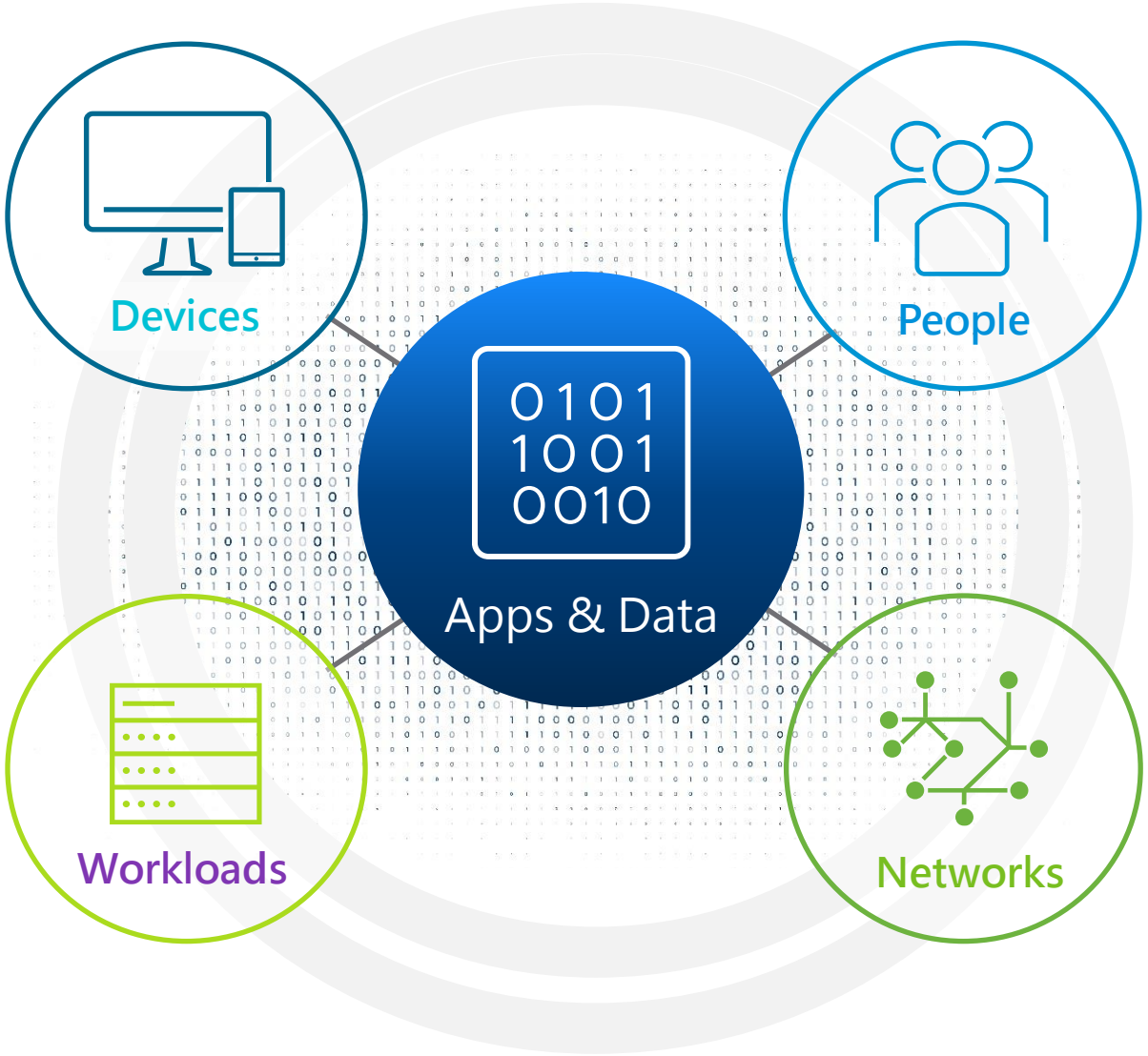
VMware Agentless Security

內建式資安與端點防護



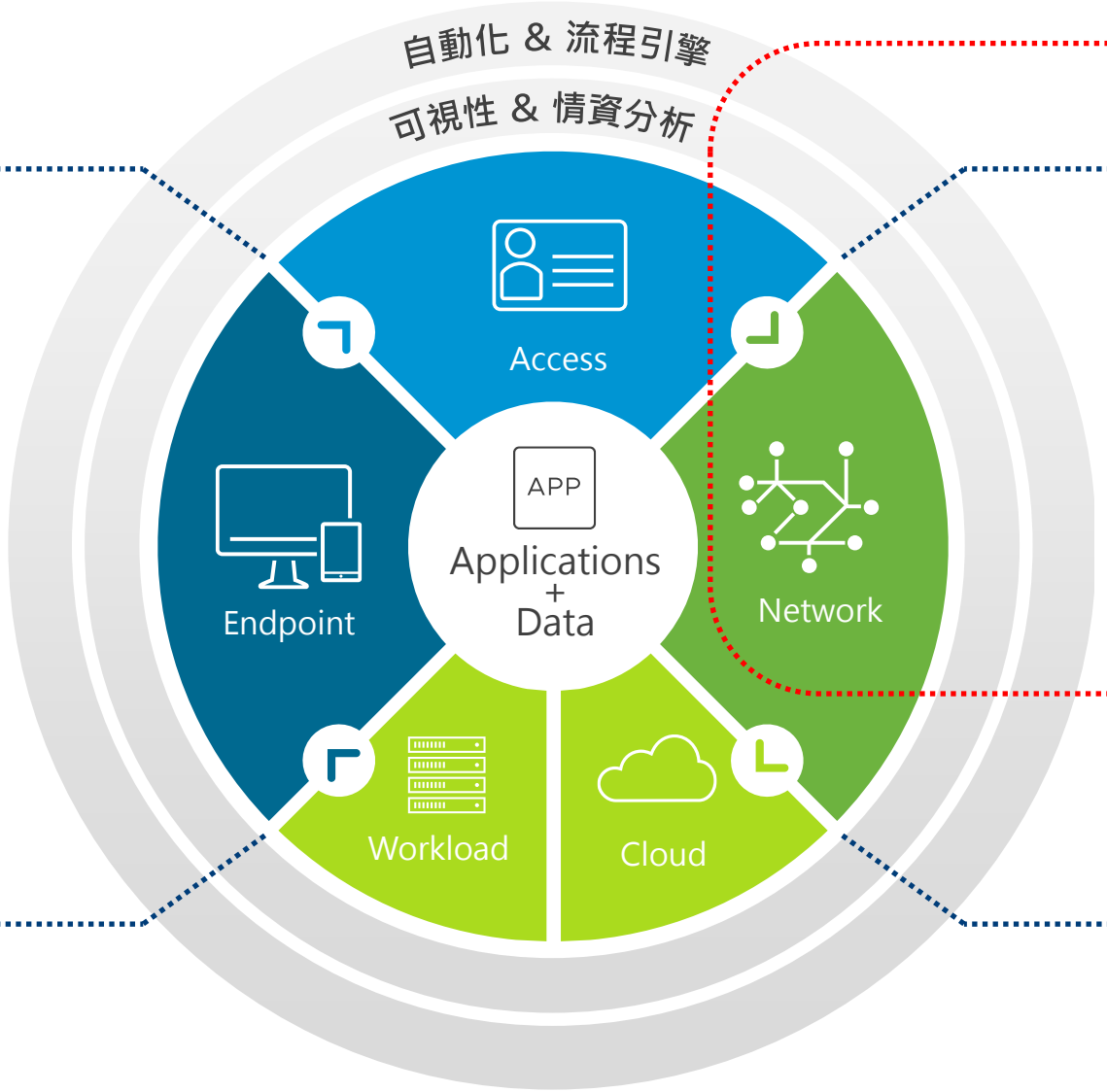
©2021 VMware, Inc.

