Evento Vmware con Aditinet

Stefania Iannelli

System Engineer Palo Alto Networks

6-7 Maggio 2015

Agenda

- Palo Alto Networks Overview
- Proteggere il Data Center
- Palo Alto Networks e NSX
- Use cases
- Q&A

paloalto networks.

Palo Alto Networks Overview

paloalto networks

Breve storia di Palo Alto Networks

Next generation:
Safely enable applications

Legacy:
Permetti o blocca
le applicazioni

Metà anni 90 – oggi

Today+

Breve storia dell'evoluzione informatica

Cloud + SaaS

webex
successfactors
BUSINESS EXECUTION SOFTWARE
workday
jive
salesforce

Social + consumerization

Gmail
LinkedIn
EVERNOTE
facebook
skype
Dropbox

Mobile + BYOD

Attacchi più sofisticati

networks.

Il nostro nuovo approccio alla network security

App-ID

Identifica le applicazioni

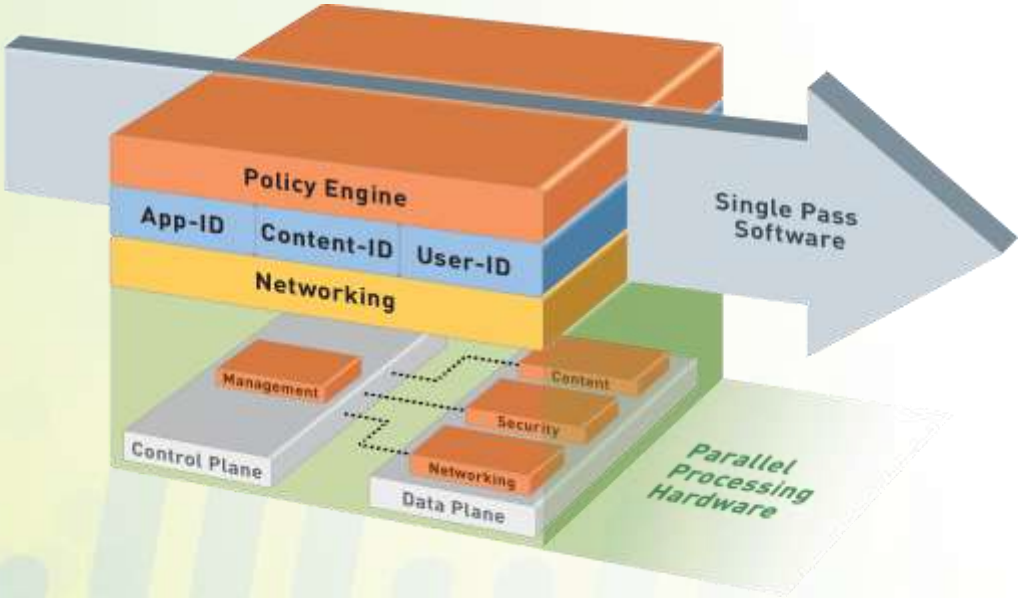
Content-ID

Analizza il contenuto

User-ID

Identifica l'utente

Palo Alto Networks platform



Dal 2011 leader del Gartner Magic Quadrant - Enterprise Network Firewalls

paloalto networks.

slideshare-uploading
application function

pdf
file type

slideshare
application

roadmap.pdf
file name

prodmgmt
group

HTTP
protocol

file-sharing
URL category

bjacobs
user

SSL
protocol

canada
destination country

172.16.1.10
source IP

tcp/443
destination port

64.81.2.23
destination IP

exe
file type

web-browsing
application

shipment.exe
file name

finance
group

HTTP
protocol

unknown
URL category

fthomas
user

SSL
protocol

china
destination country

172.16.1.10
source IP

tcp/443
destination port

64.81.2.23
destination IP

paloalto networks.

172.16.1.10
source IP

tcp/443
destination port

64.81.2.23
destination IP

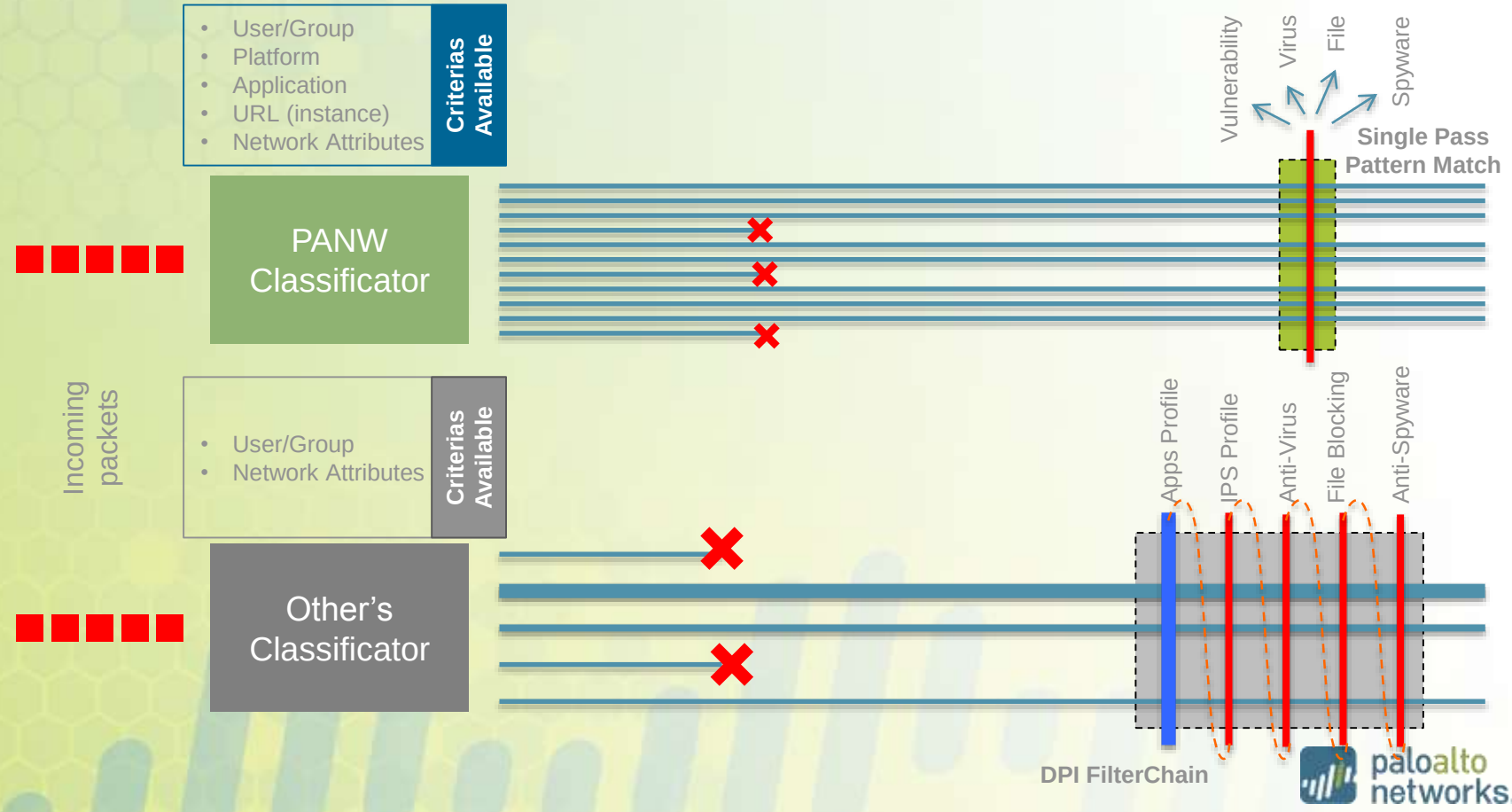
344

?

