RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Shifting Roles for Security in the Virtualized Data Center: Who Owns What?

SESSION ID: CSV-T07

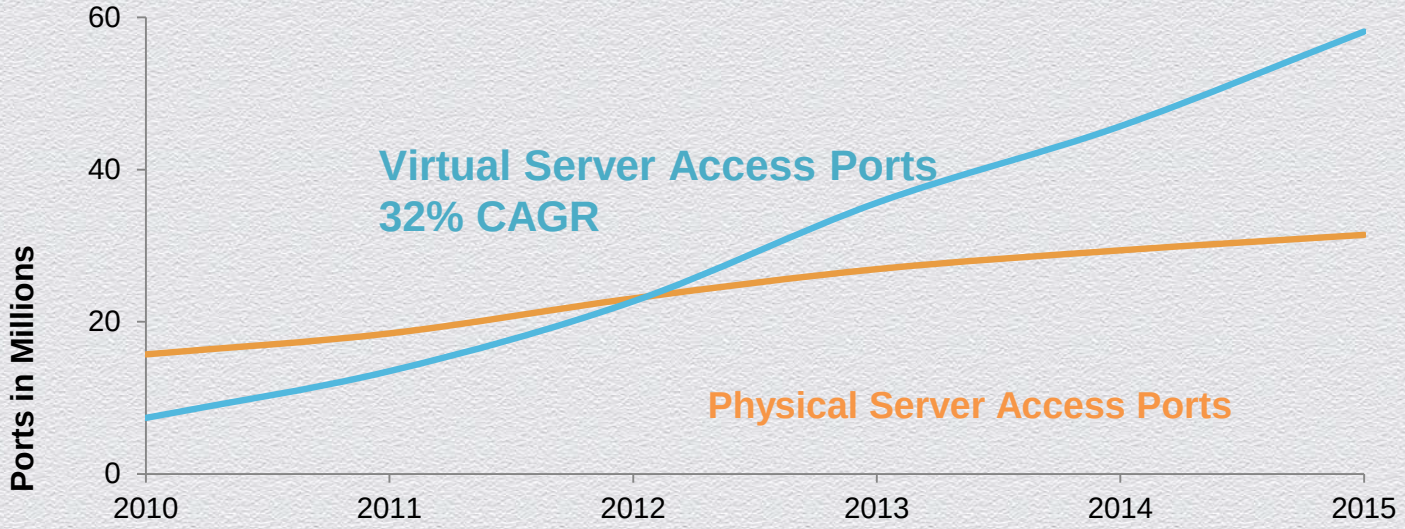
Rob Randell, CISSP
Director Systems Engineering
Principal Security Architect
VMware / NSBU

Malcolm Rieke
Director of Product Management
Catbird

Agenda

- Current State of the Data Center and the SDDC
  - Why Should I Care about the SDDC?
  - Current State of Data Center Security
  - The Software-Defined Data Center (SDDC)
- IT Organizational Structure
  - Current Roles and Duties in Data Center
  - Overlap of Roles and Duties in Data Center
  - How the SDDC is Forcing a New Convergence of Roles and Functionality

Why Do I Care???



CREHAN RESEARCH Inc.

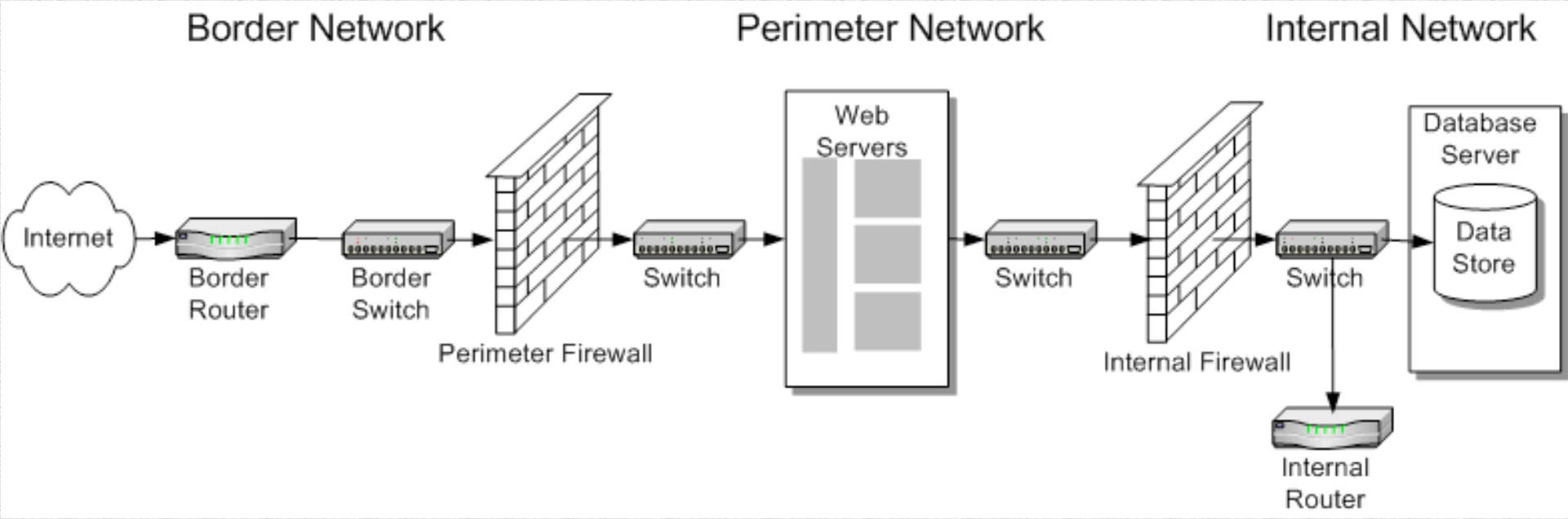
Half of all Server Access Ports are already virtual…
…and are on track to be ~67% in 2 years
*40% of vAdmins manage virtual switching

