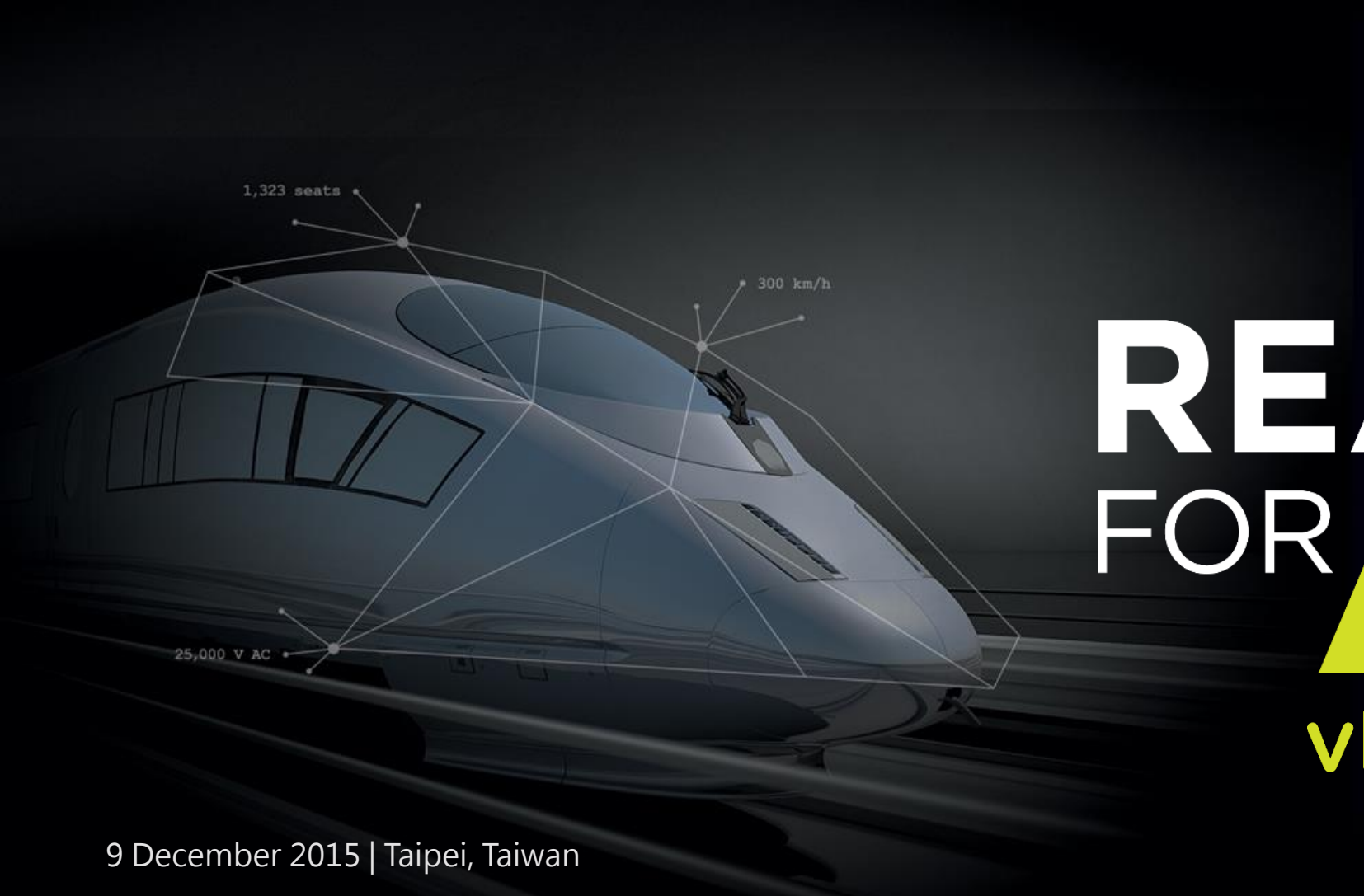


vmware

READY FOR ANY

vForum2015

9 December 2015 | Taipei, Taiwan

雲時代，安全引領變革與創新

黃茂勳
卡巴斯基台灣銷售總監

雲時代的到來.....


SkyDrive
NETFLIX
photobucket
overstock.com
EVERNOTE
PANDORA
internet radio
iBooks
YouTube
cloud
Computing
ebay
tumblr.
flickr
box
amazon cloud drive
iCloud
nook
kindle
Google play

