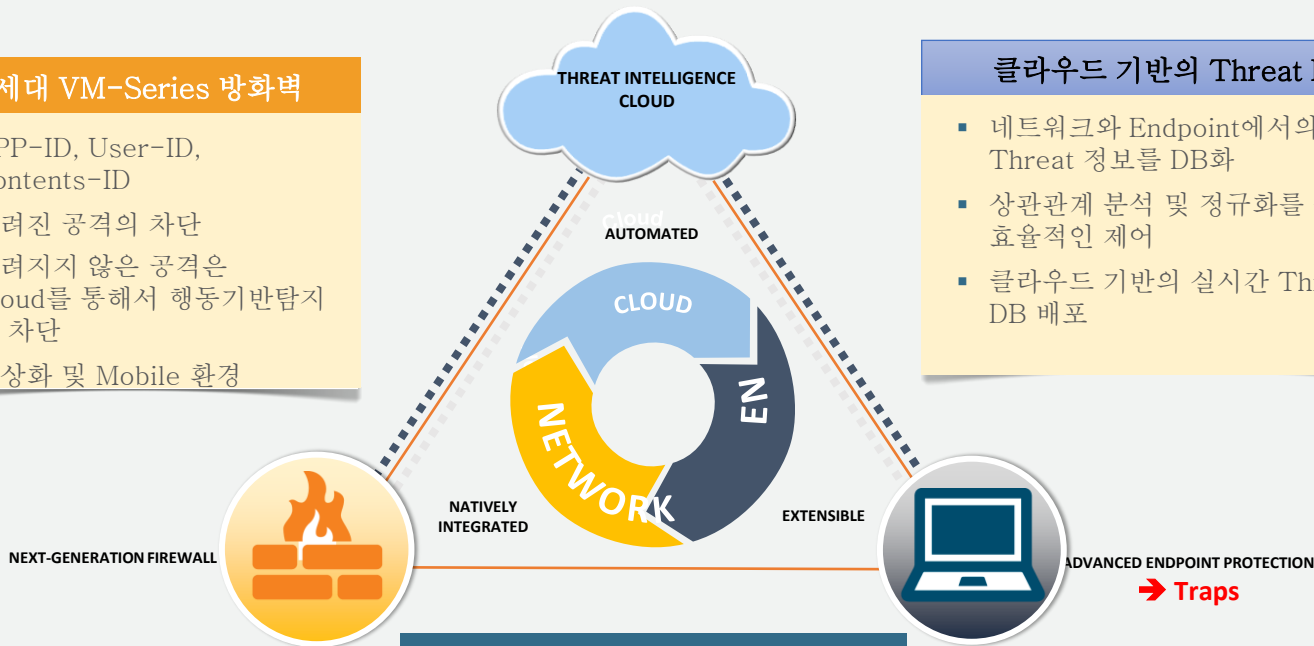
Palo Alto Networks - Enterprise Security Platform

차세대 VM-Series 방화벽

- APP-ID, User-ID, Contents-ID
- 알려진 공격의 차단
- 알려지지 않은 공격은 Cloud를 통해서 행동기반탐지 및 차단
- 가상화 및 Mobile 환경

클라우드 기반의 Threat DB

- 네트워크와 Endpoint에서의 모든 Threat 정보를 DB화
- 상관관계 분석 및 정규화를 통한 효율적인 제어
- 클라우드 기반의 실시간 Threat DB 배포



차세대 Endpoint 보안

- 모든 프로세서와 파일들의 이상징후 판단
- 단말 기반의 각종 행위를 통제
- 클라우드와 실시간 연동



클라우드 환경을 위한 Security Challenge

- Amazon Web Services
- MS Azure - Google Cloud

- VMware ESXi
- VMware NSX
- KVM w/optional OpenStack plugin
- Citrix SDX
- Cisco ACI, MS Hyper-V

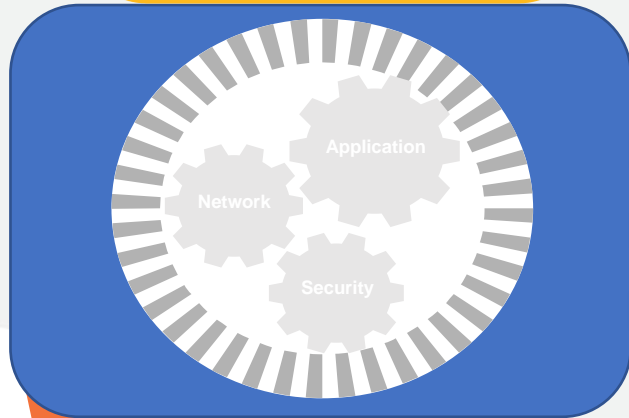


Public Cloud 차세대 보안 서비스 적용



Private Cloud 차세대 보안 서비스 적용

Orchestration

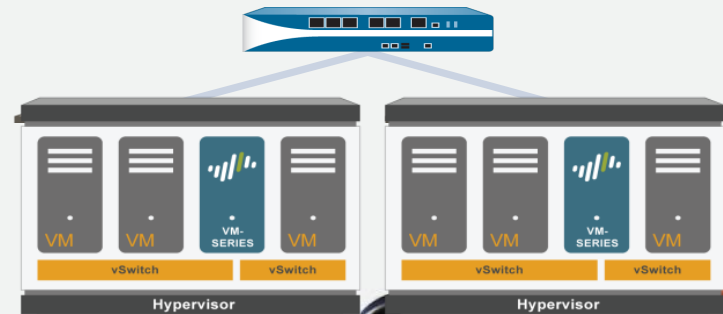


Policies

Objects

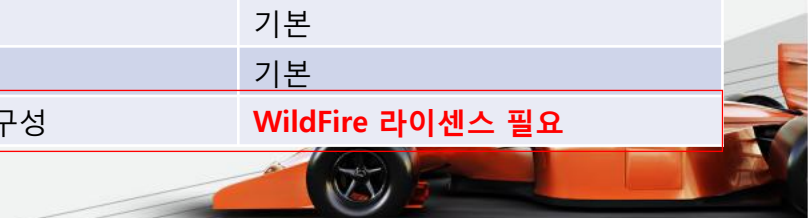
Interfaces

Dynamic Address Groups



Enterprise Security Platform : 제공 서비스

기능	세부기능	Description	라이선스
App-ID	Application detection	App 데이터 베이스	기본
	Custom App 정의		기본
User-ID	Active Directory		기본
	LDAP		기본
	Radius		기본
	Kerberos		기본
	Captive Portal		기본
Contents-ID	IPS	자체 시그니처	TP (Threat Prevention) 라이선스 하나로 세가지 기능 모두 사용
	Anti-Virus	자체 시그니처	
	Anti-Spyware	자체 시그니처	
	URL Filtering	자체 URL DB	URL 라이선스 필요 * 단 allow/block 리스트/커스텀 카테고리는 무료
	File Blocking	타일타입 인식	기본
	Data Filtering	문자열 인식	기본
APT방어	Unknown 위협 차단	Public, Private 구성	WildFire 라이선스 필요



Enterprise Security Platform : 제공 서비스(계속)

기능	세부기능	Description	라이선스
Networking	가상방화벽(Vsys)	장비별 기본제공 및 추가 라이선스 필요	기본
	DoS Protection, QoS		기본
	Policy Based Routing		기본
	High Availability		기본
VPN	Site-To-Site VPN		기본
	SSL VPN	장비별 최대 동시접속자	기본
Management/ Reporting	다양한 리포팅 기능		기본
	XML-based REST API		기본
	M-100 중앙관리서버	별도의 하드웨어 어플라이언스	

