Virtualized Data Center with Palo Alto Networks

Agenda

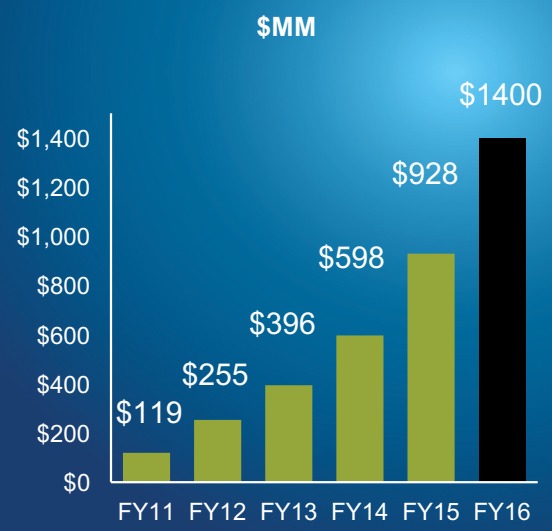
- About Palo Alto Networks
- Security challenges within Software Defined Data Centers
- Palo Alto Networks VM-Series Integration with VMware NSX
- Break
- Hands-on Workshop

Palo Alto Networks at-a-glance

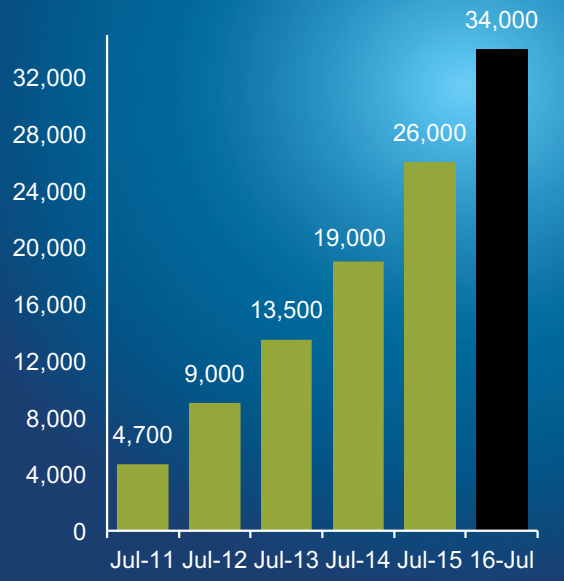
CORPORATE HIGHLIGHTS

- Founded in 2005; first customer shipment in 2007
- Safely enabling applications and preventing cyber threats
- Able to address all enterprise cybersecurity needs
- Exceptional ability to support global customers
- Experienced team of 3,800+ employees
- Q4 FY16: $401.8M revenue

REVENUES



ENTERPRISE CUSTOMERS

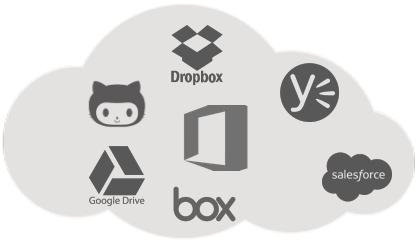


Managing security risk has become more complex

..with the emergence of private, public, hybrid and SaaS clouds…

Private Cloud(NSX, OpenStack)

Public Cloud(IaaS, PaaS)



Software as a Service(SaaS)

