RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: ANF-T08

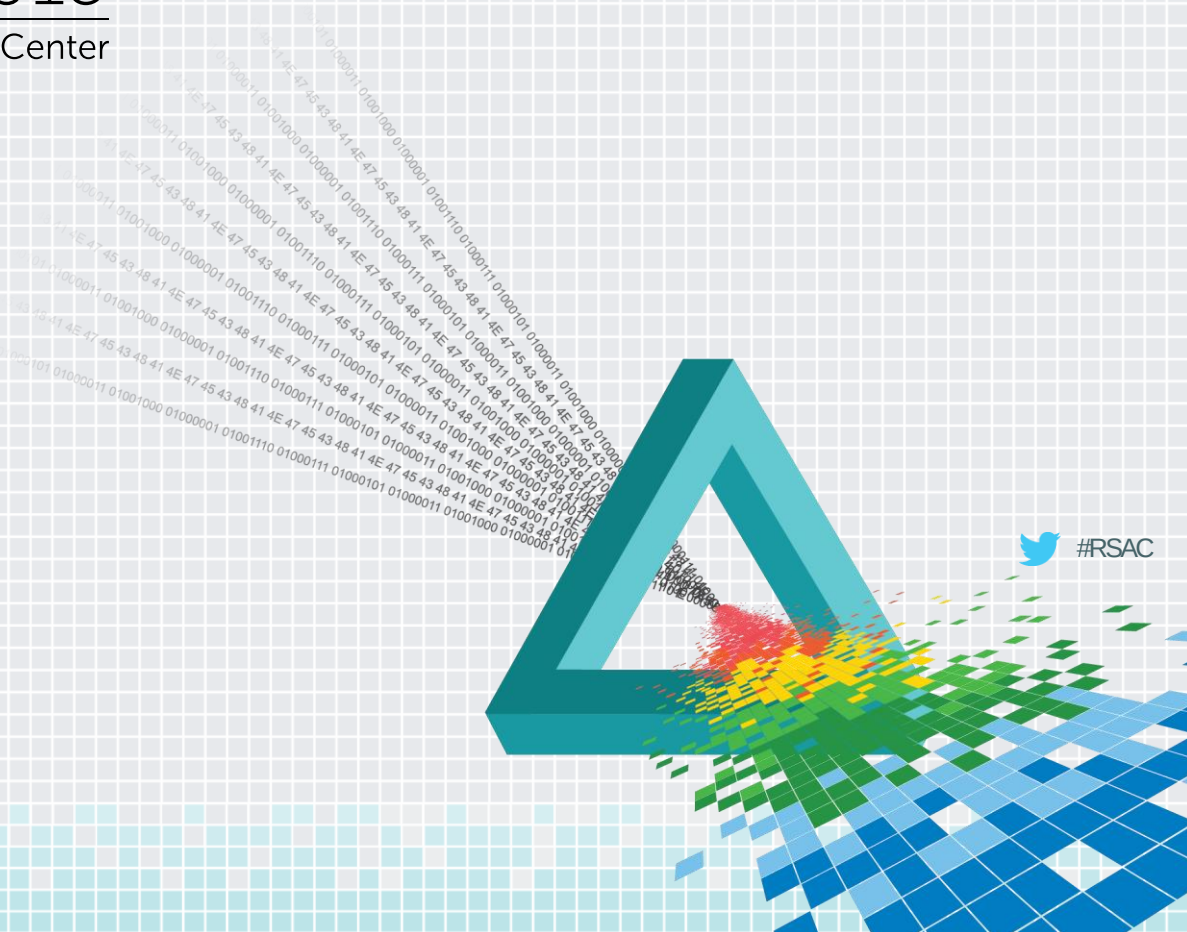
Orchestrating Software Defined Networks (SDN) to Disrupt the APT Kill Chain

Sean Doherty
VP Technology Partnerships and Alliances
Symantec
@SeandDInfo

Deb Banerjee
Chief Architect, Data Center Security Products
Symantec

RSAConference2015

San Francisco | April 20-24 | Moscone Center



A Quick Level Set

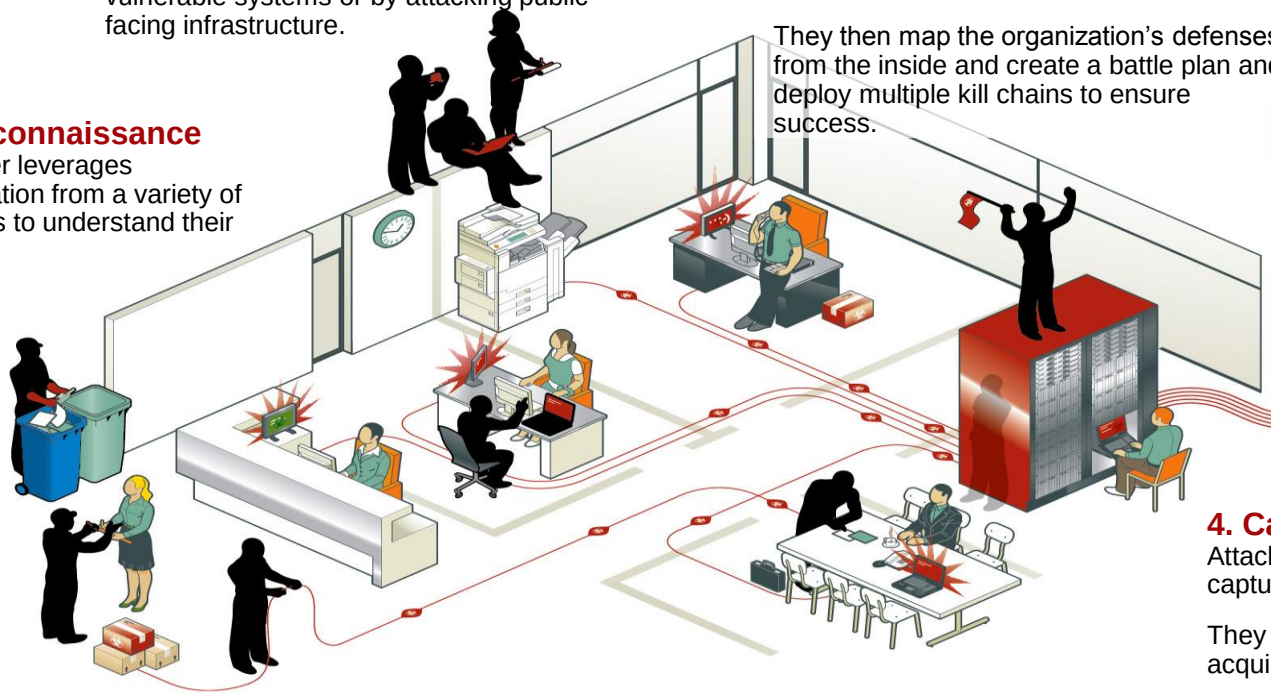
The Phases of an APT Attack

1. Reconnaissance
Attacker leverages information from a variety of sources to understand their target.

2. Incursion
Attackers break into network by using social engineering to deliver targeted malware to vulnerable systems or by attacking public facing infrastructure.

