



Securing Your Web World



# 虛擬環境與雲端安全防護

陳文權  
技術顧問



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING

# Agenda

- **資料中心的轉變與面臨的挑戰**
- **虛擬化環境安全防護**

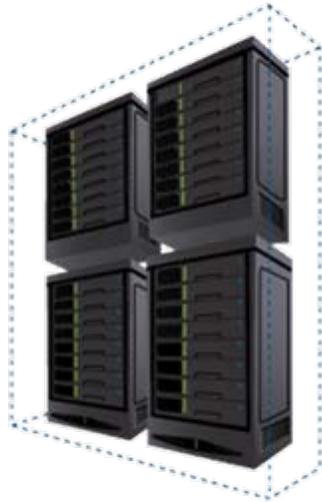


# 資料中心的轉變

PHYSICAL SERVERS



VIRTUALIZED SERVERS



CLOUD COMPUTING



Linux



Amazon Elastic Compute Cloud



# Cloud Computing “Breaches”

Amazon Elastic Compute Cloud



twitter

Dec 2009: Amazon EC2  
Hit by **Botnet**

Aug 2009: Twitter and Facebook Distributed  
Denial of Service **Attacks**



Jun 2009: U.S. Attorney **warns** of  
cloud computing threat (*CNET News*)

Google™

Sep 2008: Google Docs **flaw** could allow others  
to see files (*SC Magazine*)

salesforce.com  
Success. Not Software.®

Oct 2007: Salesforce.com security breached.  
Repeatedly **hacked** (*Washington Post*)

# 解決虛擬主機所面臨的安全挑戰

Securing Your Web World

## 虛擬主機自我防護

實體  
伺服器

- 防護
- 法規遵循
- 成本效益



### 核心安全防護

- 惡意程式防護; 防火牆; IDS/IPS
- 應用程式防護及控管
- 完整性及日誌監控

虛擬  
伺服器

針對虛擬化環境特性的  
防護機制



### 新的虛擬化挑戰

- VM移轉及擴展
- VM間流量
- 效能及彈性



雲端  
伺服器

公眾網域的防護及控管



### 公眾網域挑戰

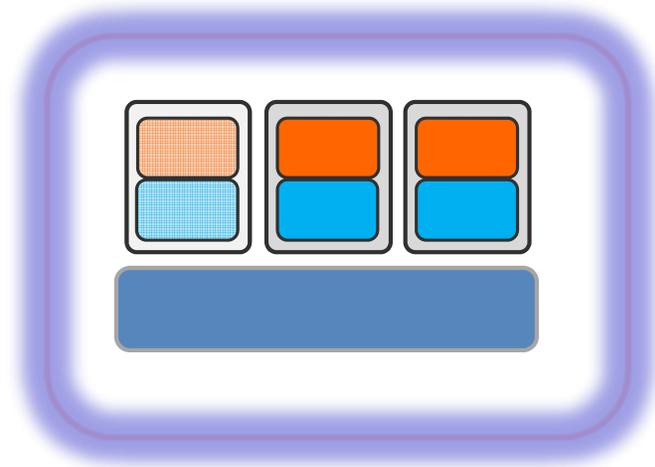
- 多租用者風險
- 遠端日誌/事件管理
- 完整的資料防護

## 虛擬化環境與實體主機面對相同的安全威脅



### 新的安全防護挑戰:

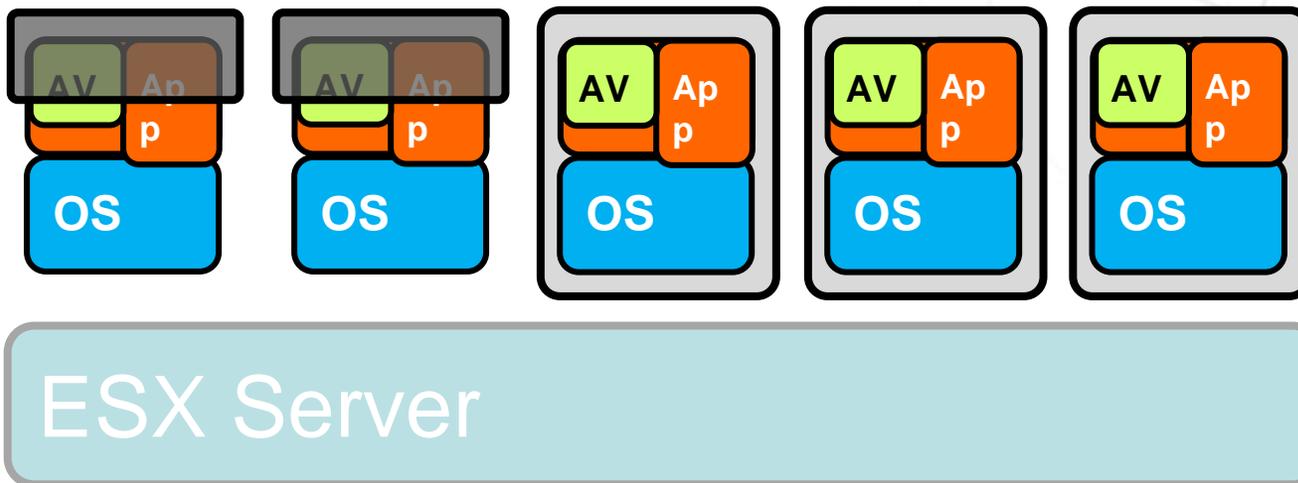
1. 休眠虛擬主機
2. 資源爭奪
3. 虛擬主機擴展
4. 虛擬主機間流量
5. vMobility