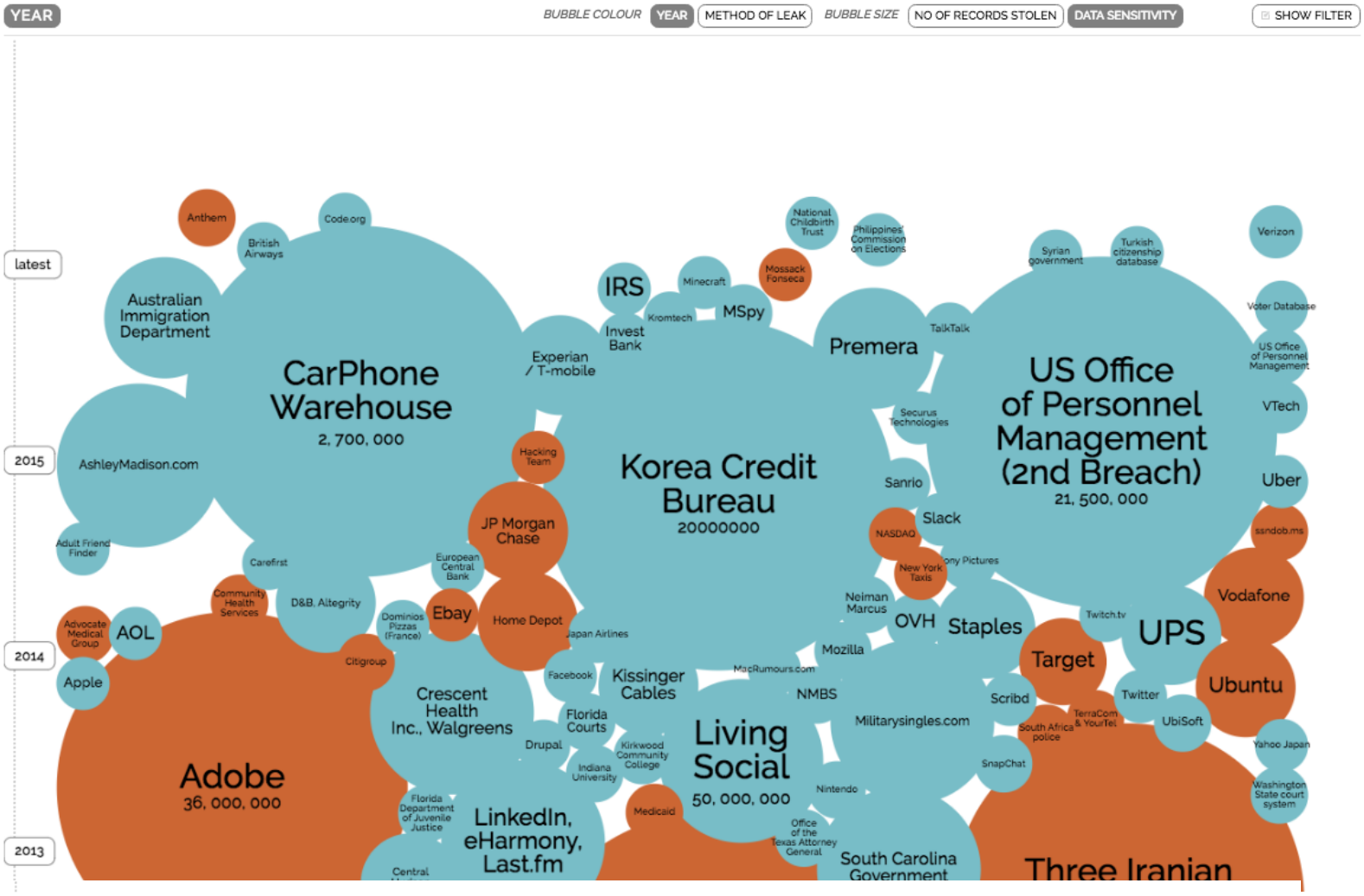
Apps & Data

Apps & Data

Data

Data Breaches

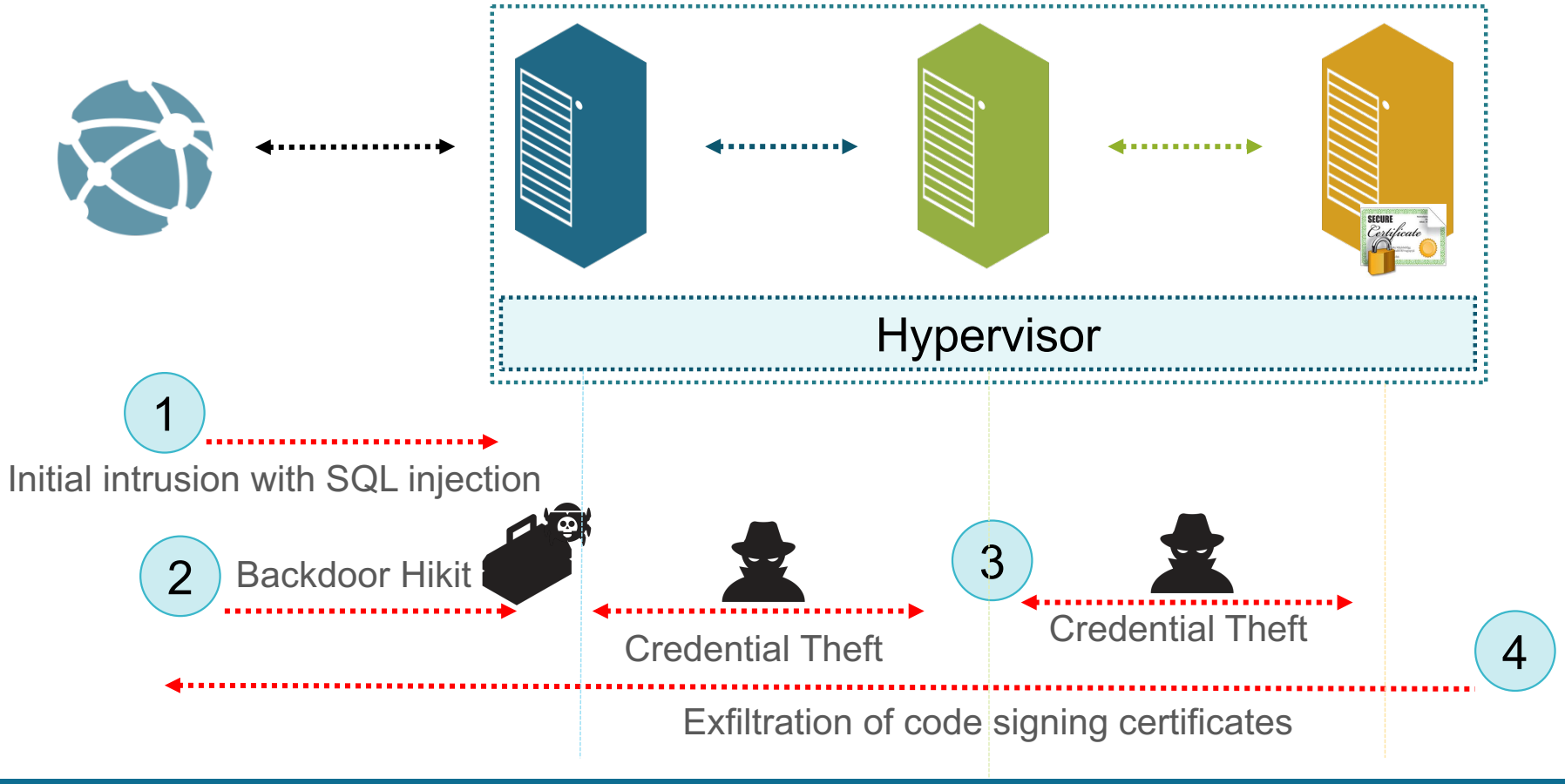
Bigger and Frequent



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

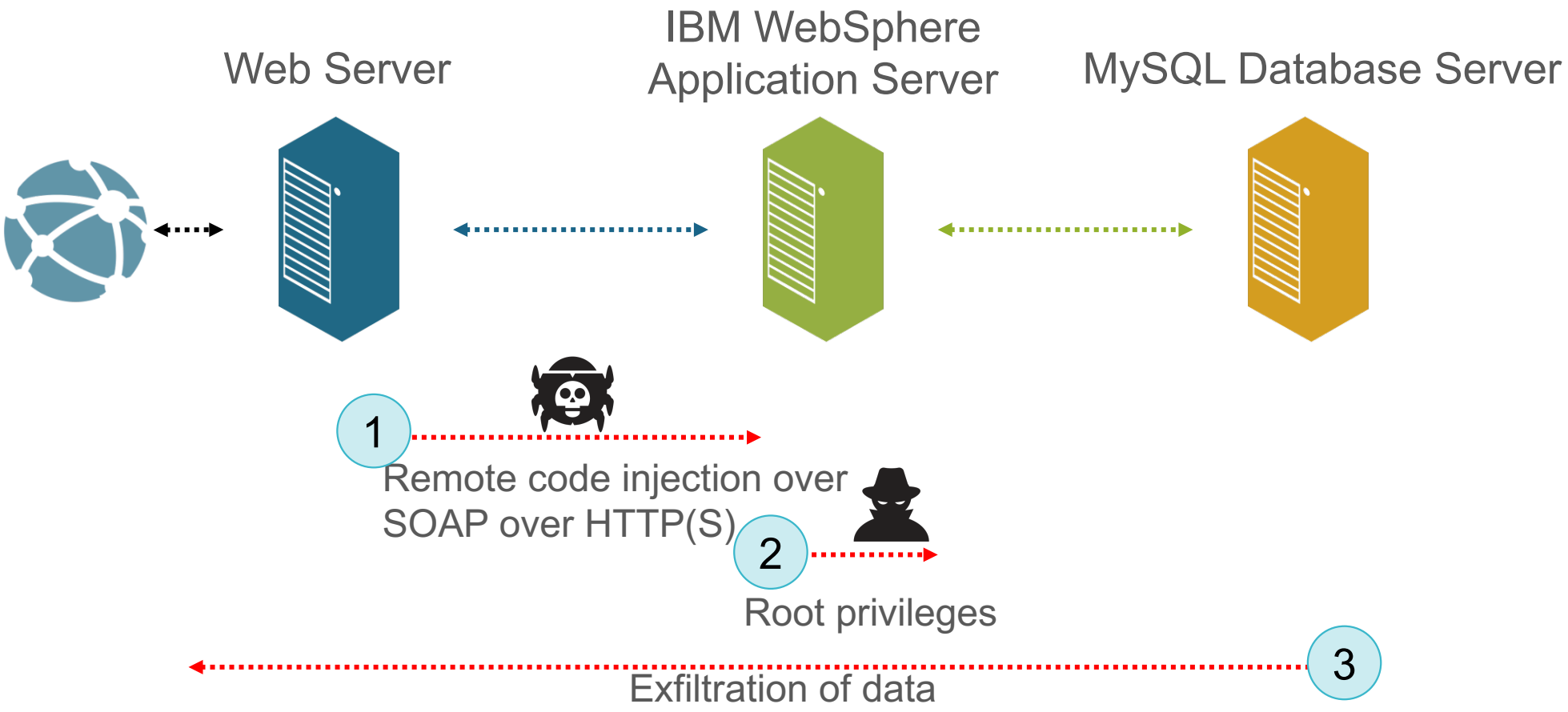
Attack propagation within a cloud

..multi-phased attack resulting in data exfiltration



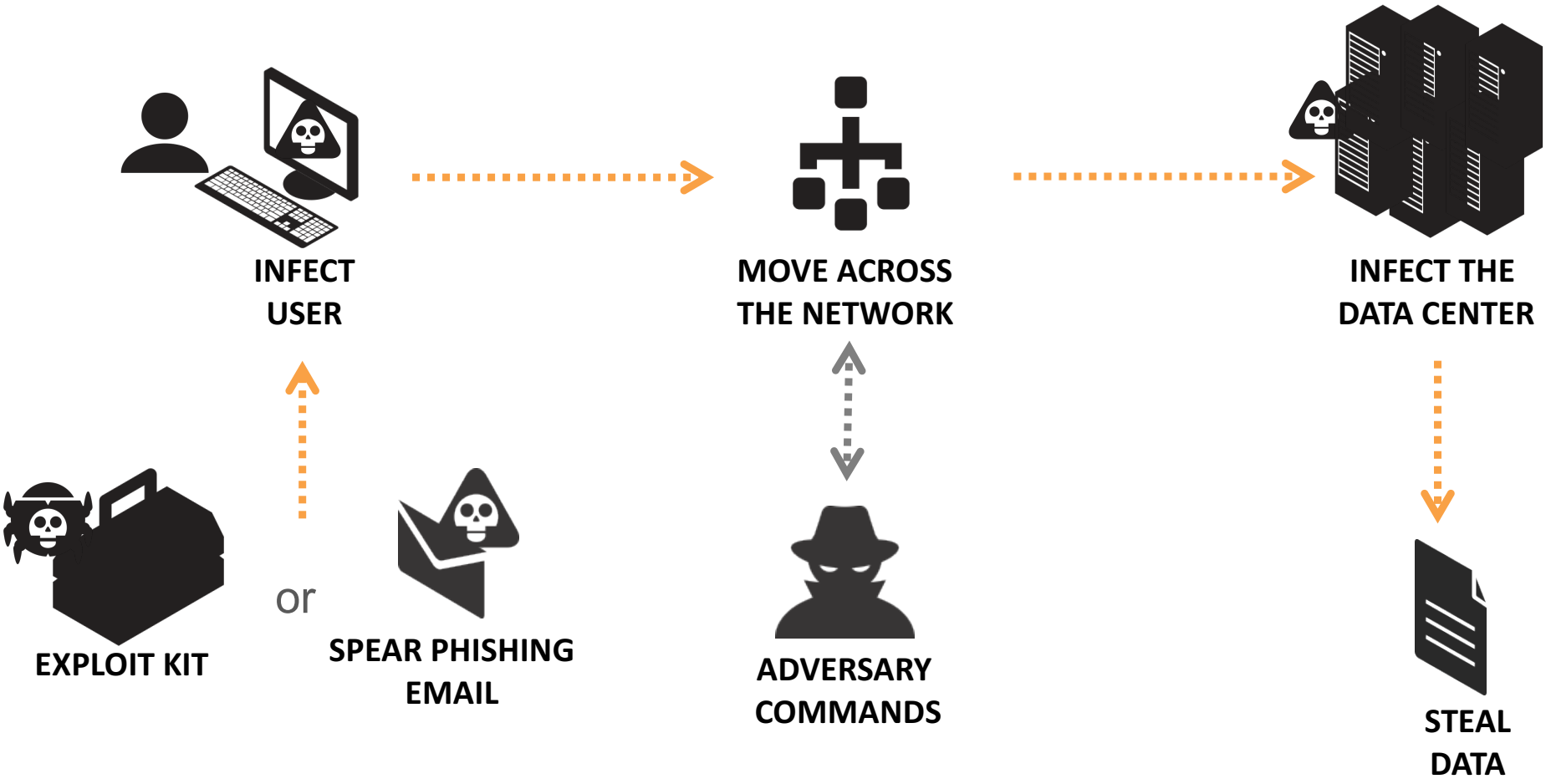
Port/protocol based controls are not enough