雲時代環境的獨特性及安全挑戰

資源集中

1、系統出現問題影響面大

2、缺乏傳統環境的隔離措施，內部感染

3、管理複雜度大幅度增加

資源分享

1、CPU、記憶體、網路、存儲、頻寬等共用資源的爭奪

2、開放的API，多終端接入

虛擬機器和應用程式變動

1、缺少最新反病毒資料庫

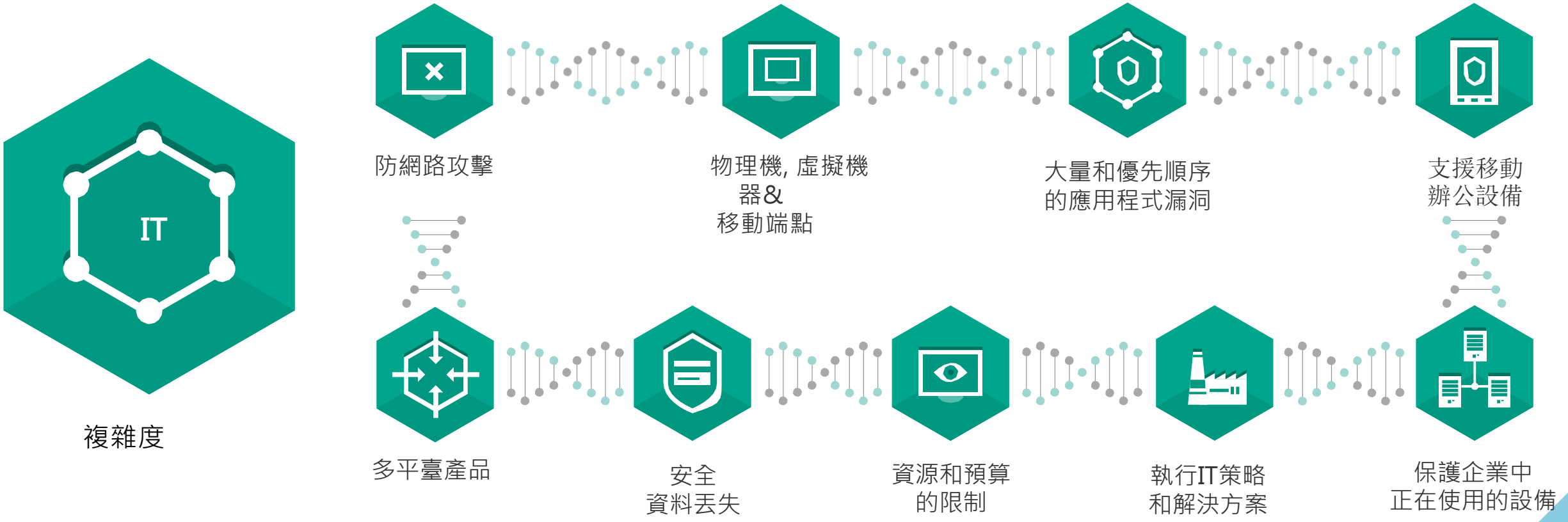
2、新的保護策略無法下發

多供應商

1、根據容量的不同選擇不同供應商

2、SaaS搭建在另一家用協力廠商IaaS的PaaS上, 發生安全問題誰來負責

複雜度是安全的最大敵人



vmware

專業

1/3 的卡巴斯基員工是研發人員

325,000 卡巴斯基實驗室每天檢測的新惡意檔的數量

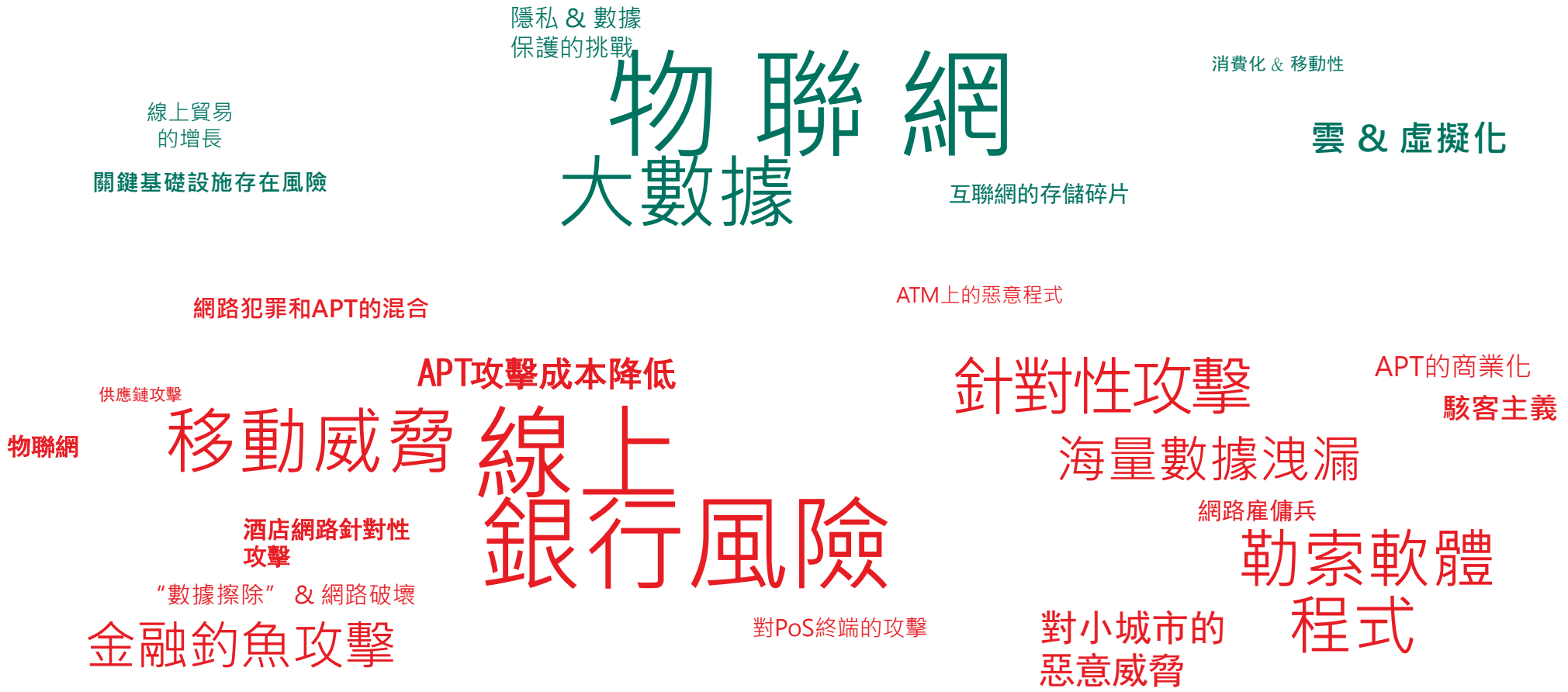
40 名全球頂尖安全專家：我們的精英團隊

我們安全專家中的全球研究和分析小組持續發掘和抵禦最先進的網路威脅

vmware

動態和威脅

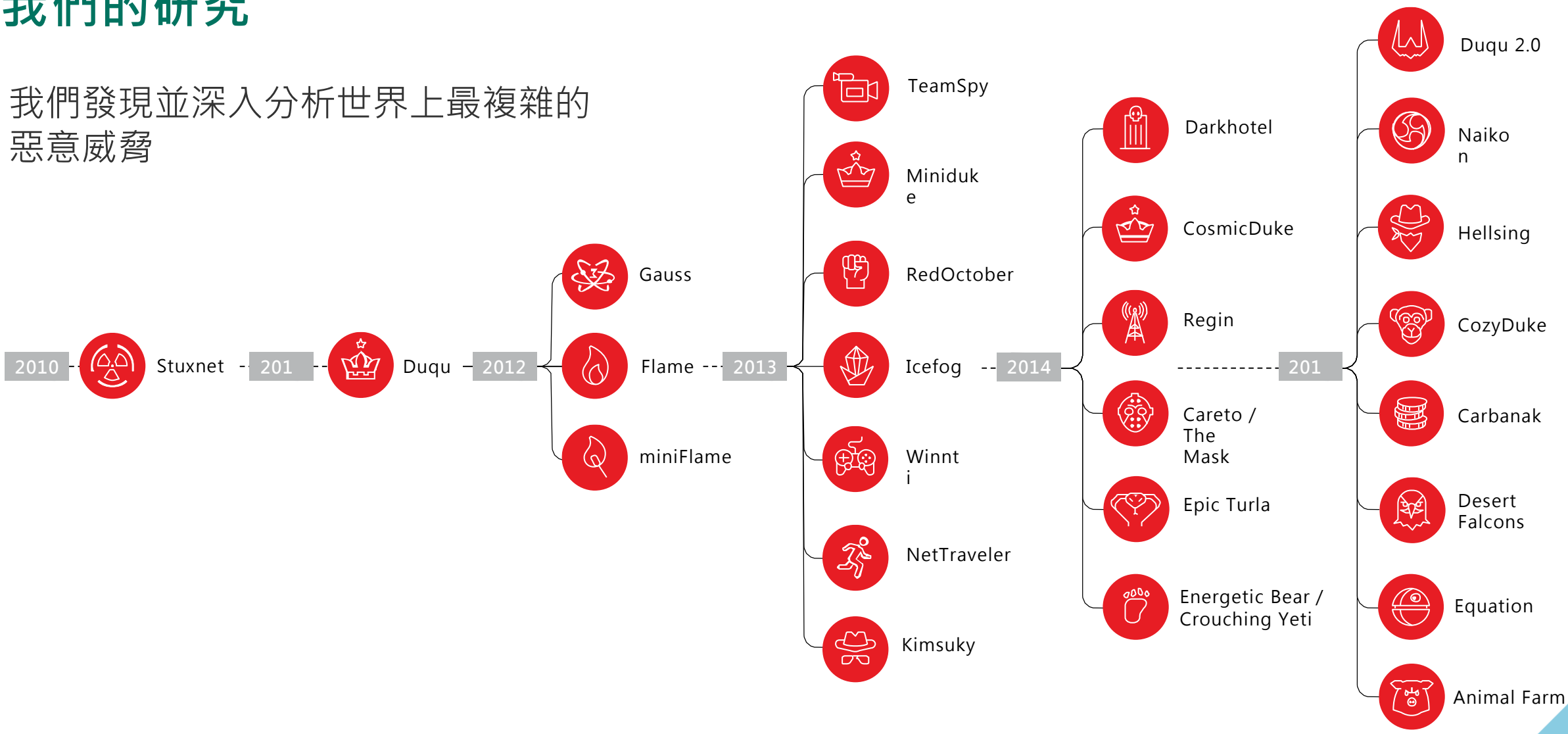
我們瞭解全球IT動態及其帶來的**威脅**



vmware

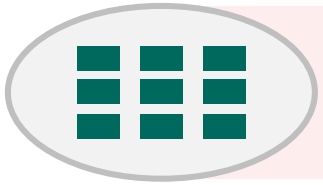
我們的研究

我們發現並深入分析世界上最複雜的惡意威脅



vmware

雲安全防護

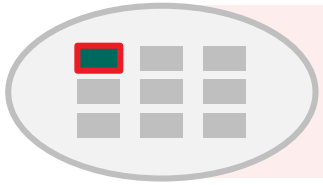


傳統保護

(有代理模式)

