RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: ASD-W03

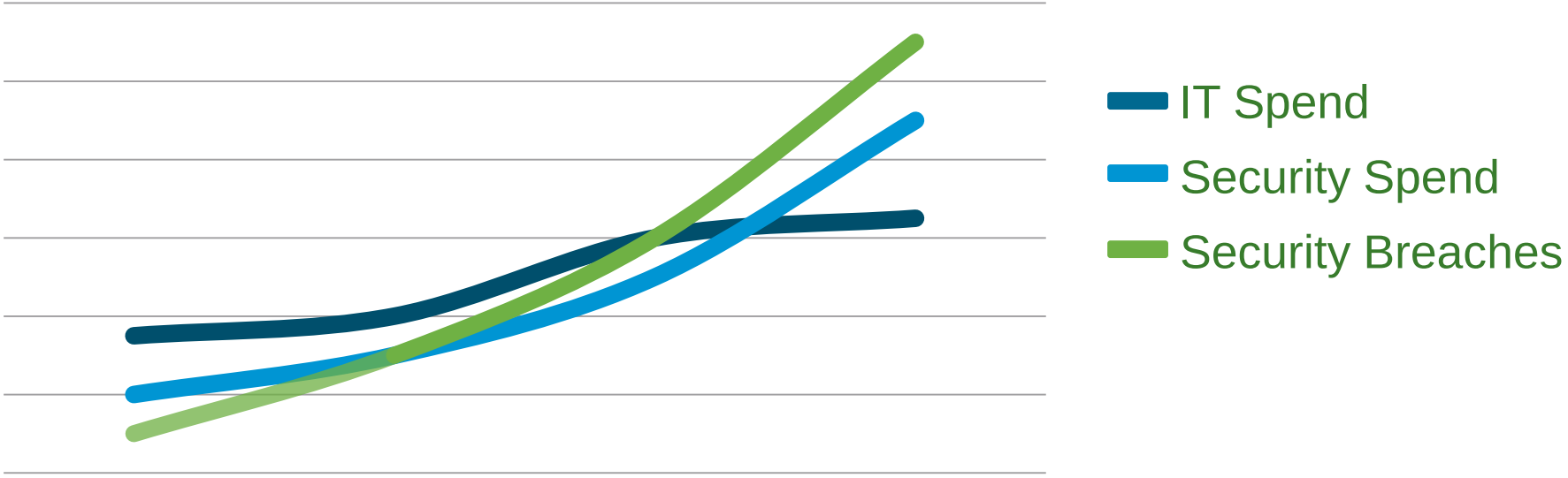
Transforming Security: Containers, Virtualization and the Softwarization of Controls

Dennis R Moreau
Senior Engineering Architect
VMware Office of the CTSO
@DoctorMoreau

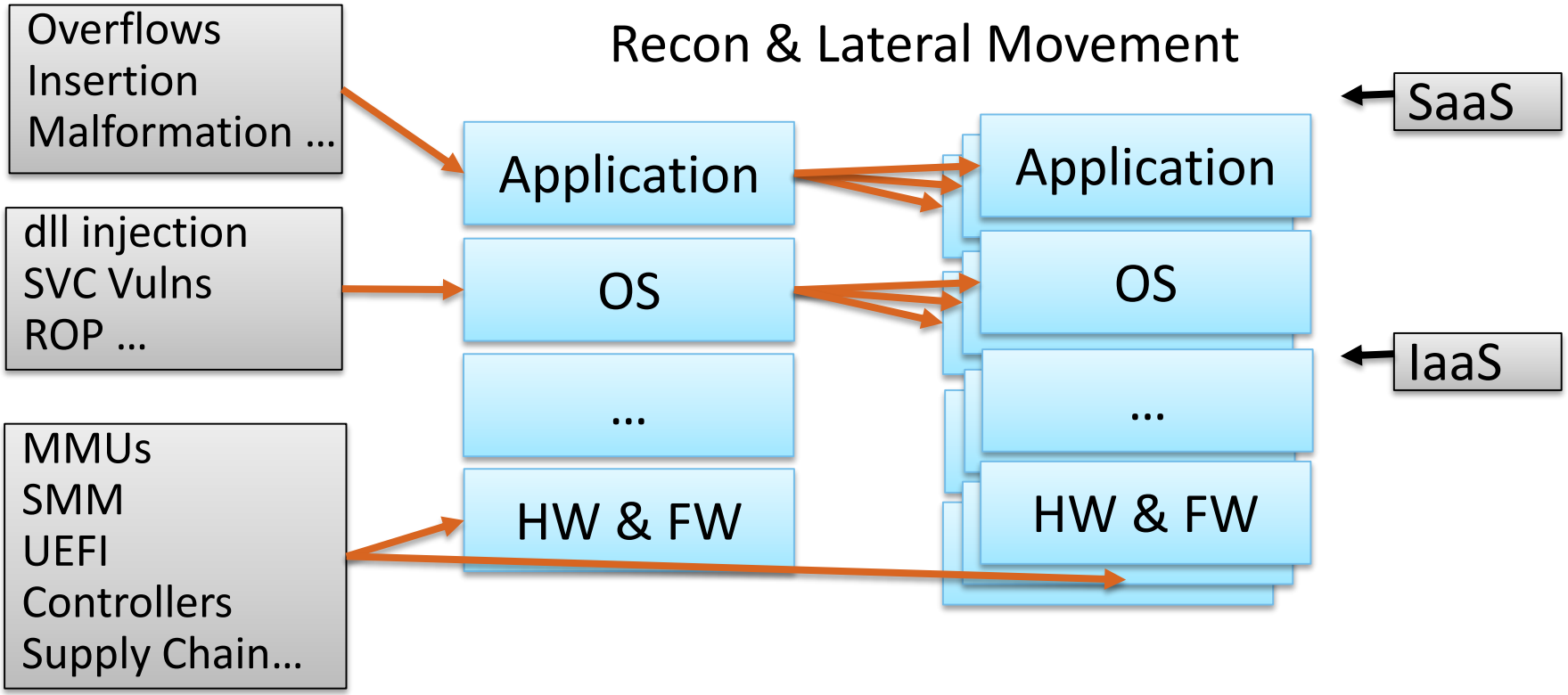
#RSAC

The Security Problem

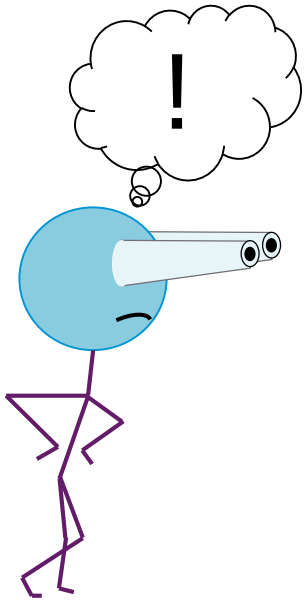
Security breach rates and losses continue to outpace security spend in “the year of the breach”.