3. Discovery
Once in, the attackers stay “low and slow” to avoid detection.

They then map the organization’s defenses from the inside and create a battle plan and deploy multiple kill chains to ensure success.

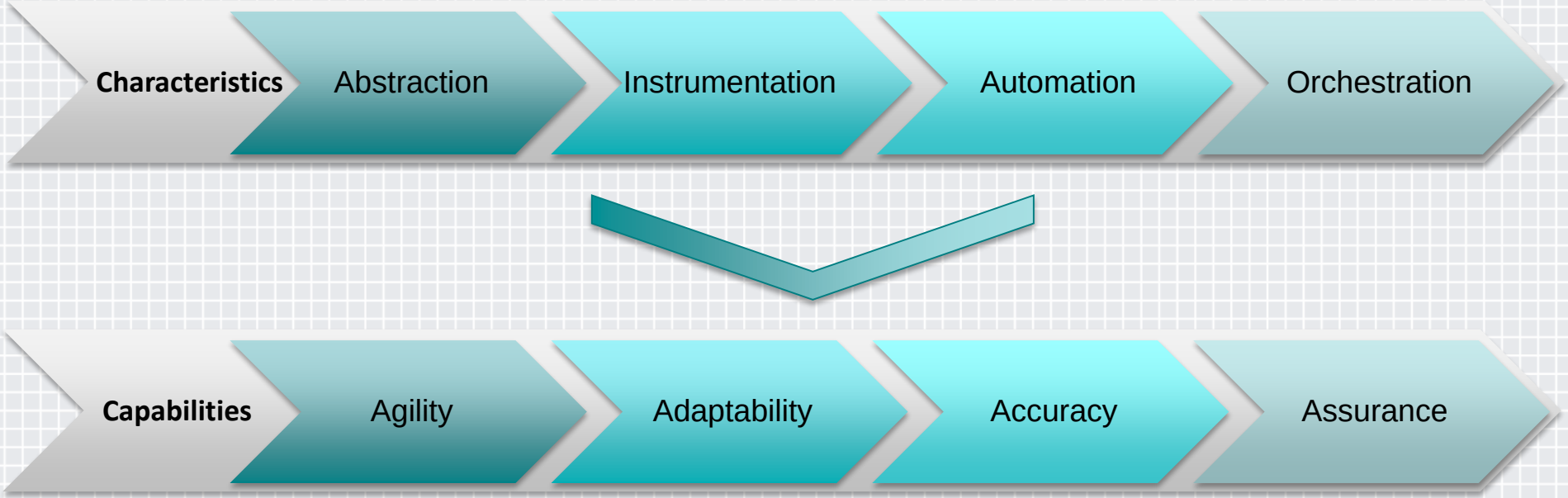


4. Capture
Attackers access unprotected systems and capture information over an extended period.

They may also install malware to secretly acquire data or disrupt operations.

5. Exfiltration
Captured information is sent back to attack team’s home base for analysis and further exploitation.

Characteristics and Capabilities of Software Defined Things



What is SDN – Definitions and Key Concepts

- This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network
- **Agile**: Abstracting control from forwarding lets administrators dynamically adjust network-wide traffic flow to meet changing needs.
- **Programmatically configured**: SDN lets network managers configure, manage, secure, and optimize network resources very quickly via dynamic, automated SDN programs,

Source: https://www.opennetworking.org/sdn-resources/sdn-definition

Data Center Security Controls: Host-Based

Controls
- IDS/IPS
- Anti-Malware
- Detection/Response

Technologies
- Signature
- Behavioral
- Correlation

Challenges
- Operational Complexity
- Impact Analysis
  - "Will updating a host-based security policy cause an outage?"
- False Positives

Shellshock Compensation: (CVE-2014-6271)

