

READY FOR ANY vForum2015

9 December 2015 | Taipei, Taiwan

面對未知威脅 Trend Micro 給您最有效的防護機制

Ken Huang 黃源慶
Trend Micro 趨勢科技 資深技術顧問

Trend Micro + VMware 長期持續的合作創新



vmware

by providing the most secure virtualization infrastructure, with APIs & certification programs



by providing security solutions architected to fully exploit the VMware platform

2009-10

Deep Security 7 supporting introspection and network traffic through hypervisor
Deep Security 7.5 first to support VMware vShield

2011

Deep Security 8 only fully agentless security platform

2012

Deep Security Support for vSphere 5.1 platform

2013

Deep Security 9 with agent recommendation scan

2014

Deep Security 9.5 NSX, vCloud Air and vCenter Operations integration

2015

Deep Security 9.6 integration with vSphere 6 & vROps 6



Trend Micro + VMware 提供最完整的安全防禦



Public Cloud



- ✓ Scalable
- ✓ Secure
- ✓ Instant On Security

End User Computing
VDI/vDaaS



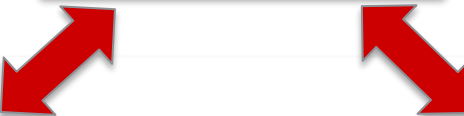
- ✓ Automated
- ✓ Scalable
- ✓ Agentless



Operations



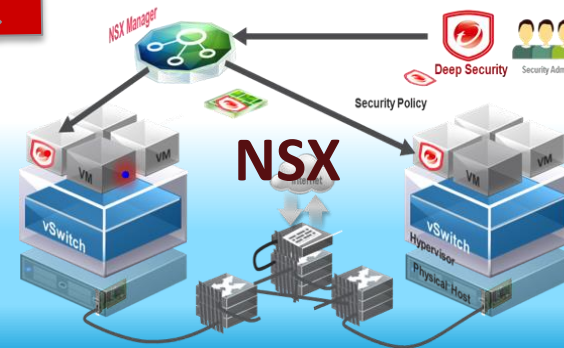
- ✓ Security alerts
- ✓ Integrated dashboard
- ✓ Correlation



- ✓ Agentless
- ✓ Automated
- ✓ vCenter integration



Software-Defined
Data Center
(Private Cloud)

