RSAConference2016

Abu Dhabi | 15–16 November | Emirates Palace

SESSION ID: CCS-T08

Virtual Machines vs. Containers vs. Unikernels: The Security Face-Offs

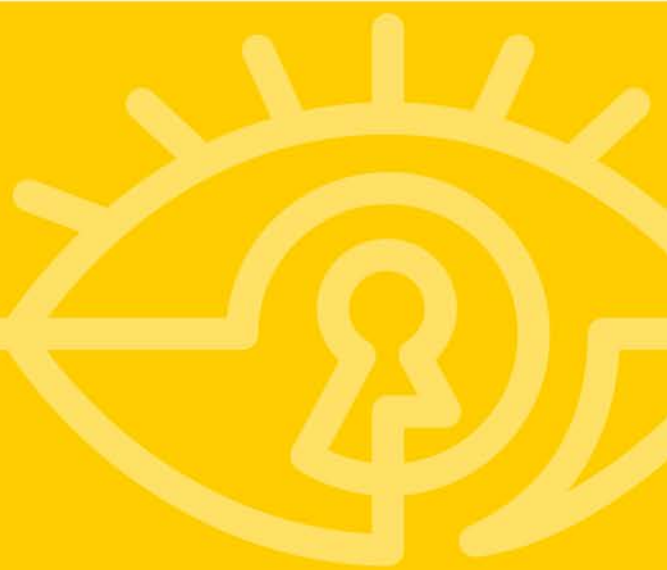
Samir Saklikar

Technical Lead,
Office of the CTO, Security Group,
Cisco

#RSAC

Agenda

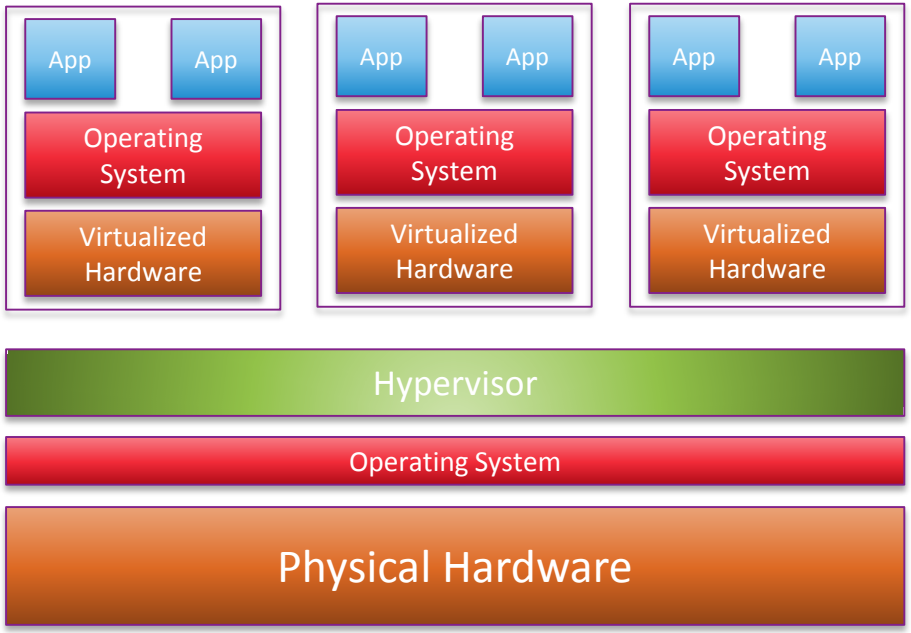
- Workload Execution Environments
  - Virtualization, Containers, Unikernels
- A Security Requirements Template
- Built-In Security Defenses of Workload Execution Units
- Applying Higher Level Security Policy to Workloads
- Apply



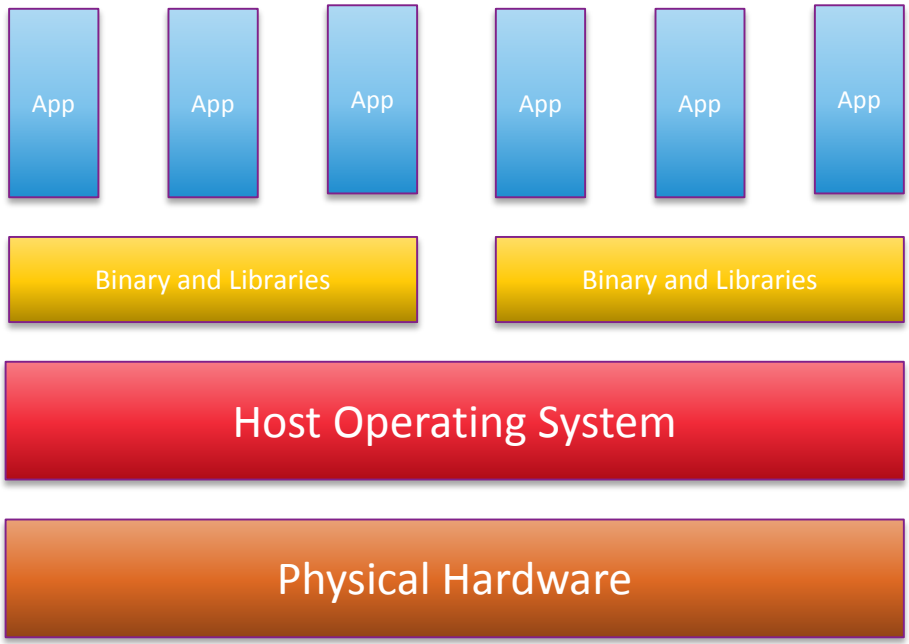
What are we working with?