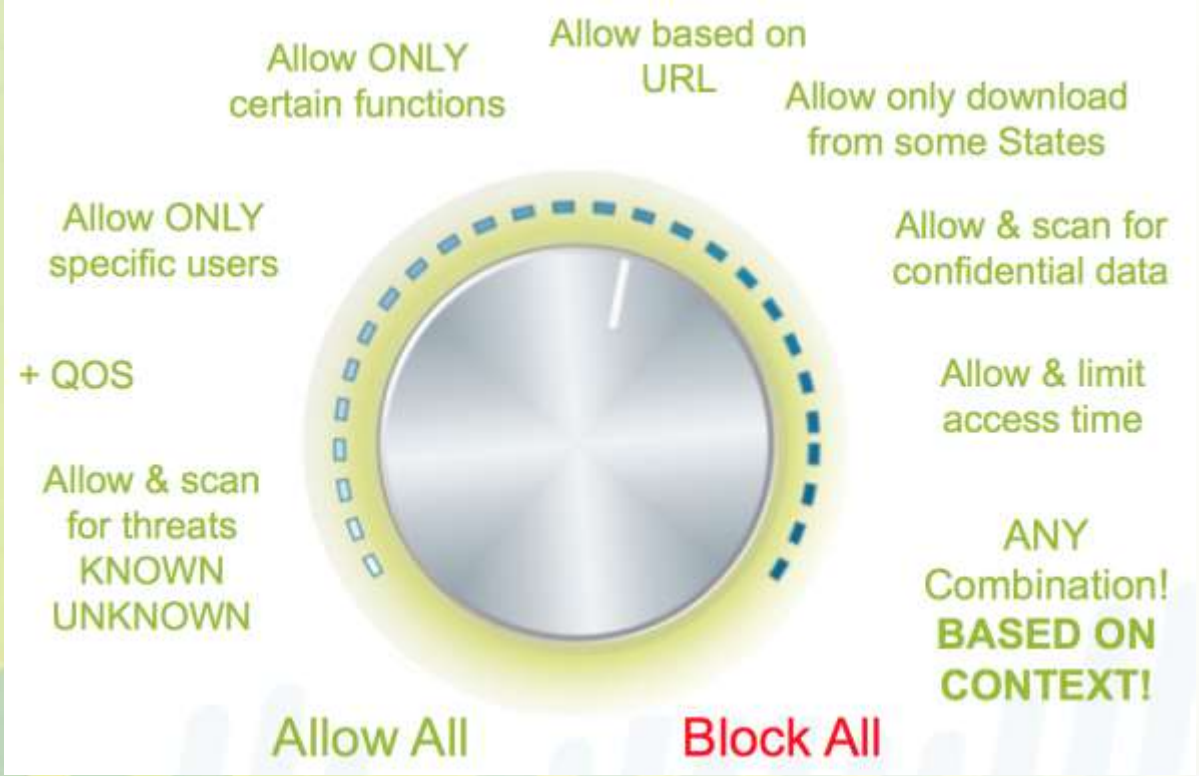
KB

paloalto networks.

Palo Alto Networks NGFW vs Legacy Firewall



Altre OPZIONI?



paloalto networks.

Il ciclo di vita di un attacco

1

Bait the end-user

L'utente finale viene attirato da un'applicazione pericolosa o un sito web con contenuti dannosi

2

Exploit

Viene sfruttata una vulnerabilita' del sistema o dell'applicazione, senza che l'utente si accorga di nulla

3

Download Backdoor

In background viene scaricato un secondo payload. Il malware viene installato

4

Establish Back-Channe

Il malware stabilisce una connessione in uscita verso l'attaccante, in modo che questo prenda il controllo