保護全面

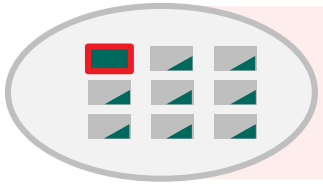
/執行效率低



無代理模式

易於部署

/適用於VMWARE



輕代理模式LA

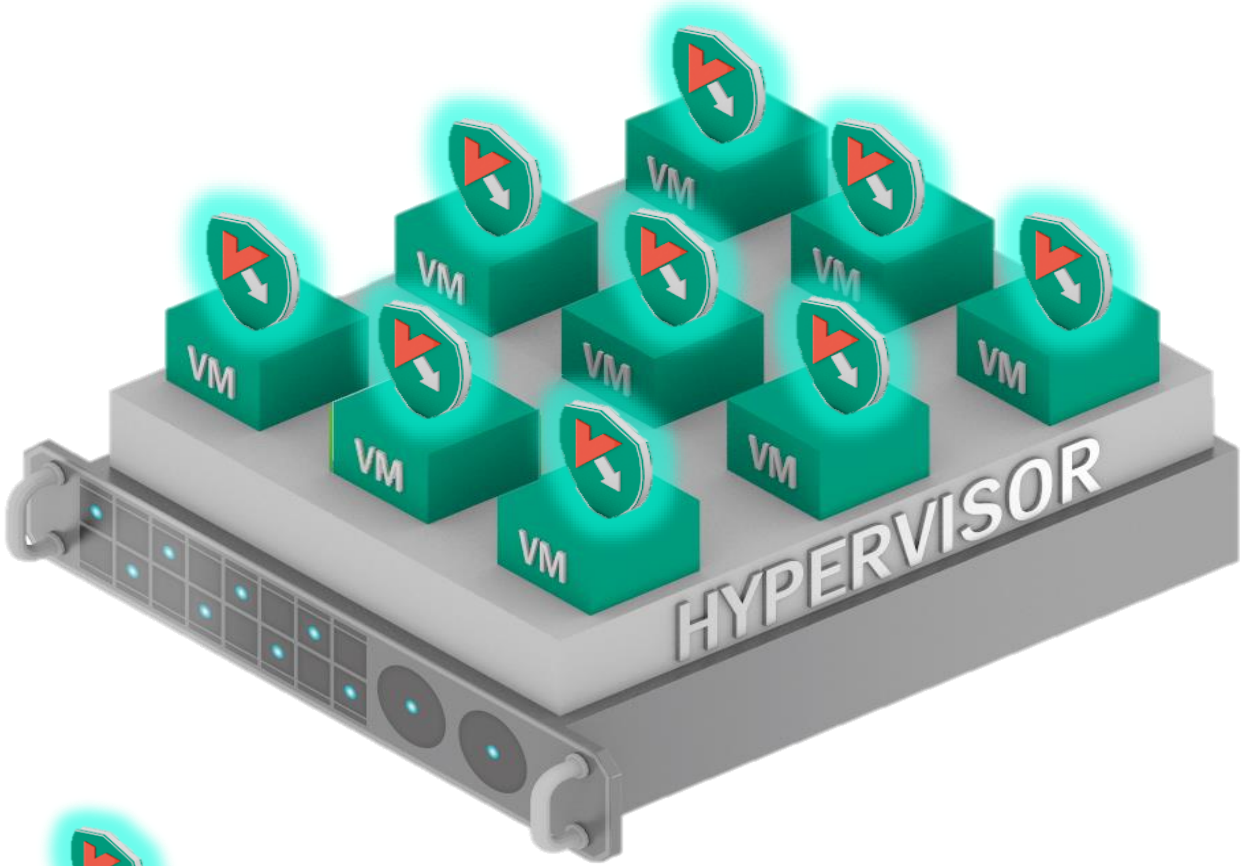
功能豐富的

安全防護

- 差異化
- 整合化
- 自動化

傳統的、基於代理的安全防護

在每個虛擬機器中載入一個完整版本的安全軟體

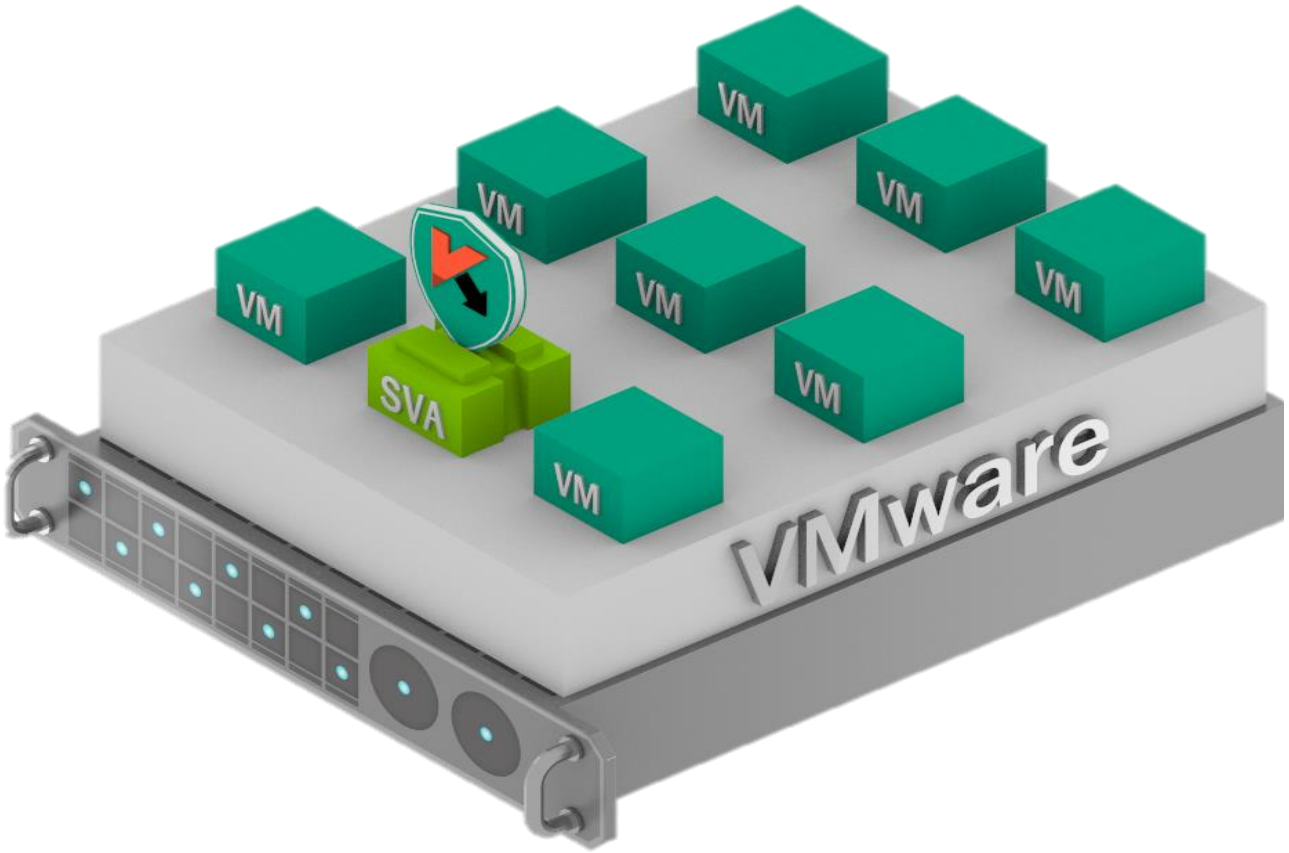


表示一個安全軟體實體

- **低效的資源利用:**
  - 冗餘的完整代理程式
  - 冗餘的反病毒資料庫
- **結果:**
  - 過度的資源消耗
  - 更新風暴
  - 防護間隙
  - 降低虛擬機器密度