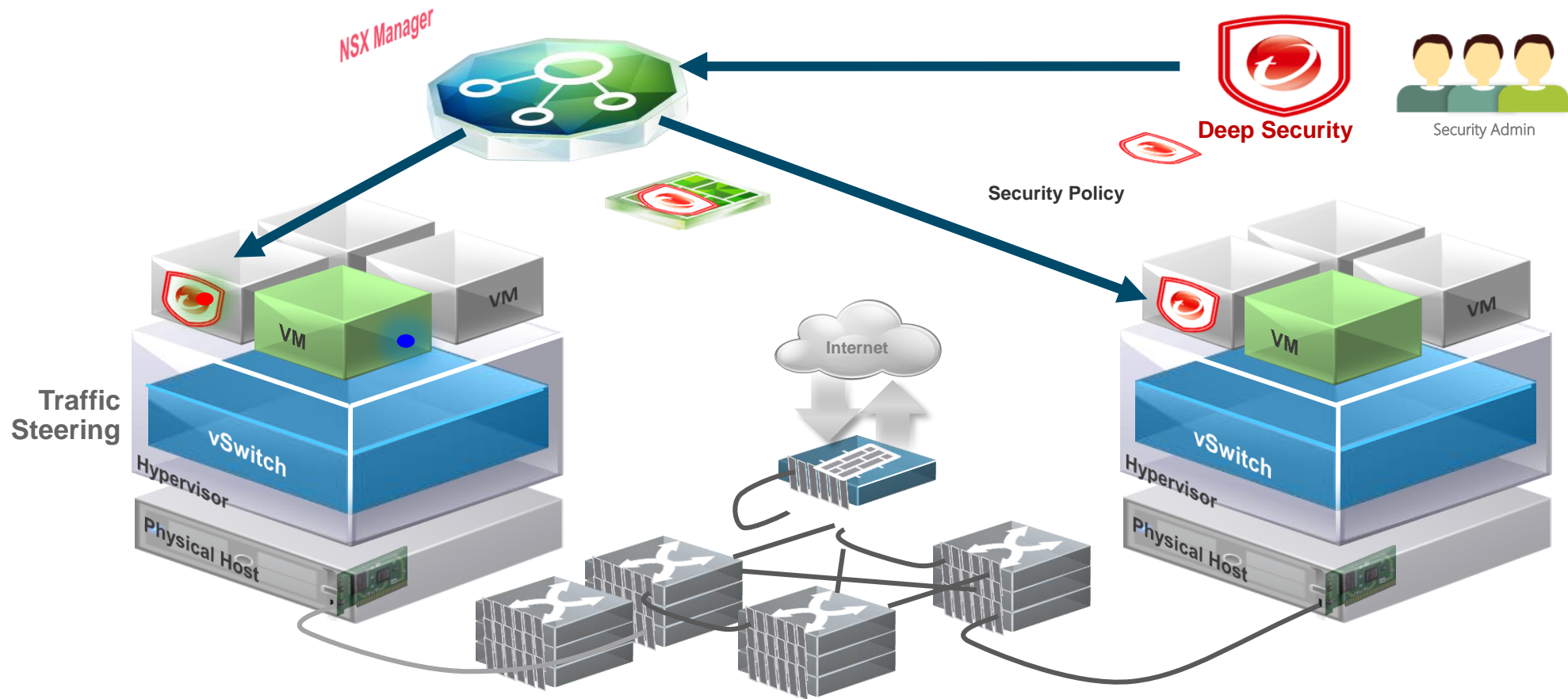


- ✓ Agentless
- ✓ Automated
- ✓ Instant-On-Security
- ✓ Server and Network controls

NSX + Deep Security 影片欣賞

NSX + Deep Security 實現安全自動化展示

NSX 與 Trend Micro Deep Security主機安全保護機制
由底層緊密結合完全整合 提供進階自動化的安全防護



NSX + Deep Security 實現安全自動化展示

透過 NSX Tagging 技術 結合 Deep Security 偵測機制
輕鬆達成動態隔離有弱點問題系統且在修復後自動還原

限制處置群組

Security Group = **Quarantine Zone**

Members = {Tag = 'ANTI_VIRUS.VirusFound'}

標準群組 Security
Group = **Web Tier**

策略 Policy 設定

Standard Desktop VM Policy

Anti-Virus – Scan

Quarantined VM Policy

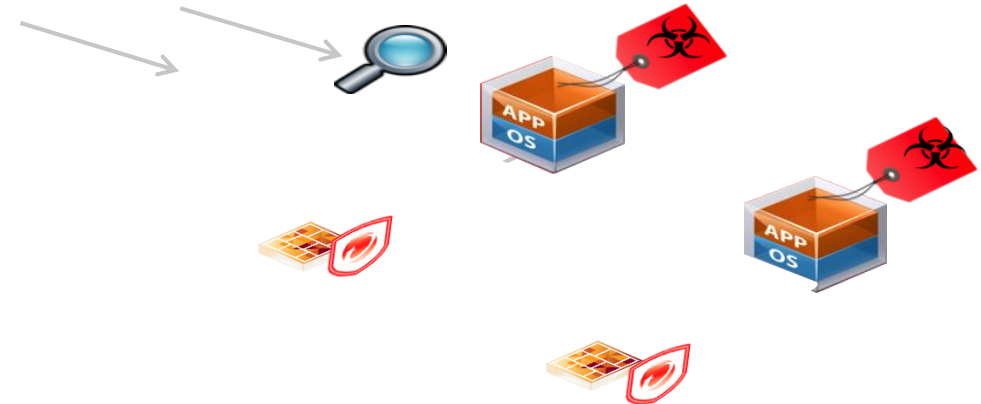
Firewall – Block all except security tools