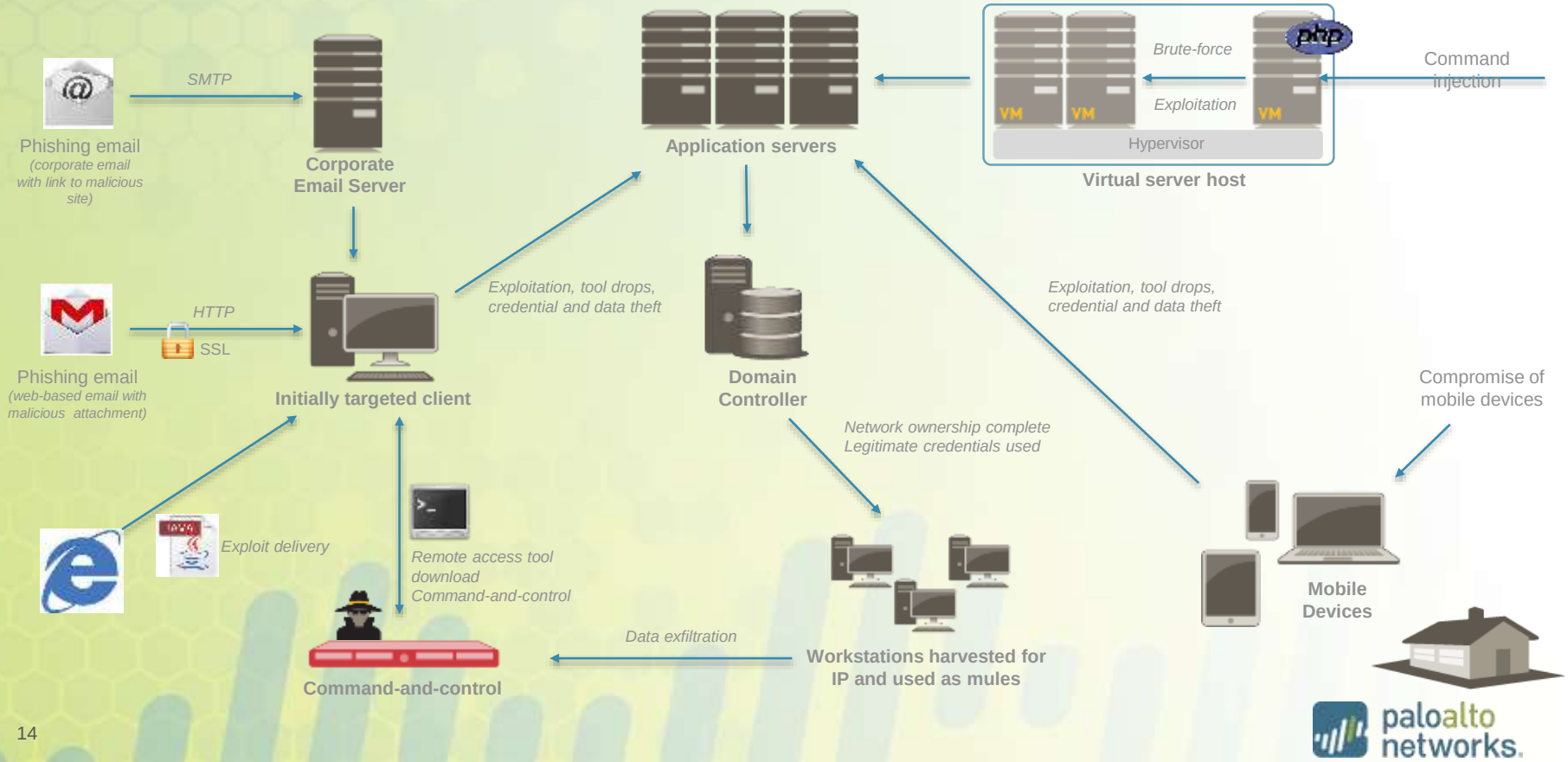
5

Explore & Steal

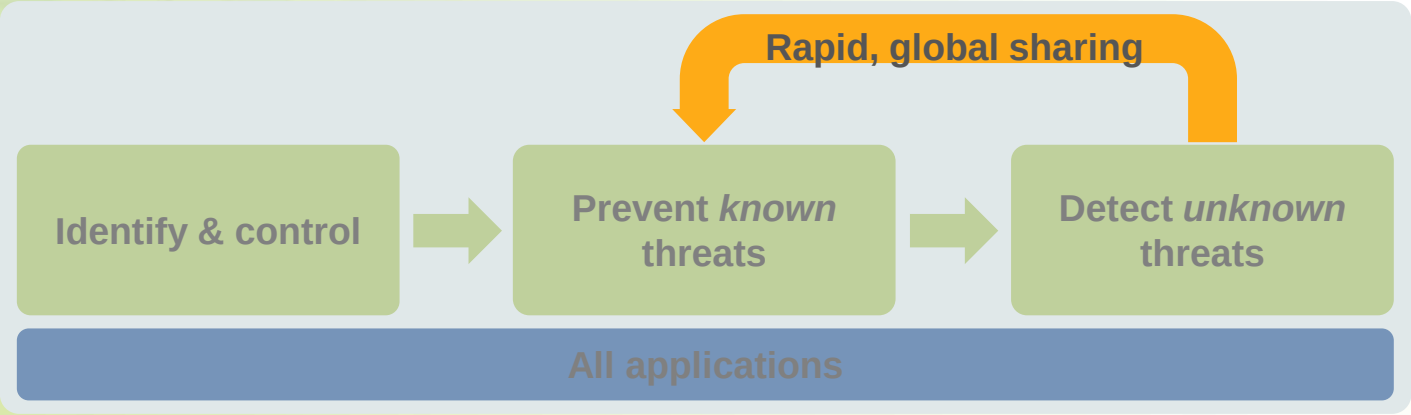
L'attaccante remoto ha il controllo all'interno della rete e intensifica l'attacco

paloalto networks.

Anatomia di una rete compromessa



Soluzione di Advanced Threat Prevention

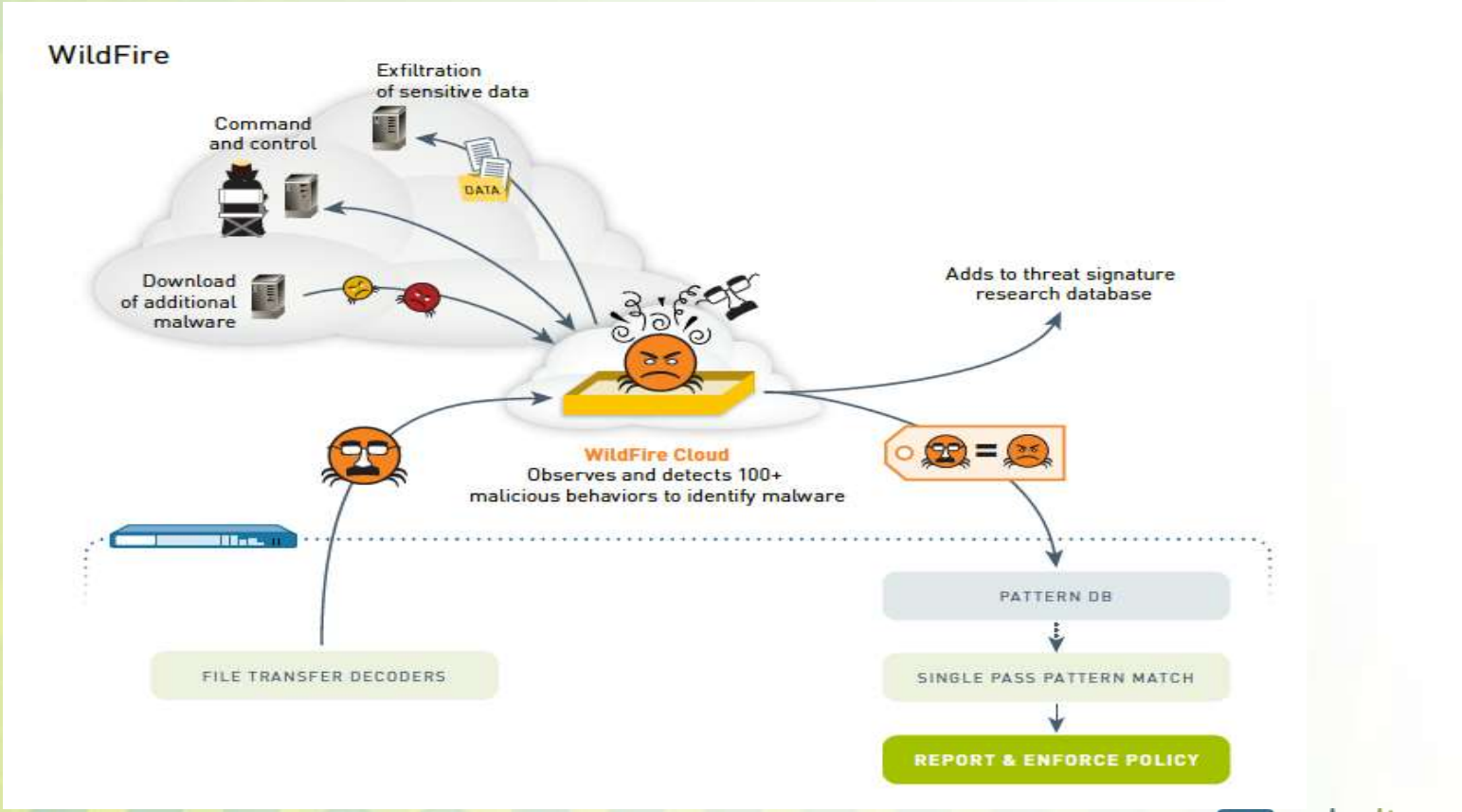


Il nostro approccio ci rende l'unica soluzione in grado di ...

- Effettuare una scansione di **TUTTE LE APPLICAZIONI** (incluso il traffico SSL) per controllare tutti gli accessi IN/OUT della rete, ridurre la superficie di attacco e fornire un contesto per l'analisi forense
- Prevenire gli attacchi attraverso **TUTTI i vettori di infezione** (exploit, DNS e URL) verso malware, command & control, con signature content-based
- Rilevare i malware e gli exploit zero day usando un **cloud pubblico o privato** e creando in automatico delle signature per tutti gli utenti, a livello globale

paloalto networks.