Heterogeneous Multi Form-Factor Workload Execution Units

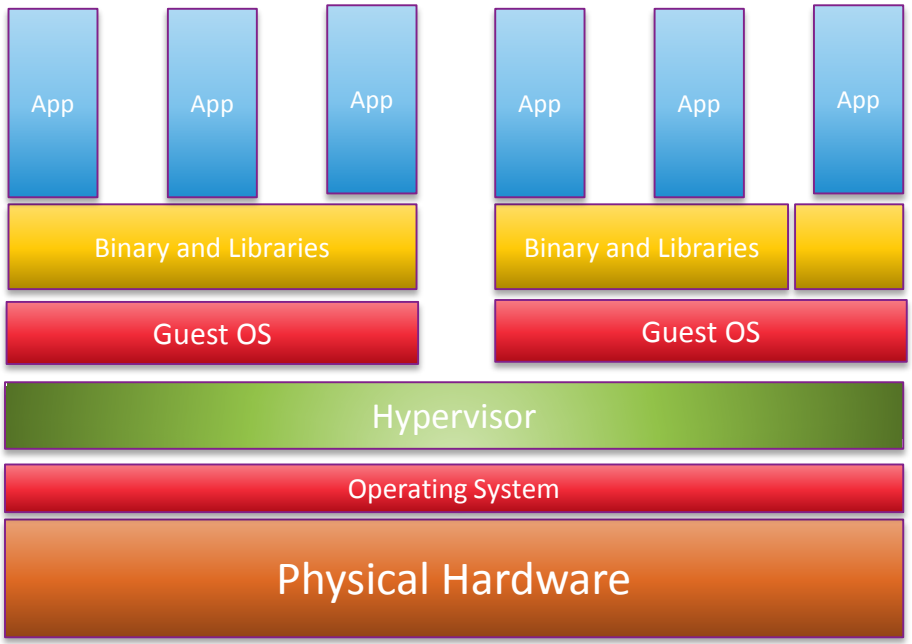
Virtual Machines



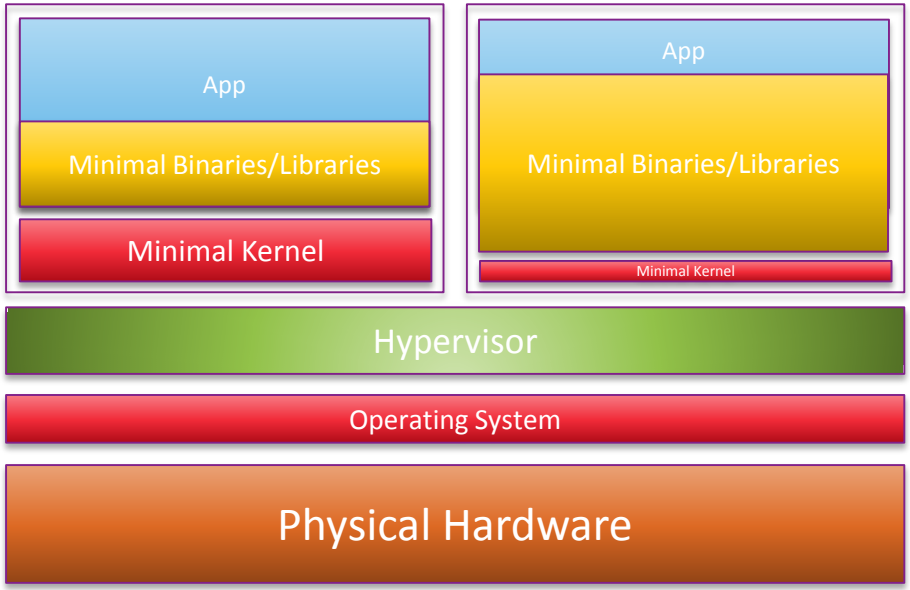
Containers

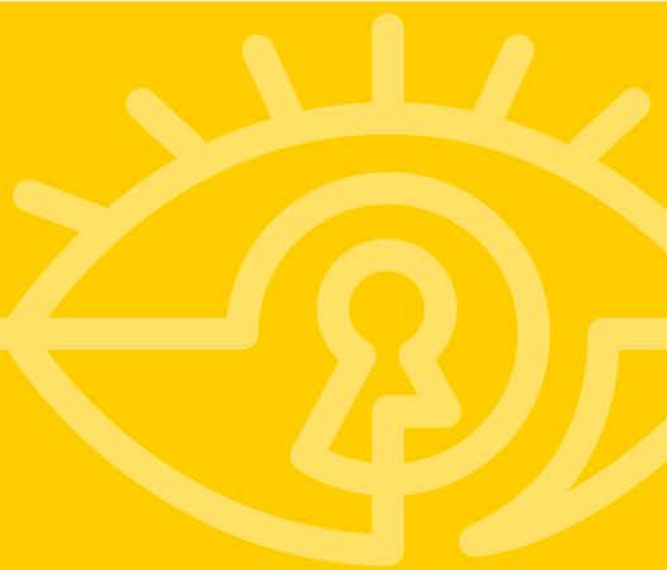


Containers within VMs (for Tenant Isolation)



Unikernels (Specialized Kernel)





What do we want ?

