managing the risks of virtualization

Chris Wraight
CA Technologies

28 February 2011
Session Number 8951

abstract

Virtualization opens the door to a world of opportunities and well managed virtualization sets the course for cloud. However, in order to get there, organizations must address various risks, including security, that virtualization brings. Some of the security risks are similar to the physical server environment, but are compounded by virtualization technology. The speaker from CA Technologies will discuss how keeping the risks in-check and extending security can make this migration fruitful, and pay off for IT.

virtualization continues to grow

> “There will be more virtual machines deployed on servers during 2011 than in 2001 through 2009 combined”!

> “By 2015, 40% of the security controls used within enterprise data centers will be virtualized, up from less than 5% in 2010.”[2]

1Gartner; “Q&A: Six Misconceptions About Server Virtualization”, Thomas J. Bittman; 29 July 2010

[2] Gartner; **“**From Secure Virtualization to Secure Private Clouds**”**; Neil MacDonald & Thomas J. Bittman; 13 October 2010

agenda

- **Technology Overview**
- Identity and Access Management Risks
- Mitigating the Risks
- Session summary

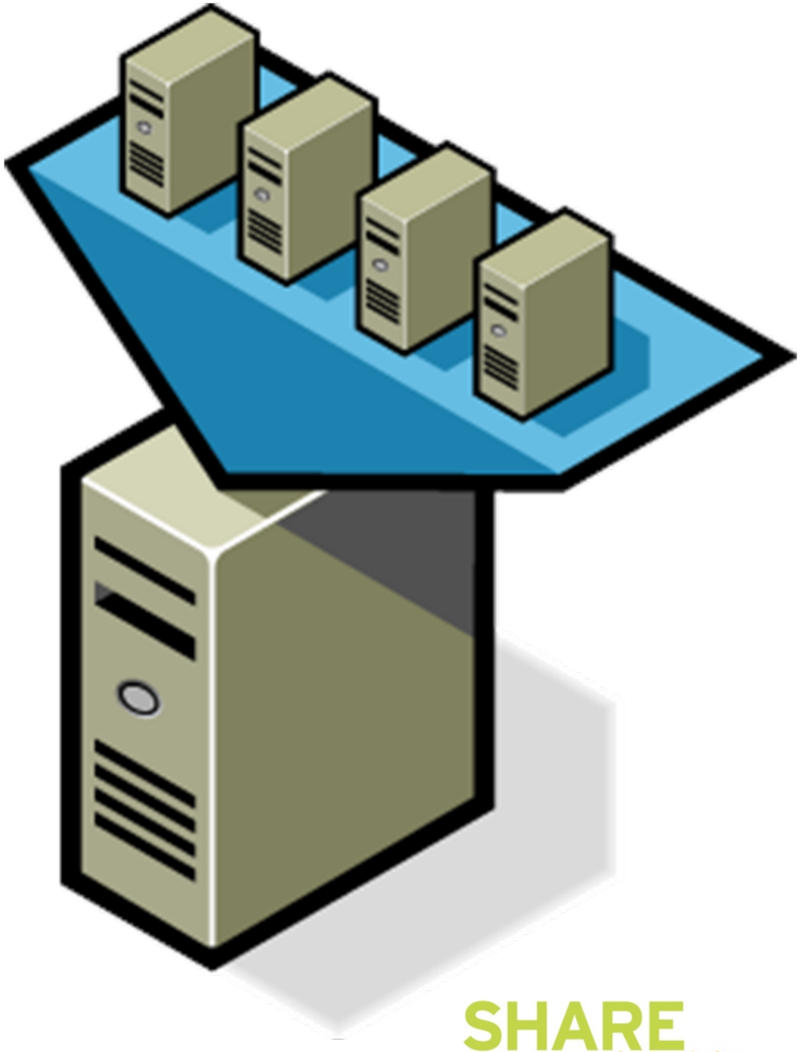
virtualization technology overview

Terms Used in this presentation:

- Virtualization “host” platform
- “guest” OS VMs, partitions
- Privileged partition (admin)
  - Hypervisor

Virtualization Architectures:

- *Hosted - VMware Workstation, Microsoft Virtual PC*
- ‘Bare metal’
- Hypervisor-based – VMWare ESX, IBM LPAR, HP VPAR
- OS-based – Solaris 10

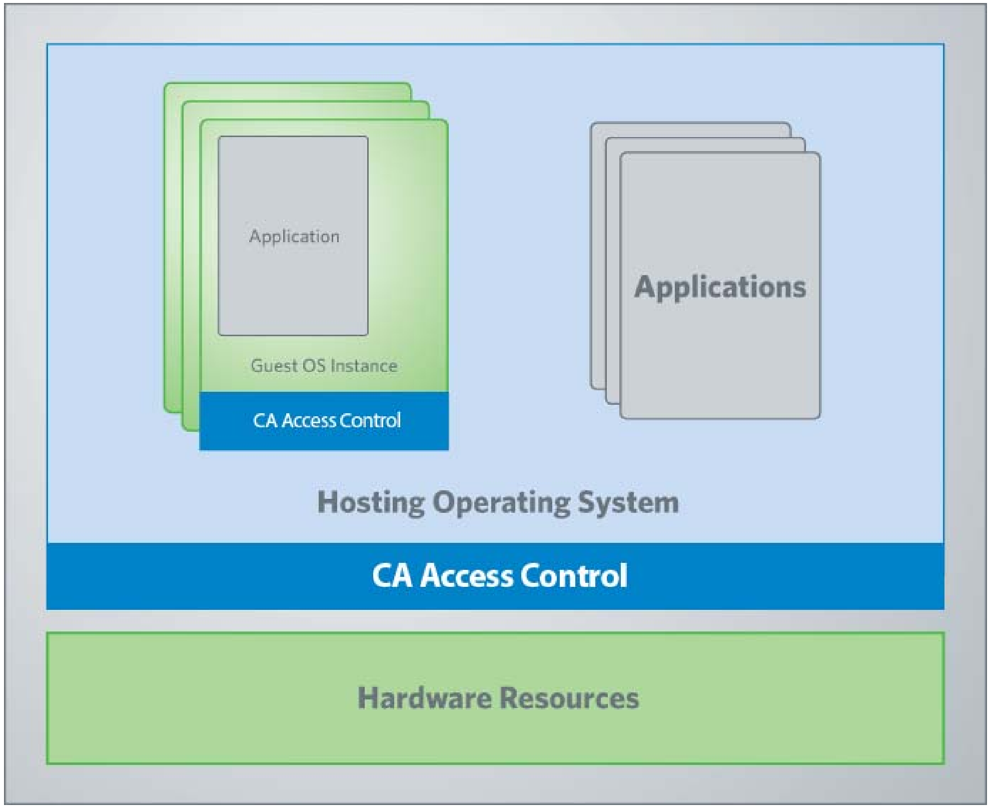


virtualization technology overview (cont'd)

Operating system-based virtualization.

- Virtualization is native to the host operating system
- Multiple isolated, virtual environment instances
- Shared OS kernel.
- Homogeneous OS guests

Example: Sun Solaris 10 Containers (Zones).