Architettura WildFire

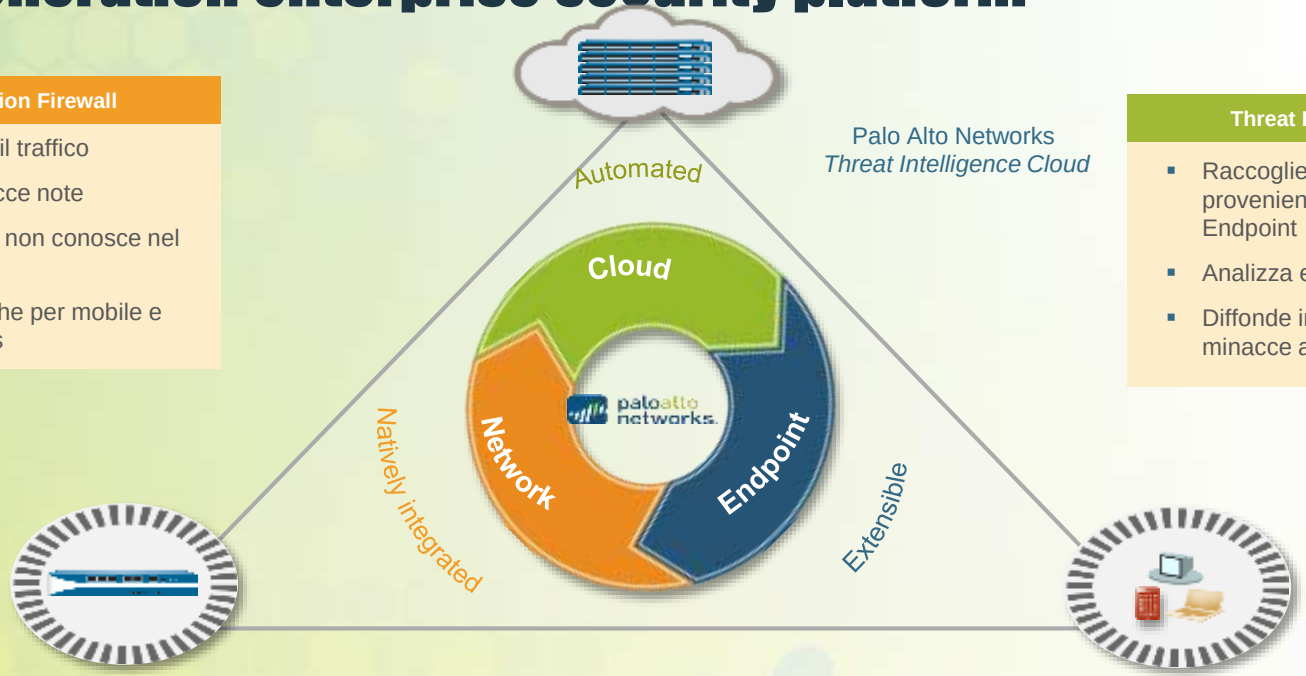


paloalto networks.

Next-generation enterprise security platform

Next-Generation Firewall

- Ispeziona tutto il traffico
- Blocca le minacce note
- Manda cio' che non conosce nel cloud
- Protezione anche per mobile e virtual networks



Palo Alto Networks
Threat Intelligence Cloud

Threat Intelligence Cloud

- Raccoglie poteziali minacce provenienti dalla rete e dagli Endpoint
- Analizza e correla minacce
- Diffonde informazioni sulle minacce alla rete e agli Endpoint

Palo Alto Networks
Next-Generation Firewall

Advanced Endpoint Protection

- Ispeziona tutti i processi e i file
- Previene sia exploit noti che sconosciuti
- Integrato con il cloud per prevenire malware noti e sconosciuti

Palo Alto Networks
Advanced Endpoint Protection

paloalto networks.

Preveniamo gli attacchi ad ogni livello della kill-chain

Breach the perimeter

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

Traps / WildFire

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

Lateral movement

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

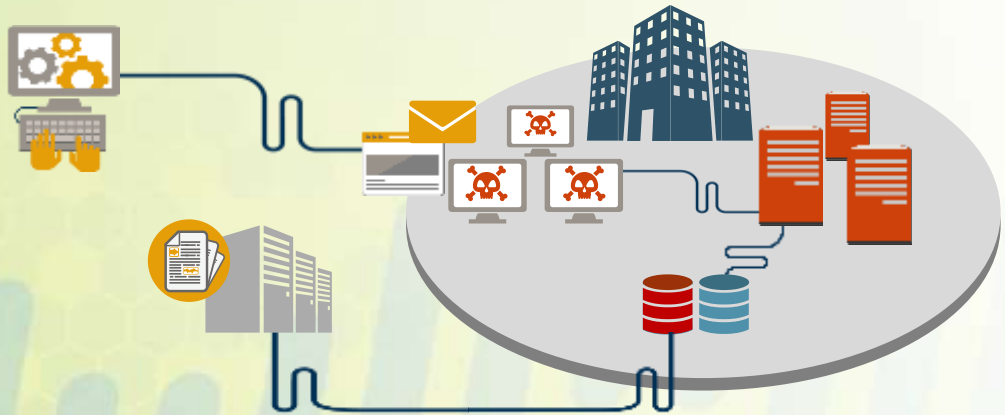
Exfiltrate data

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

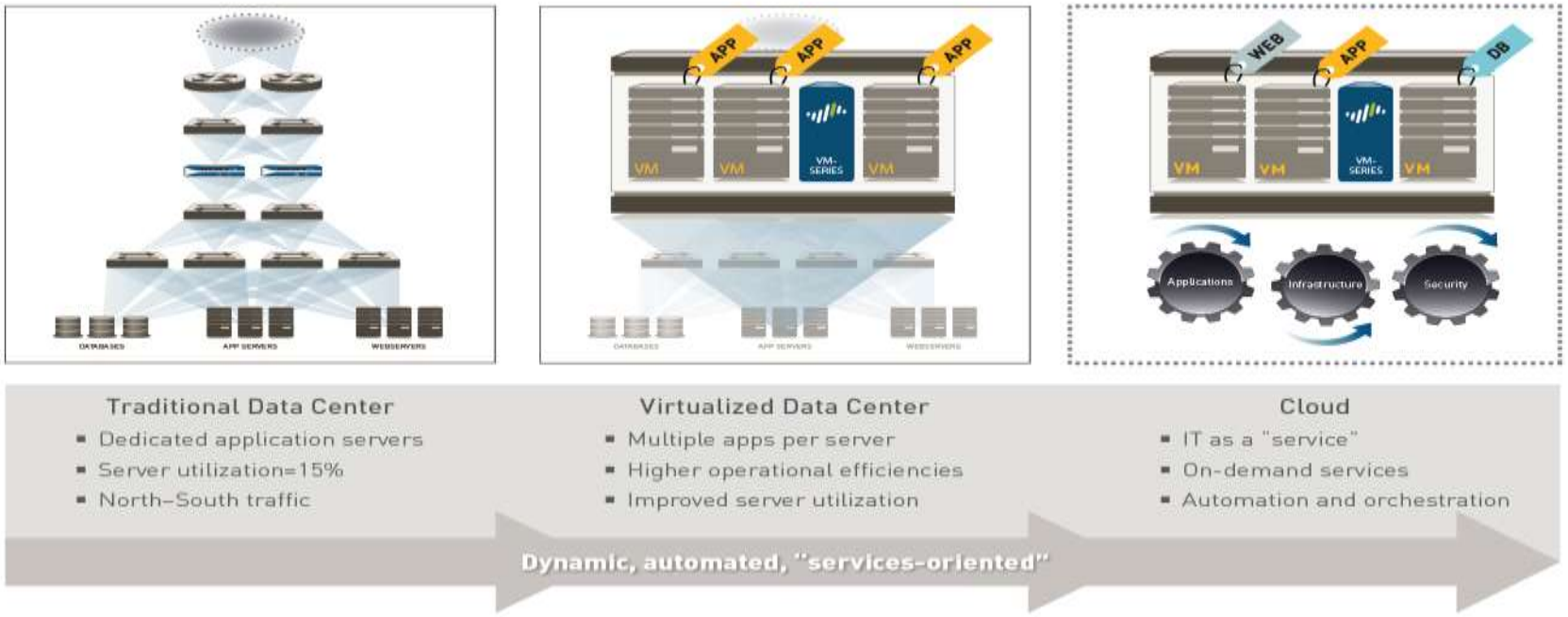


paloalto networks.

Integrazione Palo Alto Networks e VMware NSX

paloalto networks

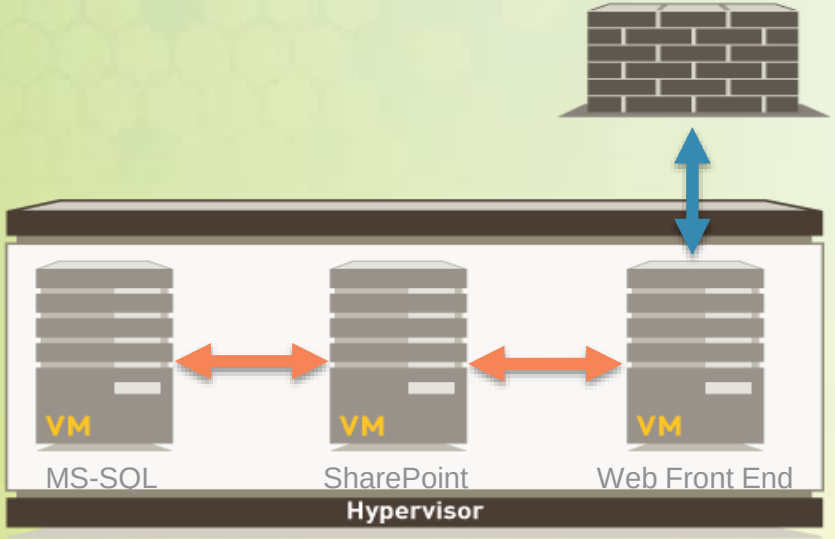
L'evoluzione verso la virtualizzazione e il cloud



paloalto networks.