Our Security Requirements

What is “Security” for Workloads?

Protect one-self?

”Well-Behaved” applications?

Policy Compliance

Defense against Attacks?

“Whole is Greater than Sum of its Parts”

Built-In Standalone Defense Mechanisms

Orchestrated Security Defense Mechanisms

Built-In Standalone Defense Mechanisms

- Software Hardening
  - Security Audits, Security Upgrades
- Strong Root of Trust
- Granular Access Control Model
- Easy Composability

Orchestrated Security Defense

- Driven by a higher level Operational Policy
  - Business Rule, Compliance Policy, Reactive Action
- Collaborative Defense with real-time Intelligence Sharing
- Unified Management across hybrid deployments
- Full Stack Visibility and Behavioral Analytics
- Easy Re-Composability

A Security Requirements Template

Smaller Footprint, Better Security Audit and Hardening

Built-in Protection, Access Control, Permissions, Capabilities

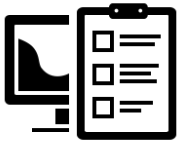
Hardened Workload Execution Environment

Business-Centric Identity and Rights Management

Operational Policy, Compliance Rules

Workload Isolation, Firewalls, Access Control

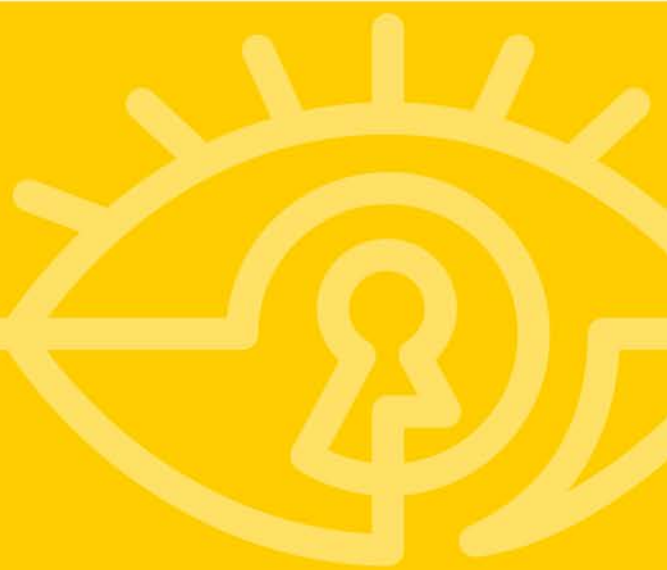
Workload Security Life Cycle



Unified Management, Auditing, Remediation Plans

Data Protection, Encryption, Access Control

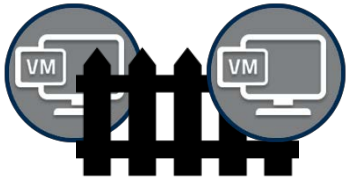
Federated Access, Secure Cloud Deployments



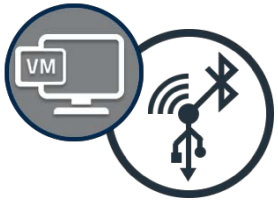
Built-In Security Defenses

Fundamental Security Capabilities of Workload Environments

VM Security (aka Hypervisor Security)

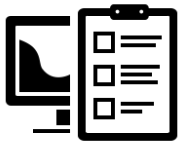


Execution Isolation



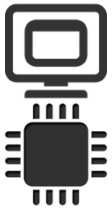
Devices Emulation & Access Control

Privileged Operations



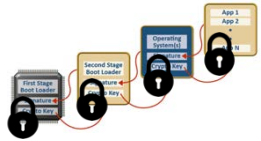
Management

Security Audit & Hardening



Hardware Assisted Virtualization

Granular Access Control

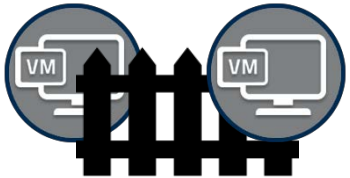


Secure Trusted Boot

Hypervisor Security (cont.)

