RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: TECH-T10

Security Advantages of Software-Defined Networking

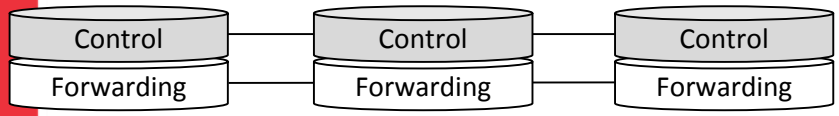
Dr. Edward G. Amoroso
Senior Vice President &
Chief Security Officer
AT&T

#RSAC

Centralized SDN Control and Virtual Forwarding

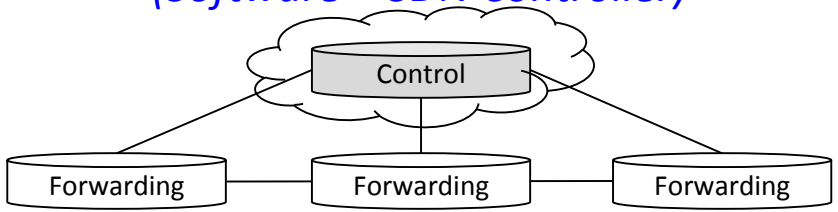
Traditional

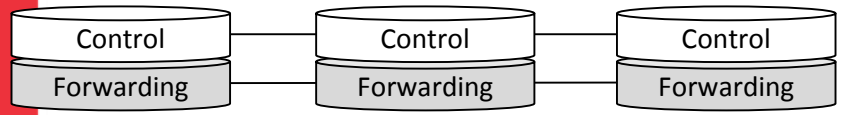
Decentralized Control (Hardware/Software)



SDN

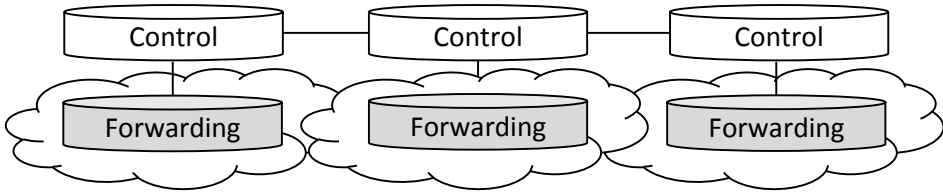
Centralized Control (Software – SDN Controller)