Le sfide alla sicurezza nel cloud

I firewall fisici non possono vedere il traffico Est-Ovest

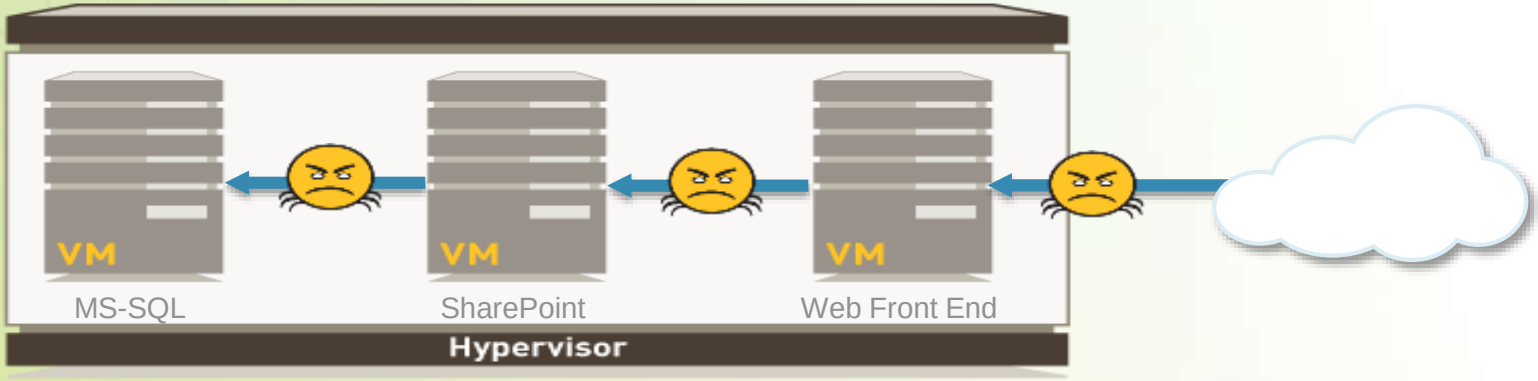


- Firewall placement is designed around expectation of layer 3 segmentation
- Network configuration changes required to secure East-West traffic flows are manual, time-consuming and complex
- Ability to transparently insert security into the traffic flow is needed

paloalto networks.

Le sfide alla sicurezza nel cloud

Security features incomplete su soluzioni di virtual security esistenti



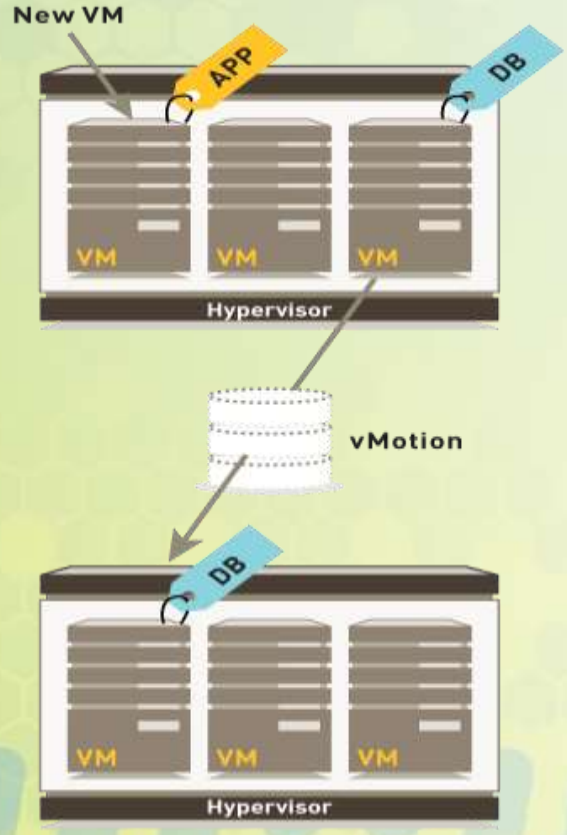
In the cloud, applications of different trust levels now run on a single server

- VM-VM traffic (East-West) needs to be inspected
- Port and protocol-based security is not sufficient
- Virtualized next-generation security is needed to:
  - Safely enable application traffic between VMs
  - Protect against against cyber attacks

paloalto networks.

Le sfide della sicurezza nel cloud

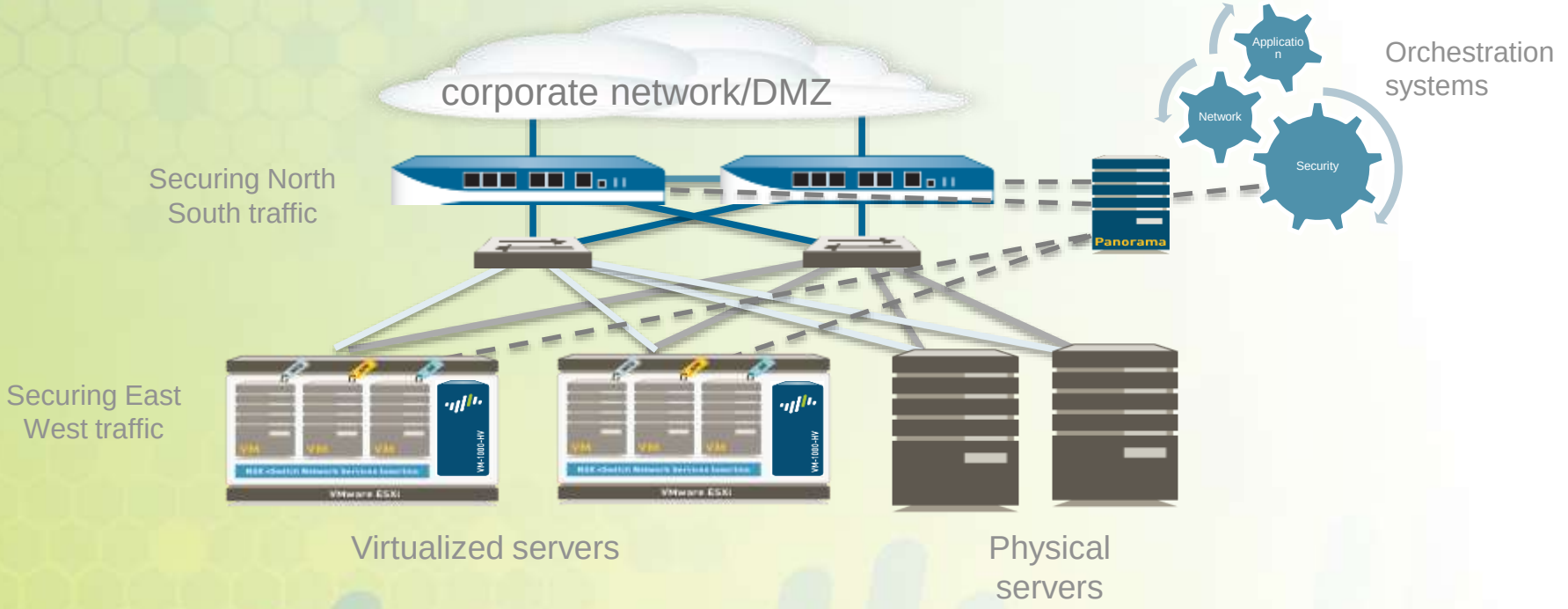
Le static policies non tengono il passo con i carichi di lavoro dinamici



- Provisioning of applications can occur in minutes with frequent changes
- Security approvals and configurations may take weeks/months
- Dynamic security policies that understand VM context are needed

paloalto networks.