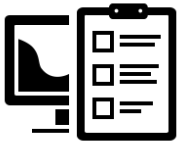
- Other Recommendations…
  - Configuration Versioning with Rollbacks
  - Regular Security Updates and Patches
  - Secure Configuration of Built-in Firewall
  - Segregating VM Management and Hypervisor Host and VM Traffic
  - More at NIST Publication - “Security Recommendations for Hypervisor Deployment”

Container Security

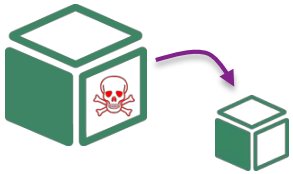


Execution Isolation

Privileged Operations



Management



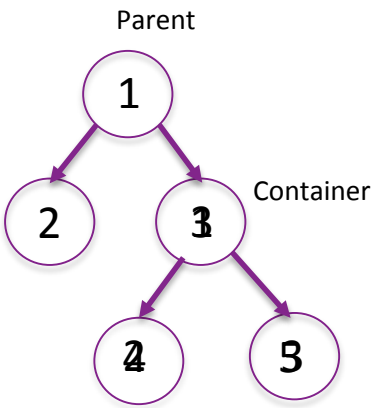
Reduced Attack Surface

Security Audit & Hardening

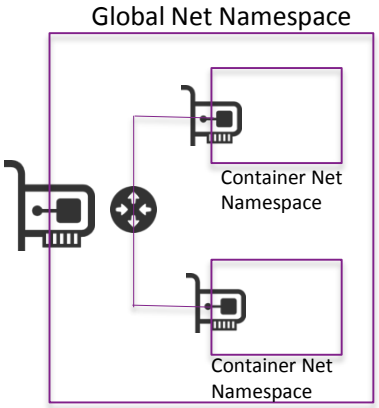
Granular Access Control

Vulnerability Management

