

瑞科技

### **Virtualization Security**

張晃崚 CCIE #13673 區域銷售事業處 麟瑞科技

### Agenda



- Virtualization security hazards
- Virtual Service Gateway

RING



# Virtualization Overview

#### Virtualization 101



 Virtualization decouples physical resources from the OS & applications

RING LINE CORPOR

 Machines are encapsulated as files





![](_page_7_Figure_0.jpeg)

### Heals Itself Automatically

![](_page_8_Picture_1.jpeg)

![](_page_8_Figure_2.jpeg)

![](_page_9_Picture_0.jpeg)

## Hazards!

![](_page_10_Picture_1.jpeg)

### **Visualize Security Challenges**

![](_page_11_Picture_1.jpeg)

![](_page_11_Picture_2.jpeg)

- Vlan segmentation not always desirable - networking complexities and limitations
- Mobile VMs across physical ports policy must follow
- Difficult to view or apply policy to locally switched traffic
- Cannot correlate traffic on physical links from multiple VMs

### No Free Lunches...

![](_page_12_Picture_1.jpeg)

麟 瑞 科 技

Virtualization Benefits	Virtualization Risks	Security and Compliance Issues
Easy machine creation	"VM sprawl"	Rapid change accelerates configuration drift
Consolidation of dozens of physical servers	"Guest escape" of control from VM into hypervisor	Malicious VM takes control of the entire virtualization server
Easy provisioning of networks	Misconfiguration errors	Breaking separation between different security zones
Mobility enables high availability, dynamic resource optimization	Mobility can break static security	Maintain isolation and network controls
Hypervisor enables consolidation	New privileged layer to be secured	Access to sensitive data in VM
	13	

![](_page_13_Figure_0.jpeg)

![](_page_14_Figure_0.jpeg)

### Defense in Depth Security Model

![](_page_15_Picture_1.jpeg)

![](_page_16_Figure_0.jpeg)

#### **Other Issues**

- Hypervisor Security
- Host/Platform Security
- Securing Communication

RING

![](_page_18_Picture_0.jpeg)

![](_page_19_Picture_0.jpeg)