Securing the Next-Generation Virtualized Data Center

Neil MacDonald

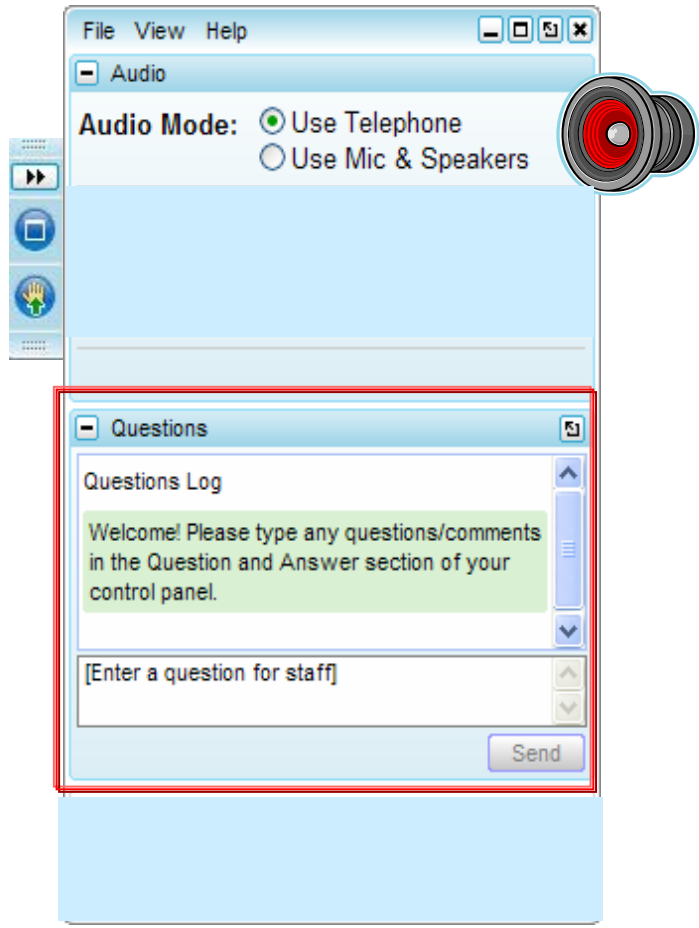
VP and Gartner Fellow

25 March 2010

Gartner®

Welcome!
Here's how to participate in today's webinar

- You can listen to the presentation using your computer's speaker system as the default (VoIP).
- Or dial the conference line by selecting Use Telephone in the webinar audio pane.
- Have a question for the presenter(s)? Type it into the Questions pane—we will answer as many as time permits.
- A recording of this presentation will be sent to you within 48 hours.
- If you would like a copy of today's presentation, contact your Gartner Account Executive or visit Gartner.com/webinars. A copy of the presentation will be available within 24 hours.
- Please note you may be polled during the webinar; only aggregate answers will appear.



Gartner

Our world-class, objective insight is drawn from thousands of daily client interactions

Gartner

Most virtual machines you deploy will be less secure than the physical systems they replace.

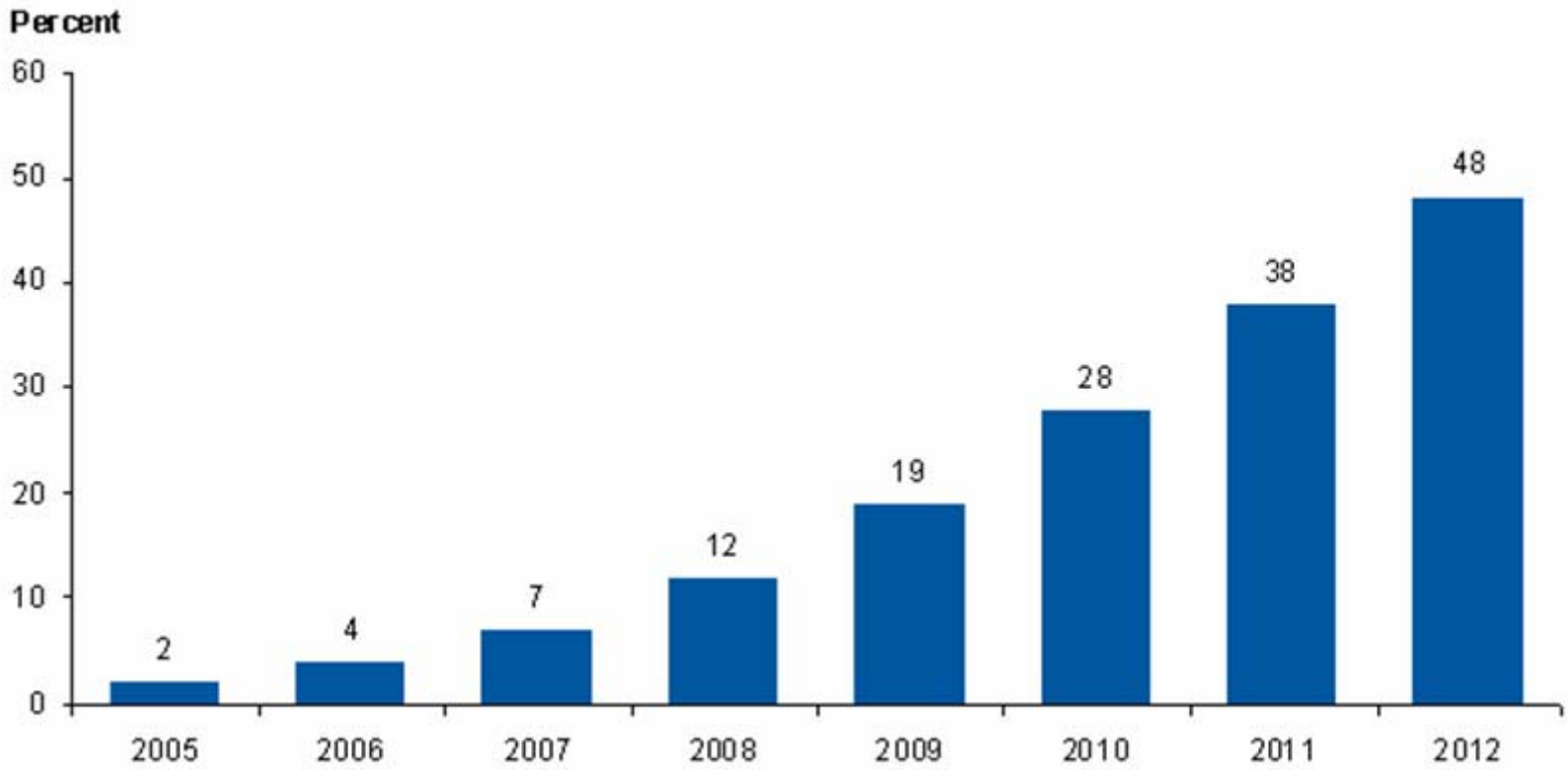
Gartner

Virtualization will radically change how you secure and manage computing environments.

Gartner

We've Only Just Started With Virtualization

Figure 1. Percentage of x86 Server Architecture Workloads That Are Running in Virtual Machines

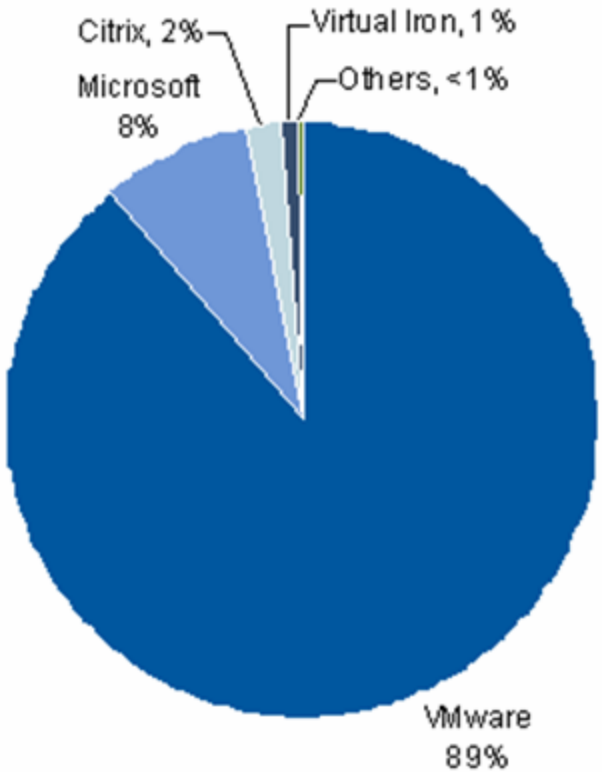


Source: Gartner (October 2009)

Gartner

VMware Dominates in Enterprises Today

Figure 2. Virtual Machine Installed Base Market Share, Year-End 2008

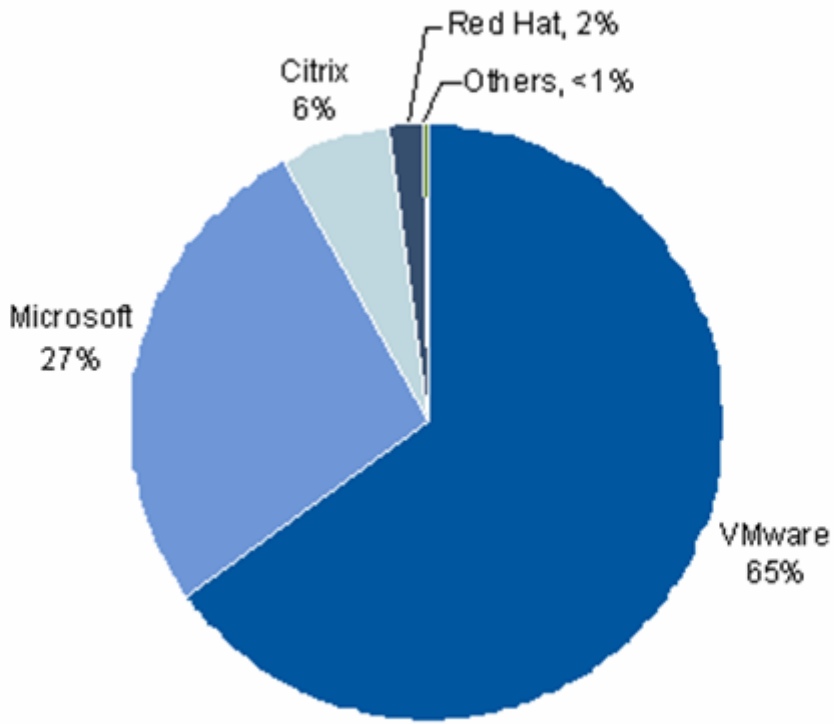


Source: Gartner (October 2009)

Gartner

But Microsoft is Gaining

Figure 4. Virtual Machine Installed Base Market Share, Year-End 2012



Source: Gartner (October 2009)

Gartner

Pick the top three virtualization security issues that concern you.
(Enter three options from most to least important)

① Information security isn't initially involved in the virtualization projects
17w

② A compromise of the virtualization layer could result in the compromise of all hosted workloads
68w

③ Lack of visibility and controls on internal VM-to-VM communications
69w

④ Potential Loss of SOD for network and security controls
29w

⑤ Restricting and auditing administrative access and management tool access
31w

⑥ Configuration management and Patching of offline images
32w

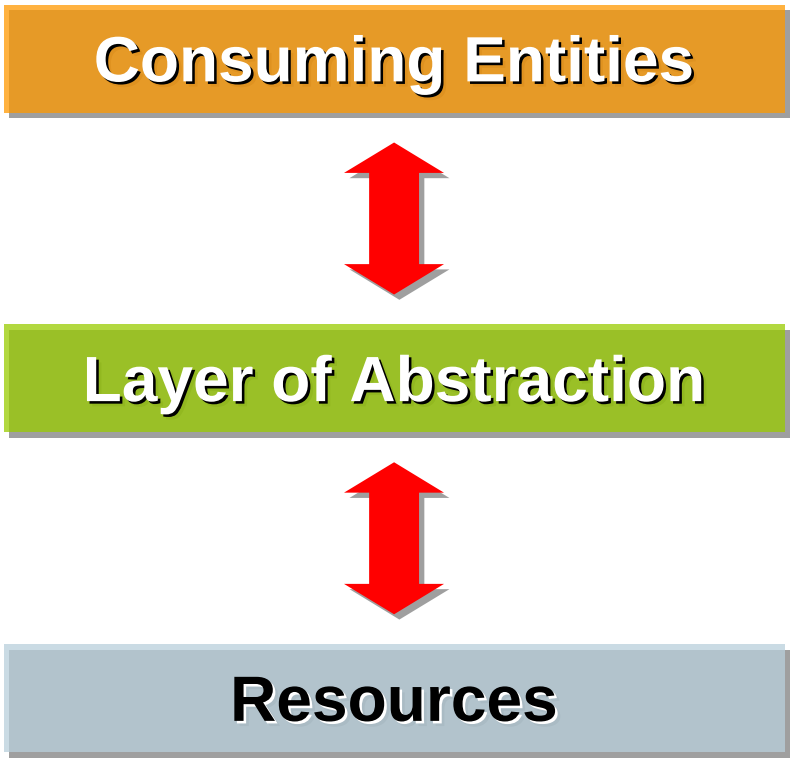
⑦ Storage area network security and protection of offline images
20w