..a targeted attack for achieving lateral movement within data centers



The common thread in data loss incidents

…same life cycle is followed across both physical or virtualized network



The security challenge

…within cloud deployments

Lack of Visibility

Manual Security Operations

Inconsistent Security Capabilities

Key requirements

…for a secure software defined data center

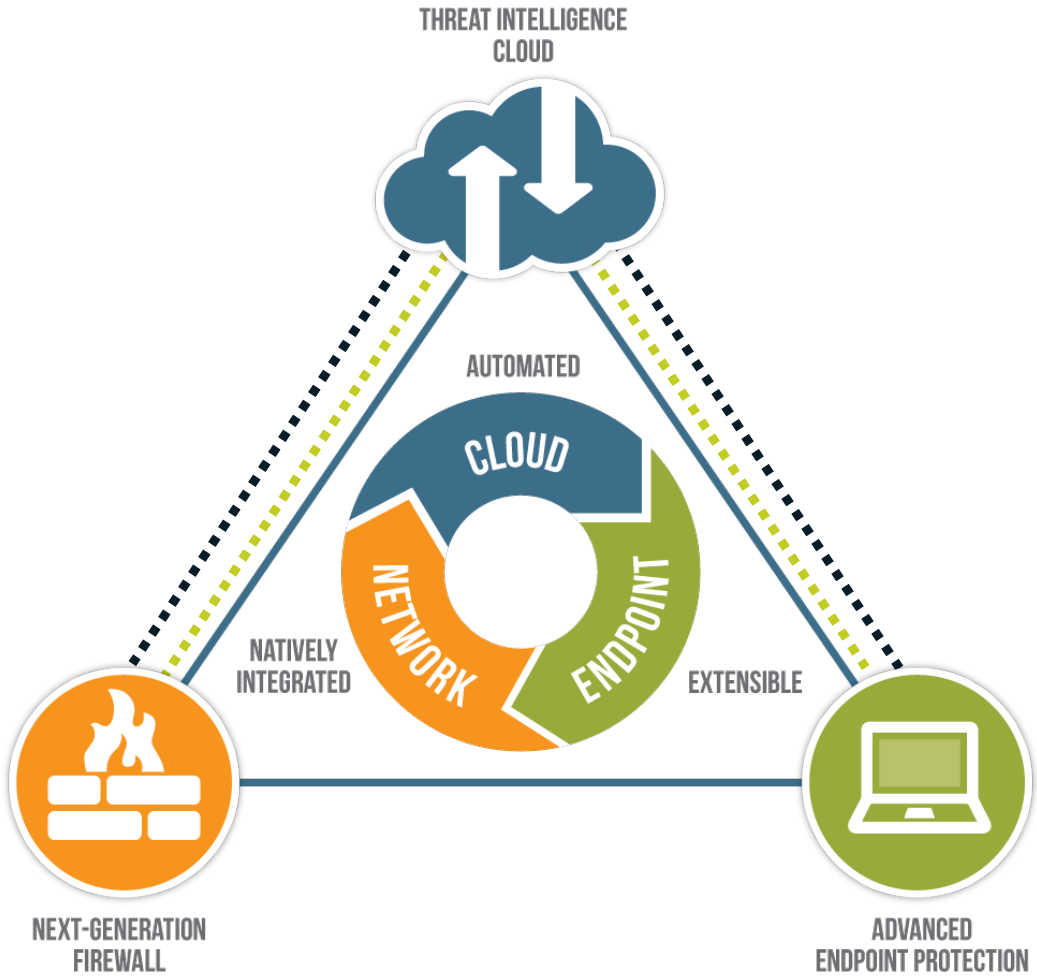
Get granular visibility into who and what Is in your network

Deploy security in lockstep with your workloads

Prevent threats from moving laterally and compromising your data center

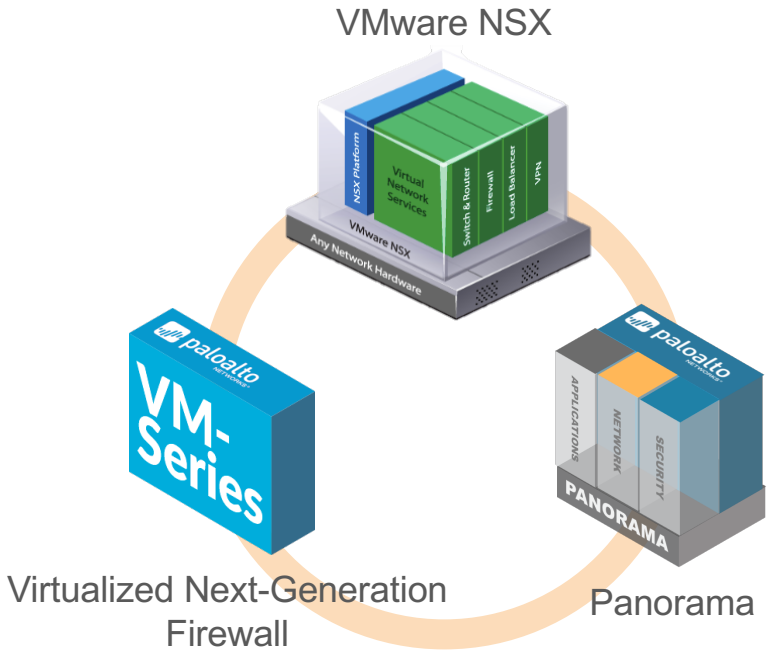
Consistent and uniform security posture

Delivering the next-generation security platform



VM-Series for NSX – Virtualized Next Generation Firewall

…delivering application visibility, control and advanced threat protection for SDDC



Automate security service insertion

Apply dynamic security policy updates

Enable micro-segmentation of applications

Protect applications and data from cyber threats

Automated security service insertion

…of Palo Alto Networks VM-Series virtualized NGFW by VMware NSX manager

Integration benefits

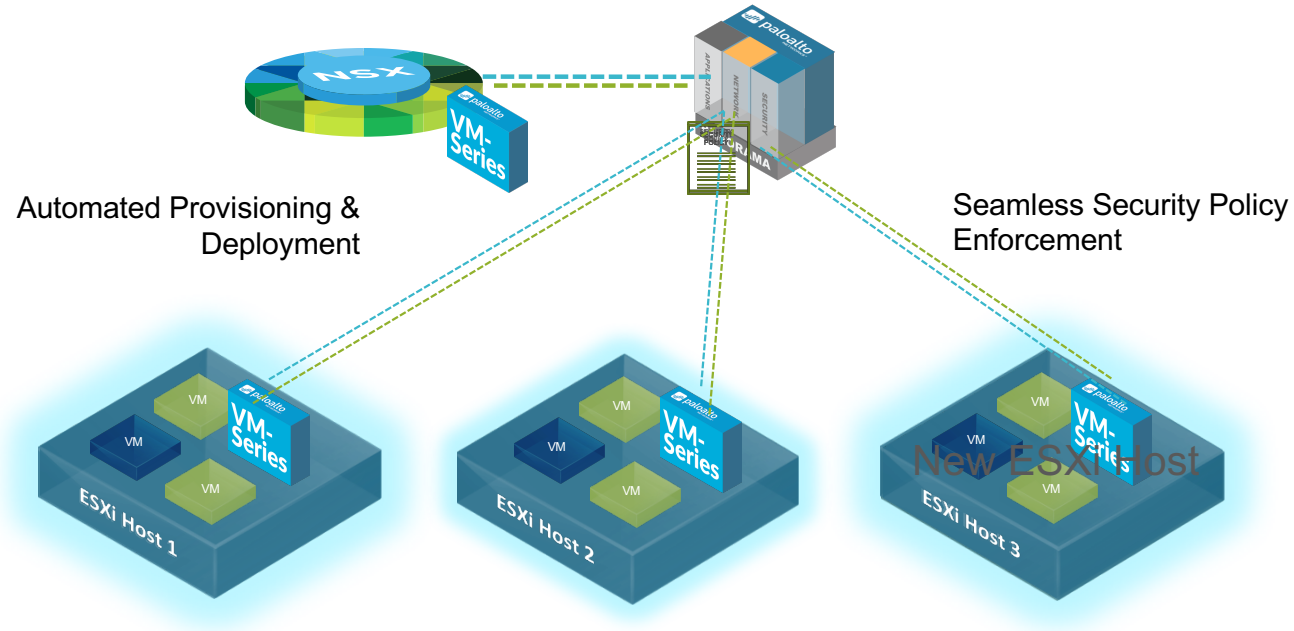
Apply security protections automatically and on-demand

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

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 policy updates

…by leveraging security tags on Palo Alto Networks VM-Series

Integration benefits

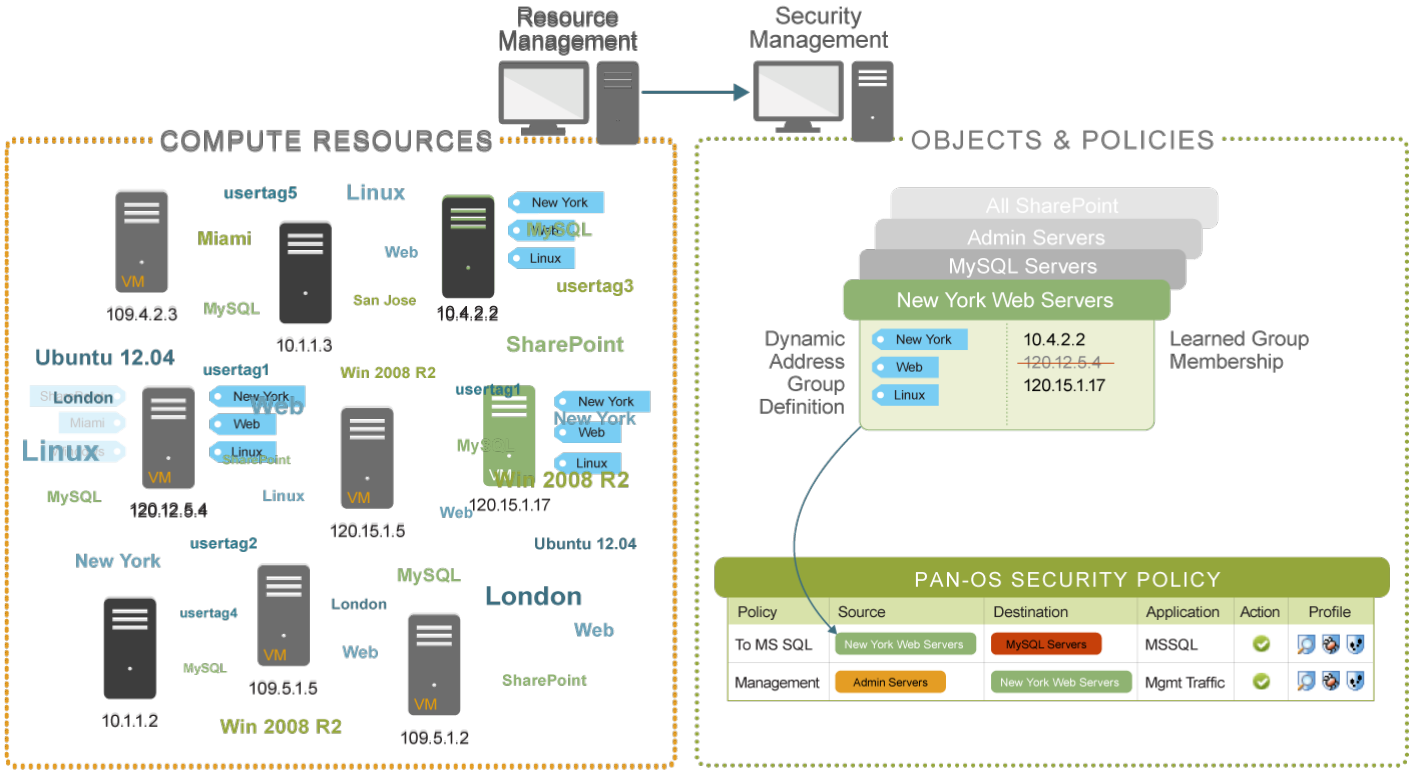
Apply security protections automatically and on-demand