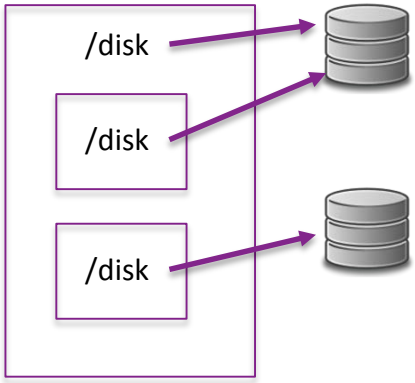
Nuts & Bolts: Linux Namespaces



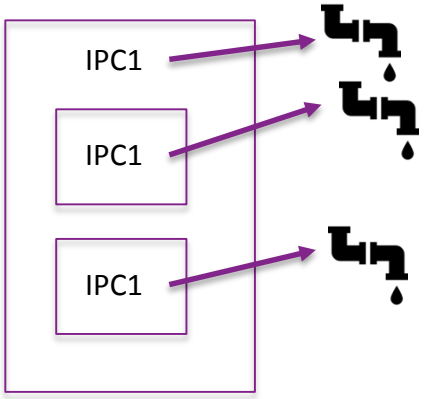
PID Namespaces



Network Namespaces

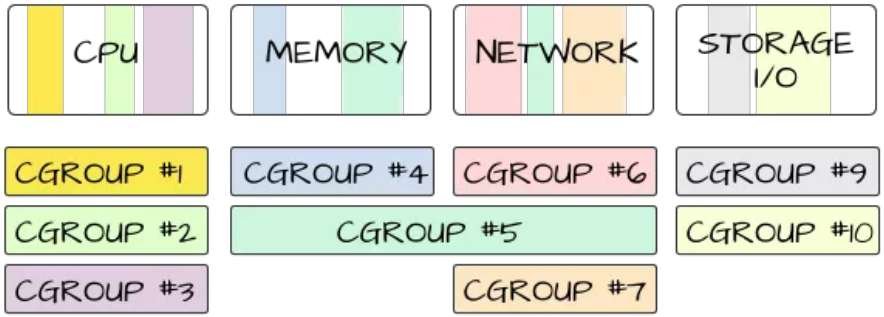


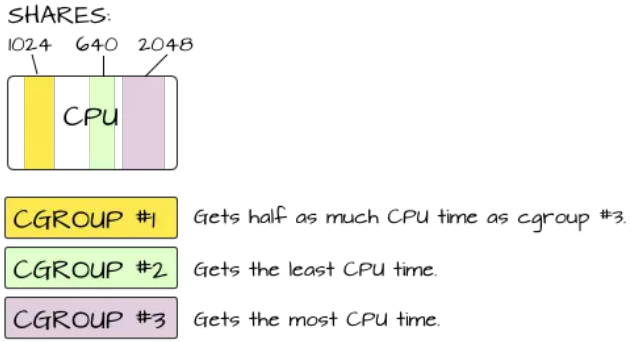
Mount Namespaces



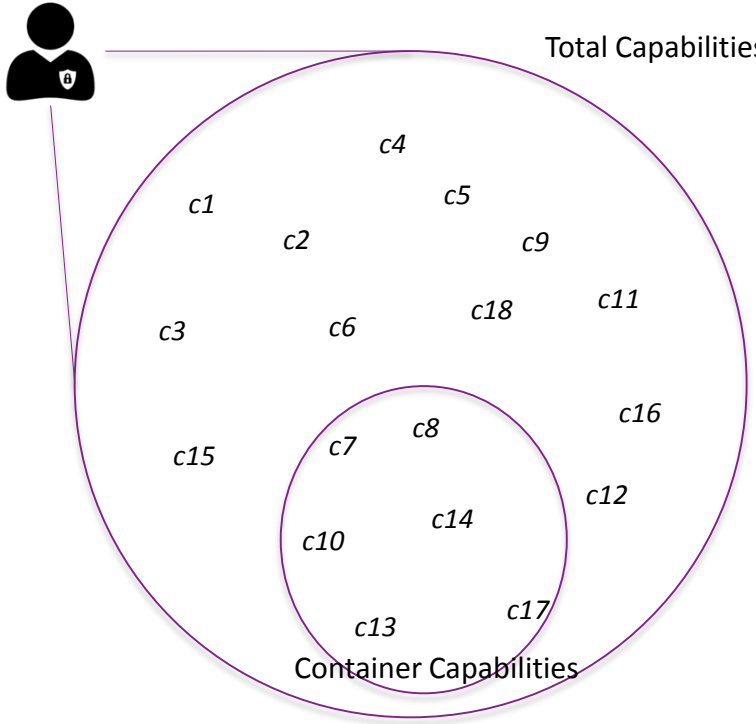
IPC Namespaces

Linux Cgroups & Capabilities

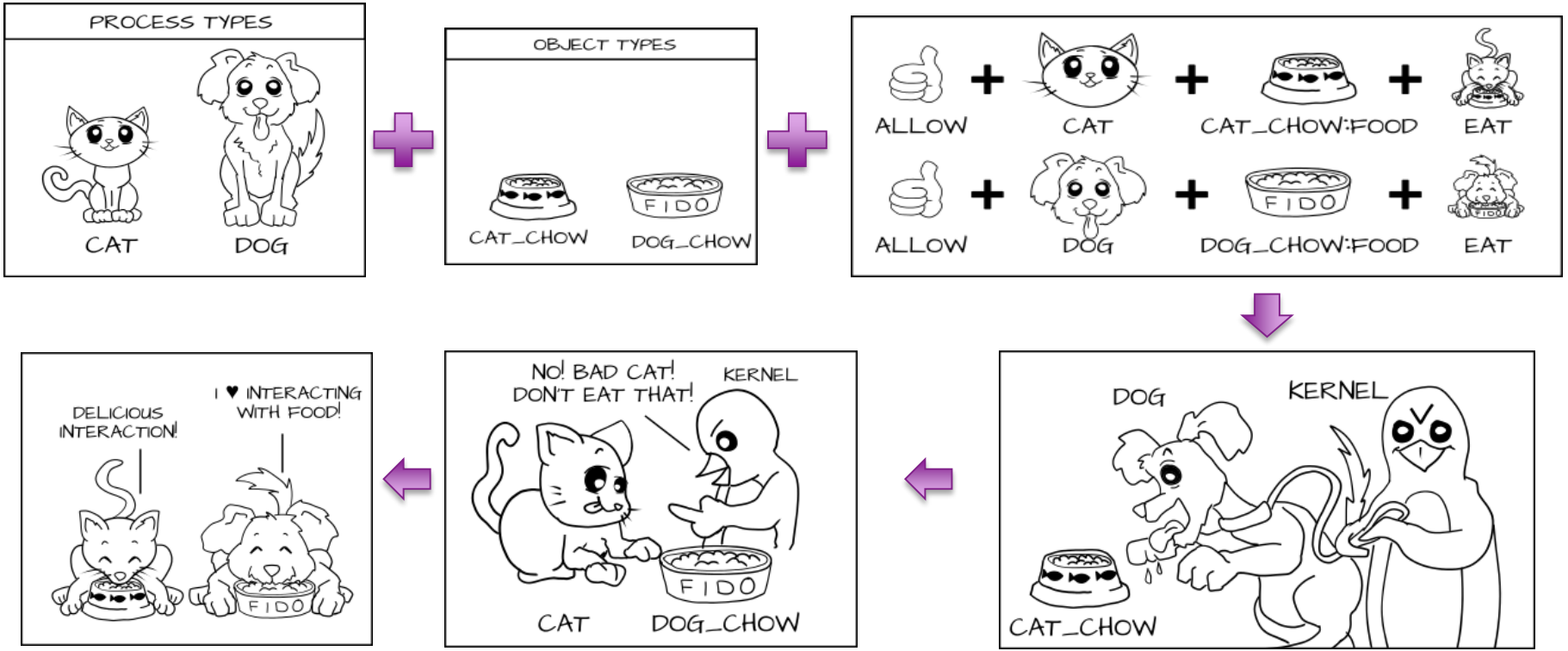




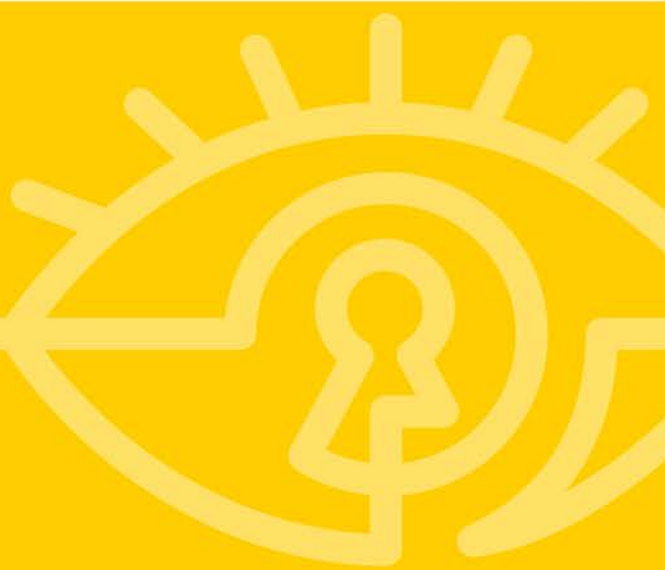
https://mairin.wordpress.com/2011/05/13/ideas-for-a-cgroups-ui/



SELinux



Ref - http://blog.linuxgrrl.com/2014/04/16/the-selinux-coloring-book/



Security Defense Orchestration

Mapping Higher Level Operational Policies to Security Primitives