vmware catbird

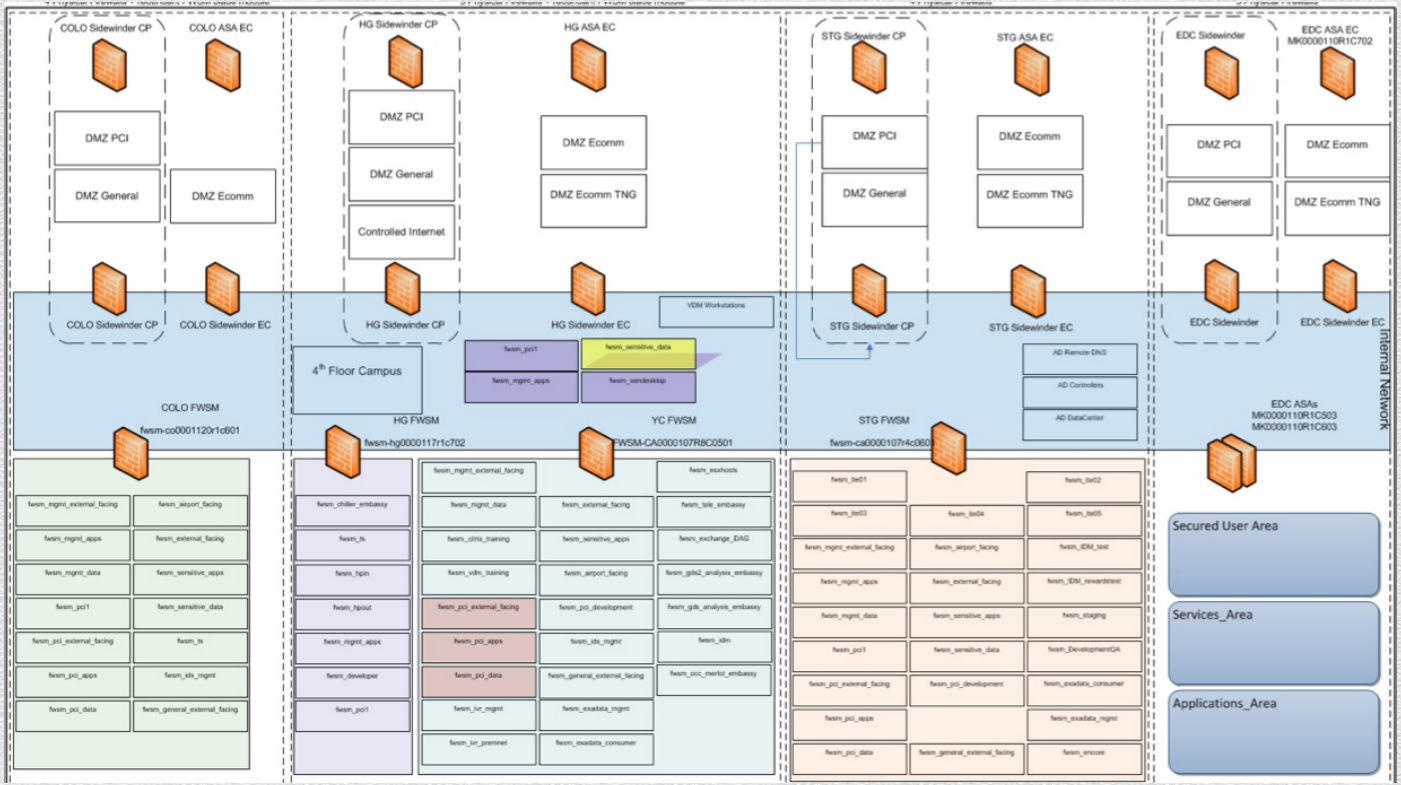
#RSAC

RSACONFERENCE2014

Traditional Network-Based Security Building Blocks



Scaling the Basic Blocks



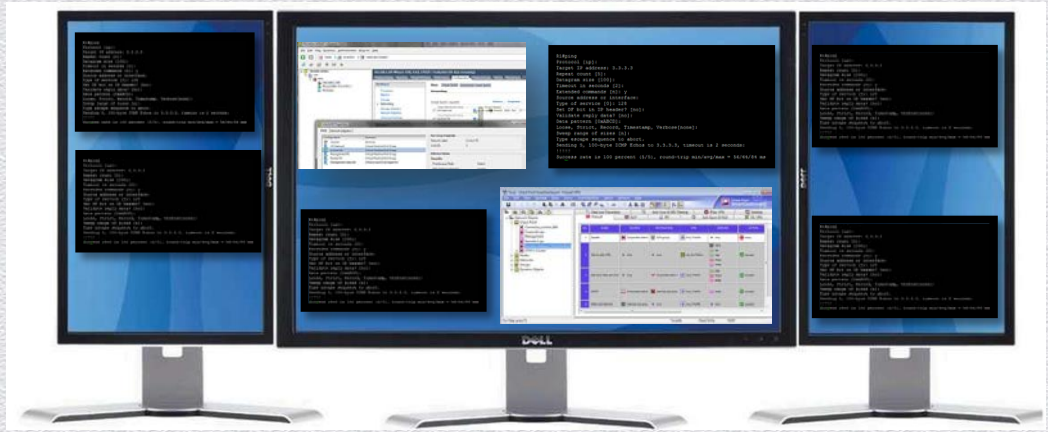
vmware catbird

#RSAC

RSACONFERENCE2014

Day in the Life of a Network/Security Admin

- Request: I want to deploy a new web application with two tiers.
- Net/Sec Admin: How do I implement that topology?



vmware catbird

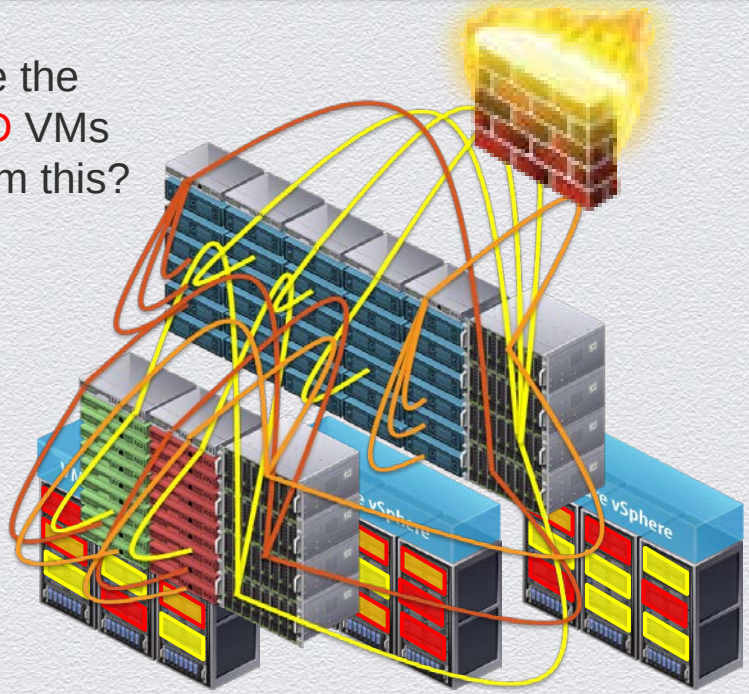
#RSAC

RSACONFERENCE2014

Challenge: Applying Security Policies is a Moving Target

Tying security policies to physical constructs is ineffective. No single source of truth for where security policies are applied in the software-defined data center

CISO: We need to make sure the Firewall is protecting the RED VMs appropriately. Can you confirm this?



vmware catbird

#RSAC

RSACONFERENCE2014

8 Fundamental Security Problems in the Modern Data Center

1	Perimeter-Centric
2	Hyper Connected Computing Base
3	Shared Component Base
4	Highly Accessible Info on I/F and Topology
5	Control Choke Points
6	Managing Security in a Distributed State
7	Security Expressed Over Bad Identifier
8	Policy Abstraction and Management

Primary Use Case: Agility & Efficiency

“Fast is the new better,
Fast is the new cheaper,
Faster is the new faster!”