: NGFW + TP(IPS, Anti-Virus, Anti-Spyware)



ww고객사의 95%가 해당 서비스를 사용중에 있음

+ URL Filtering + APT(WildFire) + VPN



VM-Series 모델

Extra small

Branch office, vCPE,
Network based MSSP

Small, Medium

Hybrid cloud, segmentation, Internet
gateway

Large, Extra Large

NFV component in virtualized data center
and service provider environments



VM-50



VM-100



VM-300



VM-500



VM-700

Up to
200M App-ID

Up to
2G App-ID

Up to
4G App-ID

Up to
8G App-ID

Up to
16G App-ID

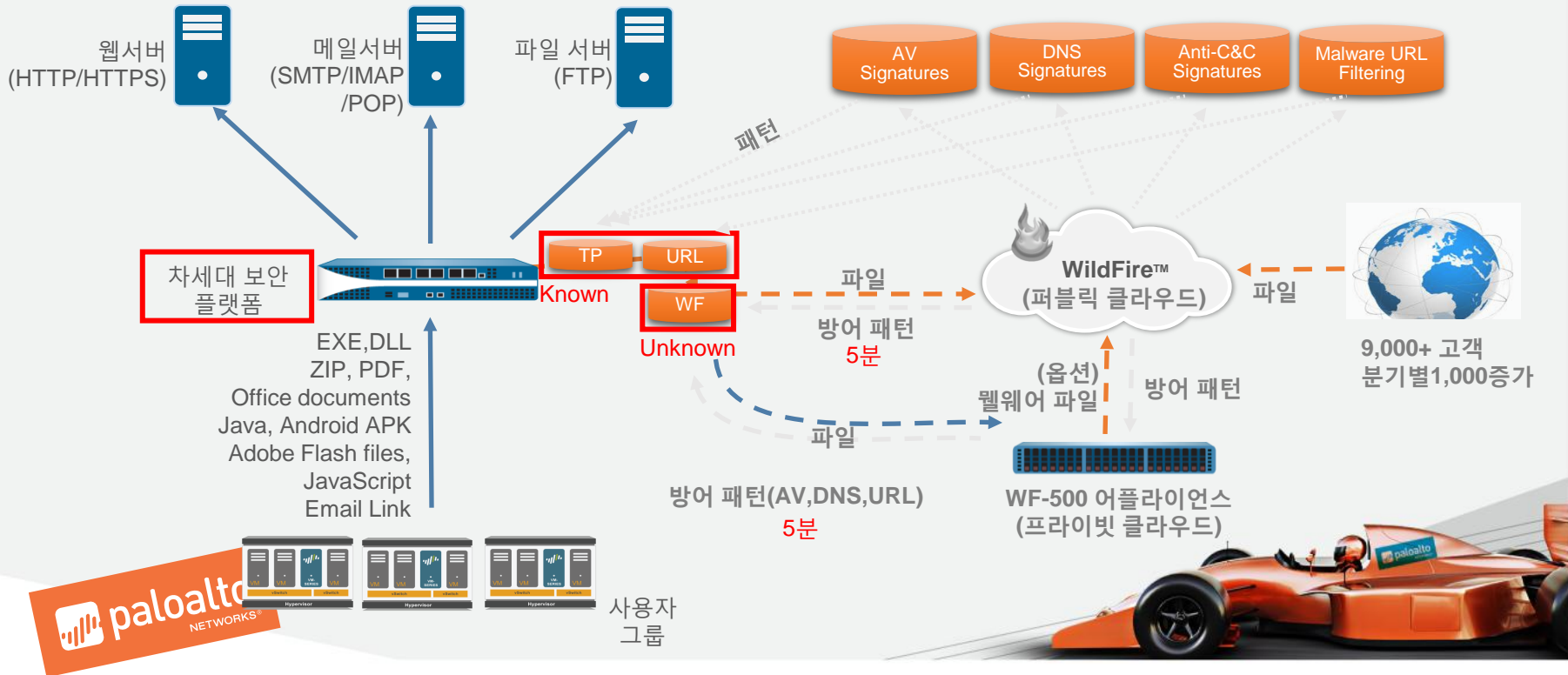


* Threat performance is half of App-ID



제공 가능 보안 서비스 구성

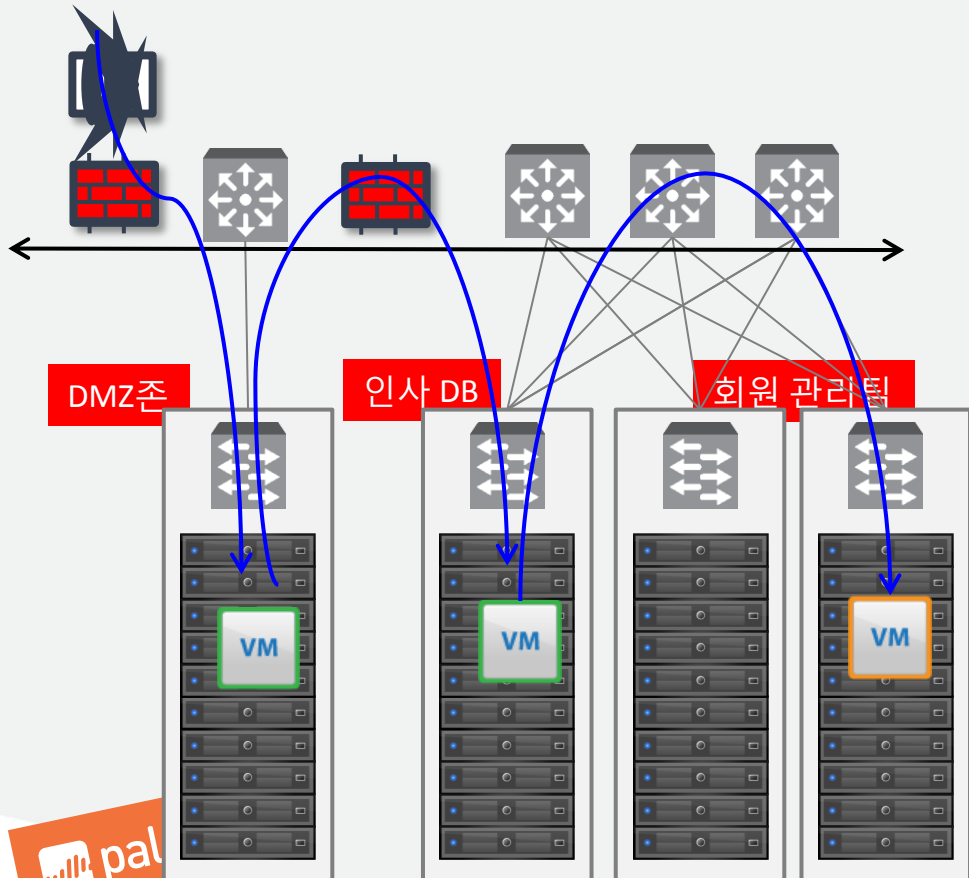
: Application 통제가 가능한 NGFW + TP(IPS, Anti-Virus, Anti-Spyware), URL Filtering, APT(WildFire)



Virtualized Firewall 동작 방식



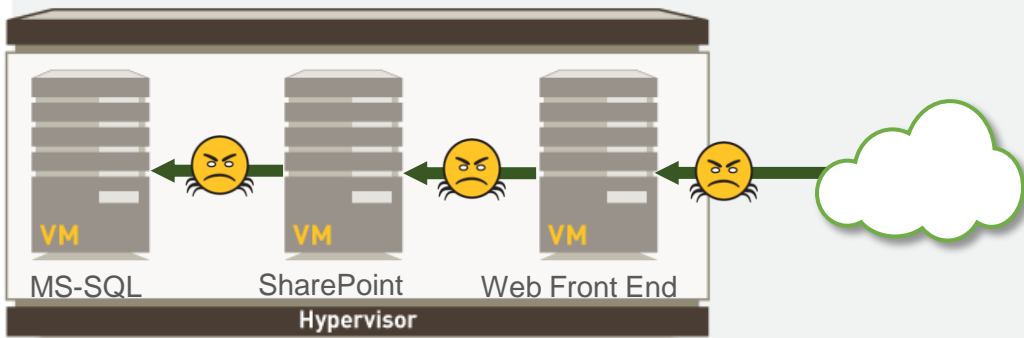
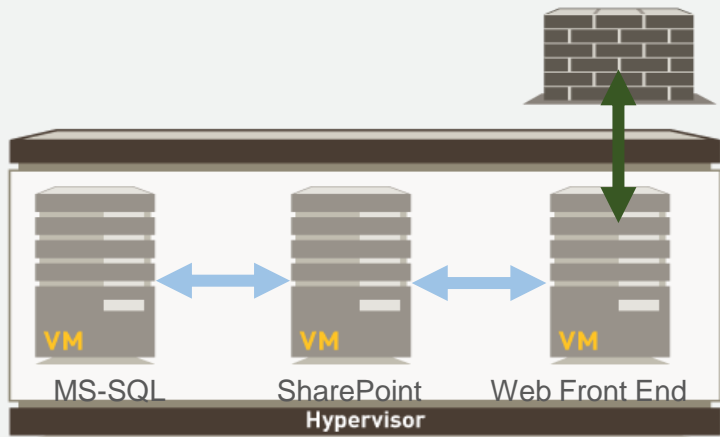
클라우드 환경을 위한 Security Challenge