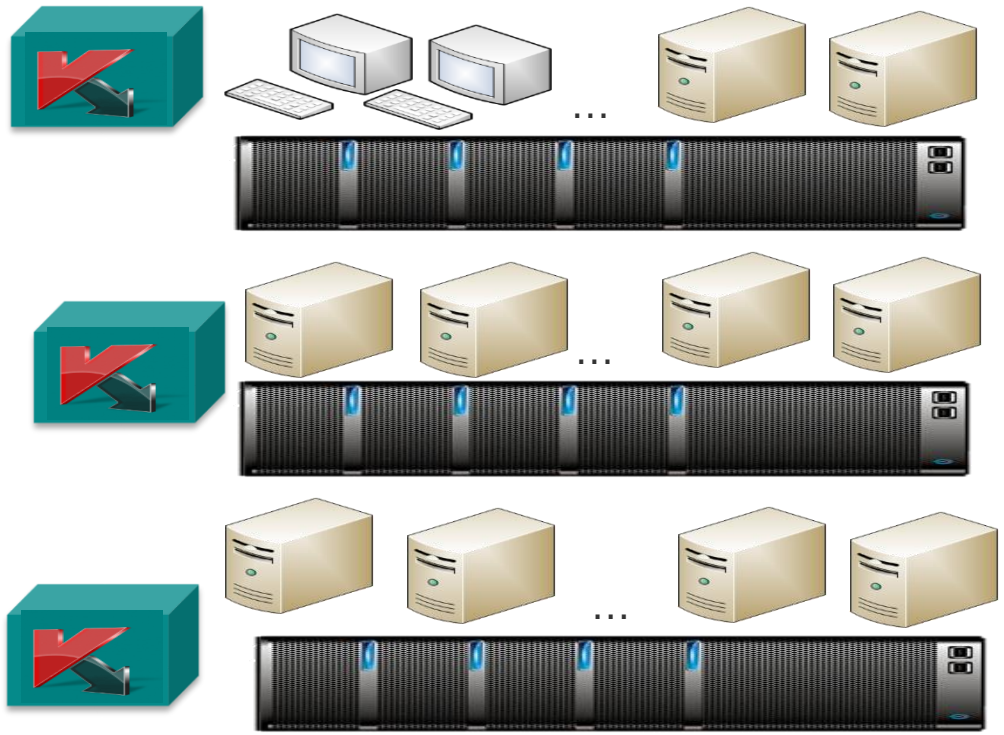
無代理方案

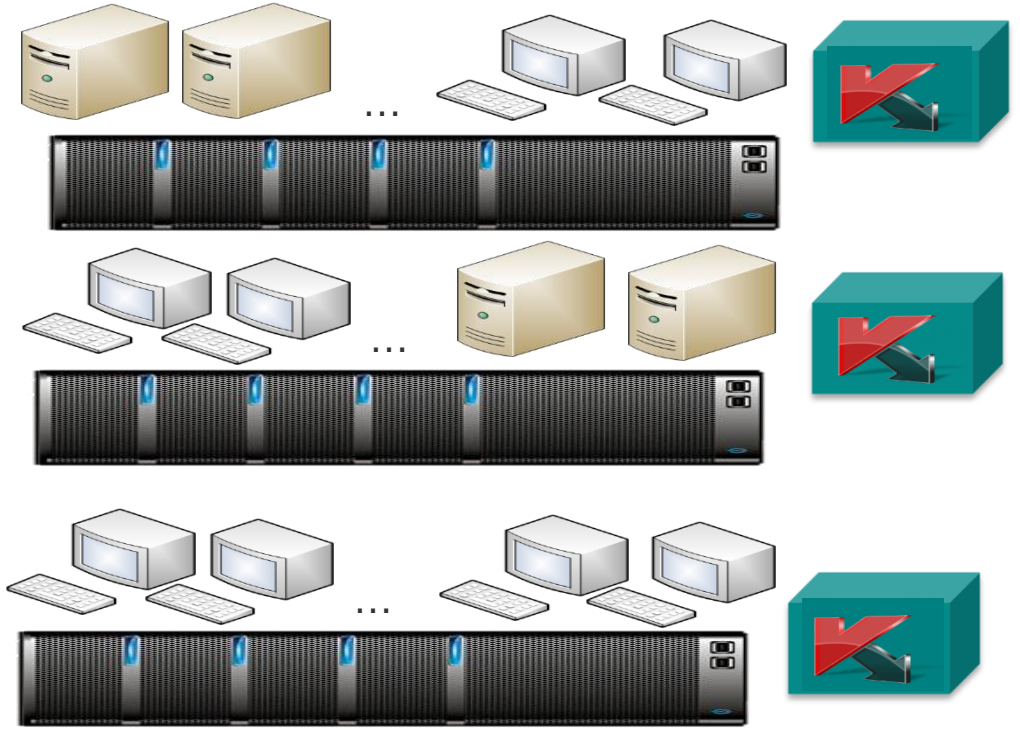
每個主機上一個安全虛擬程式執行惡意程式掃描



- **高效:**
  - 在1小時內完成安裝和操作
  - 不需要重啟或維護模式
- **避免:**
  - 過度的資源消耗
  - 更新和掃描風暴
  - 防護間隙
- **結果:**
  - 更高的虛擬機器密度

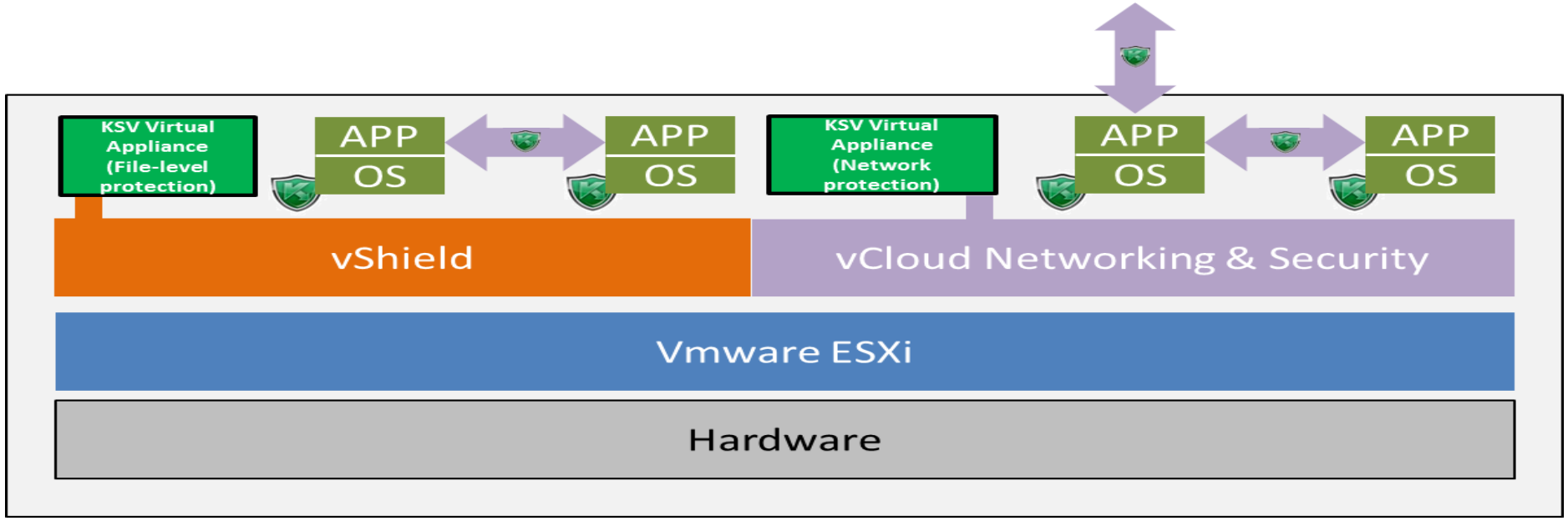
無代理方案





功能及實現方式

- 與VMware的vShield Endpoint和vCloud聯合工作
- 將反惡意程式產品載入為獨立的虛擬應用程式並集中管理
- 即時監控虛擬環境安全狀態
- 提供了入侵防禦系統 (IPS)/ 入侵偵測系統 (IDS) 來抵禦網路攻擊
- 第一個支持VMWare vCloud Networking and Security的安全解決方案提供商



