



Securing Virtual Environments

Richard Park
Senior Product Manager
Sourcefire

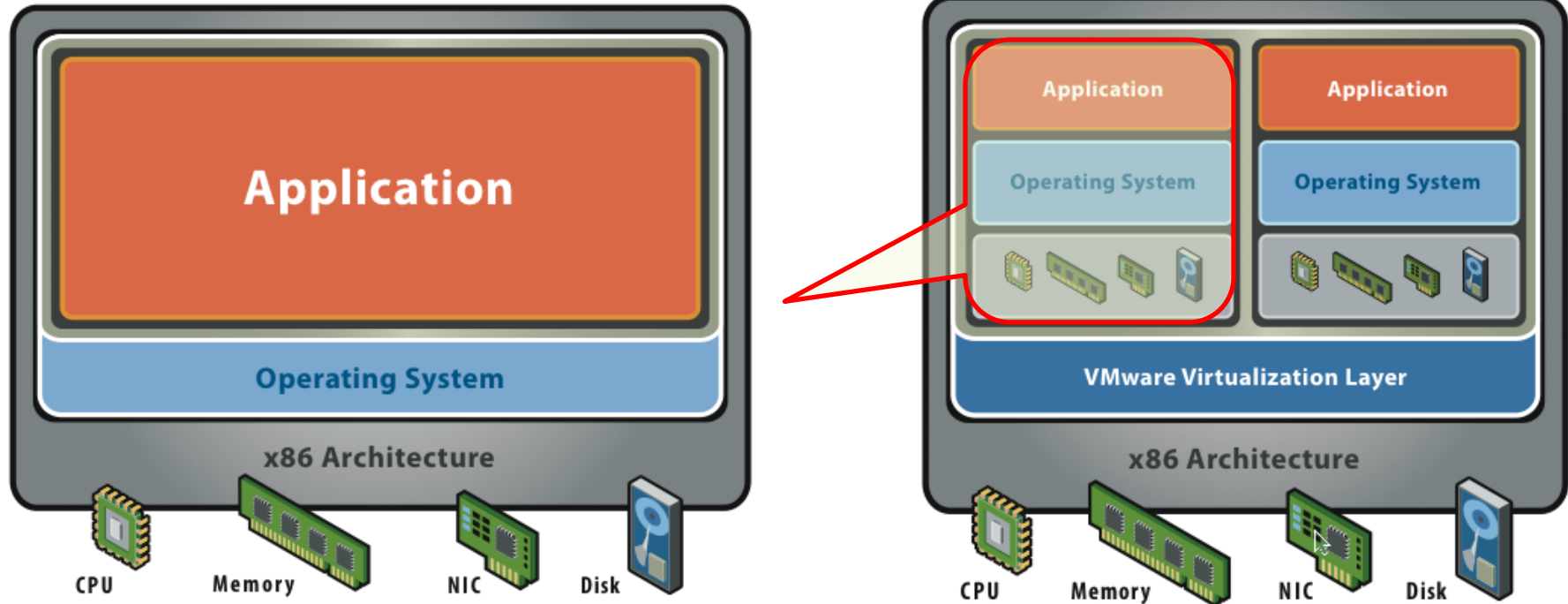


Outline

- 🔥 Benefits and Risks of Virtualization
- 🔥 Best Practices
- 🔥 Architecture for Traffic Monitoring



Benefits of Virtualization

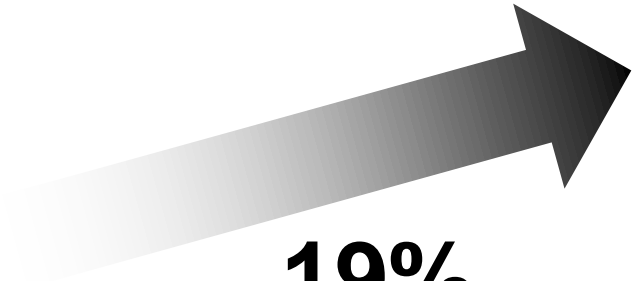


- 🔧 Savings in capital, power, space
- 🔧 Ease of provisioning and disaster recovery
- 🔧 Workload balancing



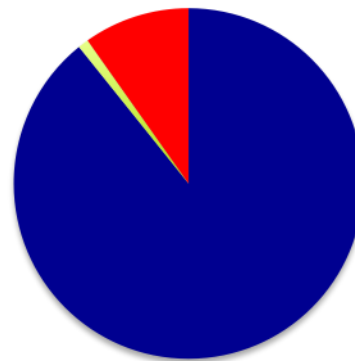
Size of Virtualization Market (2008)