Data Center Security Controls: Network-Based

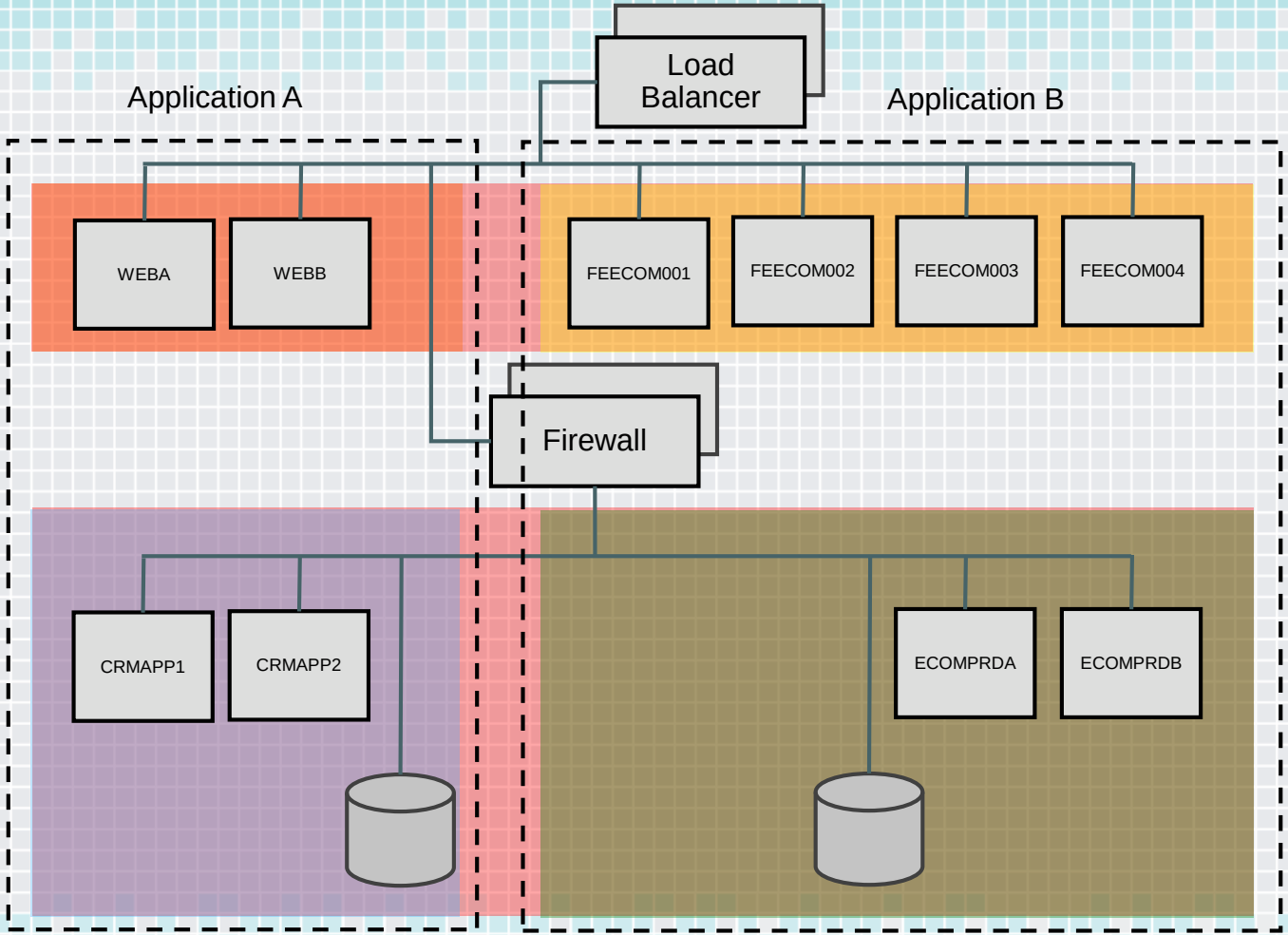
Controls

- Firewalls/VLAN-based Segmentation: Zones, Applications, Tiers,
- Network IDS/IPS
  - Packet Inspection for exploit payloads
- DLP : data egress detection

Challenges

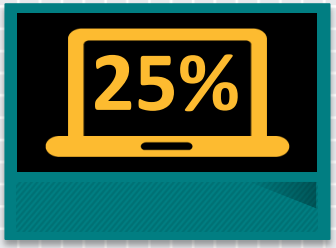
- Operational Complexity
- Resource Consumption
- False Positives
- “Can’t scan all traffic for all exploits”

A ‘Typical’ Data Center Network


Load Balancer
Application A
Application B
WEBA
WEBB
FEECOM001
FEECOM002
FEECOM003
FEECOM004
Firewall
CRMAPP1
CRMAPP2
ECOMPRDA
ECOMPRDB

Attack Scenario

- APT that leverages public facing infrastructure vulnerabilities
- Lots of these to chose from
- Our scenario a classic 3 tier public web facing application in traditional infrastructure

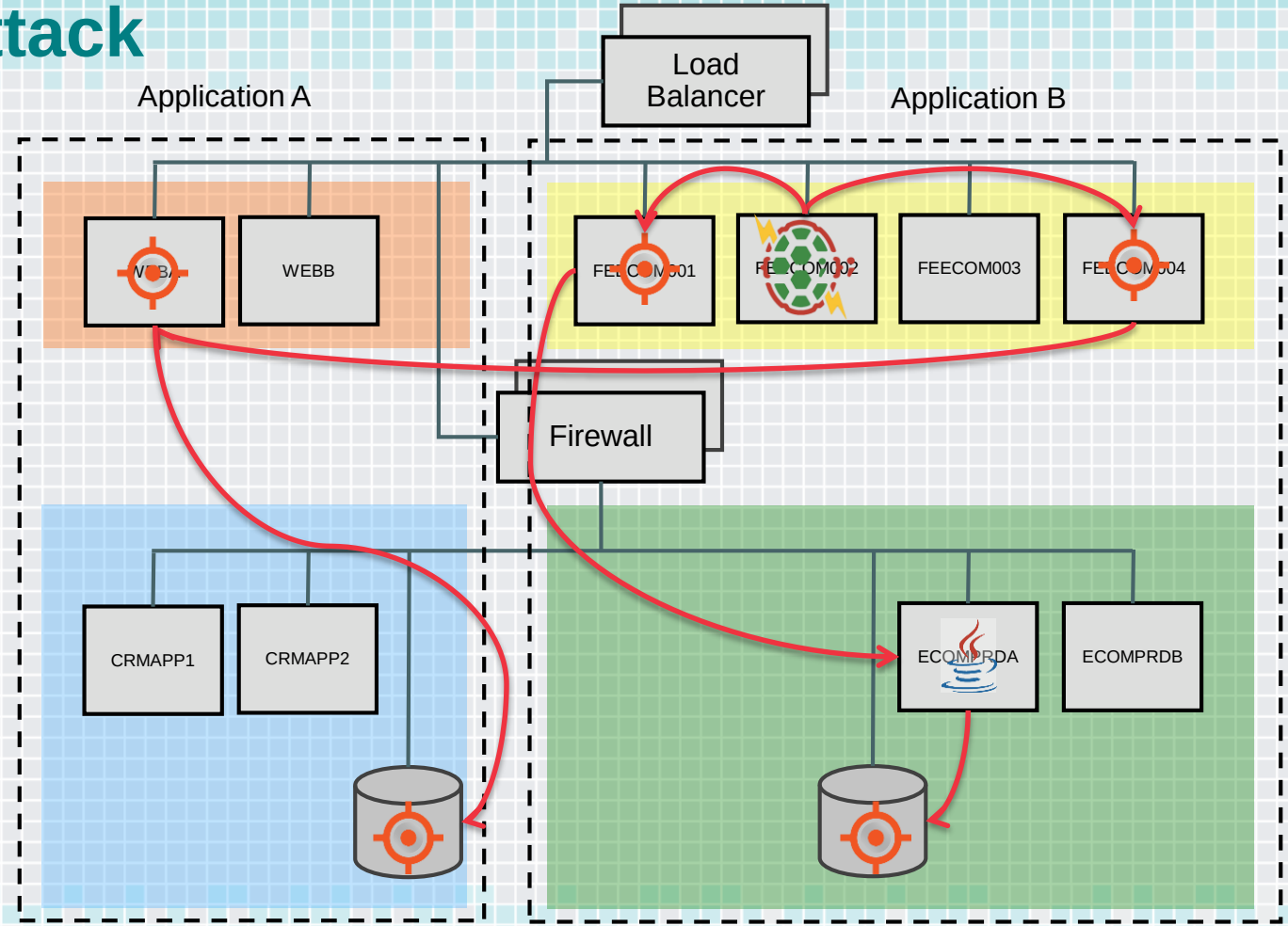


have critical vulnerabilities unpatched

of legitimate websites have unpatched vulnerabilities

Source: Symantec ISTR : Volume 18

The Attack


Load Balancer
Application A
Application B
WEBB
WEBB
FEECOM001
FEECOM002
FEECOM003
FEECOM004
Firewall
CRMAPP1
CRMAPP2
ECOMPRDA
ECOMPRDB

Micro-segmentation

A new model for data center security

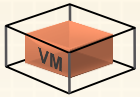
STARTING ASSUMPTIONS

Assume everything is a threat and act accordingly.