在卡巴斯基保護下的虛擬機器層

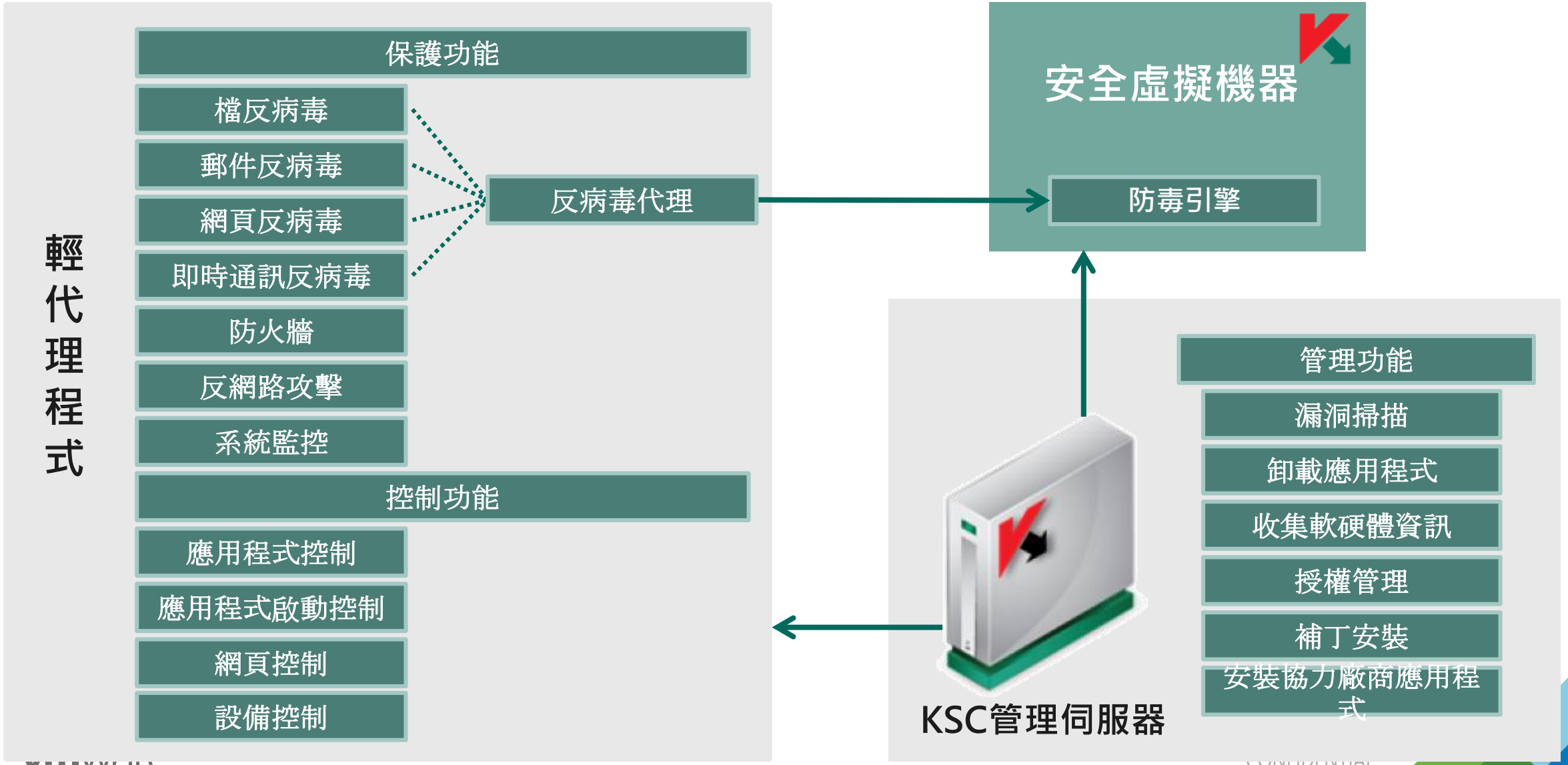
VMware層

硬體層

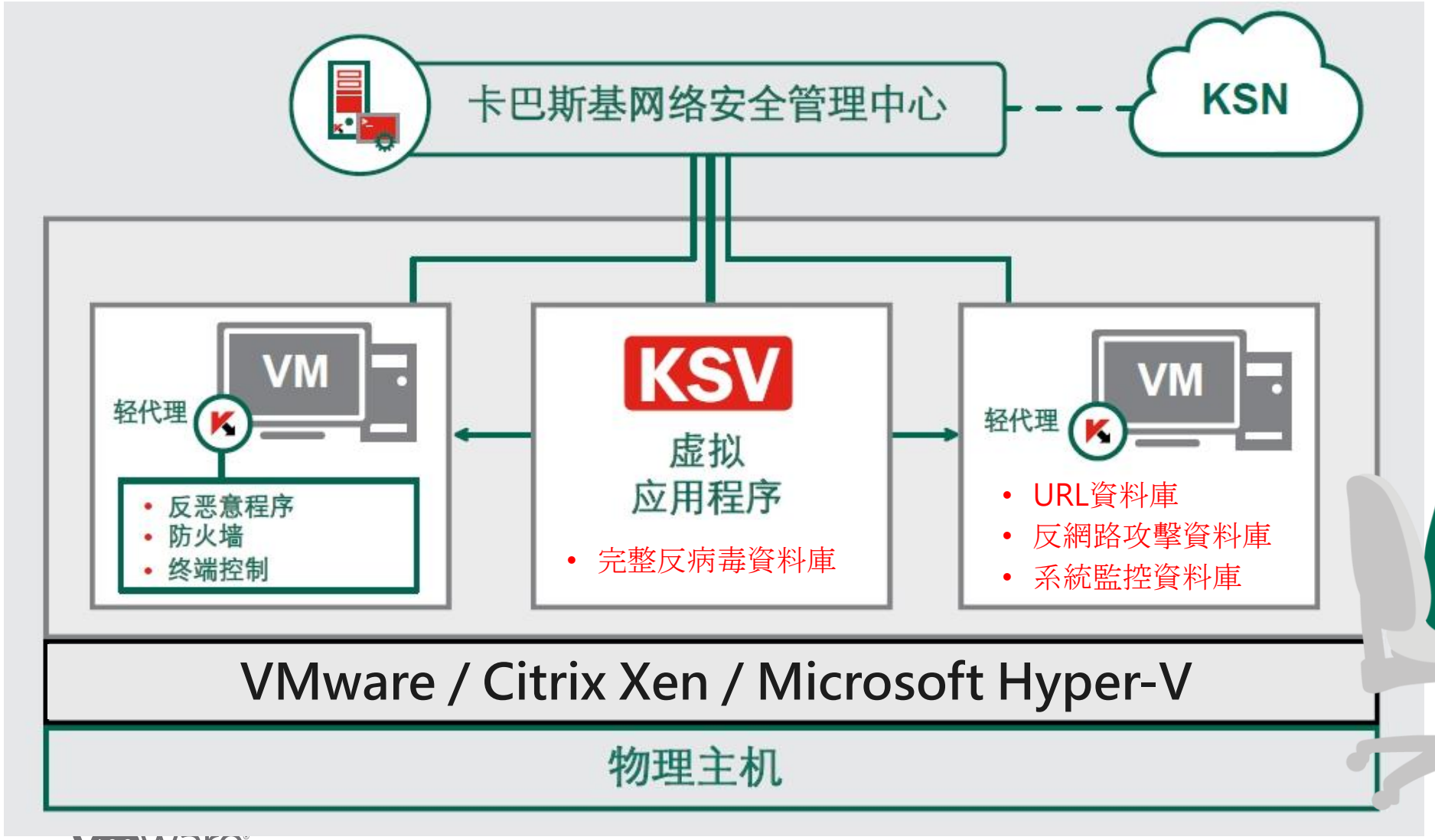
無代理防護方案優勢

- 無防病毒風暴
- 易於部署和維護
- 無防護間隙
- 無縫整合
- 高資源利用率，高VM密度比
- 傳統環境和雲環境統一管理

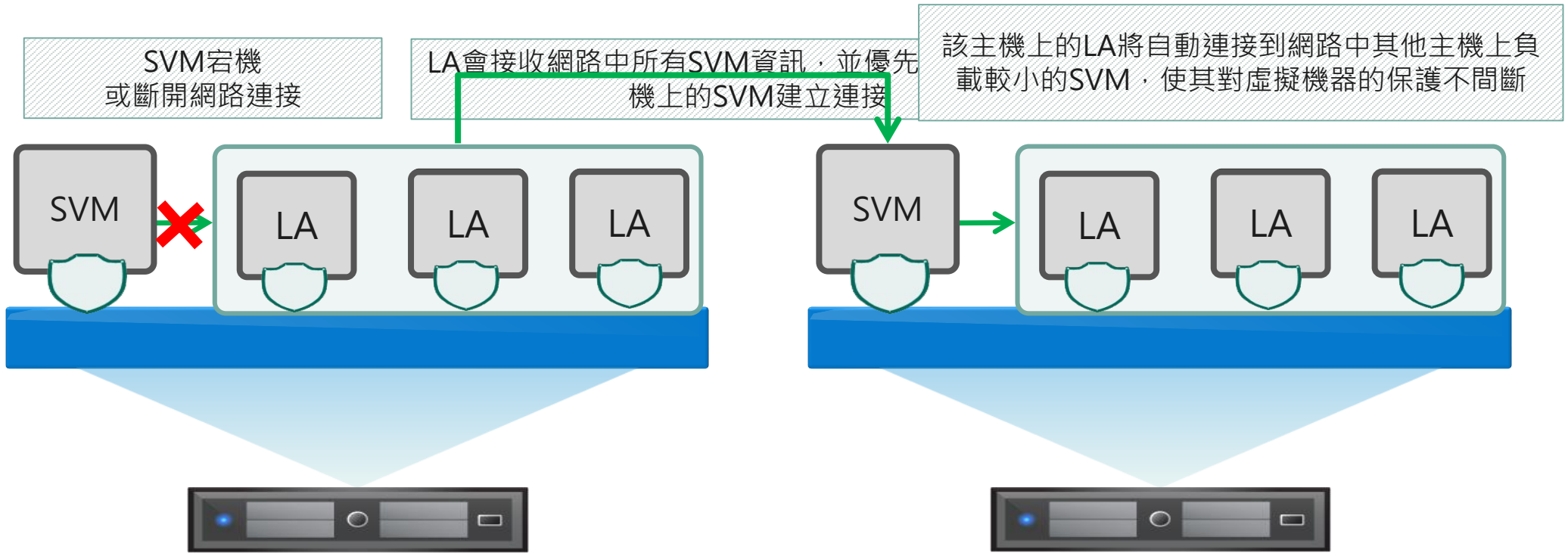
KSV 3.0 – 卡巴斯基輕代理防護方案



先進架構取得安全和資源消耗的平衡



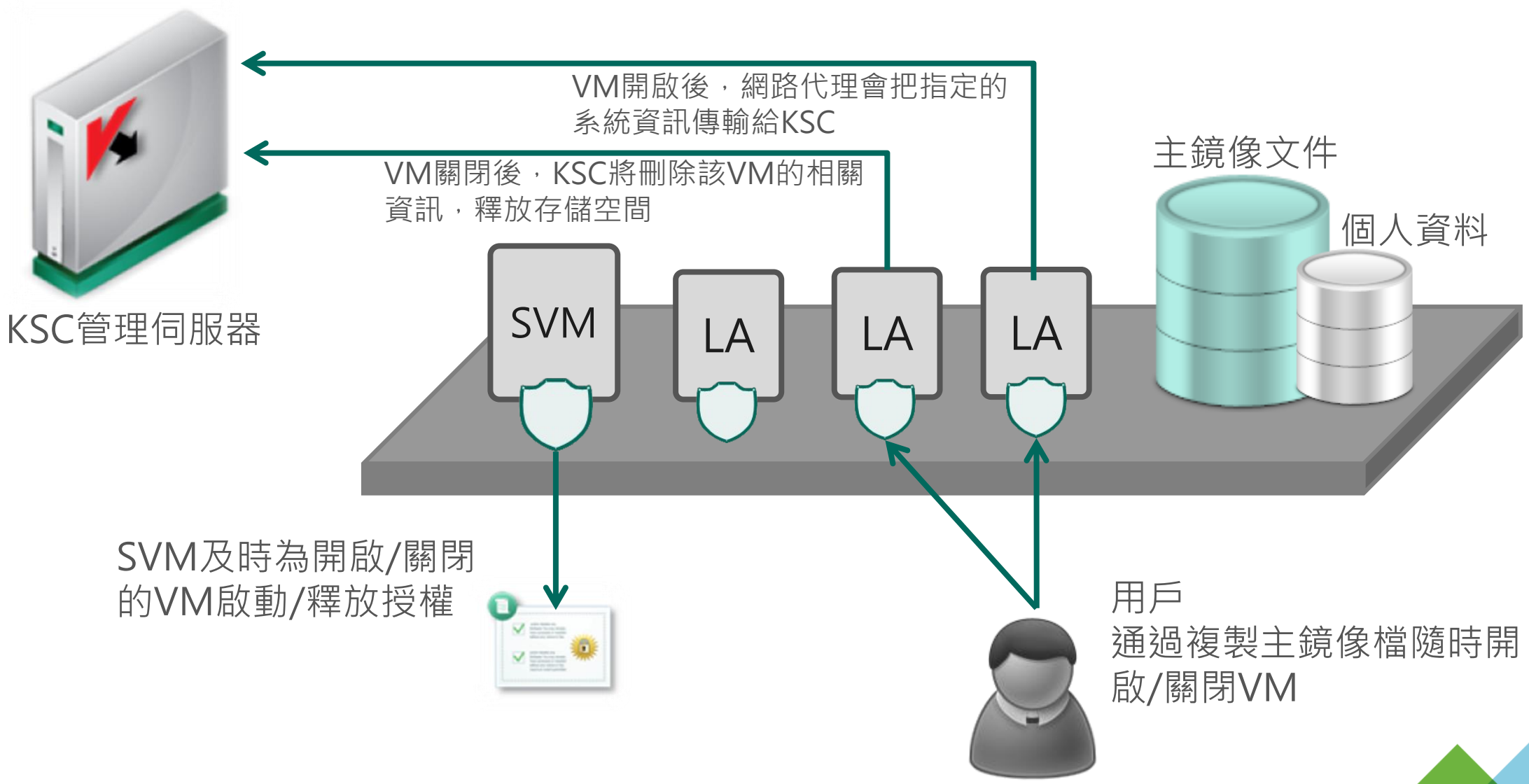
高可用性HA/永續性


SVM宕機
或斷開網路連接
LA會接收網路中所有SVM資訊，並優先
機上的SVM建立連接
該主機上的LA將自動連接到網路中其他主機上負
載較小的SVM，使其對虛擬機器的保護不間斷
SVM
LA
LA
LA
SVM
LA
LA
LA

卡巴斯基雲網路（KSN）

- 卡巴斯基安全網路(KSN) 是一個網路安全基礎設施，在獲得客戶許可的情況下，自動收集來自世界各地數百萬客戶電腦上的安全相關資料
- KSN檢測到惡意程式後，會通過卡巴斯基緊急檢測系統(UDS)和KSN及時將相關資訊傳輸給所有卡巴斯基終端使用者，比每小時的常規更新速度更快。
- 來自KSN的白名單、信譽等級和其他技術被無縫使用到用戶端的檔反病毒、網頁反病毒、應用程式的啟動/許可權控制、系統監控和掃描任務上。