Fast Hardware Forwarding

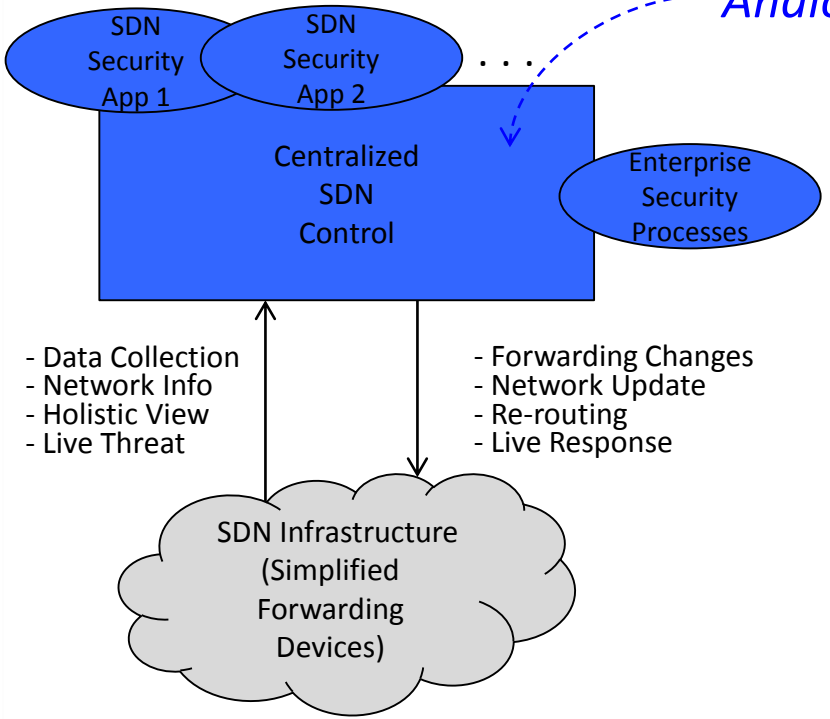
Traditional



Virtualized Network Functions

NFV

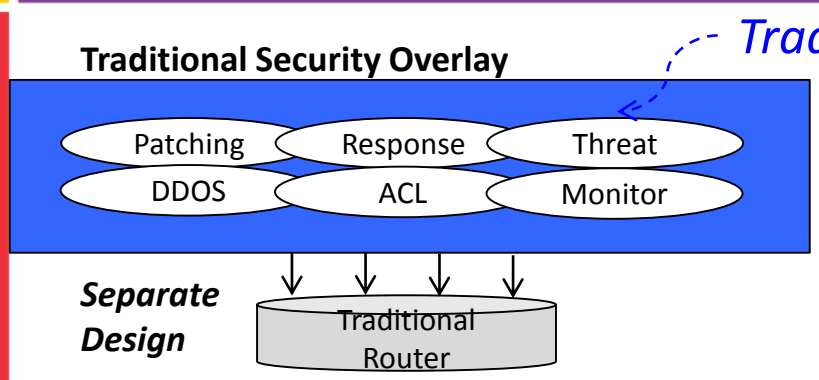
Centralized SDN Security Control



Analogous to Traditional Mainframe Security

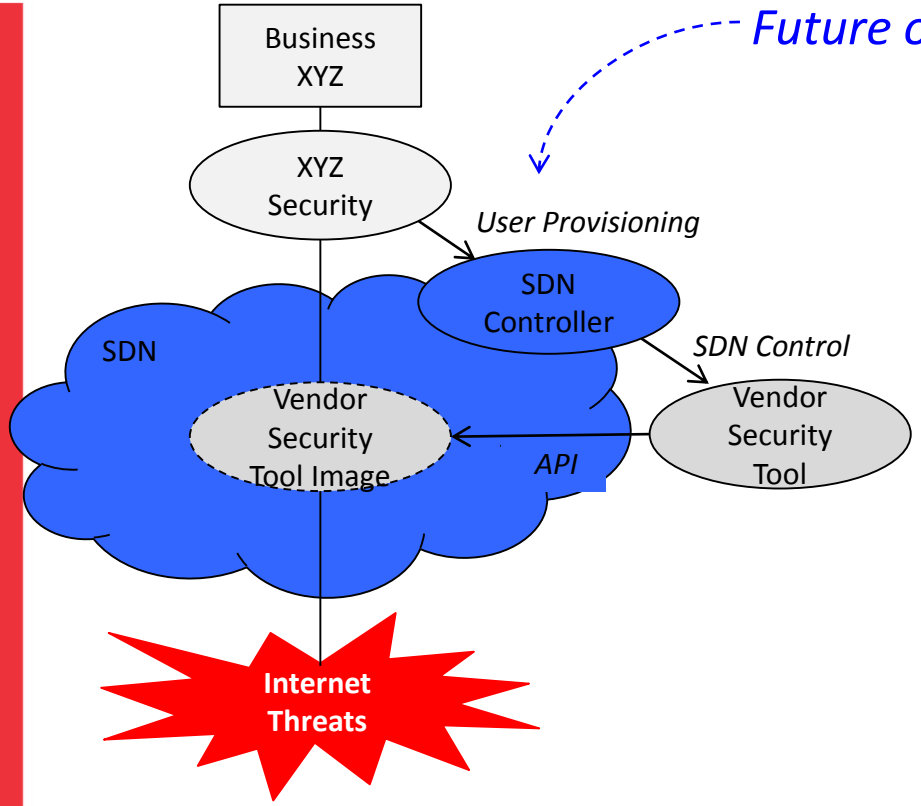
SDN Control: Centralized control allows for improved security vantage point
Management: Security management improves with full network visibility
Applications: SDN applications provide native security control functions
Data Collection: Native collection and analytics offer enhanced response
Efficiency: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