# 問題一：無法提供休眠主機防護

## Dormant VMs

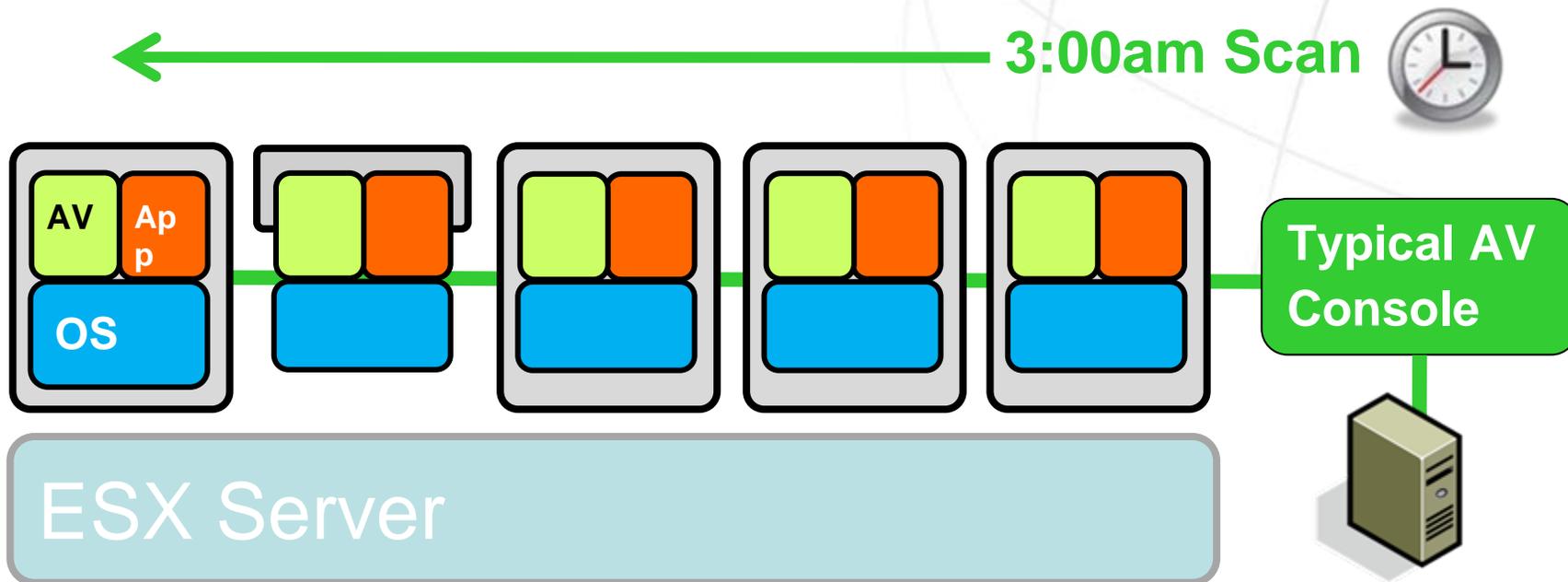
## Active VMs



**休眠VM包含VM templates 及 backups:**

- 不即時的病毒碼及修補程式
- 上線後可能因漏洞遭受惡意程式攻擊

## 問題二:全系統掃描



### 全系統掃描造成資源搶奪

- 既有防毒並未考量到虛擬化環境的特性
- 同時在一個host上執行全系統掃描將造成伺服器效能下降

# 問題三: 虛擬主機擴展

**Dormant**

**Active**

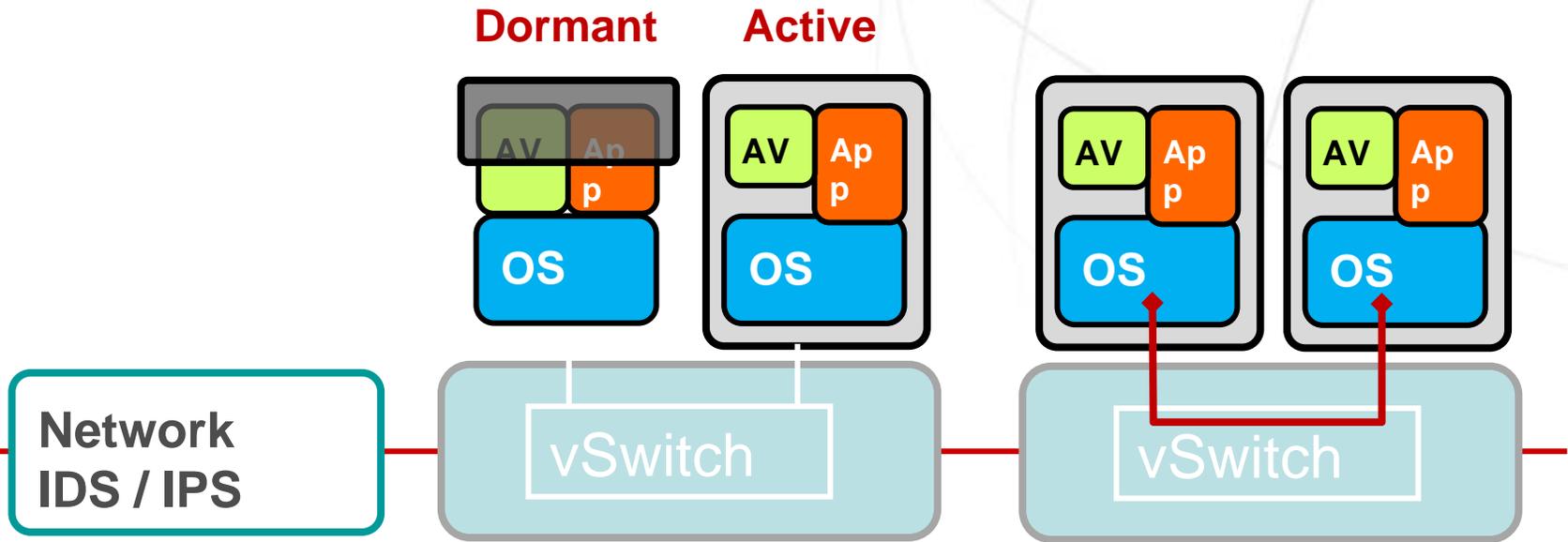
