Security Advantages of SDN

Dr. Edward G. Amoroso

Centralized SDN Control and Virtual Forwarding
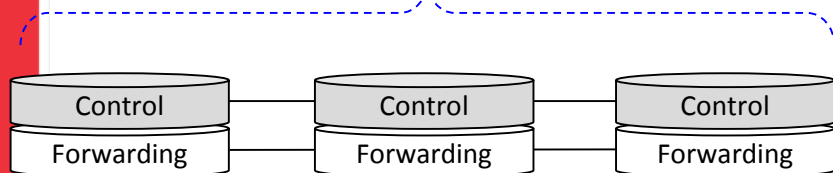
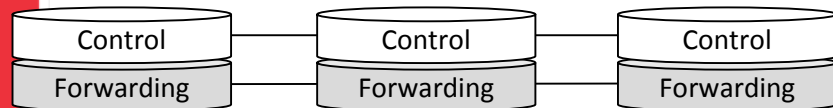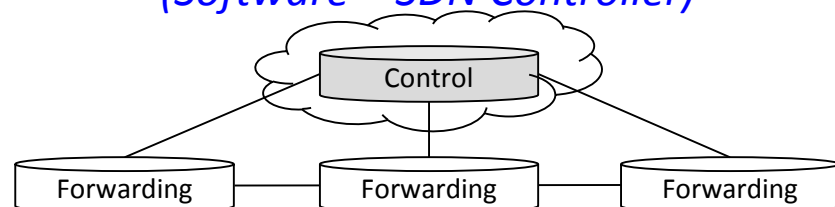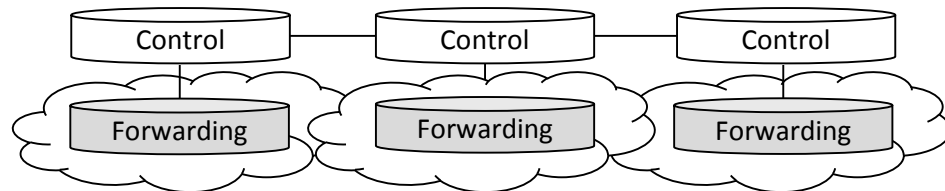**Traditional**

SDN

Decentralized Control (Hardware/Software)

Centralized Control (Software – SDN Controller)

Control	Control	Control
Forwarding	Forwarding	Forwarding

Control

Forwarding	Forwarding	Forwarding

Control	Control	Control
Forwarding	Forwarding	Forwarding

Control	Control	Control
Forwarding	Forwarding	Forwarding

Fast Hardware Forwarding

Virtualized Network Functions

Traditional

NFV

RSAConference2016

Centralized SDN Security Control
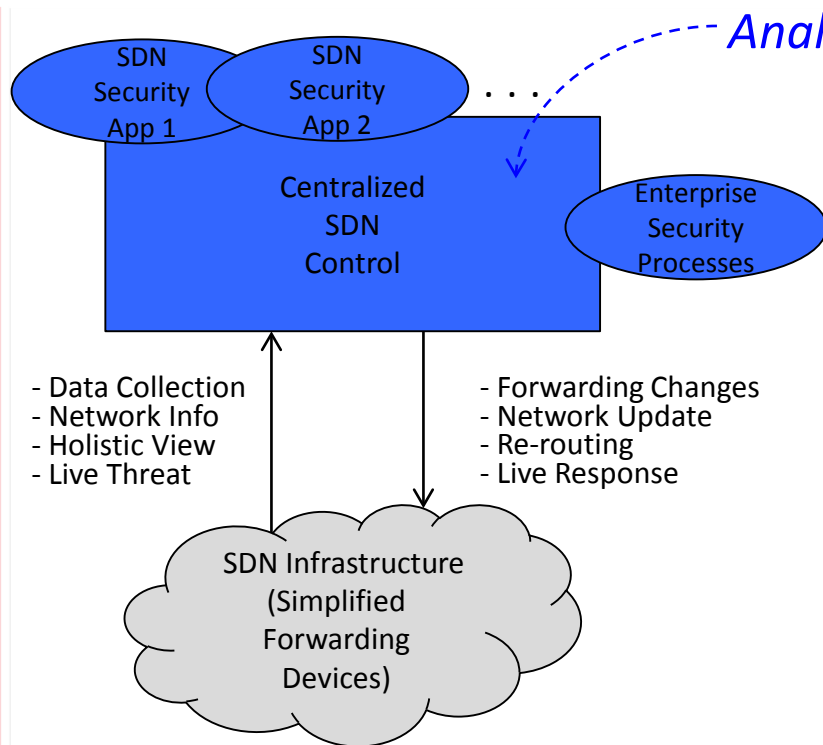
Analogous to Traditional Mainframe Security

