Virtualization: Security’s Silver Bullet
Lessons from Troy and Byzantium
Simon Crosby, CTO
The essence of virtualization-enhanced security is the ability to arbitrarily shrink the OS and network attack surface of an application to the point that it is completely isolated from everything else on a system.
I need a private cloud to ensure security & compliance
“Next-gen threat protection”
“99% of malware hashes are seen for 58 seconds or less. In fact, most malware was seen only once.”

97% of malware is unique to a specific endpoint

March 2016

Malware and potentially unwanted applications (PUAs) have become overwhelmingly polymorphic, with 97 percent of malware morphing to become unique to a specific endpoint device, according to a report from security specialist Webroot. Travis Smith, senior security researcher at Tripwire have the following comments on it.
“The rise of the targeted attack is shredding what is left of the anti-malware market’s stubborn commitment to reactive protection techniques.”

Gartner MQ for Endpoint Protection Platforms Q1, 2015, Document G00262733

“Not all threats can be prevented. The speed to detect and respond to incidents is critical. Seek to identify compromised systems even when no malware has been detected.”

Gartner Document G00256438
Firstbrook, MacDonald, Pingree
Lessons from Byzantium
“A system that...does what people expect – and nothing else – despite disruption, user and operator errors, and attacks. Design and implementation errors must be avoided, eliminated, or tolerated.”

Trust in Cyber-space (NRC)
Hardware-isolate individual user tasks and OS services using endpoint CPU virtualization.
Micro-virtualization
Micro-segmentation
and Endpoint Security
Microvisor

Intel VT-x CPU virtualization

Copy-on-write execution in hardware isolated memory

Additional CPU security features

Virtual file system & network

Hardware isolated memory

“need to know” access to system resources, files & networks

Multi-core execution

No device access
Real-time Detection & Analysis

Malware manifest
- Search for attacks in real-time
- Isolate & remediate infected devices
- Learn, Adapt & Distribute new attack vectors & IoCs
- Send to SIEM and share with peer orgs
Device Guard uses micro-virtualization to hardware-isolate two Windows Services

- Credential Guard isolates credential hashes to reduce pass-the-hash attacks
- Hypervisor enforced Code Integrity enforces white-listing for applications and the OS kernel

Windows Defender Application Guard will isolate the Edge browser (in RS2)
Bromium isolates all external attack vectors

...and monitors the OS and every app
Micro-virtualization for cloud-hosted virtual desktops
Granular isolation per task within each desktop VM
Micro-virtualization
Micro-segmentation
Micro-services

And Cloud Security
Virtual Machines

NSX Virtual Network

ESX Hosts
(Cluster)

Production
Micro-Segmentation Redux

Micro-segment Virtual Machines into different Security Groups

Security Group:
- Finance
- Legal
- Web
- Partners
- Database

VMWare NSX

Production
How can we define and deploy applications, together with their security policies, before they have configured services (eg IP addresses)

Challenge: Apps

Lack of security automation impacts business agility in delivering services, results in security gaps
Decoupling Dev & Deployment

NG Enterprise Apps

Cloud Native Apps

Datacenter Snowflakes
• Deploy in months
• Live for years
Docker **ecosystem** for **distributed** applications

An engine that enables any payload to be encapsulated as a lightweight, portable, self-sufficient container...

...that can be manipulated using standard operations and run consistently on virtually any hardware platform.

Do services and apps interact appropriately?

Can I migrate smoothly and quickly?

**Multiplicity of Stacks**

- Static website
- User DB
- Web frontend
- Queue
- Analytics DB

**Multiplicity of hardware environments**

- Development VM
- QA server
- Customer Data Center
- Public Cloud
- Production Cluster
- Contributor’s laptop
Micro-virtualization for Docker Containers

Intel Clear Containers

- Security and isolation advantages of virtualization to isolate containerized applications on Linux
- Fast booting small Linux VM per container
- Containers can reside in multi-tenant environments
Security by Design

- No false alerts
- Defeat each attack
- No remediation
- Real-time forensic detail
- Continuous detection & response

© Bromium 2014