⑧ Increased chance of misconfiguration because of the use of different tools
28w

⑨ Risks from combining workloads of different trust levels on the same physical machine
56w

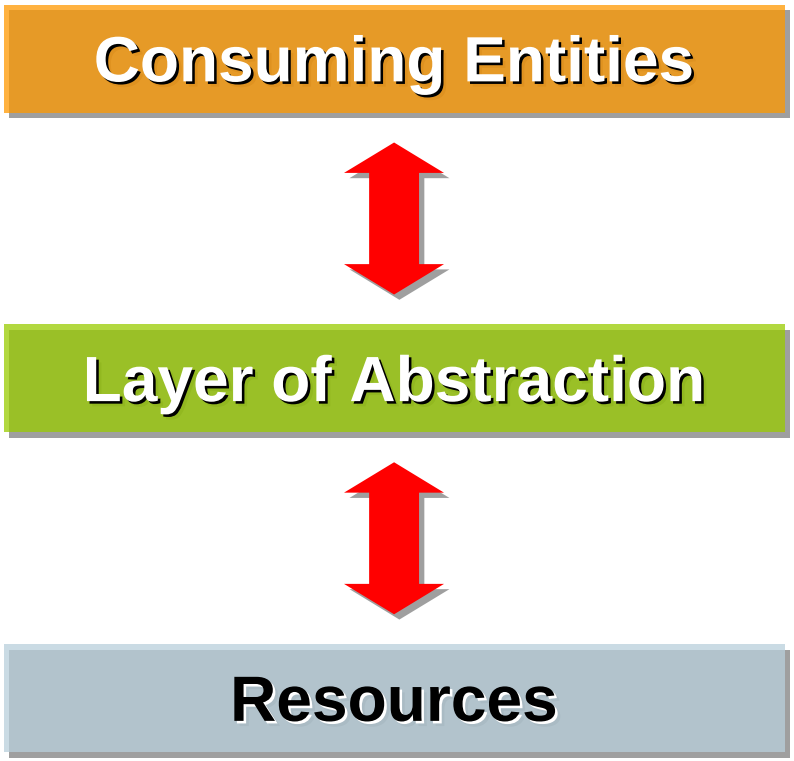
Gartner

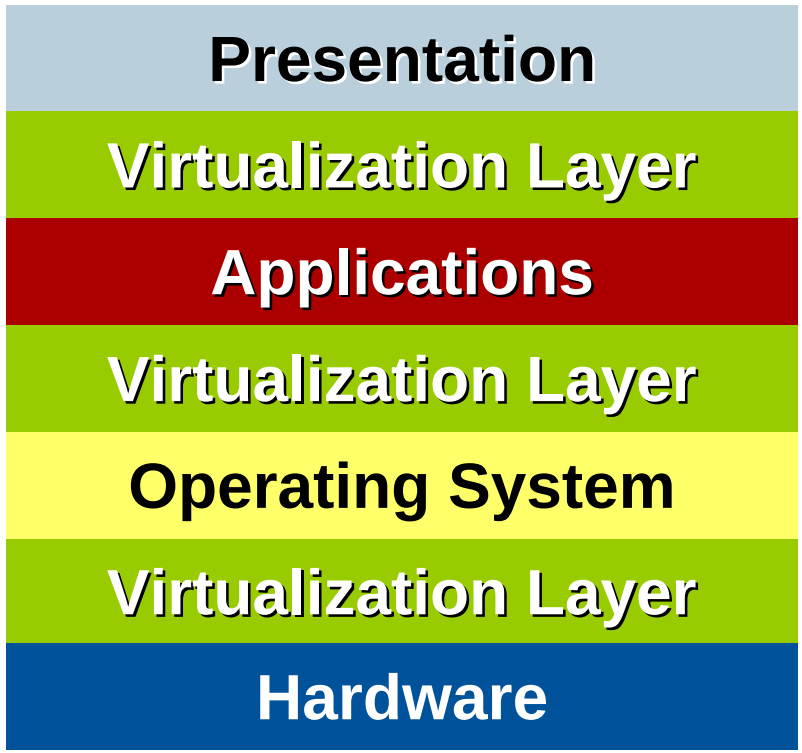
Virtualization: Simple Concept, Profound Implications



Gartner

Virtualization: Simple Concept, Profound Implications

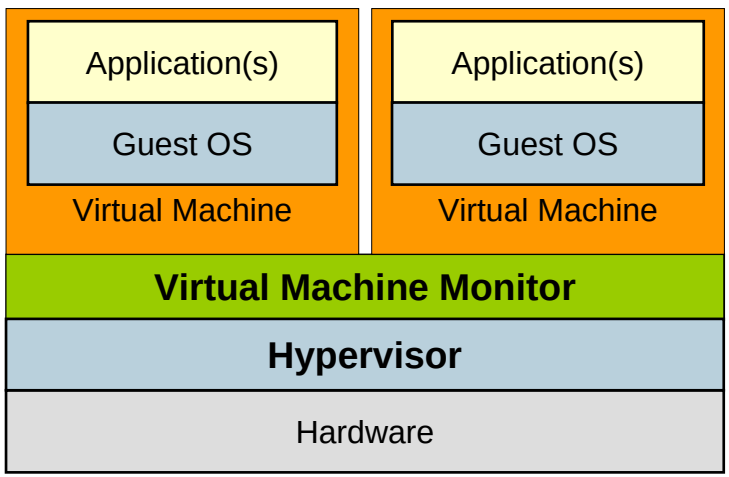




Gartner

Top Seven Virtualization Security Issues: Issue No. 1

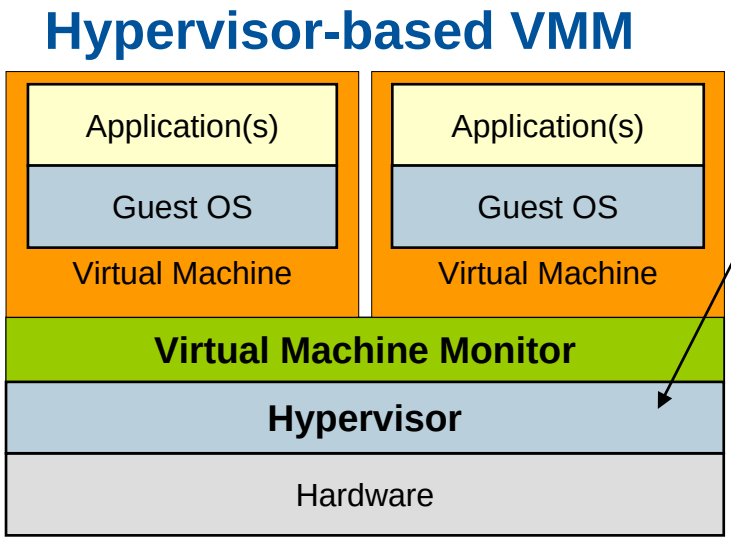
Hypervisor-based VMM



Gartner

Top Seven Virtualization Security Issues: Issue No. 1

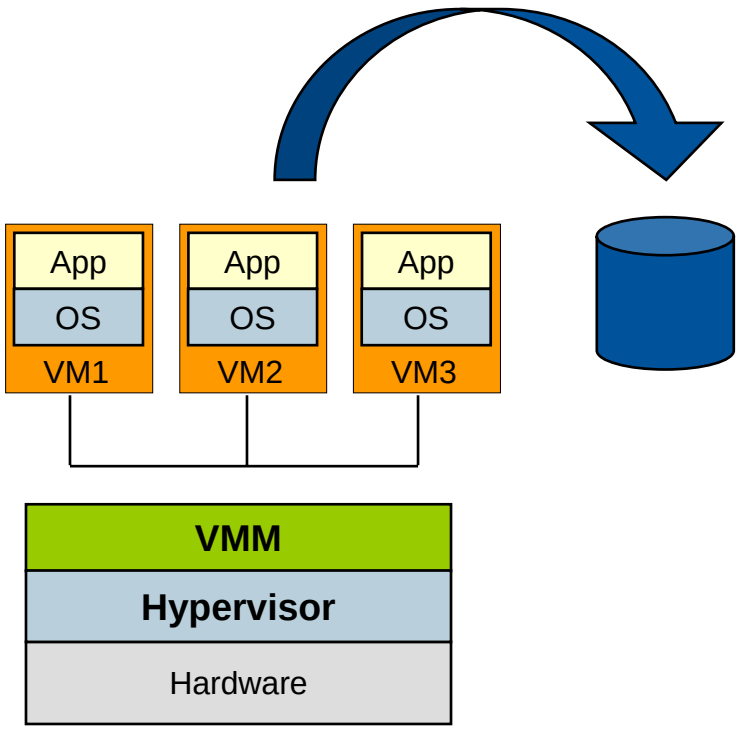
The hypervisor/VMM represents a new IT platform in our data center. We must extend out existing patch, configuration and vulnerability management processes to address this platform.



- Are you patched?
- Are you configured correctly?
- Have you been compromised?
- How would you know?

Gartner

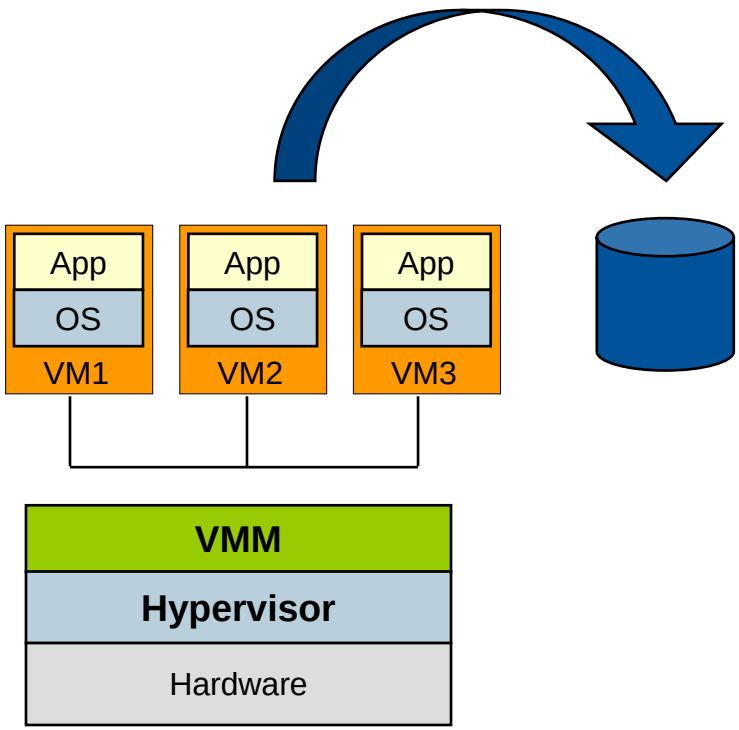
Top Seven Virtualization Security Issues: Issues No. 2, No. 3



Gartner

Top Seven Virtualization Security Issues: Issues No. 2, No. 3

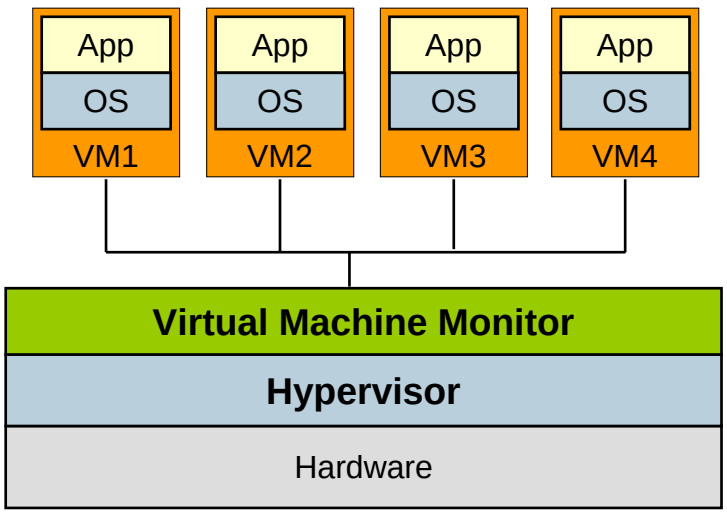
Offline VMs need to be kept up-to-date with patches, configuration changes, AV signatures, firewall rules and so on. Offline VMs will become a target for attack.