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

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



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

Granular segmentation

…with application based security policies on Palo Alto Networks VM-Series

Integration benefits

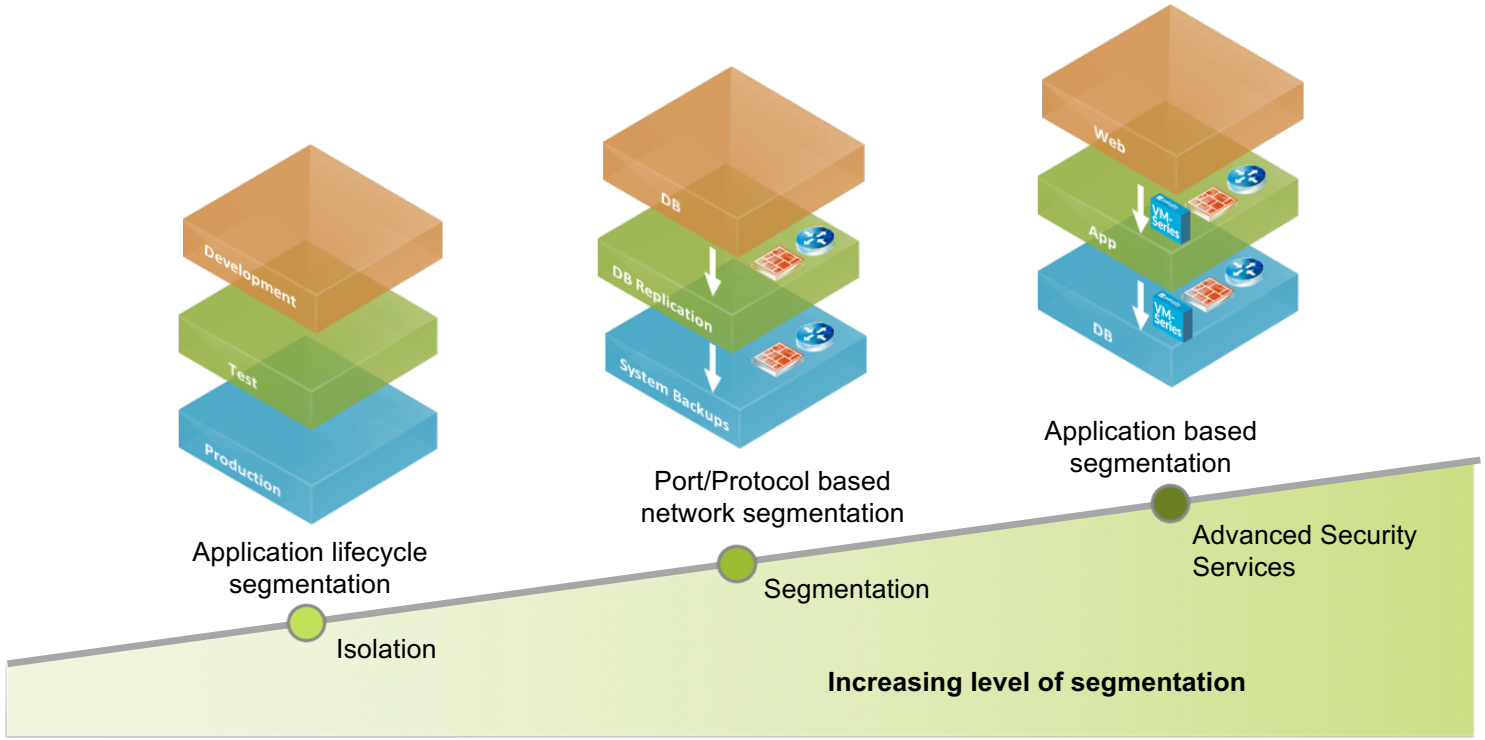
Apply security protections automatically and on-demand

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

through granular micro-segmentation



Protect your applications and data

…from known and unknown malware

Integration benefits

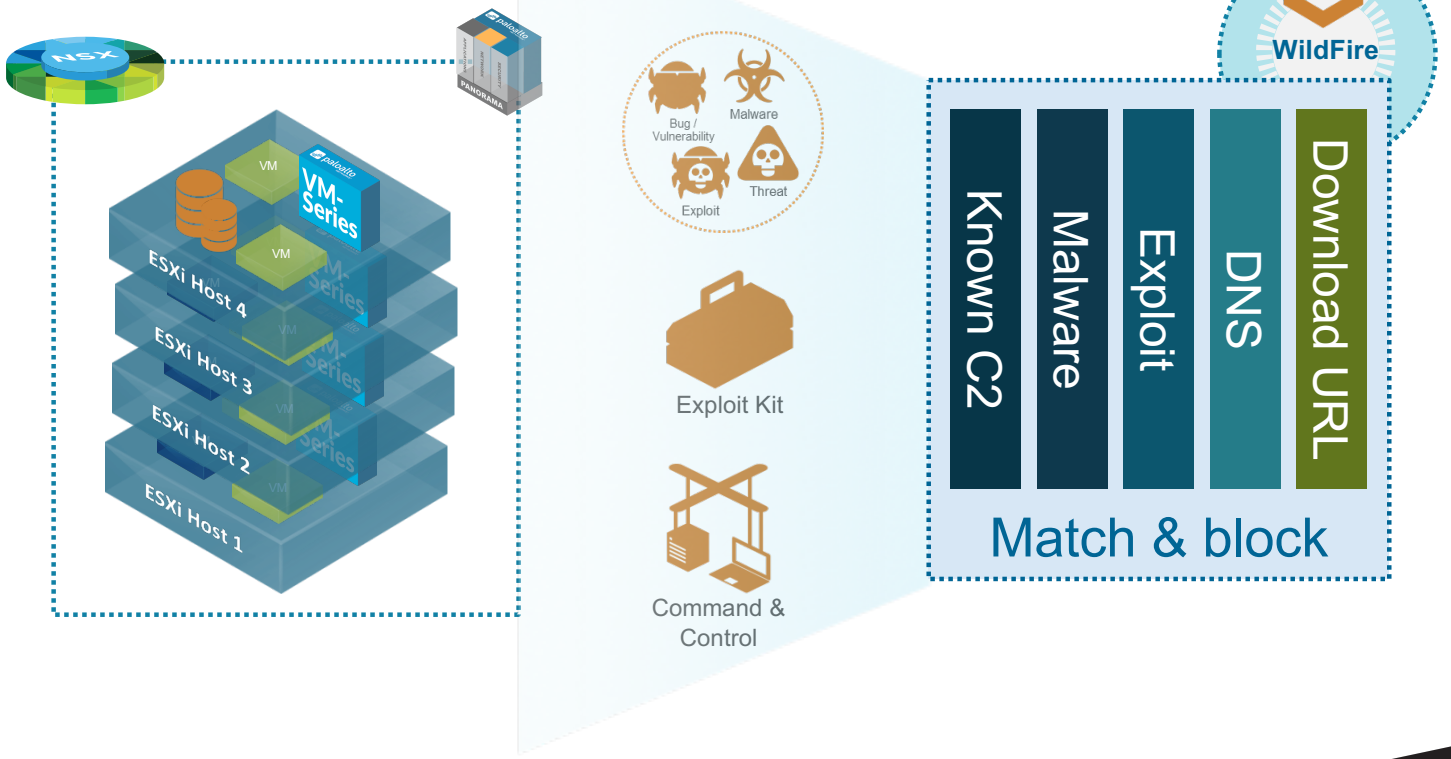
Apply security protections automatically and on-demand