Anti-Virus – Scan and remediate



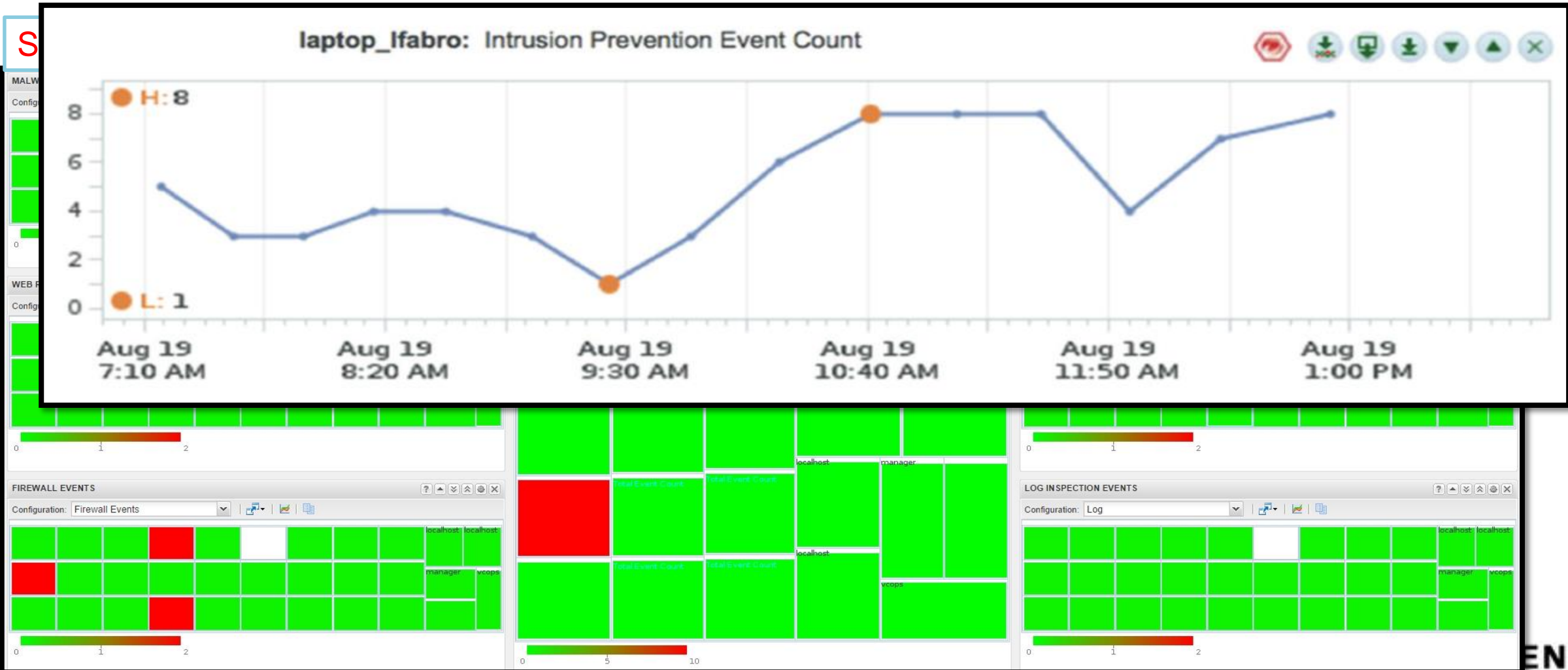
Service Composer

Cloud Management



Deep Security 整合進 VMware vRealize Operation 維運管理

Security Analysis— Metric Graph



實體 虛擬 雲端主機防護最佳選擇

雲端平台最佳整合

vmware

amazon
webservices™

Microsoft

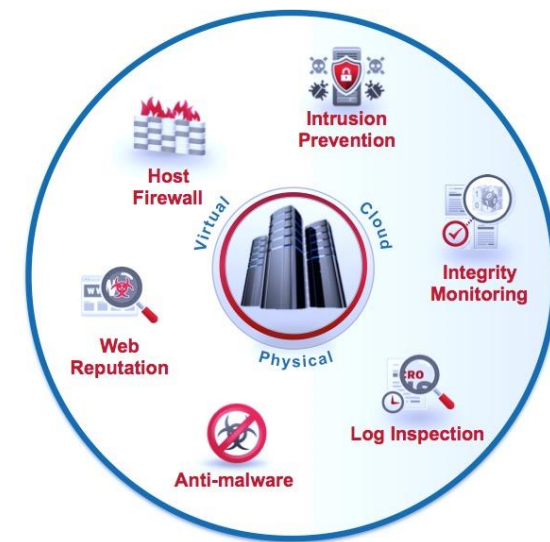


TREND
MICRO™

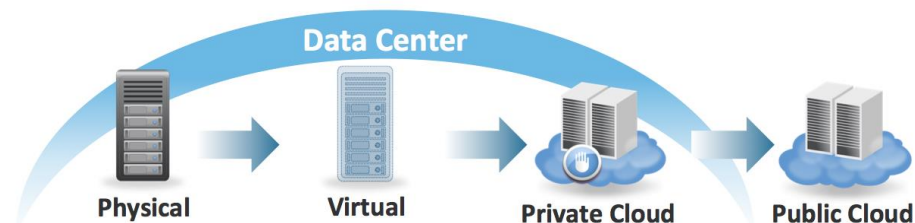
#1 in Cloud and Data Center
Security for a Reason