- The moment a snapshot is taken, it gets out of date. Patching offline images directly is not possible, but there are work-arounds:
  - Mount in a quarantined mode and patch.
  - Inject code to apply the path on boot.
- Offline VMs need encryption to protect from unauthorized access and digital signatures to detect tampering.
- Stealing an entire VM becomes as easy as copying a file.
- Storage security becomes a critical layer of our defense-in-depth strategy.

Gartner

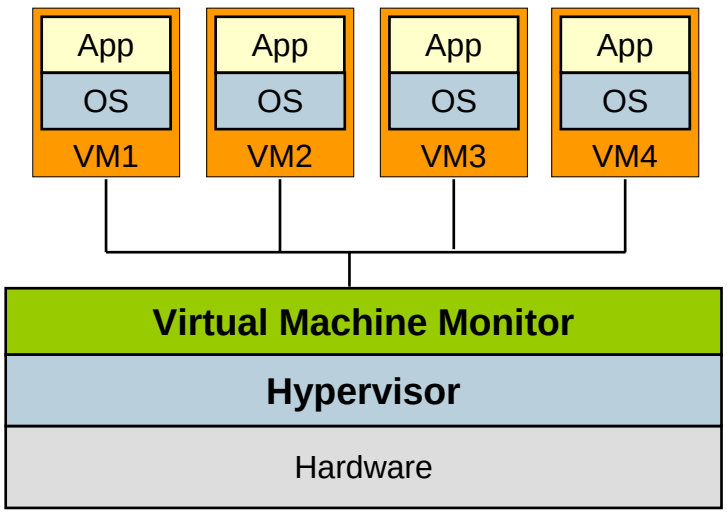
Top Seven Virtualization Security Issues: Issues No. 4, No. 5



Gartner

Top Seven Virtualization Security Issues: Issues No. 4, No. 5

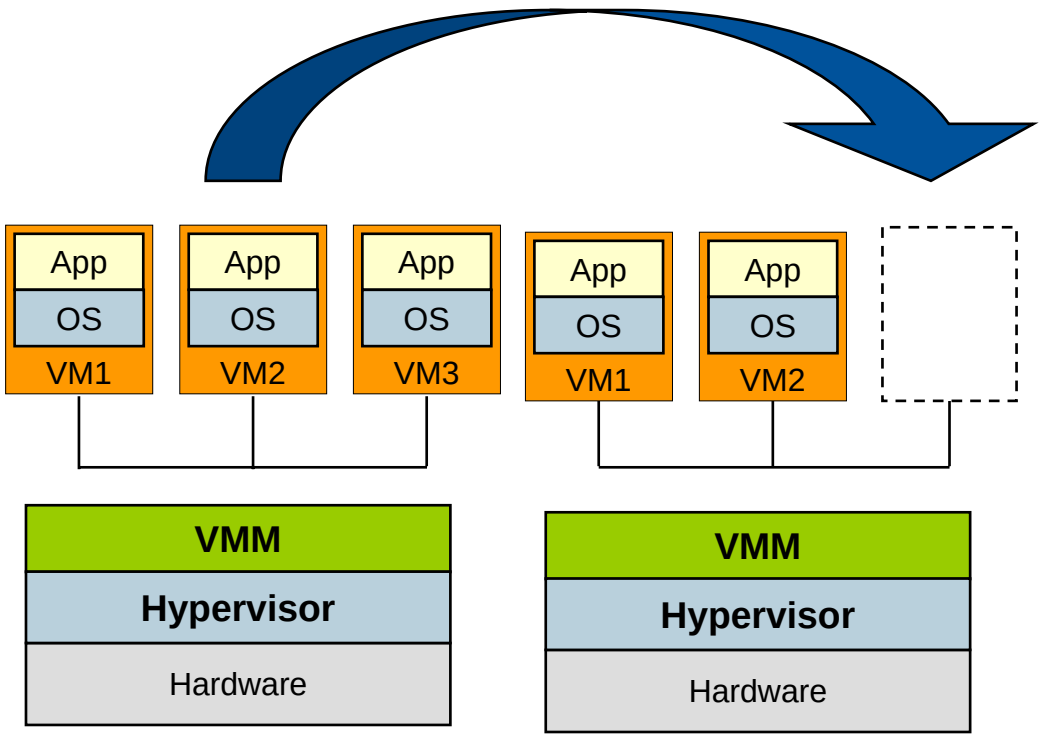
For efficiency in communications, most virtualization platforms enabled the creation of an internal virtual switch for VM to VM communications. Security controls may (or may not) be needed for traffic inspection and separation. Potential SOD issues.



- Do I need separation?
  - Dev/Test
  - DMZ
  - PCI / HIPAA
  - Top-secret / confidential
  - Critical financial- or HR-related data
- Should VM1 talk to VM4?
- Even if VM1 *should* talk to VM4, how do you know VM1 isn't attacking VM4?
- Who configures the virtual switch?

Gartner

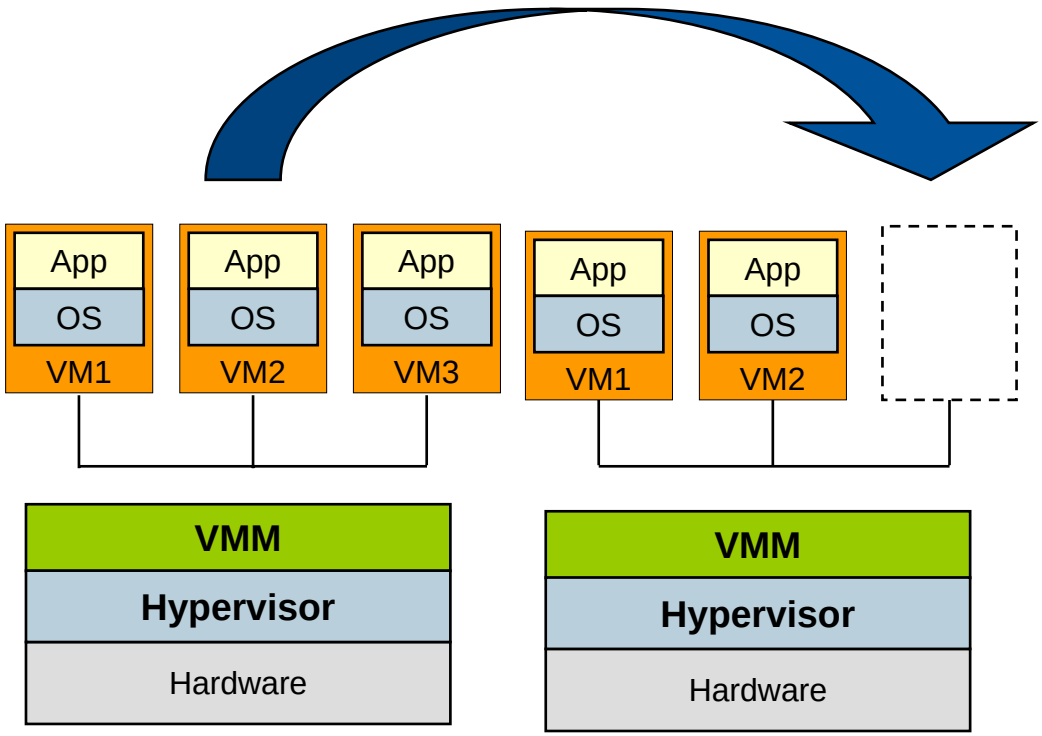
Top Seven Virtualization Security Issues: Issues No. 6, No. 7



Gartner

Top Seven Virtualization Security Issues: Issues No. 6, No. 7

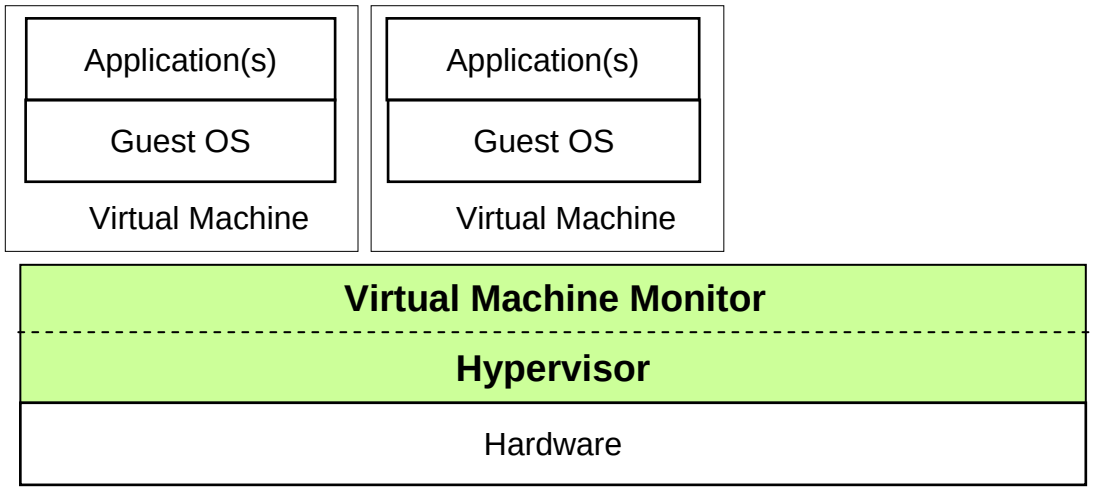
VMs will become mobile. Security policies tied to physical attributes like IP addresses or MAC addresses make no sense. Different tools for managing physical and virtual increase the chance for mistakes.



- Security policies need to be tied to logical constructs, not physical:
  - VM identities
  - Application identities
  - User identities
- Security policies need to be mobile and move with the VM
- Ideally, use tools from vendors that span physical and virtual environments

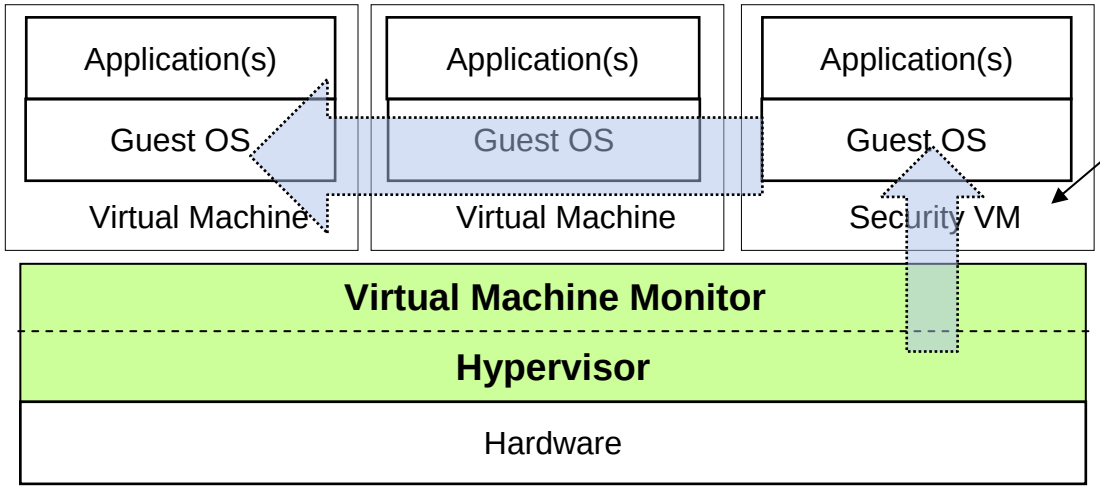
Gartner

Limited Choices Available for Virtualized Firewall/IPS Solutions



Gartner

Limited Choices Available for Virtualized Firewall/IPS Solutions

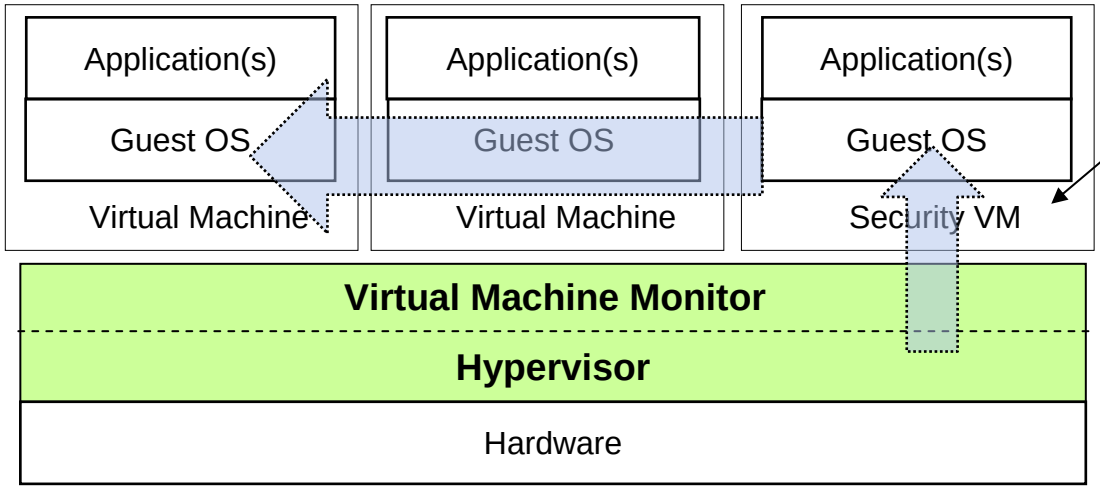


"Virtual Security Partition" in this case a "Security VM":

- Network firewall
- Application-level firewall
- Identity-aware network access control
- E-mail security platform
- Web security platform
- Unified threat management
- Directory server

Gartner®

Limited Choices Available for Virtualized Firewall/IPS Solutions



"Virtual Security Partition" in this case a "Security VM":

- Network firewall
- Application-level firewall
- Identity-aware network access control
- E-mail security platform
- Web security platform
- Unified threat management
- Directory server

- Altor Networks (formed by former Check Point employees).
- Apani offers identity-based network access control.
- Astaro Security Gateway (ASG).
- Catbird V-Agent offers integrated Snort-based IDS/IPS, NAC and vulnerability assessment.
- Check Point released its virtual firewall in 2008.
- IBM and Sourcefire announced and delivered their offerings in late 2009.
- Microsoft released a virtual appliance version of its ISA Server in 2008.
- Stonesoft has released its virtual firewall and IPS appliance.
- RedCannon released its unified threat management virtual appliance in 2009.
- Reflex's Systems Virtual Security Appliance (VSA).
- StillSecure's Strata Guard Free provides firewalling and IPS but in a rate-limited offering.
- Enterasys has IPS capabilities supported as a VM monitoring the virtual network.
- VMware has added its vShield Zones technology with vSphere 4 and higher.