VMware 資安框架與相對應的企業資安組織

Securing your critical applications and data

VMware
Workspace ONE
Access Management / Endpoint Compliance

VMware
Firewall, Advanced Threat Prevention, SASE Platform



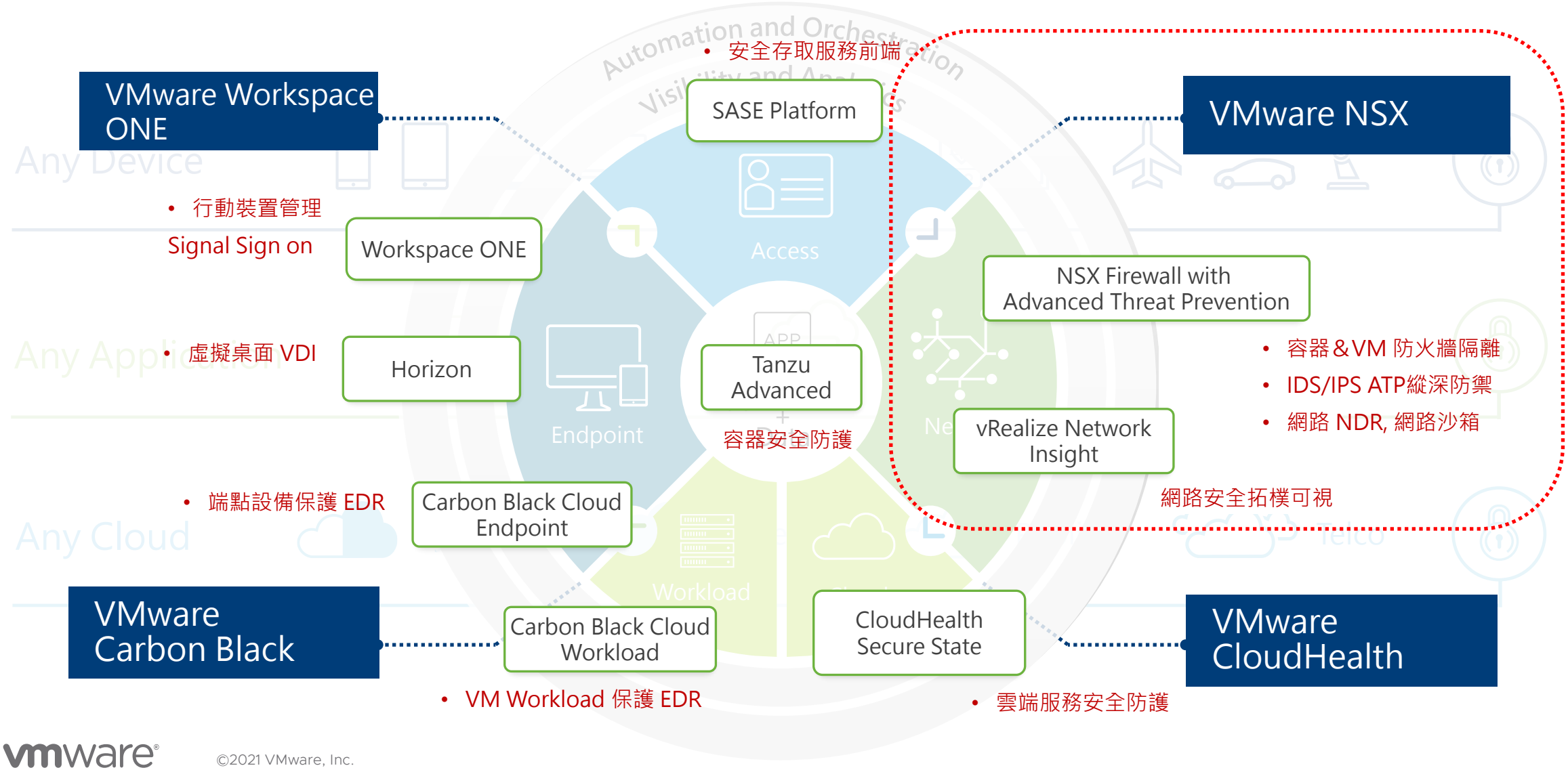
VMware
Carbon Black

VMware
CloudHealth
Secure State

©2021 VMware, Inc.

VMware 資安框架與解決方案

Securing your critical applications and data



©2021 VMware, Inc.

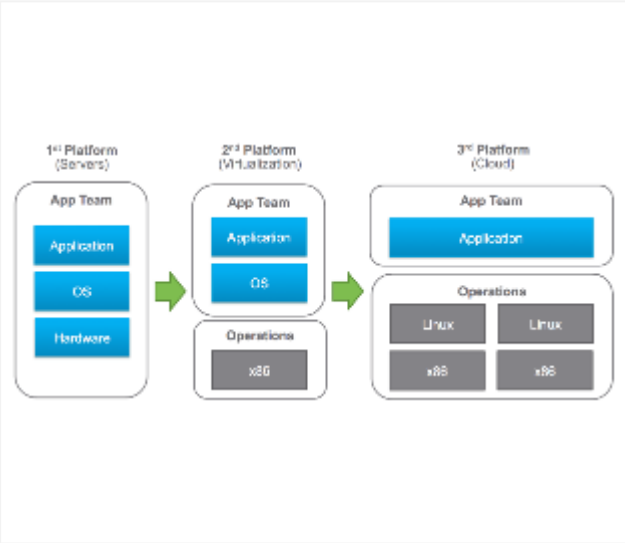
打造零信任網路，完善防護您的重要系統

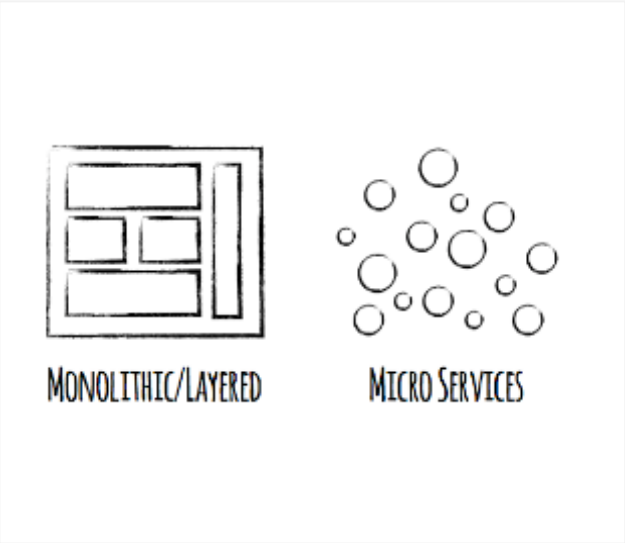
Colin Jao 饒康立

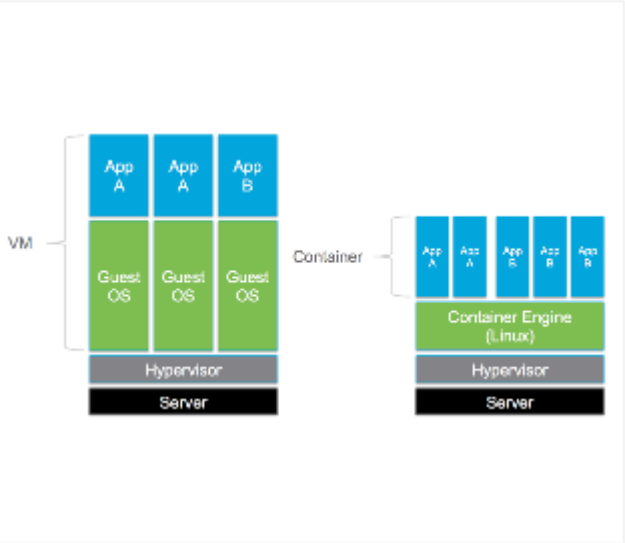
VMware 資深架構師

©2021 VMware, Inc.

應用與資料中心的演變劇烈，IT 及資安單位必須因應變化進行考量







實體設備

↓

虛擬化資源池

↓

公有雲

Mainframe

↓

三層式架構

↓

微服務

實體伺服器

↓

虛機

↓

容器

©2021 VMware, Inc.

因應企業數位轉型需求，任何資訊方案建置時需要支持雲原生應用架構

可以被程序化、自動化

- 集中化管理
  - 將控制層與作業層分離
  - 集中管理大規模環境，無需到單一設備進行配置
- 可被程序化
  - 開放的 Restful API 與 SDK
  - 支援常用組態管理工具及自動化工具 (如 Ansible / Terraform / vRA)

能夠支援虛擬化 - 容器架構

- 資源池化
  - 可快速部署，無需採購、上架、接線
  - 隨需彈性取用與移除
  - 易於橫向擴充
- 軟體架構配置
  - 以虛機的方式提供服務 (Stateful)
  - 以容器的方式提供服務 (Stateless)

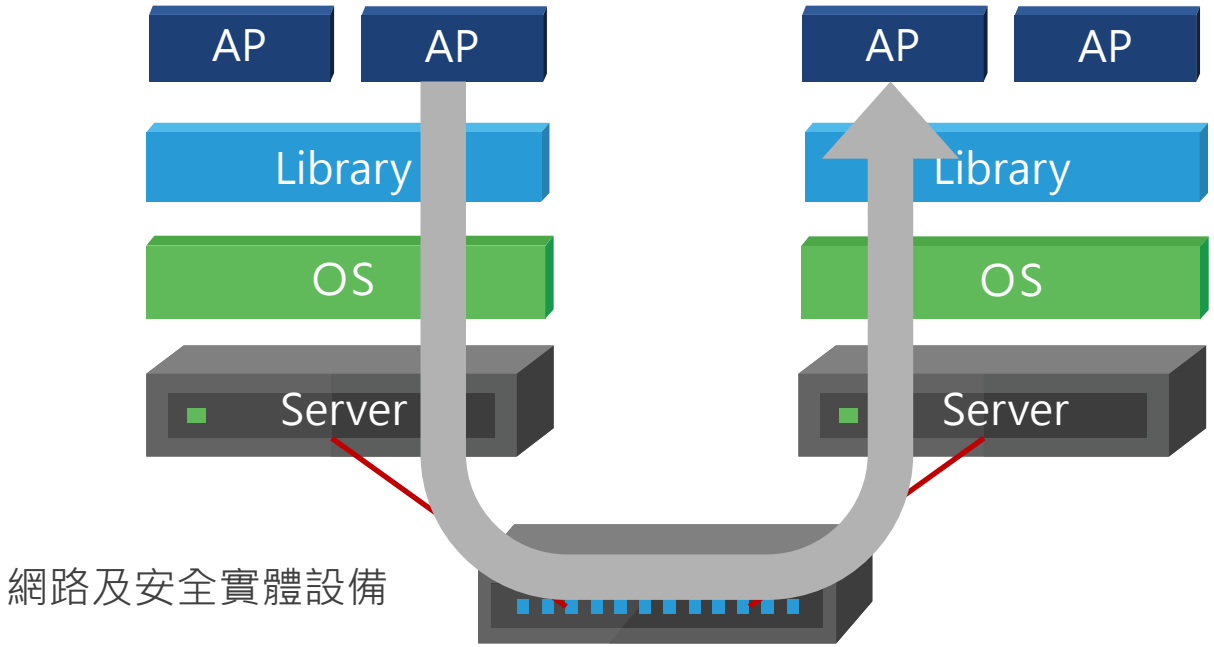
可以在不同雲環境部署

- 可以快速擴充到全球
- 可以在不同雲環境進行部署與調度

©2021 VMware, Inc.