Chris Launey
Director, Cloud Hosting
The Walt Disney Company

vmware catbird

Software-Defined Data Center

SOFTWARE-DEFINED DATACENTER

All infrastructure is virtualized and delivered as a service, and the control of this datacenter is entirely automated by software.

vmware catbird

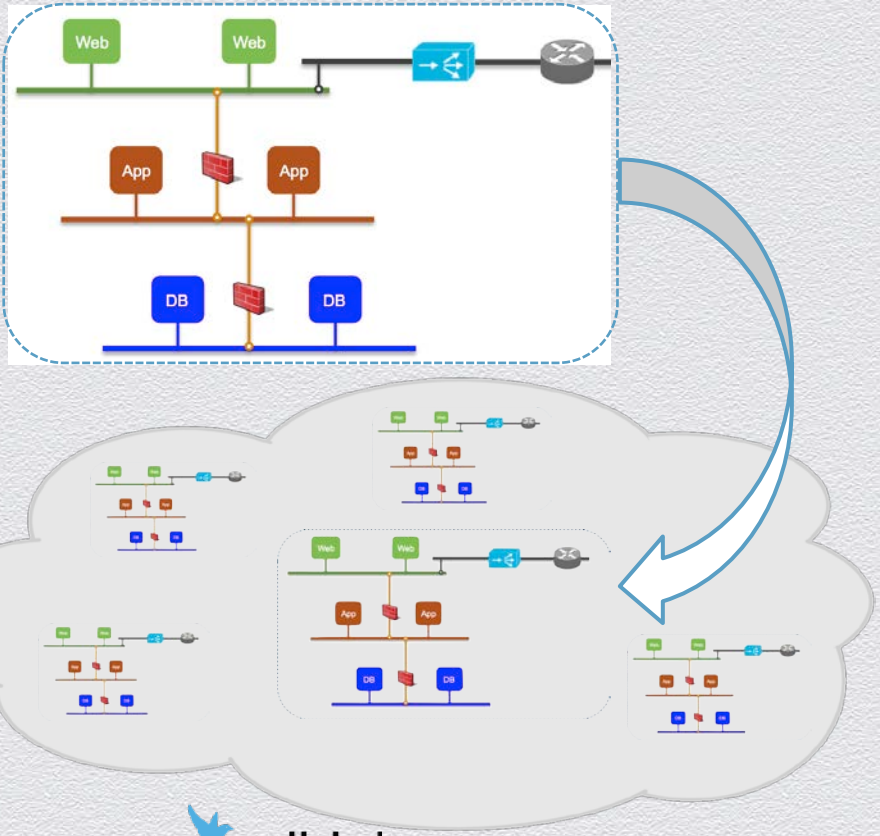
#RSAC

RSACONFERENCE2014

5 Key Security Advantages of SDDC

1 Micro-Segmentation	• Reduces number of addressable targets from any infection • Greatly limits lateral movement and makes it much more detectable.
2 Virtualized Dist. Services	• More pervasive security services • End to End visibility. Achieved more efficiently (less hair-pinning/tromboning). • Simpler policy: Control points are protecting a more focused resource (closer to the app boundary)
3 Lean/Fast Sensor	• Virtualized sensor less loaded, and therefore more scalable. • Embed security functionality into the virtual switch • Enables policy to efficiently follow the workload as it moves and scale out
4 Fewer Shared Services	• Services are smaller, less vulnerable, easier to manage. • Fewer single points of failure.
5 App-Centric Policy	• Having the context of how services are composed (relevant components, linkages) and how they relate to the virtual and physical infrastructure. • Simplify policy. Improve alignment of security controls. Greater context & transparency of gaps, etc.

Provisioning via the SDDC



- Programmatic provisioning
- Place any workload anywhere
- Move any workload anywhere
- Decoupled from hardware
- Operationally efficient

True Cloud Application!!