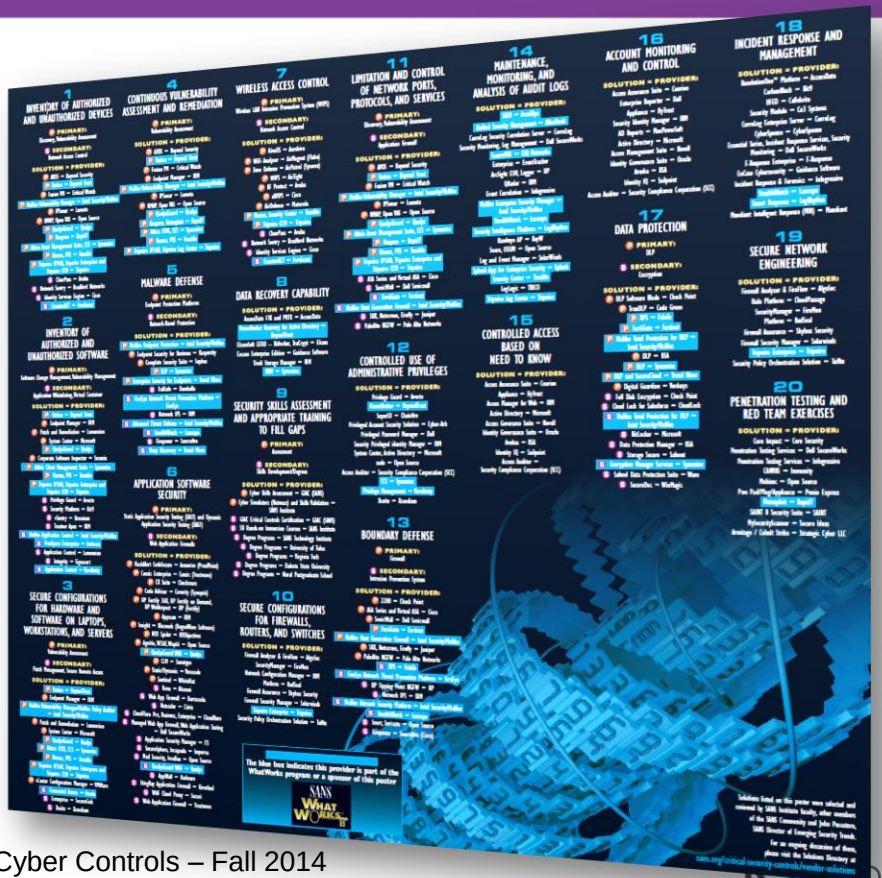


Complexity: Complex Attack Behavior



Complexity: Many Required Security Controls

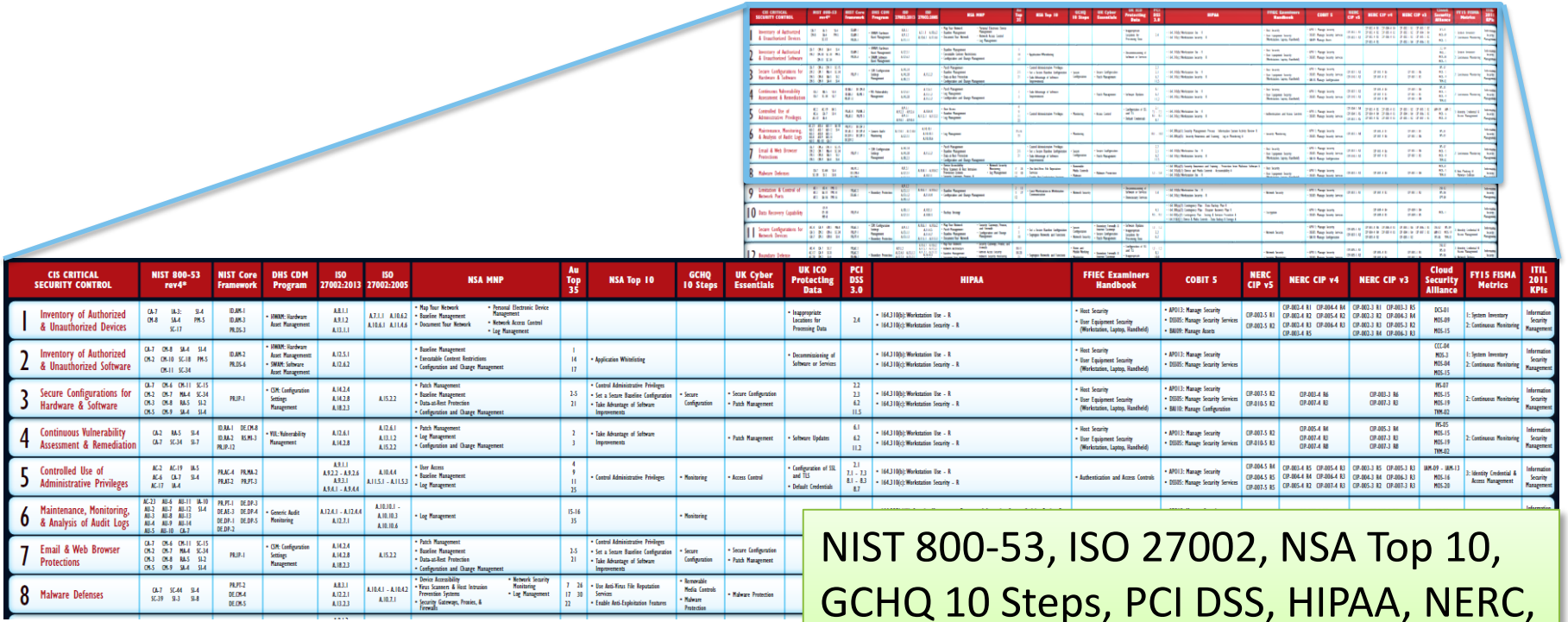




Source: SANS 20 Critical Cyber Controls – Fall 2014

https://www.sans.org/media/critical-security-controls/fall-2014-poster.pdf

Complexity: Many Security Control Standards

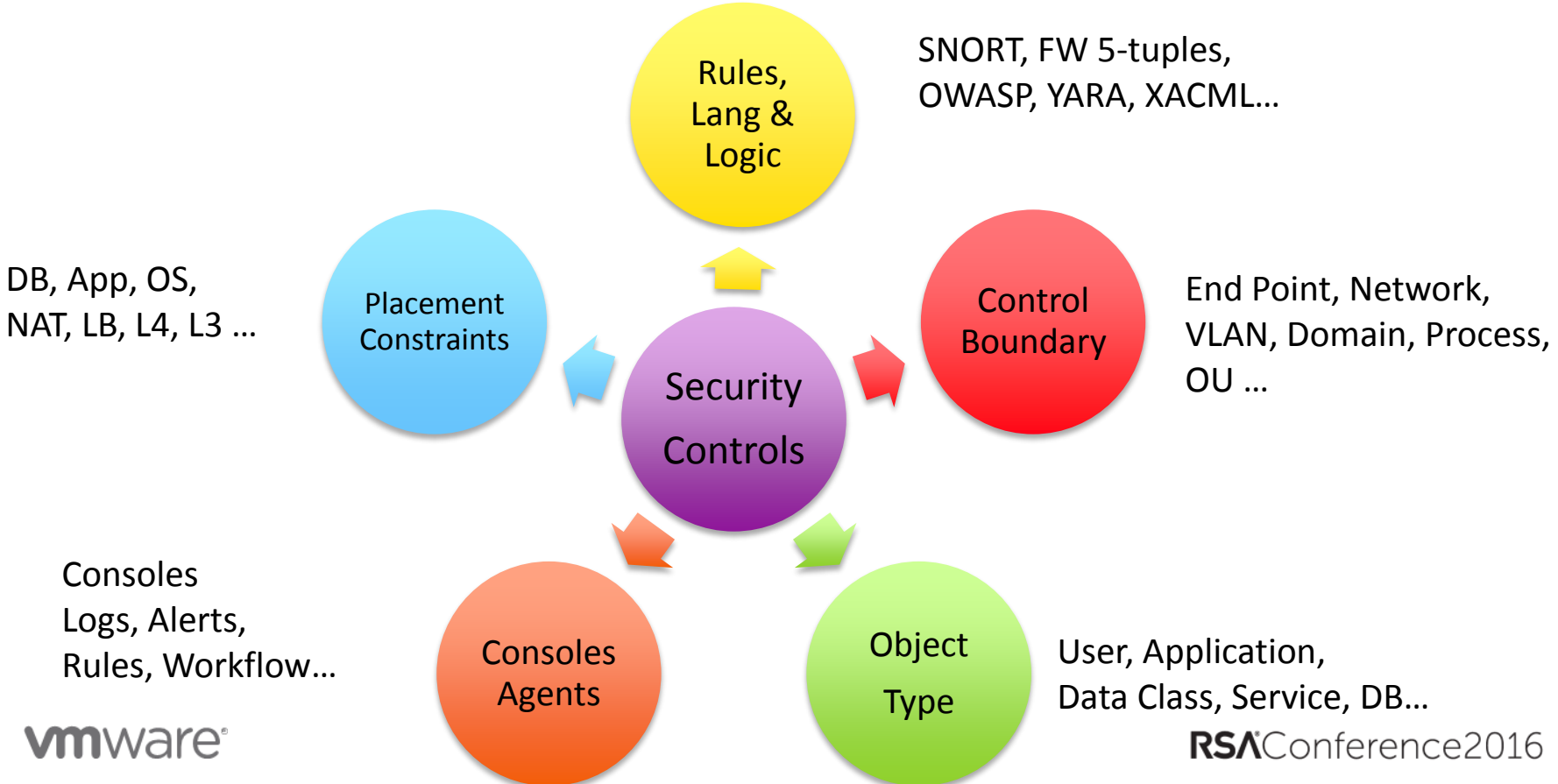


CIS CRITICAL SECURITY CONTROL	NIST 800-53 rev4[a]	NIST Core Framework	DHS CDM Program	ISO 27002:2013	ISO 27002:2005	NSA MNP	Au Top 35	NSA Top 10	GCHQ 10 Steps	UK Cyber Essentials	UK ICO Protecting Data	PCI DSS 3.0	HIPAA	FFIEC Examiners Handbook	COBIT 5	NERC CIP v5	NERC CIP v4	NERC CIP v3	Cloud Security Alliance	FY15 FISMA Metrics	ITIL 2011 KPIs
1 Inventory of Authorized & Unauthorized Devices	CA-7 CM-8 IA-3: IA-4 PM-5 SC-17	ID.AM-1 ID.AM-3 PR.DS-3	• HWAM: Hardware Asset Management	A.8.1.1 A.9.1.2 A.13.1.1	A.7.1.1 A.10.6.2 A.10.6.1 A.11.4.6	• Map Your Network • Baseline Management • Document Your Network • Personal Electronic Device Management • Network Access Control • Log Management					• Inappropriate Locations for Processing Data	2.4	• 164.310(b) Workstation Use - R • 164.310(c) Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services • BAI09: Manage Assets	CIP-002-5 R1 CIP-002-5 R2	CIP-002-4 R1 CIP-004-4 R4 CIP-005-4 R2 CIP-006-4 R1 CIP-006-4 R3 CIP-007-4 R5	CIP-002-3 R1 CIP-003-3 R5 CIP-002-3 R2 CIP-004-3 R4 CIP-002-3 R3 CIP-005-3 R2 CIP-002-3 R4 CIP-006-3 R3	DCS-01 MOS-09 MOS-15	1: System Inventory 2: Continuous Monitoring	Information Security Management
2 Inventory of Authorized & Unauthorized Software	CA-7 CM-8 SA-4 SI-4 CM-2 CM-10 SC-18 PM-5 CM-11 SC-34	ID.AM-2 PR.DS-6	• HWAM: Hardware Asset Management • SWAM: Software Asset Management	A.13.1.1 A.12.6.2		• Baseline Management • Executable Content Restrictions • Configuration and Change Management	1 14 17	• Application Whitelisting			• Decommissioning of Software or Services		• 164.310(b) Workstation Use - R • 164.310(c) Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services				CCC-04 MOS-3 MOS-04 MOS-15	1: System Inventory 2: Continuous Monitoring	Information Security Management
3 Secure Configurations for Hardware & Software	CA-7 CM-6 CM-11 SC-15 CM-2 CM-7 MA-4 SC-34 CM-3 CM-9 RA-5 SI-2 CM-5 CM-9 SA-4 SI-4	PR.IP-1	• CCM: Configuration Settings Management	A.14.2.4 A.14.2.8 A.18.2.3	A.15.2.2	• Patch Management • Baseline Management • Data-at-Rest Protection • Configuration and Change Management	2-5 21	• Control Administrative Privileges • Set a Secure Baseline Configuration • Take Advantage of Software Improvements	• Secure Configuration	• Secure Configuration • Patch Management		2.2 2.3 6.2 11.5	• 164.310(b) Workstation Use - R • 164.310(c) Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration	CIP-007-5 R2 CIP-010-5 R2	CIP-003-4 R6 CIP-007-4 R2	CIP-003-3 R6 CIP-007-3 R2	TVS-07 MOS-15 MOS-19 TVM-02	2: Continuous Monitoring	Information Security Management
4 Continuous Vulnerability Assessment & Remediation	CA-2 RA-5 SI-4 CA-7 SC-34 SI-7	ID.RA-1 ID.RA-2 PR.IP-12	• VUL: Vulnerability Management	A.12.6.1 A.14.2.8	A.12.6.1 A.13.1.2 A.15.2.2	• Patch Management • Log Management • Configuration and Change Management	2 3	• Take Advantage of Software Improvements		• Patch Management	• Software Updates	6.1 6.2 11.2	• 164.310(b) Workstation Use - R • 164.310(c) Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R2 CIP-010-5 R3	CIP-005-4 R4 CIP-007-4 R3 CIP-007-4 R8	CIP-005-3 R4 CIP-007-3 R3 CIP-007-3 R8	TVS-05 MOS-15 MOS-19 TVM-02	2: Continuous Monitoring	Information Security Management
5 Controlled Use of Administrative Privileges	AC-2 AC-19 IA-5 AC-6 CA-7 SI-4 AC-17 IA-4	PR.AC-4 PR.AC-2 PR.AT-2 PR.PT-3		A.9.1.1 A.9.2.2 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.4	A.10.4.4 A.11.5.1 - A.11.5.3	• User Access • Baseline Management • Log Management	4 9 11 25	• Control Administrative Privileges	• Monitoring	• Access Control	• Configuration of SSL and TLS • Default Credentials	2.1 7.1 - 7.3 8.1 - 8.3 8.7	• 164.310(b) Workstation Use - R • 164.310(c) Workstation Security - R	• Authentication and Access Controls	• APO13: Manage Security • DSS05: Manage Security Services	CIP-004-5 R4 CIP-004-5 R5 CIP-007-5 R5	CIP-003-4 R5 CIP-004-4 R4 CIP-005-4 R2 CIP-006-4 R2 CIP-007-4 R3	CIP-003-3 R5 CIP-004-3 R4 CIP-005-3 R2 CIP-006-3 R2 CIP-007-3 R3	IAM-09 IAM-13 MOS-16 MOS-20	2: Identity Credential & Access Management	Information Security Management
6 Maintenance, Monitoring, & Analysis of Audit Logs	AC-23 AU-6 AU-11 IA-10 AU-2 AU-7 AU-12 SI-4 AU-3 AU-8 AU-13 AU-4 AU-9 AU-14 AU-5 AU-10 CA-7	PR.PT-1 DE.DP-3 DE.AE-3 DE.DP-4 DE.DP-1 DE.DP-5 DE.DP-2	• Generic Audit Monitoring	A.12.4.1 - A.12.4.4 A.12.7.1	A.10.10.1 - A.10.10.3 A.10.10.6	• Log Management	15-16 35		• Monitoring											
7 Email & Web Browser Protections	CA-7 CM-6 CM-11 SC-15 CM-2 CM-7 MA-4 SC-34 CM-3 CM-9 RA-5 SI-2 CM-5 CM-9 SA-4 SI-4	PR.IP-1	• CCM: Configuration Settings Management	A.14.2.4 A.14.2.8 A.18.2.3	A.15.2.2	• Patch Management • Baseline Management • Data-at-Rest Protection • Configuration and Change Management	2-5 21	• Control Administrative Privileges • Set a Secure Baseline Configuration • Take Advantage of Software Improvements	• Secure Configuration	• Secure Configuration • Patch Management											
8 Malware Defenses	CA-7 SC-44 SI-4 SC-39 SI-3 SI-8	PR.PT-2 DE.CM-4 DE.CM-5		A.8.2.1 A.12.2.1 A.12.2.3	A.10.4.1 - A.10.4.2 A.10.7.1	• Device Accessibility • Virus Scanners & Host Intrusion Prevention Systems • Security Gateways, Proxies, & Firewalls • Network Security Monitoring • Log Management	7 26 17 30 22	• Use Anti-Virus File Reputation Services • Enable Anti-Exploitation Features	• Removable Media Controls • Malware Protection	• Malware Protection											

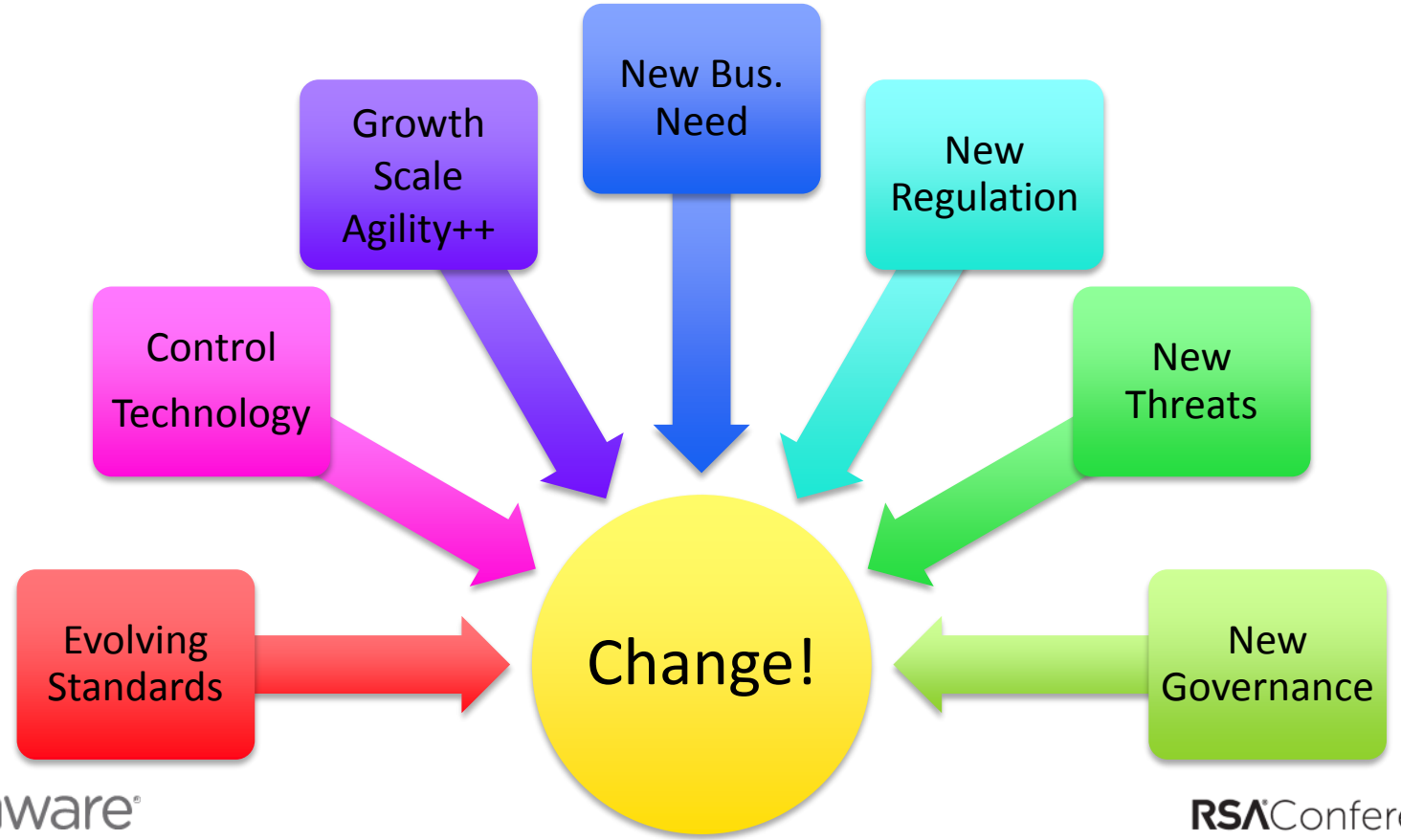
NIST 800-53, ISO 27002, NSA Top 10, GCHQ 10 Steps, PCI DSS, HIPAA, NERC, CSA, FISMA, ITIL KPIs, …

https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf

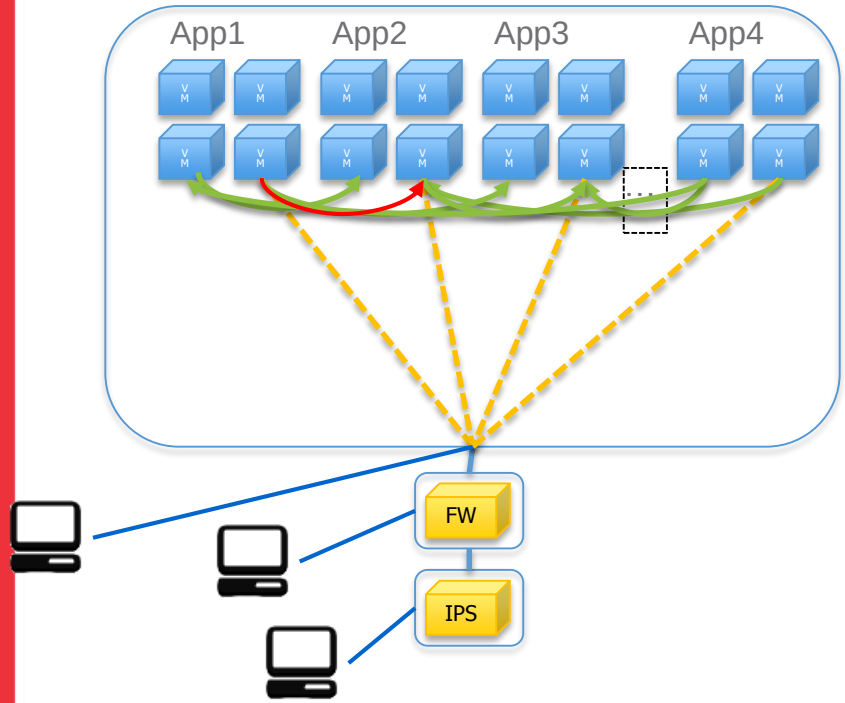
Complexity: The Balkanization of Security