- DMZ환경을 포함한 복잡한 환경에 대한 보안 서비스 접목의 어려움
- DMZ 워크로드 사이의 East-West traffic에 대한 보안 처리간 한계점 발생
- 클라우드 관리 솔루션과 방화벽 사이에서의 통합 문제 발생
- 윈도우와 리눅스 시스템을 서비스 VM으로 혼합 수용하는 구조에서 전체적인 보안 서비스 구성의 복잡성
- SSL encrypted traffic에 대한 처리 한계성
- L7에 대한 모든 트래픽을 보안 처리하기 힘든 문제 발생



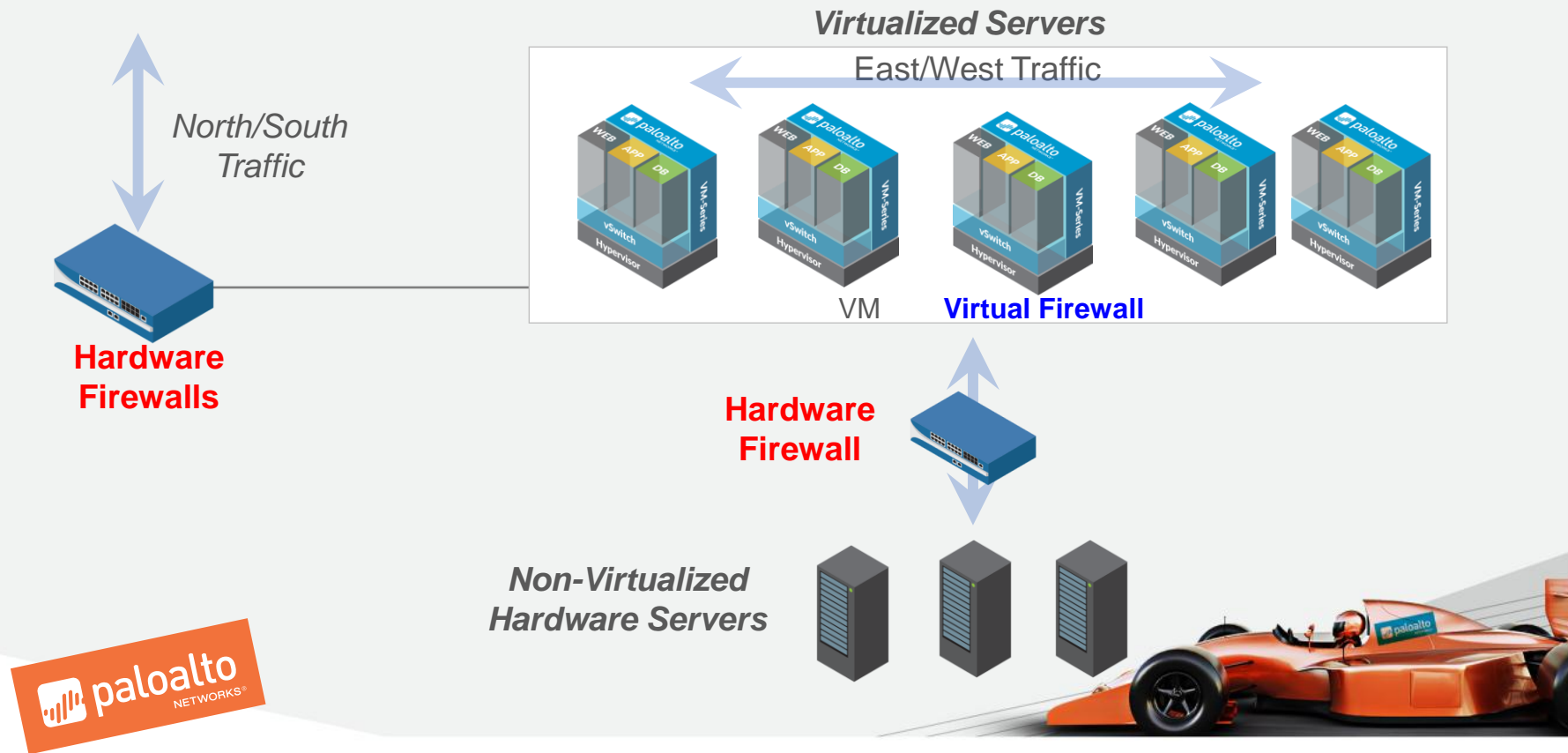
클라우드 환경을 위한 Security Challenge(계속)



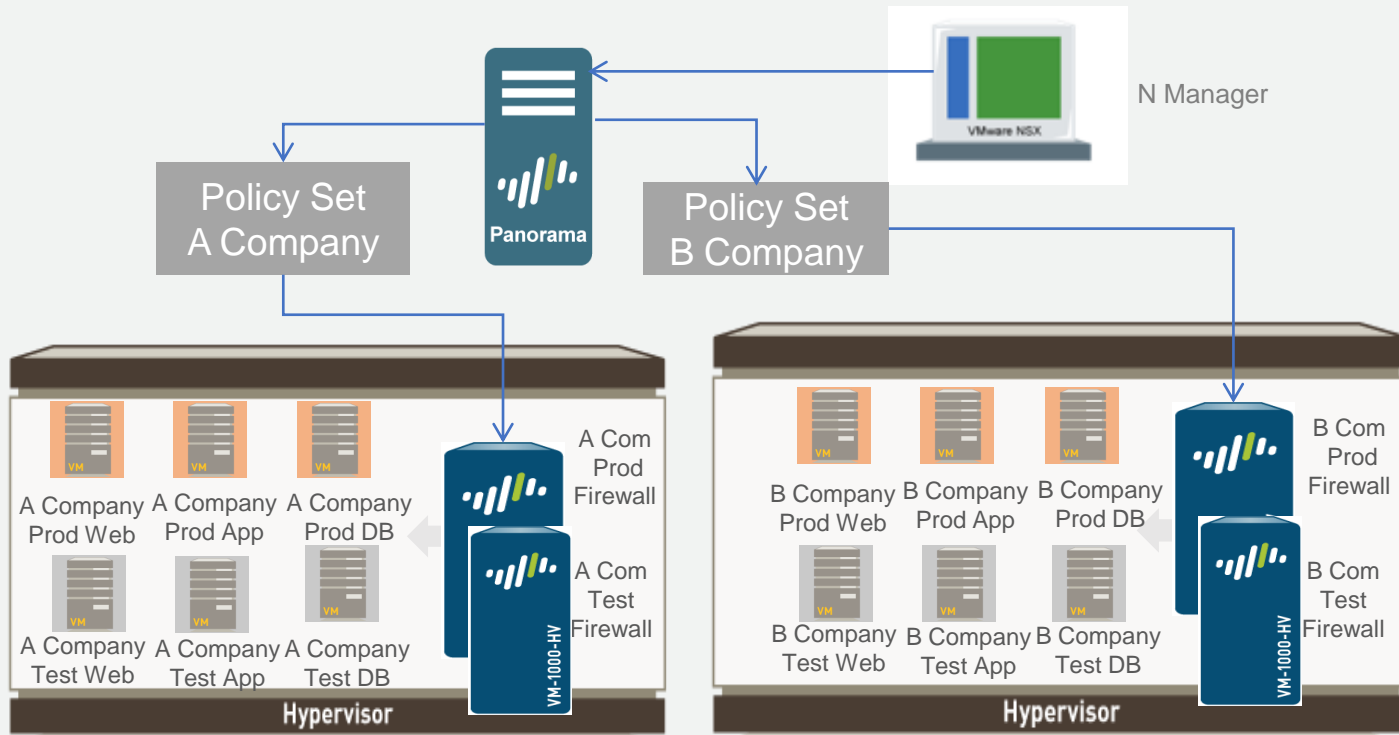
- 물리적 보안 장비로는 더이상 내부 클라우드 자원의 East-West 트래픽을 정확하게 확인 하거나 통제하기 어려움
- 또한 네트워크 Configuration의 변화만으로는 보안 정책이 적용된 East-West traffic 처리시 수동적이거나 복잡한 환경적용만이 가능함
- 클라우드 자원에 대한 자동화되고 손쉽게 적용가능한 트래픽 통제 정책 적용이 필요한 실정임



클라우드 환경을 위한 Security Challenge(계속)