軟體架構由採用實體機 – 虛擬化 – 容器化，傳統網路硬體設備對支援網路的可視性、路徑優化、安全性或可維運性會越來越難

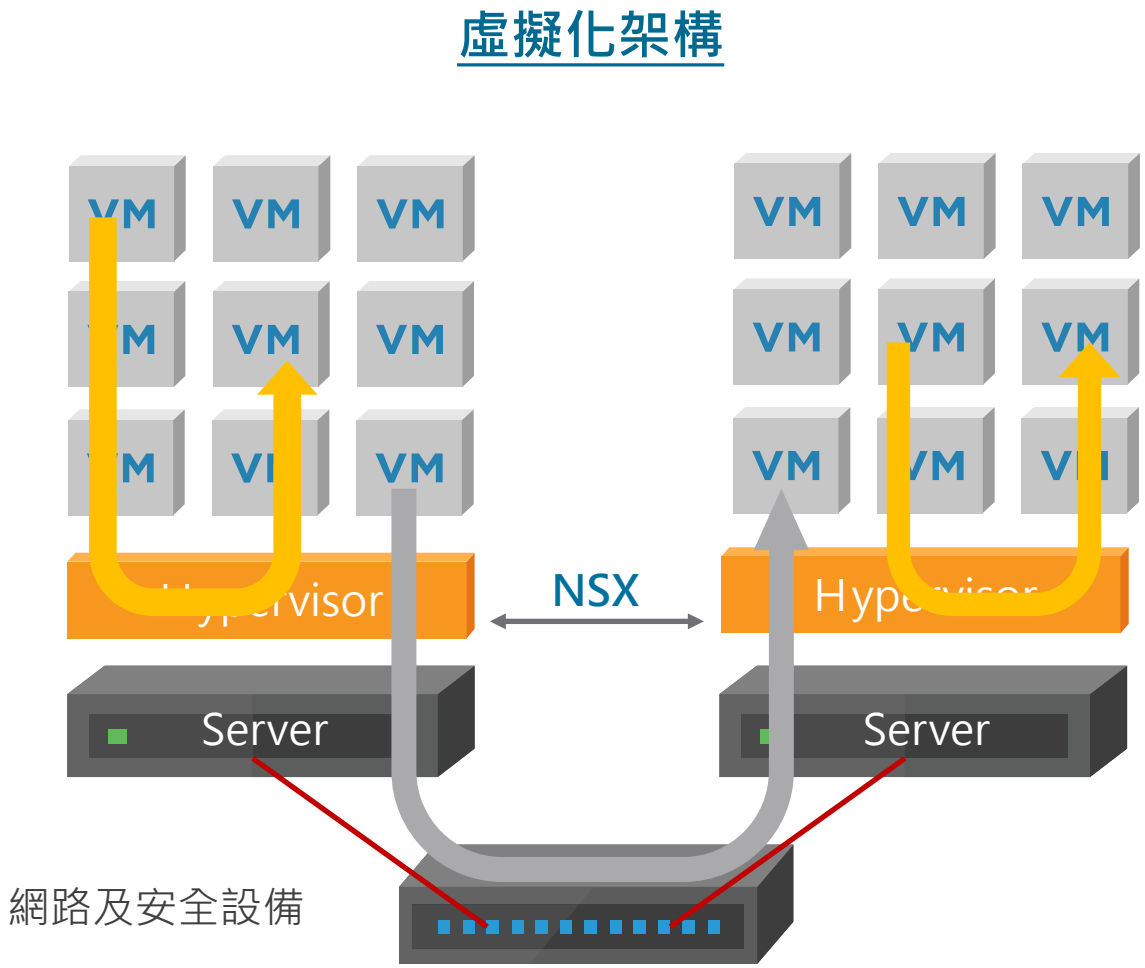
傳統實體架構

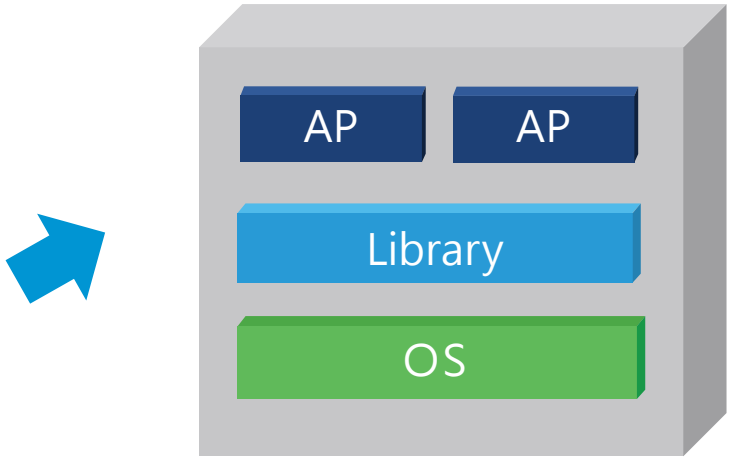


- 在傳統實體架構下，網路實體設備要看到、控制、除錯在業務應用構件間的網路流量，並不太難

©2021 VMware, Inc.

軟體架構由採用實體機 – 虛擬化 – 容器化，傳統網路硬體設備對支援網路的可視性、路徑優化、安全性或可維運性會越來越難

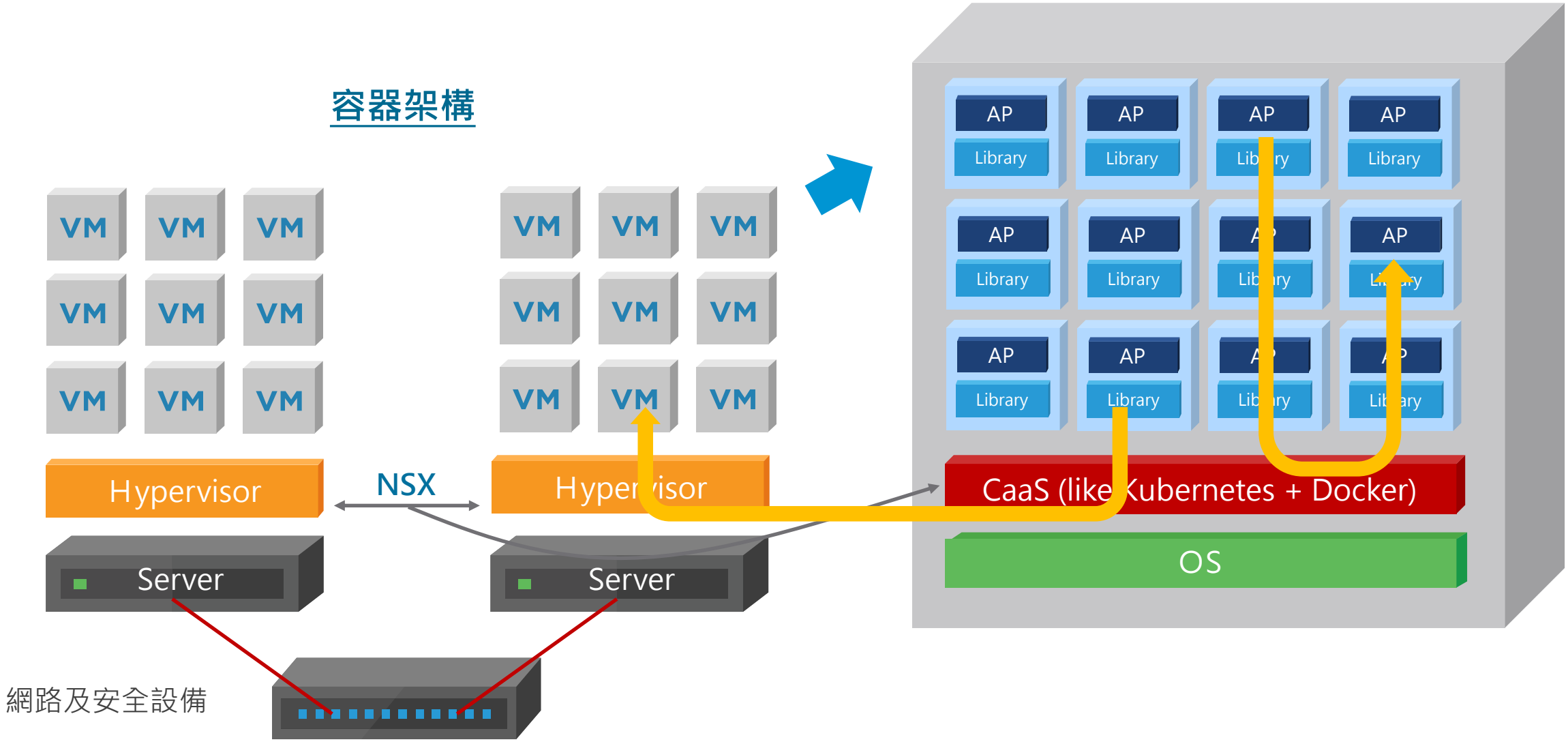




- 在虛擬化架構下，有相當部分的網路封包會在同一台實體伺服器內交換（效率較佳），實體網路設備要進行網路流的監控、除錯、控制並不容易
- 在Hypervisor層控制相當容易

©2021 VMware, Inc.