**New**



## 管理虛擬主機擴展

- 安全弱點複製迅速
- 缺乏視覺化, 整合的虛擬主控台增加管理複雜度

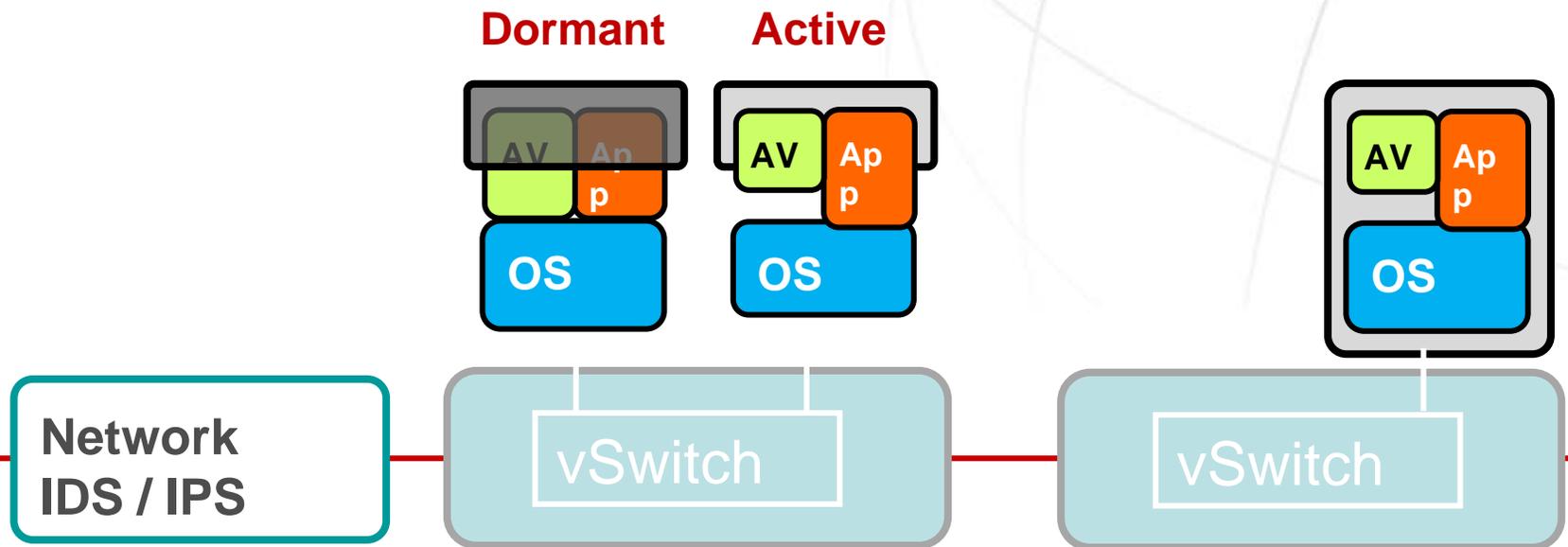
# 問題四: 虛擬主機間流量



## 虛擬主機間流量

- NIDS / NIPS 無法提供虛擬主機間的防護
- 需要新型態的防護機制以因應vSwitch的變化

# 問題五: VM Mobility

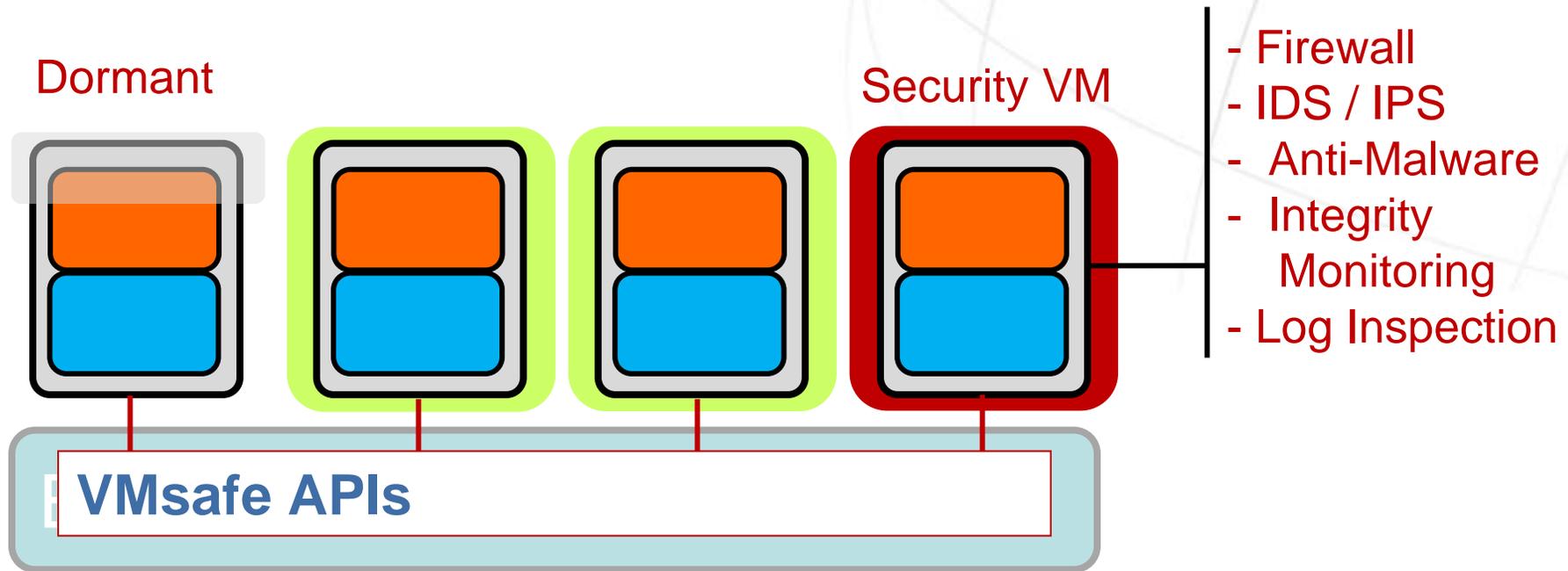


## vMotion & vCloud:

- 需要重新設定安全防護:程序繁瑣
- 同一-host上的虛擬主機具有不同的功能及特性
- 無法防護公雲(IaaS)上的虛擬主機