SDN Security App 1

SDN Security App 2

. . .

Centralized SDN Control

Enterprise Security Processes

- Data Collection
- Network Info
- Holistic View
- Live Threat

- Forwarding Changes
- Network Update
- Re-routing
- Live Response

SDN Infrastructure (Simplified Forwarding Devices)

SDN Control: Centralized control allows for improved security vantage point
Management: Security management improves with full network visibility
Applications: SDN applications provide native security control functions
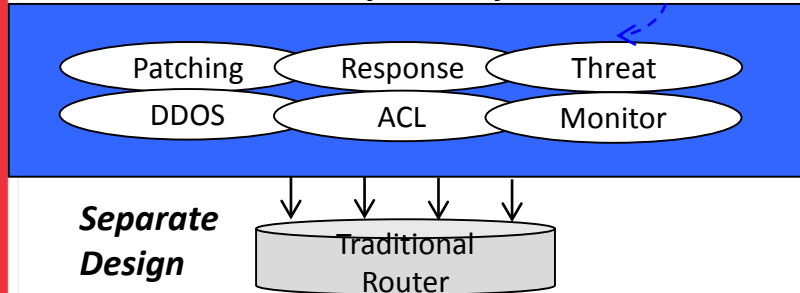*Data Collection*: Native collection and analytics offer enhanced response
Efficiency: SDN enables more immediate re-routing and infrastructure changes (Dynamic Enforcement)
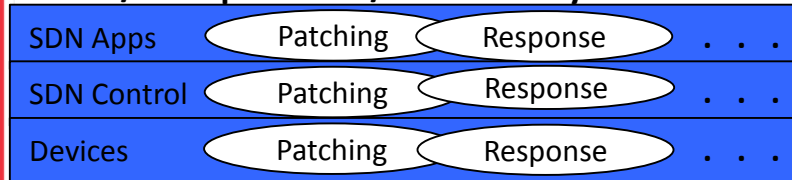
Traditional Security Overlay

Traditional Network Security Done "After the Fact"