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

With security profiles on VM-Series



Detect & prevent unknown

- Malware
- Exploits
- Command-and-control
- DNS queries
- Malware URLs

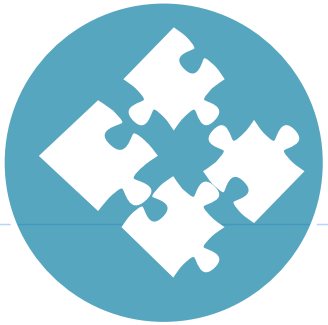
Joint integration delivers

…inherently secure software defined data centers

Pervasive Visibility & Control

Get granular visibility into who and what Is in your network

Automated Security Service Insertion

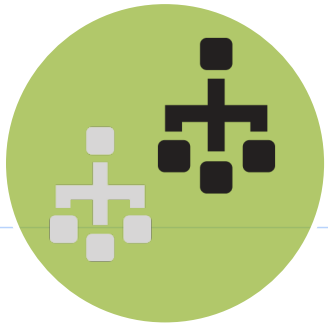


Deploy security in lockstep with your workloads

Advanced Threat Protection

Prevent threats from moving laterally and compromising your data center

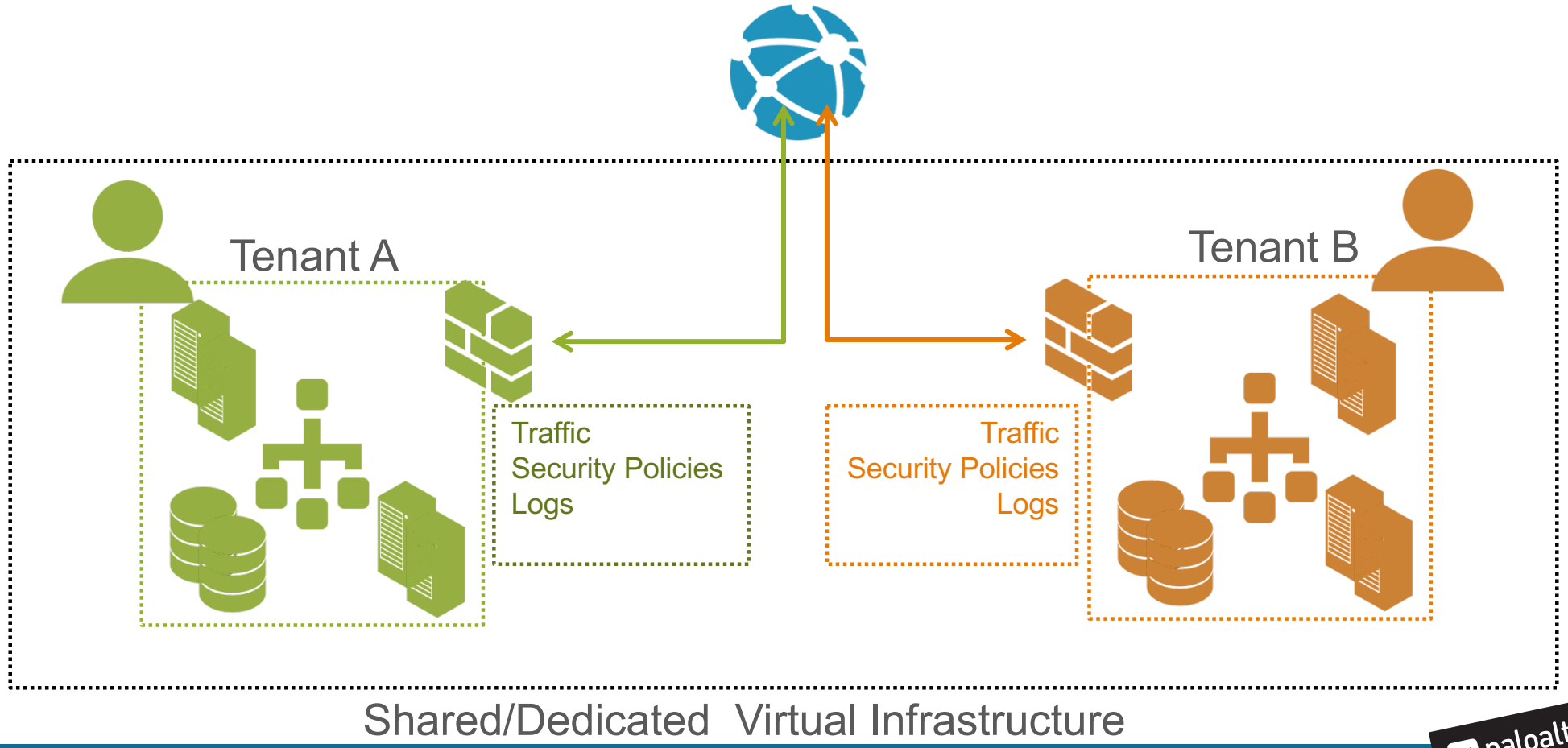
Secure Multi-Tenant Clouds



Meet your compliance and audit mandates with secure tenant isolation

The challenge of secure tenant isolation

..goes beyond traffic separation/isolation

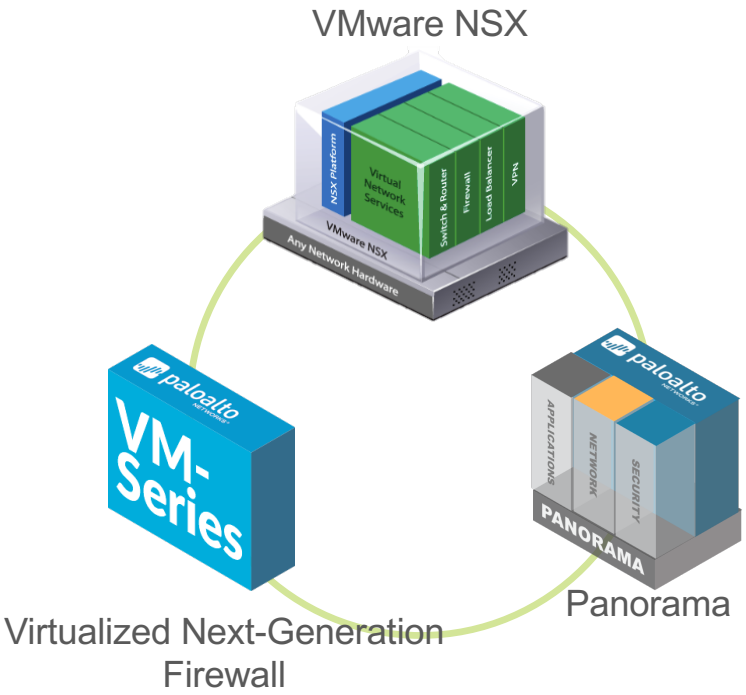


Key requirements for secure multi-tenancy within SDDC

- Ability to create unique tenant profiles
- Support tenant configurations with overlapping IP infrastructure
- Multiple VM-series firewalls on a single ESXi host

VM-Series for NSX – Virtualized next-generation firewall

…delivering application visibility, control and advanced threat protection for SDDC



Secure Multi-Tenancy & Multiple Policy Set Support

- Data Plane and Control Plane Separation
- Duplicate IP Address Support

Automate security service insertion

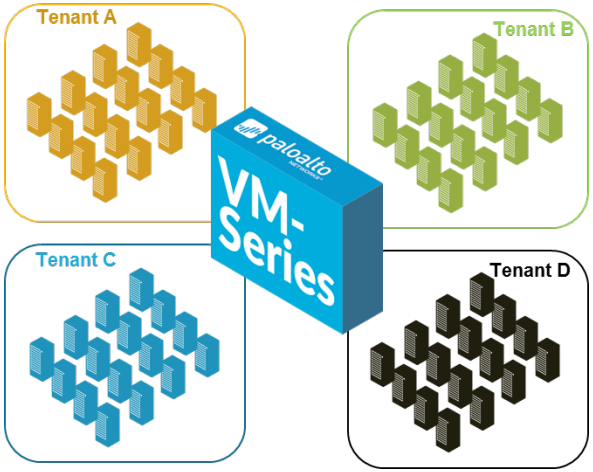
Apply dynamic security policy updates

Enable micro-segmentation of applications

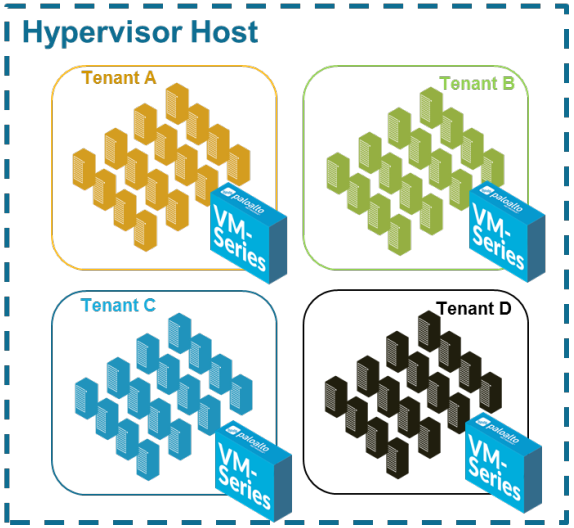
Protect applications and data from cyber threats

Design considerations

..three different approaches to deployment



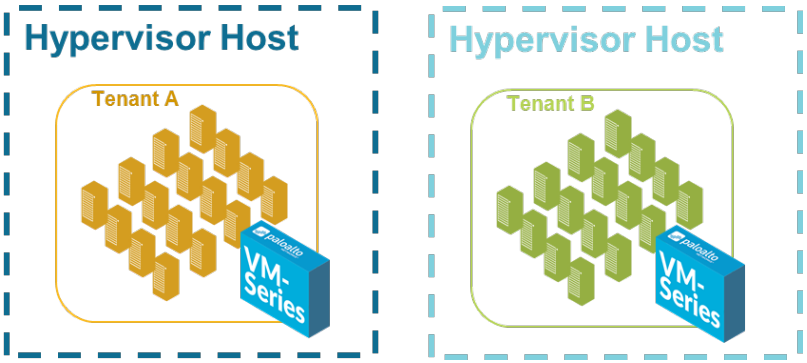
Logical tenant isolation



Dedicated security per tenant

Shared Infrastructure

NSX Manager

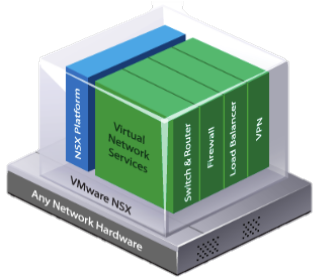


Dedicated security per tenant

Dedicated Infrastructure

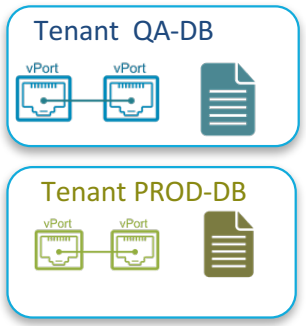
Logical tenant isolation (#1)