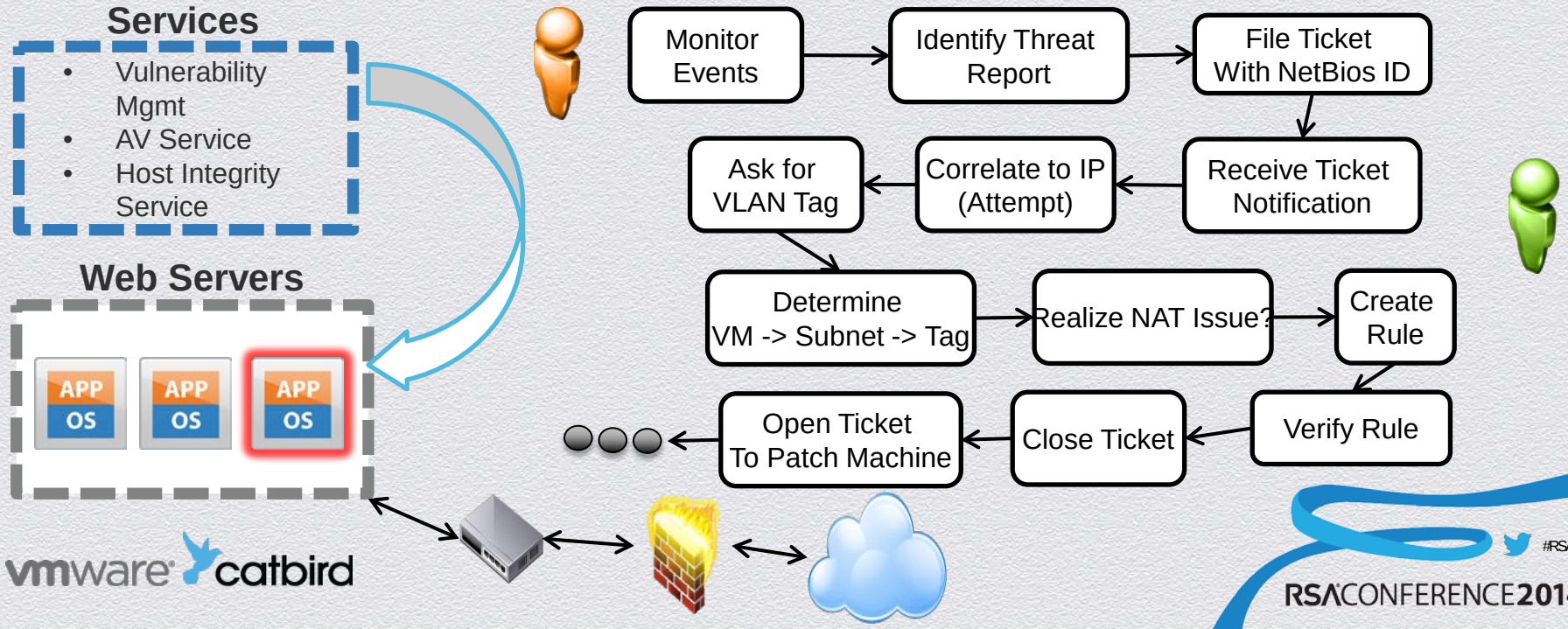
vmware catbird

#RSAC

RSACONFERENCE2014

Challenge: Manual Workflows Are Time Consuming & Error Prone

Operator uses one security product to detect an event and then has to manually trigger another security product to remediate



vmware catbird

#RSAC

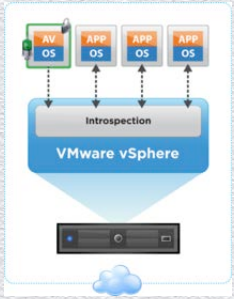
RSACONFERENCE2014

Security Service Consumption in an SDDC

Security services can now be consumed more efficiently in the software-defined data center.

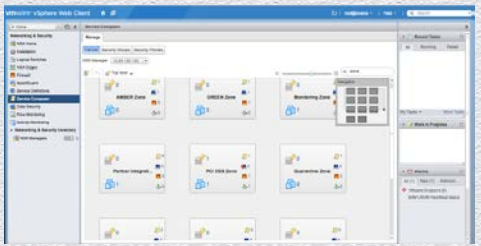
Provision.

Provision and monitor uptime of different services, using <u>one</u> method.



Apply.

Apply and visualize security policies for workloads, in <u>one</u> place.



Automate.

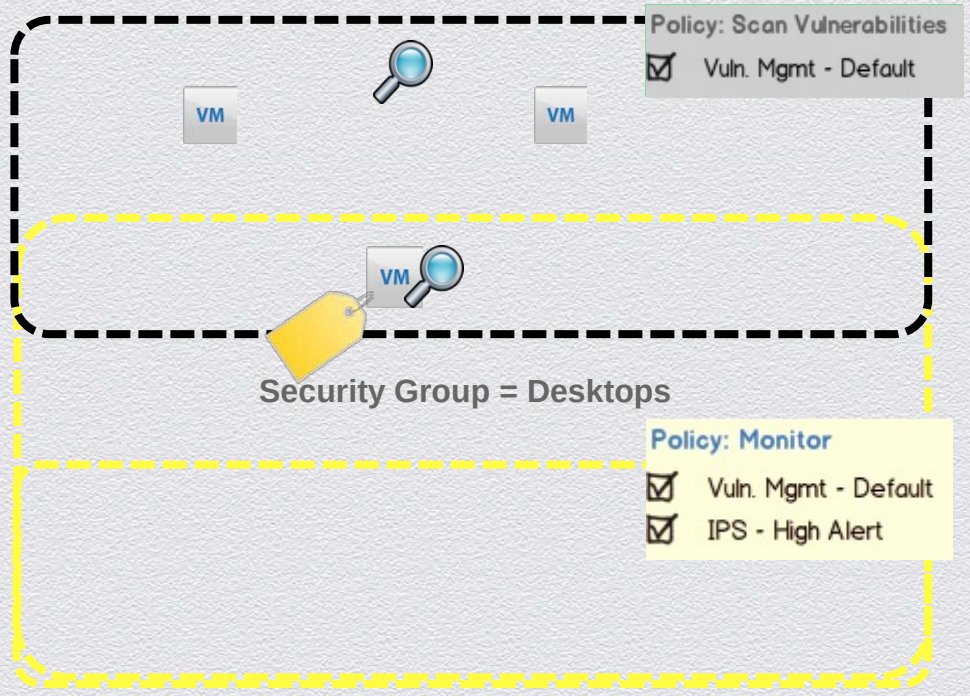
Automate workflows across different services, without custom integration.

vmware catbird

#RSAC

RSACONFERENCE2014

Automate Vulnerability Management Workflow

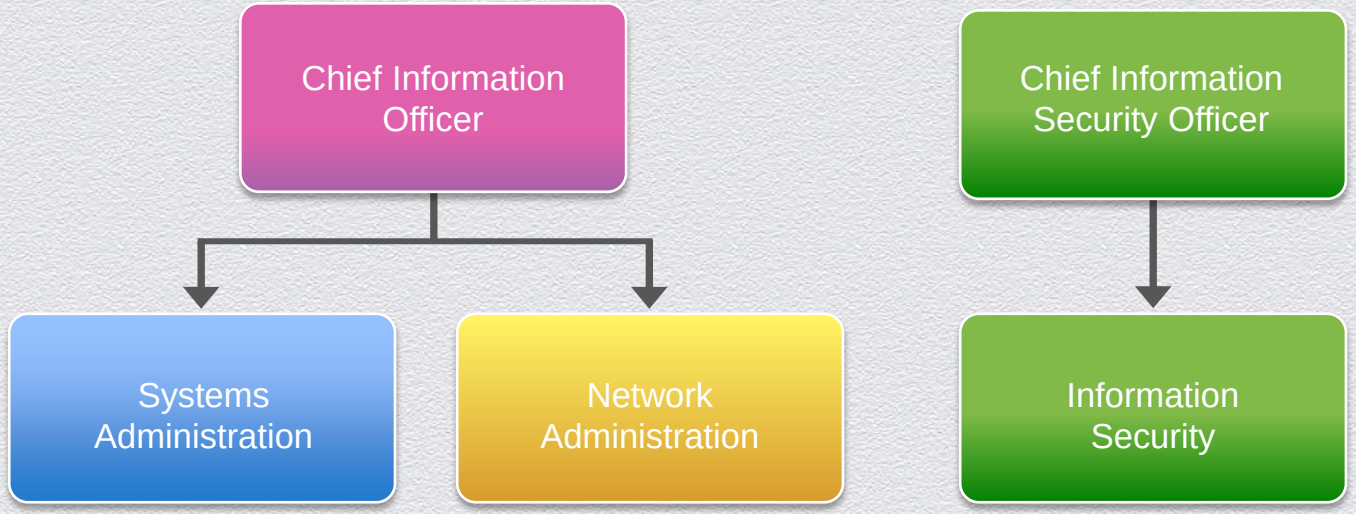


Prerequisites: Security groups defined by tag membership and relevant policies

1. Desktop group scanned scanned for vulnerabilities
2. Solution tags VMs to indicate vulnerabilities
3. Vulnerable VM automatically gets added to Monitor Zone, based on tag
4. Patches are tested in staging environment before being applied; VM is re-scanned
5. Tag removed and VM moved out of Monitor Zone