# 趨勢科技虛擬化安全防護

Securing Your Web World

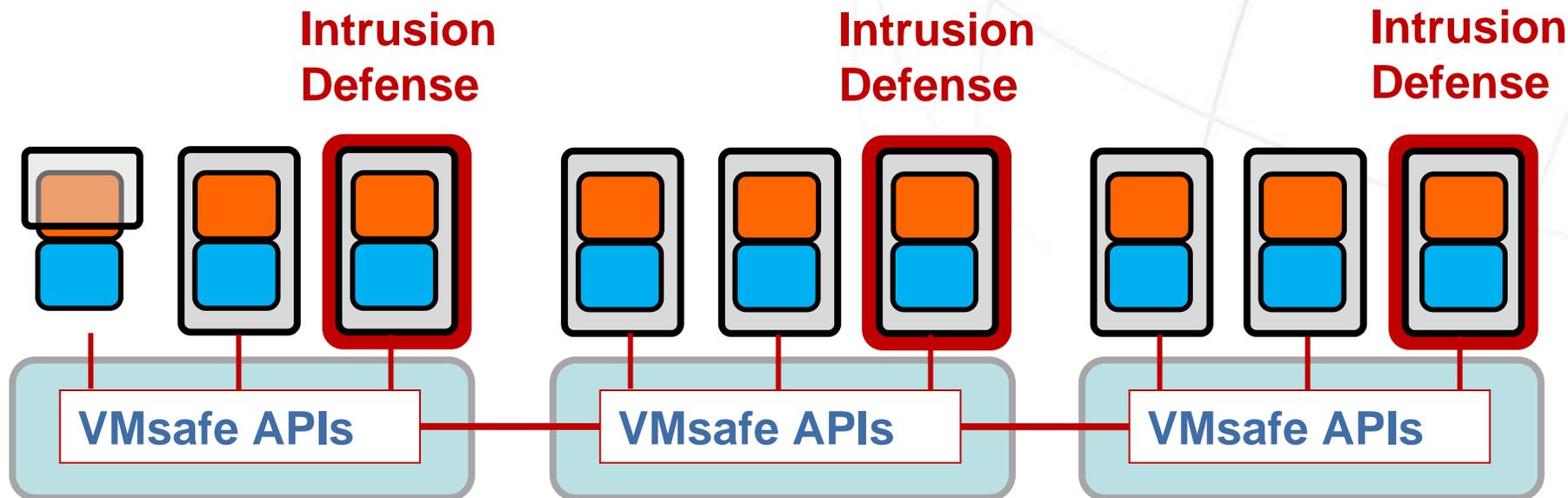


## 對所有VM提供全面性的防護

- 透過虛擬主機本機agent提供安全防護
- 由VM外部提供多種安全防護功能
- 整合VMWare vCenter 及 VMsafe

# 虛擬主機入侵防禦-Deep Security

Securing Your Web World

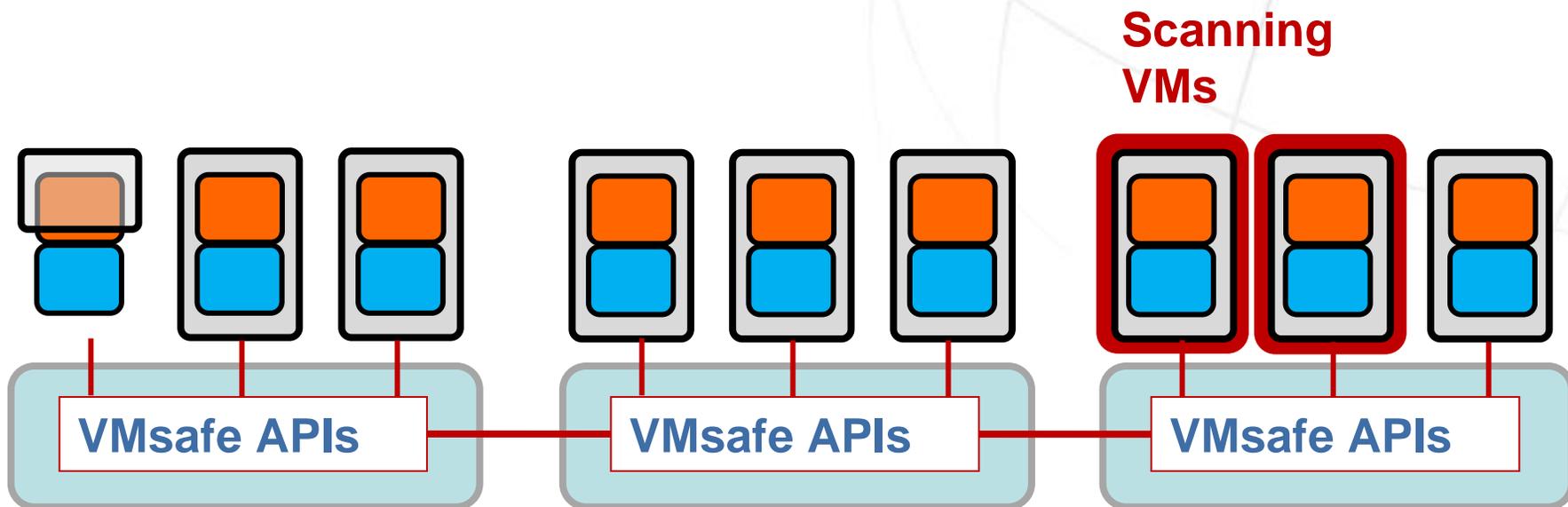


- 入侵防禦提供IDS/IPS 及防火牆防護
- 整合VMsafe-NET APIs (防火牆 及 IDS/IPS)
- 執行安全政策
- 自動提供新的虛擬主機防護