\$2 BILLION



19%

Market Share



- VMware (91%)
- Citrix (1%)
- Other (10%)

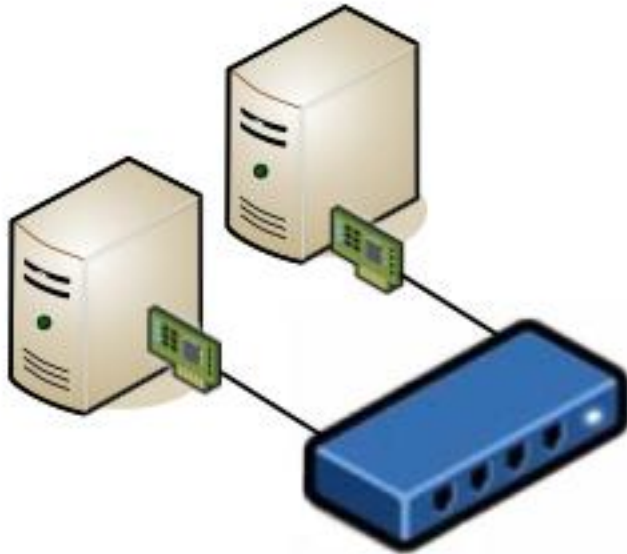


Problems Caused by Virtualization

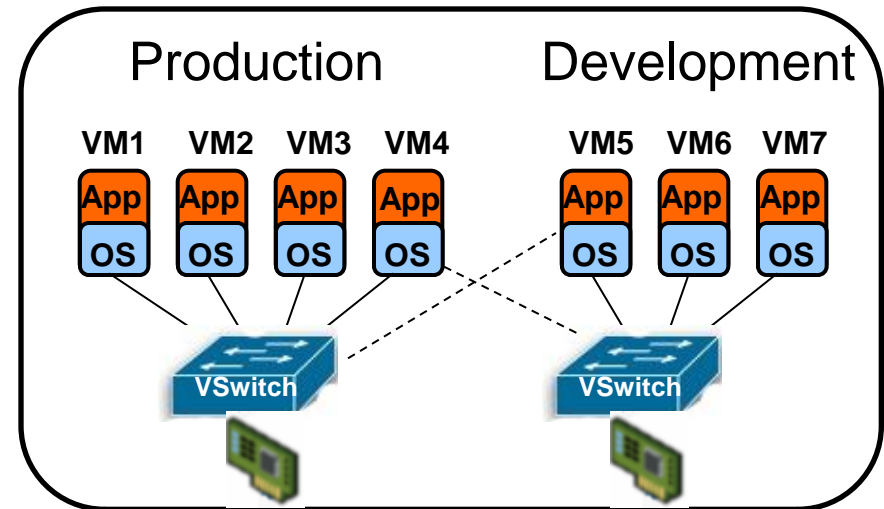


- 🚗 Blind spots
- 🚗 No separation of duties
- 🚗 Virtual machine sprawl

Blind Spots Matter More in Virtual than Physical Networks



The physical network is defined and relatively static.



The virtual network is fluid and very dynamic.