Complexity: No Finish Line



Complexity: IT Architecture



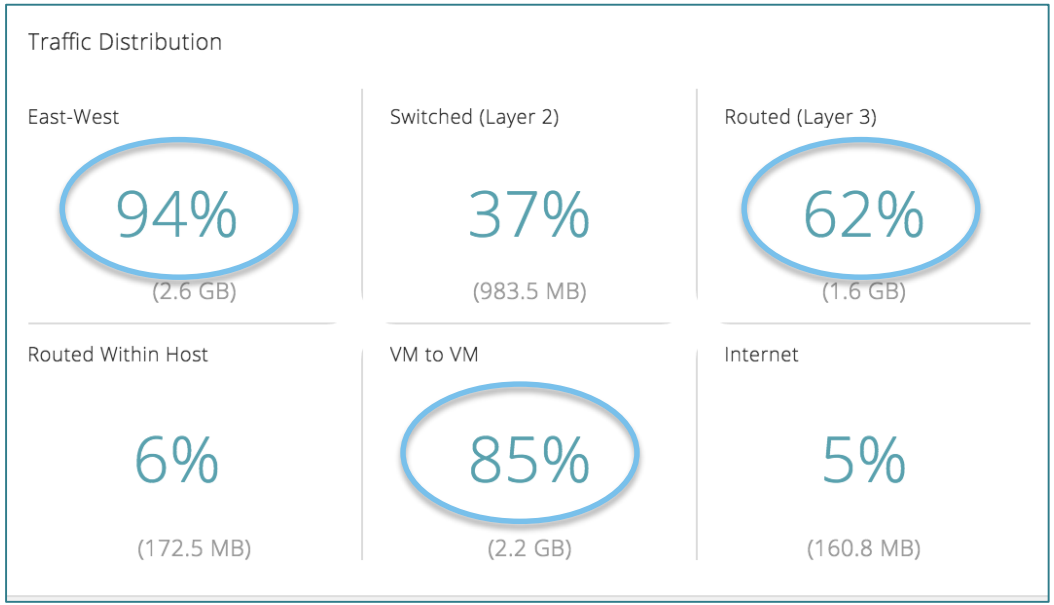
- Highly Connected
- Complex Service Protocols
- EP controls with weak isolation
- NW controls with weak context
- EP <-> NW mismatch

Complexity is the Problem!

- Misconfiguration is very common (Gartner: 95%* of FW breaches attributable to misconfiguration)
- *Gartner, Inc. “One Brand of Firewall Is a Best Practice for Most Enterprises”. November 28, 2012.
- *Gartner, Inc. “ …75 Percent of Mobile Security Breaches Will Be the Result of Mobile Application Misconfiguration” http://www.gartner.com/newsroom/id/2846017
- We need architecturally simplified security provisioning, operation, response and analytics.

Virtualization and the Softwarization of Security Controls: Enabling Policy Simplification

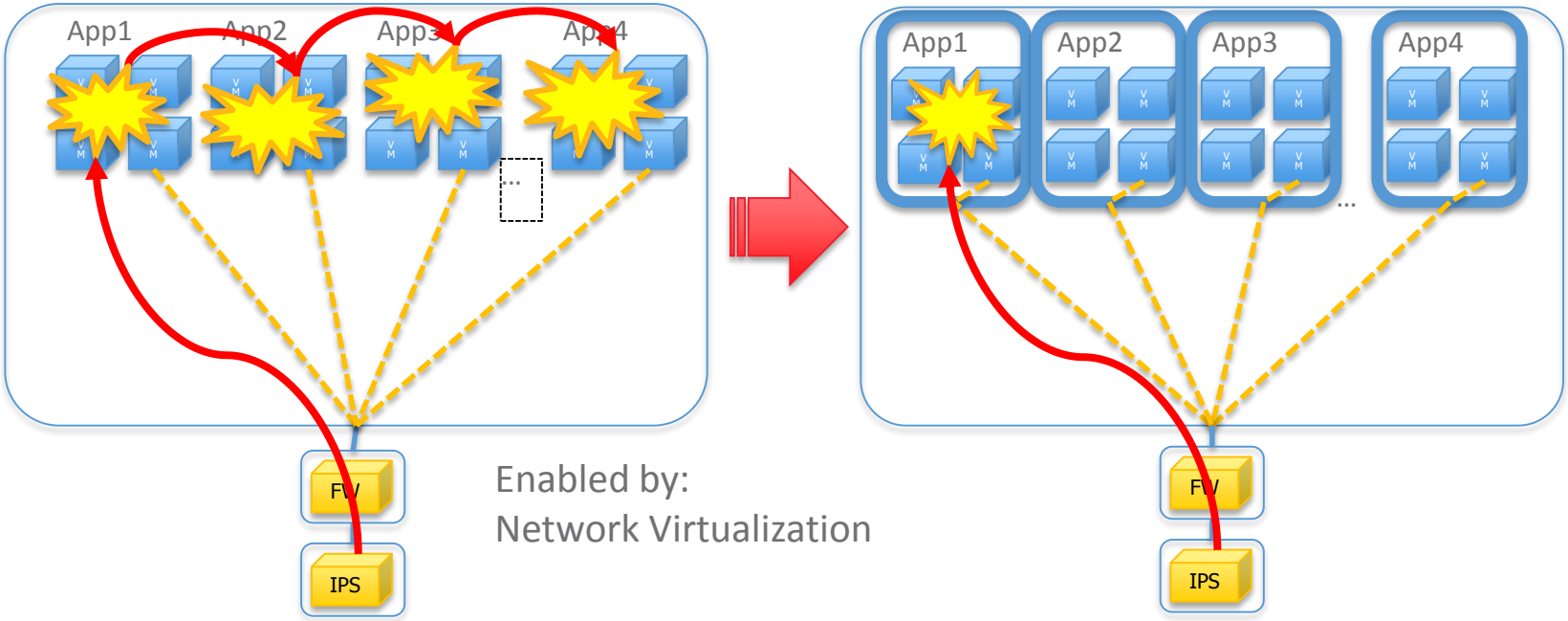
Visibility: Micro-segmentation and SW



Source: Networking data from Arkin.net deployments

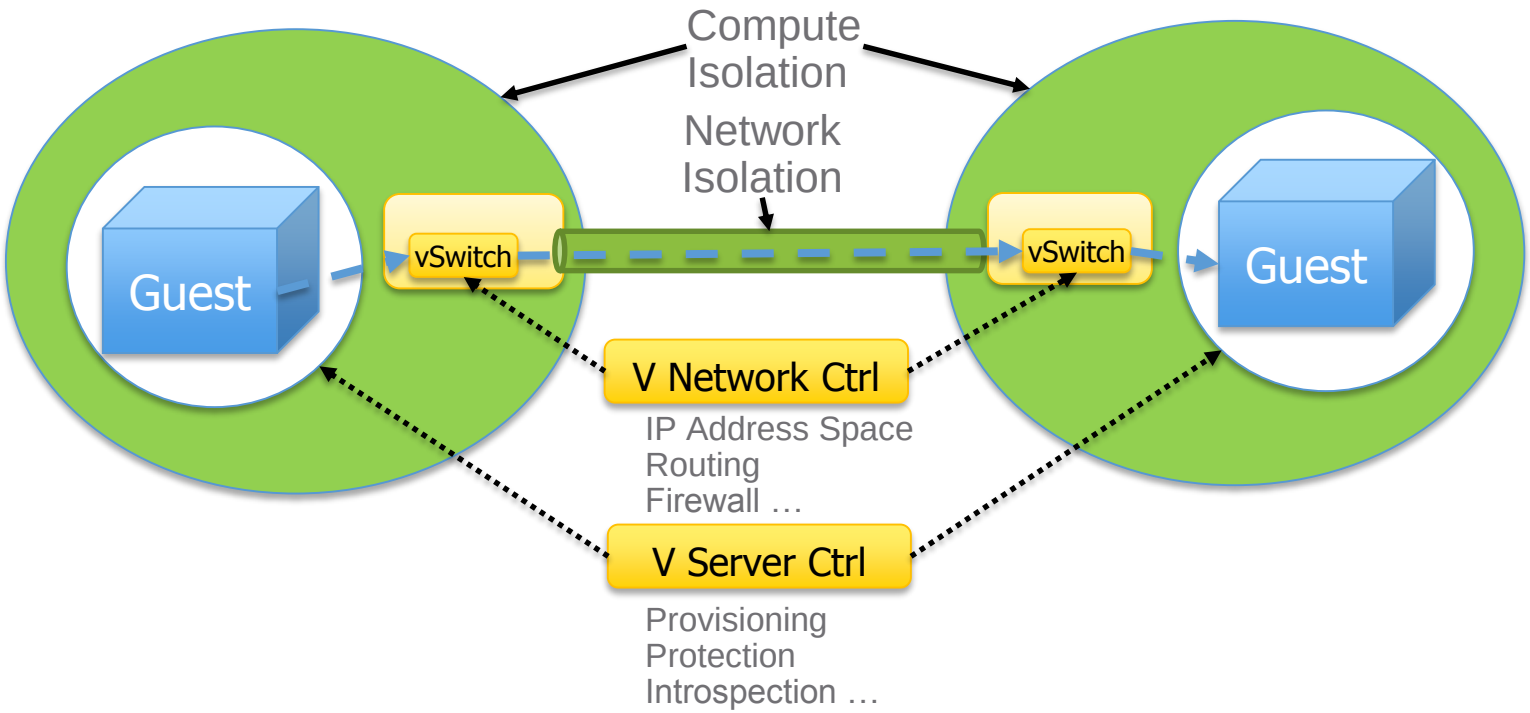
- Understand Traffic
- Here, > 80% is East-West
- Largely uninspected and unprotected
- Ops: Clearly not optimized