Security by 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)

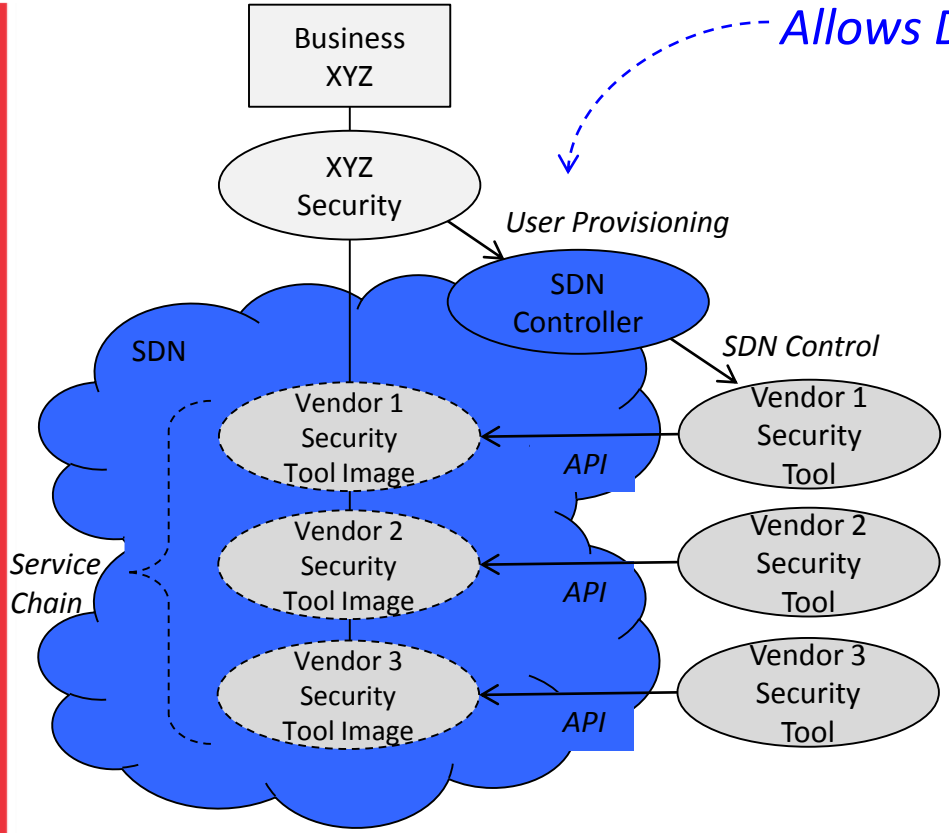
Add-On Security Protections



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

Cycle Time: Reduces provisioning from weeks/months to hours/minutes

Attack Response: Provides multiple layers of cyber defense

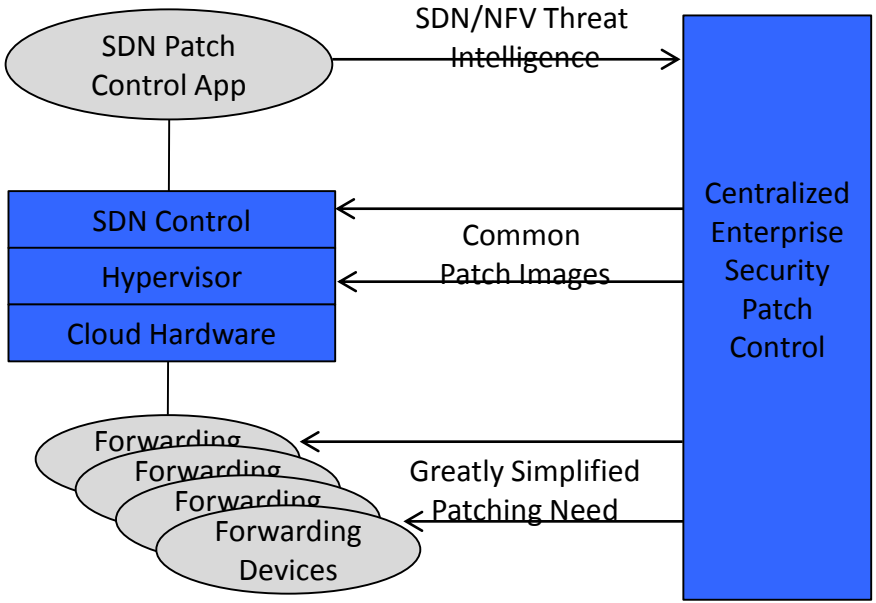
Tailoring: Allows design to include strengths of each vendor