No Separation of Duties

Networking

Security

Storage

Servers



VMware Admin

🔧 Many functions are now configured in VMware

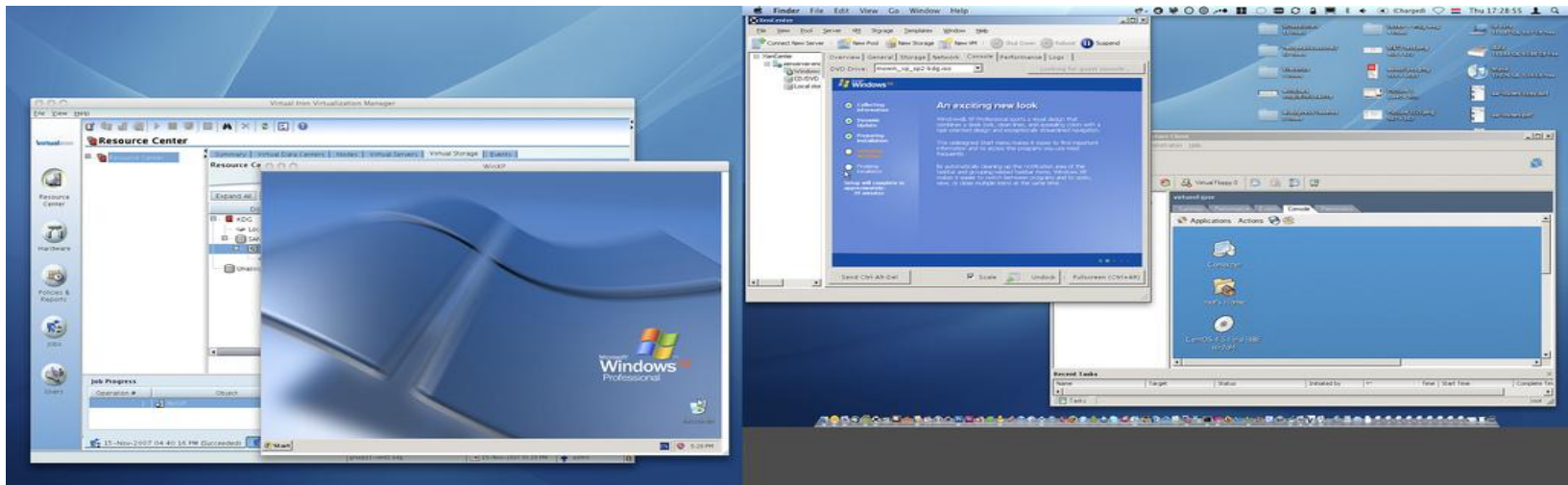
🔧 Misconfigurations are more likely

- Lack of expertise
- Insufficient communication



Virtual Machine Sprawl

- 🔊 Sprawl has multiple causes
 - Deploying VMs without sufficient planning
 - Copying VMs throughout network
 - Rolling back VM snapshots, undoing patches
- 🔊 Sprawl has impact on critical servers
 - Harder to locate and determine config/patch state
- 🔊 Rogue VMs may not be patched and configured





Best Practices

- 🔥 Don't combine in-scope and out-of-scope VMs
- 🔥 Implement one primary function per VM
- 🔥 Enforce least privilege with access controls
- 🔥 Bind sensitive VMs to separate physical network interfaces

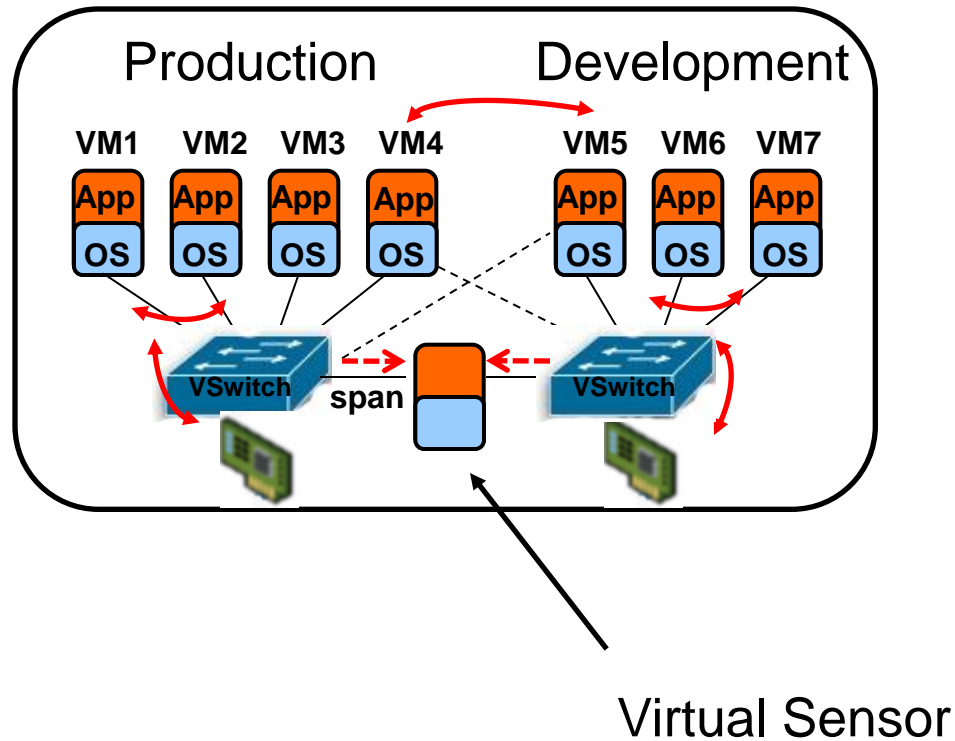
- 🔥 **Implement VM lifecycle management**
- 🔥 **Deploy virtual sensors for greater visibility**



Implement VM Lifecycle Management

- 🔍 Scan and audit VMs prior to deployment
- 🔍 Track VM migrations
- 🔍 Include offline VMs in patching process
- 🔍 Monitor VM snapshots and rollback
- 🔍 Decommission VMs when no longer needed

Monitor Virtual Traffic for Greater Visibility



Relevant PCI Requirements for Virtual Traffic Monitoring



6.3.2: Separate development/test and production environments

The development/test environments are separate from the production environment, with access control in place to enforce the separation.