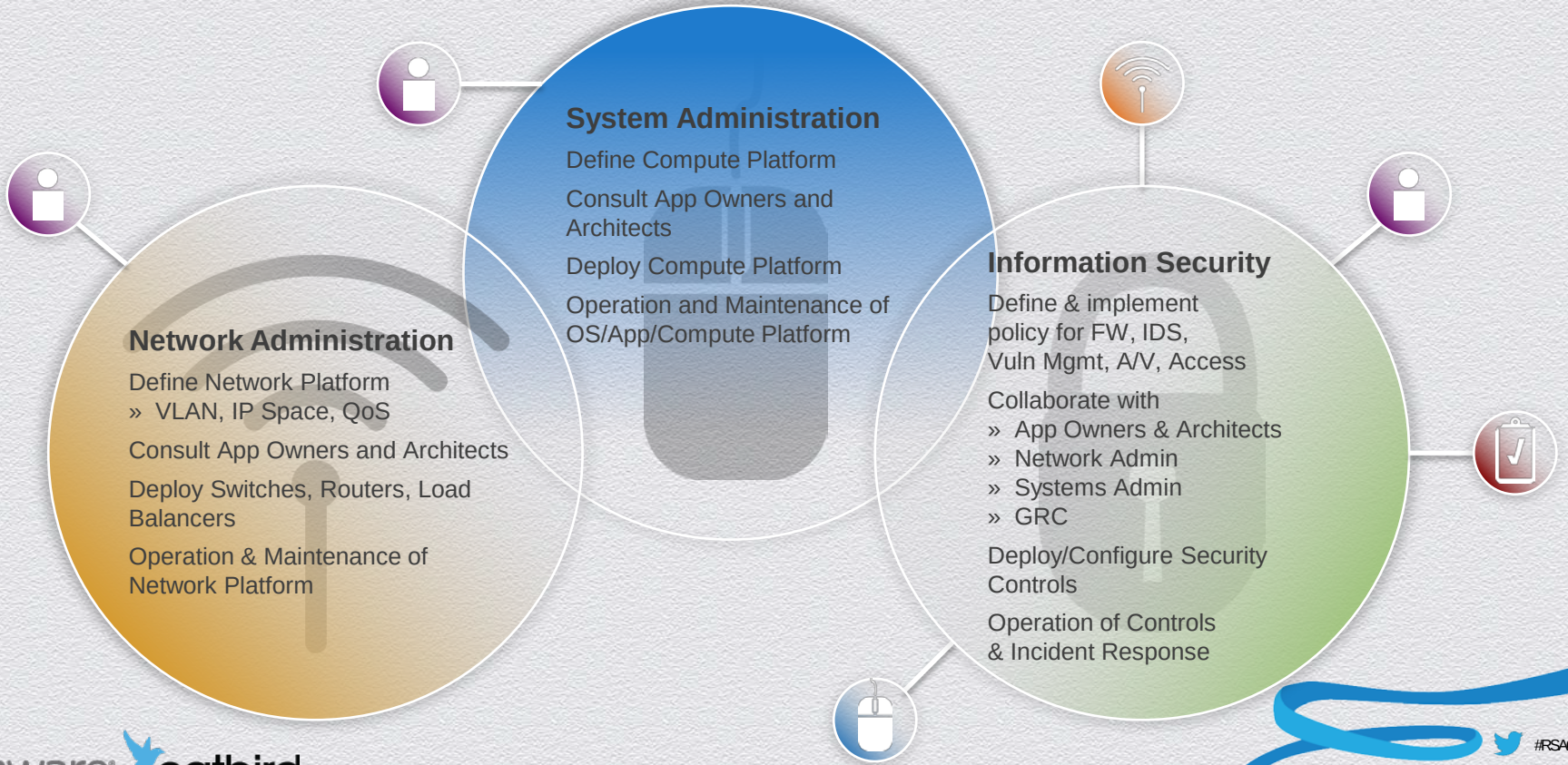
vmware catbird

Information Technology Organization



Technology skill silos are the basis for current organizational divisions.

Skill Diversity – Who Is Doing What?



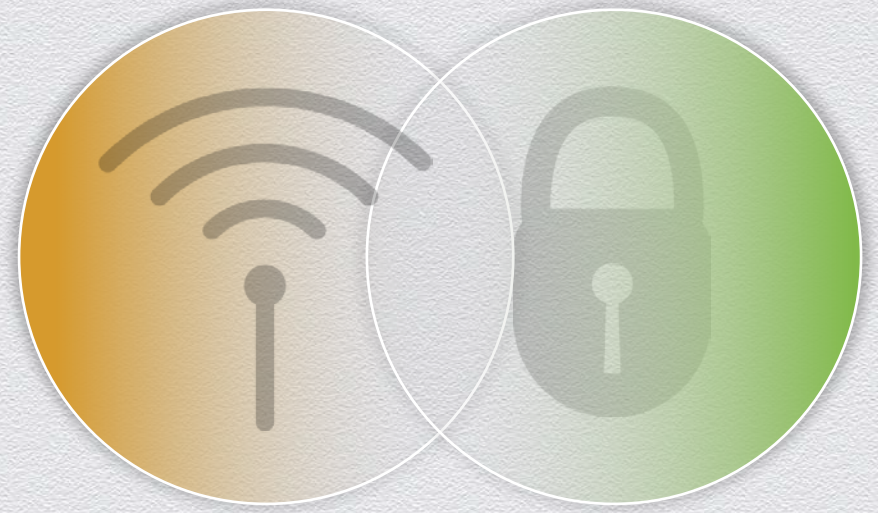
Overlap Exists – Server Admin <> Network Admin

Virtual Switching Technology:

- Consolidates Network Access Layer Administration
- Homogenizes Network Technology Skill Requirement for Access Layer
- Automated
- Dual Provisioning of Compute and Network Resources

vmware catbird

Overlap Exists – Network Admin <> Security Admin



- Firewall and IDS are network devices and by **necessity** are managed by Network Groups
- Networking resources engage in and support incident response