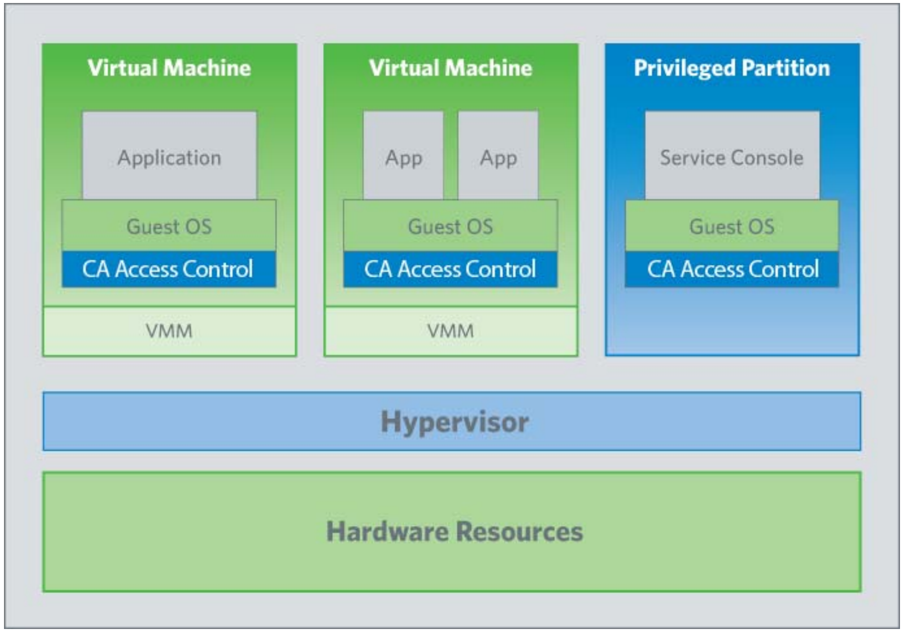


virtualization technology overview (cont'd)

Hypervisor-based virtualization

- "Bare Metal"
- Embedded or implemented in the hosting OS kernel
- Each guest runs on discrete virtual hardware
- VMs may be referred to as partitions

Example: IBM AIX LPAR, HP-UX VPAR and VMware ESX Server.



- Technology Overview
- **Identity and Access Management Risks**
- Mitigating the Risks
- Session summary

how is virtualization different?

- Each physical system becomes more critical
- A new level of administration is introduced
- Unstructured physical boundaries
- Unstructured time dimension
- Heterogeneous dynamic environments

the challenges of virtualization

- Hypervisors expose high level of privileges
- Shared resources available to virtualization
- Each virtualized guest has its own hierarchy of privileged access which should be separate from infrastructure
- VM ‘sprawl’
- Structured and unstructured data on virtualized environments is unsecure
- No central authentication source

the challenges of virtualization

- Regulatory requirements still apply
- Auditing access and identities is difficult in virtualized environments
- Privileges in a virtualized environment not well defined
- Decentralized privileged user administration (incl. virtual environments)