Containment & Protection

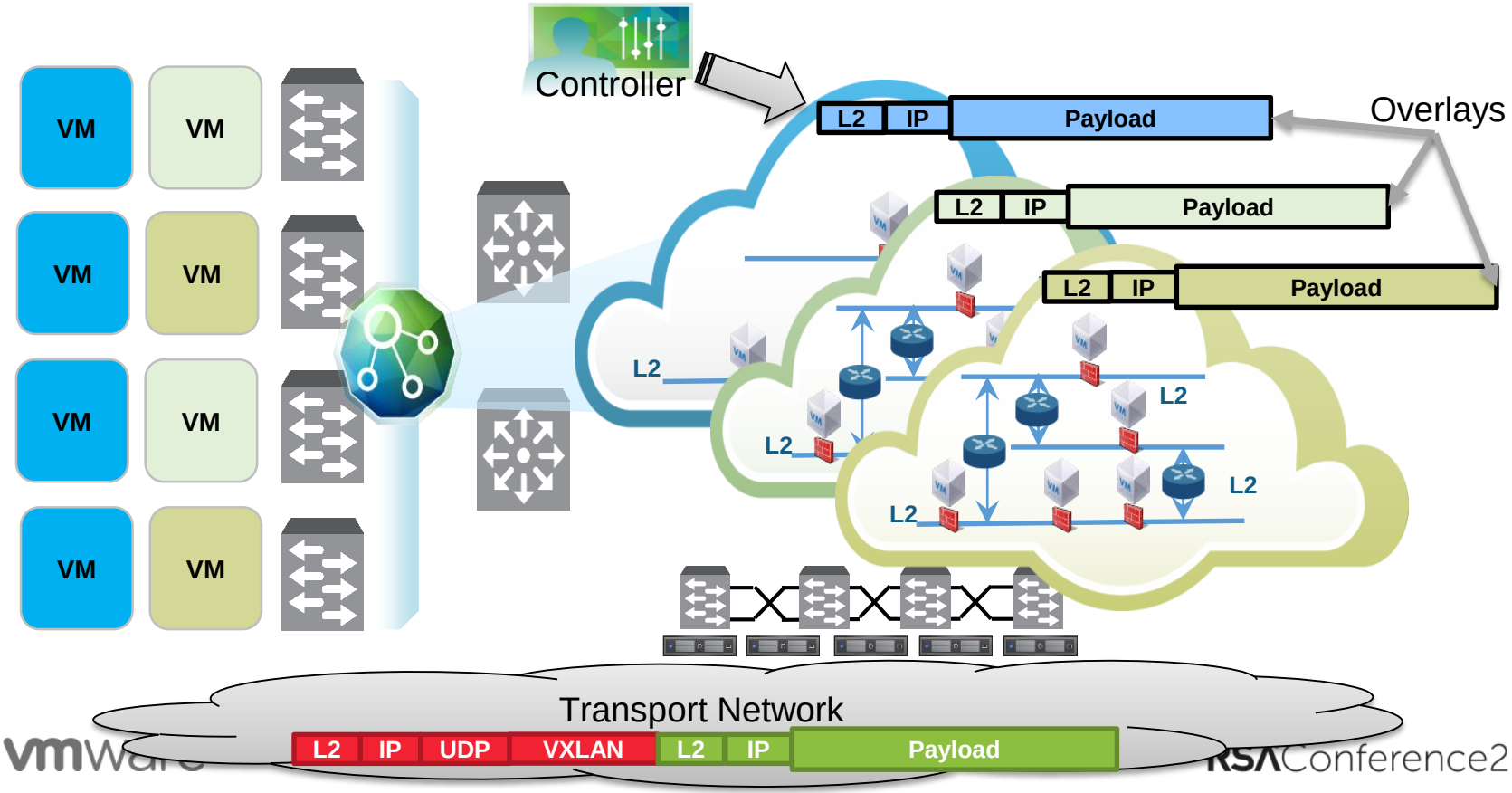


Enabled by:
Network Virtualization

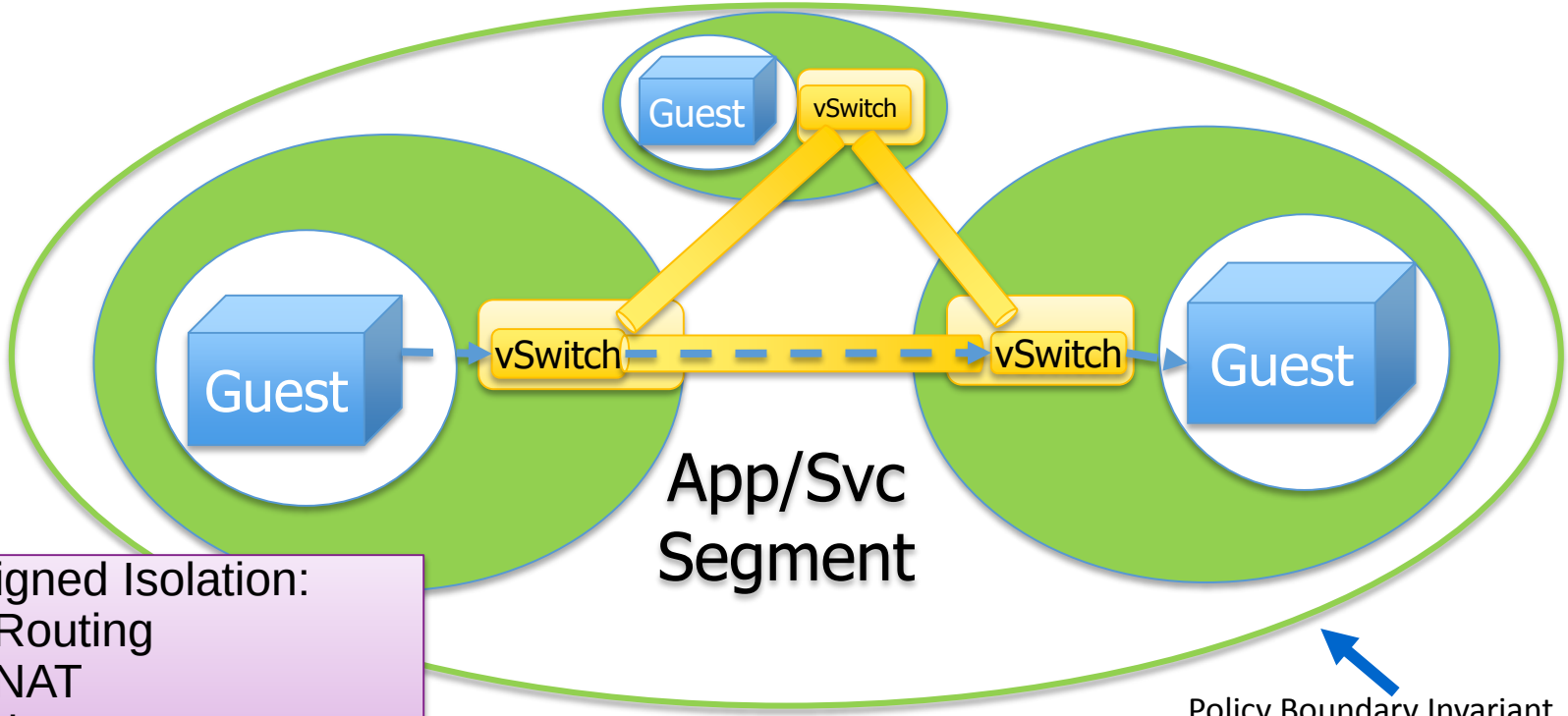
Network Virtualization



Network Virtualization: Overlays

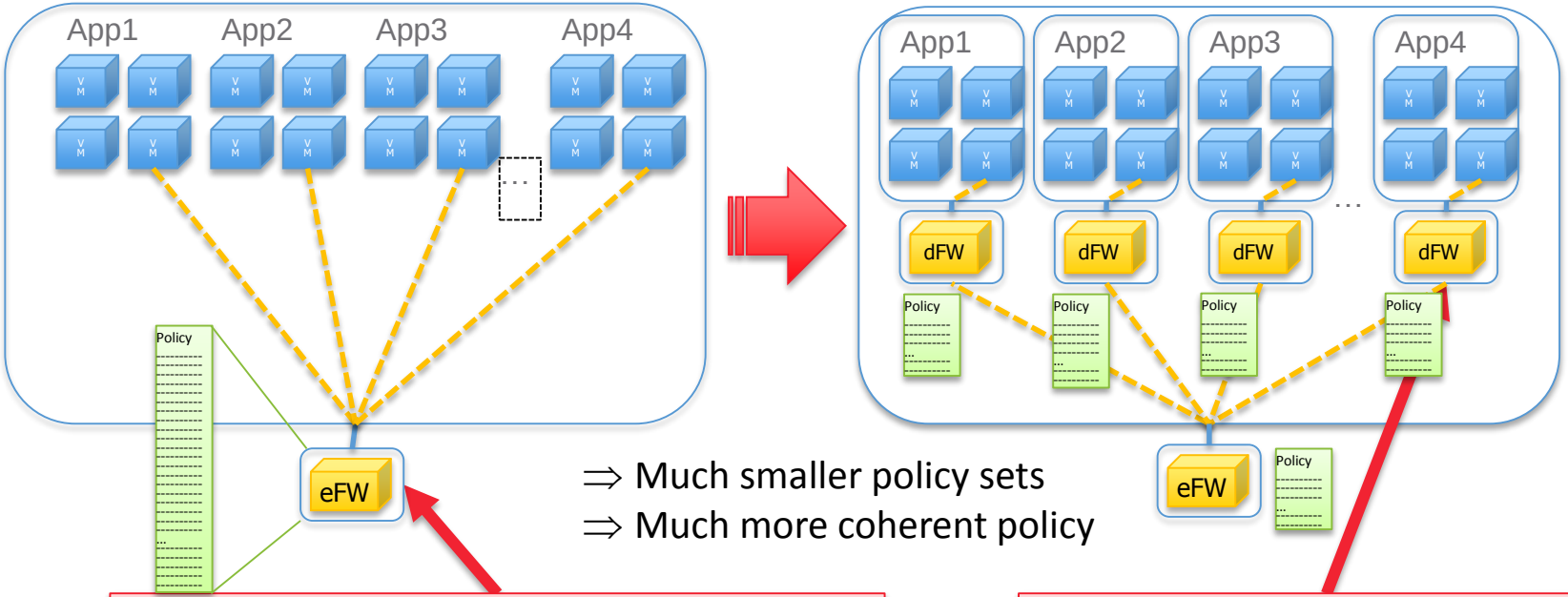


Micro-segments: A new policy primitive

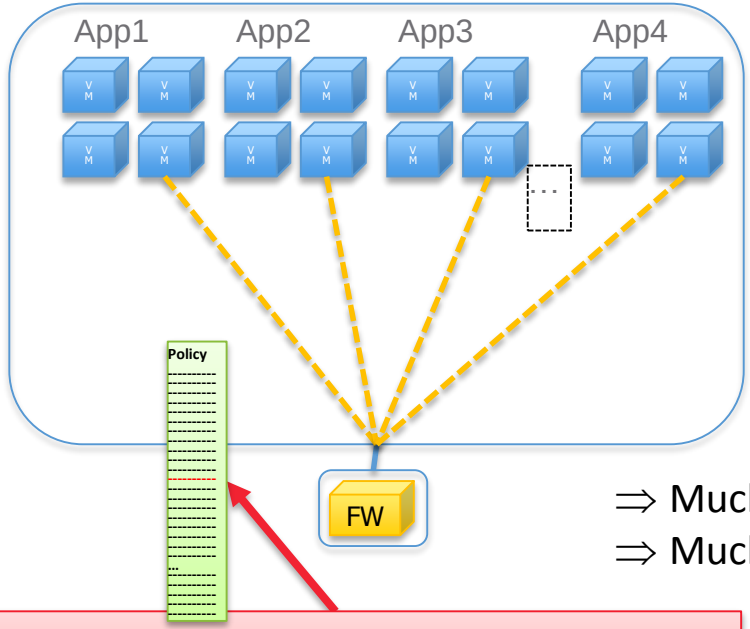


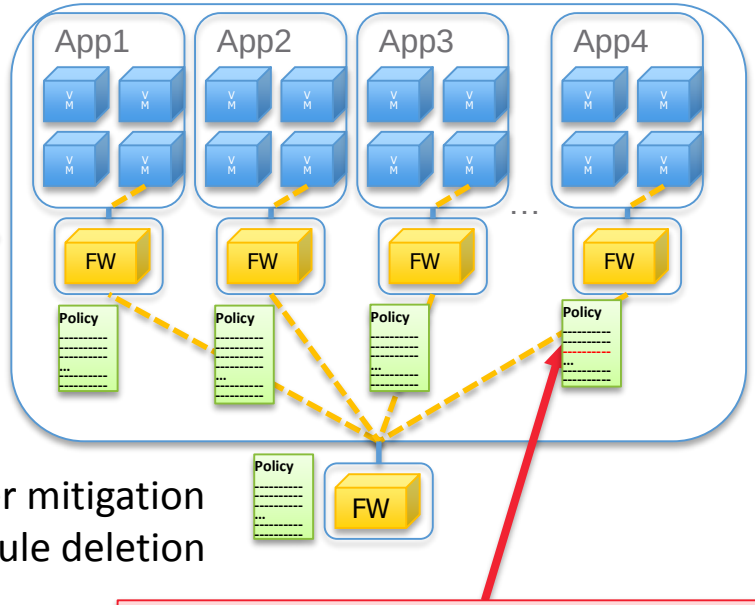
Aligned Isolation:
- Routing
- NAT
- dFW