# 虛擬主機惡意程式掃描-

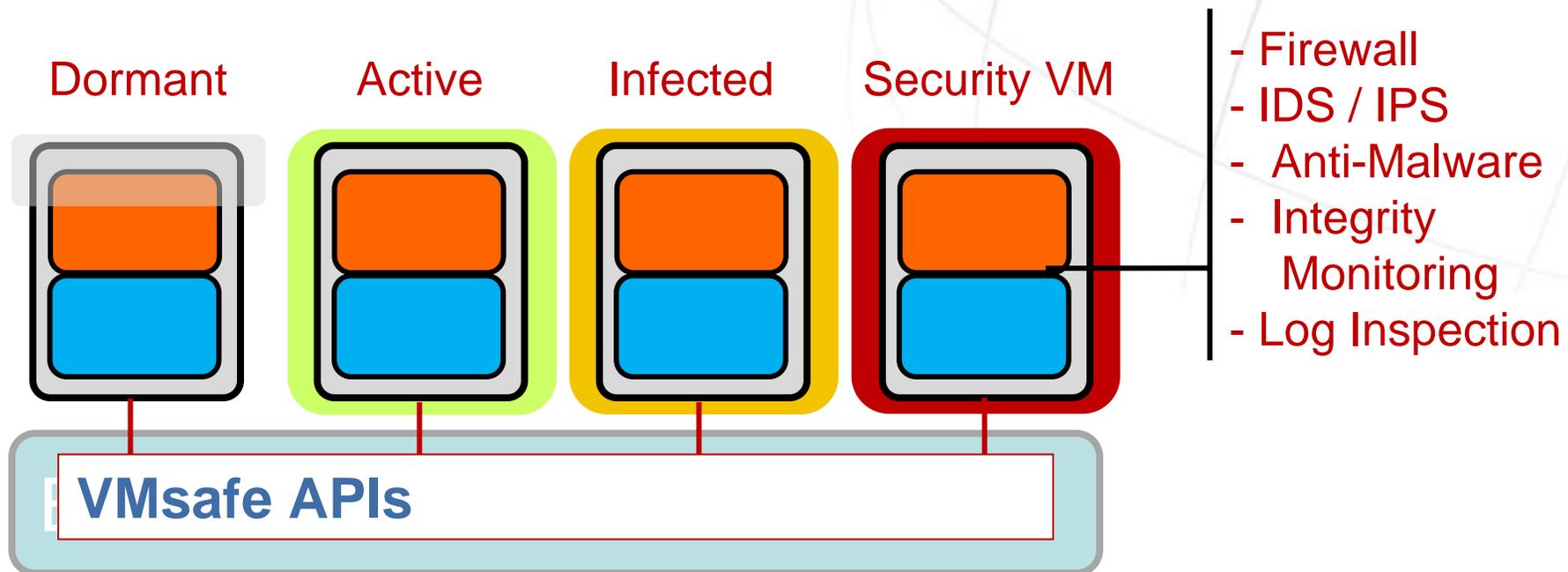
## Core Protection for Virtual Machine

Securing Your Web World



- 從外部掃描目的端VM惡意程式
- 整合VMsafe VDDK APIs 載入VM磁碟檔案
- 從掃描VM完整掃描休眠及線上

# 如何運作:防止Conficker



- **防火牆:** 阻擋遭感染VM存取其他存在弱點服務的VM
- **IDS/IPS:** 防止MS008-067 暴露
- **惡意程式防護:** 偵測及清除Conficker
- **Integrity Monitoring:** 偵測到機碼變更
- **Log Inspection:** 收集暴力密碼攻擊安全事件日誌

# Deep Security

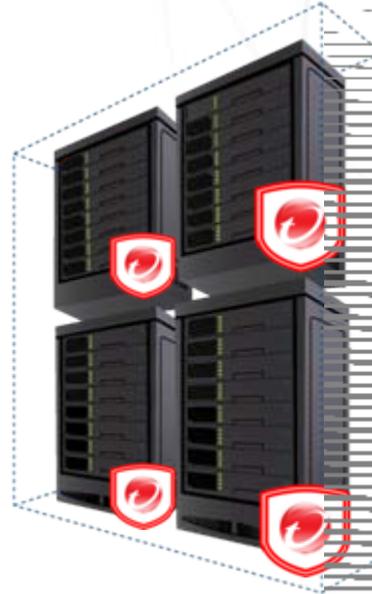
## 伺服器及應用程式的防護



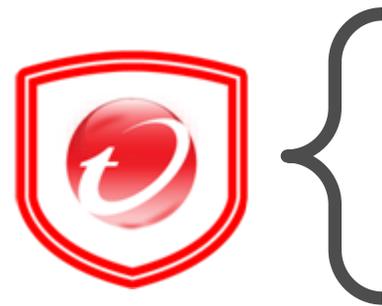
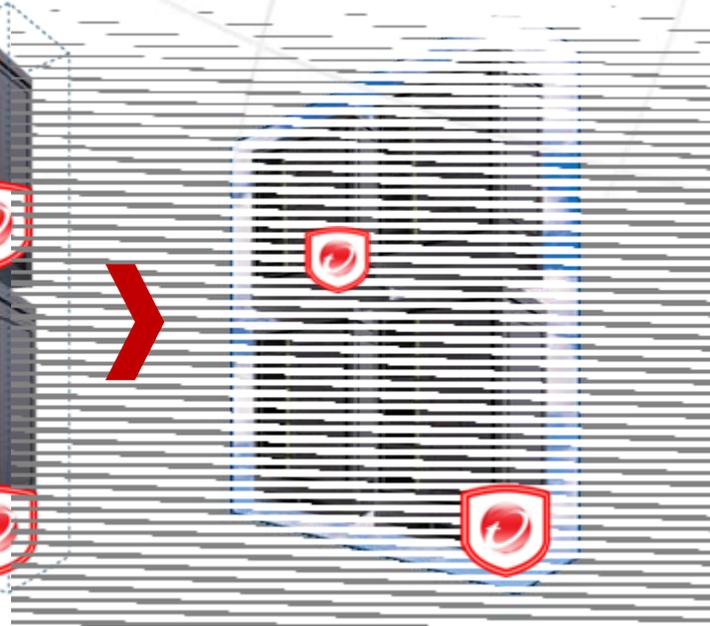
實體