unstructured physical boundaries

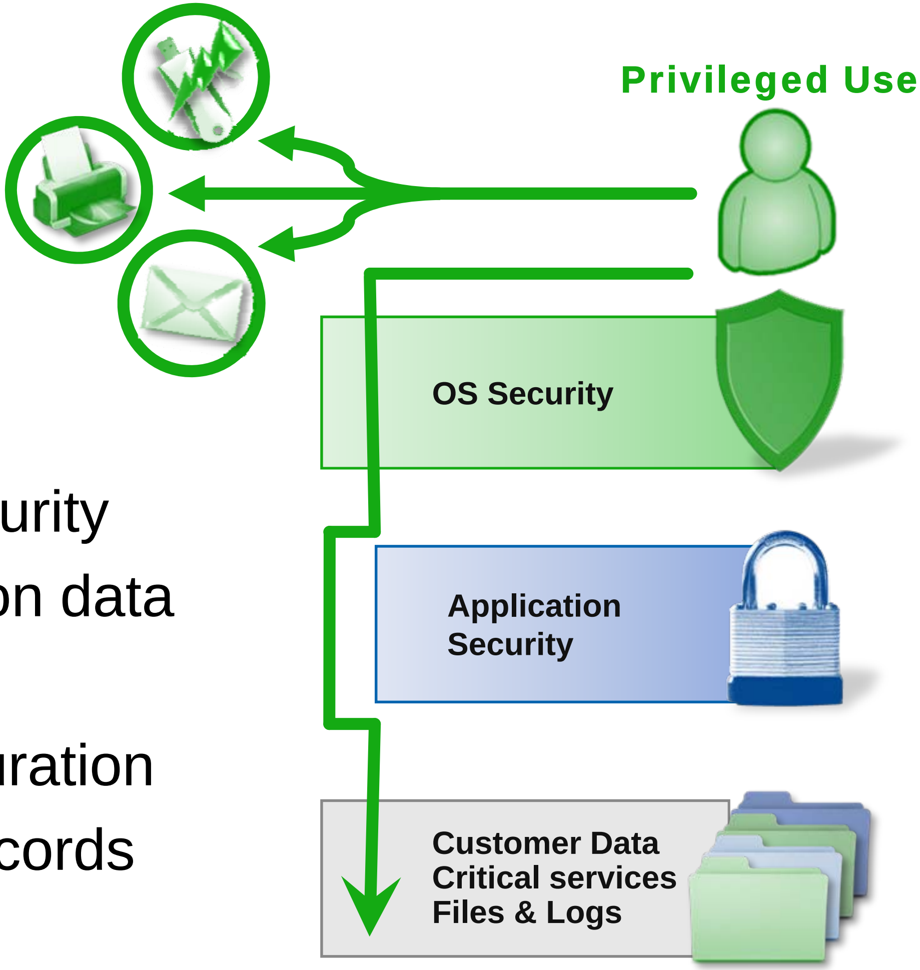
- VM mobility beyond the server room
  - VMs can be copied, or cloned
  - Machine memory is accessible from the host
  - Disk space can be accessed from storage
- Challenging physical security
  - Copying a VM = Stealing a server from the server room
  - The virtual DC is distributed – Not a mainframe

managing the 4th dimension - time

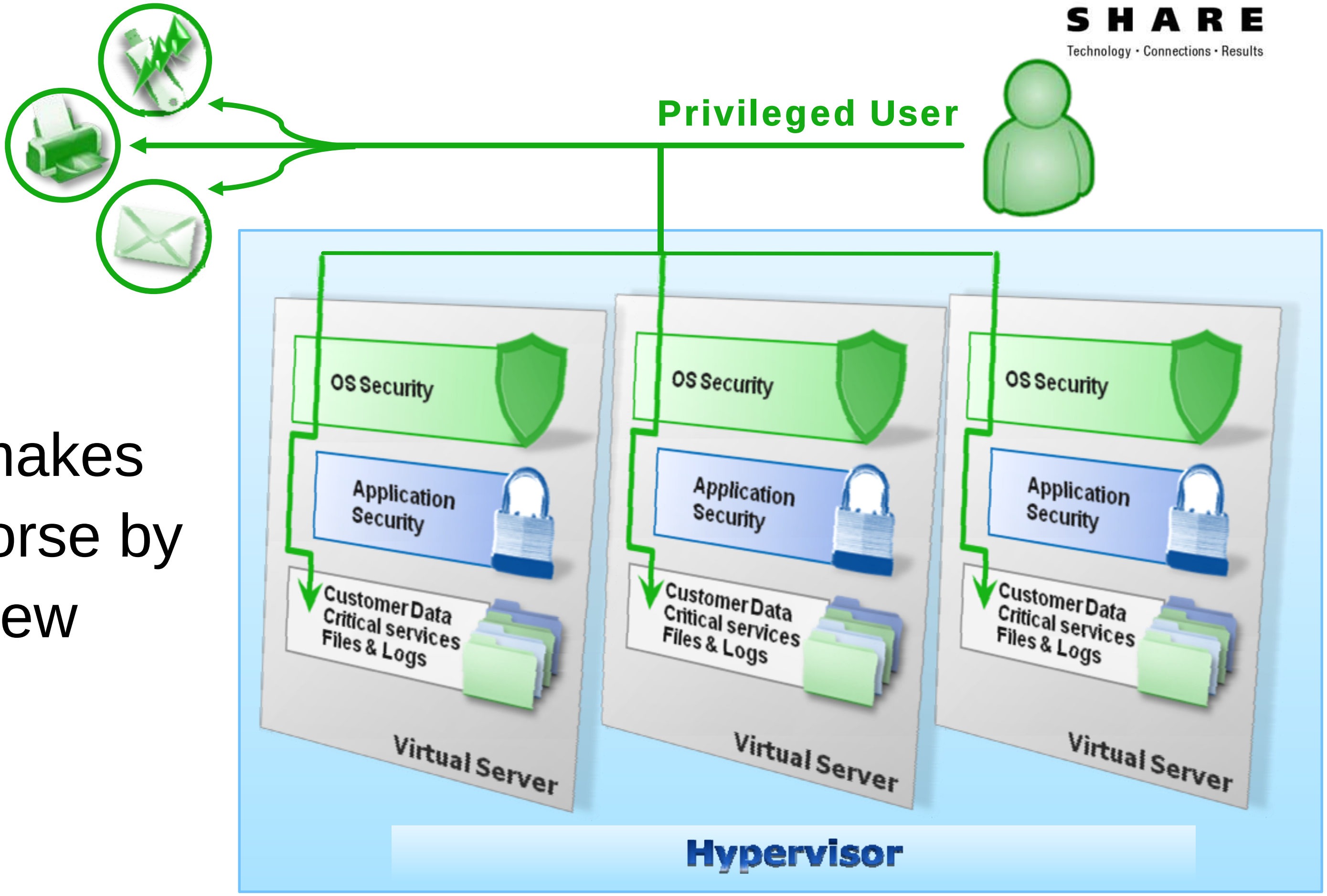
- What happens when we revert to prior snapshot?
  - **<u>Lose</u>** audit events
  - **<u>Lose</u>** configuration
  - **<u>Lose</u>** security policy
- Am I still compliant with my policy?