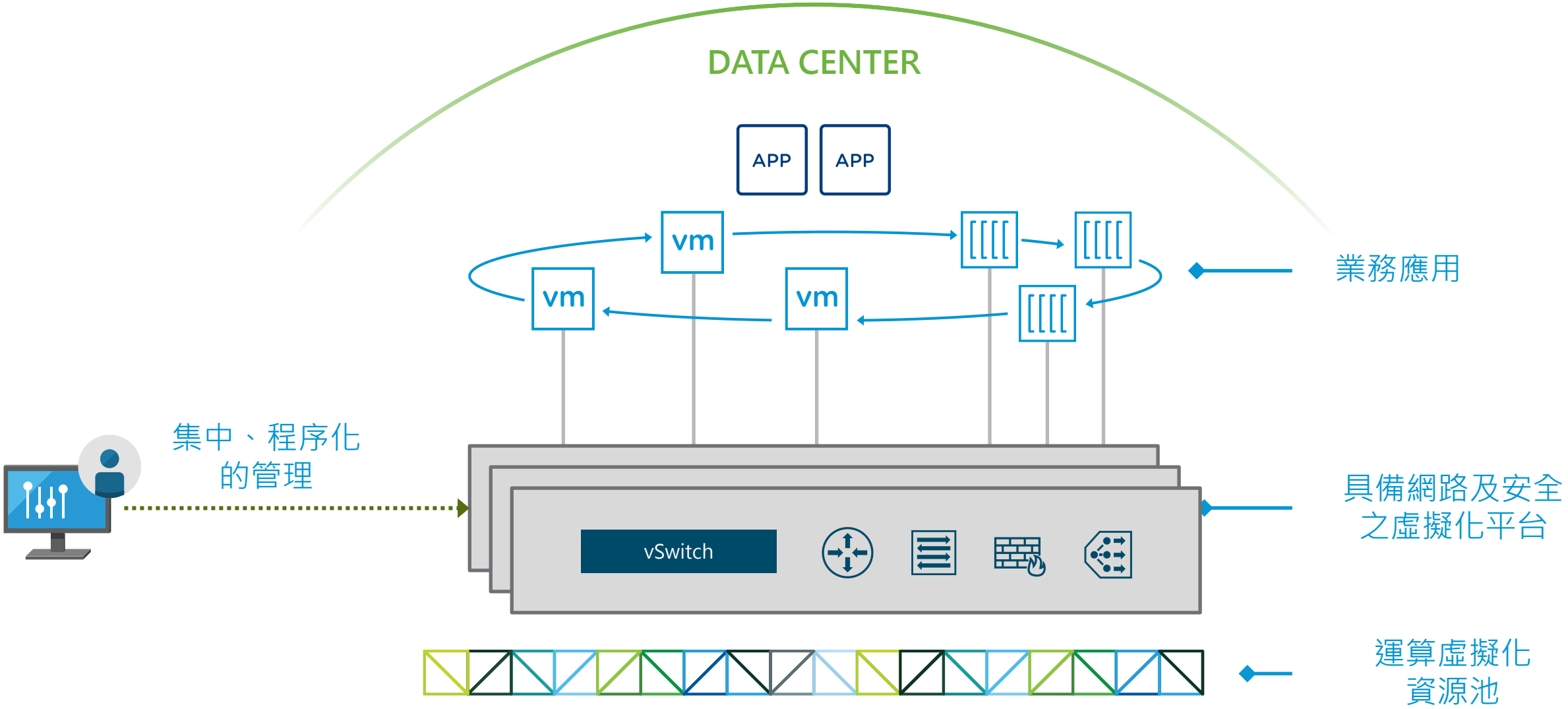
軟體架構由採用實體機 – 虛擬化 – 容器化，傳統網路硬體設備對支援網路的可視性、路徑優化、安全性或可維運性會越來越難



©2021 VMware, Inc.

VMware 對應新型態工作負載的統合安全與網路管理機制

以資源池的方式快速建立工作負載，直接於資源池內提供需求之網路及安全功能



©2021 VMware, Inc.

對於現代化工作負載（虛機及容器），於網路及安全的設計要求

以分散式、最佳路徑優化於工作負載間的連接，以及封包檢視等維運需求

提供每個工作負載前的網路安全防護

快速提供工作負載需求的上層服務如負載平衡等機制，且易於擴充

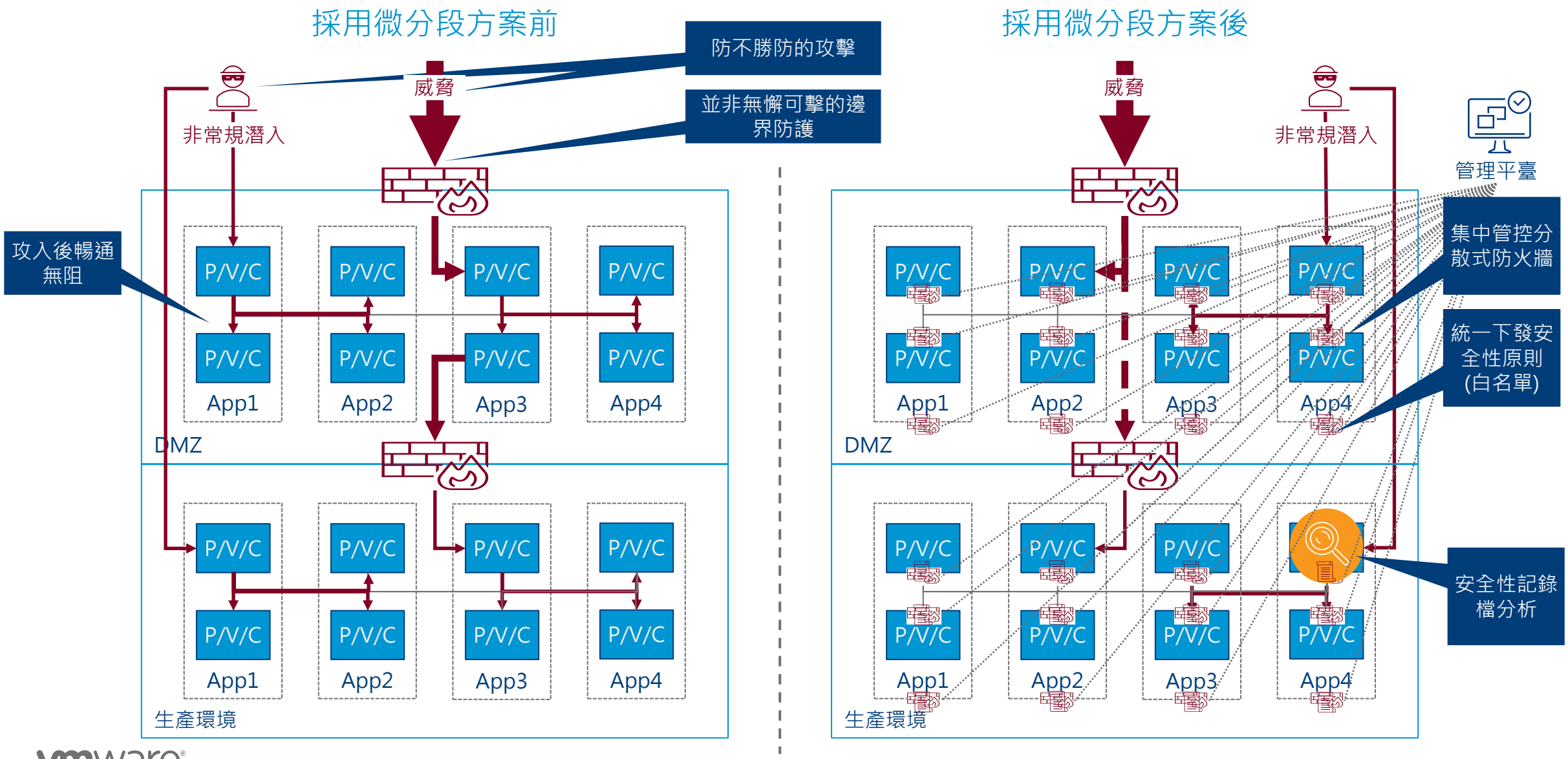
以集中、可程序化的方式提供網路及安全管理

與硬體解構，可於開放式網路環境內運作

支持於私有雲及公有雲異質環境運作

©2021 VMware, Inc.