虛擬



雲端

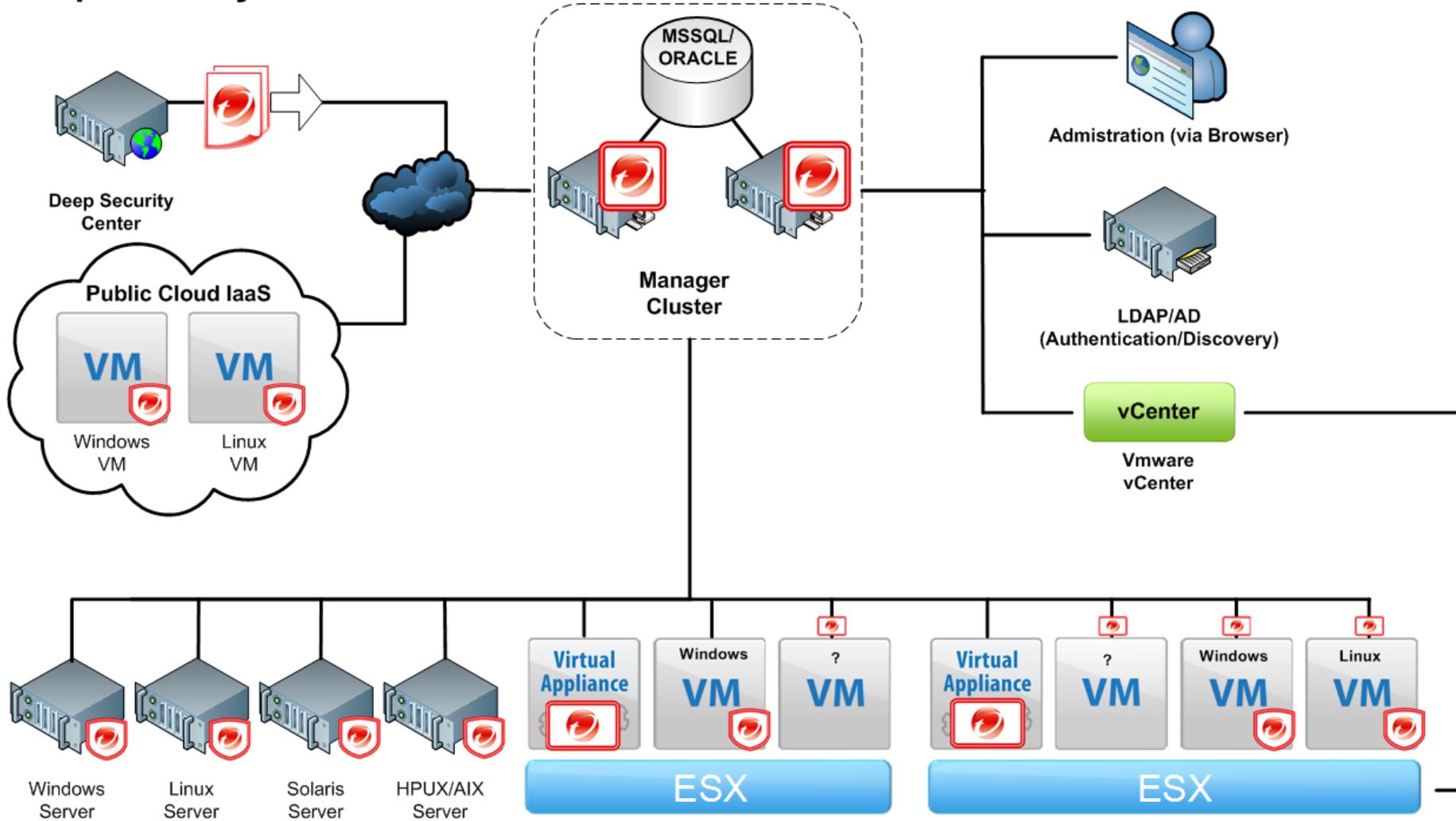


Within the DSVA

Q3/2010  
(Deep Security

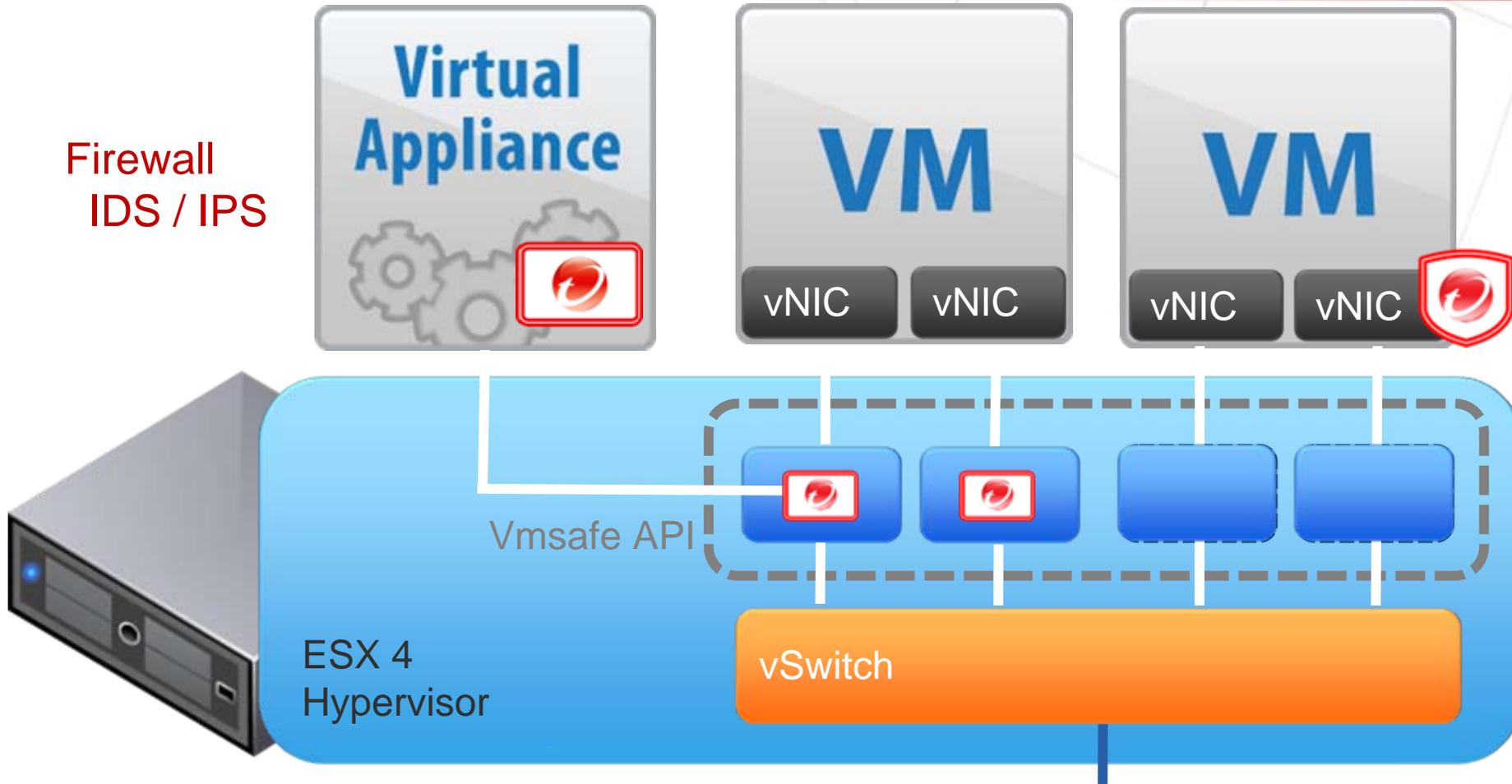
# Deep Security 7.0 產品架構

## Deep Security 7.0



# Deep Security Virtual Appliance

Securing Your Web World



- 透過檢查虛擬元件以保護虛擬主機
- 由虛擬主機外部提供防護,無須更動既有虛擬主機
- 完全整合VMWare vMotion, Storage vMotion, HA等功能
- 整合Virtual Center



## Firewall

- 集中管理伺服器防火牆規則
- 事先定義的一般企業類型伺服器規則樣板
- 依需求設定過濾: IP & MAC addresses, Ports
- 支援所有IP-based 通訊協定: TCP, UDP, ICMP, IGMP ...