Separate Design

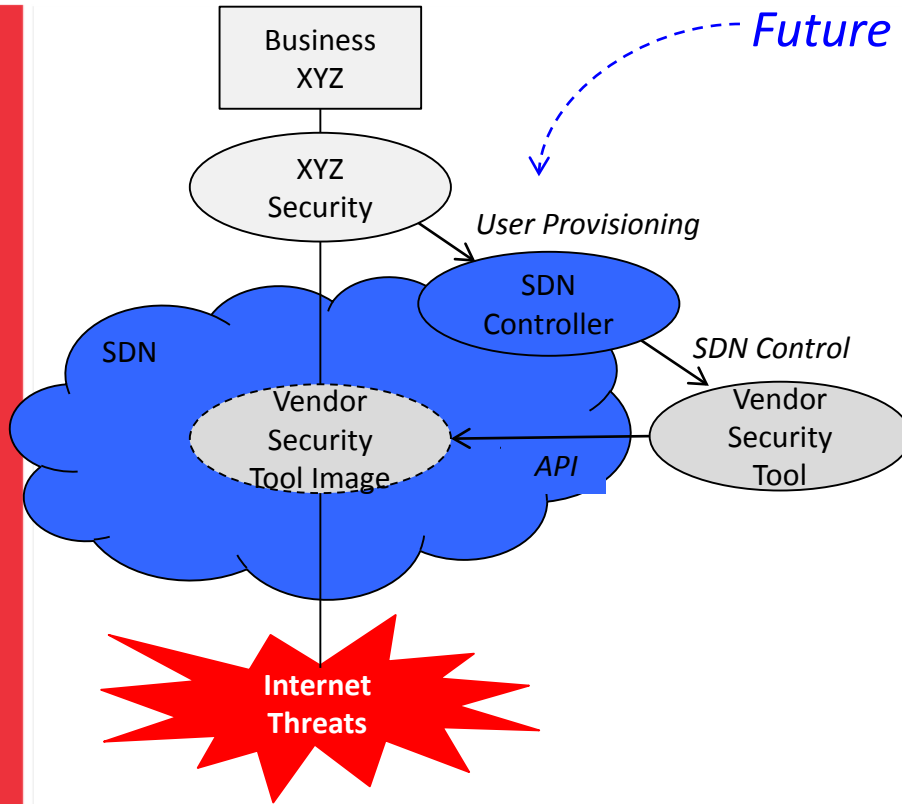**ISP/Enterprise SDN/NFV Security**

Integrated Design

Retrofit: Existing networks have been retrofit with security after-the-fact
Routers: Existing router complexity degrades response and patching
Native: SDN and NFV include native security embedded during design
Integration: Security by design in SDN results in more integrated security
Complexity: Fresh SDN and NFV design provide opportunity for simplification (Security Designed In)

RSAConference2016

Add-On Security Protections

Business XYZ

XYZ Security

User Provisioning

SDN Controller

SDN

SDN Control

Vendor Security Tool Image

Vendor Security Tool

API

Internet Threats

Future of Managed Security Services: On-Demand

Cycle Time: Reduces provisioning from weeks/months to hours/minutes
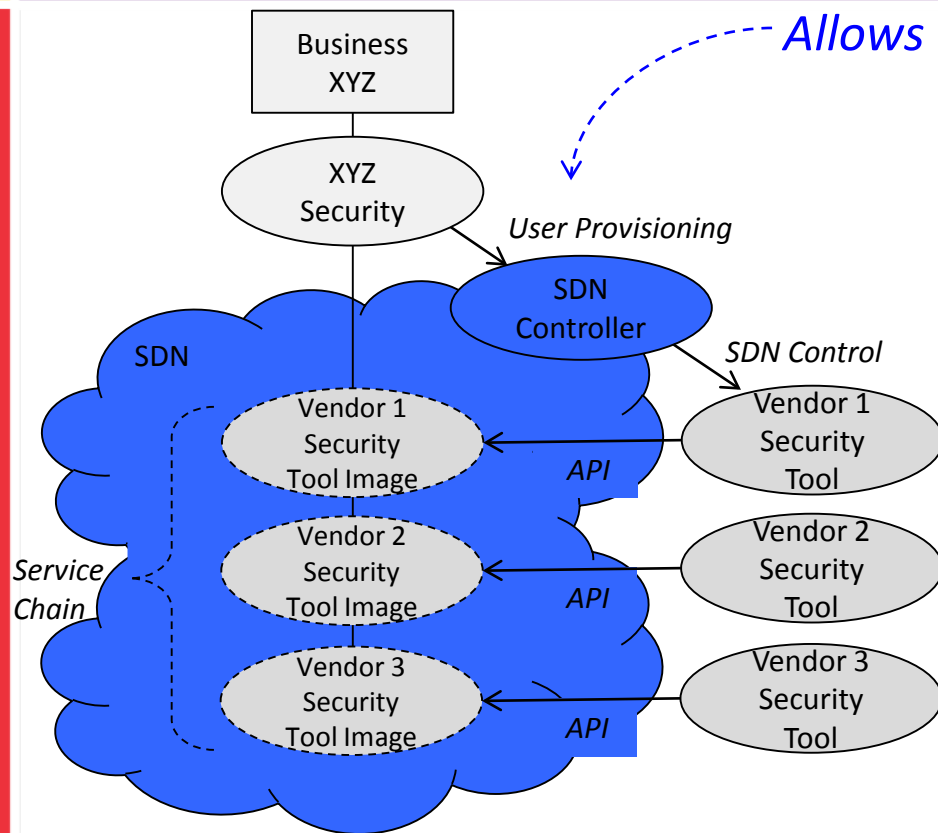*Attack Response*: Improves defensive posture during live cyber attack
Planned Upgrade: Enhances defensive posture in advance of planned need
Economics: Avoids expense of vendor hardware appliance investment
Platform: Establishes underlying SDN base for cyber security product market