Importance of An Operational Policy

Smaller Footprint, Better Security Audit and Hardening

Built-in Protection, Access Control, Permissions, Capabilities

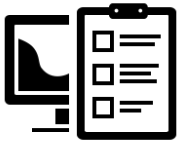
Hardened Workload Execution Environment

Business-Centric Identity and Rights Management

Operational Policy, Compliance Rules

Workload Security Life Cycle

Workload Isolation, Firewalls, Access Control



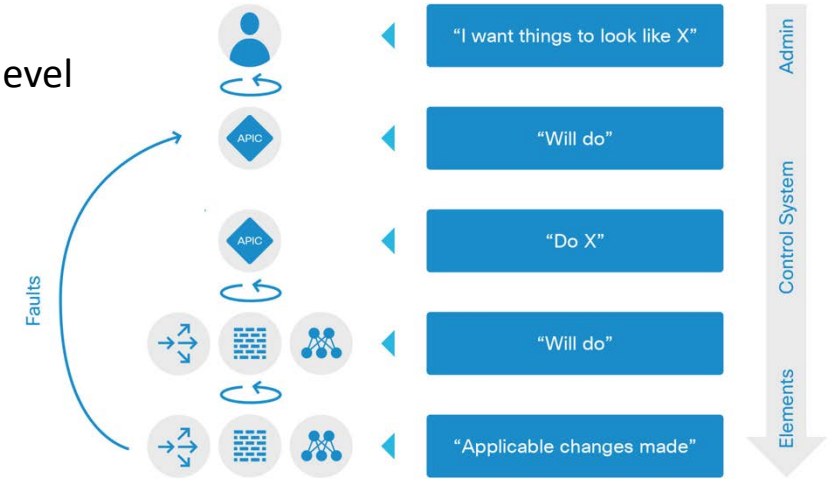
Unified Management, Auditing, Remediation Plans

Data Protection, Encryption, Access Control

Federated Access, Secure Cloud Deployments

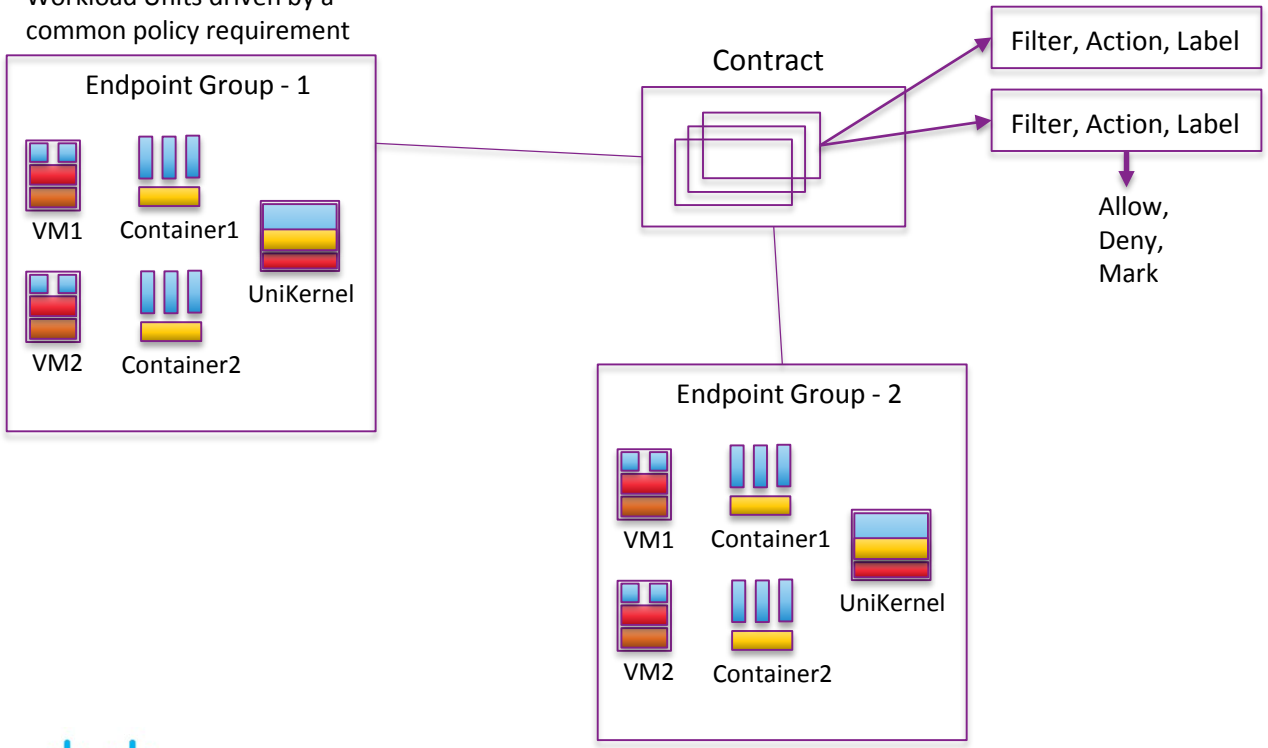
Inspiration from Policy Defined Networking