智能支援虛擬桌面架構（VDI）



性能提升 — 緩存技術iSwift

本地緩存 → 用戶端虛擬機器的本地緩存——iSwift技術。

共用緩存

- 如果檔在虛擬機器上已被掃描，該檔的安全資訊會被放入共用緩存。
- 完全相同的檔存儲在不同的虛擬機器上，這類文件將不會被再次掃描。
- 如果檔案被更改過，那麼KSV將不會使用之前的判定結果。

防護能力--主動防禦Automatic Exploit Prevention

針對目前最容易被攻擊的應用/程式

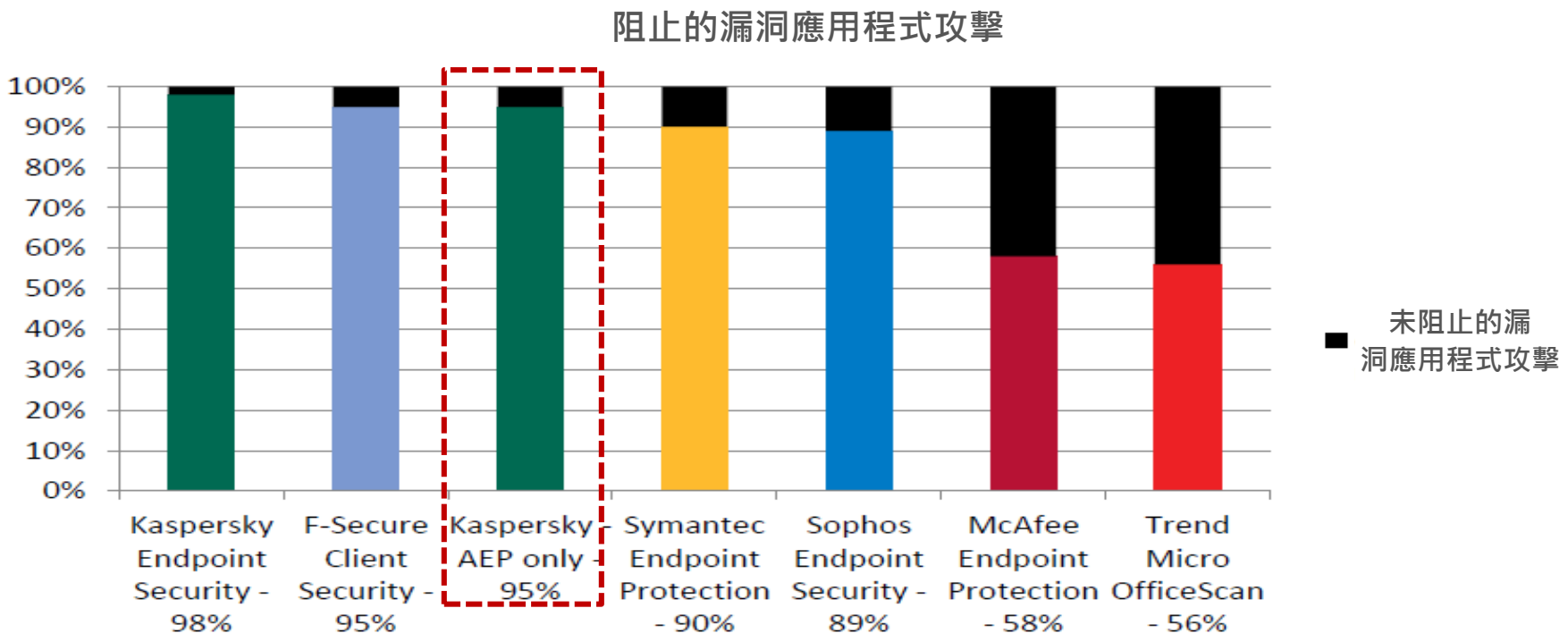
分析歸納所有攻擊的可能方式、程式的正常行為

跟蹤程式列為、文件來源等

防護零日攻擊

漏洞利用防護測試對比

不需病毒碼的情況下，卡巴能偵測95%的漏洞程式攻擊



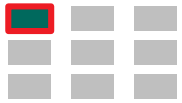
注：AEP—Automatic Exploit Prevention（自動漏洞入侵防護）

來源： MRG Effitas–Real world enterprise security exploit prevention – February 2014