11.4: Use IDS/IPS to monitor all traffic in the cardholder data environment

Verify the use of IDS/IPS and that all traffic in the cardholder data environment is monitored.



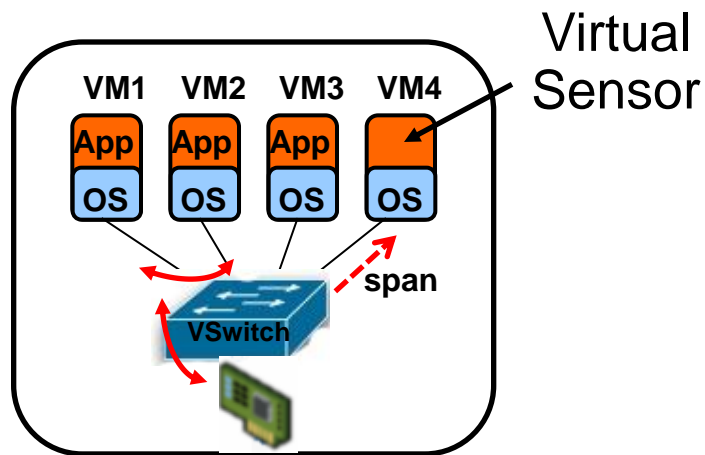
Virtual Traffic Monitoring Scenarios

- 🔥 Passive & Inline Monitoring
- 🔥 Monitoring within a Cluster
- 🔥 Monitoring Physical Traffic (Remote Locations)
- 🔥 Monitoring with a Blade Server