- Policy Driven Application Composition
- Promise-Theory Driven
- Security is Implicit – Zero Trust Model
- Multi-Level Policy Formats derived from higher level Policy

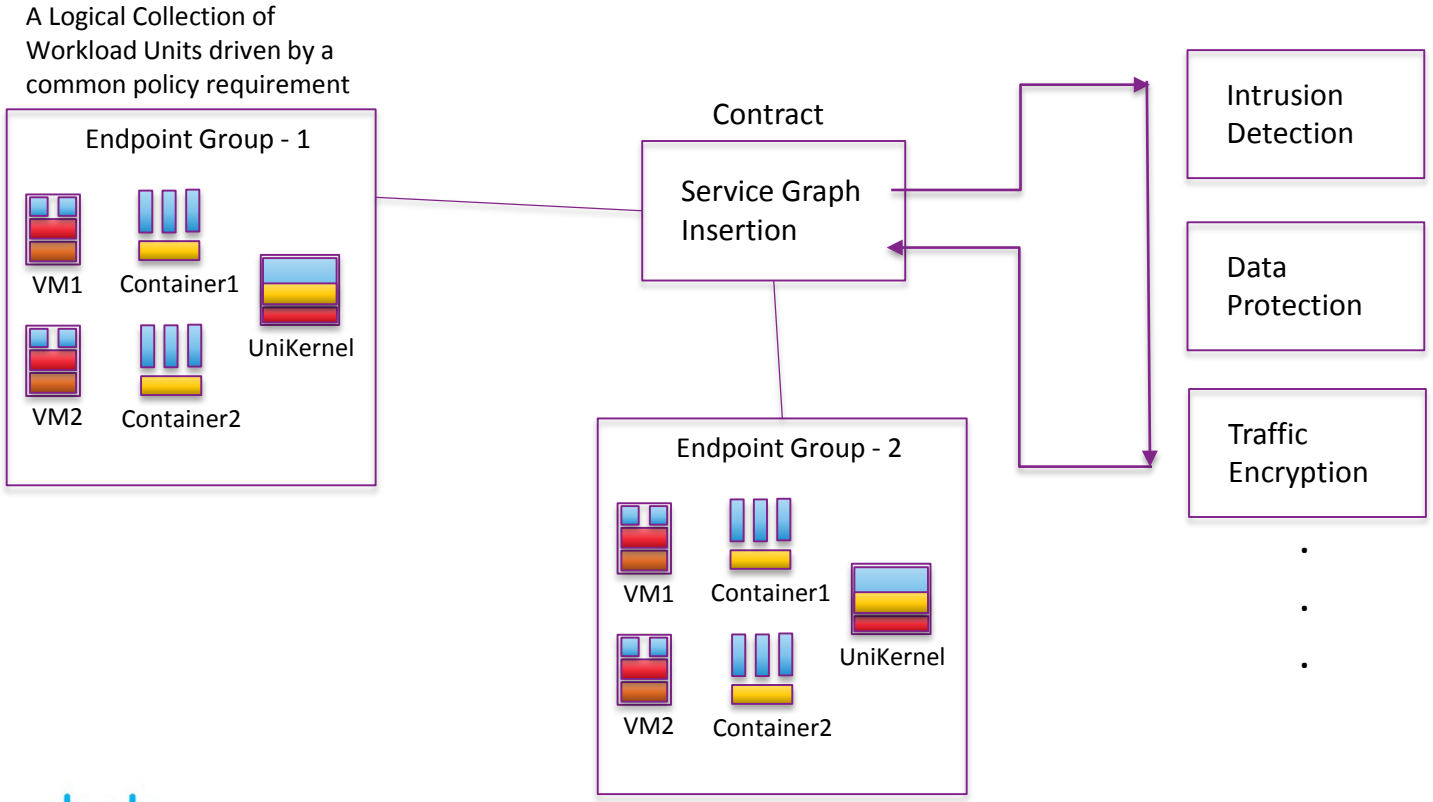


Building a Policy Format…

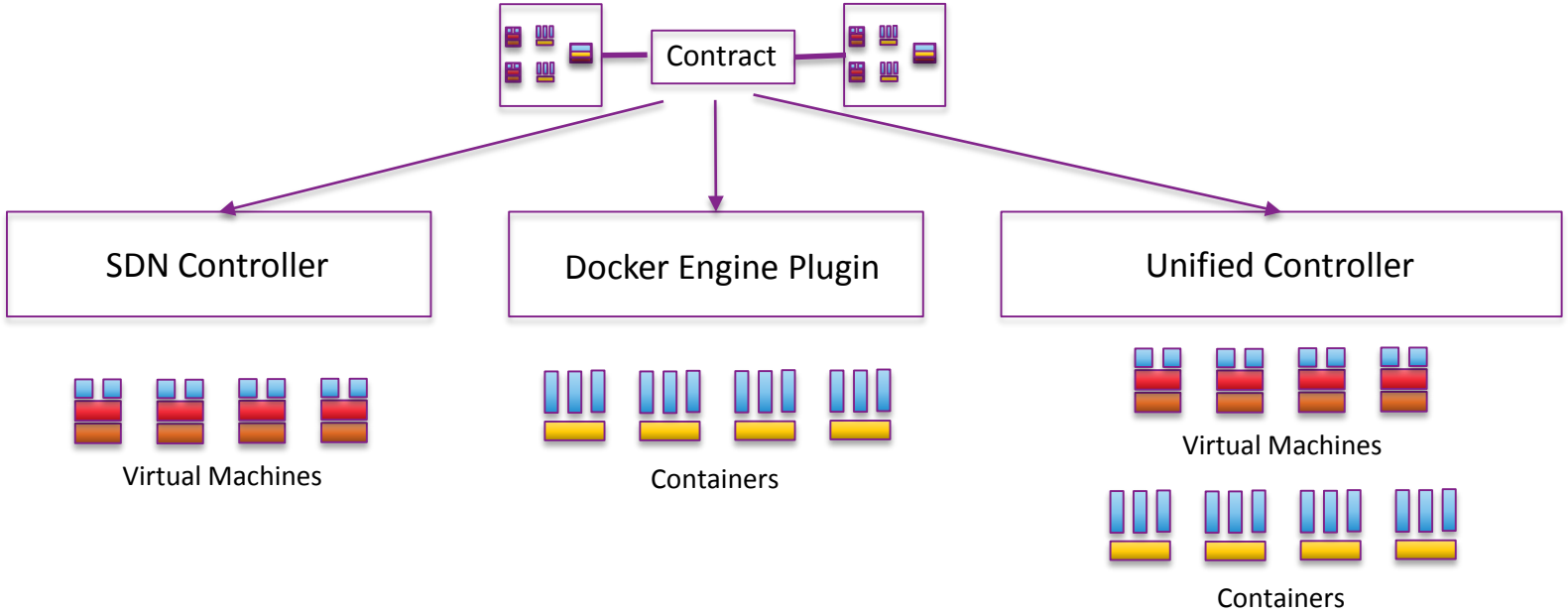
A Logical Collection of Workload Units driven by a common policy requirement



... with pluggable Extensibility.

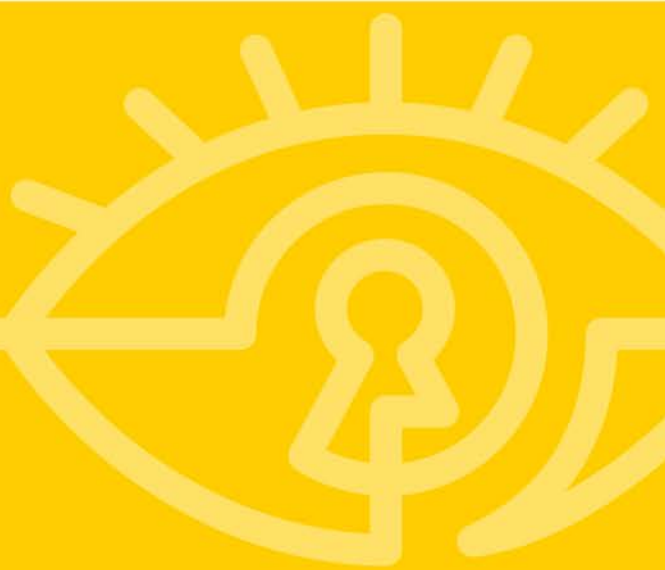


Operationalizing the Security Policy



Apply What You Have Learned Today

- Next Week you should:
  - Understand Built-In Security Capabilities of your Workload Environments
  - Verify your Container environment is making right use of Linux Namespaces, cgroups and SELinux.
- In three months, you should:
  - Identify your high-level Operational Policy Set and check if and how it is enforced on your workloads
  - Identify the best workload unit composition (VM, Container etc.) for the type of your workloads
  - Verify and Setup a Software Patch and Upgrade policy for your workload units
- In six months, you should:
  - Setup a mechanism to operationalize your high-level business policy uniformly across different workload environments



Thanks & Questions

Email – ssaklika@cisco.com