Gartner®

Discontinuity: Virtualization of Security Controls

Physical Appliances

- Approximately $25K per Gbps FW and IPS
- Approximately $150K for 10 Gbps FW/IPS
- State of the art today is about 20 Gbps FW/IPS inspection speed for $250K; chassis alone is about $30K

- Serial processing
- High cost makes us "ration security“
- Static, hard to change
- Expensive, custom hardware

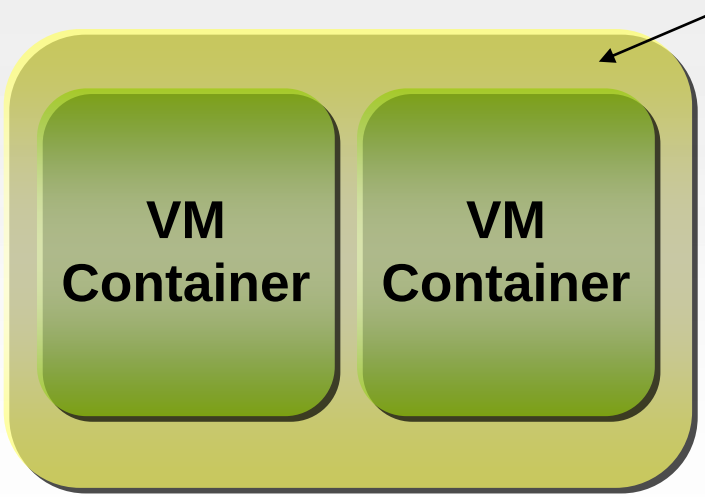
Virtual Appliances

- Approx. $2K per 500 Mbps on ESX 3.x
- With VMsafe and "fast path," this improves about 10x (5 Gbps), still $2K
- 10 ESX servers give 50 Gbps of parallel inspection for about $25K

- Multiple, parallel processing
- Security when and where needed
- Adaptive, policies move with workloads
- Less expensive, commodity hardware

Gartner

Decoupled from Hardware, Workloads Become Mobile



Open Virtualization Format (OVF):

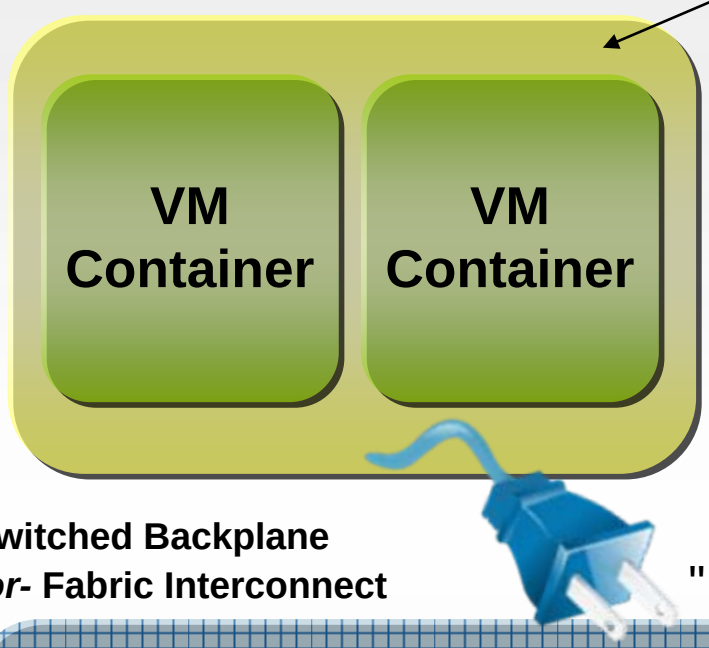
Wrap (package) the VM in XML-based metadata, digitally signed for tamper resistance.

Can specify:

- Memory requirements
- Processor requirements
- Storage requirements
- Networking requirements
- VM dependencies and load order

Gartner

Decoupled from Hardware, Workloads Become Mobile

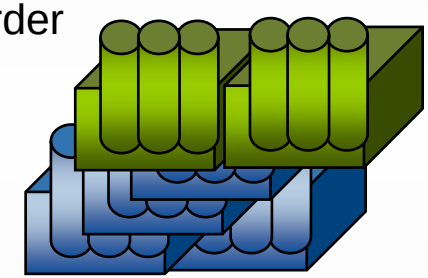


Open Virtualization Format (OVF):

Wrap (package) the VM in XML-based metadata, digitally signed for tamper resistance.

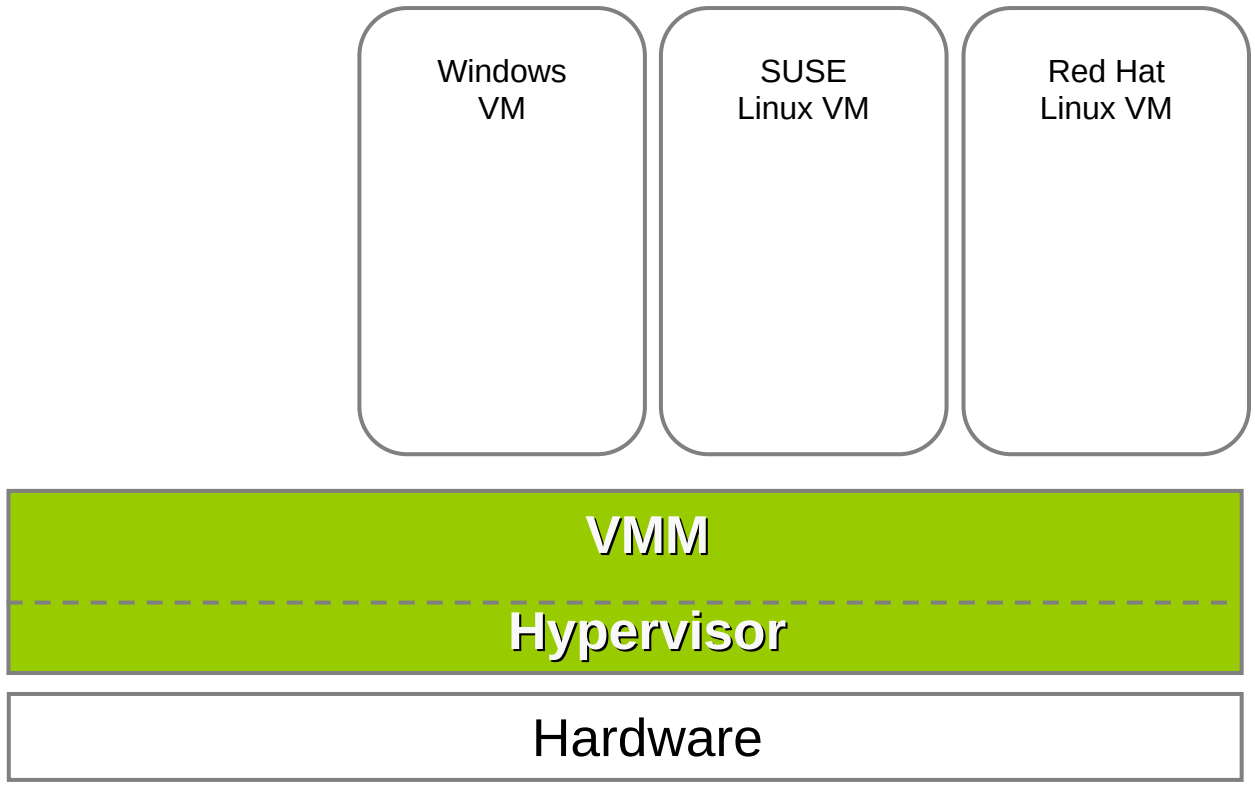
Can specify:

- Memory requirements
- Processor requirements
- Storage requirements
- Networking requirements
- VM dependencies and load order



Gartner

Discontinuity: VM State Inspection --Agentlike Functionality, Without Agents

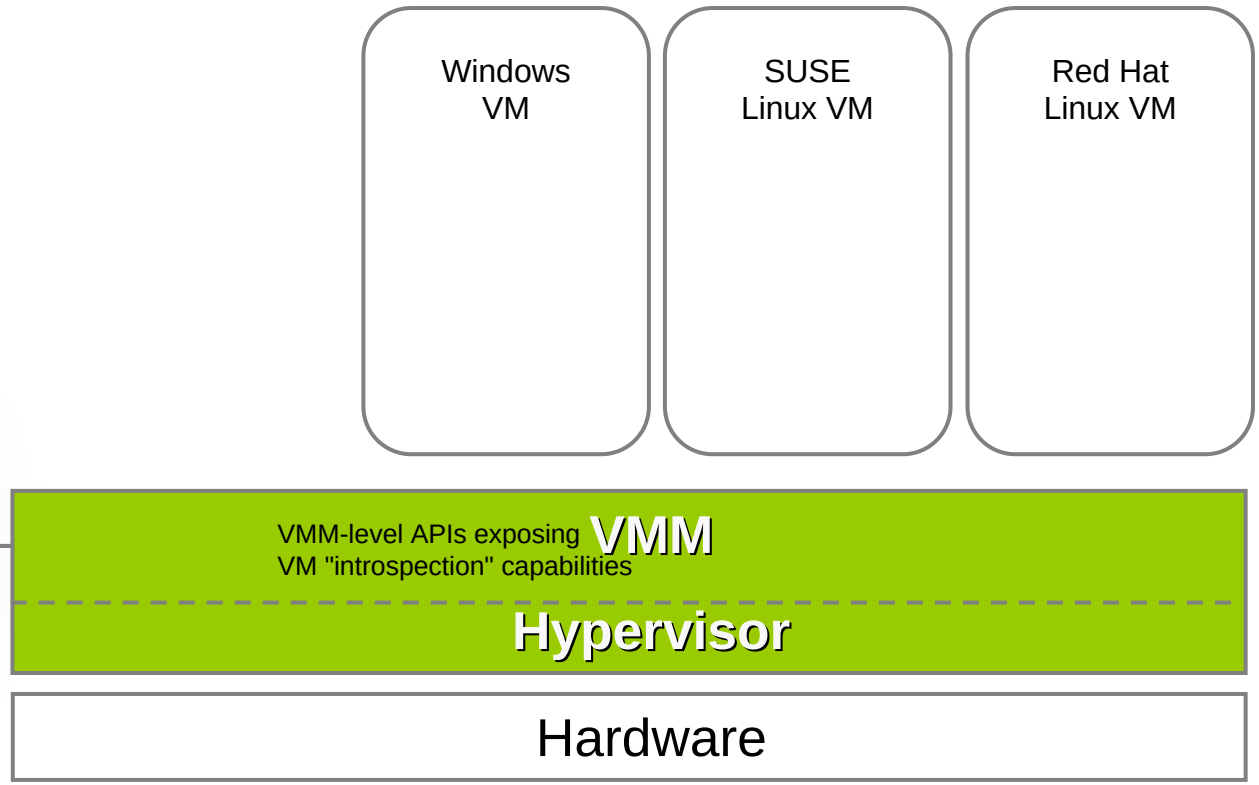


Gartner

Discontinuity: VM State Inspection --Agentlike Functionality, Without Agents

VM state information:

- Processor state
- Memory pages
- Network state
- Disk blocks
- Process control blocks