## Deep Packet Inspection

- IDS / IPS, 網站應用程式防護
- 網路應用程式控管
- 檢查進出的流量:
  - 通訊協定異常
  - 內容攻擊
  - 政策違反
- 屏蔽弱點



## Integrity Monitoring

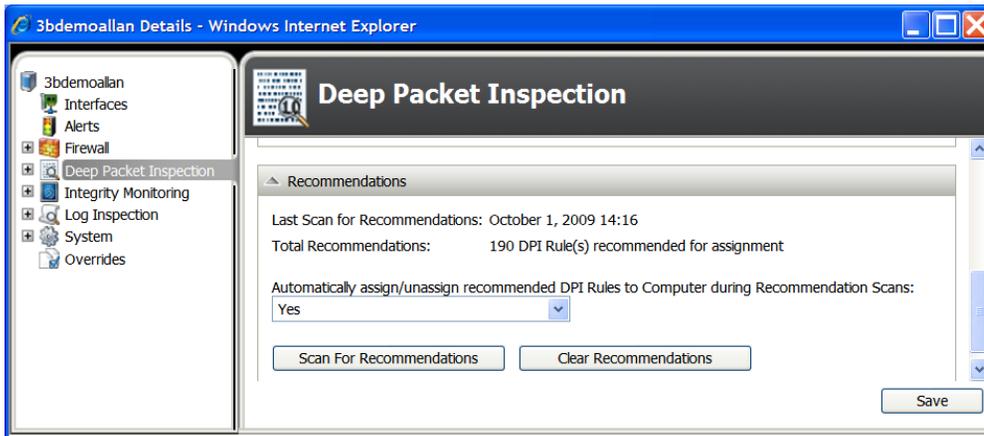
- 監控重要檔案,系統機碼變更
  - 檔案,資料夾,機碼值



## Log Inspection

- 收集分析作業系統及應用程式的安全事件
- 最佳化規則確保由幾個日誌紀錄中辨識出安全事件

# Recommendation Scans



- **透過掃描分析自動建立伺服器的防護**
  - 確認既有OS, Service Pack及修補程式
  - 確認已安裝的應用程式及版本
  - 自動套用新的DPI規則來屏蔽已知的弱點以提供攻擊防護
  - 當修補程式更新後, Recommendation Scan將自動套用新的DPI規則

# Deep Security Virtual Appliance

Securing Your Web World

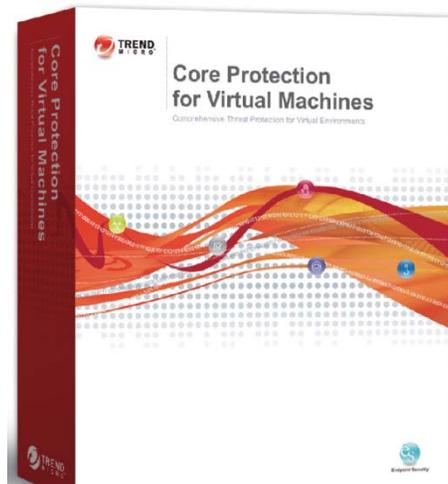
Protection Modules	Supported	Description
Firewall	Yes	<ul style="list-style-type: none"><li>· 透通防護虛擬主機</li><li>· 可依網路介面指定不同安全政策</li><li>· 當虛擬主機的agent離線或未執行時自動確保防火牆政策執行</li></ul>
Deep Packet Inspection	Yes	<ul style="list-style-type: none"><li>· 完整DPI 支援 (IDS/IPS, 網站應用程式防護, 應用程式控管)</li><li>· 當虛擬主機的agent離線或未執行時自動確保DPI政策執行</li></ul>
Integrity Monitoring	No	<ul style="list-style-type: none"><li>· 需安裝Agent於虛擬主機</li></ul>
Log Inspection	No	<ul style="list-style-type: none"><li>· 需安裝Agent於虛擬主機</li></ul>

**Agent-** VMware 3.x, Citrix, and Hyper-V  
Virtual Appliance – VMware vSphere 4 (ESX 4)

# Trend Micro Core Protection for Virtual Machines (CPVM)

Securing Your Web World

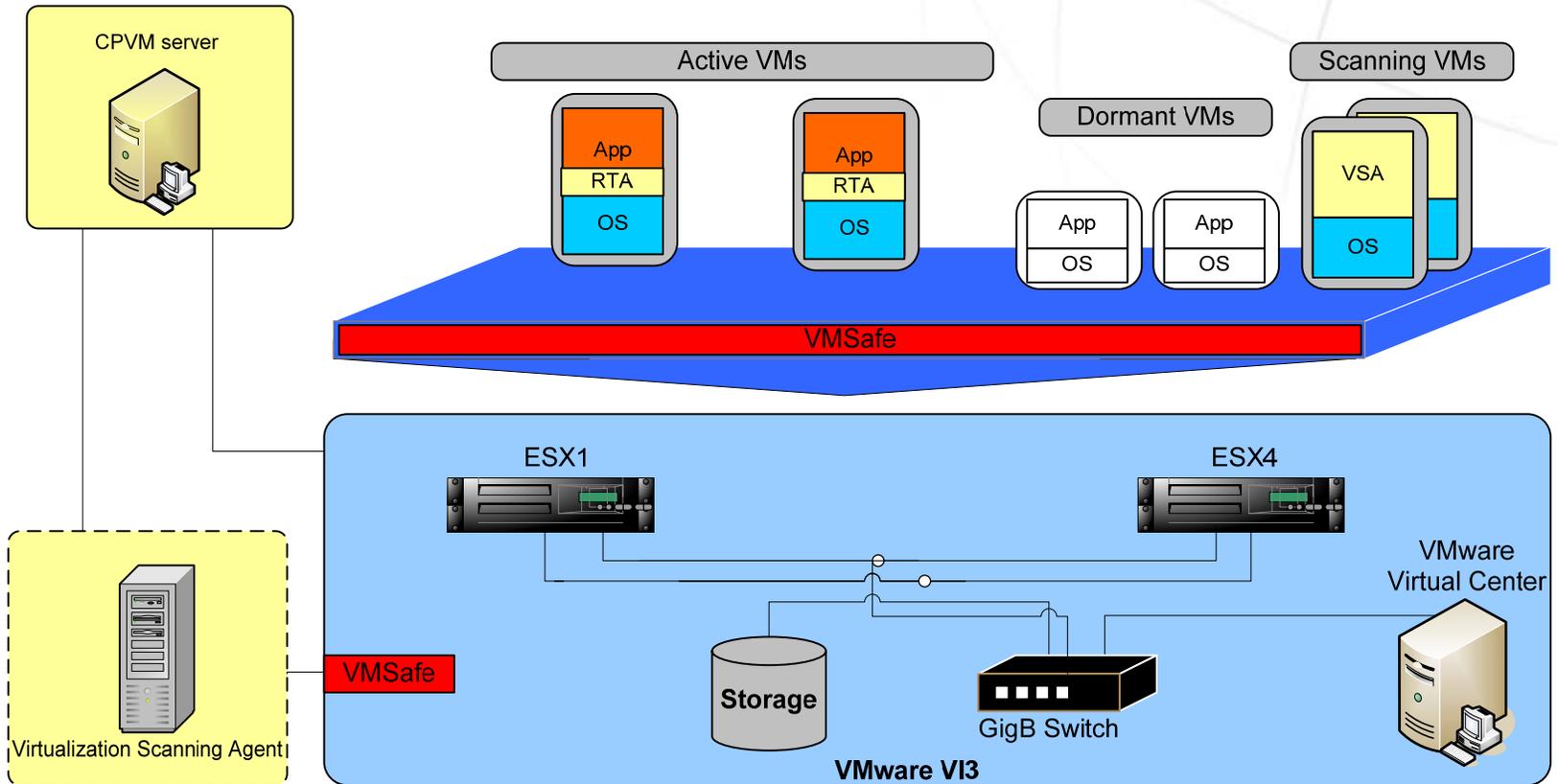
- 透過獨立的掃描VM掃描離線VM
- 透過獨立的掃描VM排程掃描線上VM
- 透過本機即時掃描agent即時掃描線上VM本機