Overlap Exists – Security Admin <> Server Admin

Virtualized Security Components:

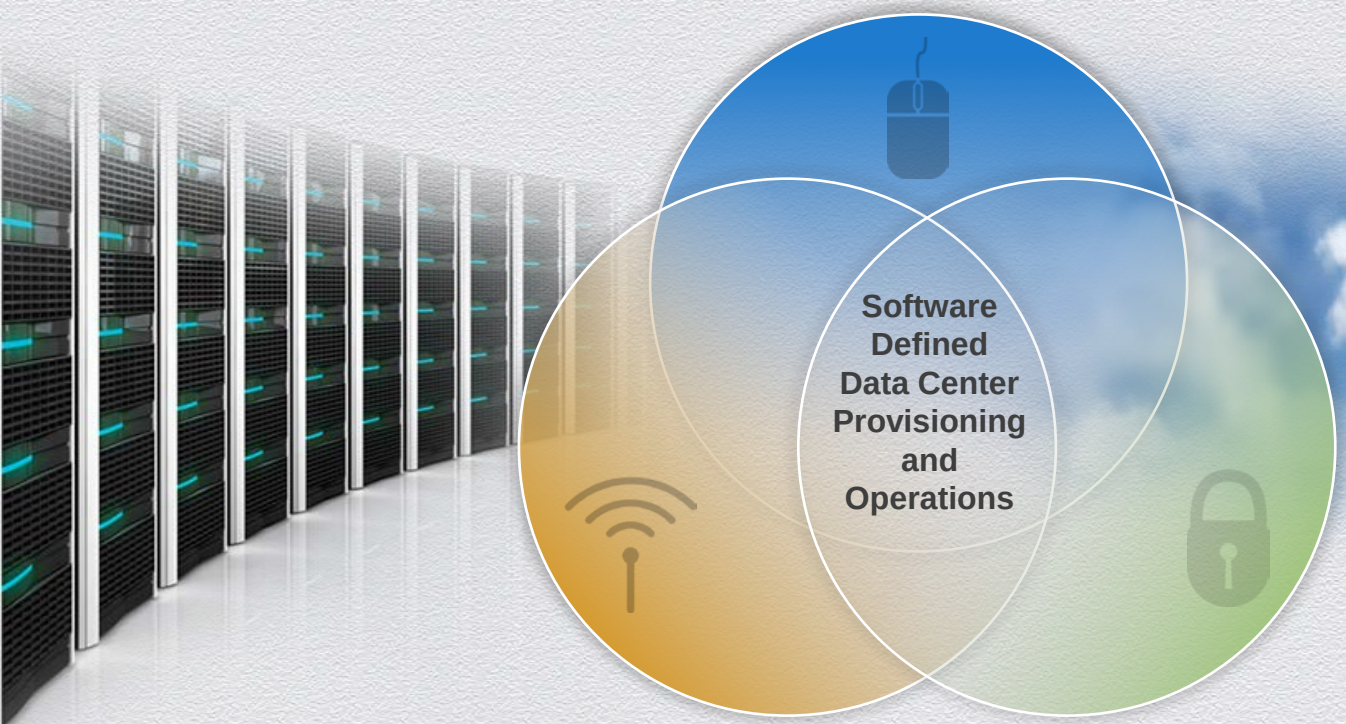
- Leverage Perfect Inventory
- Provision in concert with Computer and Network
- Leverage commodity hardware
- Breaking existing skill and organizational silos