SMART • SIMPLE • SECURITY THAT FITS

最完整的安全防禦



單一管理平台 整合實體 虛擬 雲端主機防護





Deep Security
AS A SERVICE

Data Center



防毒

入侵偵測

防火牆

異動管理

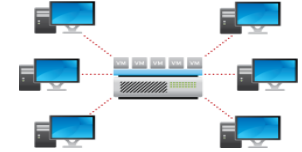
登錄檔分析

資料加密

雲端與資料中心資安政策



採用 Deep Security 的優點 專為虛擬環境所設計，無代理程式的資安防護



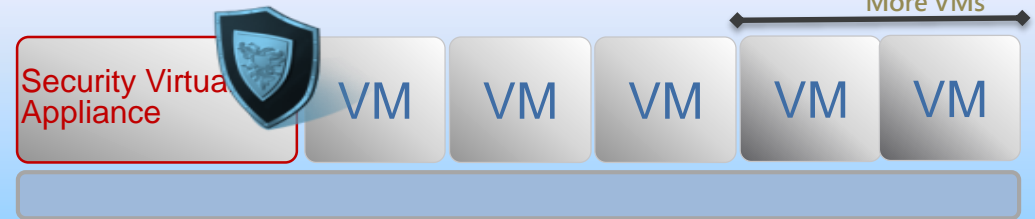
The Old Way 傳統設計



提高VM密度

優化資源

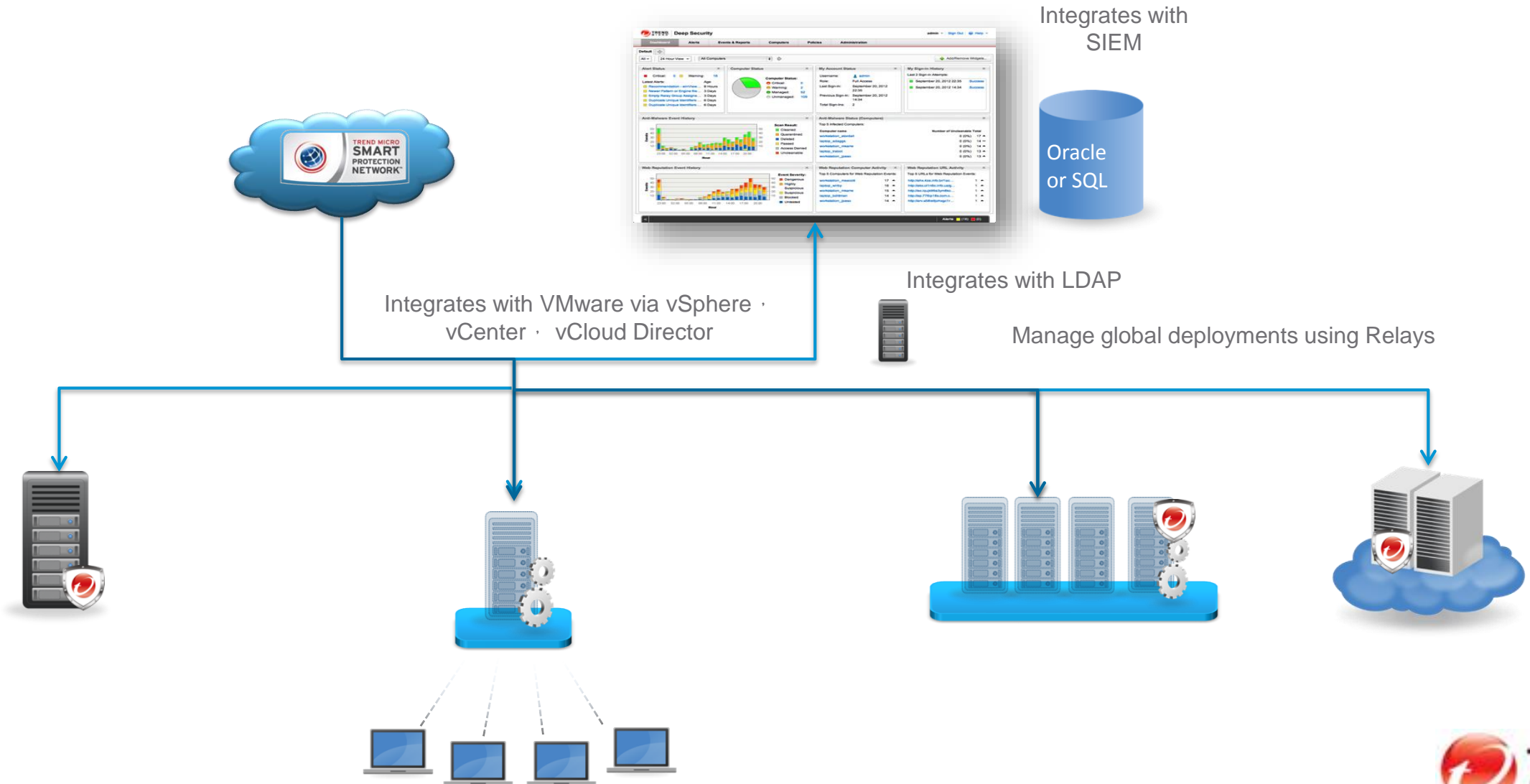
With Deep Security 創新設計



簡易管理

強化資安

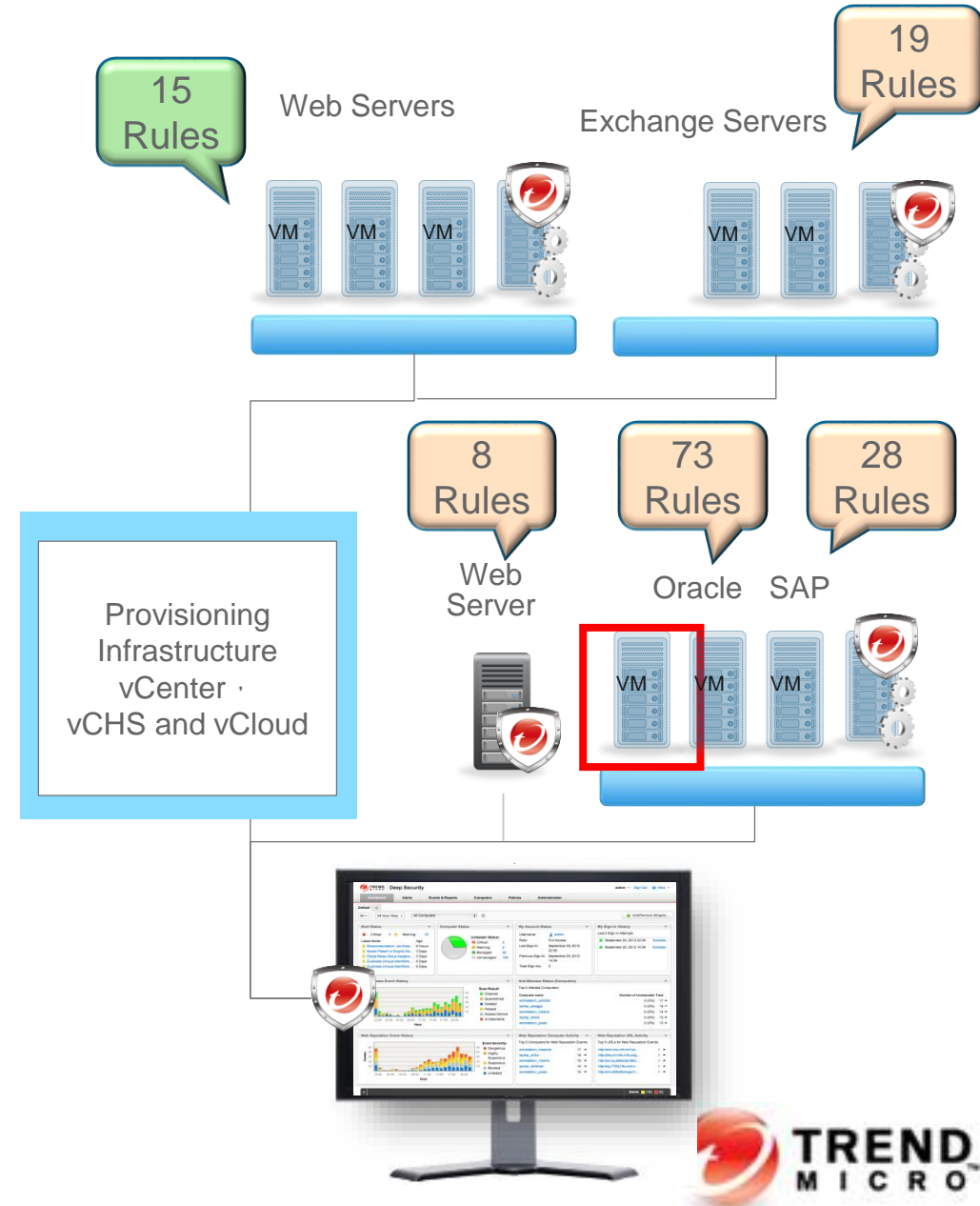
保護管理所有新擴展主機 **Manage across environments**