Defense in Depth Architecture

Allows Dynamic Security Service Chaining

Business
XYZ

XYZ
Security

User Provisioning

SDN
Controller

SDN Control

SDN

Vendor 1
Security
Tool Image

Vendor 1
Security
Tool

API

Vendor 2
Security
Tool Image

Vendor 2
Security
Tool

API

*Service
Chain*

Vendor 3
Security
Tool Image

Vendor 3
Security
Tool

API

Cycle Time: Reduces provisioning from weeks/months to hours/minutes
Attack Response: Provides multiple layers of cyber defense
Tailoring: Allows design to include strengths of each vendor
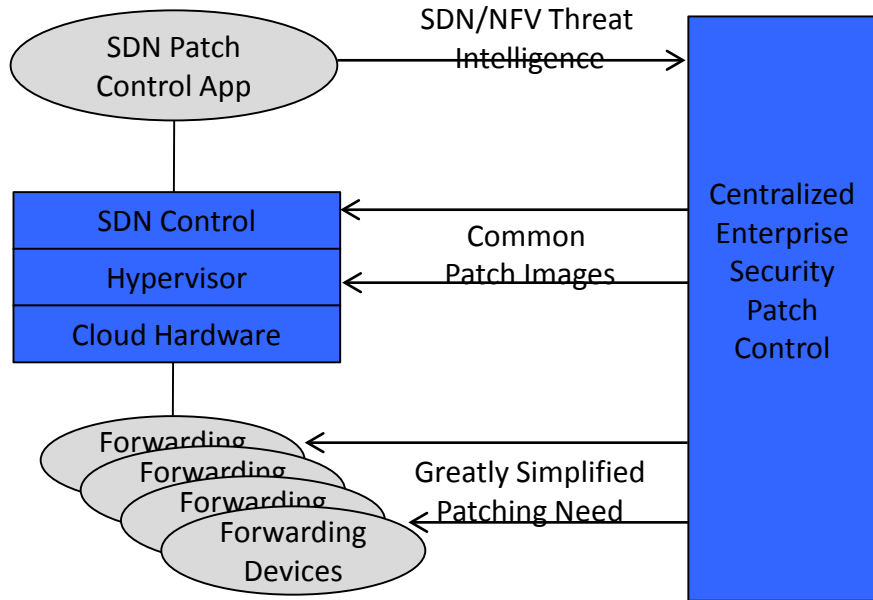*Chaining*: Creates opportunity to create virtual security chains
Platform: Abstracts hardware differences between security vendors