Tenant별 독립적으로 적용 가능한 방화벽 구성



32 Cores Server
16 cores for Compute
4 – 4 core VM Series Firewalls

- 동일 호스트내에서 각각의 Tenant별 독립 방화벽 구성
- 동일 호스트내에서 Multiple Firewall 구성을 통한 성능 향상

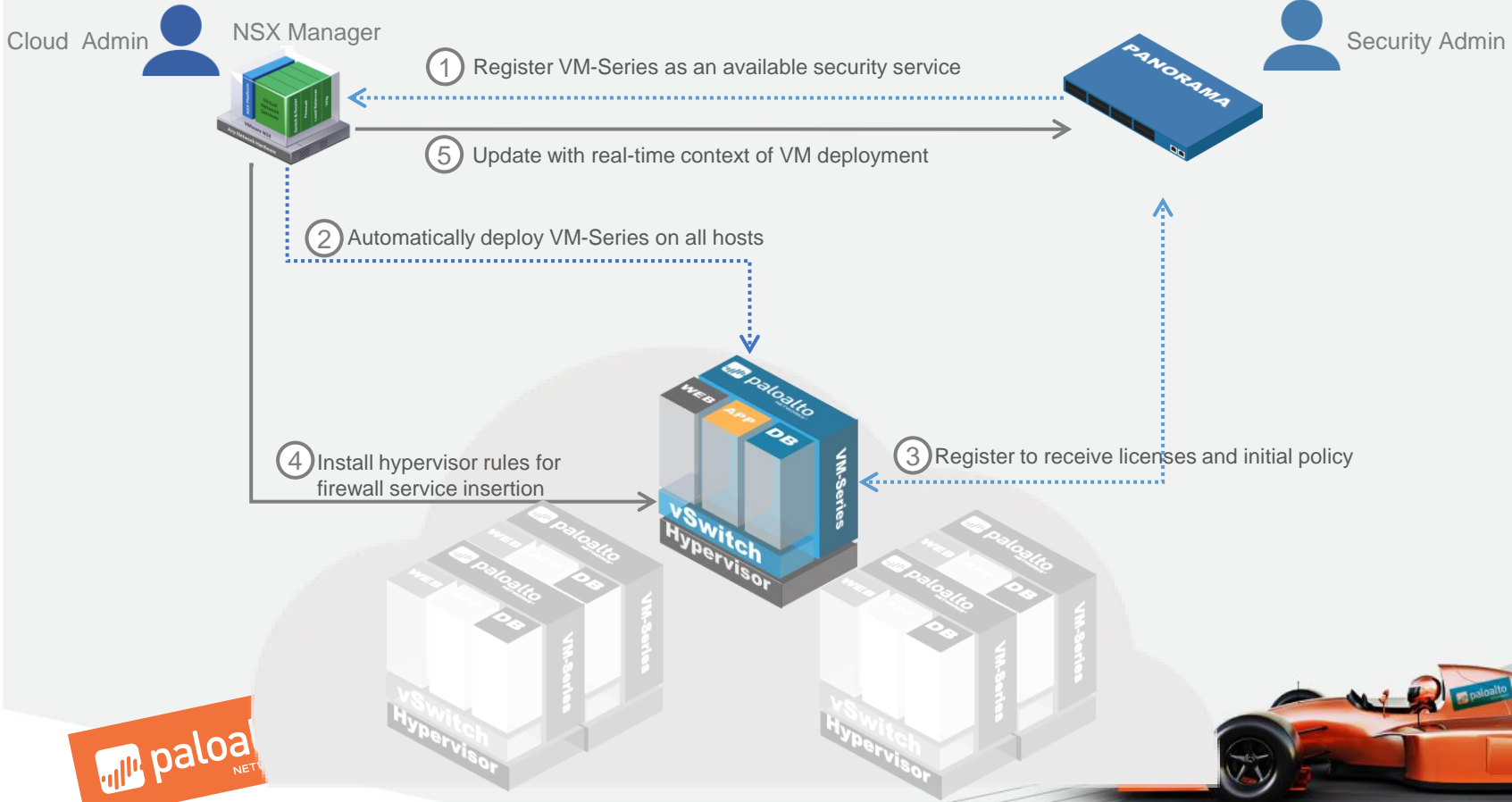


Virtualized Firewall

자동 보안 정책 적용 방안



NFV환경에서의 서비스 통합



Automated Security 서비스

V사의 N manager와의 통합 연동을 통해 팔로알토 네트워크의 VM-Series 방화벽이 차세대 보안서비스를 적용 시킬 수 있음

Integration benefits

Apply security protections automatically and on-demand

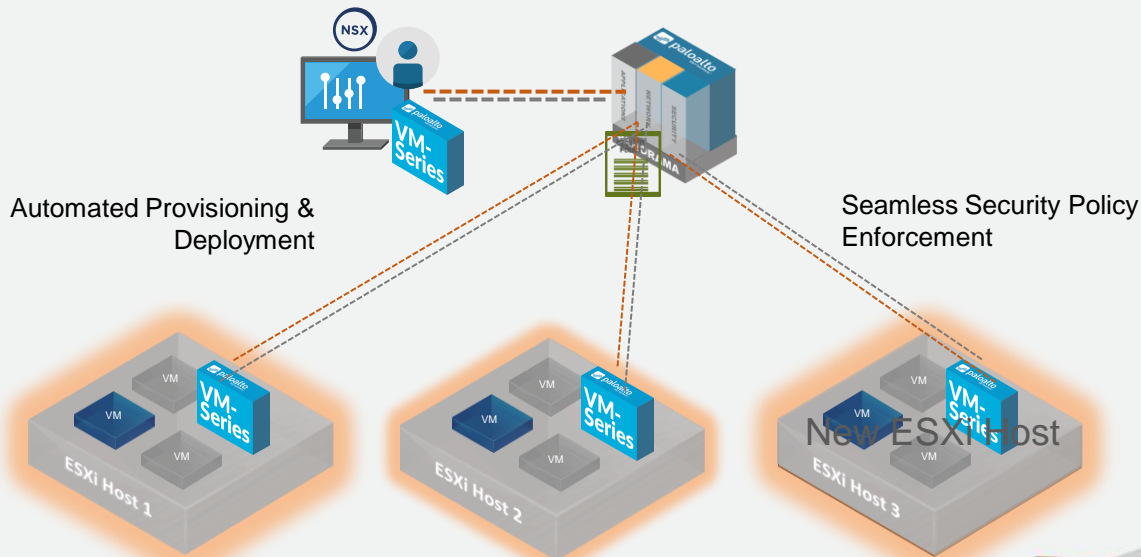
Keep security in lock-step with workload creation and movements

Reduce attack surface area within your software defined data centre

Protect your high-value assets from known and unknown cyberthreats

Automate security actions based on security event triggers

With automated security service insertion and provisioning of VM-Series virtualized next-generation firewall



New ESXi host is added to a cluster. NSX will auto-provisioning VM-Series instance on the ESXi host.



DYNAMIC SECURITY 정책 업데이트

팔로알토 네트워크스 VM-Series 방화벽의 Security Tag를 활용하여 Dynamic 정책 적용 기능 지원

Integration benefits

Apply security protections automatically and on-demand

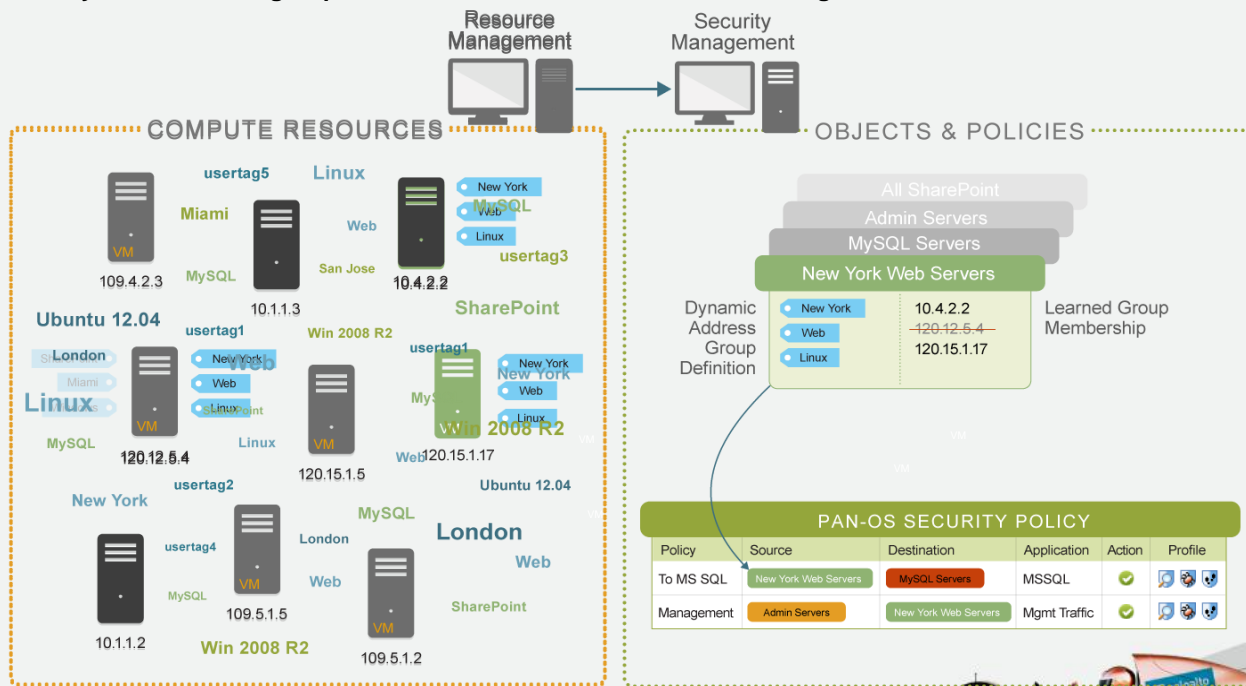
Keep security in lock-step with workload creation and movements

