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

- Physical Hardware
  - Hypervisor
  - Operating System
  - Virtualized Hardware
  - Virtualized Hardware
  - Operating System
  - App
  - App
  - App

- Operating System
- Virtualized Hardware
Containers

Physical Hardware

Host Operating System

Binary and Libraries

App

Binary and Libraries

App

App

App

App
Containers within VMs (for Tenant Isolation)

Physical Hardware

Operating System

Hypervisor

Guest OS

Binary and Libraries

App

App

App

App

App

App
Unikernels (Specialized Kernel)

- Physical Hardware
- Hypervisor
- Operating System
- Minimal Kernel
- Minimal Binaries/Libraries
- App
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”

Orchestrated Security Defense Mechanisms

Built-In Standalone Defense Mechanisms
Built-In Standalone Defense Mechanisms

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

**Smaller Footprint, Better Security**

- Audit and Hardening
- Built-in Protection, Access Control, Permissions, Capabilities
- Workload Isolation, Firewalls, Access Control

**Hardened Workload Execution Environment**

- Business-Centric Identity and Rights Management
- Operational Policy, Compliance Rules
- Unified Management, Auditing, Remediation Plans

**Workload Security Life Cycle**

- Data Protection, Encryption, Access Control
- Federated Access, Secure Cloud Deployments

CISCO

rsaconference2016 Abu Dhabi
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

We Need:

1. Security Audit & Hardening
2. Hardware Assisted Virtualization
3. Granular Access Control
4. Secure Trusted Boot
Hypervisor Security (cont.)

- Other Recommendations...
  - Regular Security Updates and Patches
  - Configuration Versioning with Rollbacks
  - 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

We Need:

Access Control
Nuts & Bolts: Linux Namespaces

PID Namespaces

Network Namespaces

Mount Namespaces

IPC Namespaces
Linux Cgroups & Capabilities

- CPU
- MEMORY
- NETWORK
- STORAGE I/O

- CGROUP #1
- CGROUP #2
- CGROUP #3
- CGROUP #4
- CGROUP #5
- CGROUP #6
- CGROUP #7
- CGROUP #8
- CGROUP #9
- CGROUP #10

Shares:
1024 640 2048

CGROUP #1 gets half as much CPU time as CGROUP #3.
CGROUP #2 gets the least CPU time.
CGROUP #3 gets the most CPU time.

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

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
- Workload Isolation, Firewalls, Access Control
- Data Protection, Encryption, Access Control
- Federated Access, Secure Cloud Deployments

Hardened Workload Execution Environment

- Business-Centric Identity and Rights Management
- Operational Policy, Compliance Rules
- Unified Management, Auditing, Remediation Plans

Workload Security Life Cycle
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

Endpoint Group - 1
- VM1
- Container1
- UniKernel
- VM2
- Container2

Endpoint Group - 2
- VM1
- Container1
- UniKernel
- VM2
- Container2

Contract

Filter, Action, Label
- Allow
- Deny
- Mark
... with pluggable Extensibility.

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

Endpoint Group - 1
- VM1
- Container 1
- UniKernel
- VM2
- Container 2

Contract
- Service Graph Insertion

Endpoint Group - 2
- VM1
- Container 1
- UniKernel
- VM2
- Container 2

Intrusion Detection
Data Protection
Traffic Encryption
Operationalizing the Security Policy

SDN Controller

Docker Engine Plugin

Unified Controller

Virtual Machines

Containers

Virtual Machines

Containers
Apply What You Have Learned Today

Next Week you should:
- Understand your Workload Environment Composition – Distribution across VM, Containers and why is it so?
- Understand Built-In Security Capabilities of your Workload Environments.
- Last Hardening Audit, Enabled Capabilities for your Containers, VM Configurations etc.

In three months, you should:
- Identify the best workload unit composition (VM, Container etc.) for the type of your workloads
- Investigate and Setup a Unified Software Patch and Upgrade policy for your workload units
- Identify your high-level Operational Policy Set and check if and how it is enforced on your workloads

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