Bisogna proteggere tutto il traffico del Data Center



Segment North South (physical) and East West (virtual) traffic

Tracks virtual application provisioning and changes via dynamic address groups

Automation and orchestration support via REST-API

paloalto networks.

Un approccio “platform” per combattere le minacce nel DC

Identify, control & decrypt

Detect & prevent *known & unknown* threats

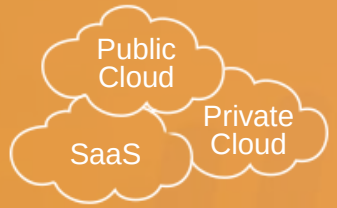
Automated forensics & remediation

Network

Endpoint

Traditional infrastructure

Cloud



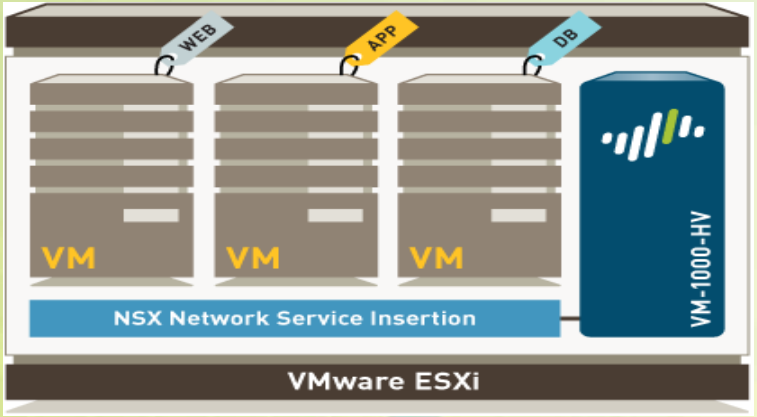
Mobile devices

Cloud

paloalto networks.

VM-Series per VMware NSX

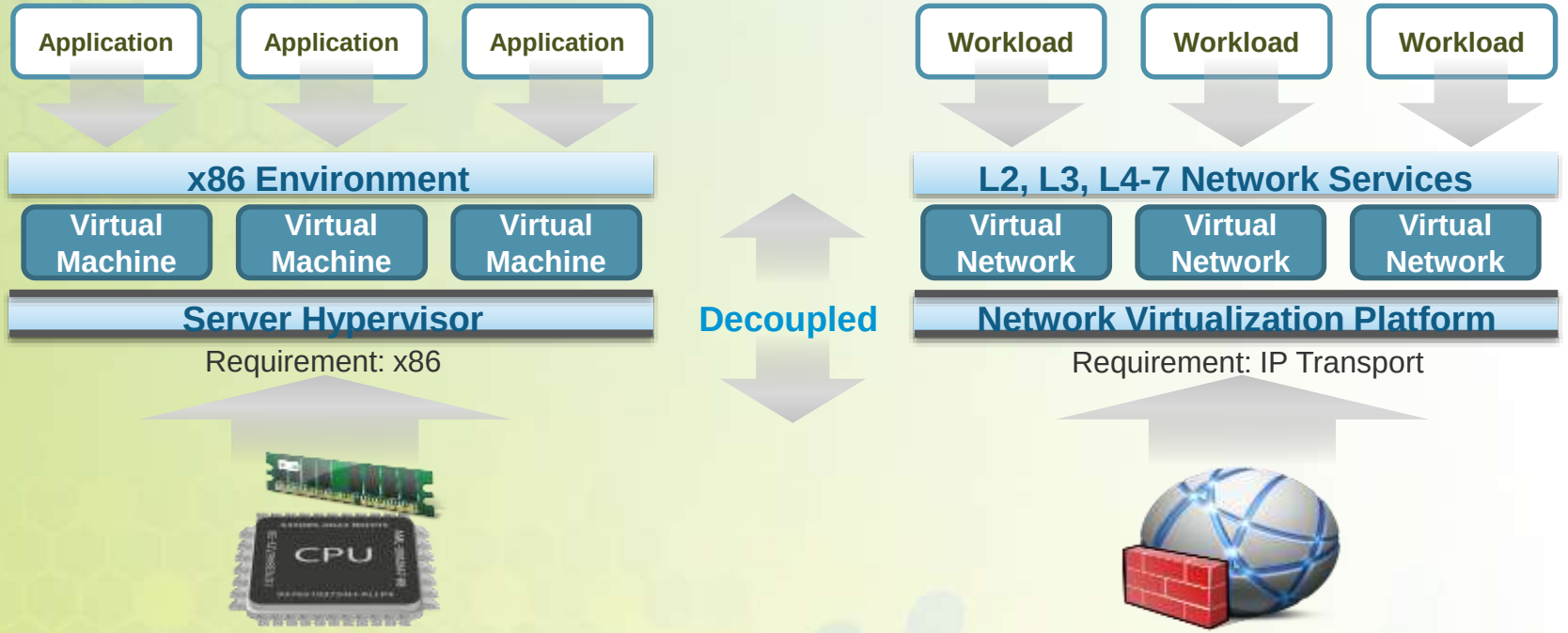
New VM-Series for VMware NSX deployed as a service



- Integrated solution with VMware for East-West traffic inspection
- Automated provisioning and deployment where a VM-Series is deployed on every ESXi server
- NSX automatically steers traffic to VM-Series
- Dynamic context sharing between NSX and Panorama

paloalto networks.

Cos'e' la network virtualization di Vmware NSX?



Physical Compute & Memory

(Dell, HP, IBM, Quanta,…)

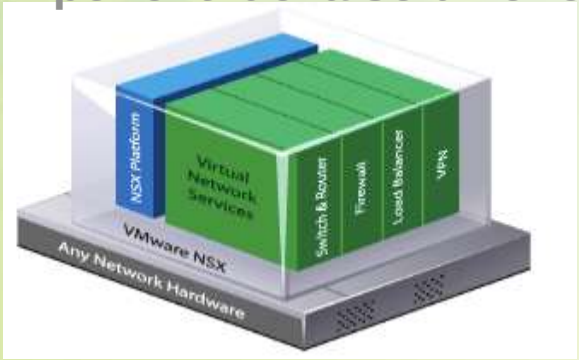
Physical Network

(Arista, Cisco, HP, Juniper, Cumulus,…)

paloalto networks.

Trasformare la network security per il data center

Componenti della soluzione:



VMware NSX

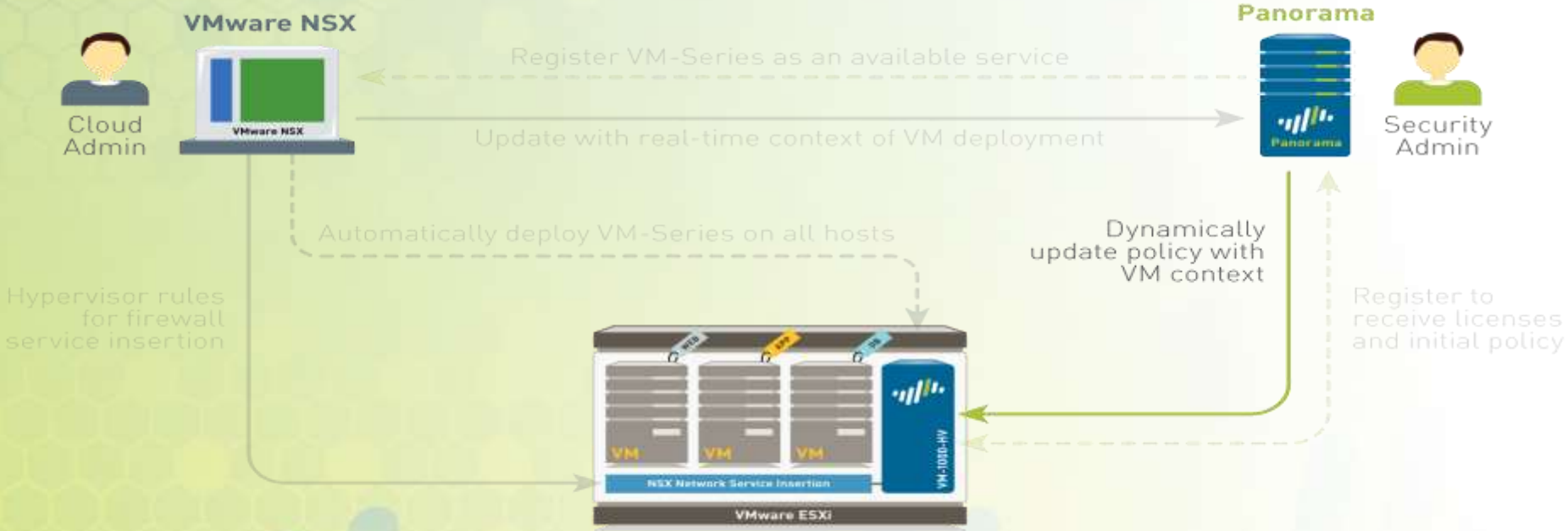
VM-Series

Panorama

Challenges	Solution
Firewall doesn't see the traffic	Automated, transparent services insertion at workload
Incomplete security capabilities	Virtualized next-generation security built from PAN-OS™
Static policies	Dynamic security policies with VM context

paloalto networks.

Come funziona : Dynamic Address Groups – Address updates



paloalto networks.

Incontrare le esigenze sia di infrastruttura che di sicurezza

Cloud

- **Accelerates app deployments** and unlocks cloud agility
- **Meets expectations** of security in this new operating model

Security

- **Increases visibility** and protection against cyber attacks
- **Maintains** consistent security controls for all DC traffic

paloalto networks.

VM-1000-HV per VMware NSX

VM-100	VM-200	VM-300	VM-1000-HV
50,000 sessions	100,000 sessions	250,000 sessions	250,000 sessions
250 rules	2,000 rules	5,000 rules	10,000 rules
10 security zones	20 security zones	40 security zones	40 security zones

- Next-generation firewall in a virtual form factor
  - **Consistent PAN-OS™ features** as hardware-based next-generation firewall
  - **Tracks VM creation and movement** with dynamic address groups
  - Supports **single-pass software architecture** to minimize latency
- Supports 2, 4, 8 CPU cores
- Performance is 1 Gbps FW throughput (App-ID enabled) and 600 Mbps threat protection

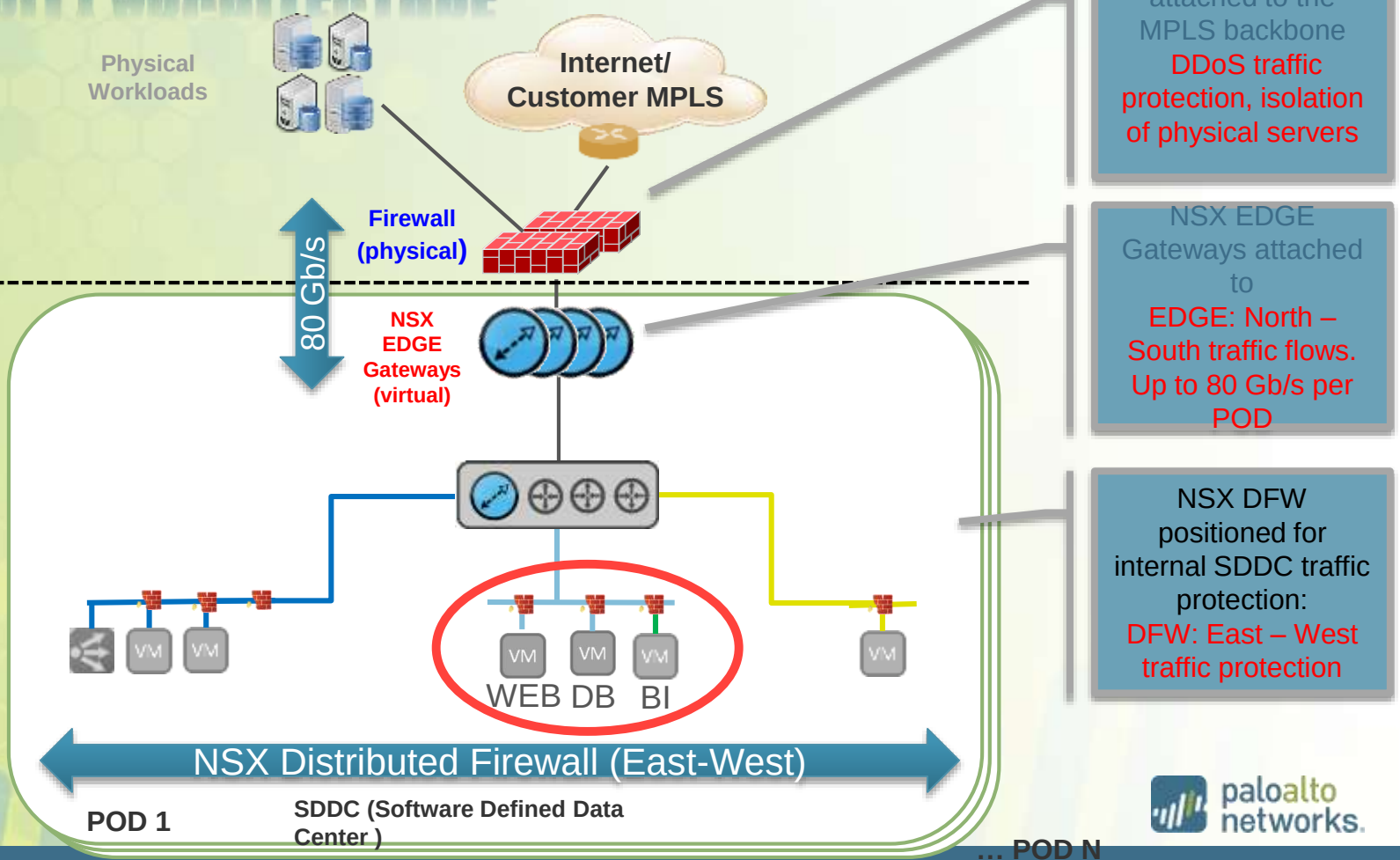
paloalto networks.