Reduce attack surface area within your software defined data centre

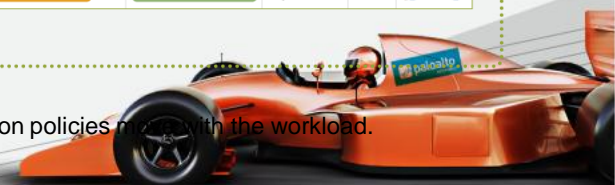
Protect your high-value assets from known and unknown cyberthreats

Automate security actions based on security event triggers

With dynamic address groups and context awareness between N Manager and Panorama



Advanced threat protection and application level segmentation policies move with the workload.



진화된 클라우드 보안을 위한 제안



진화된 보안 위협 차단의 올바른 선택!! GO!! 팔로알토 네트워크스!!

..protect east-west traffic flows from known and unknown malware

1

공격 접점을 줄이고,

- Whitelist applications or block high-risk apps
- Block known viruses, exploits
- Block commonly exploited file types

2

알려지지 않은 위협을 검출하여,

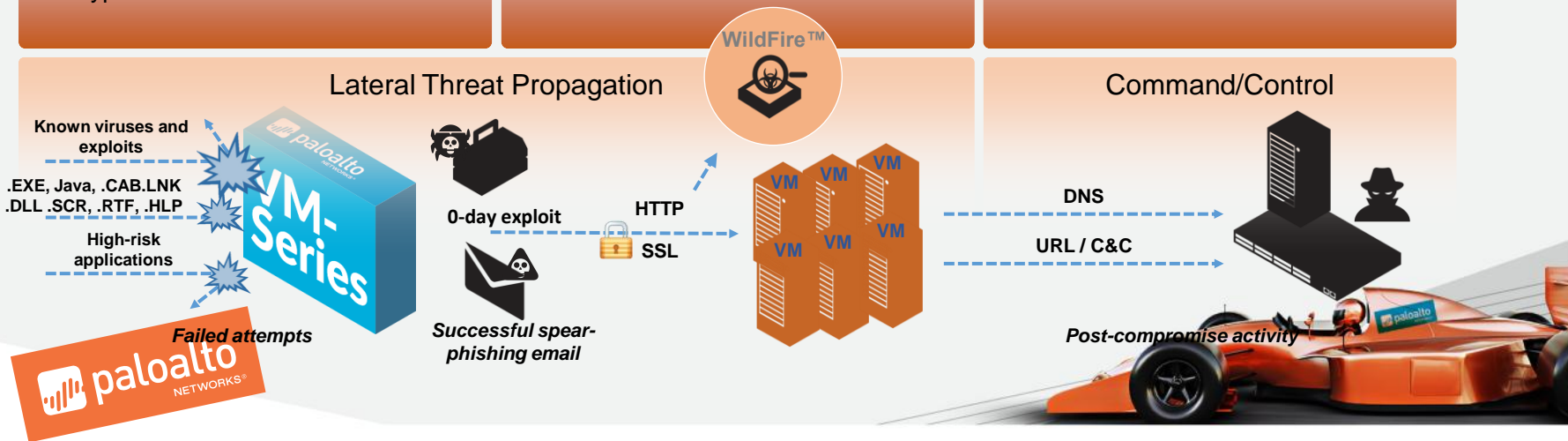
- Analysis of all application traffic
- SSL decryption
- WildFire sandboxing of exploitive files

3

차세대 보안 정책을 통한 자동 차단

Detection and blocking of C&C via:

- Bad domains in DNS traffic
- URLs (PAN-DB)
- C&C signatures (anti-spyware)



Zero Trust : DataCenter 네트워크를 위한 보안 플랫폼

Panorama:
Virtualized F/W에 대한 중앙통제



Hardware Firewalls

Dynamic Routing

Virtual Firewalls

Wildfire
Cloud-Based
Threat Intelligence

Data Center Perimeter



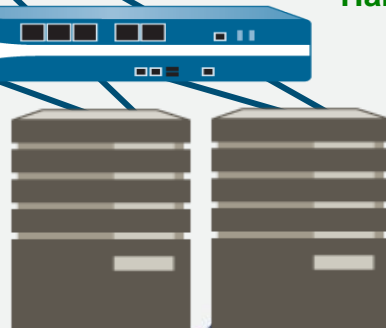
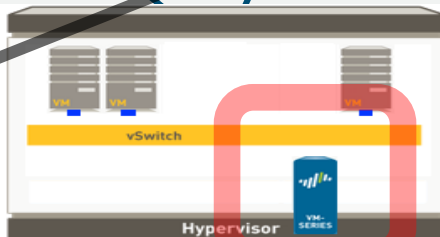
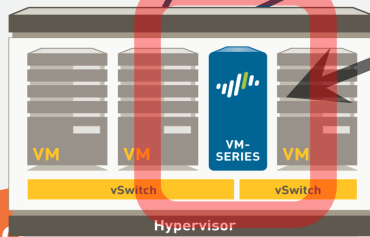
Network Core



Public Cloud



Hardware Firewalls



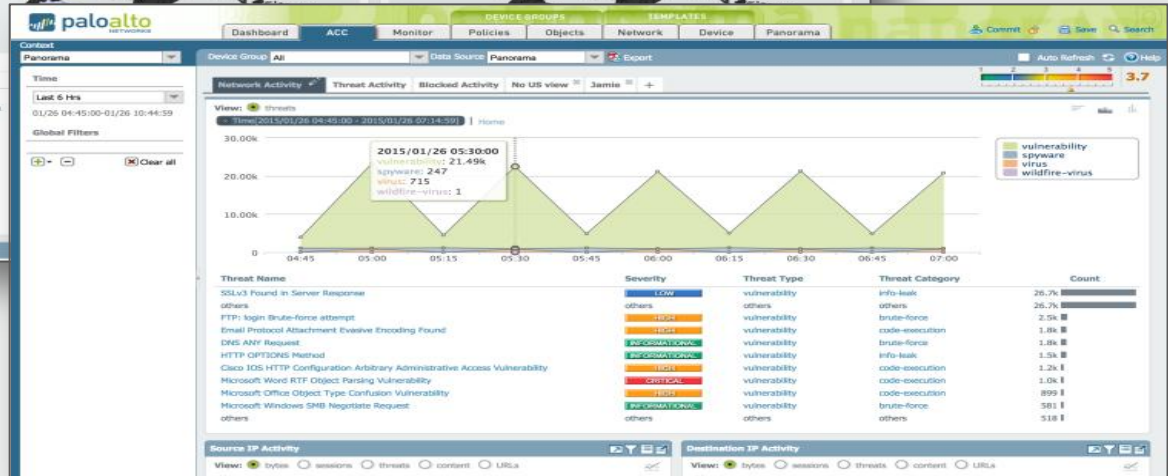
물리적 서버



Virtualized Servers / Private Cloud
VMware



혁신적인 가시화 툴 제공(계속)



Cyber Attack LifeCycle에 대한 단계별 방어



Breach the perimeter [준비단계]

Next-Generation Firewall / GlobalProtect

- Visibility into all traffic, including SSL
- Enable business-critical applications
- Block high-risk applications
- Block commonly exploited file types

Threat Prevention

- Block known exploits, malware and inbound command-and-control communications

URL Filtering

- Prevent use of social engineering
- Block known malicious URLs and IP addresses