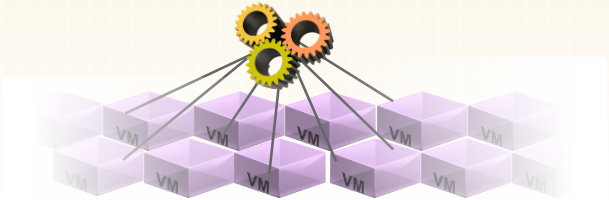
DESIGN PRINCIPLES

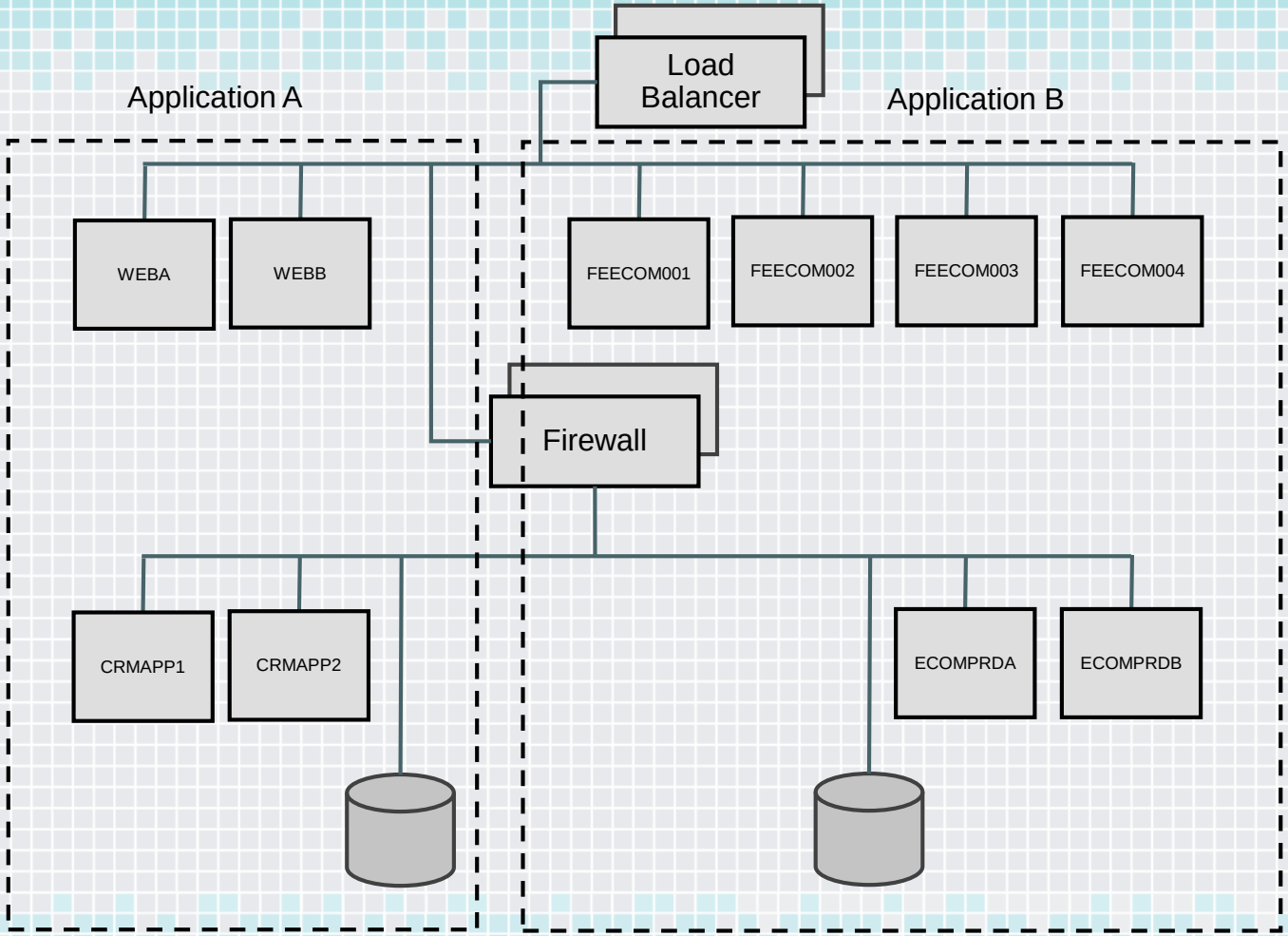
1. Isolation and segmentation

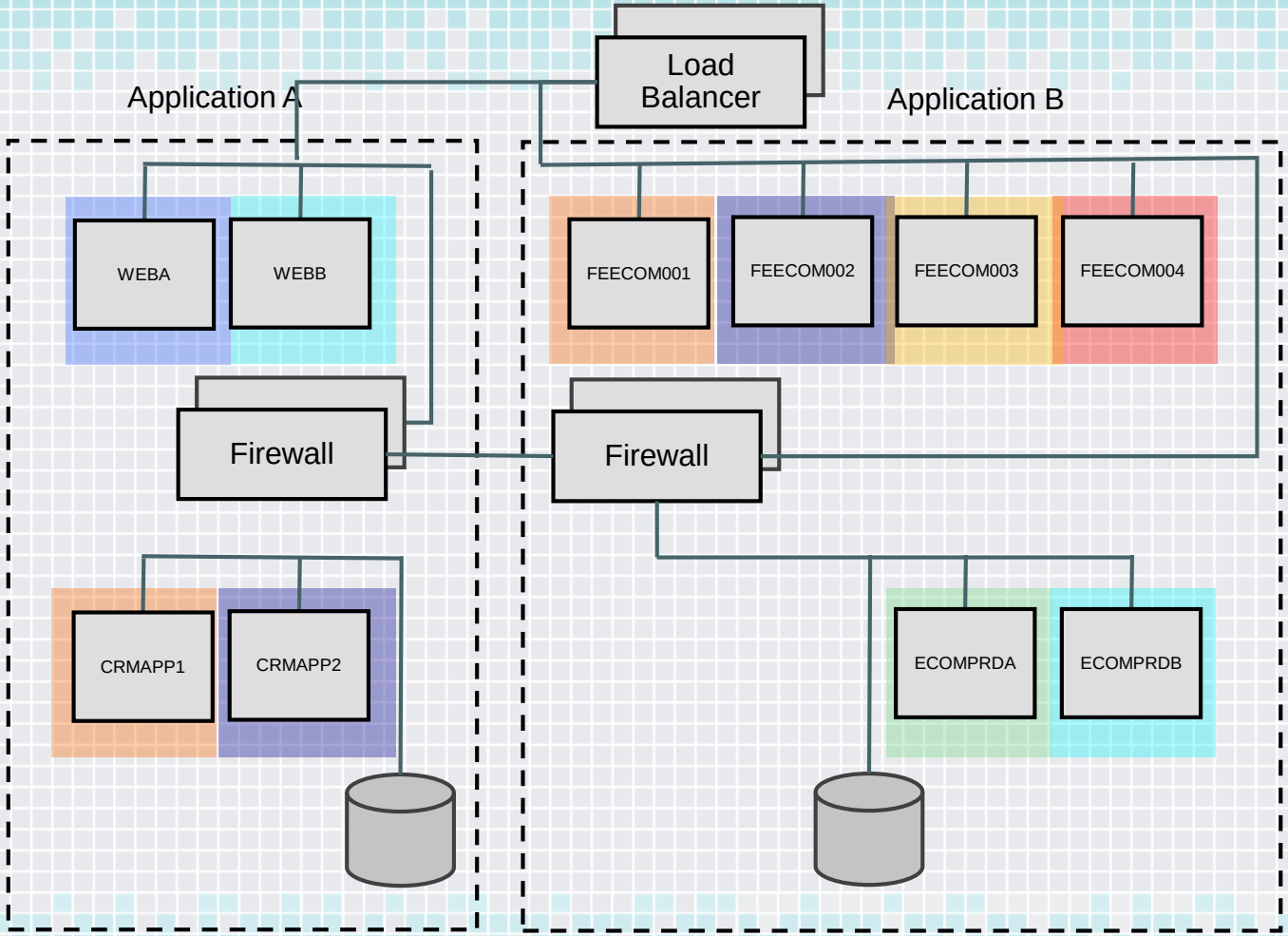
2. Unit-level trust / least privilege



3. Ubiquity and centralized control

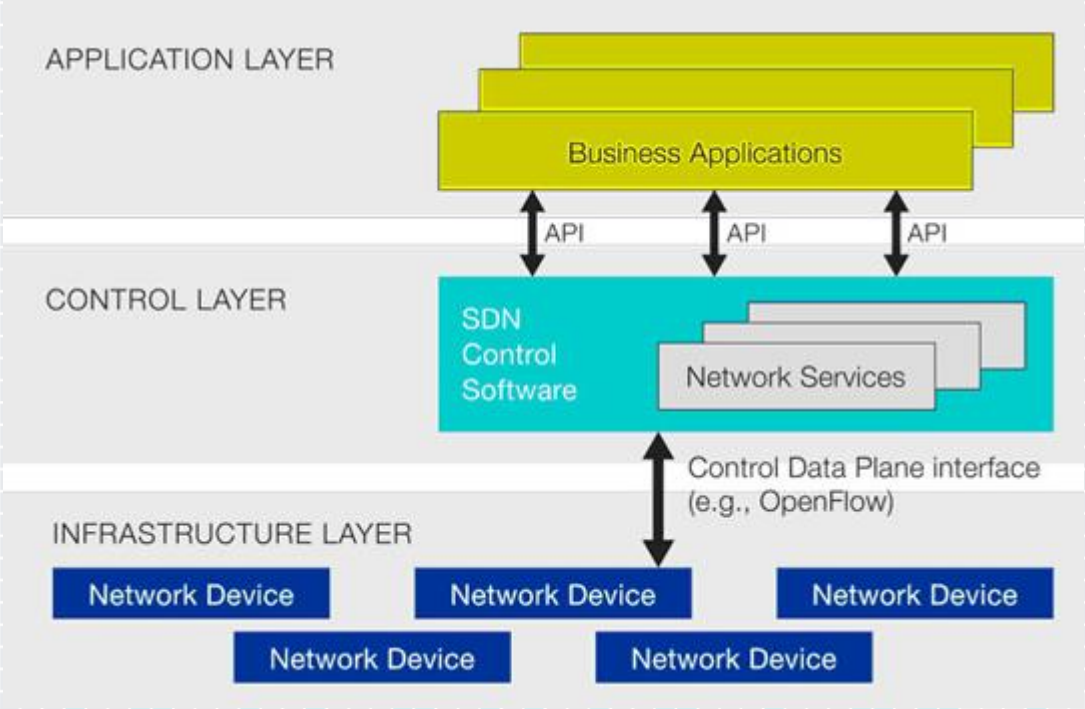



Load Balancer
Application A
Application B
WEBA
WEBB
FEECOM001
FEECOM002
FEECOM003
FEECOM004
Firewall
CRMAPP1
CRMAPP2
ECOMPRDA
ECOMPRDB


Load Balancer
Application A
Application B
WEBA
WEBB
FEECOM001
FEECOM002
FEECOM003
FEECOM004
Firewall
Firewall
CRMAPP1
CRMAPP2
ECOMPRDA
ECOMPRDB