RSAConference2016

Streamlined Security Patching

Allows Install of Common Patched Images

SDN Patch Control App

SDN/NFV Threat Intelligence

SDN Control

Hypervisor

Cloud Hardware

Common Patch Images

Centralized Enterprise Security Patch Control

Forwarding Forwarding Forwarding Forwarding Devices

Greatly Simplified Patching Need

Cycle Time: Reduces patch cycles from weeks/months to hours/minutes

Automation: SDN controllers enable automation based on intelligence

Inventory: SDN/NFV infrastructure offers live inventory for common images

Validation: Patch metrics and posture can be collected in real-time

Simplification: Simplified devices have smaller software patch surface

## Hardware Swapped and Sent Intact to Forensics
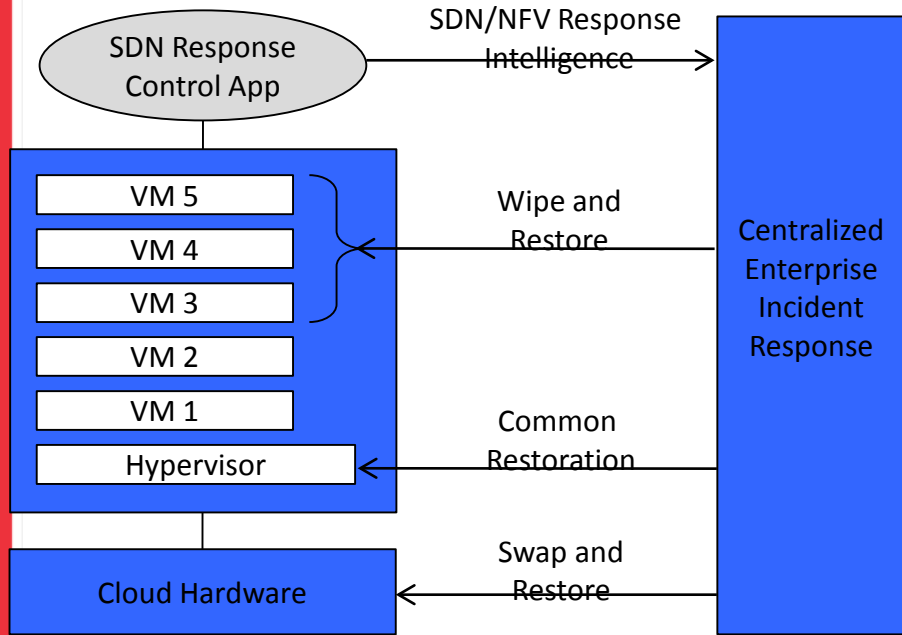
Cycle Time: Reduces response from days/hours to minutes/seconds

Automation: SDN/NFV approach allows response based on intelligence

Inventory: Virtualization enables wipe and restore response for VMs

Forensics: Restoration allows swap and capture for off-line forensics

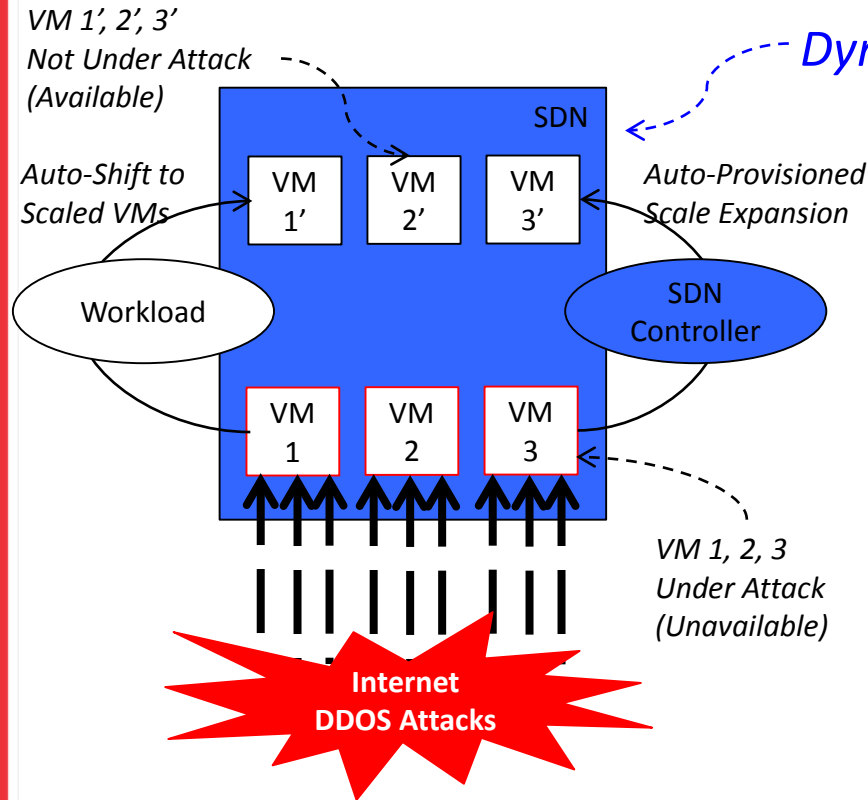*Simplification*: Common hardware enables swap and restore response