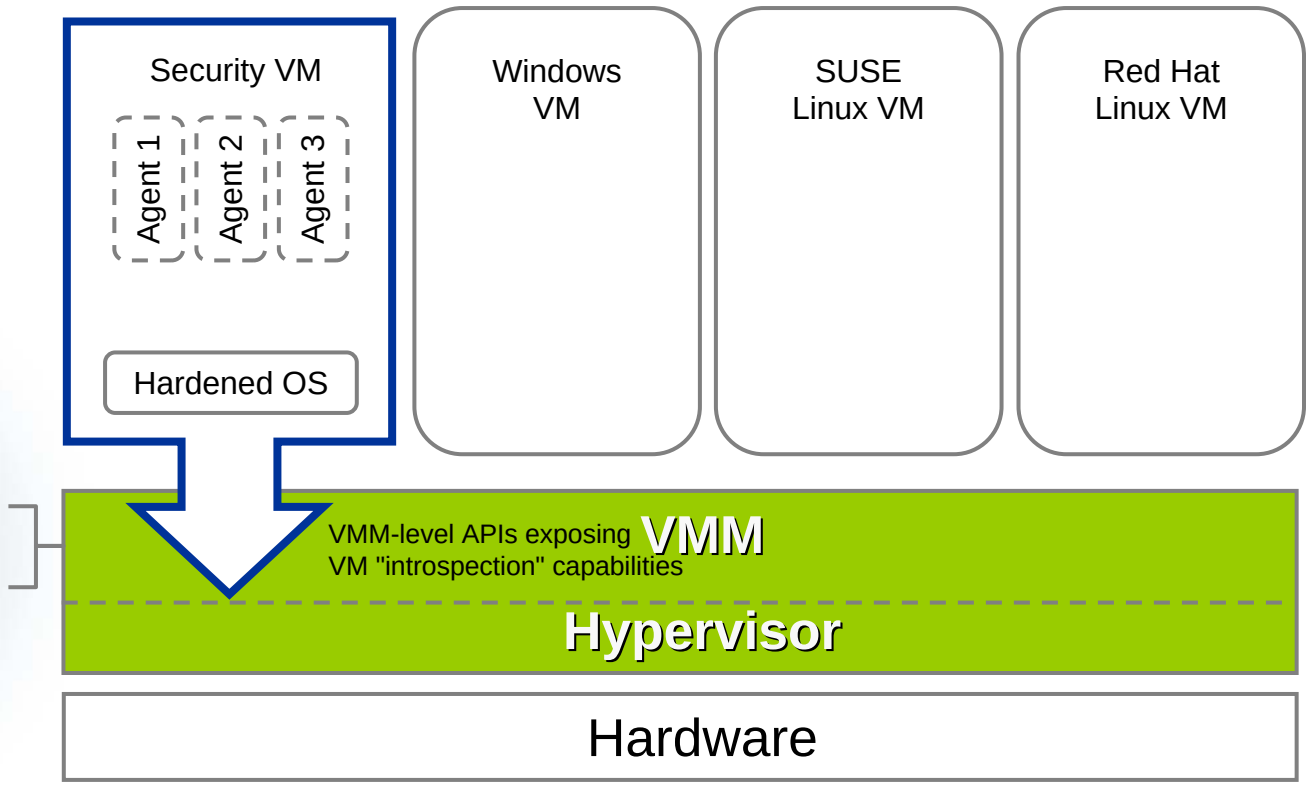


Gartner

Discontinuity: VM State Inspection --Agentlike Functionality, Without Agents

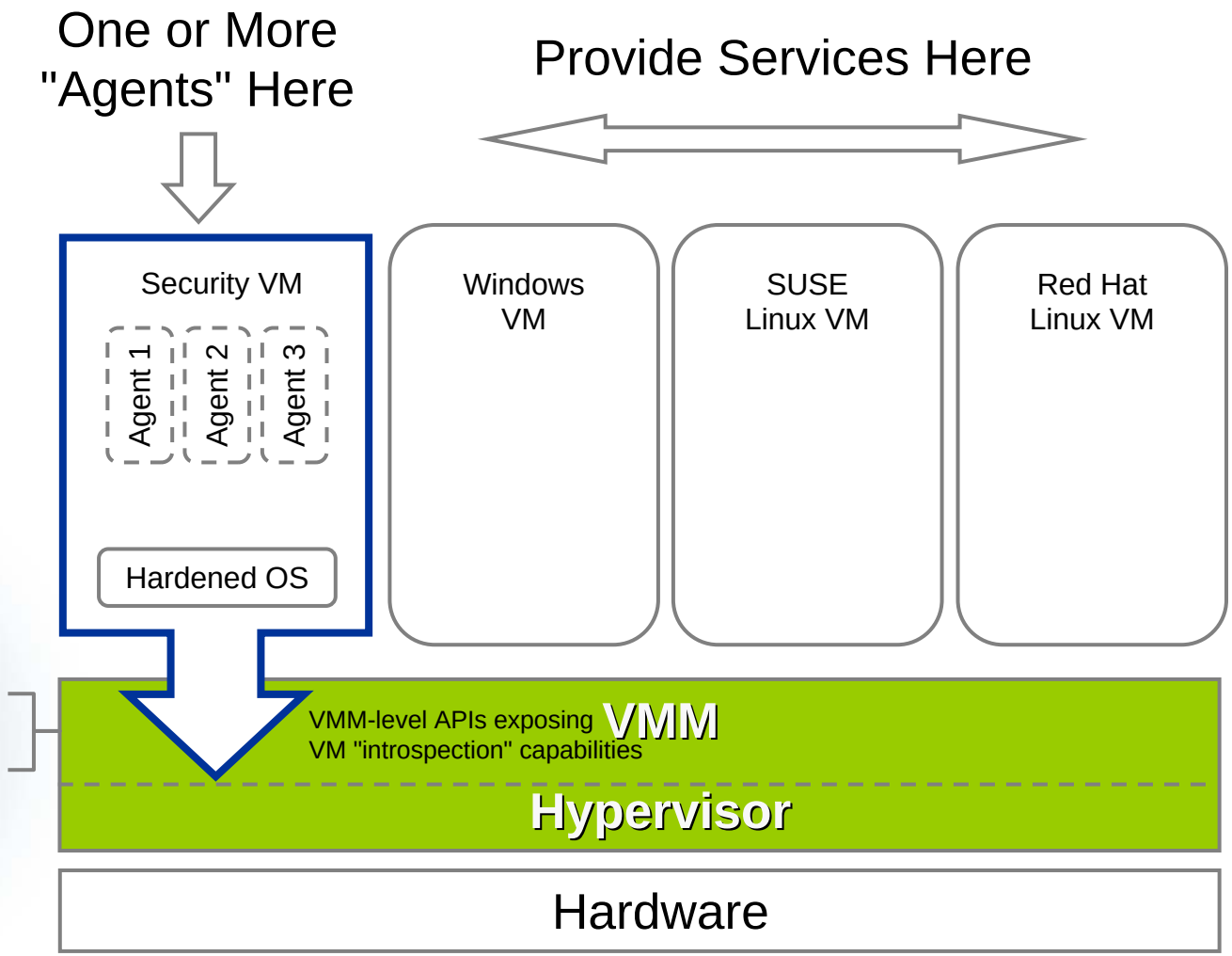
VM state information:

- Processor state
- Memory pages
- Network state
- Disk blocks
- Process control blocks



Gartner

Discontinuity: VM State Inspection --Agentlike Functionality, Without Agents



VM state information:

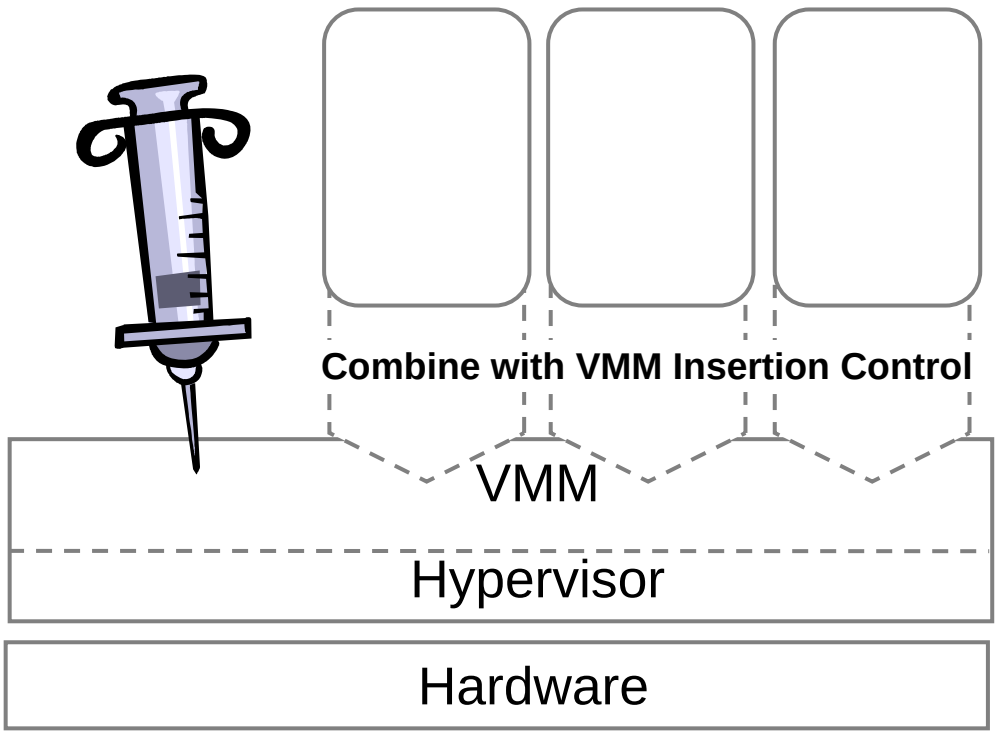
- Processor state
- Memory pages
- Network state
- Disk blocks
- Process control blocks

"Control what the VM does, not what the VM is"

Gartner

Contextual and On-Demand Provisioning of Security Policy Enforcement

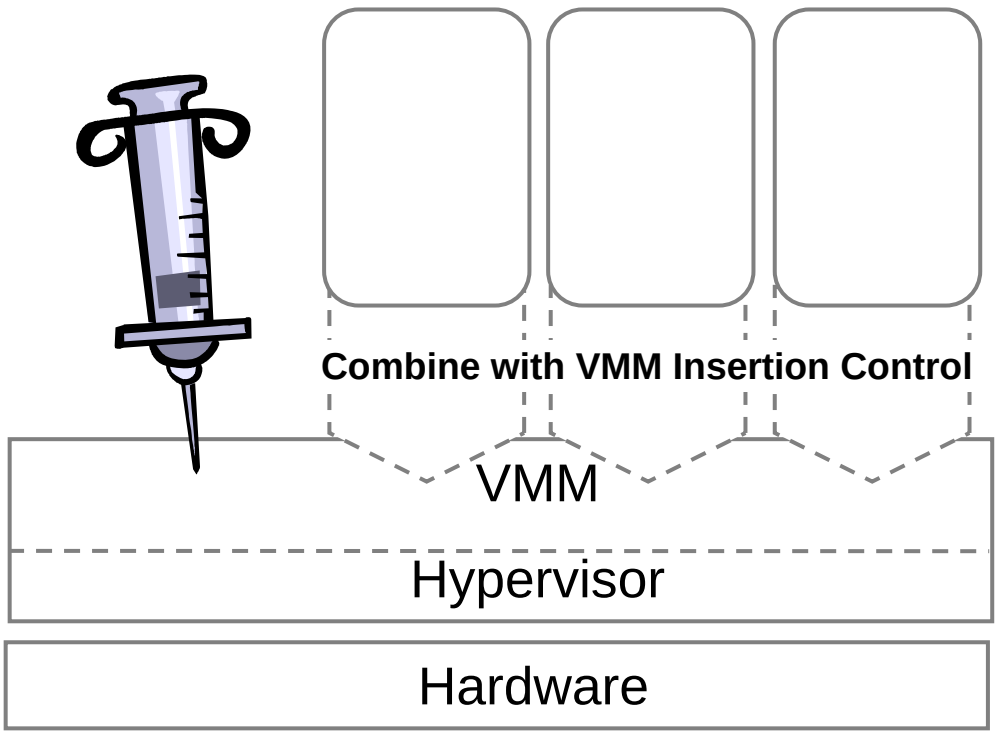
Security and management policy can be "injected" when and where needed into server and desktop workloads



Gartner

Contextual and On-Demand Provisioning of Security Policy Enforcement

Security and management policy can be "injected" when and where needed into server and desktop workloads