VMware & Palo Alto Networks

Use cases

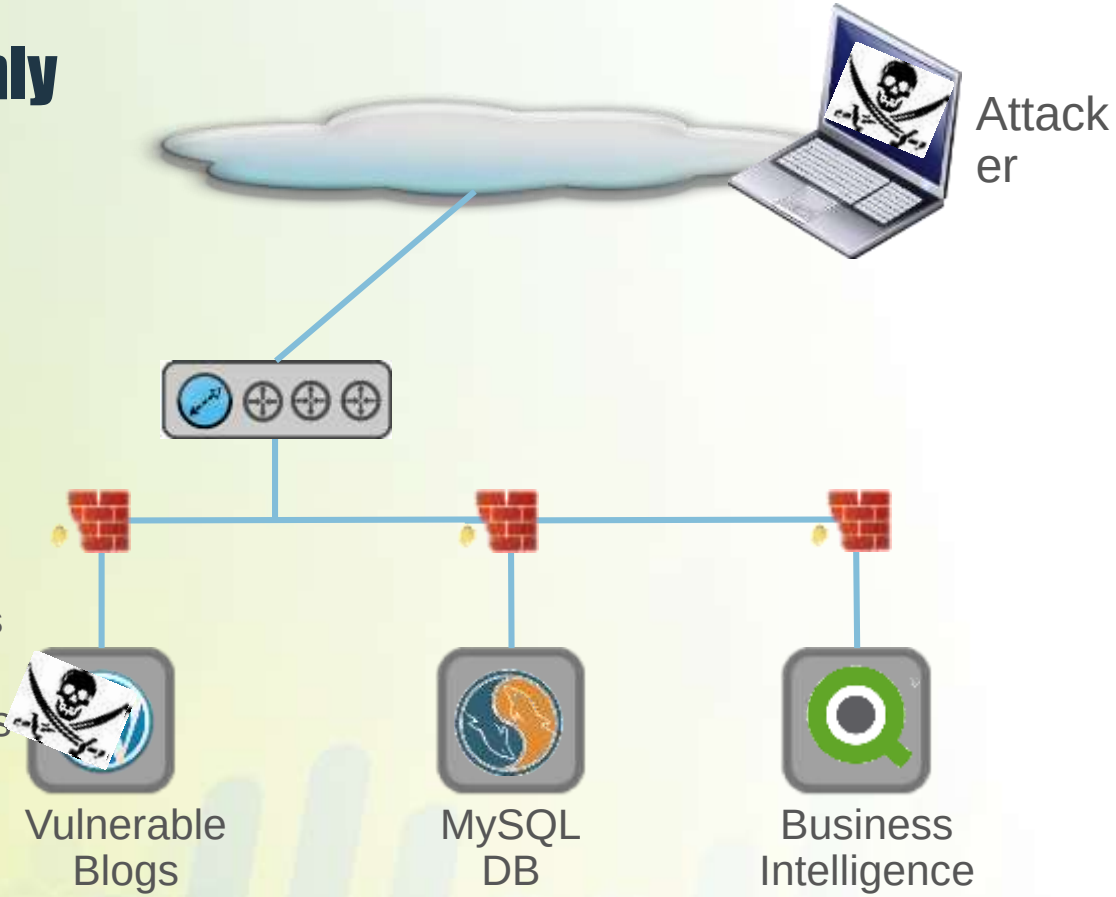
paloalto networks

SECURITY ARCHITECTURE



Attack Scenario – NSX Only

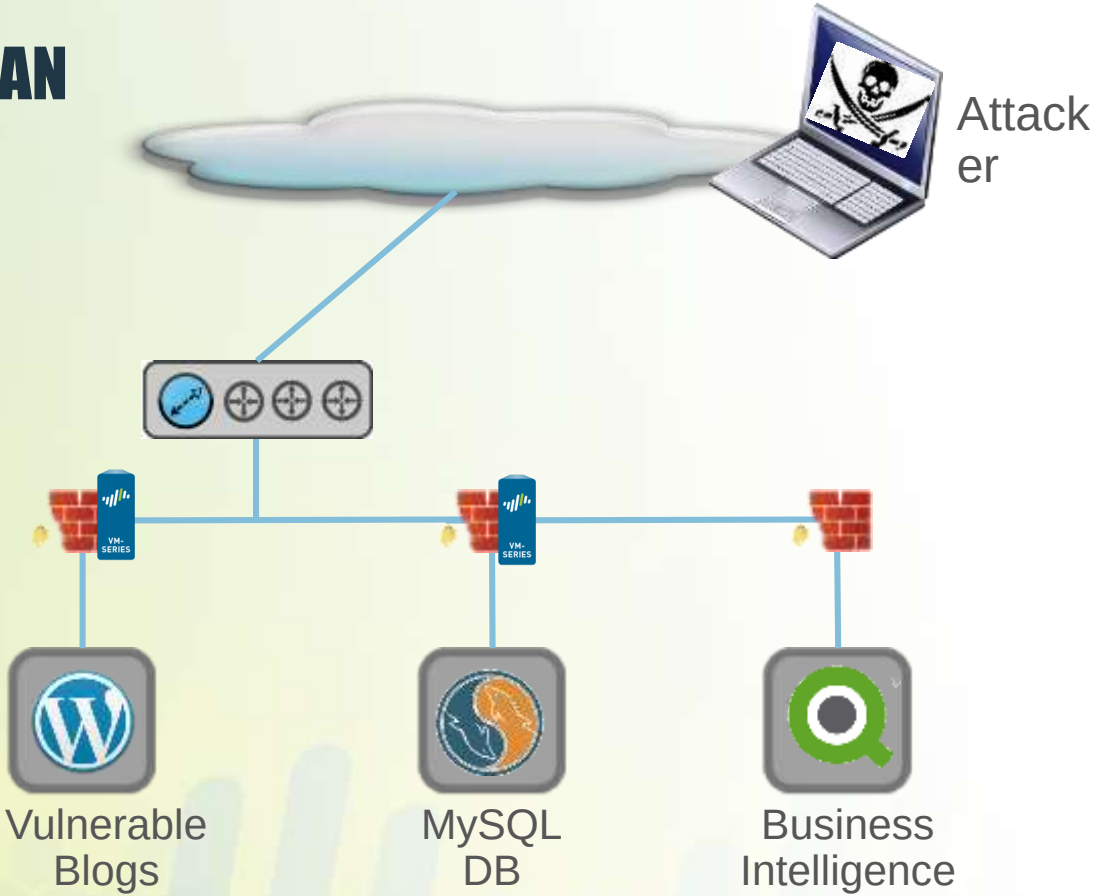
- All VMs are in the same subnet
- NSX Stateful L4 Firewall in place:
  - Allow SSH and PING to VMs
  - Allow HTTP to Web Server
  - Allow MySQL between Web & DB
  - Reject all other traffic
  - BI VM is isolated from other VMs
- Web Server hosts 2 blogs with known application vulnerabilities
- Attacker gets control of Web VM
- Then he can brute force MySQL
- BI VM is still protected by NSX



paloalto networks.

Attack Scenario – NSX + PAN

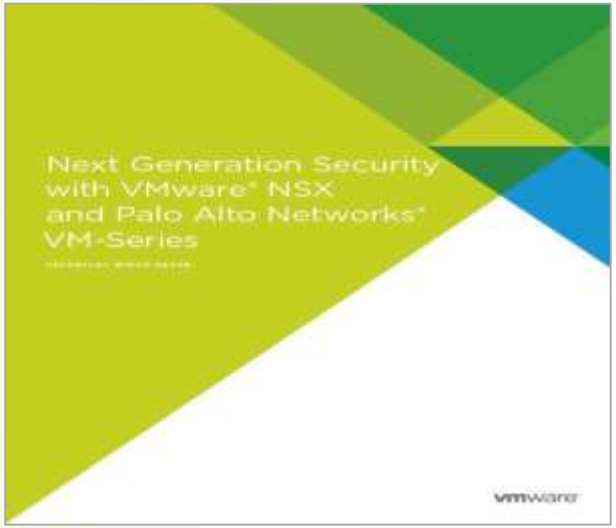
- Same L4 policies as before
- NSX steers traffic to PAN VMs:
  - HTTP from any to Web Server
  - MySQL from Web Server to DB
- Web Server is still vulnerable!
- Attacks to Web VM fail!
- No other VM is compromised!



paloalto networks.

Per saperne di piu'…

- Leggete il nostro documento tecnico congiunto sui casi di integrazione e di utilizzo:



- Altre info:

www.paloaltonetworks.com/vmware

http://www.vmware.com/products/nsx/resources.html

VMware Hands-On-Labs: http://labs.hol.vmware.com
Integration Lab: HOL-PRT-1462

VMware NSX Design Guide:
https://communities.vmware.com/servlet/JiveServlet/previewBody/27683-102-3-37383/NSXvSphereDesignGuidev2.1.pdf

paloalto networks.

paloalto networks.

paloalto networks.