Simplify: Smaller more aligned policy



Simplify: Change with less side effect



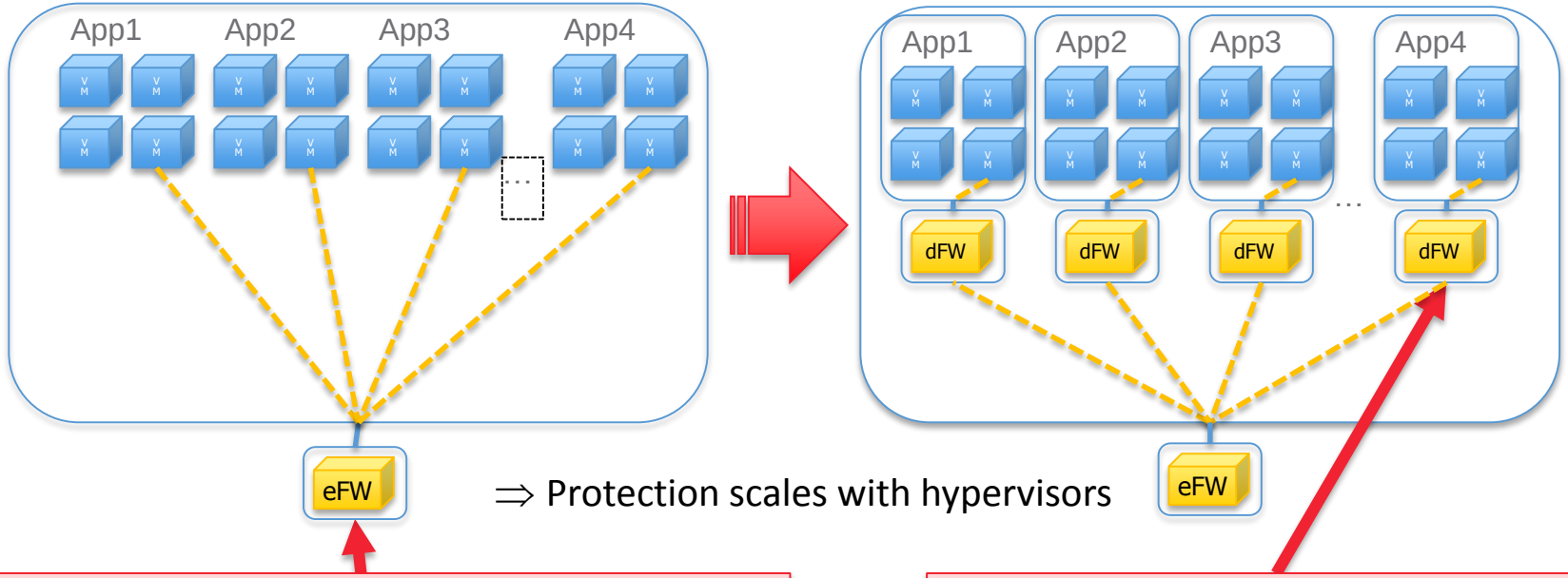


⇒ Much simpler mitigation
⇒ Much safer rule deletion

Policy change here is coupled across apps

Policy change here is far safer

Simplify: Policy that follows the workload

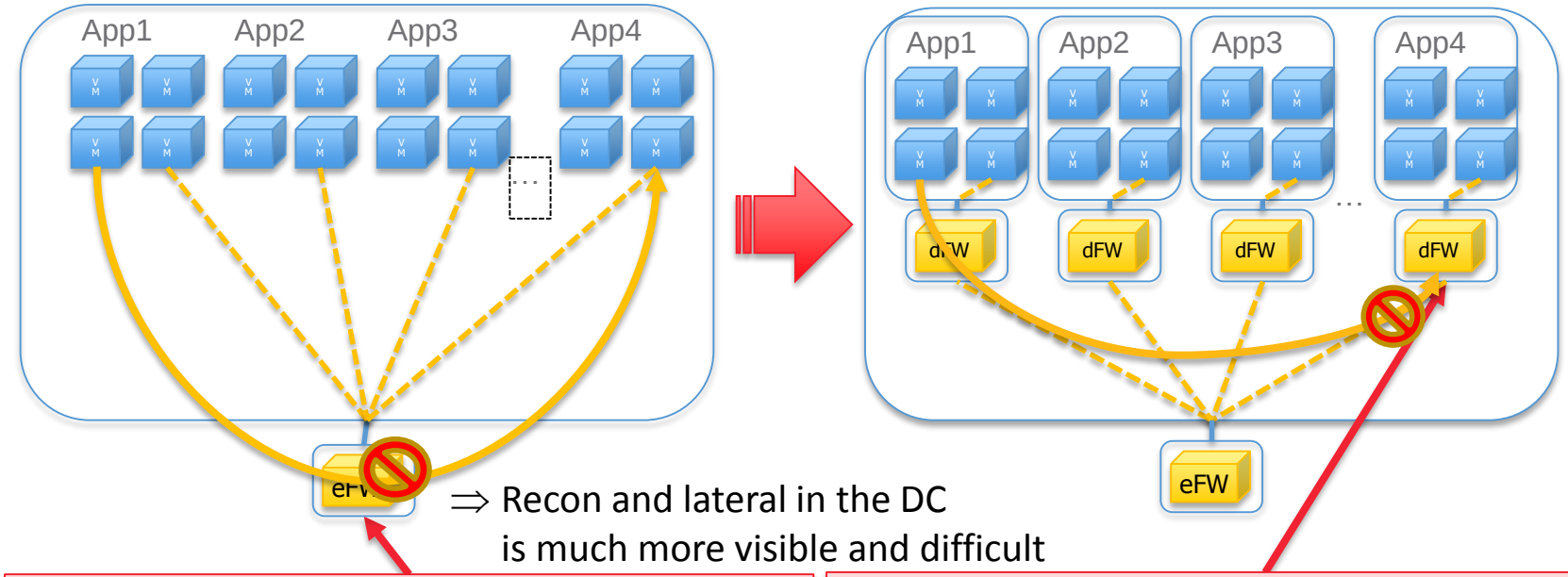


⇒ Protection scales with hypervisors

Only traffic steering determines protection/visibility

Classification (SG) determines protection & visibility

Simplify: Default deny posture

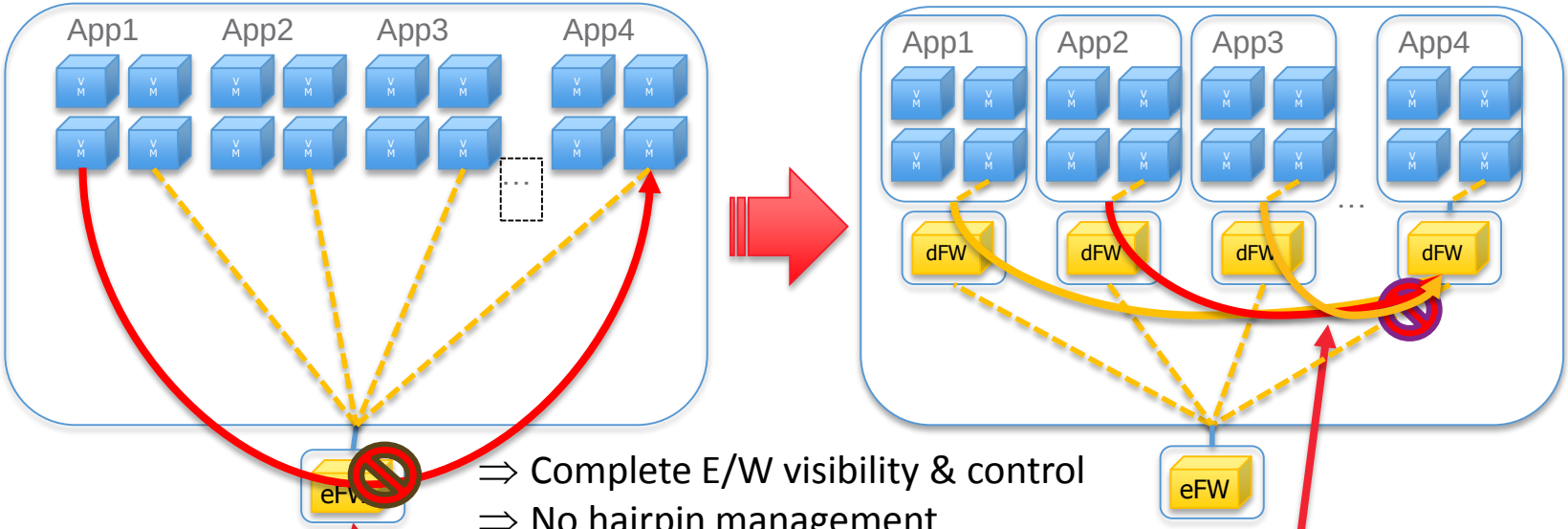


⇒ Recon and lateral in the DC is much more visible and difficult

Default deny policy here is blunt, coupled across apps, partial and weakly scale-able

Default deny policy here is precise, efficient, scale-able, …

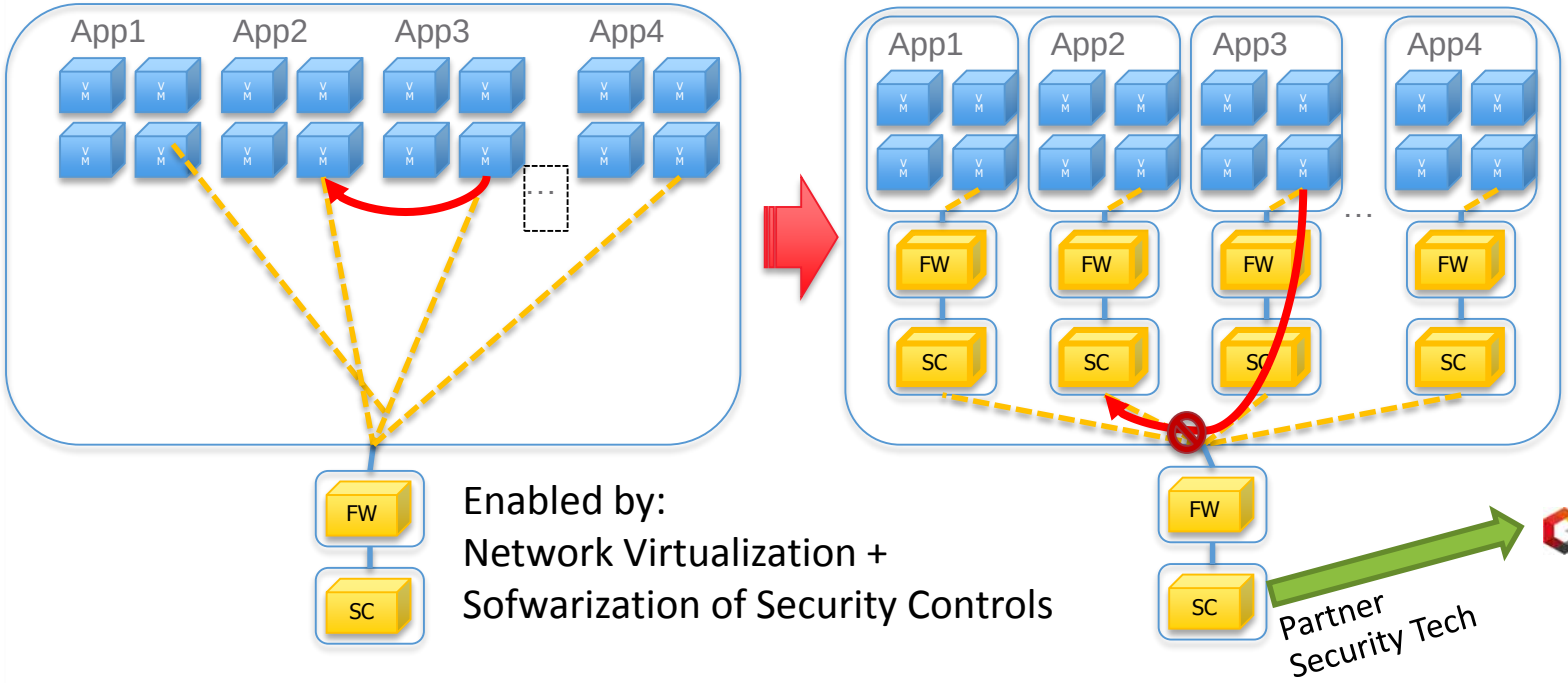
Simplify: Intrinsic E/W visibility/control



E/W traffic hair-pinned for visibility at the DC edge

All E/W traffic is visible and filtered according to policy

Control Placement and µSegments

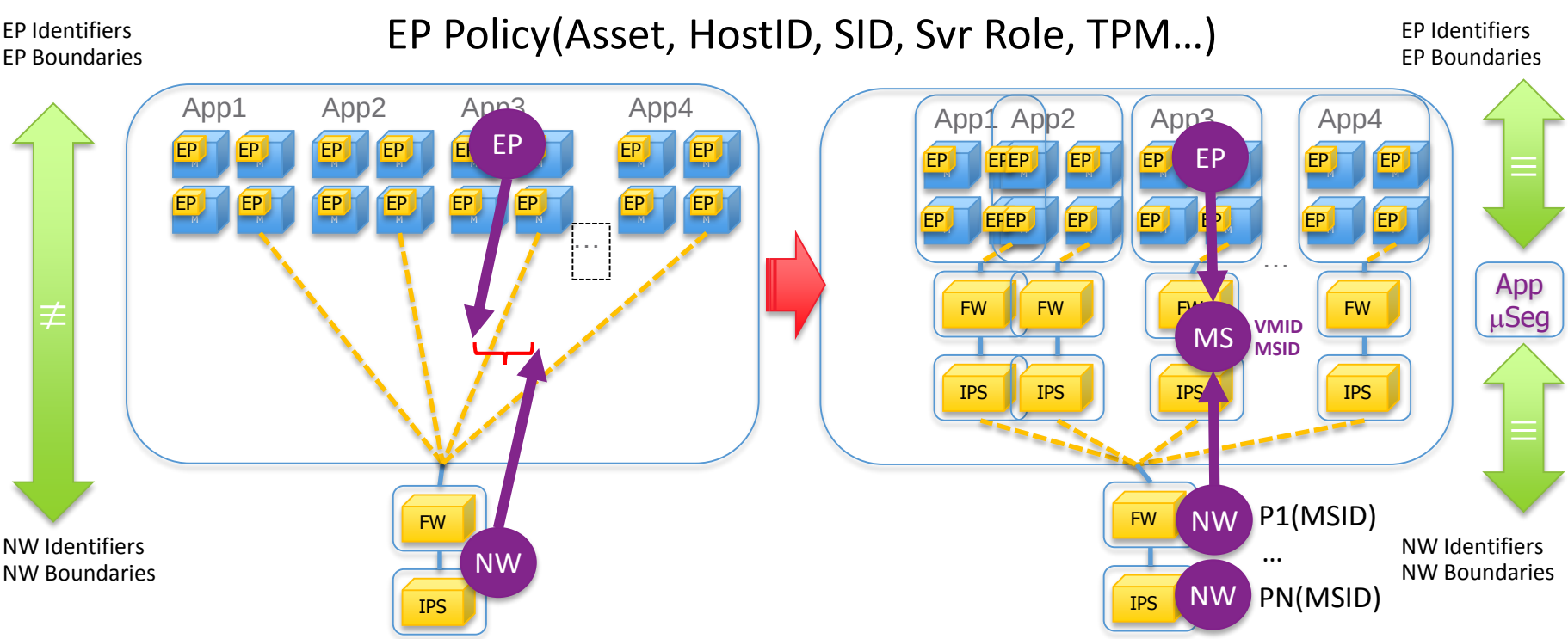


Enabled by:
Network Virtualization +
Sofwarization of Security Controls

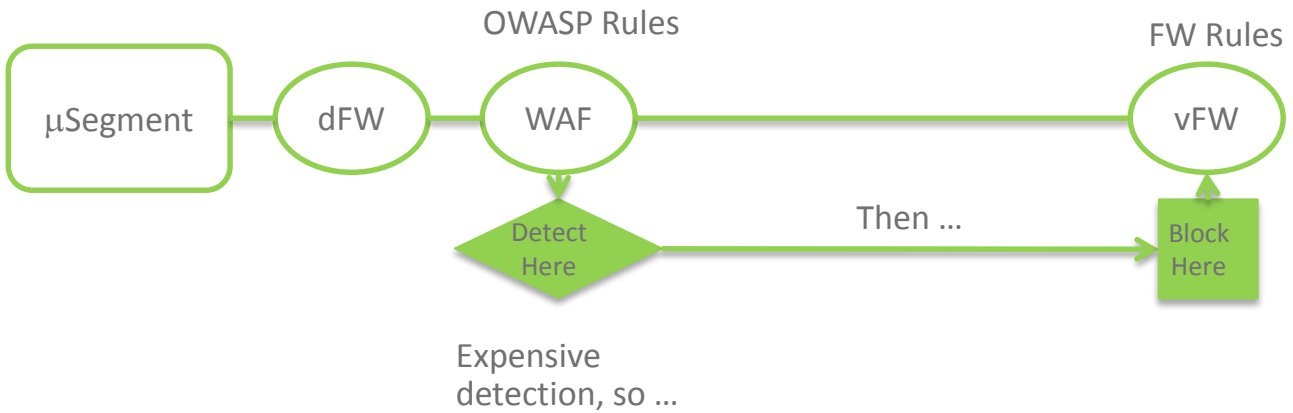
TREND MICRO
Symantec.
intel Security
paloalto NETWORKS
Check Point SOFTWARE TECHNOLOGIES LTD.
FORTINET
ARKIN
GuardiCore
VECTRA