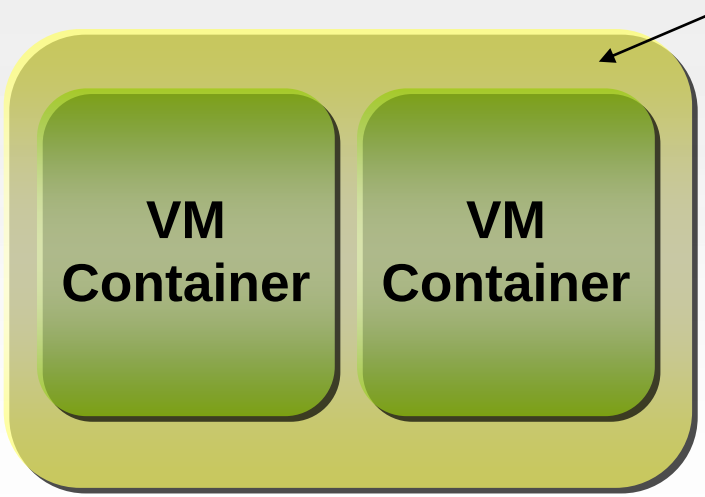


Examples:

- Based on context: time of day, location, sensitivity of workload
- Hot patching
- "Batten down the hatches"
- Unmanaged workloads
- Nonconformant workloads that try to insert into the VMM
- Enterprise workloads hosted on nonenterprise systems (for example, "in the cloud")
- During a full audit, inject monitoring and logging agents

Gartner

Decoupled from Hardware, Workloads Become Mobile



Open Virtualization Format (OVF):

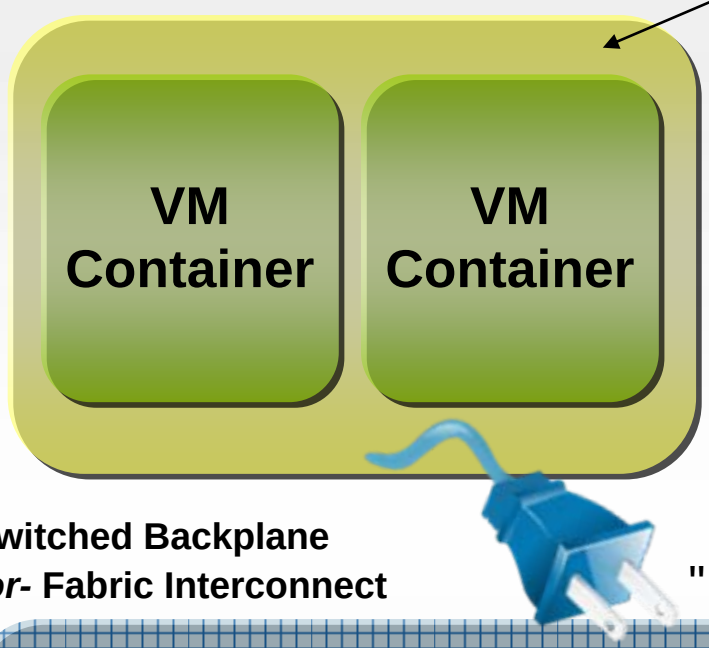
Wrap (package) the VM in XML-based metadata, digitally signed for tamper resistance.

Can specify:

- Memory requirements
- Processor requirements
- Storage requirements
- Networking requirements
- VM dependencies and load order

Gartner

Decoupled from Hardware, Workloads Become Mobile

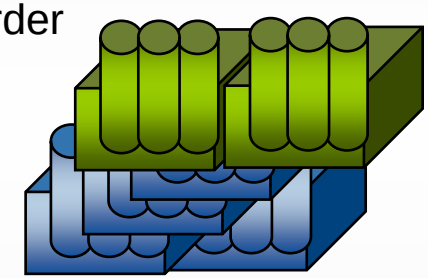


Open Virtualization Format (OVF):

Wrap (package) the VM in XML-based metadata, digitally signed for tamper resistance.

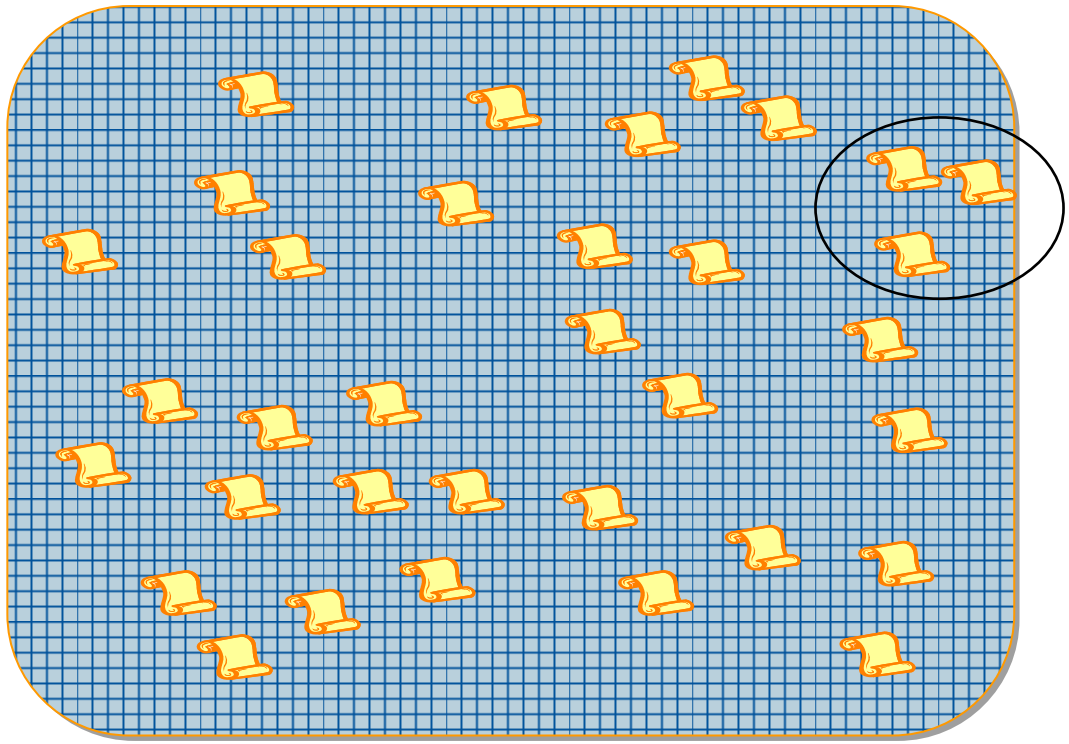
Can specify:

- Memory requirements
- Processor requirements
- Storage requirements
- Networking requirements
- VM dependencies and load order



Gartner

Enables Adaptive Logical Zoning to Enforce Security and Operational Policy

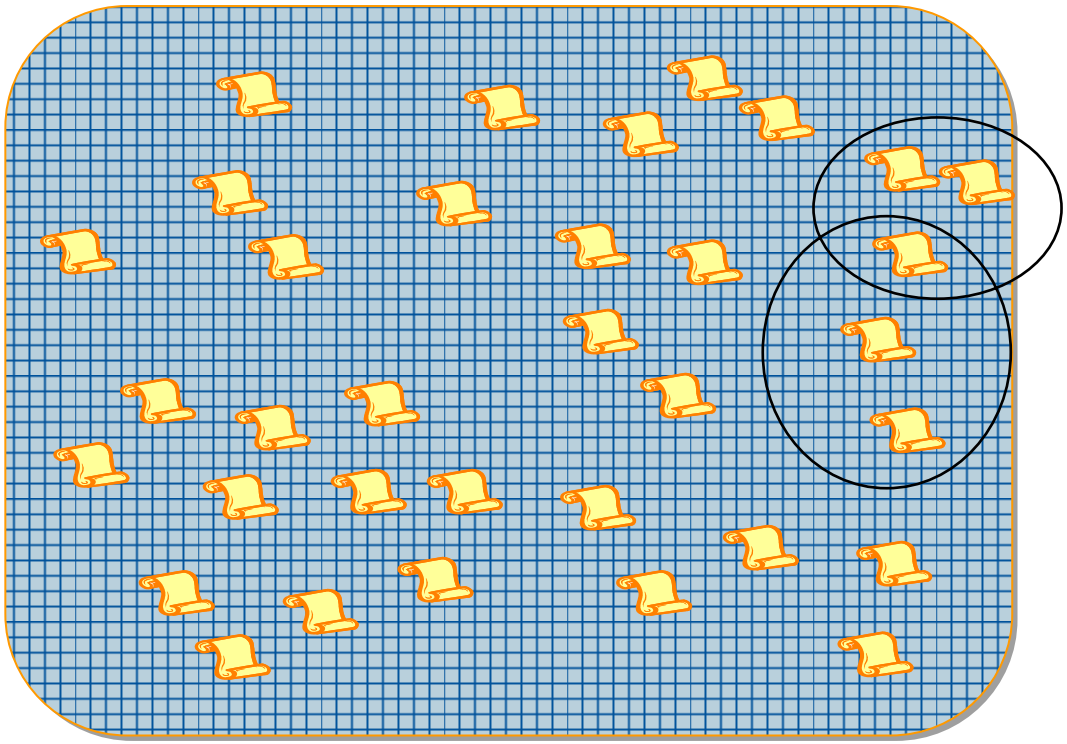


Security Zones

- DMZ-related workloads

Gartner

Enables Adaptive Logical Zoning to Enforce Security and Operational Policy

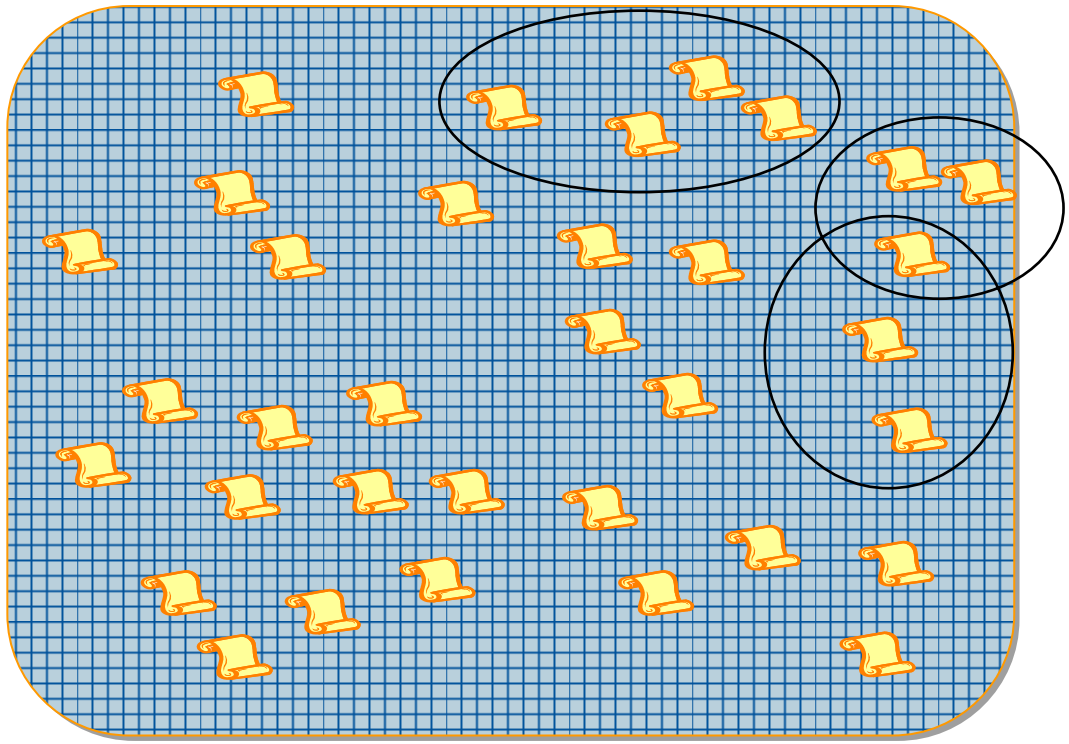


Security Zones

- DMZ-related workloads
- PCI-related workloads

Gartner

Enables Adaptive Logical Zoning to Enforce Security and Operational Policy

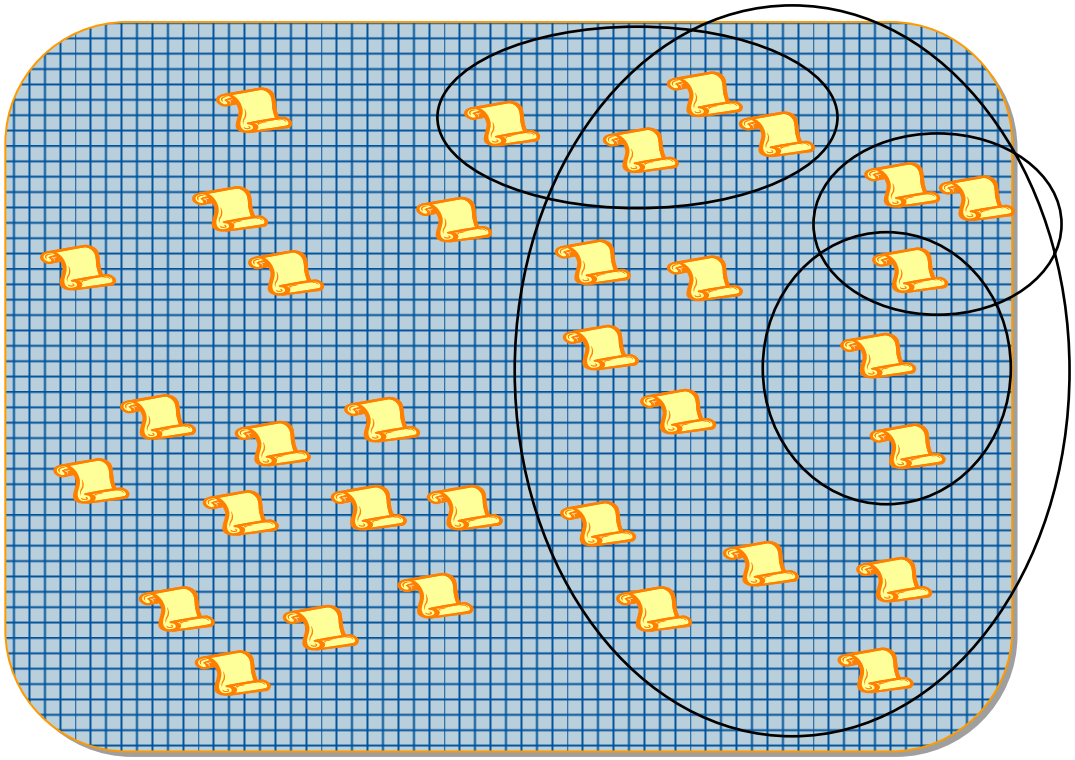


Security Zones

- DMZ-related workloads
- PCI-related workloads
- HIPAA-related workloads
- Servers with sensitive data
- Financial close related workloads