the privileged user

- Normal user
  - Is identified
  - Access is controlled
- ‘root’ administrator
  - Is anonymous
  - Can bypass application security
  - Can see and alter application data
  - Can change system files
  - Can change system configuration
  - Can alter logs and erase records



the virtualization privileged user



Virtualization makes the problem worse by introducing a new privilege layer.

unrestricted privileged access

- Data exposure
  - Different business owners
  - VMs can be copied exposing sensitive data
- Business continuity and availability - isolation is not enough!
  - Halting critical VMs
  - Tampering with configurations
- Management and Control
  - Administrators can deploy new VMs very easily
  - Increases the chance for mistakes
  - Improperly-configured VMs can be vulnerable

managing complexity

- Virtualization: Making the complex appear simple
  - Configuration and change management
  - Network management
  - Storage management
  - Capacity management

managing complexity

- Virtualization: Making the complex appear simple
  - Configuration and Change Management
  - Network Management
  - Storage Management
  - Capacity Management

Handled by IT Management

- But what about security management?
  - Heterogeneous VMs
  - Highly-distributed
  - Dynamically changing
- How do I manage the complexity?

audit, audit, audit!

- Each virtualization host becomes more important.
  - One host running many VMs = Critical Infrastructure
  - Critical infrastructure = Business impact
  - Business impact = Compliance requirements
- Compliance requirements mandate additional controls!