Virtualization and the Softwarization of Security Controls: Improved Alignment

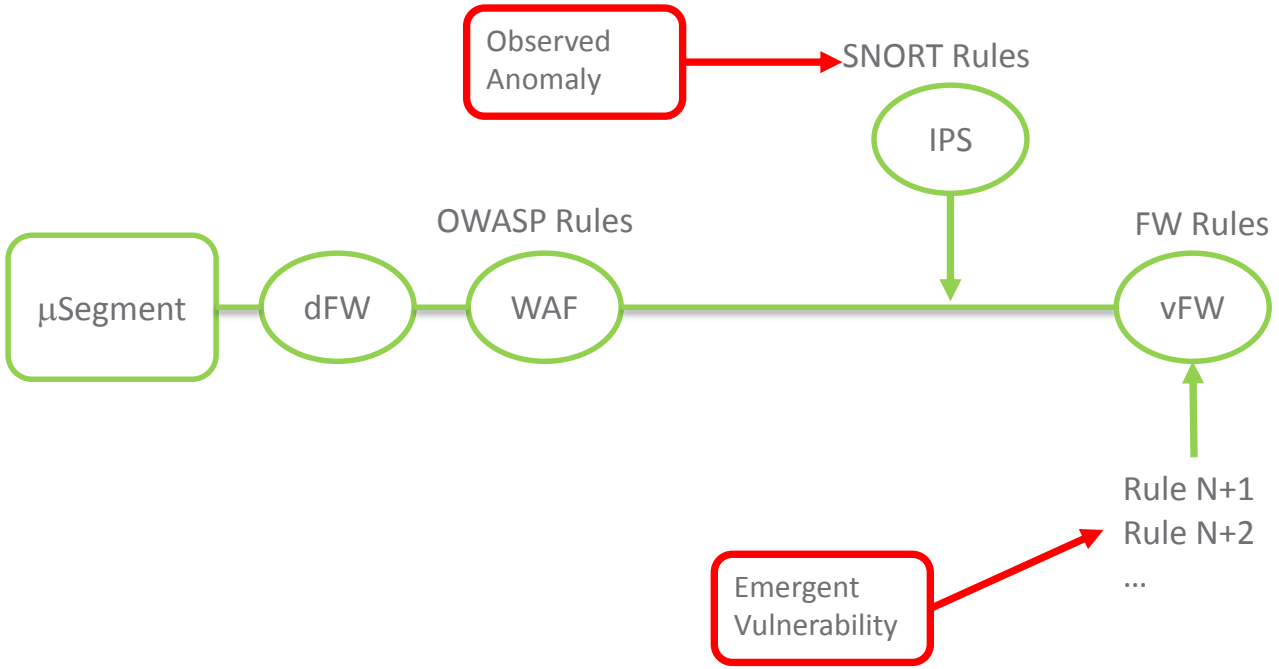
Align: NW/EP Control Aligned on µSegments



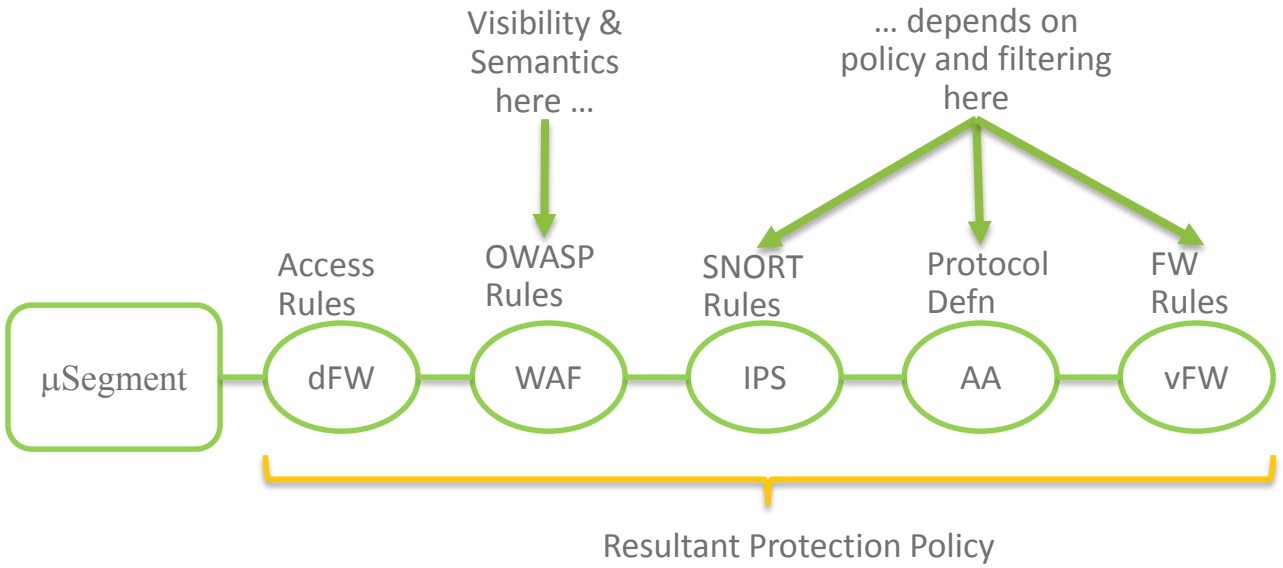
Align: Coordinated Controls



Align: Coordinated Controls



Align: Controls Context



Order Matters: So topological context is required for many security use cases.

Containers and Operationally Plausible Default Deny Policy

Sources of Plausible Micro-segment Policy

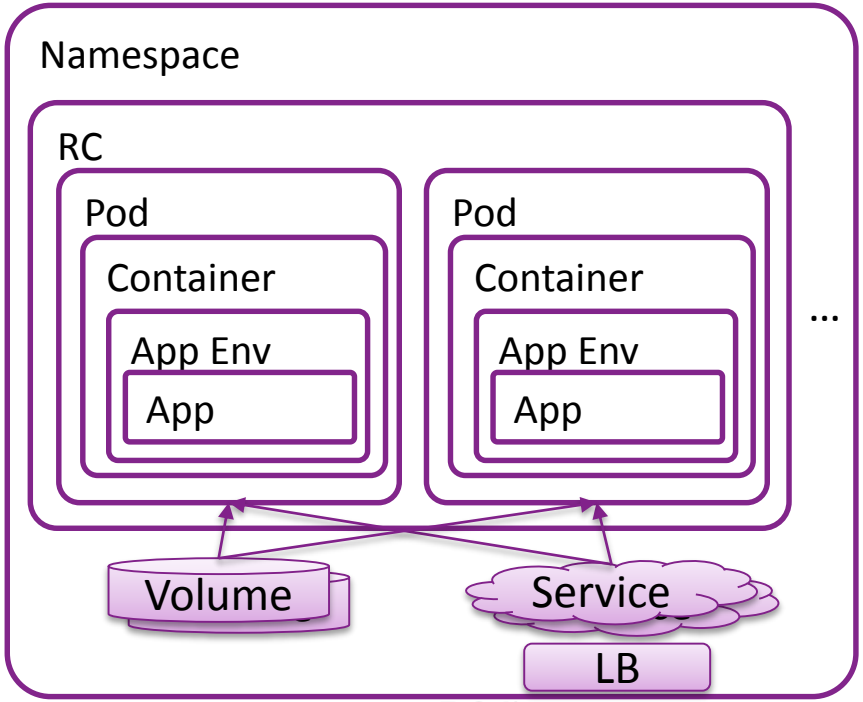
1. Provenance, Manifests & Provisioning Information
2. Application Network Behavior
3. Infrastructure Services (or Micro-services) Connectivity & Dynamics

Containers: App/Svc Focused Context

Ex. Authoritative Context

- App Configuration & Resources
- Resource Sharing Across Apps
- Colocation of Containers
- Service Components
- Services within a Namespace
- Network Dynamics (LB, HA, …)

Example Contextual Structure



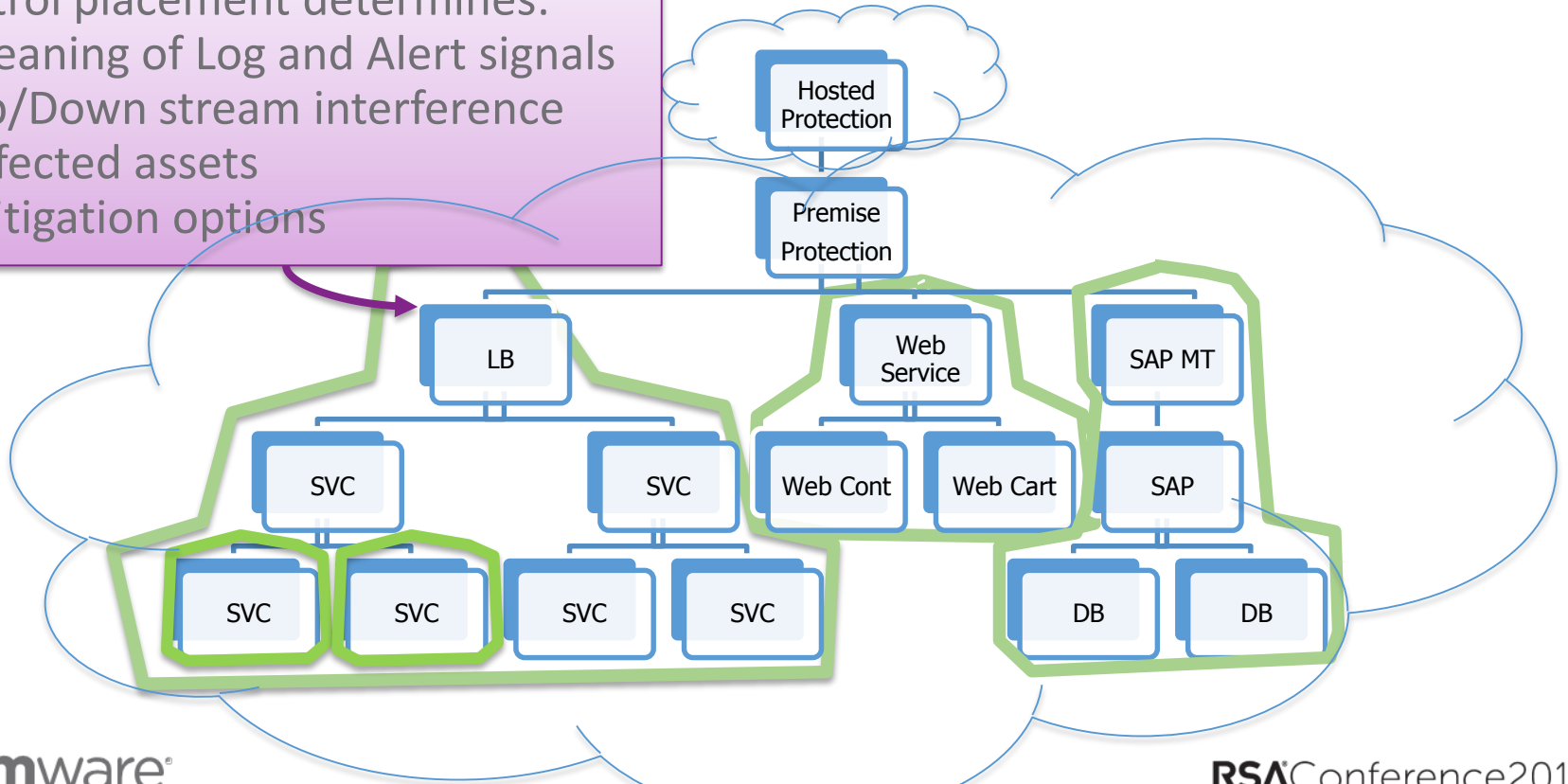
Containers: EP Compliance

Compliance scan of Docker image
    Usage: docker-oscap image IMAGE_NAME [OSCAP_ARGUMENTS]
Compliance scan of Docker container
    Usage: docker-oscap container CONTAINER_NAME [OSCAP_ARGUMENTS]
"Vulnerability scan of Docker image"
    Usage: docker\-oscap image\-cve IMAGE_NAME [--results oval-results-file.xml [--report report.html]]
"Vulnerability scap of Docker container"
    Usage: oscap-docker container-cve CONTAINER_NAME [--results oval-results-file.xml [--report report.html]]
Ref: https://github.com/OpenSCAP/container-compliance

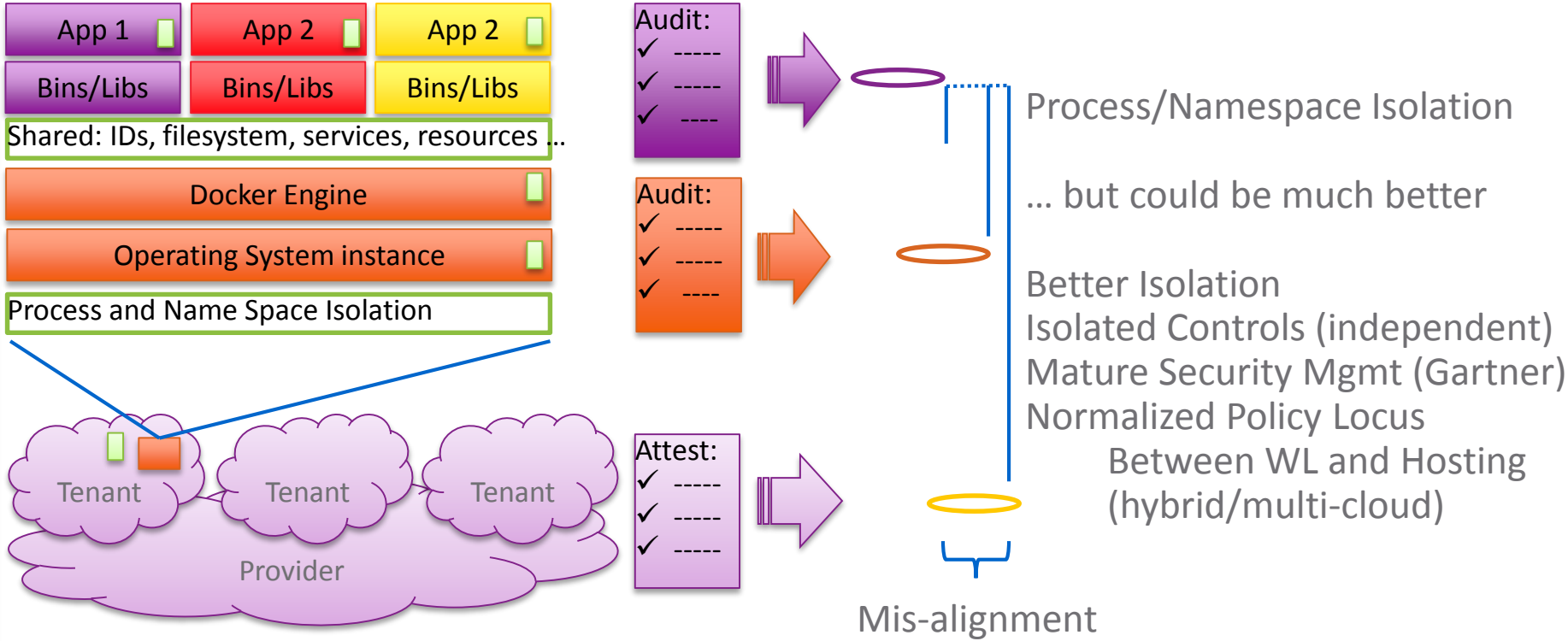
Alignment: Network Context

Control placement determines:

- Meaning of Log and Alert signals
- Up/Down stream interference
- Affected assets
- Mitigation options