…over shared infrastructure



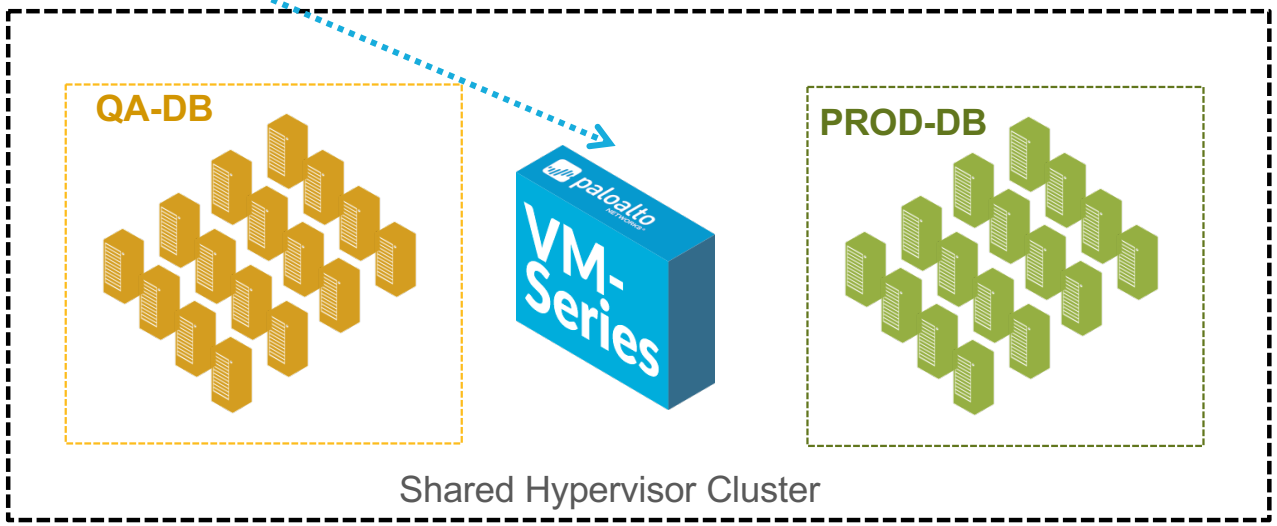
QA-DB Service Profile

PROD-DB Service Profile



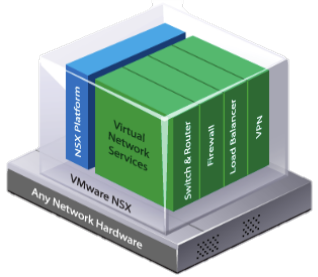
Duplicate IP Address Support

Tenant QA-DB	Tenant PROD-DB
192.168.10.0/24	192.168.10.0/24



Logical tenant isolation (#1)

..over shared infrastructure

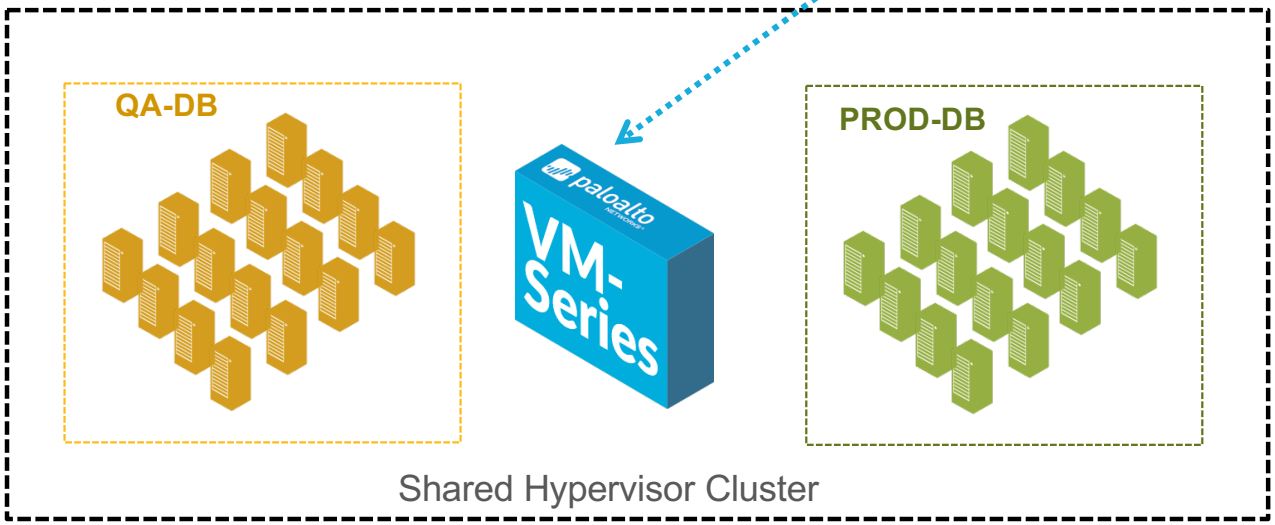


QA-DB Service Profile
PROD-DB Service Profile

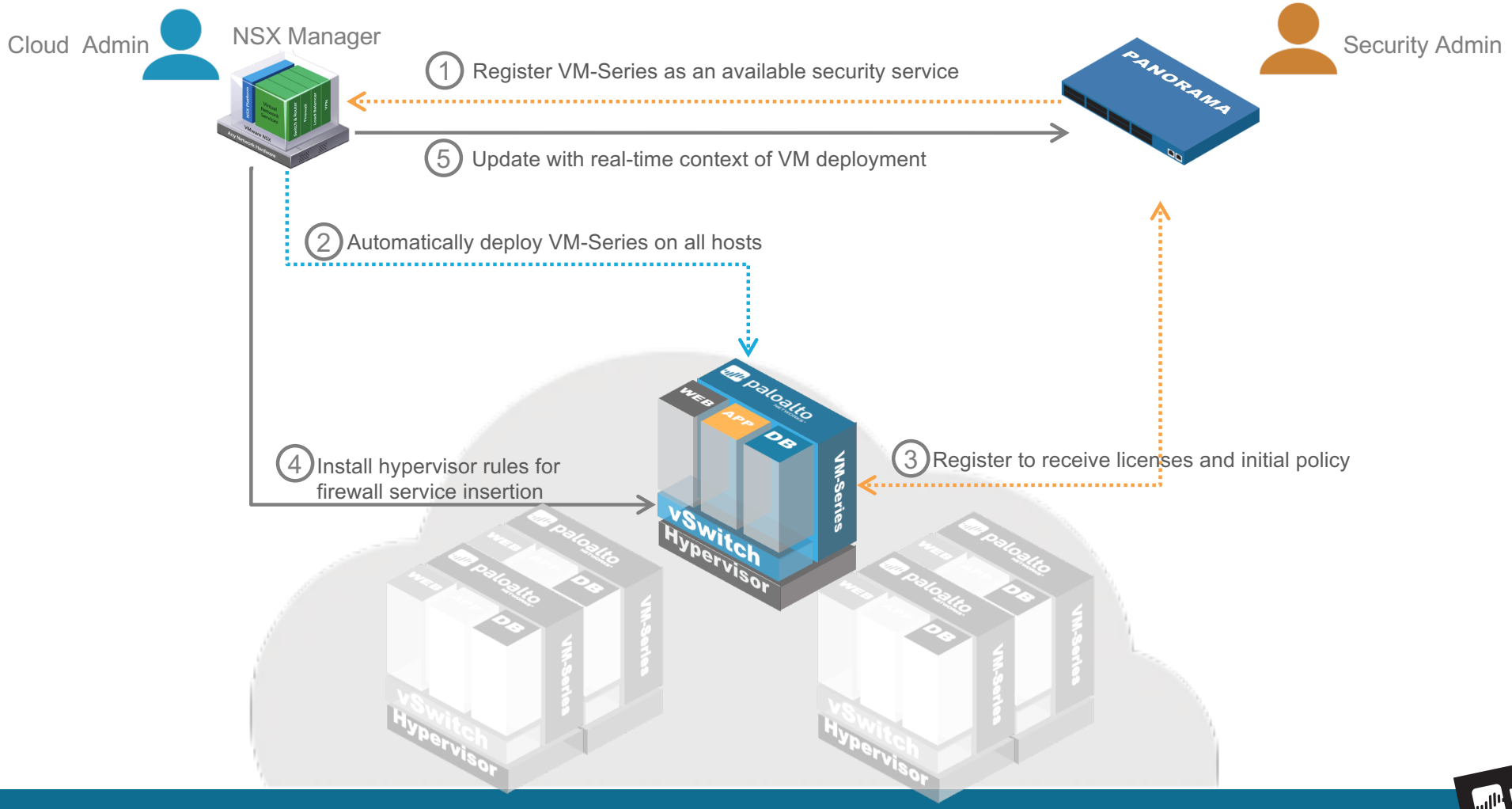
Policy Set
Template
OVF version
License Auth-Code

QA-DB Service Definition
PROD-DB Service Definition

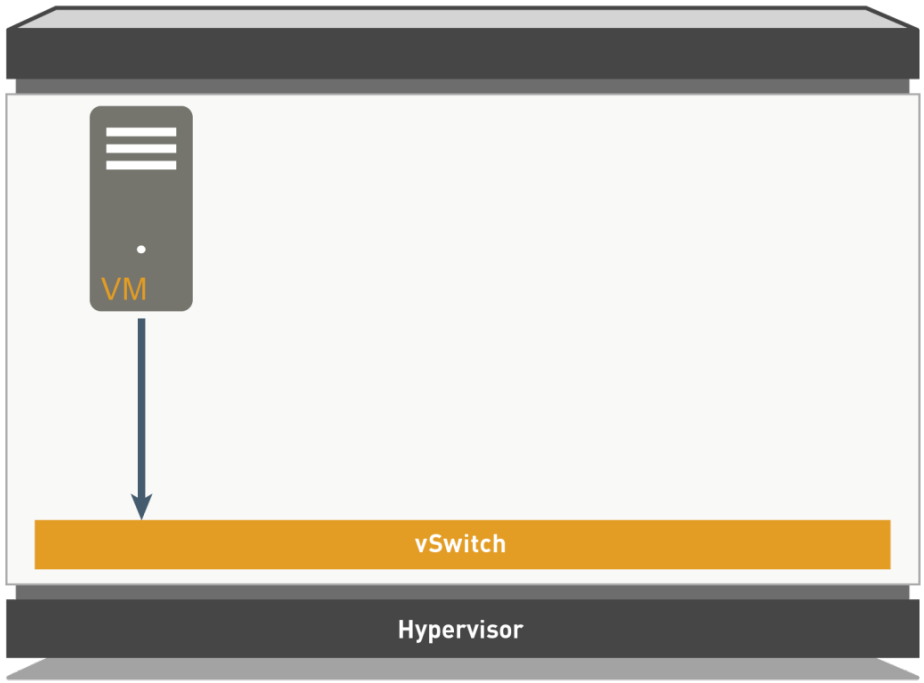
Policy Set
Template
OVF version
License Auth-Code