微分段方案：打造零信任網路的不二方法



©2021 VMware, Inc.

微分段方案提供網路安全防護的四項重點

網路防護機制保護 每一台虛擬機與容器，所有網路流量都可以被防護與隔離

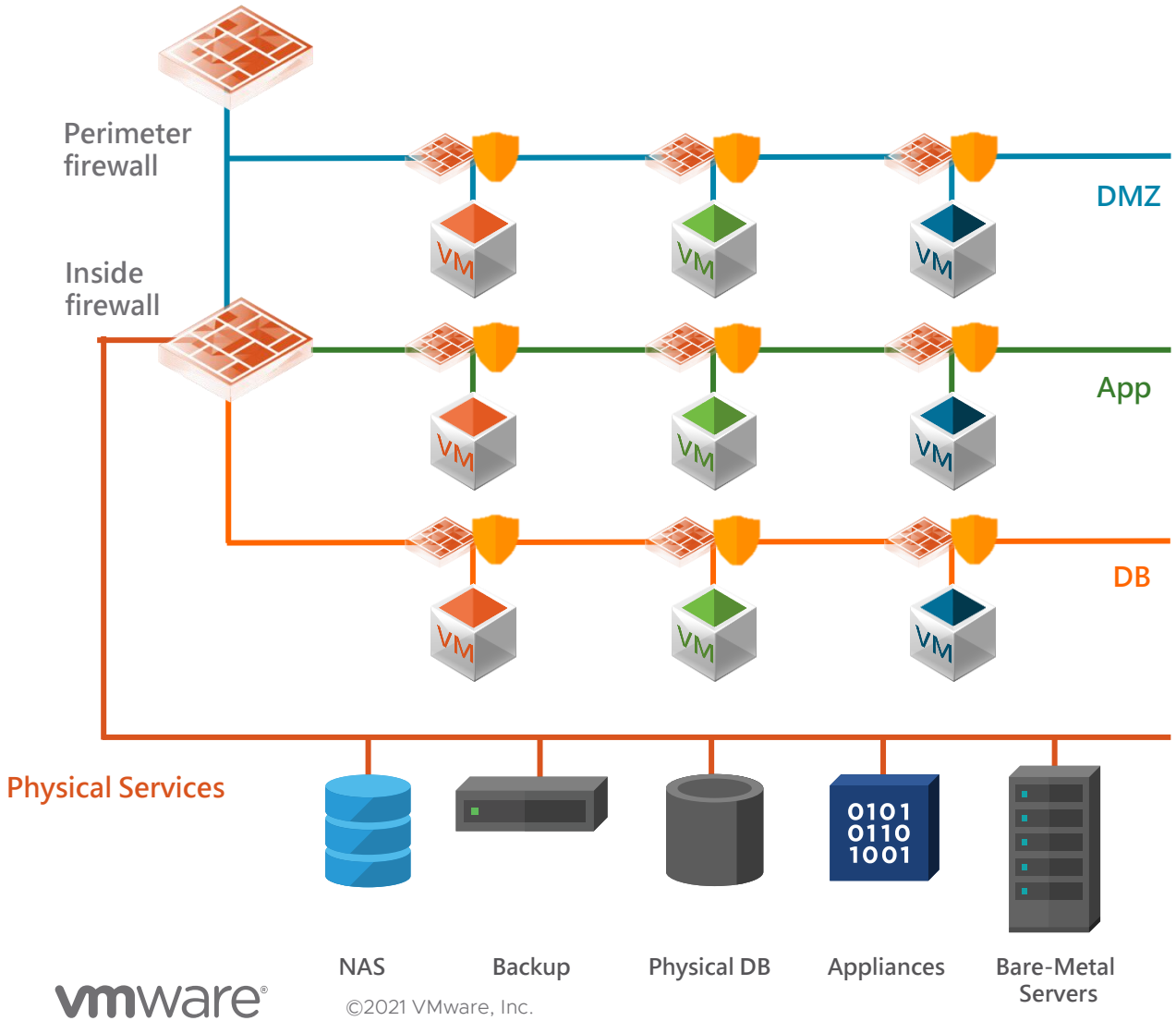
資安政策設定方式與業務直接連結，與網路地址解構，達成安全自動化

提供自下而上，完整的網路安全防護功能

可針對工作負載網路流進行記錄、監看、及安全防護建議

©2021 VMware, Inc.

重點一：於資源池內，每個虛機及容器前直接提供網路安全防護功能



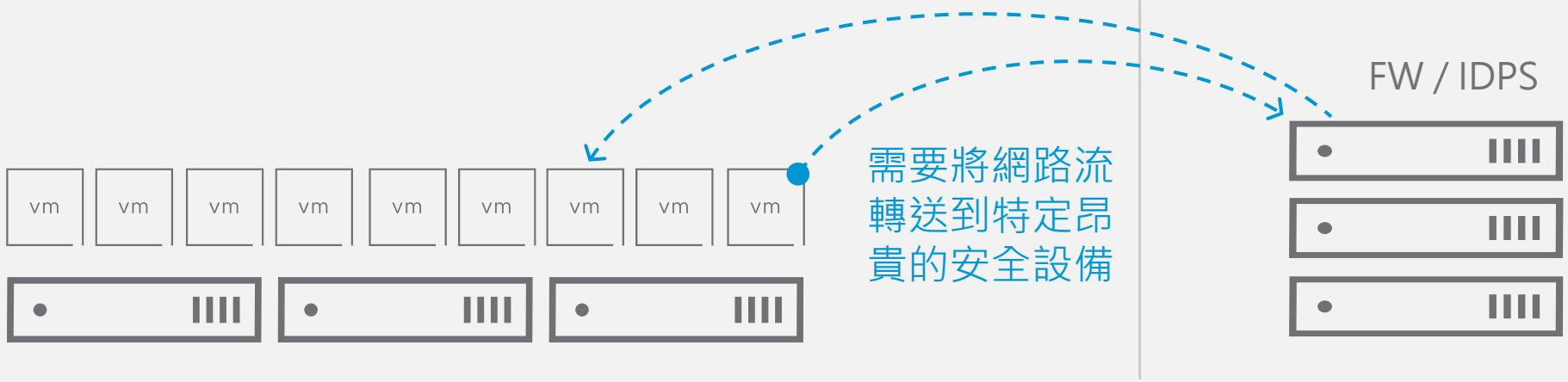
- 每一個虛機或容器都成為自己的安全微分段，每個封包都能夠得到檢查
- 每一個虛機或容器前均能進行安全控制，無論虛機或容器是位於同一網段或同一工作主機
- 於虛機或容器無需安裝 Agent
- 無需異動網路架構即可部署（無需更改架構，將網路封包導向實體防火牆）

©2021 VMware, Inc.

傳統的硬體、單一虛機網路安全防護架構： 集中化、成本高、複雜

若考慮在東西向配置網路防護機制，會有大量的網路流髮夾彎及過高部署成本

傳統網路安全防護 | 東西向微分段機制



流量限制

網路部署機制複雜

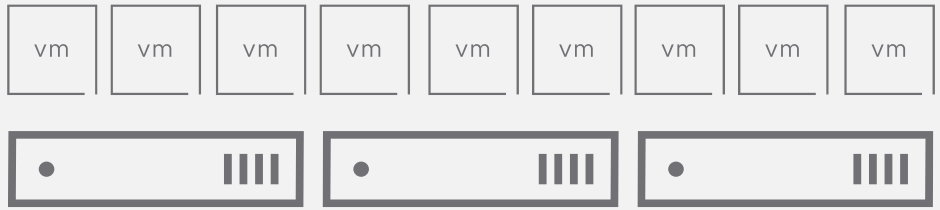
與虛擬化環境內需求之
vMotion等機制無法結合

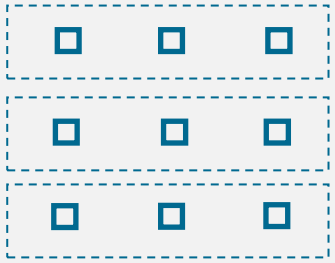
©2021 VMware, Inc.

東西向微分段機制：

分散式架構易於擴張、可監控所有虛機 / 容器之網路流、集中管理、最佳化應用網路傳輸

傳統網路安全防護 | 東西向微分段機制





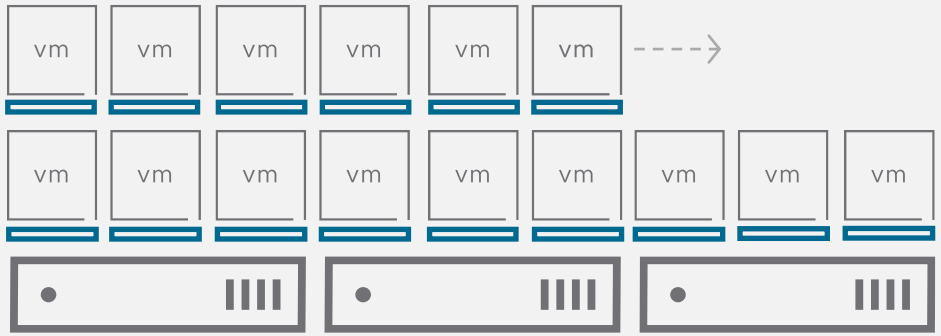
©2021 VMware, Inc.