WildFire

- Send specific incoming files and email links from the internet to public or private cloud for inspection
- Detect unknown threats
- Automatically deliver protections globally



Deliver the malware [내부망 침입]

Traps / WildFire

- Block known and unknown vulnerability exploits
- Block known and unknown malware
- Provide detailed forensics on attacks



Lateral movement [목표시스템 이동]

Next-Generation Firewall / GlobalProtect

- Establish secure zones with strictly enforced access control
- Provide ongoing monitoring and inspection of all traffic between zones

WildFire

- Detecting unknown threats pervasively throughout the network



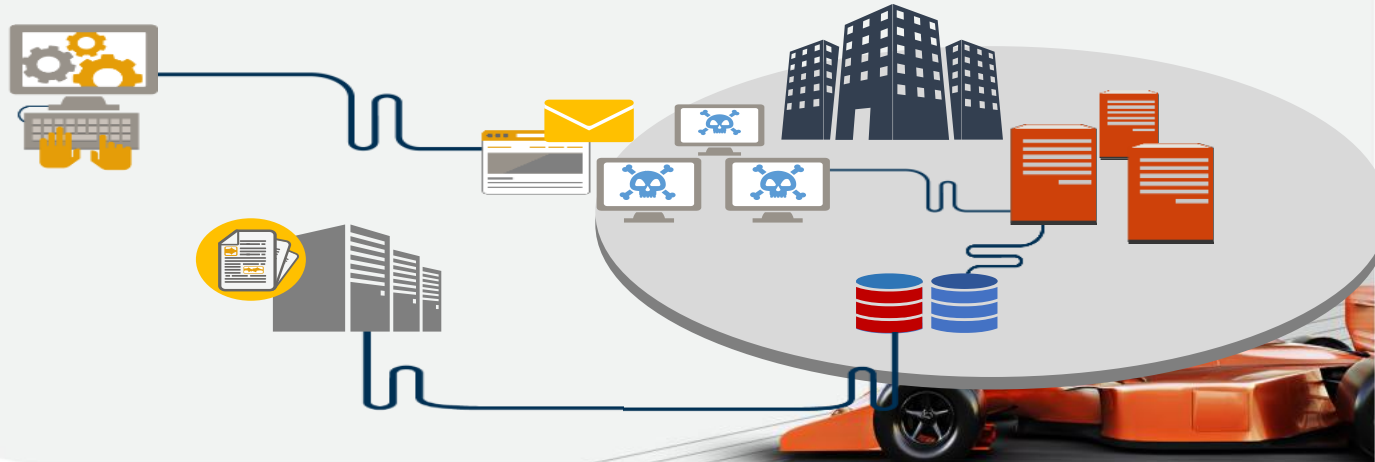
Exfiltrate data [목표공격 및 자료탈취]

Threat Prevention

- Block outbound command-and-control communications
- Block file and data pattern uploads
- DNS monitoring and sinkholing

URL Filtering

- Block outbound communication to known malicious URLs and IP addresses



새로운 보안에 거는 우리의 기대..



사전차단 및 안전한
비즈니스 지원



자동화 및 솔루션간 연계



보안기술 및 해킹에
대한 치밀한 대비



참고 소개 동영상

팔로알토 네트워크스 & VMware

<https://www.youtube.com/watch?v=fHu1Tyh3P9g>



VMware NSX를 위한 팔로알토 네트워크스 VM시리즈

전자신문 U-TV



팔로알토 네트워크스 & AWS

<https://www.youtube.com/watch?v=fHu1Tyh3P9g>

[오늘의 지식방송] AWS클라우드 컴퓨팅, 팔로알토 네트워크 차세대 보안을 만나다



[AD] 새것보다 전시품 50% 반값할인

4월 21일 오후 2시 ~ 오후 3시 30분

아마존이 서비스하는 '아마존웹서비스(AWS)' 서울 리전이 런칭되면서 국내 많은 기업이 AWS 클라우드로 이전을 준비 중이다. 클라우드 컴퓨팅 시대 본격화로 기존 온프레미스 기반 보안 장비와 같은 수준이나 그 이상을 제공하는 보안 솔루션에 대한 수요가 함께 늘었다. 기존 물리적 보안 장비만으로는 내부 클라우드 자원 관련 트래픽을 정확히 통제·관리하기 어렵기 때문이다.



<김민석 팔로알토네트워크스코리아 수석 부장>





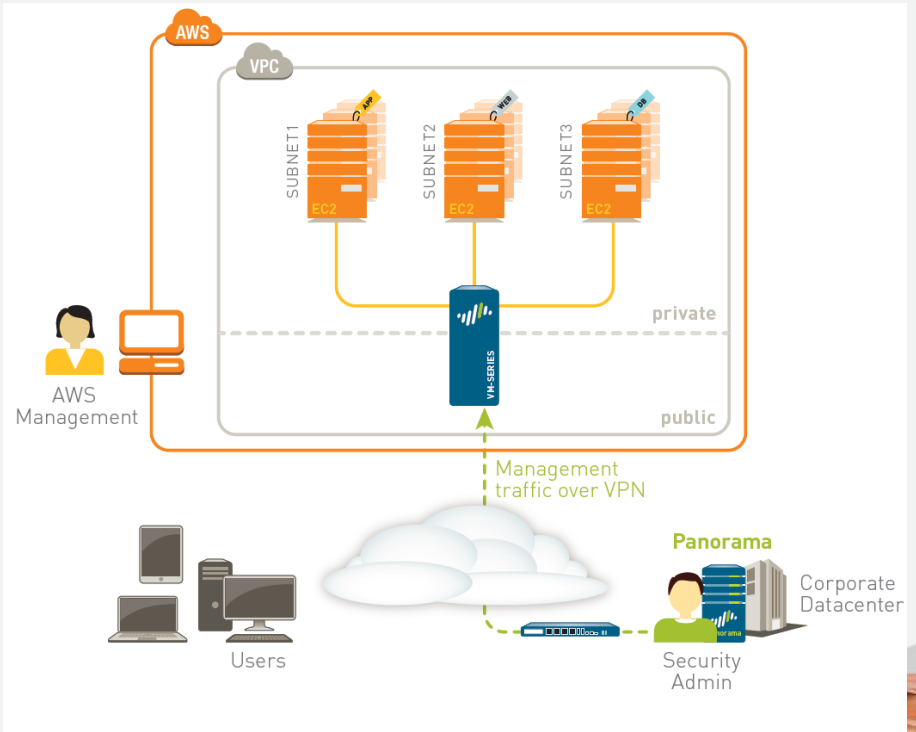
감사합니다!!!

참고 자료



VM-Series for Amazon Web Services

- AWS console를 통한 VM-Series 설치
 - Use case: 외부 트래픽 경계 부분에서 내부 VPC(Virtual Private Cloud)안쪽으로 유입되는 트래픽에 대한 NGFW protection 적용
 - Use case: IPSec VPN 연결을 통해 회사내부 DC에 연결
 - Use case: VM과 VM간의 위협요소들의 이동을 차단하며, 다양한 Application에 대한 보안 적용
- EC2(Elastic Compute Cloud) 변경시 내부 보안 정책에 대한 자동화 변경 Feature를 지원



VM-Series for Amazon Web Services(계속)



Amazon Web Services Home

Sign in or Create a new account

Your Account | Help | Sell on AWS Marketplace

Shop All Categories

Search AWS Marketplace

GO

Your Software

Desktop Apps

Software Infrastructure

Application Development
Application Servers
Application Stacks
Big Data
Databases & Caching
Network Infrastructure
Operating Systems
Security

Developer Tools

Issue & Bug Tracking
Monitoring
Source Control
Testing

Business Software

Business Intelligence
Financial Services
Collaboration
Content Management

NEXT-GENERATION FIREWALL FOR AWS



APPLY APPLICATION-SPECIFIC FIREWALL POLICIES
PREVENT KNOWN AND UNKNOWN THREATS
GAIN APPLICATION VISIBILITY

TRY THE VM-SERIES NOW

Featured Products



Security



TREND MICRO

McAfee Public Cloud Server Security S...

InfoReliance Corporation
\$0.155 to \$19.406/hr for software + Charges for EC2 with Windows
Free Trial

Trend Micro Deep Security

Trend Micro
Starting from **\$1.74/hr** or from **\$9,990/yr** for software
Free Trial



AlienVault Unified Security Management...