Use of Cloud Can Exceed Existing Perimeter Security
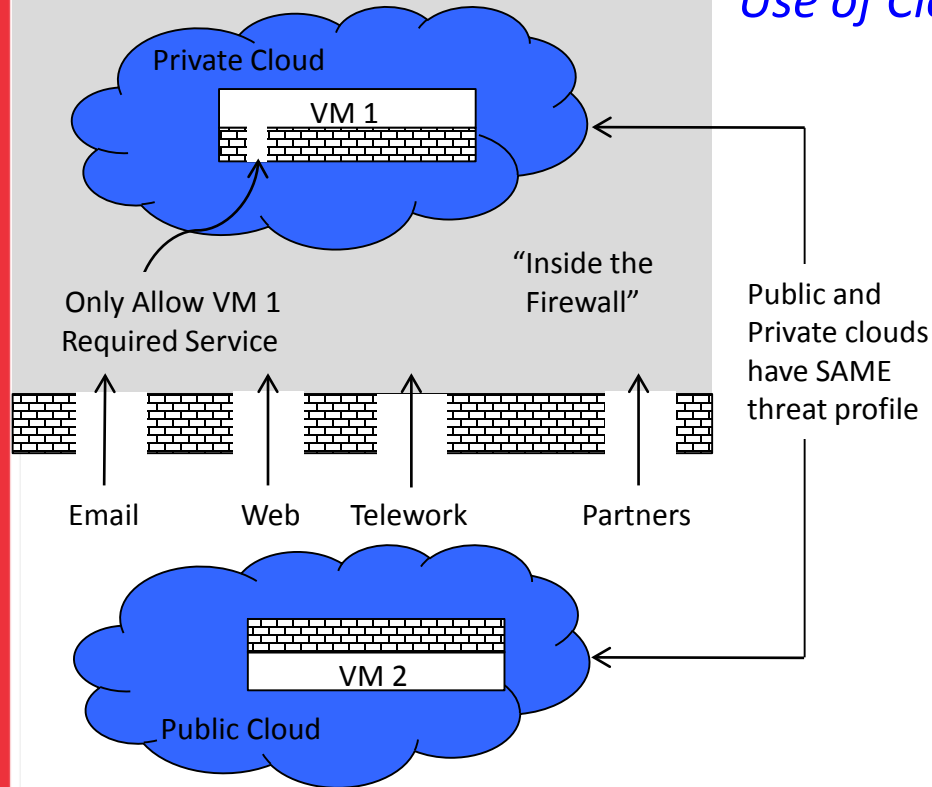
Current Perimeter: Enterprise perimeter weaknesses require immediate action

Micro-Perimeter: Virtualization enables embedded cloud micro-perimeters

Independence: Virtualized security works In both private and public clouds

APT Attacks: Virtual micro-perimeters in the cloud are resilient against APT

Equivalence: With virtual security, public and private clouds are <u>threat equivalent</u>

DDOS Resilience

VM 1', 2', 3'
Not Under Attack
(Available)

Auto-Shift to
Scaled VMs

SDN

VM 1'   VM 2'   VM 3'

Auto-Provisioned
Scale Expansion

Workload

SDN Controller

VM 1   VM 2   VM 3

VM 1, 2, 3
Under Attack
(Unavailable)

Internet
DDOS Attacks

Dynamic Rule and Route Modification

DDOS Threat: Many enterprise networks remain vulnerable to Layer 3/7 DDOS
Layer 3: DDOS defenses rely on more powerful defense than offense (Gbps)
Layer 7: Application-level DDOs attacks likely to increase (per Layer 3 defenses)
Expansion: Virtualization allows for dynamic, expansion under attack
Consequence: Approach is similar to CDN expansion to reduce attack consequence

RSAConference2016

- Application for virtual data center design
- Source selection in ISP/MSP services
- Design base for virtualizing micro-segments
- New platform for MSSP operations
- Modified set of compliance issues for security