compliance and audit

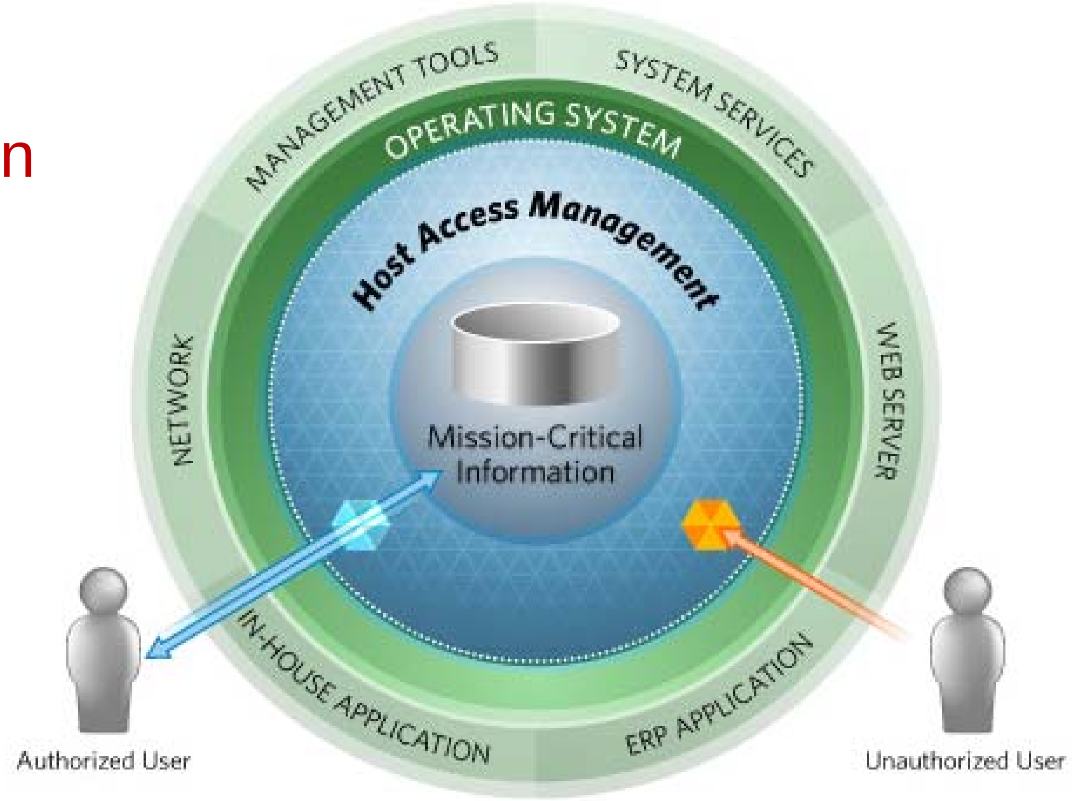
- Virtualization audit issues haven't yet been flagged
- What will drive priorities?
  - Education
  - Compliance and regulatory pressures are expected to increase
  - Public exposure
- Will require adjusted controls for separation of management, and control

- Technology Overview
- Identity and Access Management Risks
- **Mitigating the Risks**
- Session summary