東西向微分段機制：

分散式架構易於擴張、可監控所有虛機 / 容器之網路流、集中管理、最佳化應用網路傳輸

傳統網路安全防護 | 東西向微分段機制

在每個虛機前進行安全檢查



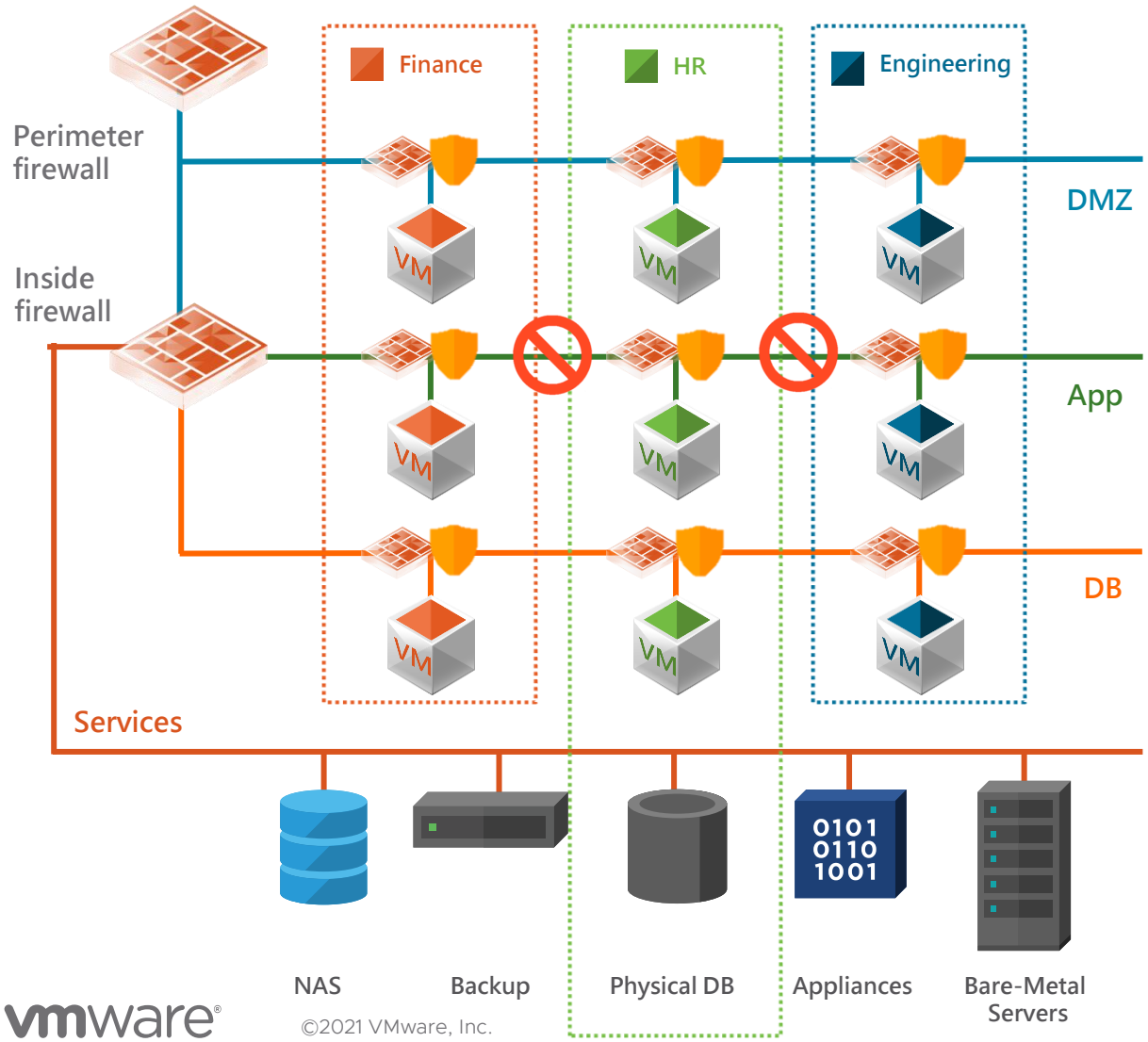
分散式架構，易於擴張，
可提供極大吞吐頻寬

不異動網路架構下，每個虛機 /
容器都可進行網路封包檢查

虛機移動時，安全政策
隨之移動且連線不中斷

©2021 VMware, Inc.

微分段機制應可與網路地址解構，建立業務相關之群組，並進行群組間防護

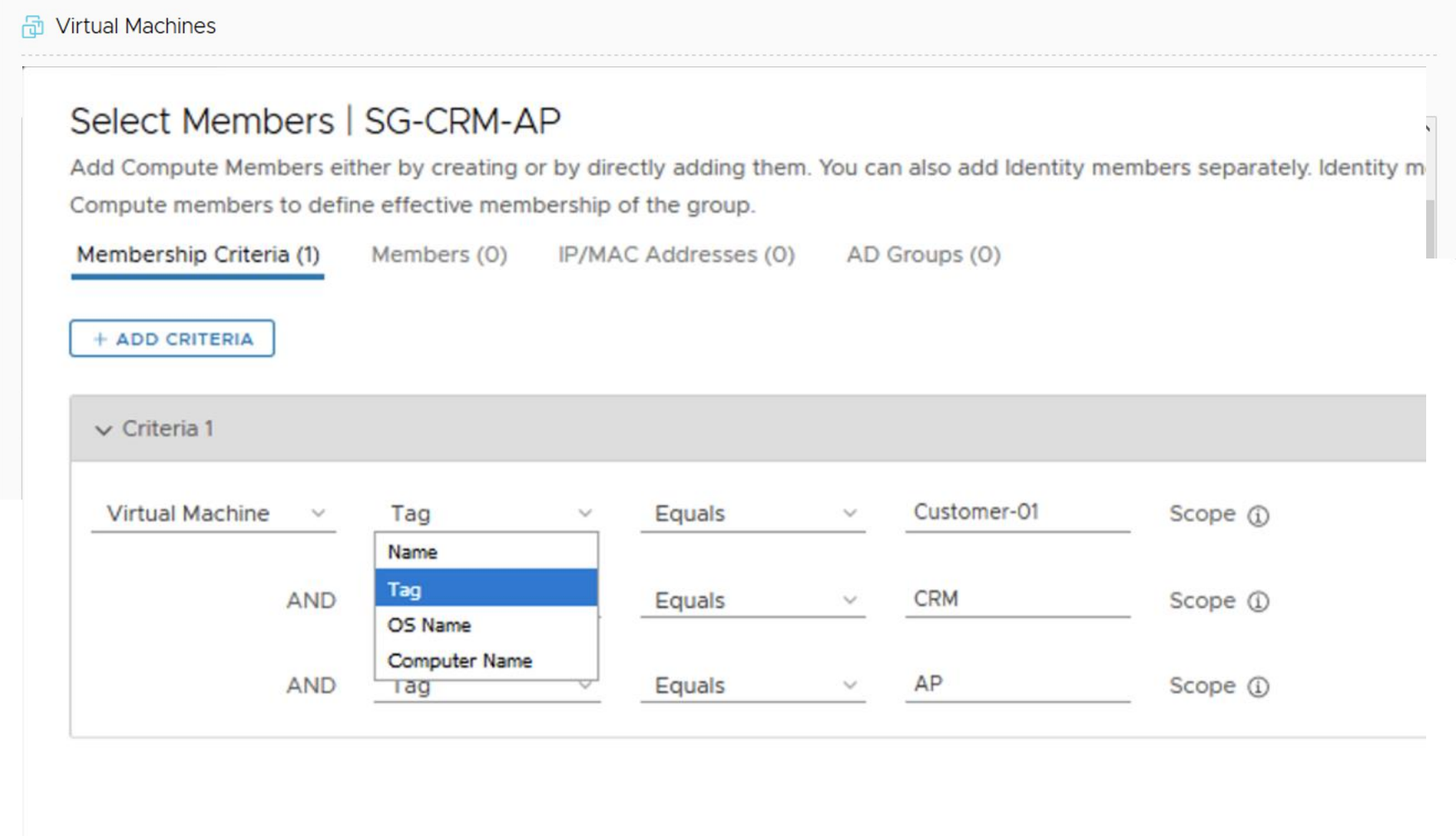


- 管理者可建立群組，直接進行指定資訊系統、特定業務、特定區域與企業組織間的安全防護機制
- 依據虛機或容器的特性（如標籤）進行動態到群組的配置
- 虛機或容器進行擴充 (Auto-Scaling) 與網路地址異動 (IP Re-addressing)時，無需變更安全防護政策

©2021 VMware, Inc.