應用環境的安全防護方式

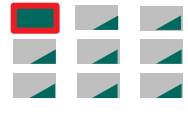
傳統的
有端點防毒代理模式

- 所有平臺



無代理
虛擬安全防護

vmware



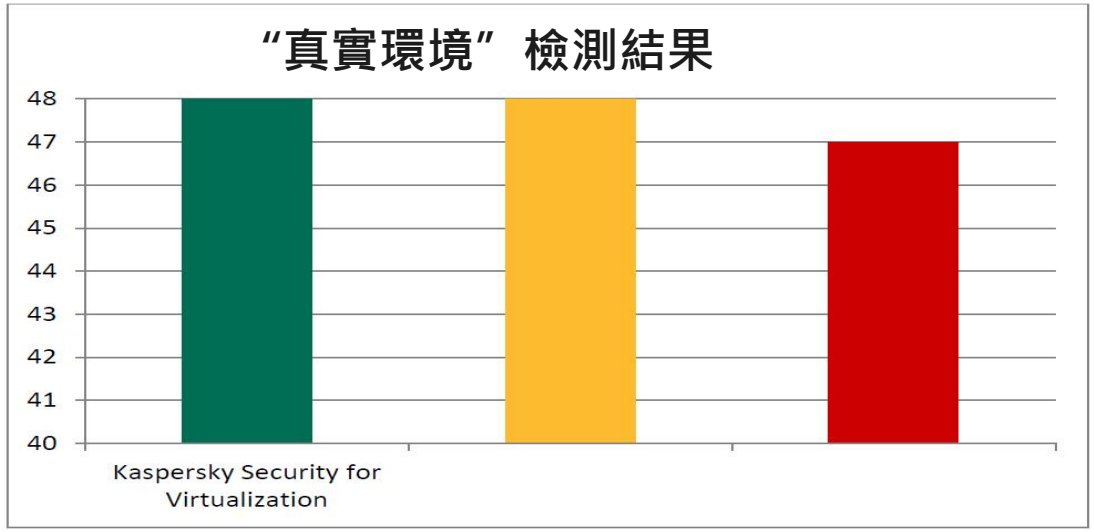
輕代理LA
虛擬安全防護

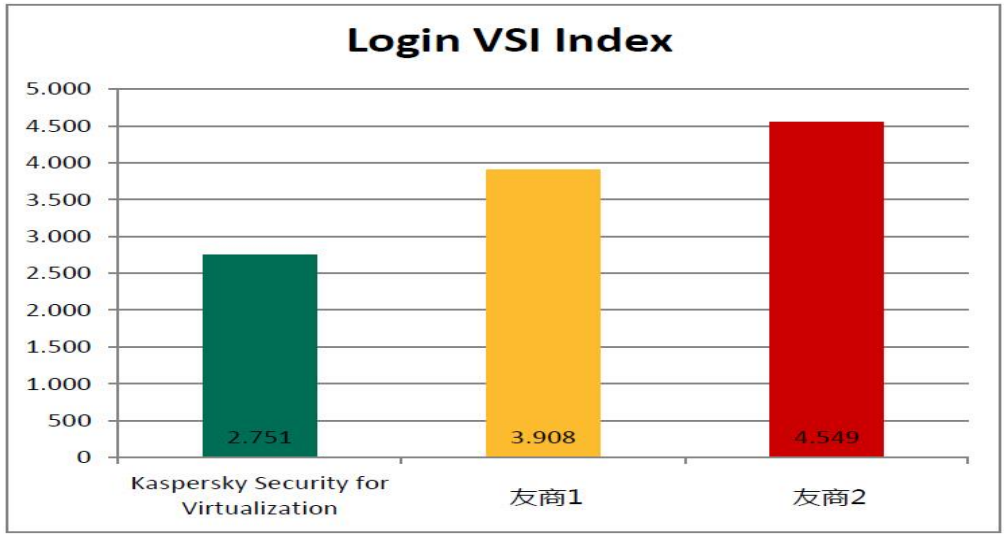
vmware

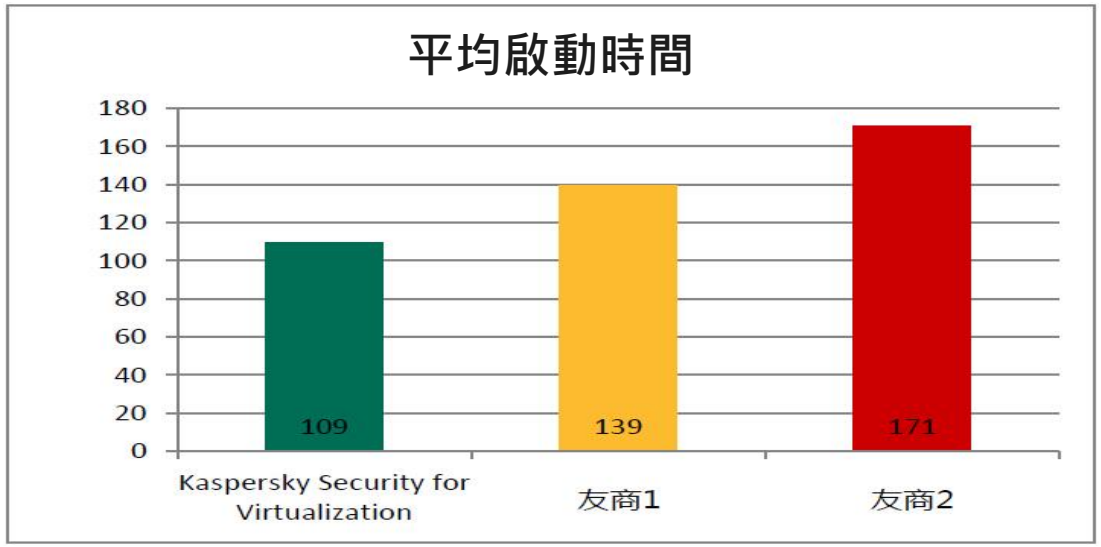
CITRIX

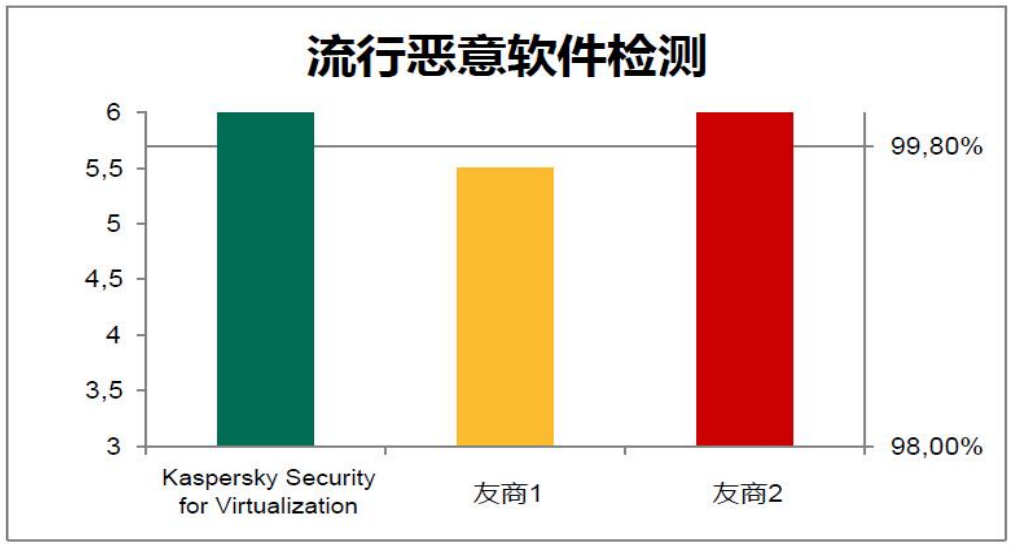
Windows Server 2008
Hyper-V

AV-Test卡巴斯基虛擬化測試結果









統一視角 統一管理

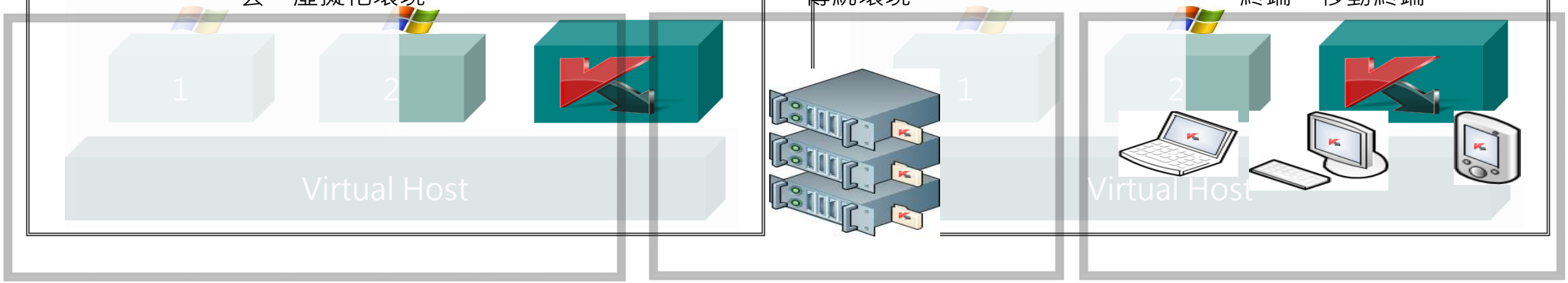
卡巴斯基網路安全管理中心KSC

Administrator

雲、虛擬化環境

傳統環境

終端、移動終端



一個平台一個介面，無須重複登入不同管理介面

卡巴斯基雲安全解決方案優勢

無代理/輕代理防護方案

支援VMware、Citrix、Hyper-V跨平台

具有傳統安全的安全性，
但資源消耗大幅減少

高性能，高可靠性

傳統環境、移動環境、雲環境
統一管理

市場驗證，快速革新

卡巴斯基安全解决方案成功案例

KASPERSKY LAB FERRARI'S CHOICE FOR IT SECURITY

PARTNERING FOR SUCCESS

In April 2013, Ferrari announced that Kaspersky Lab's IT security technology would be installed on more than 2,500 endpoints across the business by the end of the year. Additional rollouts are continuing to take place in 2015, aiming to cover mobile devices and, eventually, infrastructure servers.

This commercial decision marks an evolution in a relationship going back to 2010, when Kaspersky Lab became a sponsor of the Ferrari F1 team. Both partners are now looking forward to a future of shared collaboration.

"We're looking forward to further developing our partnership in the technological field and hope that this five-year deal is just the first stage," says Ferrari CIO Boero. Kaspersky Lab's Marketing Director for Europe, Aldo del Bo' says the partnership reflects the beginning of new developments and opportunities for next-generation products, as smart technologies become more widespread in high-end vehicles.

But, even more importantly, says Del Bo': "Ferrari is one of the most valuable brands in the world. And Kaspersky Lab is protecting it. You can only begin to imagine how this partnership will evolve, as we begin to innovate and combine our technologies and values with those of Ferrari."

卡巴斯基安全服務

專業的定期巡檢
和應急處置

及時的健康檢查和升級

問題分級處置

專業的分析報告

培訓和知識更新

我們在全球IT安全共同體中的角色

INTERPOL | STRATEGIC PARTNER

我們參與全球IT安全體及國際組織的協同行動和網路威脅調查，包括 INTERPOL 和 Europol, 全球範圍的執法部門和電腦應急回應小組

我們為INTERPOL和Europol人員以及很多國家的員警機關提供定期培訓課程，例如倫敦警察局

我們在全球大會上提供專業的演講，例如達沃斯全球金融論壇

我們舉辦年度卡巴斯基實驗室安全專家峰會，彙聚世界上最優秀的IT安全專家

vmware

READY
FOR ANY
vForum2015