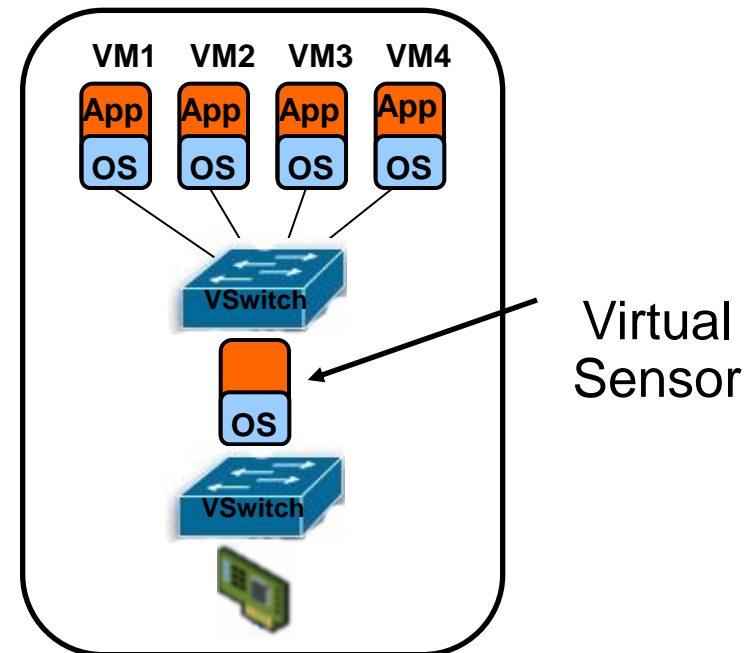


Passive & Inline

Passive Monitoring

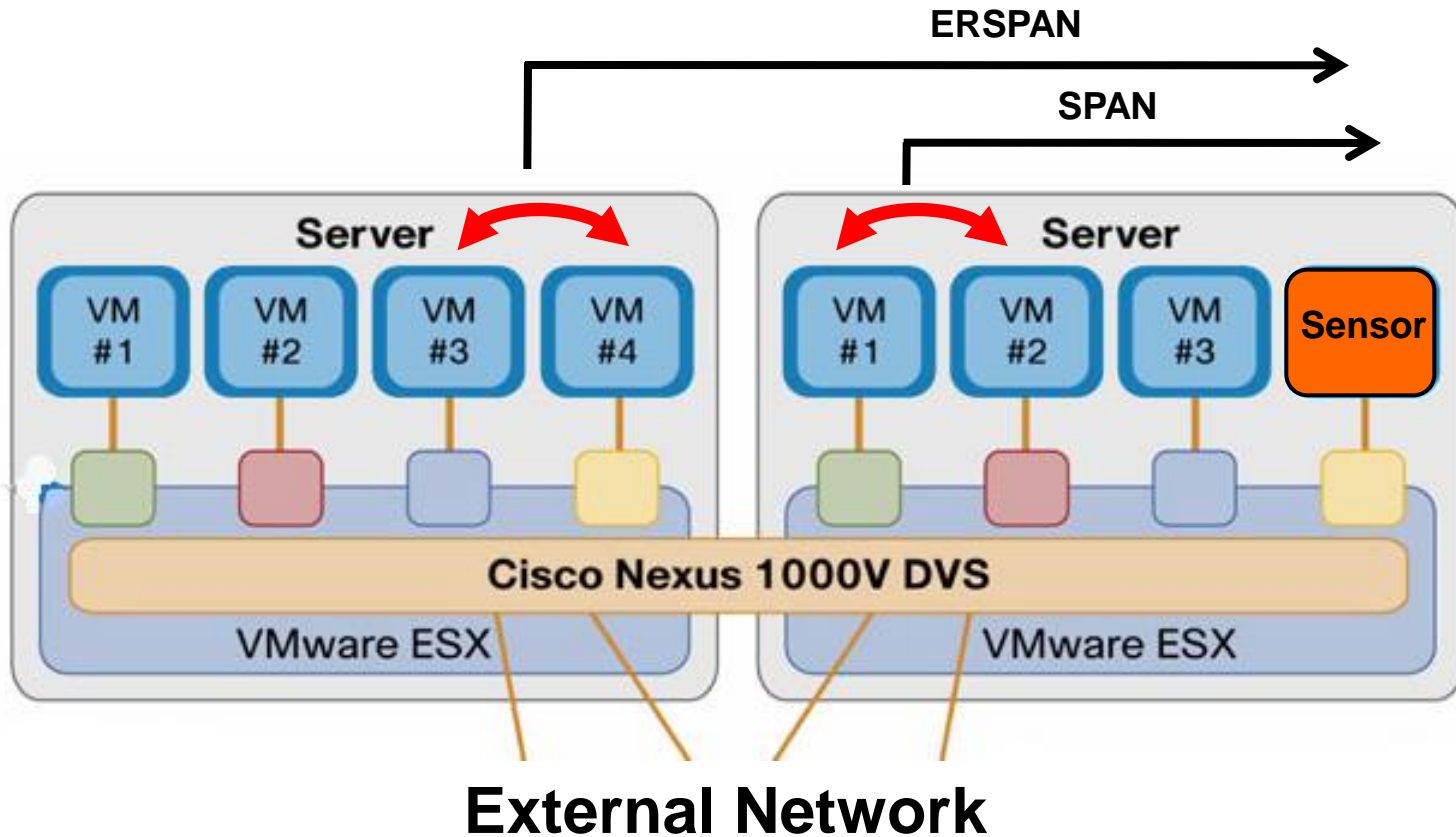


Inline Monitoring



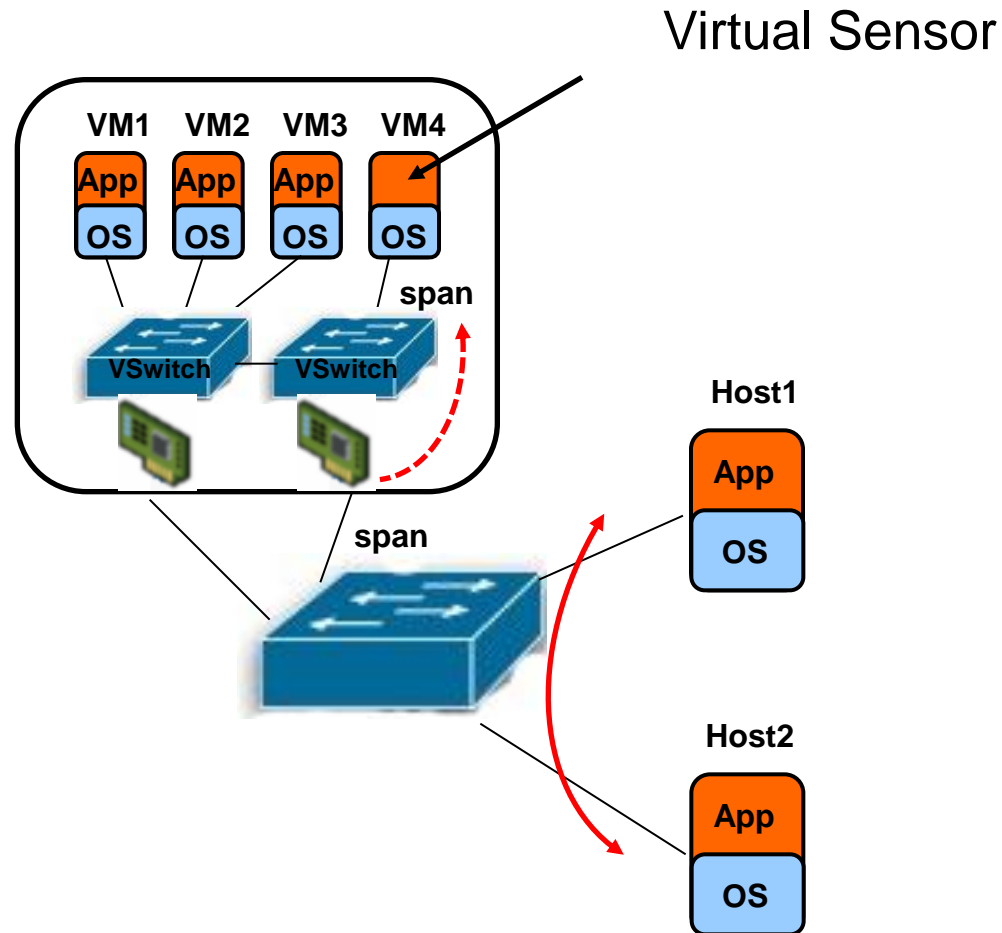


Cluster Monitoring