AlienVault
\$1.00/hr or **\$7,750/yr** for software
Free Trial

Operating Systems



Amazon Linux AMI (HVM / 64-bit)
Amazon Web Services
\$0.013 to \$8.14/hr incl EC2 charges



CentOS 7 (x86_64) with Updates HVM
Centos.org
\$0.00/hr for software



Oracle Linux 6.6



VM-Series for Amazon Web Services(계속)

AWS Services Edit

MINSUK KIM Sydney Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 1: Choose an Amazon Machine Image (AMI)

Cancel and Exit

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Quick Start

My AMIs

AWS Marketplace

Community AMIs

Categories

All Categories

Software Infrastructure (3)

Operating System

Clear Filter

All Linux/Unix

Other Linux (3)

Software Pricing Plans

Hourly (2)

Annual (2)

Bring Your Own License (1)

Software Free Trial

Free Trial (2)

Search: palo alto

1 to 3 of 3 Products

paloalto **VM-Series Next-Generation Firewall Bundle 2** [Select](#)

★★★★★ (1) | PAN-OS 7.1.0 [Previous versions](#) | Sold by Palo Alto Networks

\$1.28/hr or \$4,500/yr (60% savings) for software + AWS usage fees

Free Trial Linux/Unix, Other PAN-OS 7.1.0 | 64-bit Amazon Machine Image (AMI) | Updated: 4/1/16

The VM-Series for AWS Bundle 2 includes a VM-300 next-generation firewall license, subscriptions for Threat Prevention (includes IPS, AV, malware prevention), WildFire, ...

[More info](#)

paloalto **VM-Series Next-Generation Firewall Bundle 1** [Select](#)

★★★★★ (1) | PAN-OS 7.1.0 [Previous versions](#) | Sold by Palo Alto Networks

\$0.86/hr or \$3,000/yr (60% savings) for software + AWS usage fees

Free Trial Linux/Unix, Other PAN-OS 7.1.0 | 64-bit Amazon Machine Image (AMI) | Updated: 4/1/16

The VM-Series for AWS Bundle 1 includes a VM-300 next-generation firewall license, a Threat Prevention subscription (includes IPS, AV, malware prevention) and Premium ...

[More info](#)

paloalto **VM-Series Next-Generation Firewall (BYOL)** [Select](#)

★★★★★ (0) | PAN-OS 7.1.0 [Previous versions](#) | Sold by Palo Alto Networks

Bring Your Own License + AWS usage fees

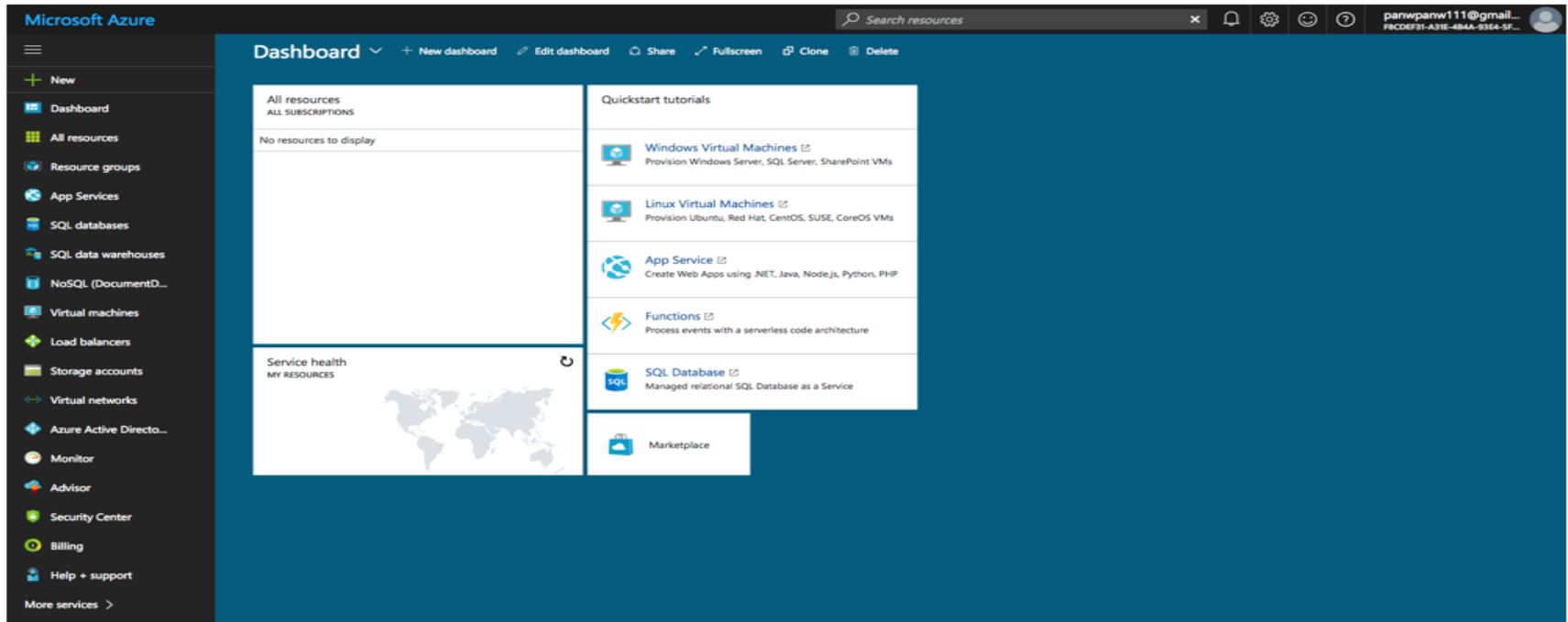
Linux/Unix, Other PAN-OS 7.1.0 | 64-bit Amazon Machine Image (AMI) | Updated: 4/1/16

The VM-Series BYOL allows you to pick and choose the VM-Series related licenses and subscriptions that are appropriate for your needs. Regardless of which components you ...

[More info](#)

VM-Series for MS-Azure

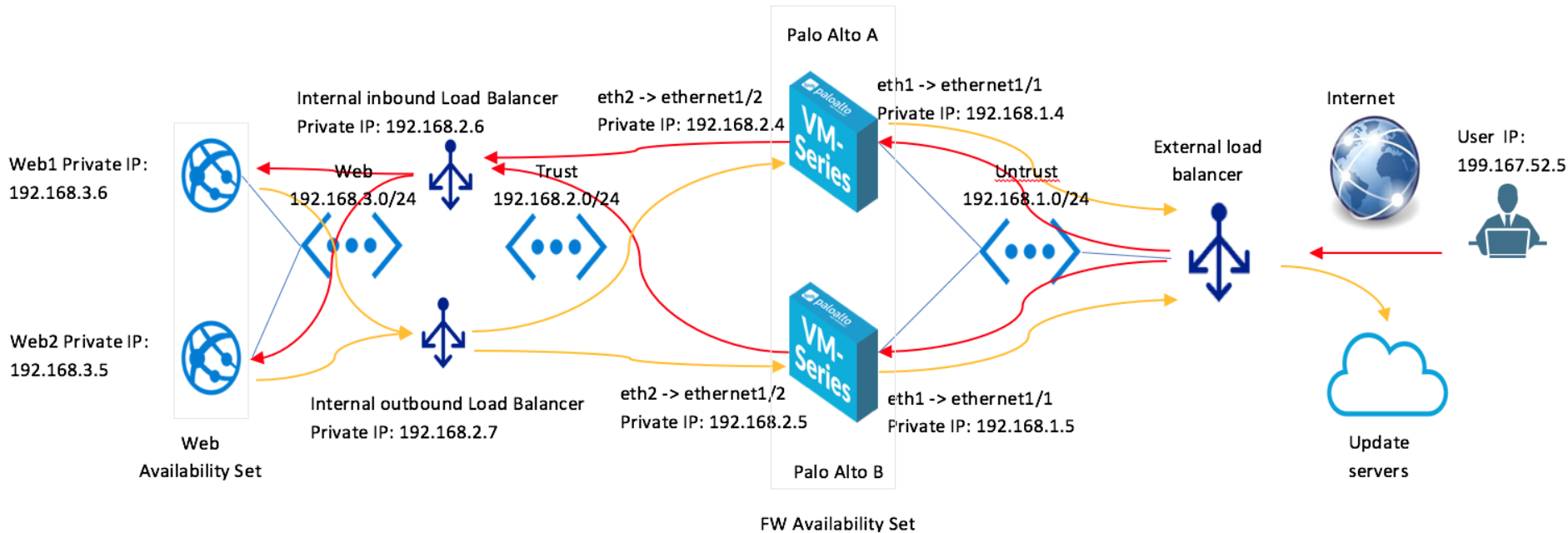
Go to <https://portal.azure.com> and login with the account created.
Once login, Azure portal dashboard will be displayed.