主機移轉保護 - 沒有空窗期

完整結合vCenter and vCloud Director 管理
負載主機

- 動態自主弱點建議檢查(recommendations Scan)及套用保護資料中心
- 主機負載移轉全過程安全防護自動套用
-沒有安全空窗期



Deep Security 如何防護重要伺服器？

已知威脅

防毒

網路
防護

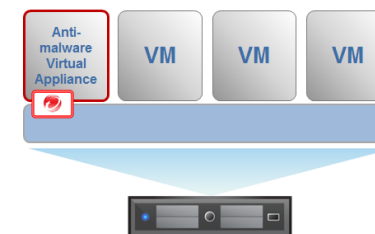
未知威脅

安全日誌
管理

系統異動
監控



實體主機



虛擬平台



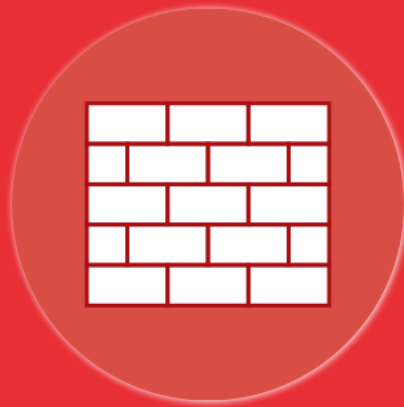