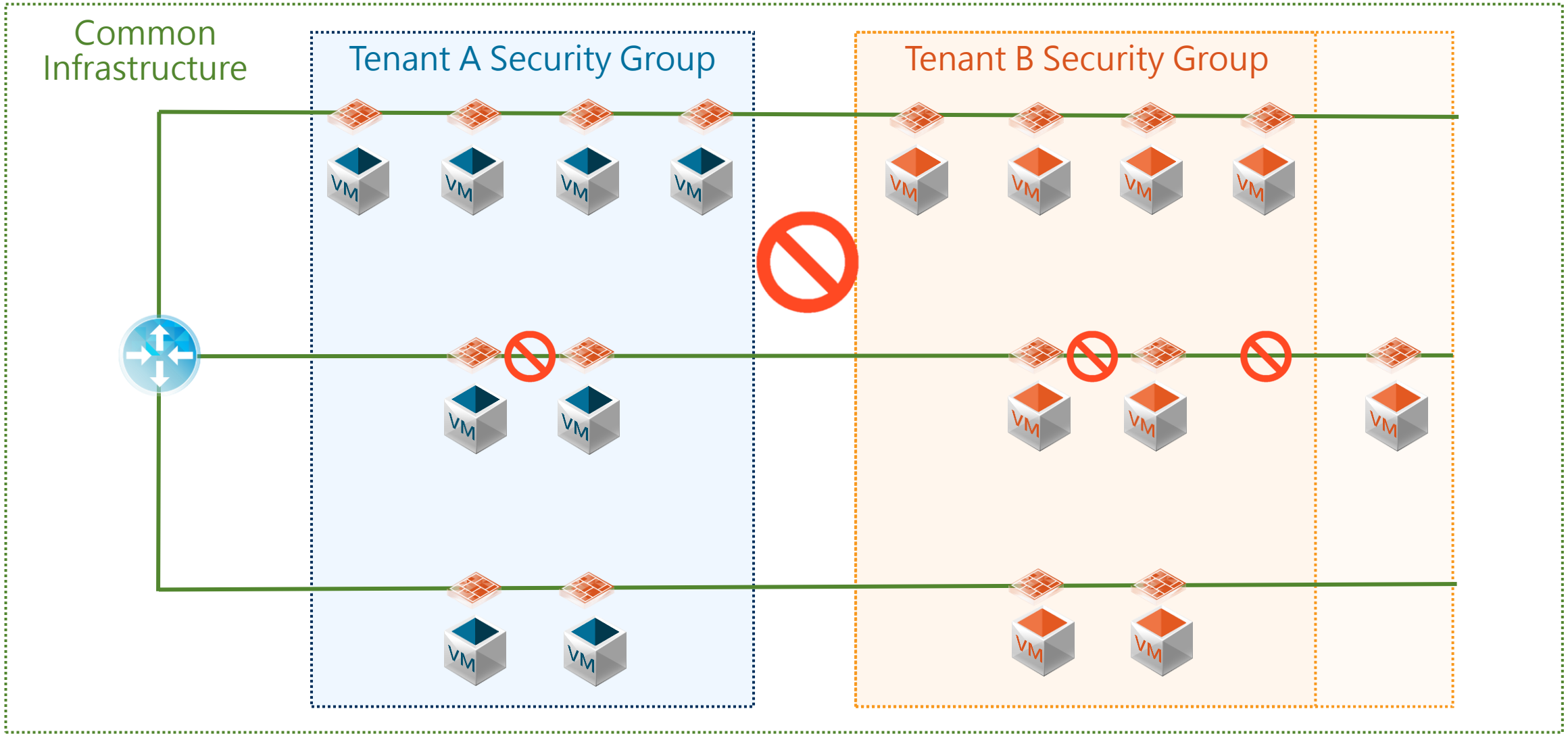
展示：基於群組的安全自動化

- 在 VMware NSX 內，可透過不同機制與資訊，進行群組配置：
- 容器或虛機的安全標籤
  - 雙層架構： Scope / Tag
- 虛機本身的資訊
  - 虛機名稱
  - 虛機作業系統
  - 虛機主機名稱
  - 對應的網卡以及 IP 地址



©2021 VMware, Inc.

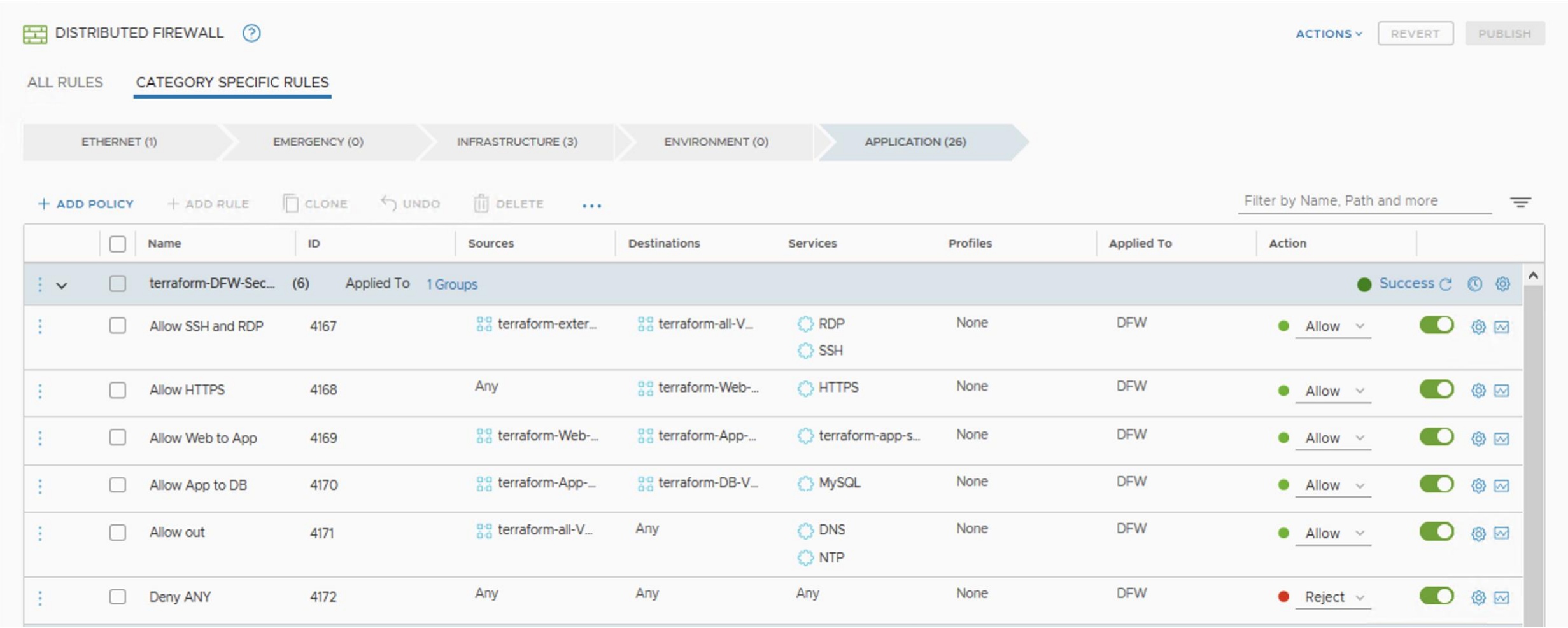
基於群組的自動化安全阻隔概念



©2021 VMware, Inc.

集中式的網路安全配置，支援基於群組的政策配置

- 統合管理、可基於動態群組配置、支援 L4~7 層服務，於虛機 / Pod 前直接提供防護的企業級防火牆



©2021 VMware, Inc.

微分段應能提供完整的資料中心網路防禦方案

達成在工作負載前的完整防護

減低攻擊平面：
提供工作負載由
L2 至 L7的防火牆保護

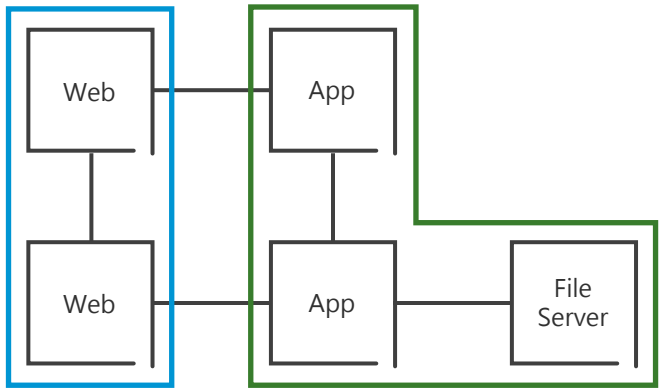
+

已知攻擊比對：
基於特徵值的 IDS/IPS 保護

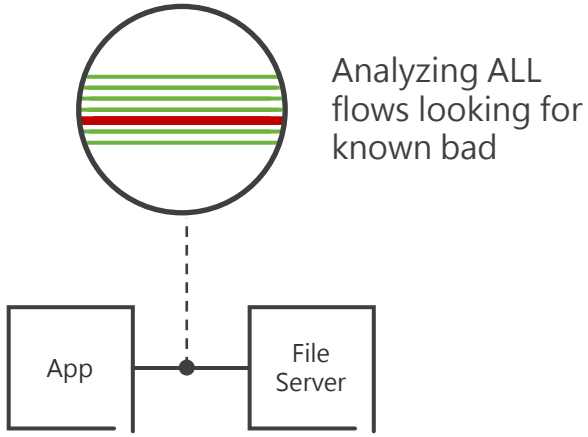
+

未知攻擊行為保護：
網路流分析、沙箱、新一代
NDR

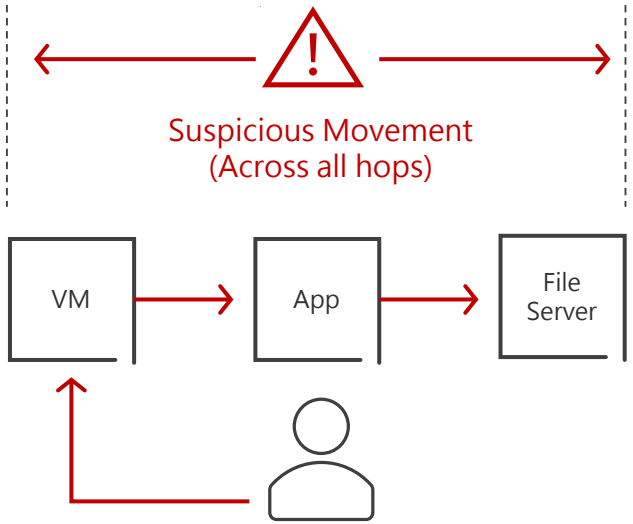
STEP 1



STEP 2



STEP 3



©2021 VMware, Inc.