The screenshot displays the Microsoft Azure portal dashboard. The top navigation bar includes the Microsoft Azure logo, a search bar for resources, and user account information for 'panwpanw111@gmail...'. The left sidebar lists various services such as Dashboard, All resources, Resource groups, App Services, SQL databases, SQL data warehouses, NoSQL, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Billing, and Help + support. The main content area is titled 'Dashboard' and features several tiles: 'All resources' (showing 'No resources to display'), 'Service health' (with a world map), 'Quickstart tutorials' (listing Windows Virtual Machines, Linux Virtual Machines, App Service, Functions, and SQL Database), and 'Marketplace'.

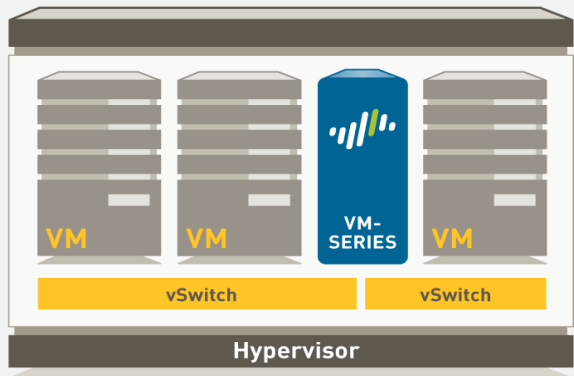
VM-Series for MS-Azure(계속)

The following is the network diagram of this lab. We will attempt to build this in the AWS environment. There will be 1 Virtual Network (vnet). Within the vnet, we will deploy 2 x Azure Load Balancers and 2 x Linux web servers behind the Palo Alto Networks Firewall. The inbound traffic from the internet will be load balanced by an external Azure Load Balancer (ALB).



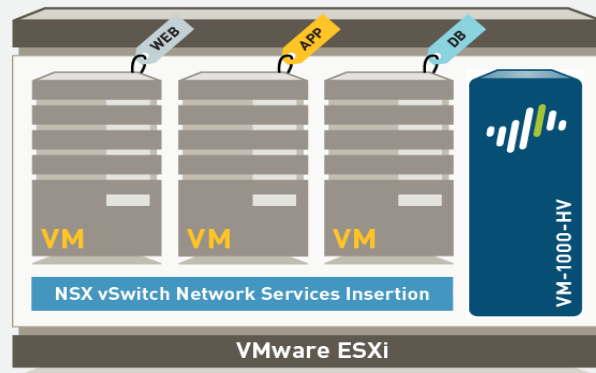
VM-Series for VMware

VMware vSphere (ESXi)용 VM-Series



- VMware의 ESXi상에서 Guest OS로서 VM-100, VM-200, VM-300 및 VM-1000-HV를 배포 가능
- Traffic inspection을 위해 virtual network configuration의 일부로 배포됨

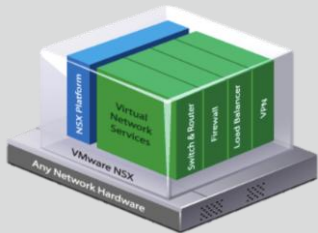
VMware NSX용 VM-Series



- VMware NSX와 Panorama가 서비스의 일부분으로 VM-Series NSX에 설치됨
- 내부 VM간의 트래픽을 inspection할 수 있음



VM-Series for VMware 구성요소



VMware NSX



VM-1000-HV



Panorama



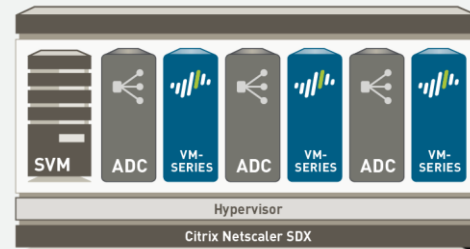
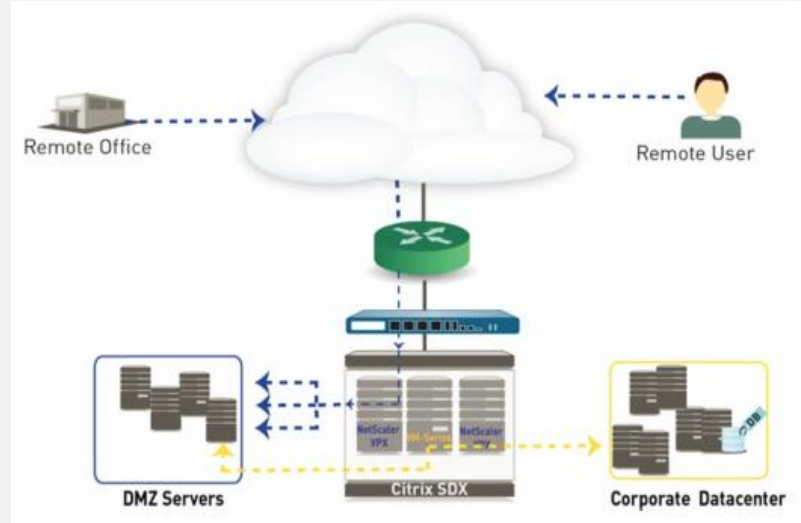
가상 공간에서 발생할 수 있는 사이버 공격에 대해 최적화된 보안 적용이 가능하며 차세대 보안 플랫폼 접목을 통해 안전한 어플리케이션의 사용이 가능함

- 자동화된 배포 및 장비 설정 기능 지원
- 중단없는 서비스 제공 및 제거가 가능함
- 다이나믹한 보안 정책 적용이 가능함



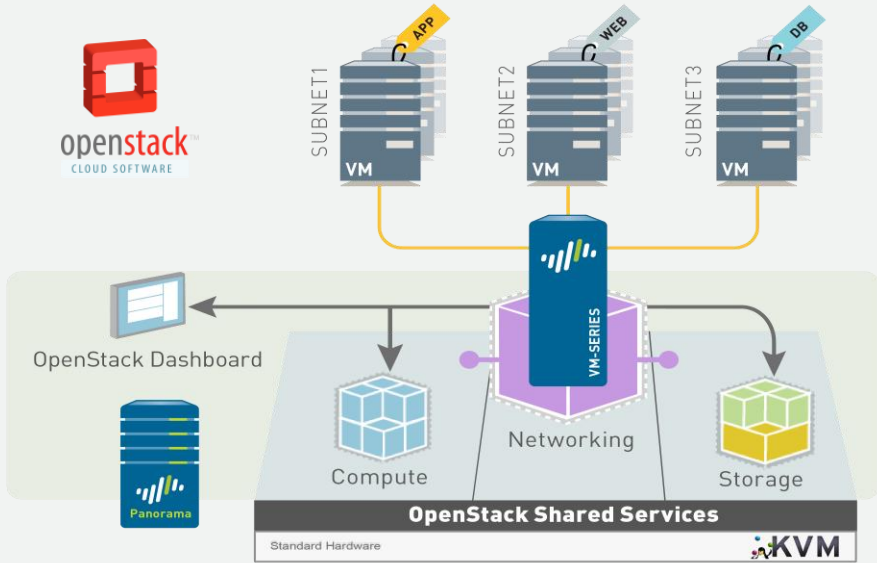
VM-Series for Citrix Netscaler SDX

- VM-Series on Citrix NetScaler SDX
 - 사용중인 Application들을 안전하게 User별, Content별로 운영할 수 있음
 - 알려진 위협과 알려지지 않은 위협에 대해 방어할 수 있음
 - SDX 11500과 17550 Series에서 연동 가능
- Key use cases
 - XenApp/XenDesktop 연동을 위한 확장된 보안 및 가용성을 제공하는 솔루션 기능 제공
 - Multi-tenant를 위한 Cloud Deployment (business units, application owners, service provider)



VM-Series for KVM

- “build-your-own” 사용자를 위한 이상적인 Suits 제공
- Enterprises with large Linux base
 - 외부 경계점에서의 firewall과 threat prevention
- Service providers
 - Home-grown cloud computing platform
- Optional하게 OpenStack plugin은 Panorama 빅데이터 분석 솔루션을 자동화 모델로 확장시킬수 있음



VM-Series for KVM(계속)

Software Versions

- Ubuntu : 12.04 LTS
- CentOS/ RedHat Enterprise Linux: 6.5
- Open vSwitch: 1.9.3 with bridge compatibility mode