If only everything was as easy as a diagram in PowerPoint

Logical View of SDN Architecture

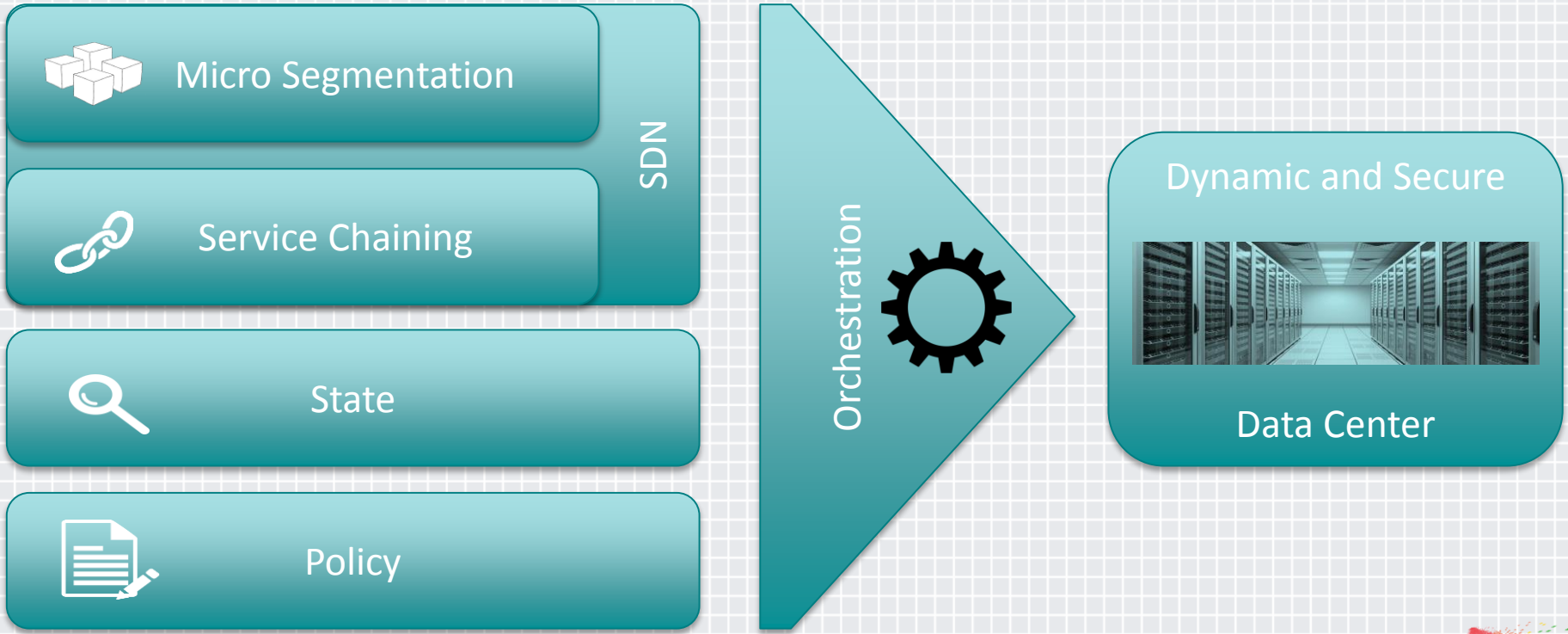


NSX Manager,
APIC Manager

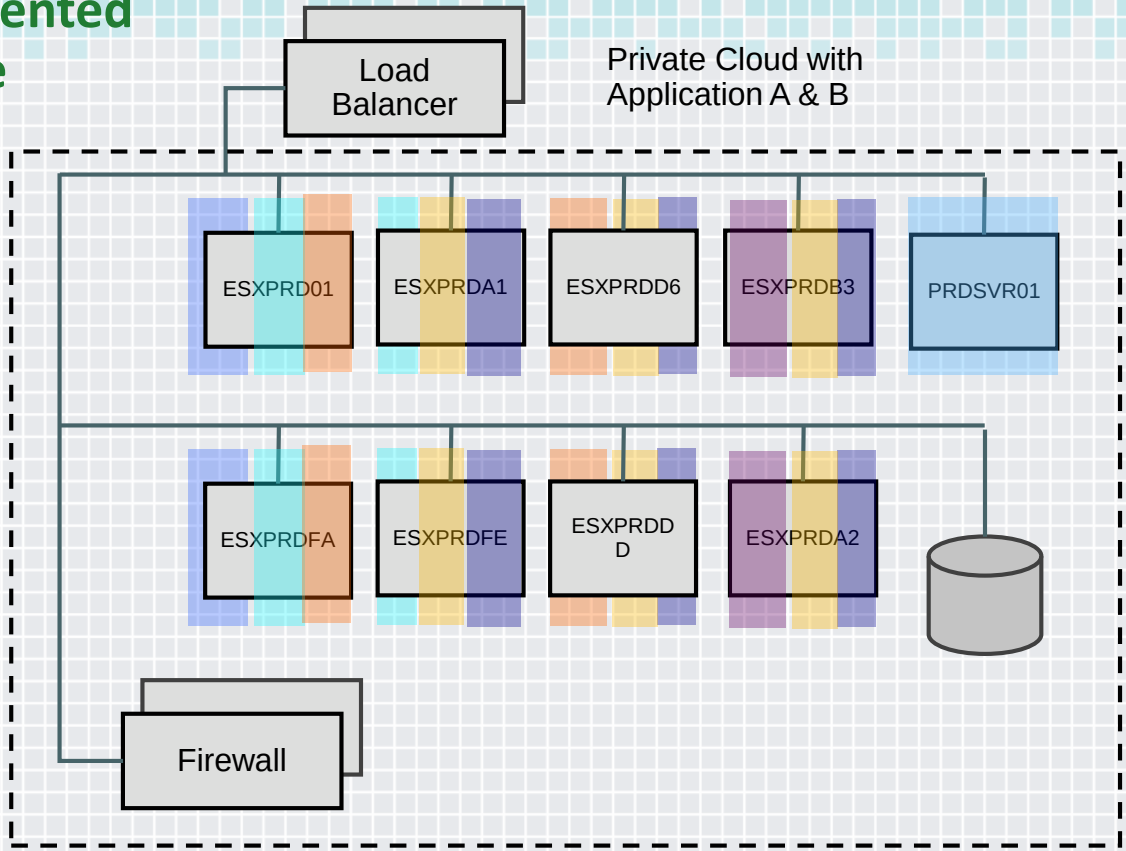
NSX Controller,
Nexus 9000

Firewalls,
Network IDS/IPS,
Network DLP

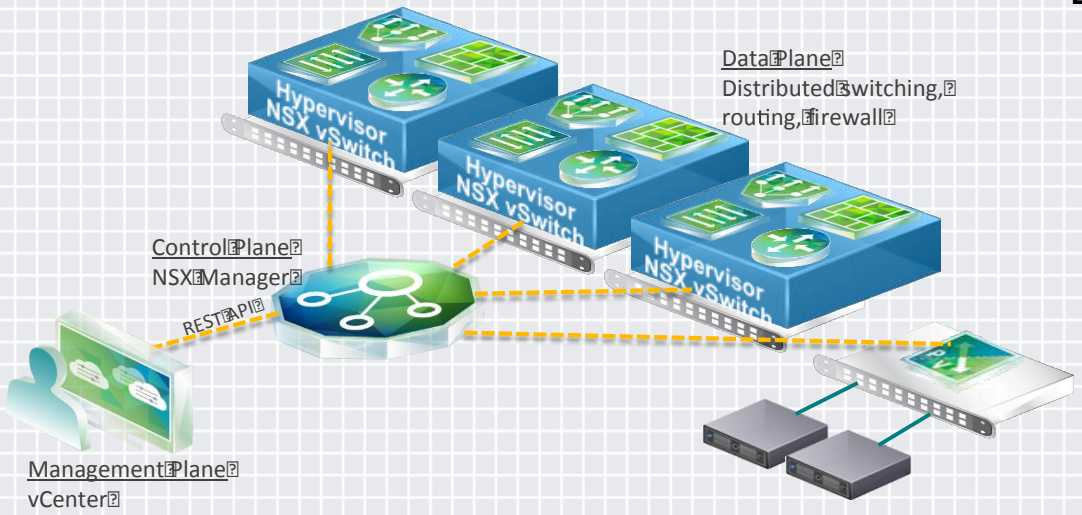
Creating the Dynamic and Secure Data Center



Micro-Segmented Architecture



Micro-segmentation with SDN



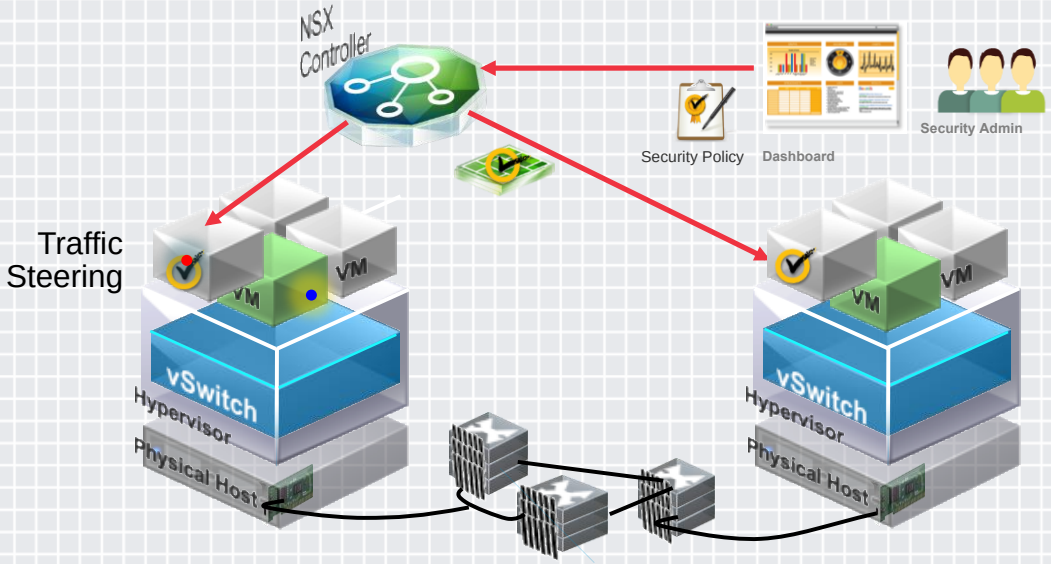
Example Using VMware NSX

Each Workload is:

- Isolated
- Requires all routing to be pre defined

Physical workloads and VLANS

Service Chaining with SDN



Example VMWare NSX and Symantec DCS:Server

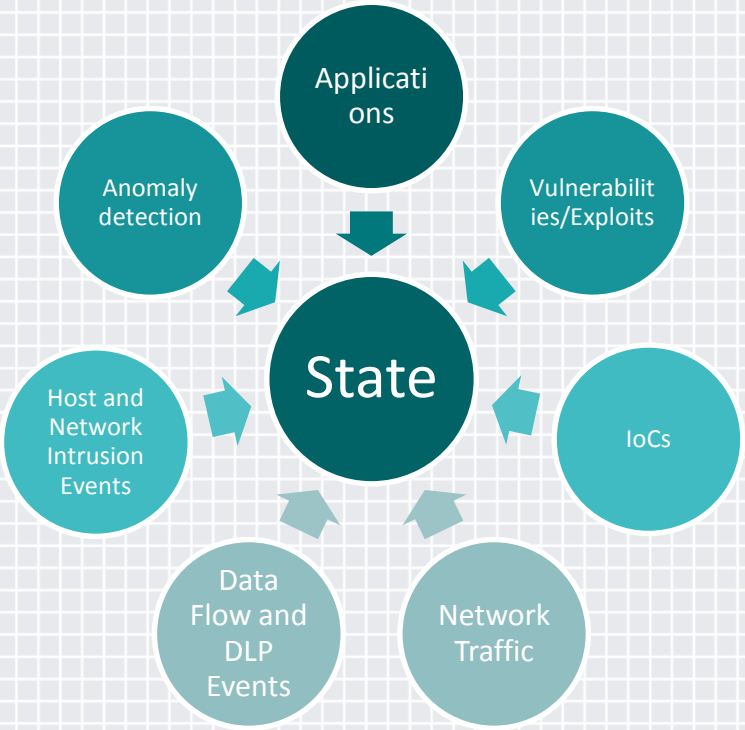
Security controls including

- IPS
- Firewall
- DLP

can be dynamically added to any traffic flow

State

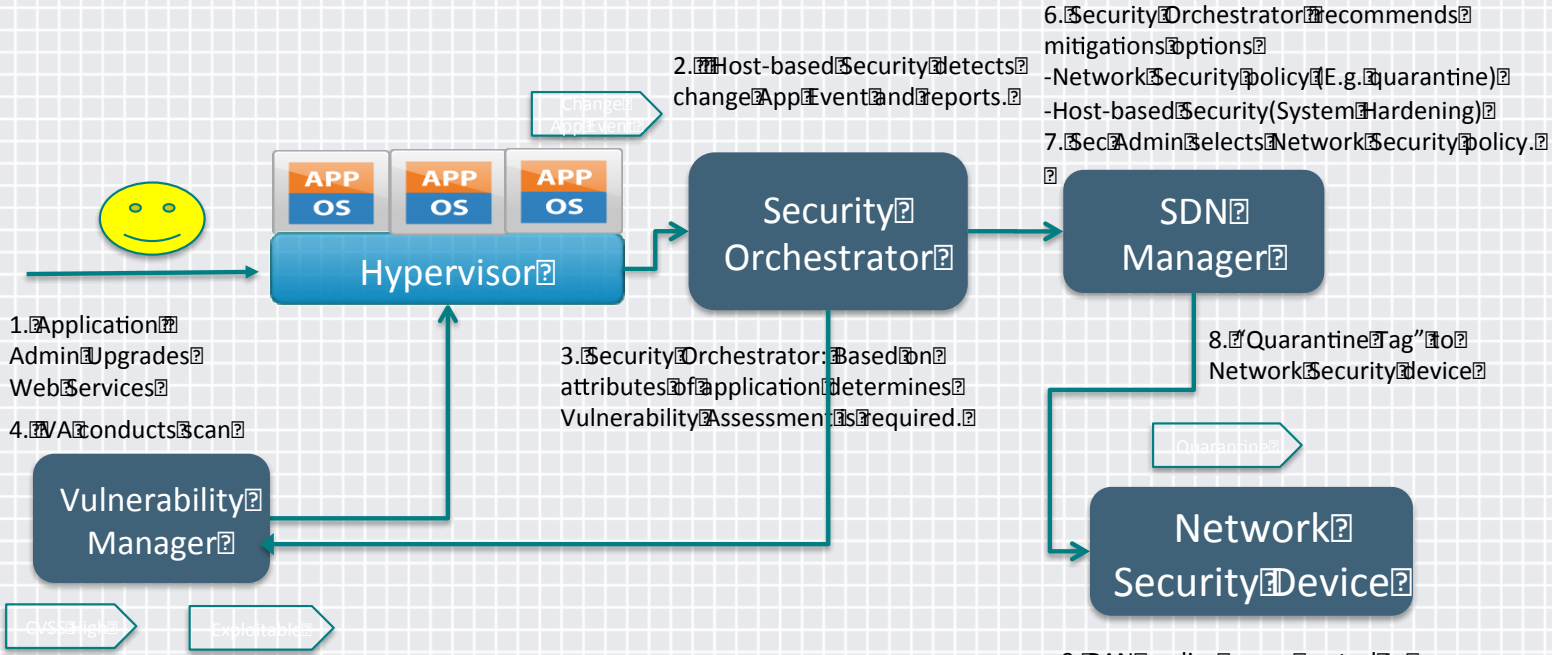
- Static State
  - Applications
  - Vulnerabilities/Exploits
- Dynamic State
  - IoCs
  - Network Traffic
  - Data Flow and DLP Events
  - Host and Network Intrusion Events
  - Anomaly detection