Gartner

Enables Adaptive Logical Zoning to Enforce Security and Operational Policy



Security Zones

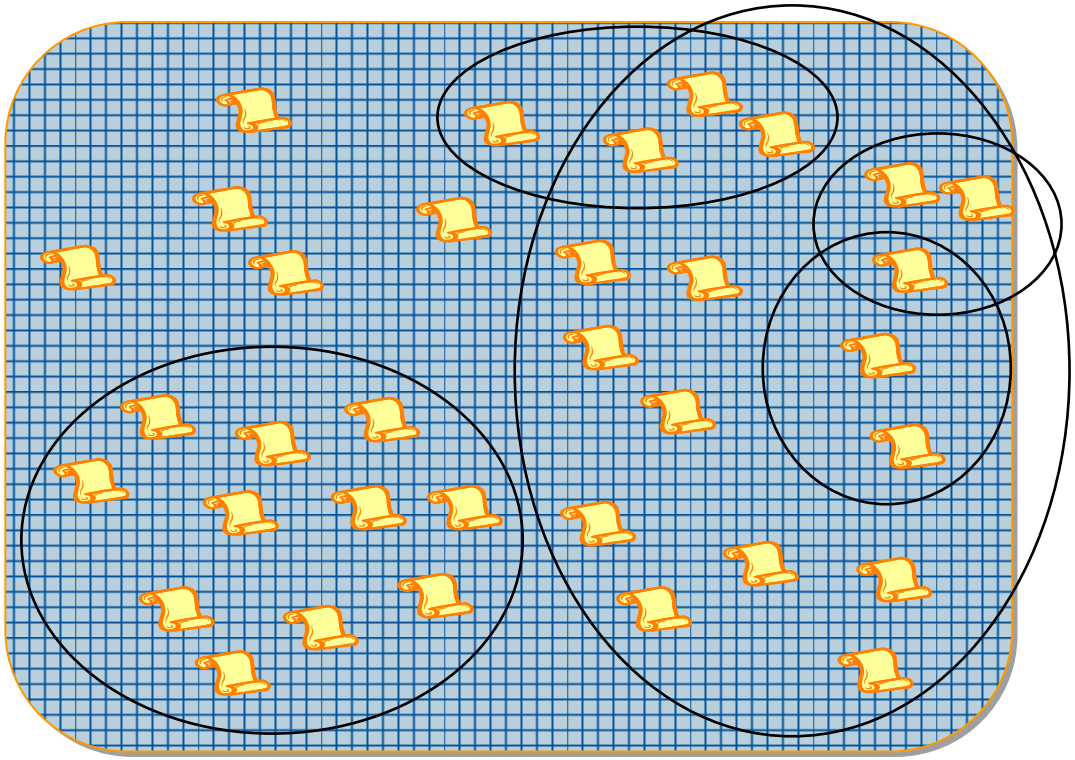
- DMZ-related workloads
- PCI-related workloads
- HIPAA-related workloads
- Servers with sensitive data
- Financial close related workloads

Operational Zones

- Highest availability

Gartner

Enables Adaptive Logical Zoning to Enforce Security and Operational Policy



Security Zones

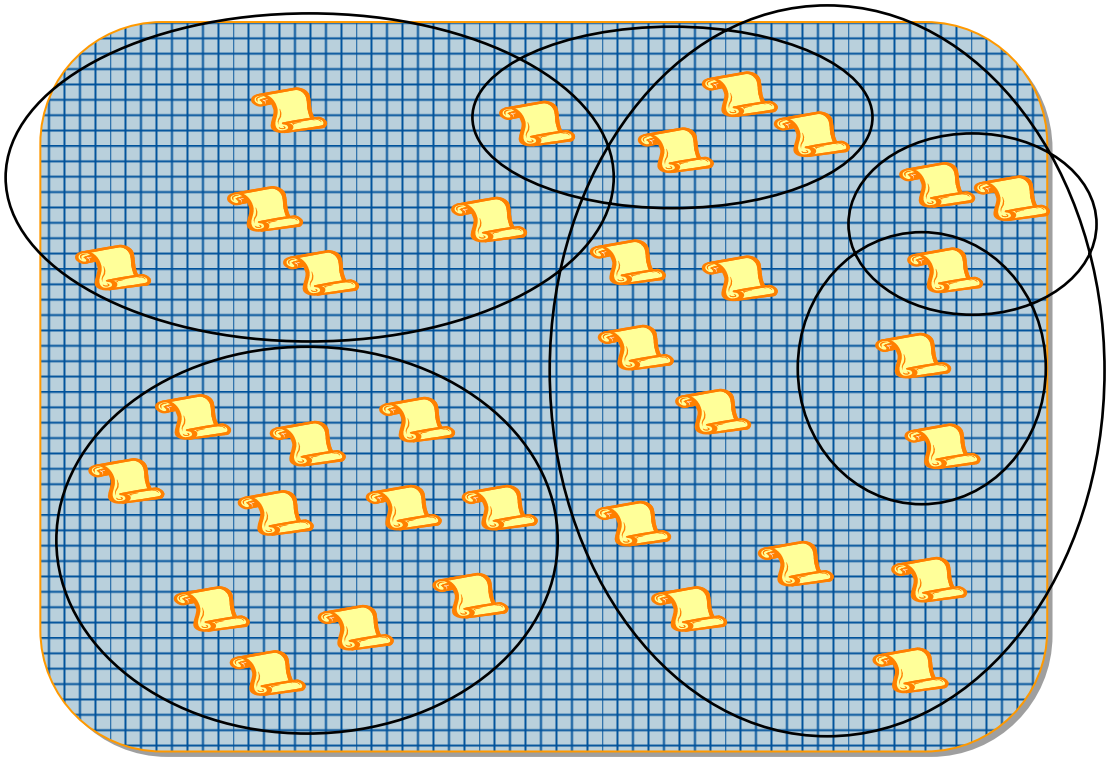
- DMZ-related workloads
- PCI-related workloads
- HIPAA-related workloads
- Servers with sensitive data
- Financial close related workloads

Operational Zones

- Highest availability
- High availability

Gartner

Enables Adaptive Logical Zoning to Enforce Security and Operational Policy



Security Zones

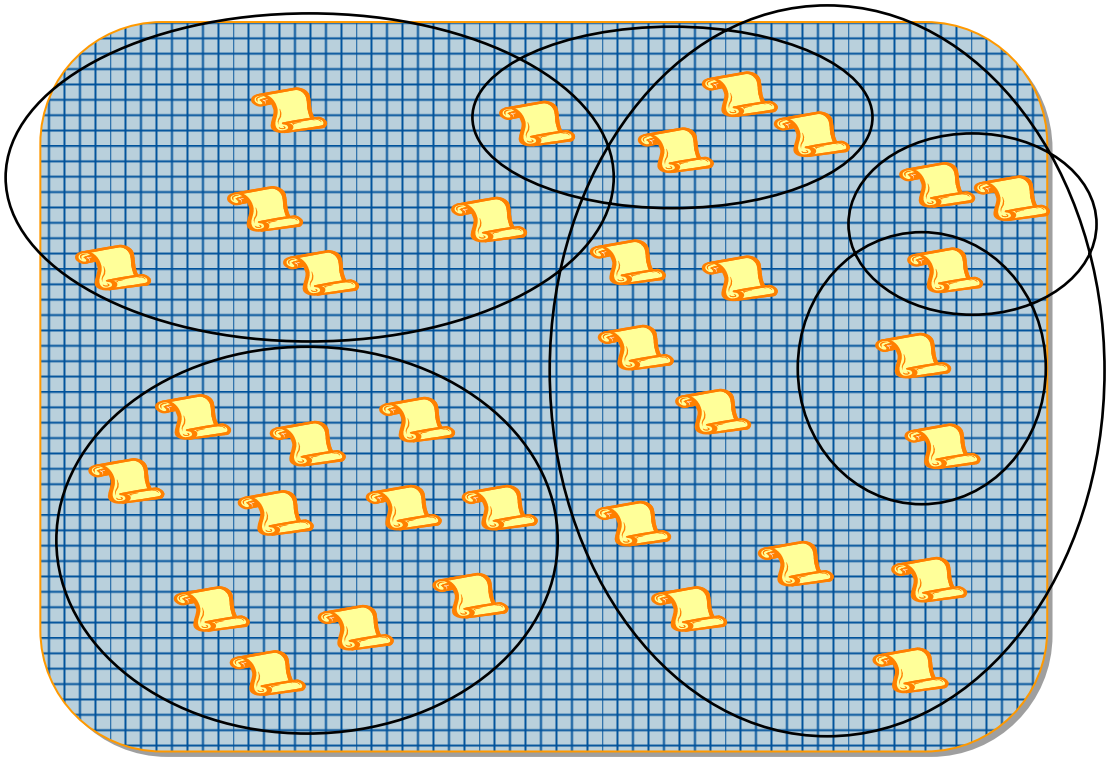
- DMZ-related workloads
- PCI-related workloads
- HIPAA-related workloads
- Servers with sensitive data
- Financial close related workloads

Operational Zones

- Highest availability
- High availability
- Medium availability

Gartner

Enables Adaptive Logical Zoning to Enforce Security and Operational Policy



Virtualization Enables Adaptive Zones

- Move with workload
- Can overlap and be combined
- Independent of network topology
- Policy can change based on context (e.g. time of month, in an outbreak)

Security Zones

- DMZ-related workloads
- PCI-related workloads
- HIPAA-related workloads
- Servers with sensitive data
- Financial close related workloads

Operational Zones

- Highest availability
- High availability
- Medium availability

Gartner

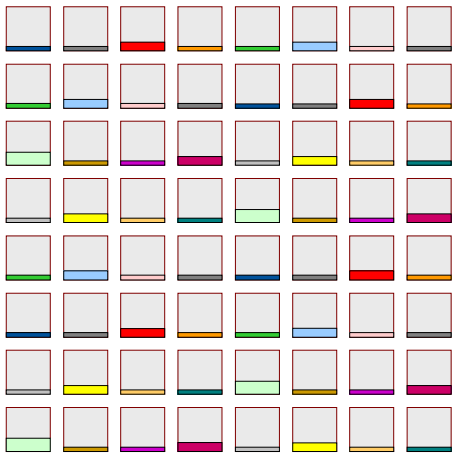
The (R)evolution of the Data Center (and Private Cloud Computing)