vmware catbird

#RSAC

RSACONFERENCE2014

Skillset Convergence in SDDC and Cloud



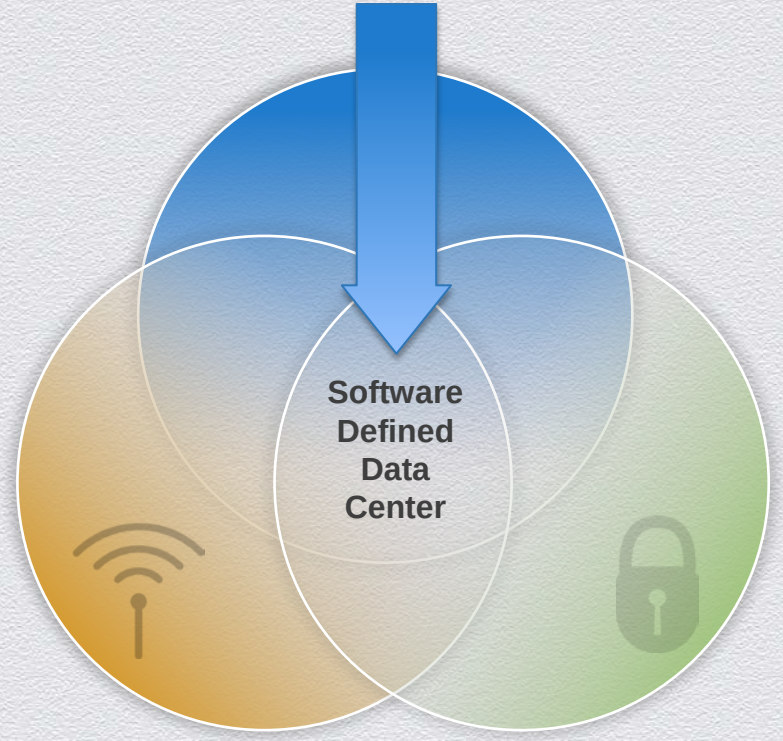
vmware catbird

#RSAC

RSACONFERENCE2014

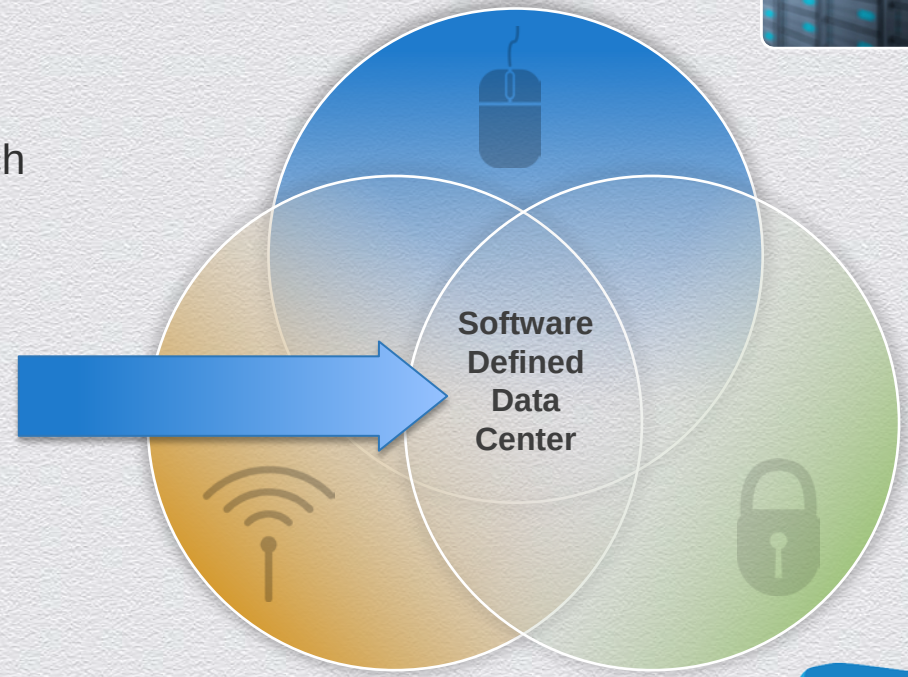
Convergence – Systems Administration

- In progress with the adoption of virtualization technologies
- Network Virtualization at switch layer approaching 50% of access layer
- Routing and Network topologies becoming virtual

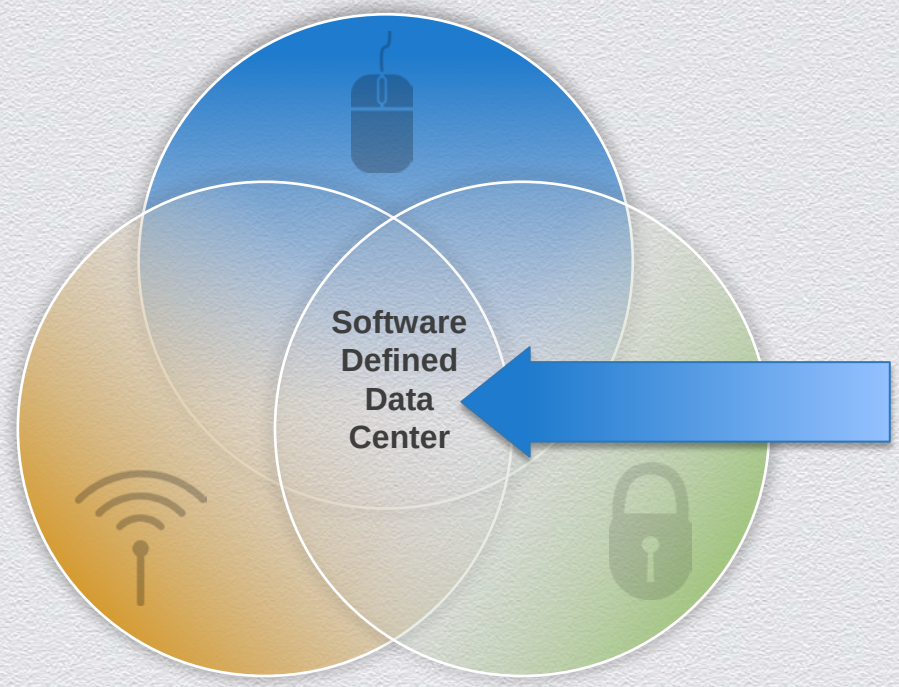


Convergence – Network Administration

- Network technology vendors moving to virtual
- Cisco Nexus 1000v virtual switch extends physical network configuration paradigm into VI
- VXLAN and VXLAN Routing support
- Native virtualized switches typically managed by vAdmin



Convergence – Security Administration



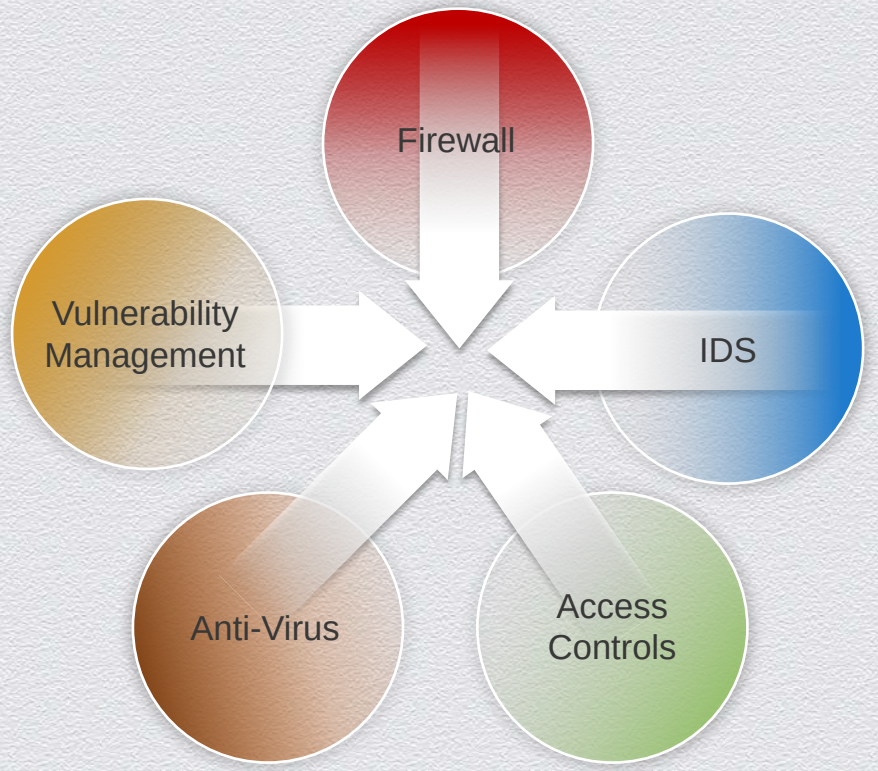
- Virtualized and virtualization aware security components
- Endpoint security completely virtualized (no agents)
- Perfect inventory from VI enhances all security controls
- vSwitch integration and control adds determinism and automation to network based security controls