best practices: segregate duties - restrict admins

Segregate Administration

- System
- Virtualization
- Audit



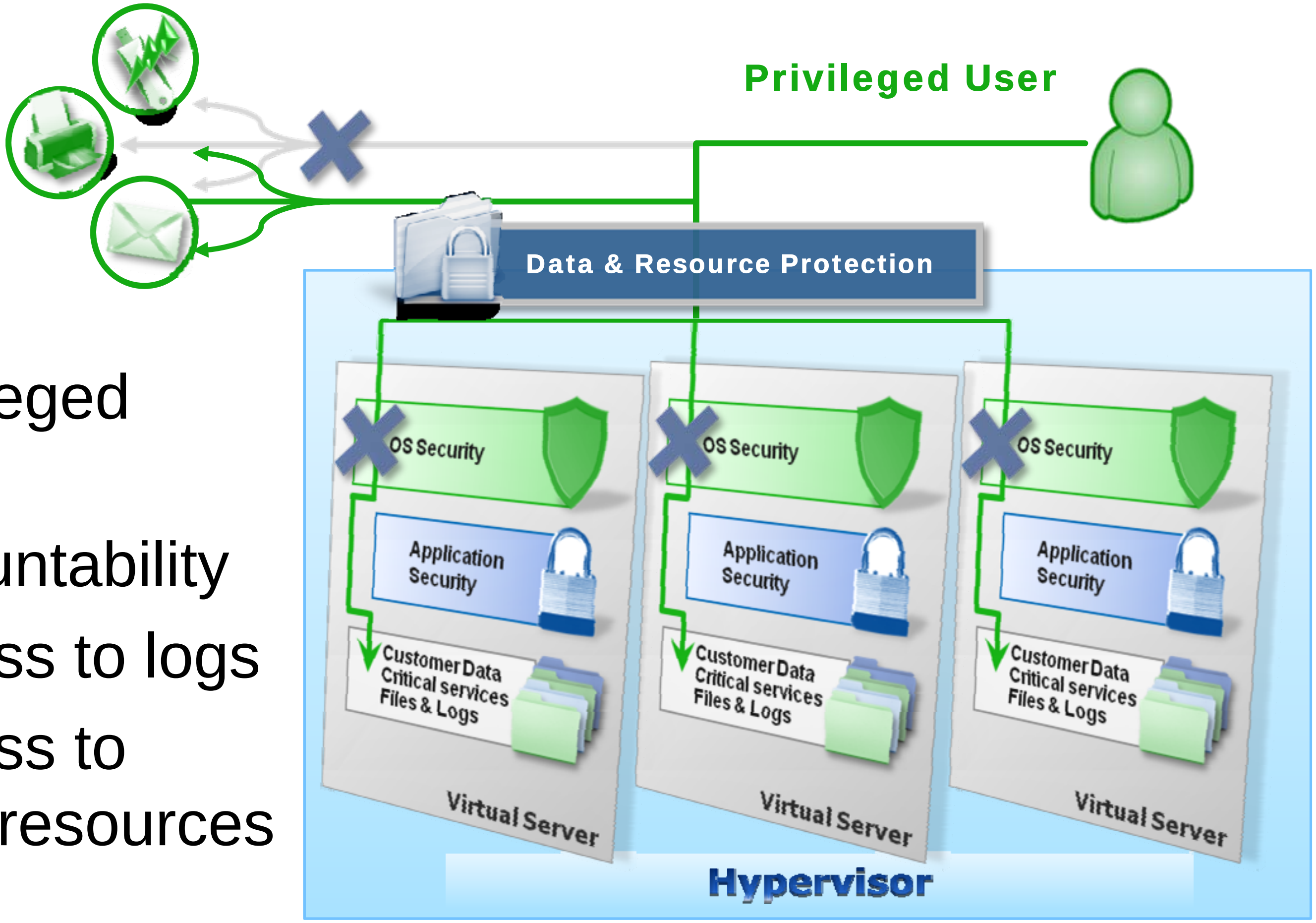
Restrict access to logs

Restrict access to virtualization resources

- Deny sys admins
- Allow only through admin tools

full privileged user management

- Restrict privileged access
- Ensure accountability
- Restrict access to logs
- Restrict access to virtualization resources



central access policy management

- Enforce the policy across all VMs and virtualization platform
- Centralization - Do **not** rely on local policies
- Enforce policy change control
- Manage deviations from the policy
- Report on policy compliance

complete and secure auditing

- Monitor the virtualization platform
  - Monitor administrative activity (including impersonation)
  - Monitor all access to virtualization resources
  - Centralize audit logs
  - Notify on significant events
  - Integrate with SIEM systems

- Technology Overview
- Identity and Access Management Risks
- Mitigating the Risks
- **Session summary**

conclusions

- Security and control are the number one inhibitors to virtualization/cloud adoption by the enterprise
- Automation is an imperative
- Security will become a cloud differentiator
- The IT roles are reversing

apply

- Be aware of the security implications
  - Physical boundaries are changing
  - The definition of time is changing
  - An additional administration layer is introduced
  - The virtualization host is critical infrastructure
- Organizations should prepare now for increasing audit scrutiny
- Demand visibility and control
  - Privileged user access management
  - Consistent security policies
  - Complete and secure auditing

questions and answers

thank you

Chris Wraight
chris.wraight@ca.com
+1 508 628 8134