公有雲架構



**Anti-
Malware**



**Web
Reputation**



Firewall



**Intrusion
Prevention**

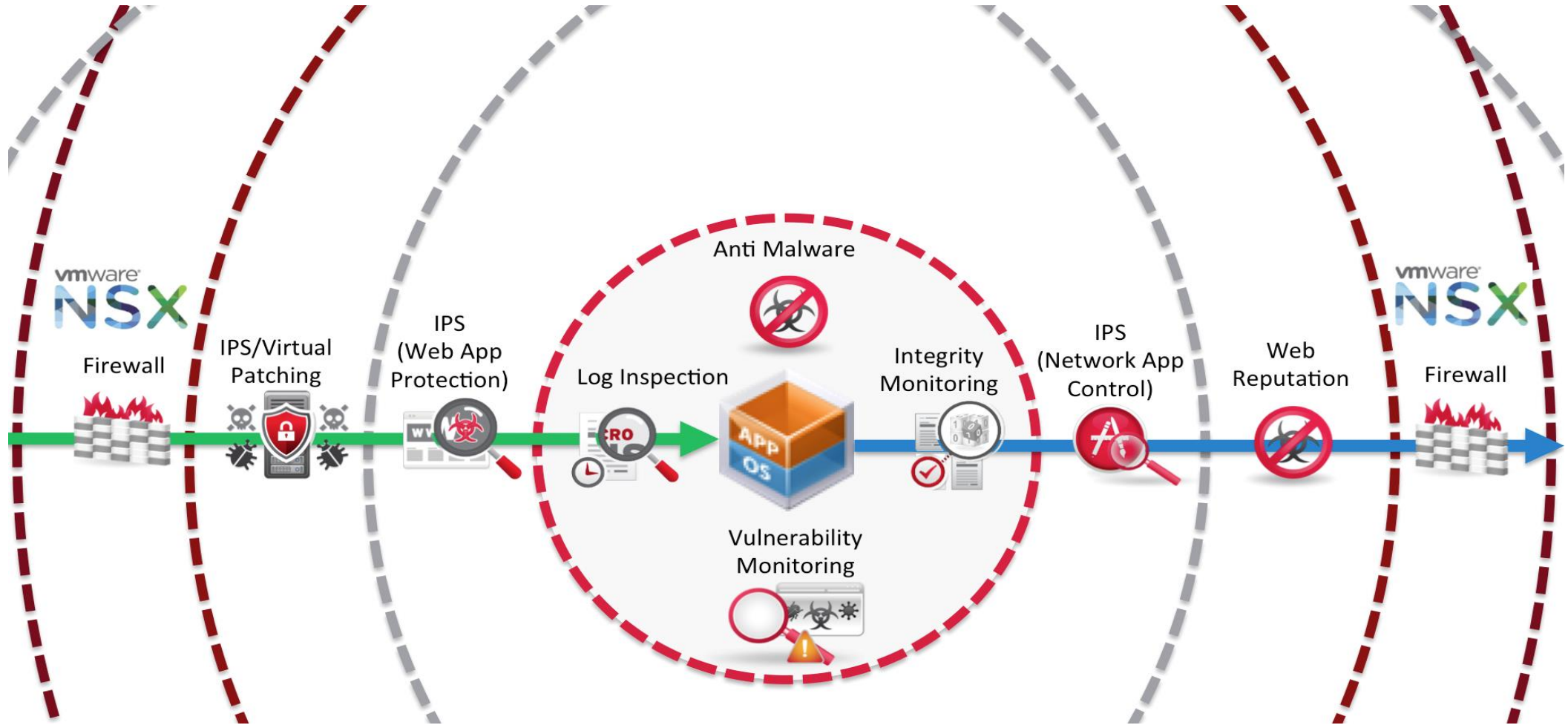


**Integrity
Monitoring**



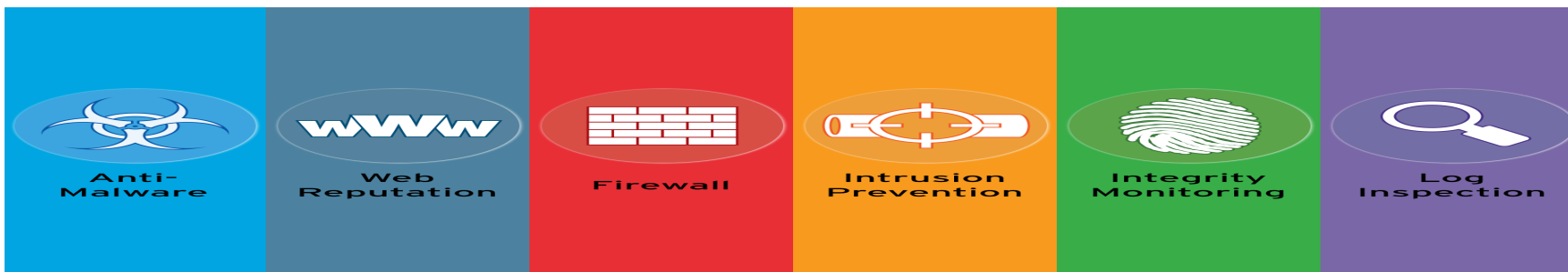
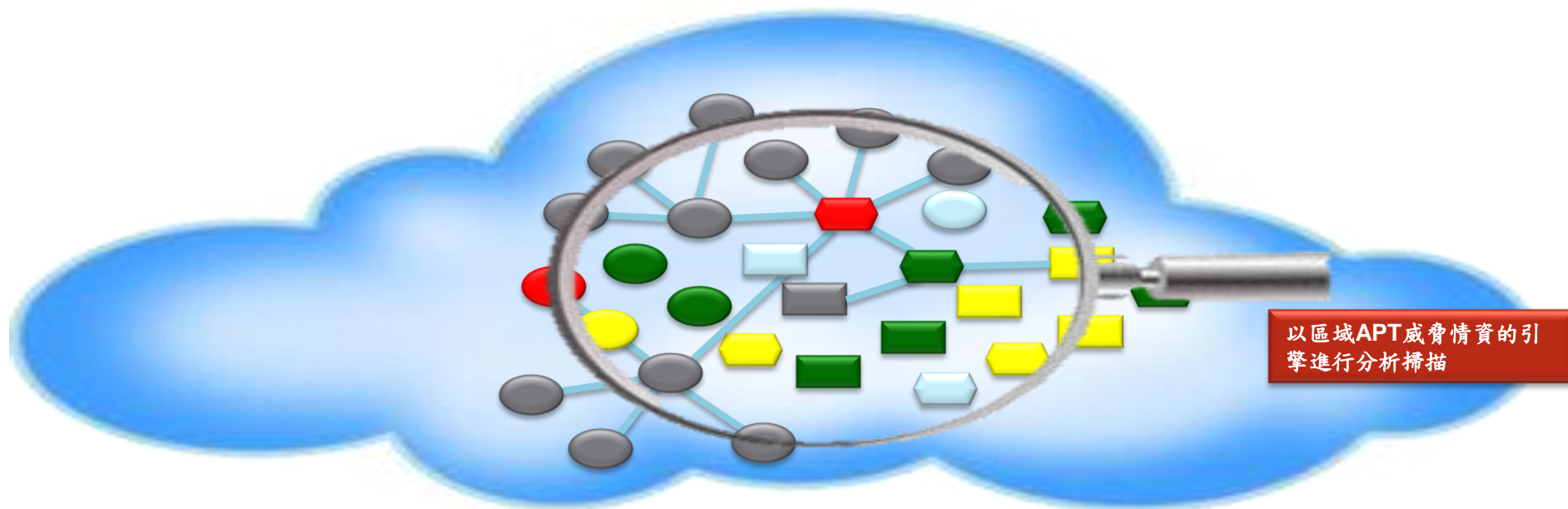
**Log
Inspection**