vmware catbird

#RSAC

RSACONFERENCE2014

Convergence of Security Controls

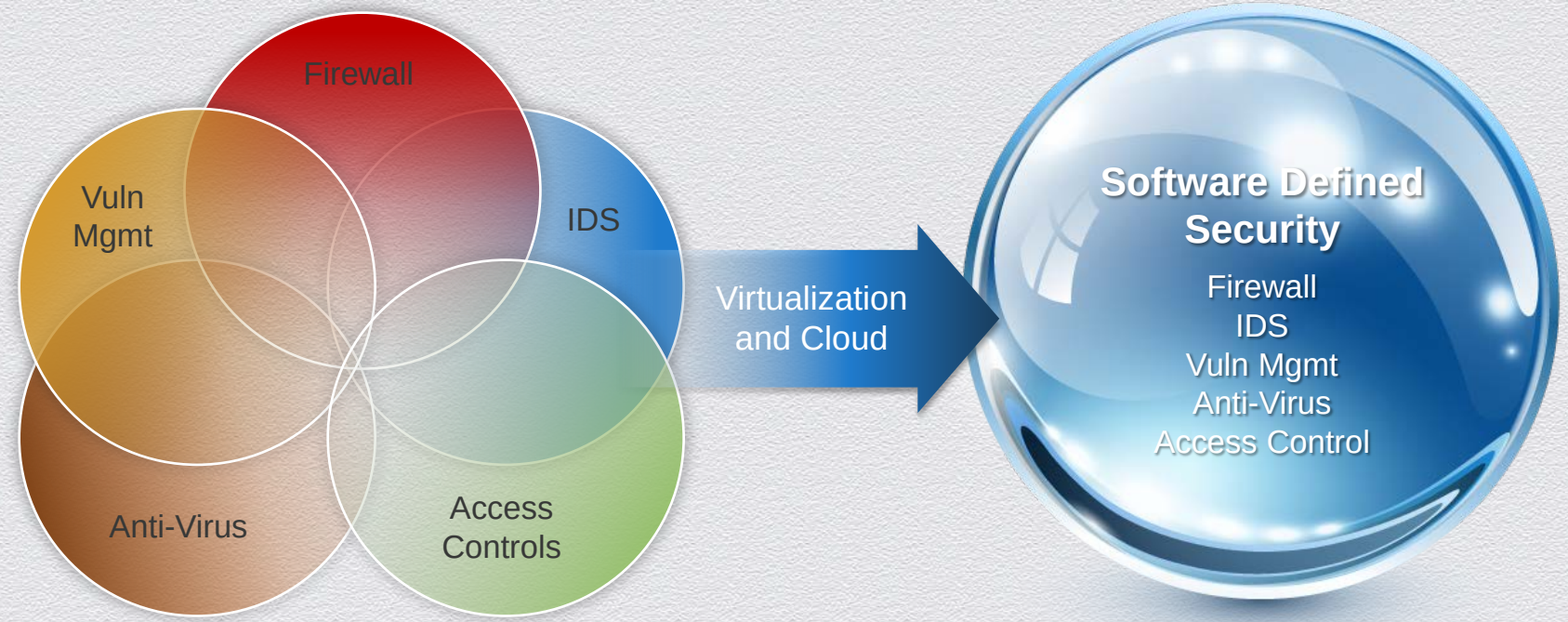


vmware catbird

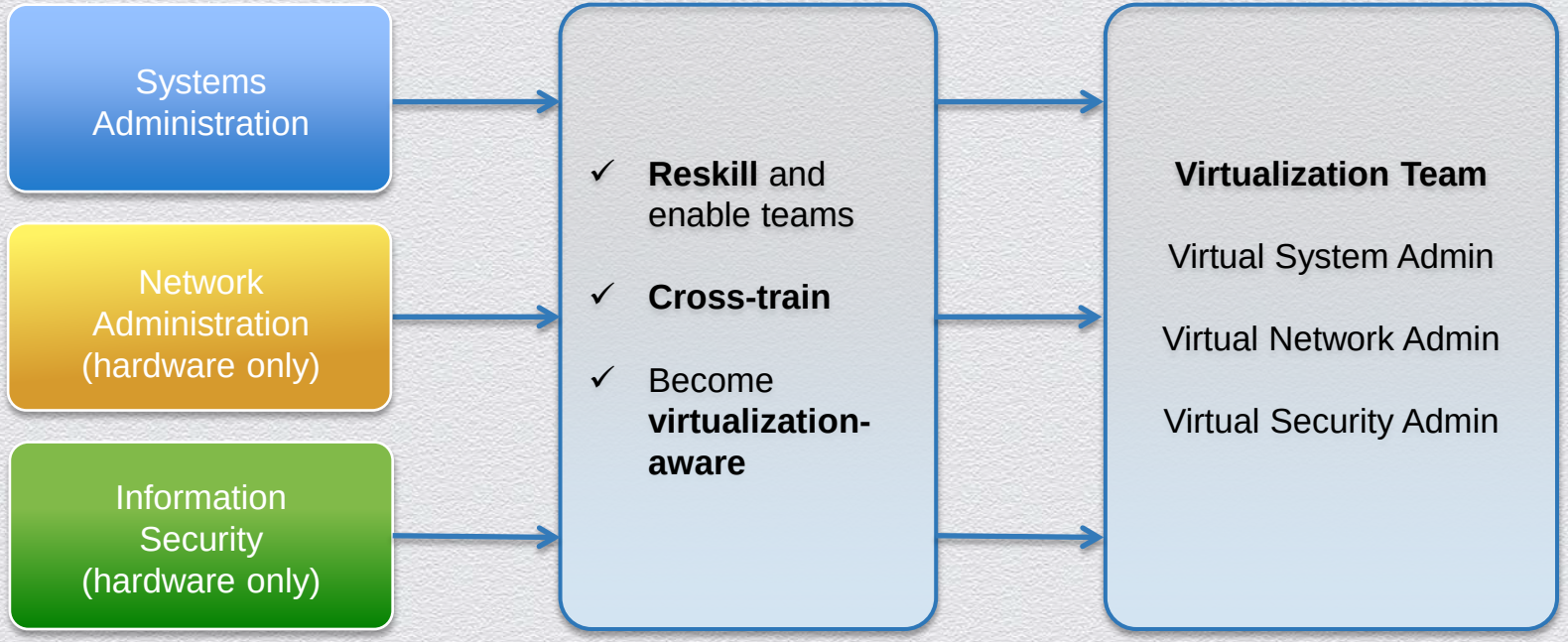
#RSAC

RSACONFERENCE2014

Converged Software Defined Security Controls



Shifting Skills to Match Shifting Roles



Key Takeaways

- Systems administration has been greatly enhanced through the adoption of virtualization technologies
- Networks are becoming virtualized at access layer and will support virtual network topologies independent of physical network (flattening physical network)
- Virtualized and Virtualization aware security technologies benefit from speed and automation of virtualization making security controls as easy to deploy and manage as virtual machines
- Organizational divisions based on Systems/Network/Security skill siloes struggle to realize benefits of all three skills sets
- Software Defined Data Center “features” ubiquitously secure applications providing higher levels of security if your organization can embrace and adapt to these technologies

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Visit Catbird in
booth 2505
to be entered in
an exclusive raffle for
session attendees!

Q&A

Rob Randell
rrandell@vmware.com
VMware
Booth 1621

Malcolm Rieke
malcolm@catbird.com
Catbird
Booth 2505