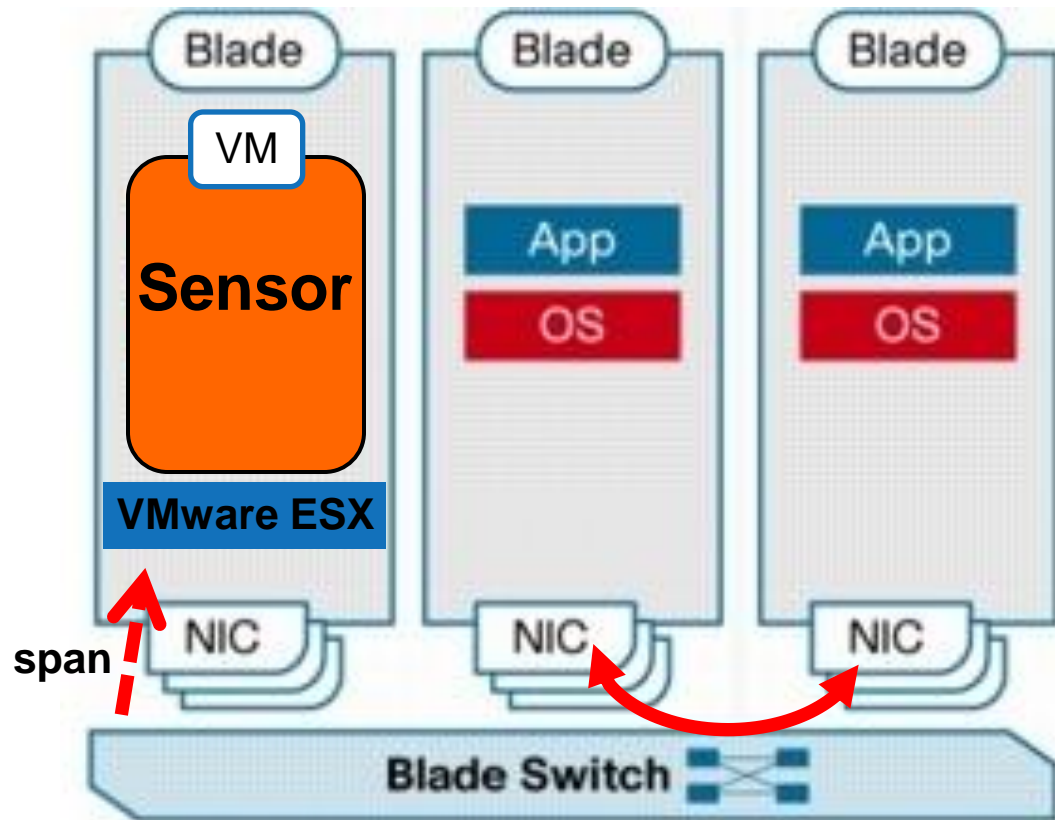


Monitoring Physical Traffic



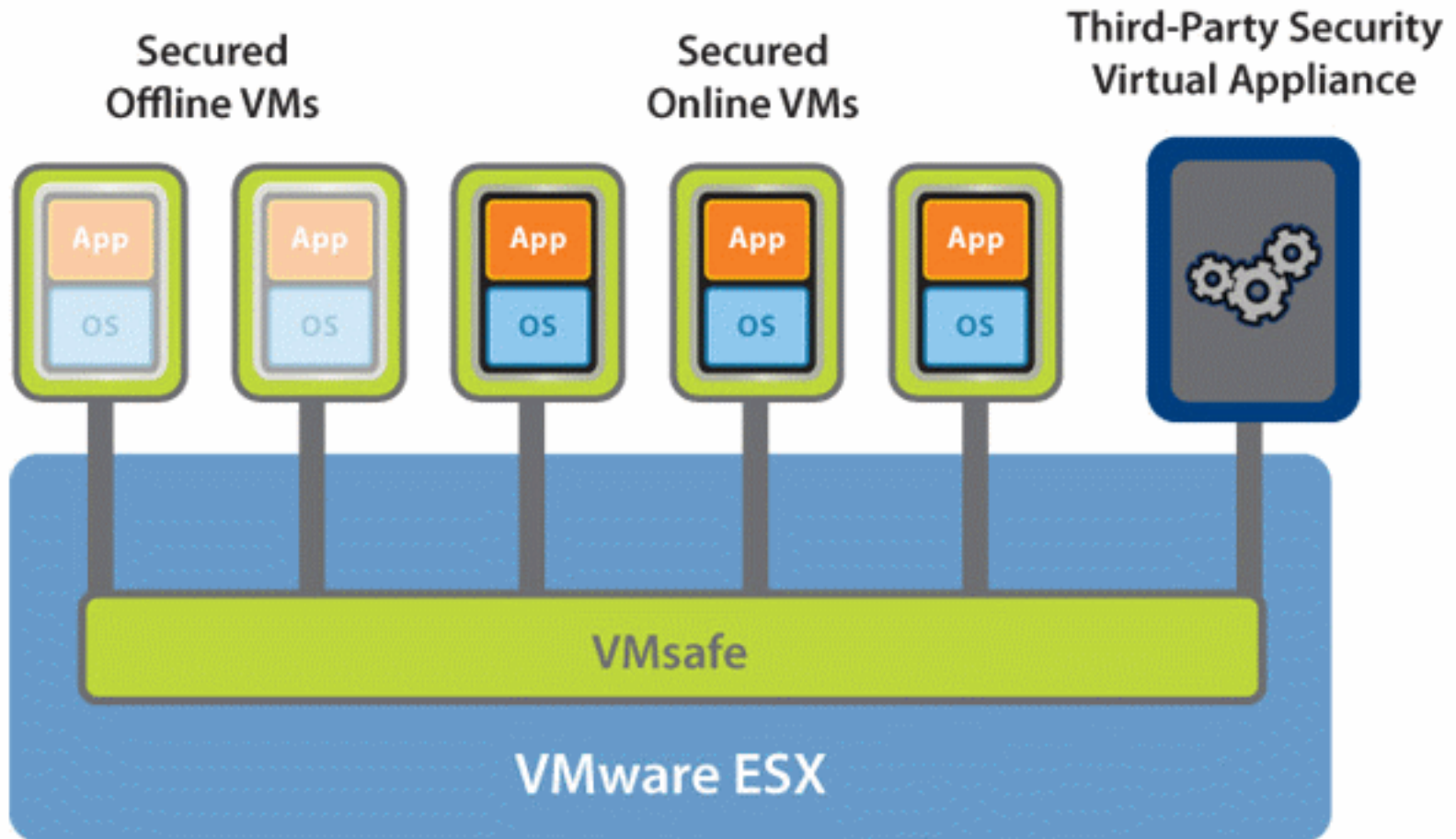


Inspecting in Blade Environment



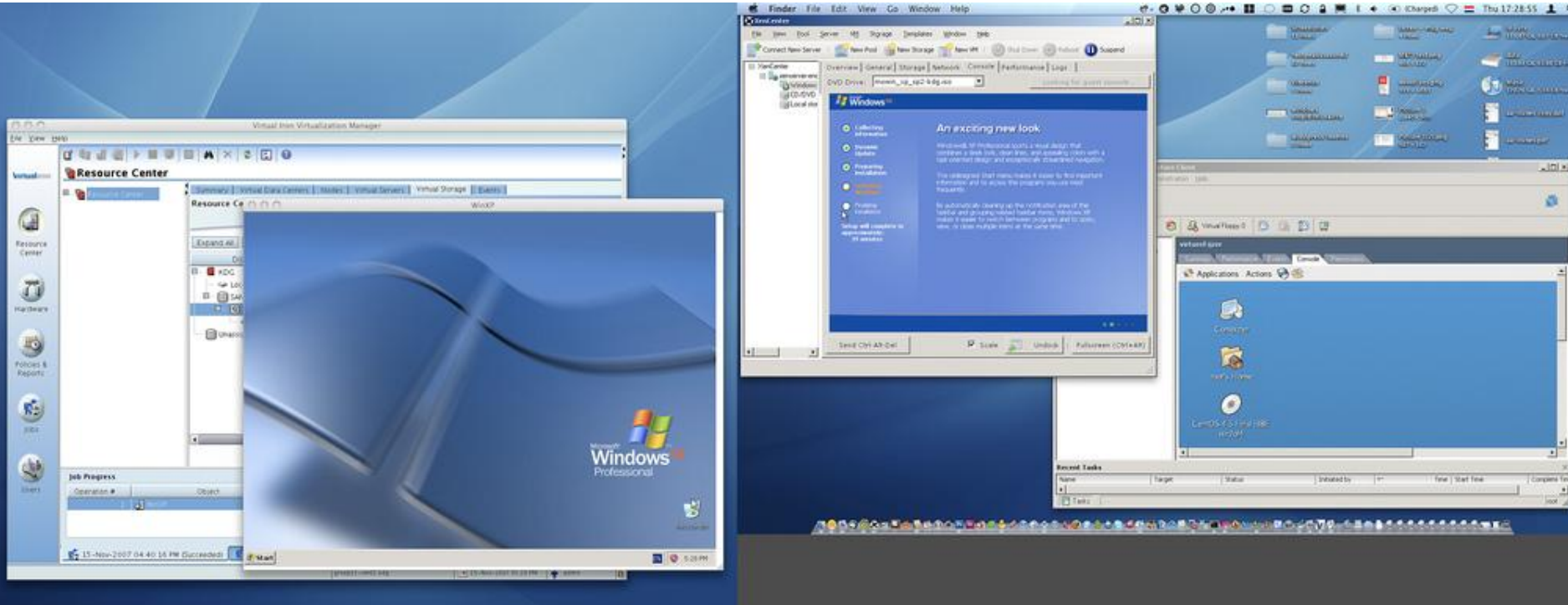


Vision of VMsafe



“VM Introspection”