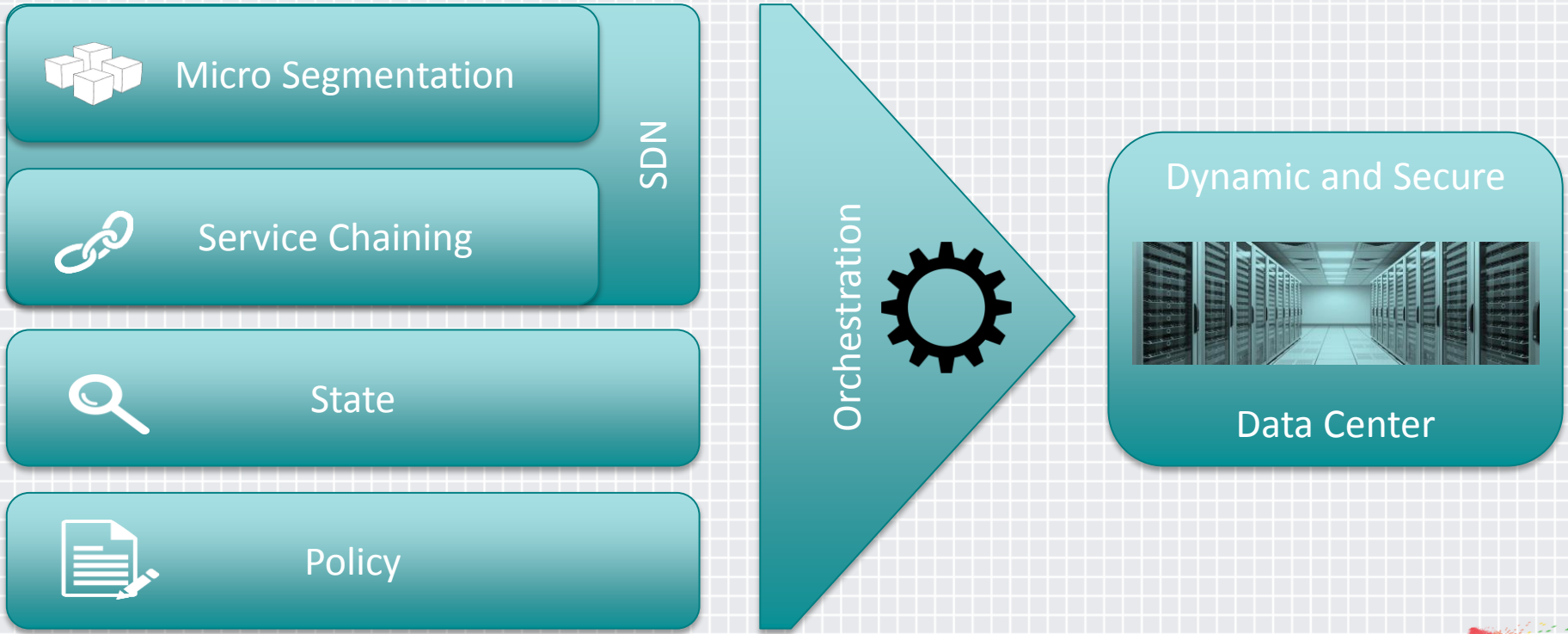
Policy

Infrastructure Provisioning	Security Provisioning Policies	Security Response Policies
• vCenter • NSX • ACI • AWS	• Firewall, Segmentation • IPS • Anti-Malware • DLP • Host Integrity	• Currently Ad-Hoc in the future standards required

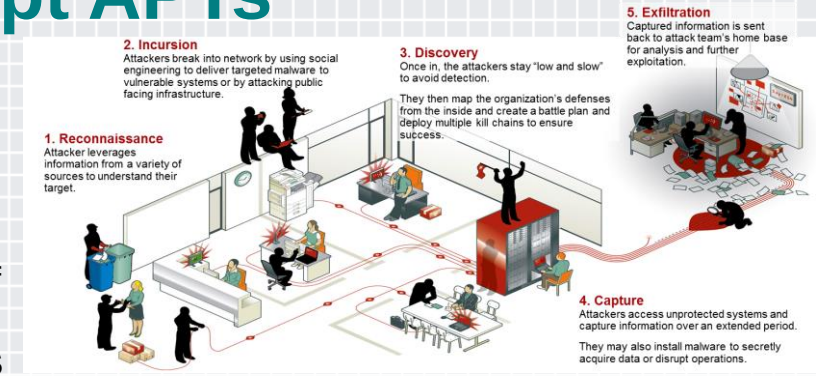
Orchestration = SDN + State + Policy



Creating the Dynamic and Secure Data Center



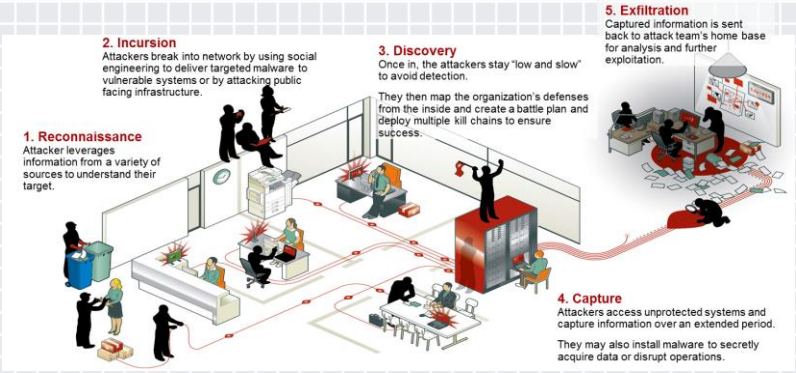
Orchestrating SDNs to disrupt APTs



- Automated Policy Based Provisioning
  - Consistently apply appropriate controls
  - Moves with the workload, and cleans up behind itself
- Remove 'Legacy' or Temporary Rules and Routes
  - Restrict the ability for the attacker to traverse the network east-west
- Transparent Service Chaining of Compensating Controls
  - Add, change or remove controls without detection
  - Leverage real-time intelligence to automate this process

Orchestrating SDNs to disrupt APTs cont.

- Tap/Probe insertion during IR
- Systematic Workload Provisioning
  - Give the attacker a moving target to hit without disrupting the application
- Honey-Pots and Honey-Nets



Summary

- SDN is a key capability for introducing micro-segmentation and service chaining to facilitate dynamic response to APT attacks
- Security controls must offer API's for feeds and for automated response for incidents
  - Apply the persistence of malware against the attack
- Security orchestration systems can automate policy updates to network and host-based security controls for faster and targeted APT responses
  - SDN's enable us to optimize infrastructure and operational resource consumption for APT responses

Apply What You Have Learned Today

- Short Term
  - Evaluate how SDN can help you create fine-grained segmentation zones with lower operational costs
- Medium Term
  - Redefine your data center strategy for orchestration
    - Threat Detection: malware, data loss, behavioral and IoC's
    - Vulnerability Management: assessment, prioritization and compensation
    - Automation: Controls with APIs, application level policies and context
  - Pilot Security Automation on SDN
- Long Term
  - Change the asymmetry of the APT attack