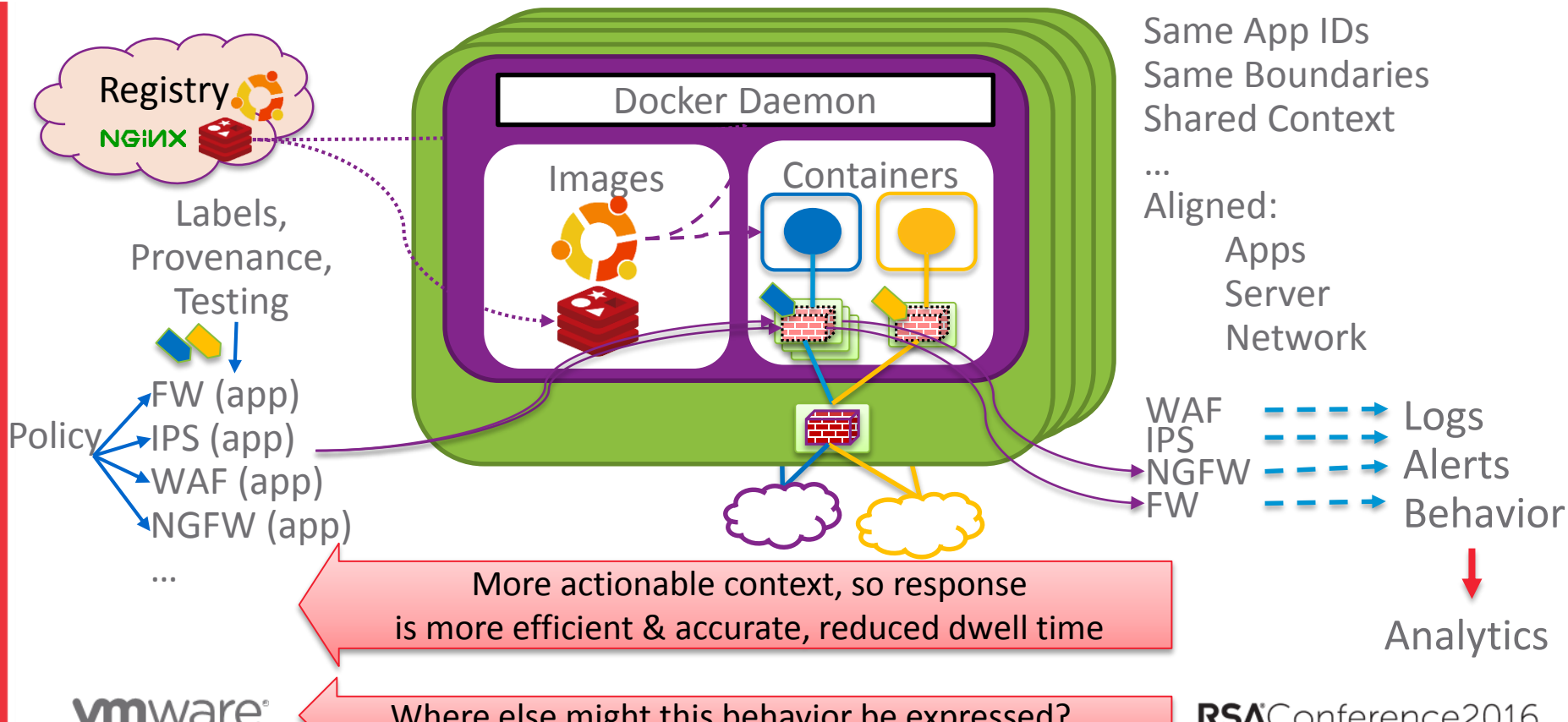


But “containers don’t contain”

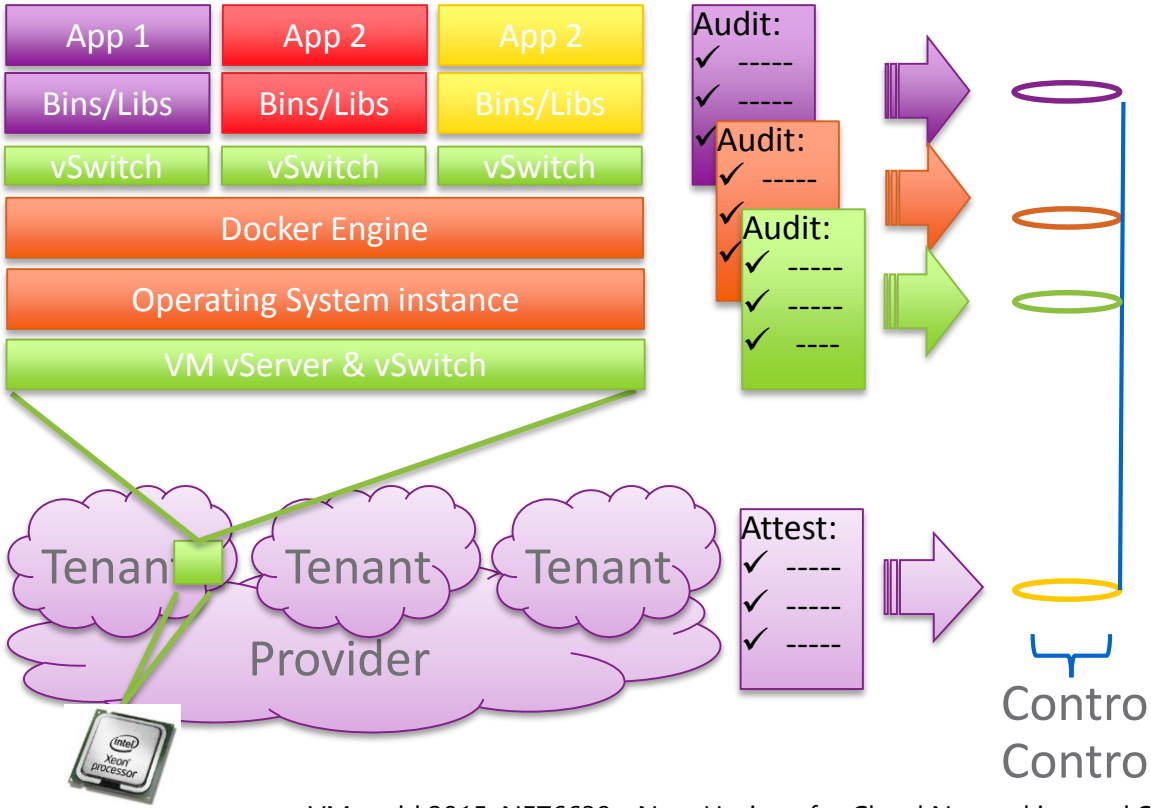


https://opensource.com/business/14/7/docker-security-selinux
http://www.projectatomic.io/blog/2014/09/yet-another-reason-containers-don-t-contain-kernel-keyrings/
http://blog.docker.com/2014/06/docker-container-breakout-proof-of-concept-exploit/
Gartner: Security Properties of Containers Managed by Docker

Directional: Containers + Virtualization



Containers + Virtualization



Consistent boundary X Stack
Same identifier (msid, vmid)
Alignment … in any state
Independent verification
Authoritative context (OOB)

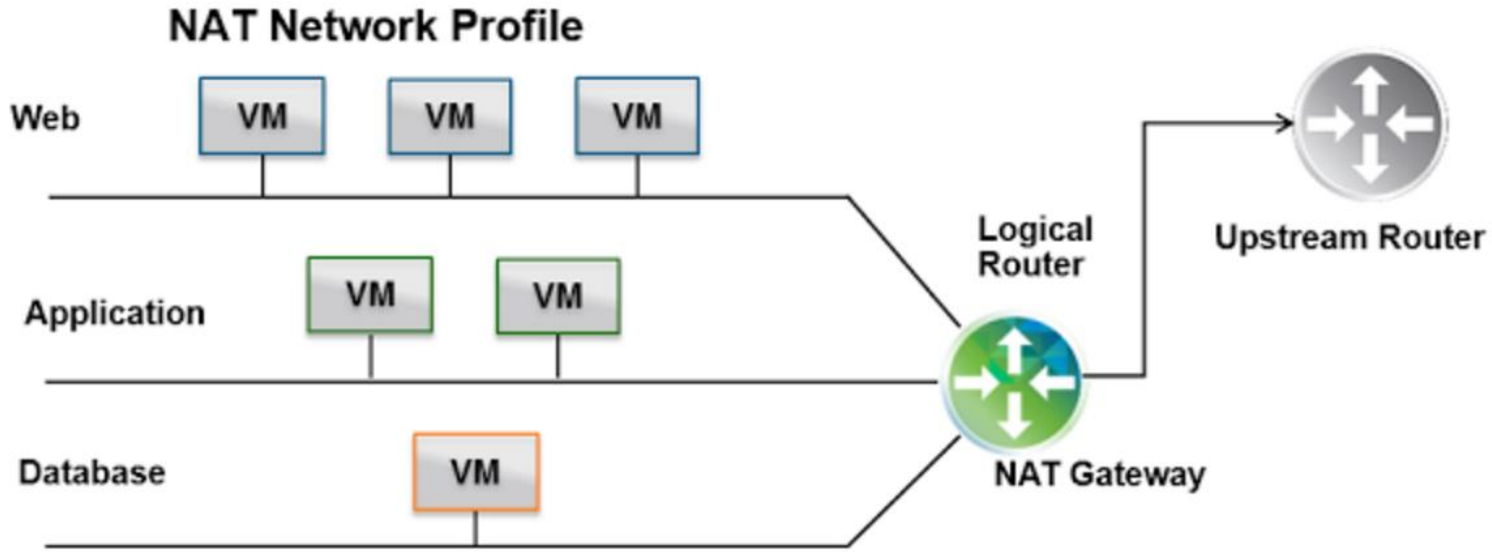
Control Boundary &
Controls Alignment

vmware

VMworld 2015: NET6639 - Next Horizon for Cloud Networking and Security:
https://www.youtube.com/watch?v=RBJ-KoAM-OQ&feature=youtu.be

Application Blueprint Example - vRealize

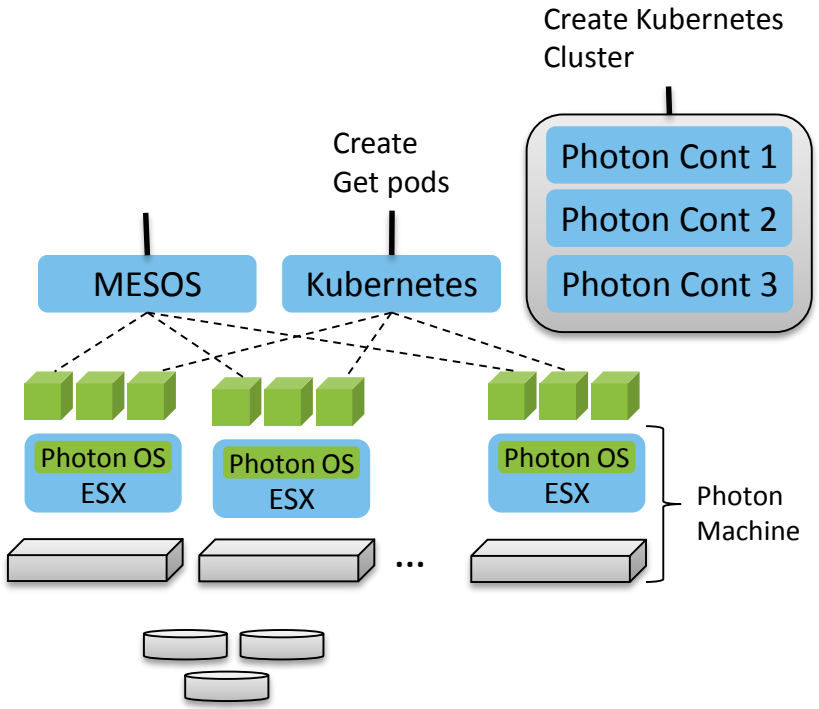
- Application structure and external connectivity are completely exposed to inform operationally plausible security policy



Enterprise Infrastructure & Containers

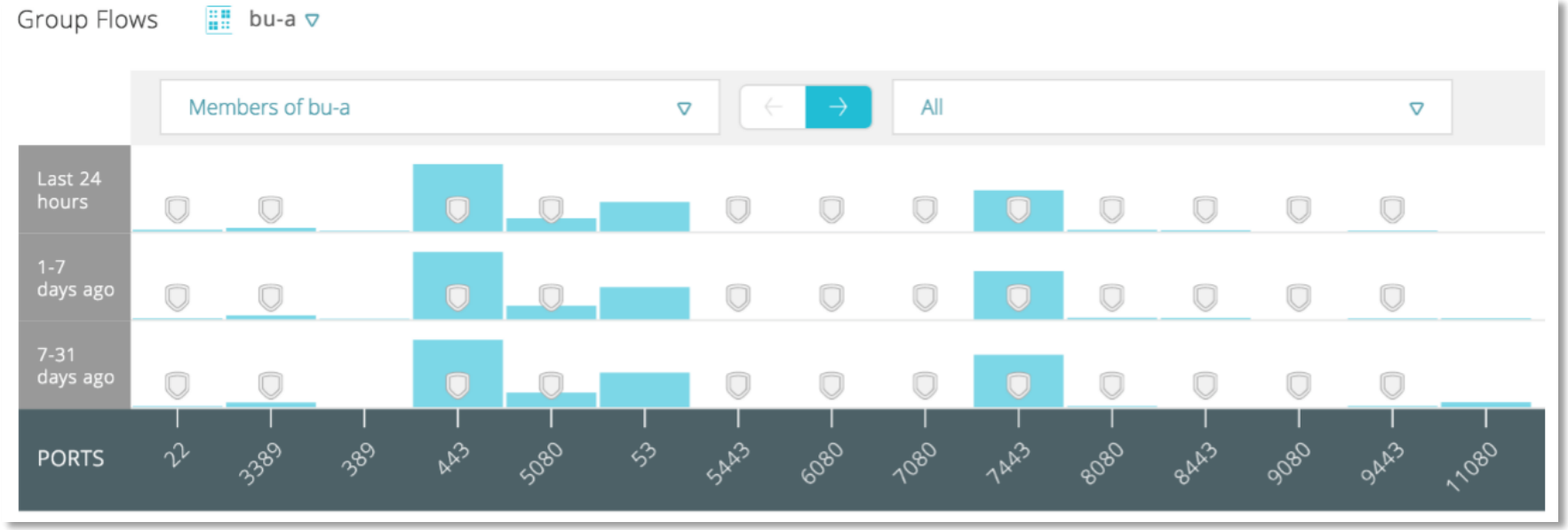
Infrastructural Context

- Leveraging of PBS, PBN, Infrastructural Services
- Legacy apps to cloud native apps, on the same infrastructure
- Integration of governance, CJA, context (for logs, alerts, response RCA, …)



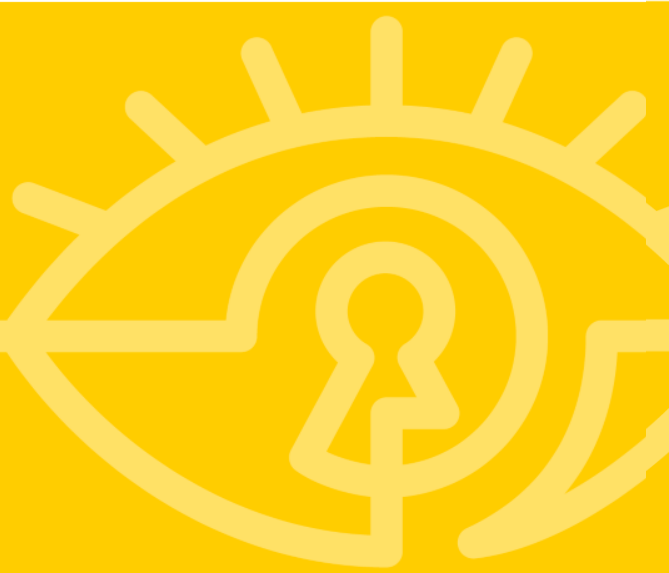
App Behavior Analysis: Arkin Example

Insight into application network behavior drives 1st order operationally plausible default deny posture.