整合分散式防火牆及 IDPS 功能，達成完善工作負載防護作業

在每個虛機前提供由底層到應用的完善安全防護

分散式防火牆

降低攻擊平面

客戶環境區塊阻隔

應用間阻隔

虛機 / 容器間微分段機制達成零信任架構

具狀態的 L2-L7 防火牆, FQDN 過濾, 身份識別防火牆

分散式 IDPS

防護攻擊由合法通道滲透

基於標準開放特徵值的防護

於每張網卡提供特徵值比對

支持告警及阻擋

基於 MITRE ATT&CK / CVE / CVSS 提供分類

每個網卡均取得保護

軟體定義

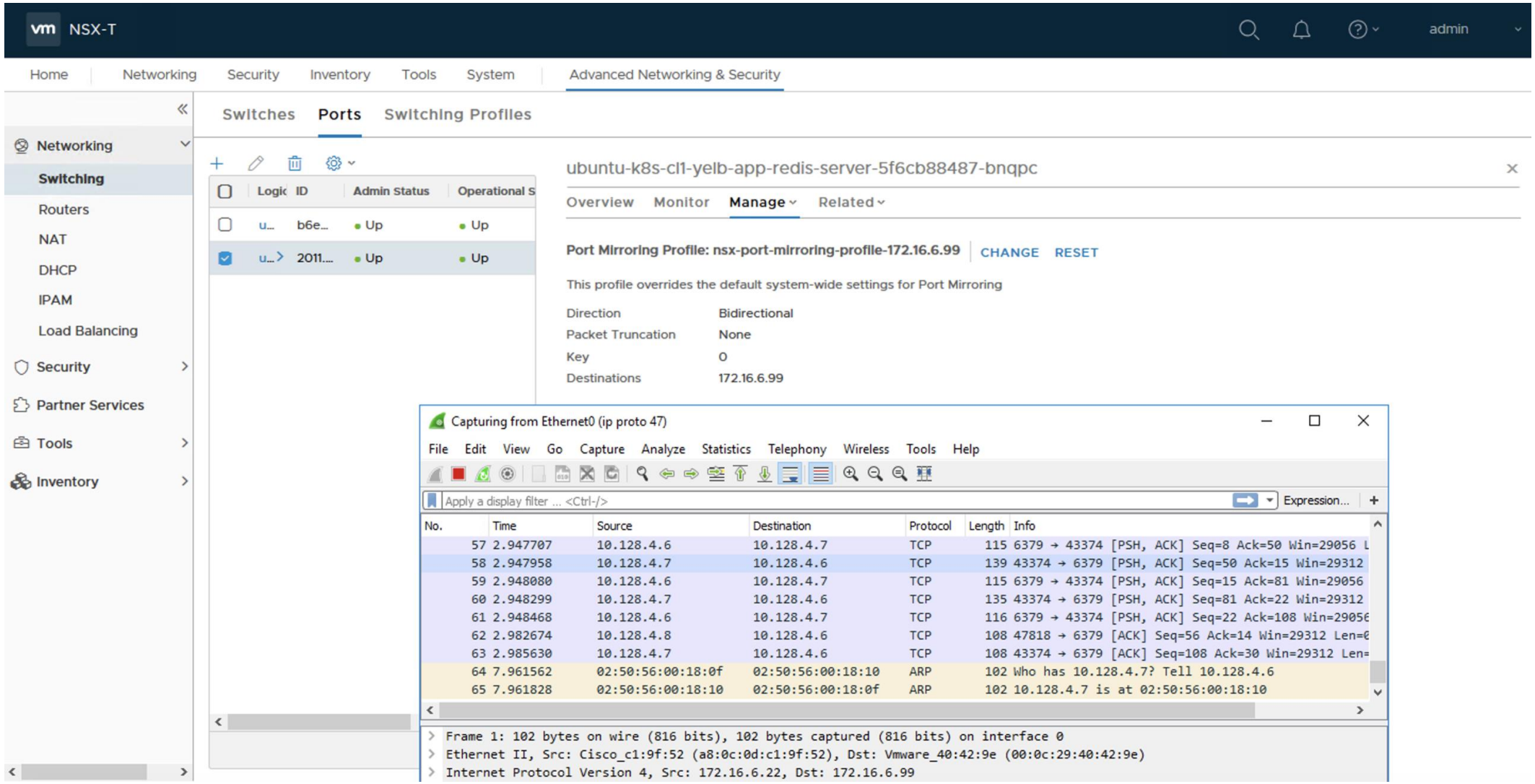
基於群組的管理

無需更動網路架構

分散式架構
易於橫向擴充

©2021 VMware, Inc.

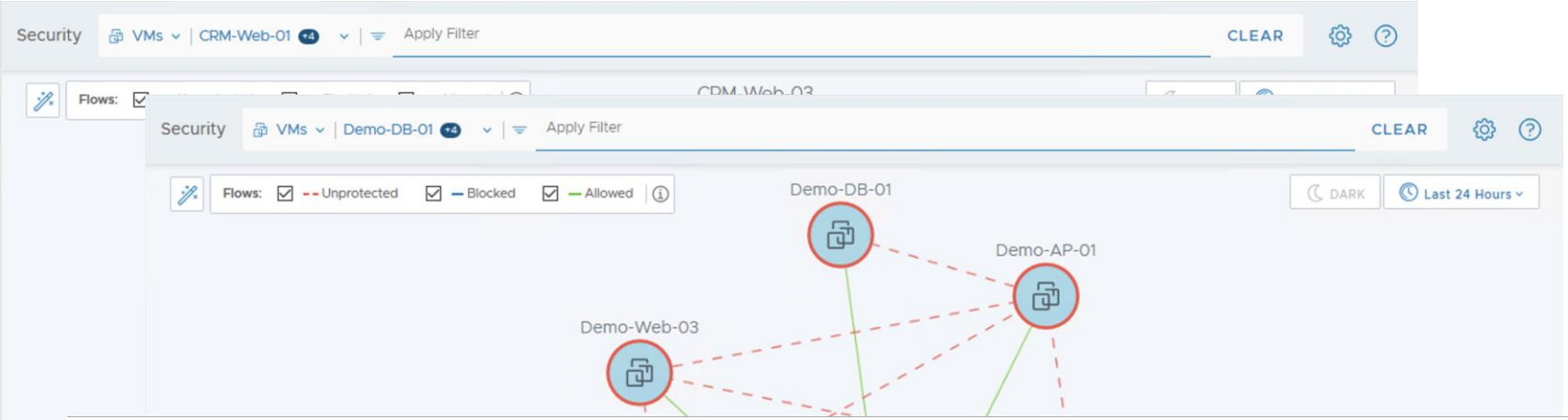
工作負載網路維運：進行虛機及容器的封包擷取



©2021 VMware, Inc.

工作負載網路維運：應用網路流收集及防火牆規則推薦

支援防火牆政策觀測及推薦



- 持續進行網路流檢視
- 可選定虛機 / 應用進行網路流分析，並直接進行防火牆政策派送（至東西向防火牆）

CRM-Application

Category: **Application** Recommended Rules: **4** Recommended Groups: **5** Recommended Services: **0**

Name	Sources	Destinations	Services	Profiles	Applied To	Action
Policy-1 (CRM-Application)		(4)				
Rule-1 (CRM-Application)	Group-1 (CRM-Applicati...	Group-2 (CRM-Applicati...	SSH	None	CRM-Application	Allow
Rule-2 (CRM-Application)	Any	Group-3 (CRM-Applicati...	HTTP	None	CRM-Application	Allow
Rule-3 (CRM-Application)	Group-4 (CRM-Applicati...	Group-5 (CRM-Applicati...	MySQL	None	CRM-Application	Allow
Rule-4 (CRM-Application)	Group-3 (CRM-Applicati...	Group-4 (CRM-Applicati...	Vmware-VC-WebAccess	None	CRM-Application	Allow

©2021 VMware, Inc.

結語：利用微分段方案，打造核心工作負載的完善網路安全防護

網路防護機制保護 每一台虛擬機與容器，所有網路流量都可以被防護與隔離

資安政策設定方式與業務直接連結，與網路地址解構，達成安全自動化

提供自下而上，完整的網路安全防護功能

可針對工作負載網路流進行記錄、監看、及安全防護建議

©2021 VMware, Inc.