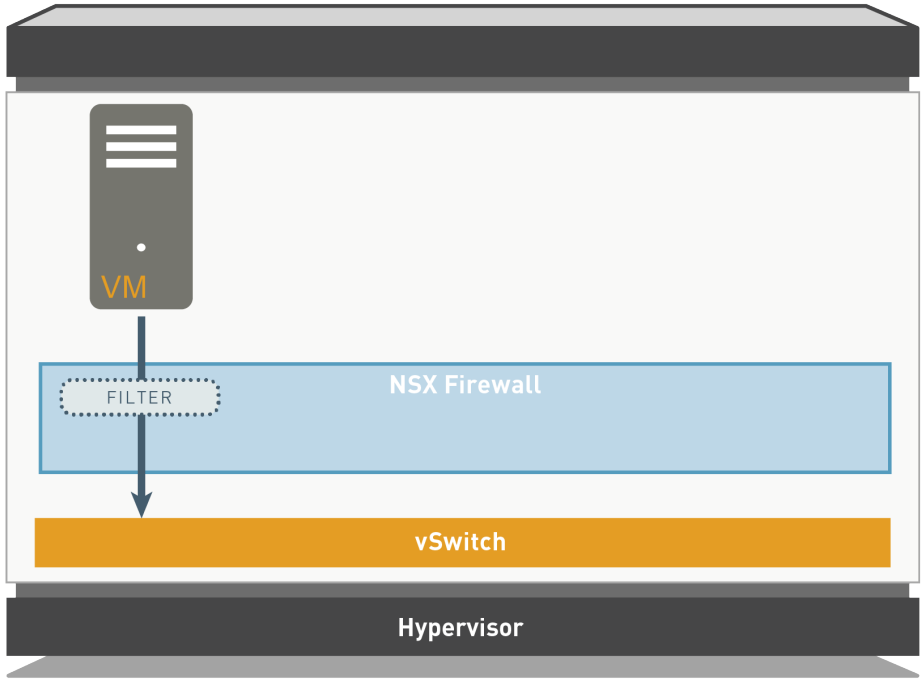
VM-Series integration workflow with VMware NSX