Deep Security 提供 (由外到內 + 由內到外) 多層次安全防護



趨勢科技 Deep Security for 大數據 APT資安管理

大資料平台關聯出 主機攻擊事件及威脅進程



Deep Security for APT Solution 主機防禦管理

Deep Security 完整呈現 APT三階段主機防禦稽核管理



攻擊階段 > Point Of Entry 網路威脅 漏洞攻擊



攻擊來源IP

利用哪些弱點攻擊主機

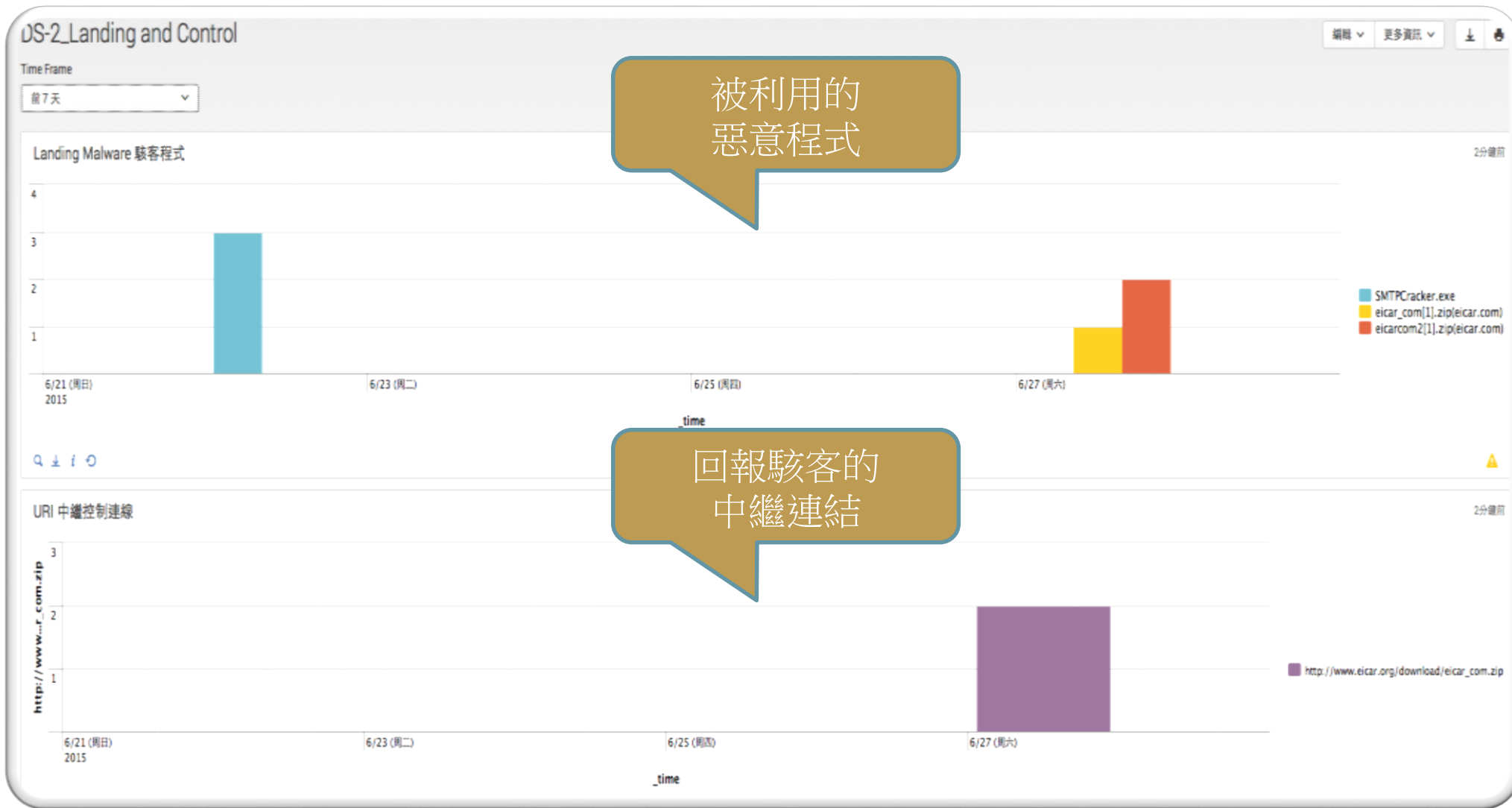
攻擊階段

控制階段

活動與擴散階段



控制階段 > Landing and Control 後門及中繼控制



活動擴散 > Hacking Activity 駭客行為活動



攻擊階段

控制階段

活動與擴散階段



全球大客戶的採用



全球前50大企業
48家採用



全球前10大汽車
公司
全數囊括



全球前10大電信
業者
全數採用



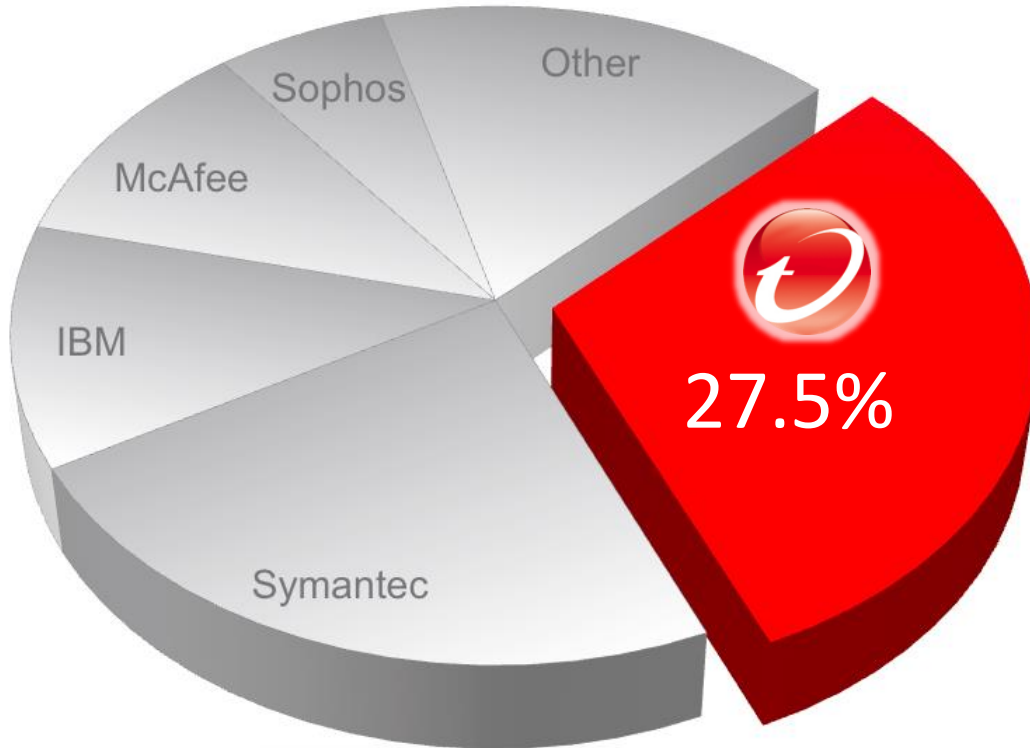
全球前10大銀行
8家採用



全球前10大石油
公司
9家採用



#1 Corporate Server Security Market Share



Microsoft Partner
Gold Application Development



READY
FOR **ANY**
vForum2015