Real-Time Infrastructure

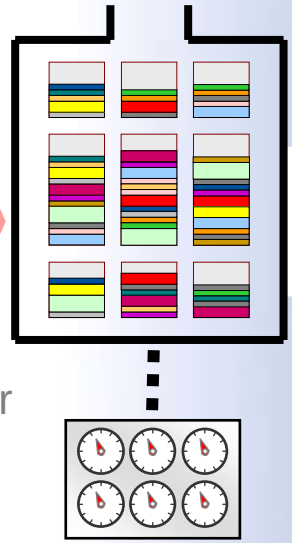
Sprawled
Component-Orientation

Virtualized
Layer-Orientation

Automated
Service-Orientation

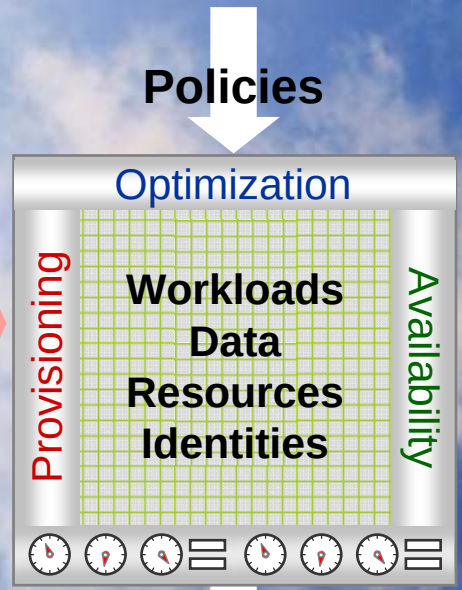


Asset, power costs down, flexibility up



Cloud-enabled

Service levels and agility up



2002

2002 to 2012

2010 to 2020

Pool of flexible, manageable capacity

Gartner

Cloud Computing: Definition and Key Attributes

Cloud Computing

A style of computing where scalable and elastic IT-enabled capabilities are delivered as a service to ~~external~~ customers using Internet technologies

Gartner

Cloud Computing: Definition and Key Attributes

Consumer

Requirements   Results

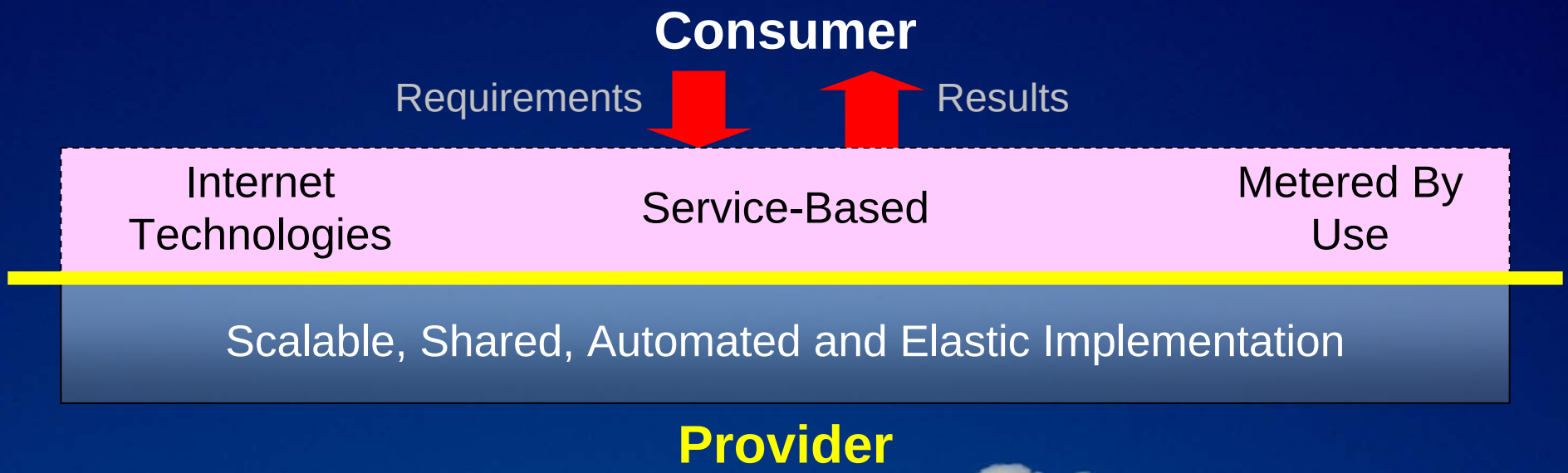
Provider

Cloud Computing

A style of computing where scalable and elastic IT-enabled capabilities are delivered as a service to ~~external~~ customers using Internet technologies

Gartner

Cloud Computing: Definition and Key Attributes

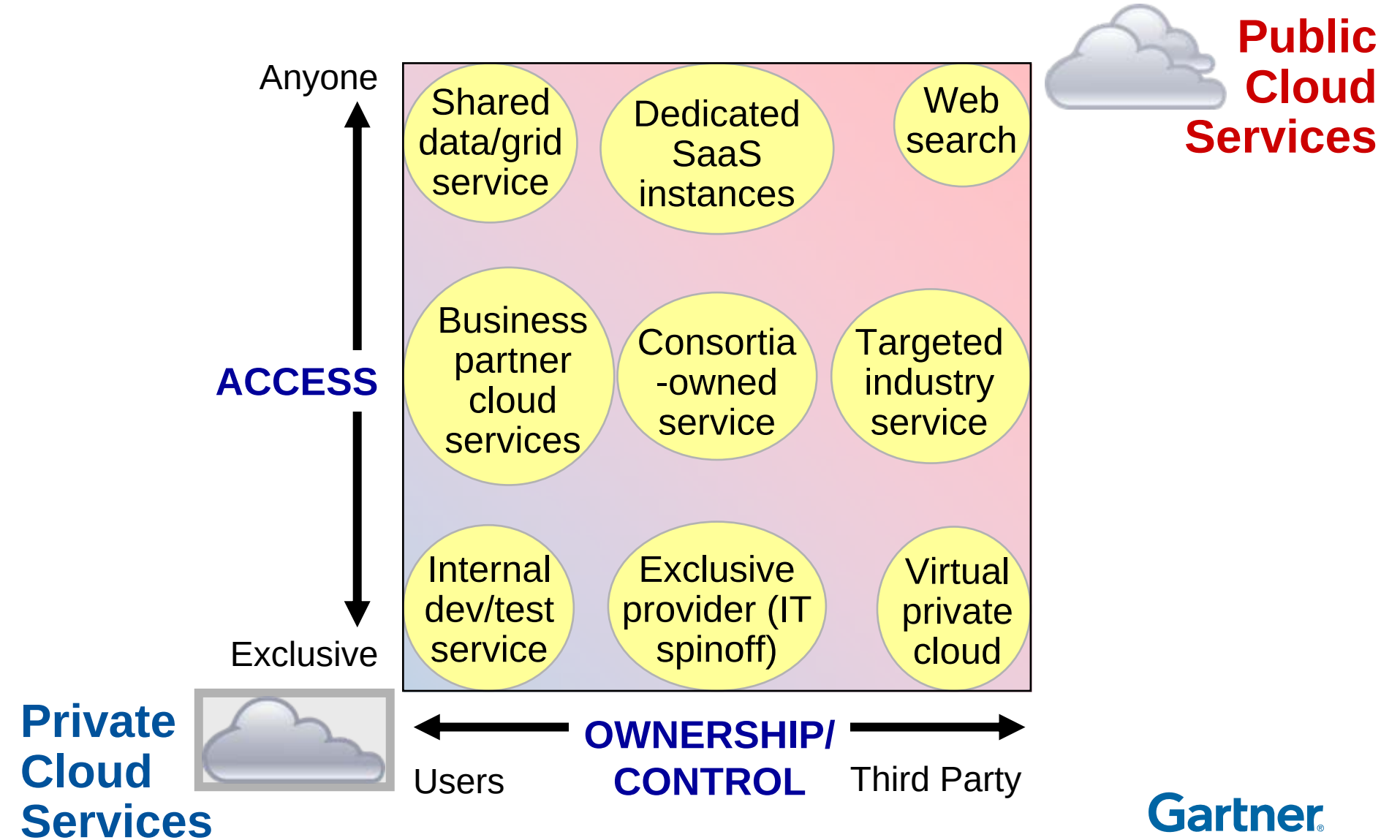


Cloud Computing

A style of computing where scalable and elastic IT-enabled capabilities are delivered as a service to ~~external~~ customers using Internet technologies

Gartner

The Spectrum of Private to Public Cloud Services



Gartner

Adaptive Security Infrastructure Will Require Changes in People, Process and Technology

Conventional Wisdom	New Mind-Set
Trust is binary	Trustability; reputation services
Point solutions	Platforms that correlate and share
Rigid, fixed rules hard-coded to applications and boxes	Contextual policies externalized and virtualized, delivered as a service
Data location is critical	Location of data shouldn't matter
Security solutions siloed	Security as a system
Security and ops. siloed	Security and ops. integrated
Security added after the fact	Security intent captured at design
"Lockdown"	Composite workspaces
Policies tied to physical	Policies tied to logical
One perimeter, outside in	Many perimeters, add inside out
Protect devices	Protect workloads and information
Deploy all controls possible to avoid most risks	Orchestration from a controls palette in a context of managed risk

Gartner

Related Gartner Research

- ***Addressing the Most Common Security Risks in Data Center Virtualization Projects***
  Neil MacDonald (G00173434)

- ***Security Considerations and Best Practices for Securing Virtual Machines***
  Neil MacDonald (G00144828)

- ***Server Virtualization Can Break DMZ Security***
  Neil MacDonald, Greg Young (G00147785)

- ***Tactical Guidelines for Evaluating Virtualization Security Solutions***
  Neil MacDonald (G00163703)

- ***Radically Transforming Security and Management in a Virtualized World: Concepts***
  Neil MacDonald (G00167598)

- ***Radically Transforming Security and Management in a Virtualized World: Considerations***
  Neil MacDonald (G00156107)

Gartner

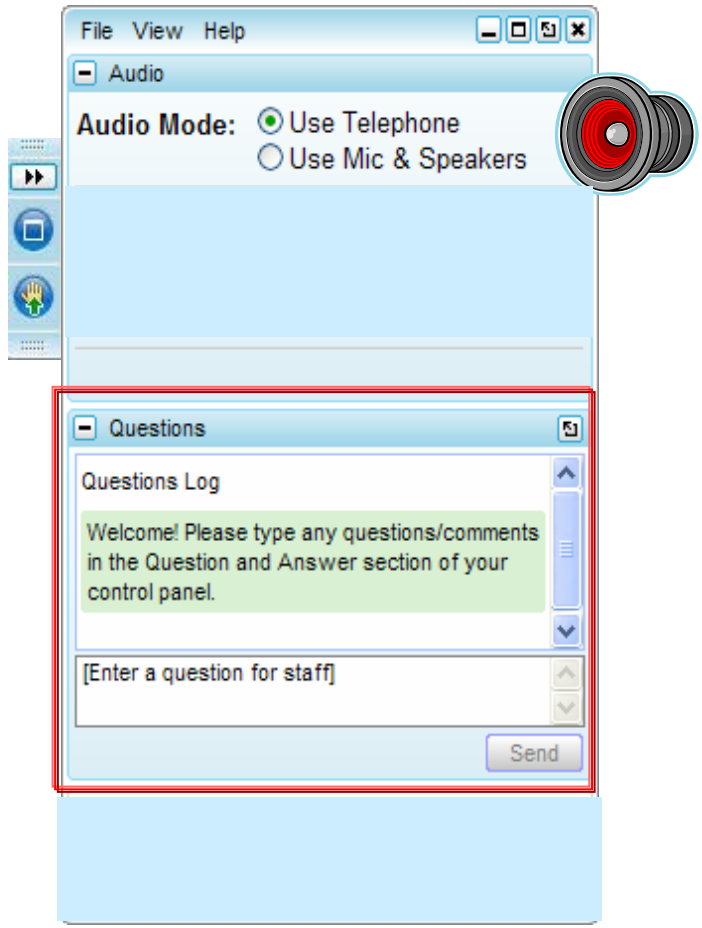
Recommendations

- ✓ Don't let operations-led projects lower your security profile. Engage in a discussion of the issues now, not after the fact.
- ✓ Take part of the virtualization TCO savings and fund security efforts.
- ✓ Pressure security and virtualization vendors to plug the major gaps highlighted in this presentation:
  - Pressure your security vendors to provide tools that natively support virtualized environments — VMs, host OSs, hypervisors.
  - Provide offline VM image integrity, patching, configuration and updates.
  - Move to trusted hypervisors, VMMs and VMs.
  - Be wary of monolithic VM and VM application "appliances." Understand what's inside before you buy.
  - Require vulnerability assessment vendors to scan for the presence of rogue VMs and appliances at the client and server.
- ✓ Define your standards for secure VM and VMM configuration. Scan to ensure these are followed.
- ✓ VMsafe and similar APIs can enable new approaches to security, but make sure these don’t reduce your overall security profile.
- ✓ Beyond just cost cutting, virtualization provides the foundation for radically new approaches to security and management in the next decade

Gartner®

Thanks for participating!
Do you have any questions?

- If you haven't done so already, please type your questions into the Questions pane.
- We will answer as many of your questions as time permits.



Gartner

Securing the Next-Generation Virtualized Data Center

Neil MacDonald

VP and Gartner Fellow

25 March 2010

Gartner®