Version 1.0

- 支援 VI3 及vSphere 4
- 獨立或整合於 OSCE 8 sp1/OSCE 10 嵌入式
- 緊密整合VI 及VMSafe API

# CPVM架構

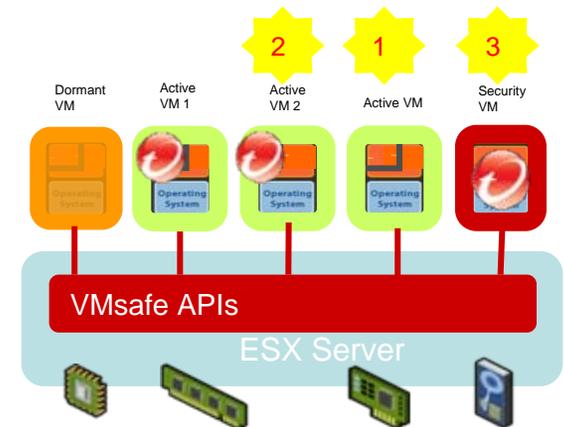
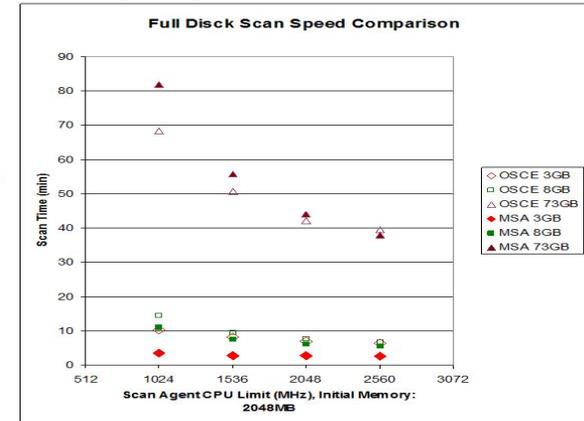


RTA = Virtualization Security Real-Time Agent  
VSA = Virtualization Scanning Agent

# 效能

- 6.17 min for VSA to perform a full scan on 8GB storage (CPU= 2Ghz and 2GB of RAM).
- There are no significant difference in scanning time when VSA\* scans active or dormant VMs:
  - Full scan on 3GB storage (CPU = 2Ghz and 2GB of RAM):
    - Active = 2 min and 27 sec
    - Dormant = 2 min and 44 sec
- It takes less time for VSA to scan\* a VM in comparison to OSCE:
  - VSA takes 42 sec to scan itself 3
  - VSA takes 136 sec to scan VM 1
  - OSCE takes 409 sec to scan VM 2

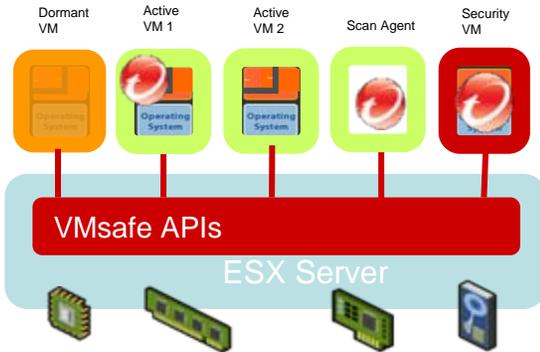
Full disk scan speed comparison: CPVM vs OSCE 8



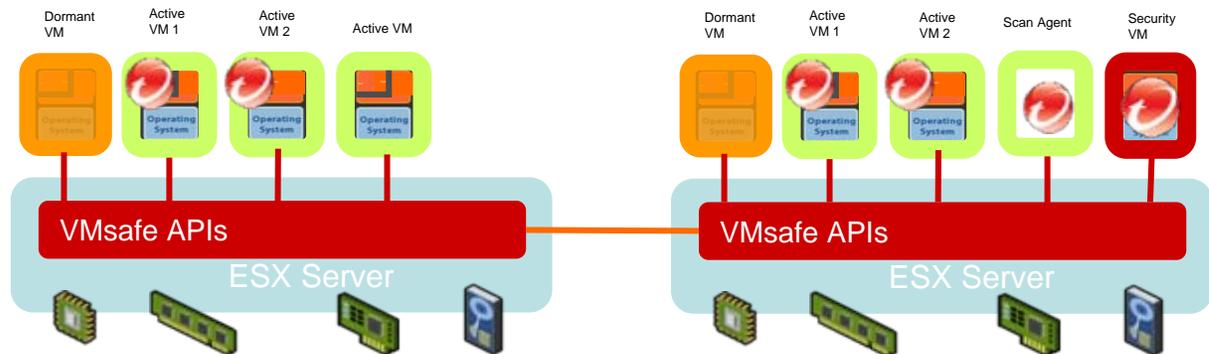
\*Intelliscan on 3GB VM, OSCE 8.0

# CPVM部署架構

## Alternative 1 – Single ESX



## Alternative 2 – Multiple ESXs



# Thank You

Trend Micro

Securing Your Web World



**TREND**  
MICRO™