Container

- Intrinsically Captures Application Structure, Provenance, and Classification (pre-launch)
- Always Current Configuration (immutability)
  - No “intended” vs. “actual” gap
  - Operations & Security perspectives
- Immutability accommodates “moving target” defense techniques
- Expose *implicit* network requirements in App context context.
- Expose *implicit* app deployment requirements
  - Level of req’d awareness of virtual network topology
  - Req’d SVCs

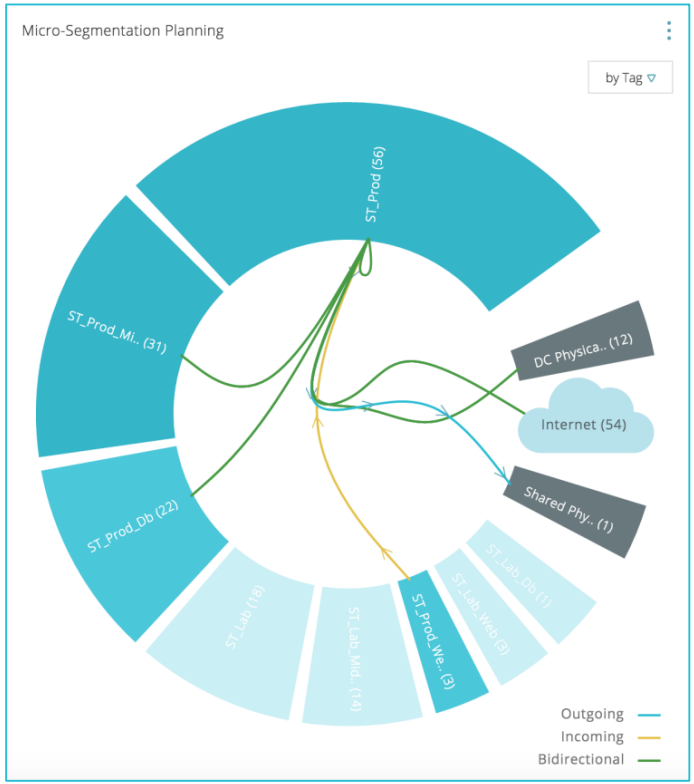


Refining Micro-Segmentation Using Analytics

Sources of Plausible Micro-segment Policy

1. Provenance, Manifests & Provisioning Information
2. Application Network Behavior
3. Infrastructure Services (or Micro-services) Connectivity & Dynamics

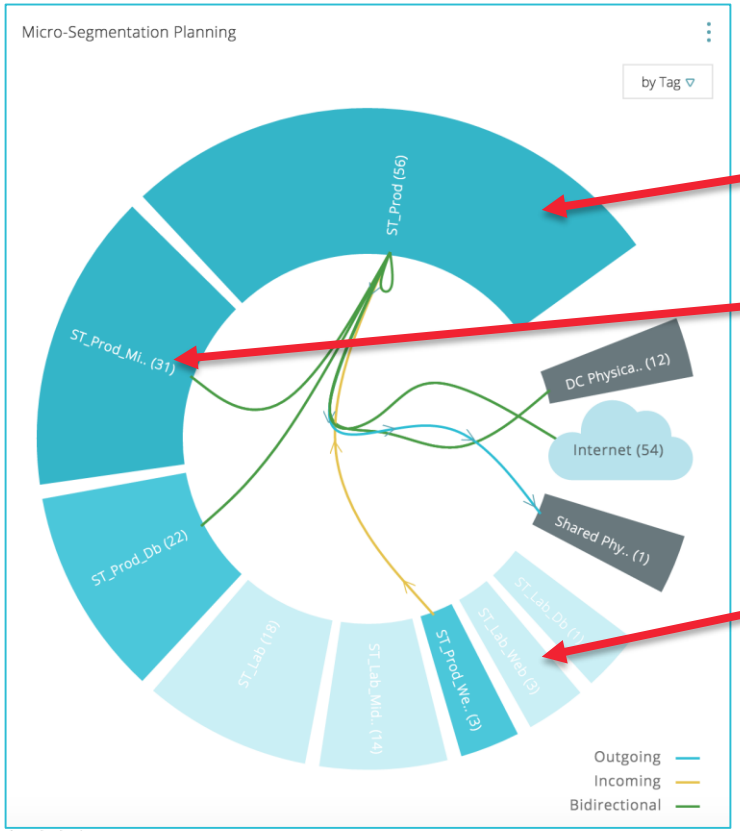
Micro-Segmentation: Model & Secure



- Model apps, app tiers, regulatory scopes, network, org boundaries, etc.
- Default Deny: Only allow what's necessary, Deny everything else.

Source: Arkin.net Screenshot

Micro-Segmentation in Action: Modeling Security Groups

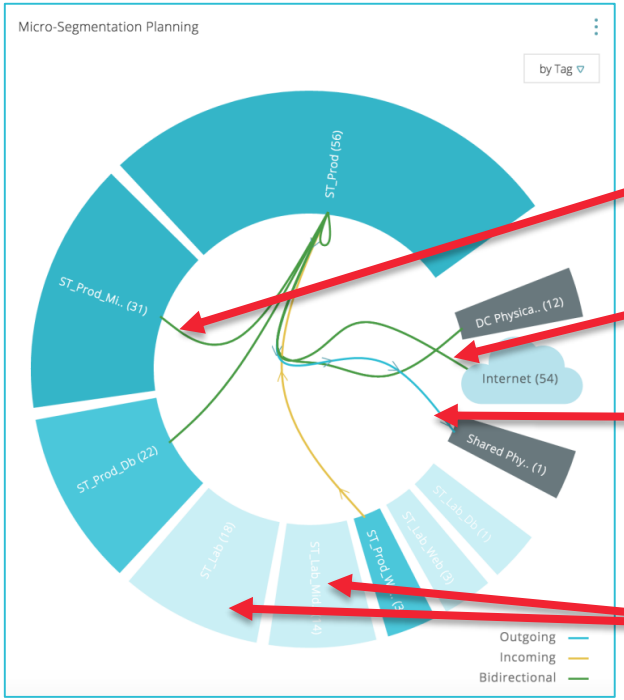


Segment by applications, app tiers, security zones, L2/L3 network boundaries, virtual-physical boundaries, organizational levels, etc

vmware

Source: Arkin.net Screenshot

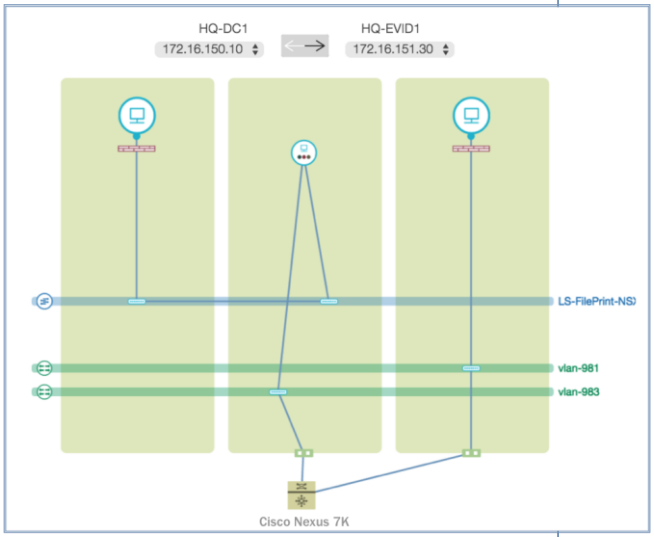
Micro-Segmentation in Action: Modeling Security Policies



Source: Arkin.net Screenshot

- Inter and Intra Segment (VM to VM) Communication
- Some services require internet access.
- Allowed access to shared services
- “Deny All” to these segments (…and confirm it)

Micro-Segmentation in Action: Validate Compliance



NSX Firewall (Firewall)

Applicable Firewall Rules Showing 5 of

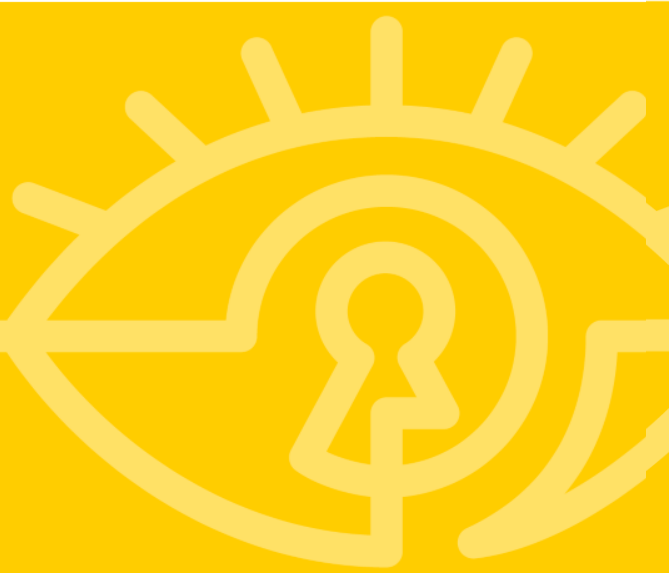
Seq ID	Name	Source	De			
2	File Print in	Any	Fi Sc			
3	File Print Out	FilePrint-SG	Any	Any	ALLOW	File Print :: NSX Service Composer - Firewall
16	Default Rule NDP	Any	Any	IPv6-ICMP Neighbor Solicitation, IPv6-ICMP Neighbor Advertisement	ALLOW	Default Section Layer3
17	Default Rule DHCP	Any	Any	DHCP-Client, DHCP-Server	ALLOW	Default Section Layer3

Applicable Firewall Redirect Rules Showing 3 of 3 (View all firewall rules)

Seq ID	Name	Source	Destination	Services	Action	Section Name
3	FilePrint-dynAdd	FilePrint-SG	Any	Any	DONT_REDIRECT	File Print :: NSX Service Composer - Network Introspection
6	Logical Switch IN	Any	Logical-Switch-SG	Any	REDIRECT	Logical-Switch-Palo-Security :: NSX Service Composer - Network Introspection
7	Logical Switch Out	Logical-Switch-SG	Any	Any	REDIRECT	Logical-Switch-Palo-Security :: NSX Service Composer - Network Introspection

Runtime Effective Policy between any two points in the Datacenter

Source: Arkin.net Screenshot



Summary

Summary

- Complexity is at the heart of today's security challenge
- Virtualization and Softwarization allows app focused placement and policy alignment
- Containerization provides the essential context for realizing an operationally plausible default deny policy
- This resulting in transformationally simpler policy and more effective protection.

Apply: Assess

When you return to work:

- Evaluate your current policy complexity
  - Policy set size
  - Policy testing workflow
- Estimate its effect on security policy management
  - Latency in security policy updates
  - Estimate the degree of your “default deny” posture
  - Identify related instances of policy misconfiguration

Apply: Dev Ops

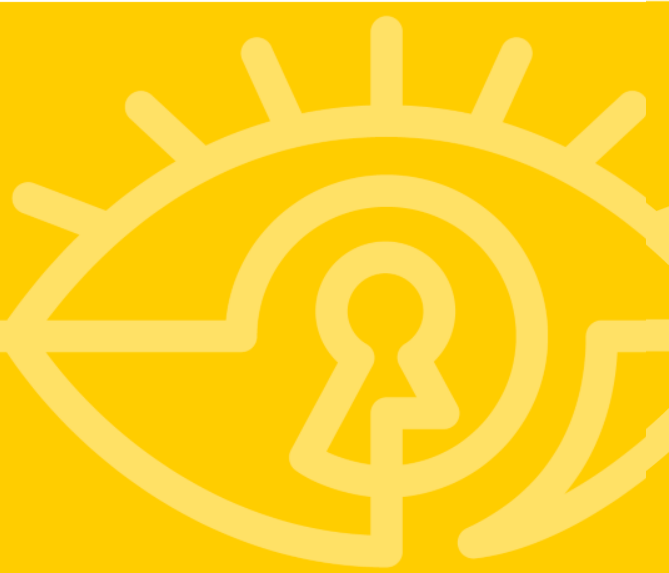
As move forward in DevOps:

- For selected applications determine
  - Operationally plausible default deny posture by observed logs
  - Application policy requirements from container blueprints/manifests
  - Application component dynamics: continuity, scaling, …
- For important and cross application cutting services
  - Document discovery, election, failover, … protocol dynamics

Apply: Plausible Micro-segment Policy

Plausible Policy Information Sources

1. Provenance, Manifests & Provisioning Information
2. Application Network Behavior
3. Infrastructure Services (or Micro-services) Connectivity & Dynamics



Thank You!

Questions?

Dennis R Moreau: dmoreau@vmware.com