Are We There Yet?



Are We 100% Virtualized?

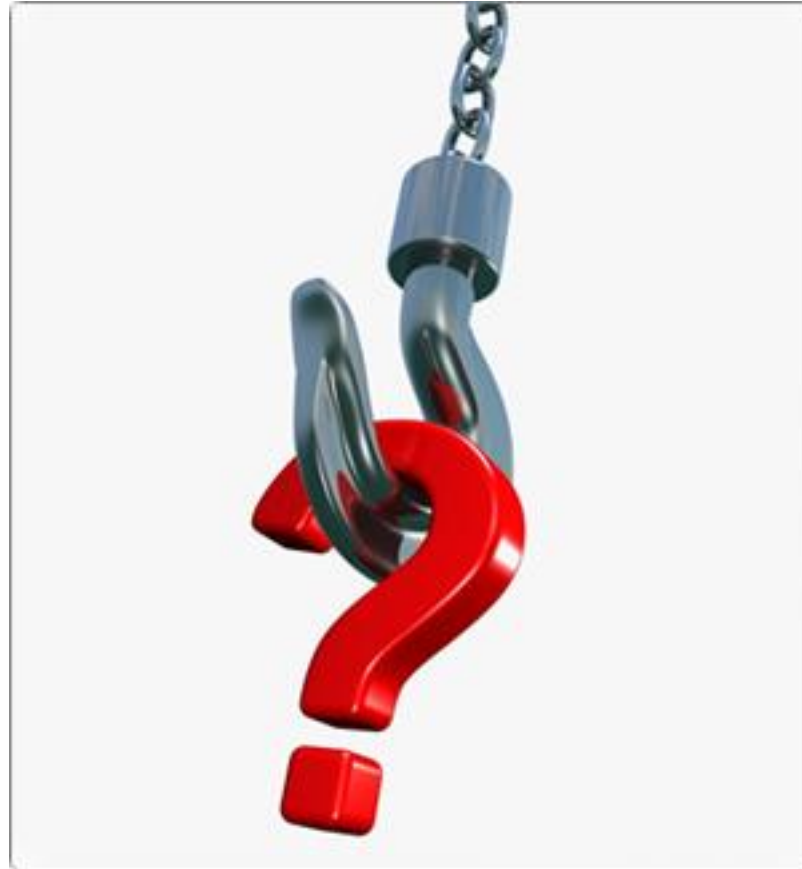
Are We Inspecting 100% of Virtual Traffic?



Conclusions

- 🔥 Visibility in a virtual environment is more important than in a physical environment
 - Misconfiguration
 - VM Sprawl
- 🔥 Best security practices involve both process and technology
- 🔥 Virtual traffic monitoring will help recover the visibility lost by virtualizing

Questions?



richard.park@sourcefire.com