Chaining: Creates opportunity to create virtual security chains

Platform: Abstracts hardware differences between security vendors

Streamlined Security Patching

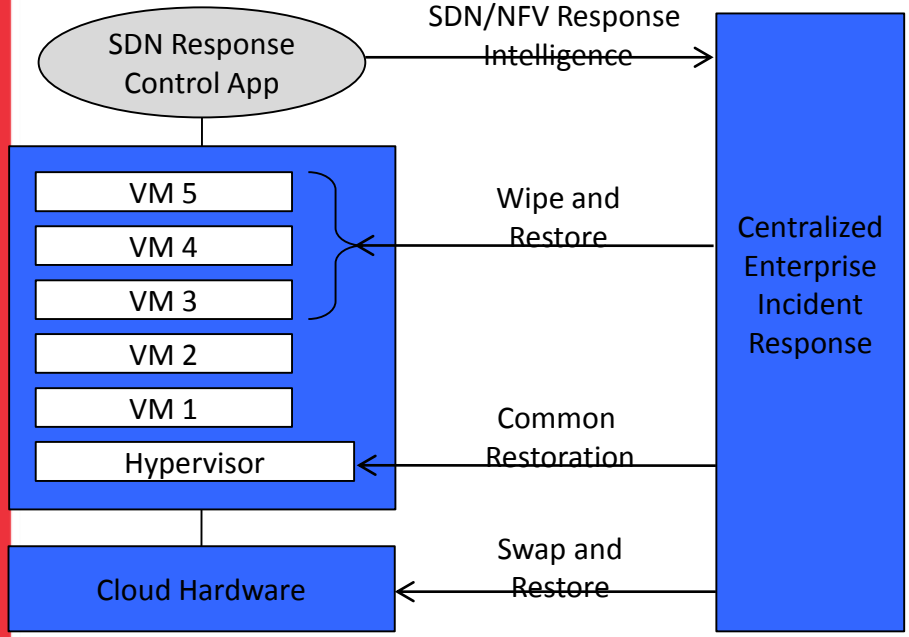
Allows Install of Common Patched Images



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

Improved Incident Response

Hardware Swapped and Sent Intact to Forensics



Cycle Time: Reduces response from days/hours to minutes/seconds

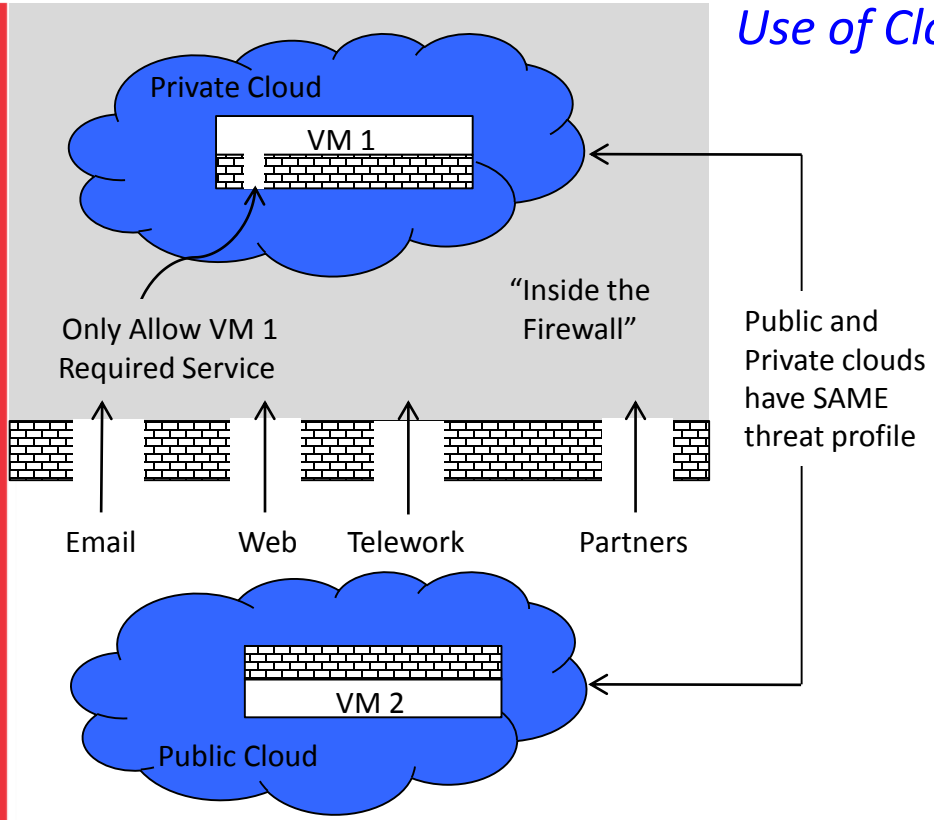
Automation: SDN/NFV approach allows response based on intelligence