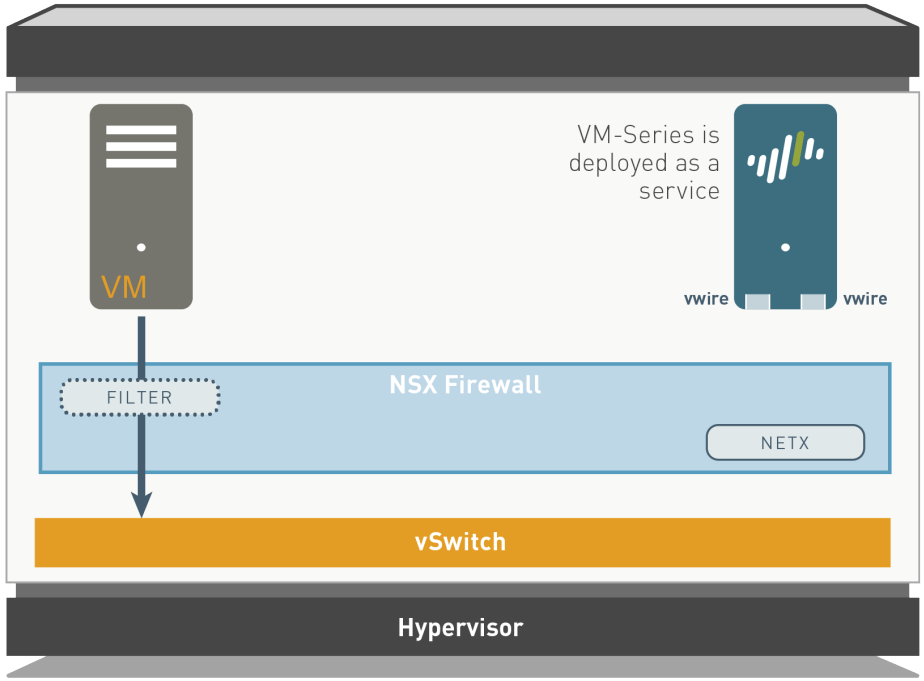
NSX + VM-Series packet flow



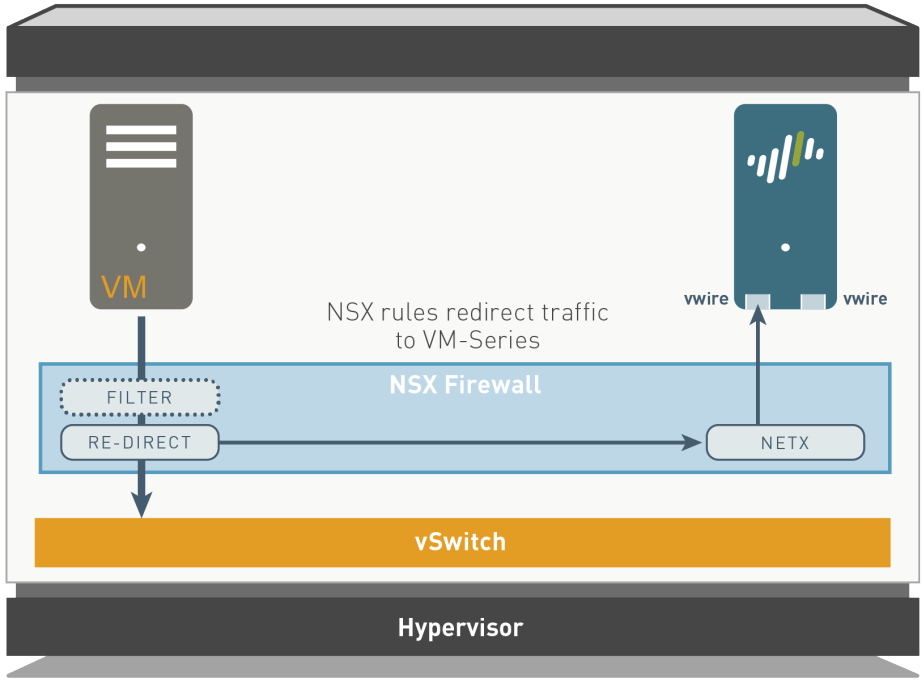
Packet Flow: NSX firewall



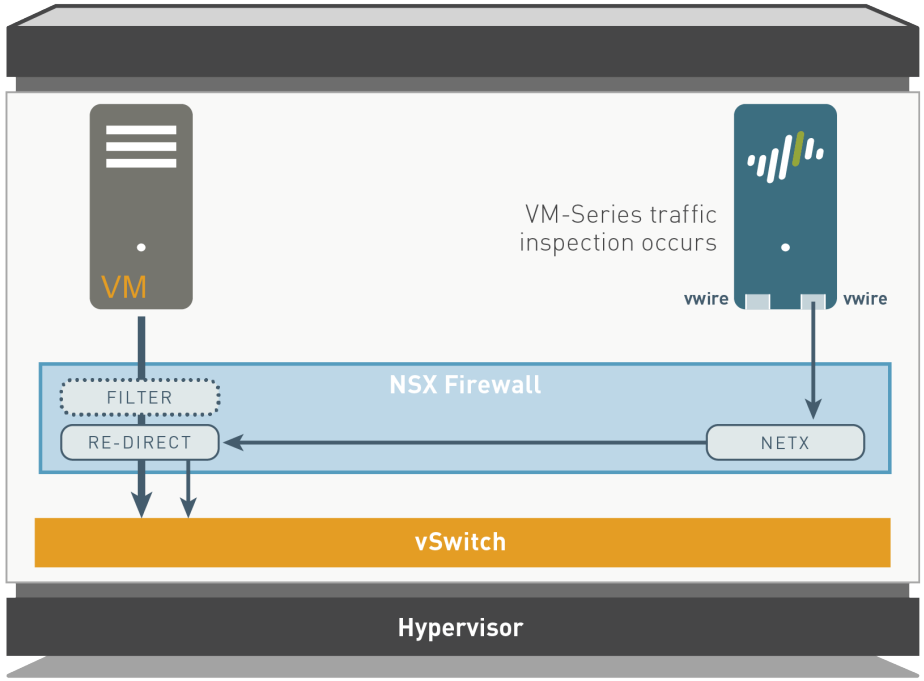
Packet Flow: VM-Series deployed



Packet Flow: traffic redirection rules enabled

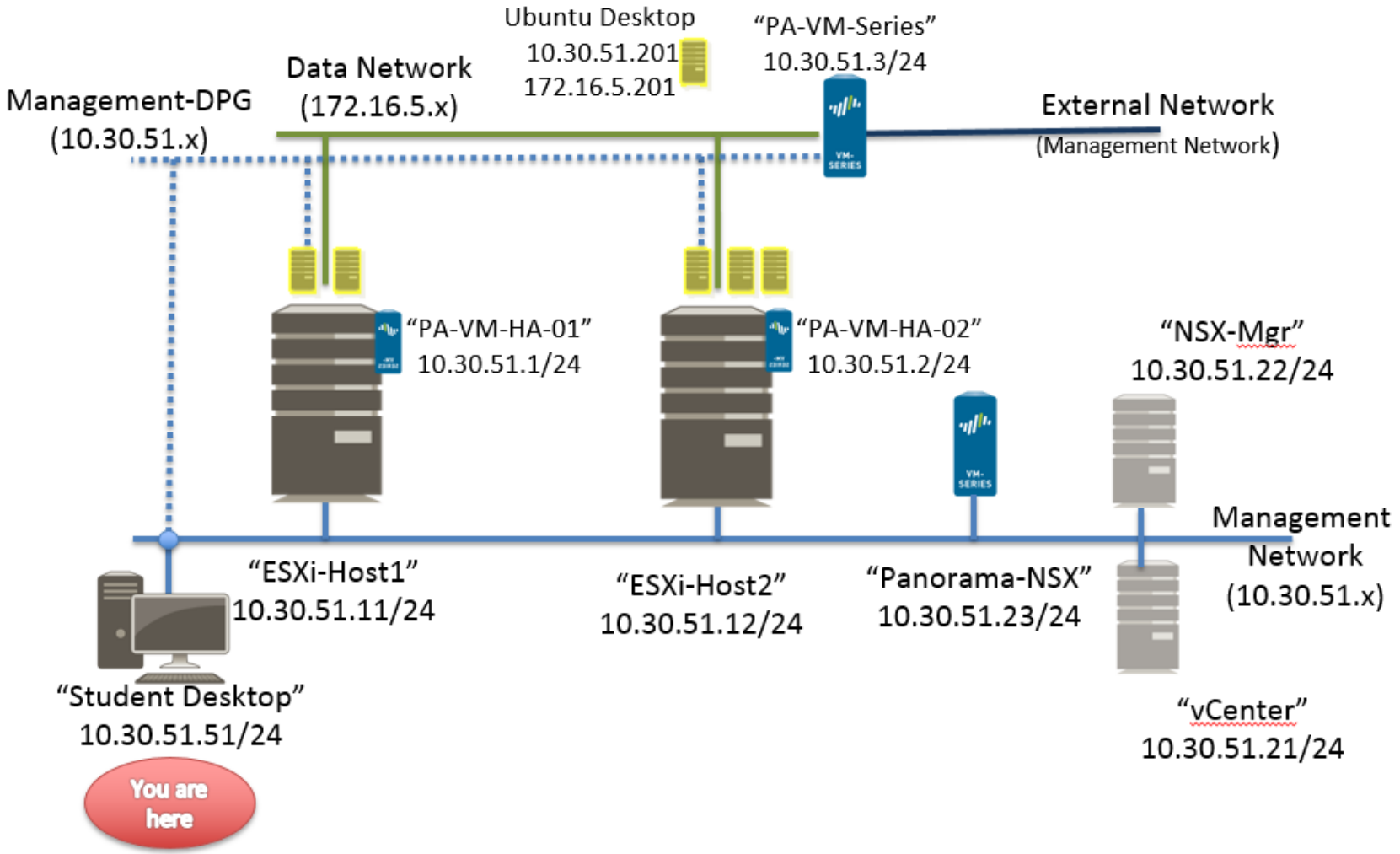


Packet Flow: select traffic inspected



Hands-on Workshop

UTD: VDC Lab Environment



CLASS LOG IN

- **Student Login Link**
  https://use.cloudshare.com/Class/zepi0
- **Student Passphrase**
  DTS IS THE BEST

Activity 0 – Login to UTD Workshop

In this activity student will:

- Login to the Ultimate Test Drive Workshop from their laptop
- Connect to the student desktop and verify the connectivity to other lab devices
- Review the workshop network

Activity 1: VM-Series, Panorama and NSX Intro

- Background
  - The VM-Series firewall extends safe application enablement to virtualized and cloud environments using the same PAN-OS feature set that is available in physical security appliances. The core of the VM-Series is the next-generation firewall, which natively classifies all traffic, inclusive of applications, threats and content, then ties that traffic to the user, regardless of location or device type. Panorama, the centralized management solution, provides you with the ability to manage the Palo Alto Networks virtual and physical firewalls from a centralized location. This means you will be able to view all your firewall traffic; manage all aspects of device configuration; push global policies; and generate reports on traffic patterns or security incidents - all from one central location. This activity introduces the integration between VM-Series firewall, Panorama, VMware vCenter and the NSX solution.

- In this activity student will:
  - Review the Panorama centralized management solution
  - Learn about context switching in Panorama
  - Login and review the configuration needed for NSX integration on:
  - Panorama
  - vCenter and NSX Manager
  - Review VXLAN configuration and Distributed Firewall on NSX Manager

Activity 2: Enable application with VM-Series NGFW

- Background
  - Many organizations use virtual local area networks (VLANs) to segment their network. Though VLANs do isolate network traffic within the layer-2 domain, they cannot enforce the control of privileged information. Specifically, VLANs cannot control applications within the same VLAN. True network segmentation - which happens at the application layer - requires a firewall that understands your applications, users, and content without being limited by the network topology.

- In this activity student will:
  - Modify firewall policy to enable an application using App-ID
  - Commit the firewall policy to device group through Panorama

Activity 3: Dynamic Address Groups and vCenter

- Background
  - In a data center, virtual machines are added, moved or deleted in a matter of minutes creating an ever-changing environment that is very difficult for security administrators to manage and maintain without an automated security workflow. Through the integration with NSX Manager, Dynamic Address Groups (DAG) provides the ability to tie security policies to a virtual machine's changes and movement instantaneously. DAG enables the VM-Series firewall to automatically keep track of the IP addresses assigned to your guest VMs. .

- In this activity student will:
  - Create DAG on Panorama and linking it to a Security Group in vCenter
  - Create a dynamic NSX Security Group using Security Tags in vCenter

Activity 4: Application visibility with VM-Series

- Background
  - Visibility is an important step in controlling network traffic and applications in the data center. In order to take a proactive approach to managing accessibility and risk in the data center, network and security administrators must have full visibility into the application mix on the physical and virtual networks. With the integration between NSX Security Policies, Palo Alto Networks VM-Series firewall can provide full visibility at the hypervisor layer, providing complete application visibility and control between guest VMs on the same or different hosts.

- In this activity student will:
  - Setup security policy to redirect the traffic between guest VMs to the VM-Series firewall
  - Use VM-Series firewall policy to enable applications and utilize Application Command Center (ACC) to monitor applications between guest VMs

Activity 5: Safely enable applications

- Background
  - Network-based threat protection has evolved to include many disciplines from the prevention of vulnerability exploits (IPS) to a wide range of malware protection, botnet detection and protection. We will demonstrate the core threat prevention capabilities of the Palo Alto Networks platform and how it can be used to protect guest VMs.

- In this activity student will:
  - Enable Antivirus, Vulnerability Protection and Anti-Spyware to protect application between guest VMs
  - Review the threat logs on Panorama

Activity 6: VM-Series for Non-NSX Environment

- Background
  - Multi-tenancy on the VM-Series firewall enables you to secure more than one tenant or more than one sub-tenant. A tenant is a customer or an organization such as Palo Alto Networks. A sub-tenant is a department or business unit within the organization such as Marketing, Accounting, or Human Resources. To allow you to secure multiple tenants, Panorama provides the flexibility to create multiple sets of security policy rules for each tenant, and multiple zones to isolate traffic from each sub-tenant and redirect traffic to the appropriately configured VM-Series firewall. You can also deploy more than one instance of the VM-Series firewall on each host within an ESXi cluster..

- In this activity student will:
  - Review the configuration of the second tenant in Panorama and vCenter
  - Create a new steering rule under the NSX Partner Security Services
  - Review overlapping IP addresses in Dynamic Address Groups and on individual VMs
  - Review tenant configuration from firewall CLI

Activity 7: VM-Series for Non-NSX Environment

- Background
  - While Palo Alto Networks VM-Series (VM-1000-HV) seamlessly integrates with VMware NSX solution, the VM-Series can also reside on the ESXi or other supported hypervisor as guest VM to provide another flexible deployment options. By placing VM-Series in the path of the traffic using standard virtualized networking tools, the VM-Series can easily integrates with the existing virtual networks and provides application security and threat protection needed for the virtualized environments.

- In this activity student will:
  - Identify VM-Series Interfaces that are disconnected and re-connect interfaces to the virtual networks
  - Review traffic logs on Panorama to confirm traffic is passing through the firewall

Activity 8: Modern Malware Protection

- Background:
  - For the past decade adversaries have been dramatically evolving, blending multiple advanced attack techniques to evade traditional security solutions. WildFire automatically prevents and detects targeted and unknown malware through direct observation in a virtual environment. If malware is present, protection is created and delivered to you and to all other WildFire users within 15 minutes. WildFire is an integral piece of the Palo Alto Networks enterprise security, platform which delivers full visibility and control of all traffic including tunneled, evasive, encrypted and even unknown traffic. In this activity, we will review policy considerations include which include applications and file types to apply the WildFire file blocking/upload profile.

- In this lab you will:
  - Modify existing file blocking policy to enable the Wildfire service
  - Review built-in WildFire Activity Report

Activity 9: ACC and Custom Report

- Background
  - Informative visualization tools and reports are very important to network and security administrators to monitor and identify potential network problems and attacks. Comprehensive built-in visualization tools and reporting features in the firewall can provide visibility into network activity, which in turn can help you make more informed security decisions.

- In this lab you will:
  - Use Application Command Center (ACC) in Panorama
    - Built-in visualization tools that provides a clear view on the applications, users and threats data on your network
  - Manage custom reports
    - Create a custom report using traffic stats logs

Activity 10 – Feedback on Ultimate Test Drive

- Please complete the survey and let us know what you think about this event.


paloalto
NETWORKS®