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

Perimeter Independence



Use of Cloud Can Exceed Existing Perimeter Security

Current Perimeter: Enterprise perimeter weaknesses require immediate action

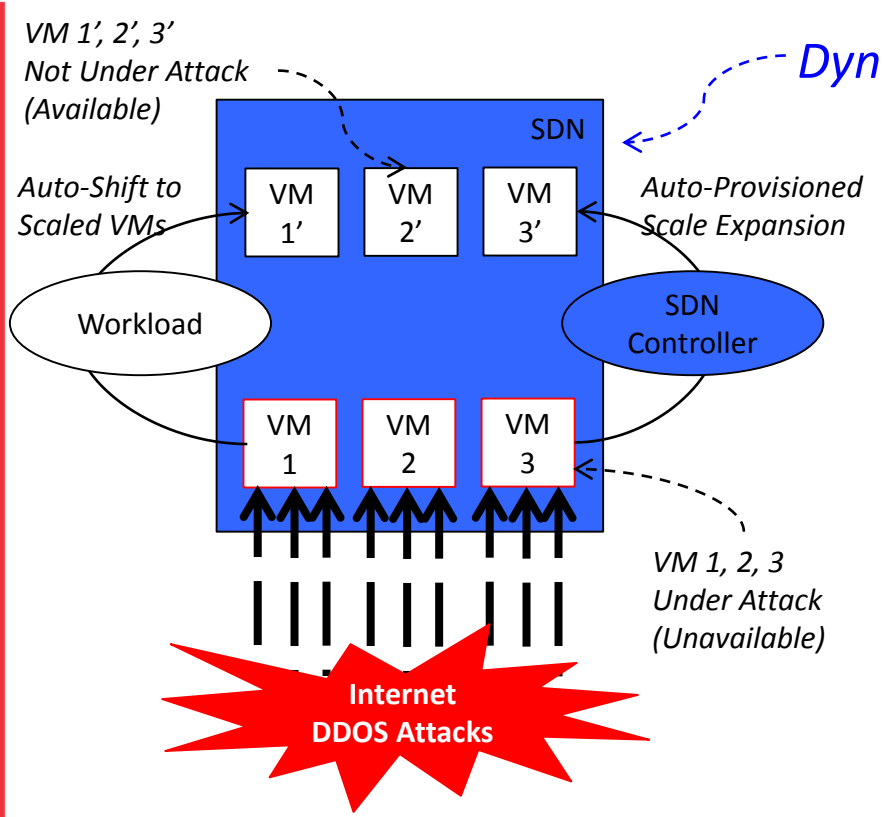
Micro-Perimeter: Virtualization enables embedded cloud micro-perimeters

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 threat equivalent

DDOS Resilience



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

Implications for Attendees

- 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