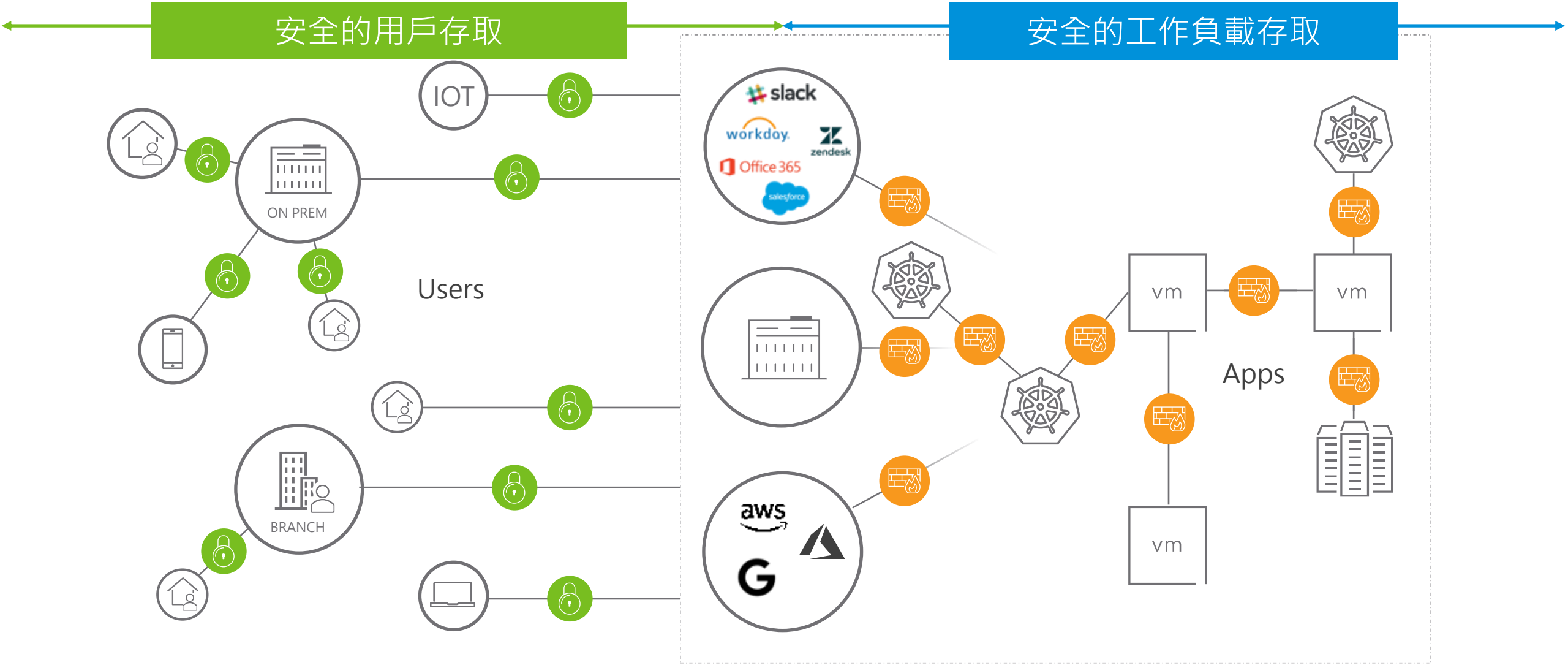
讓駭客很累的分散式防禦技法 – 以分散式防火牆搭配 NDR 建構資料中心零信任防護網

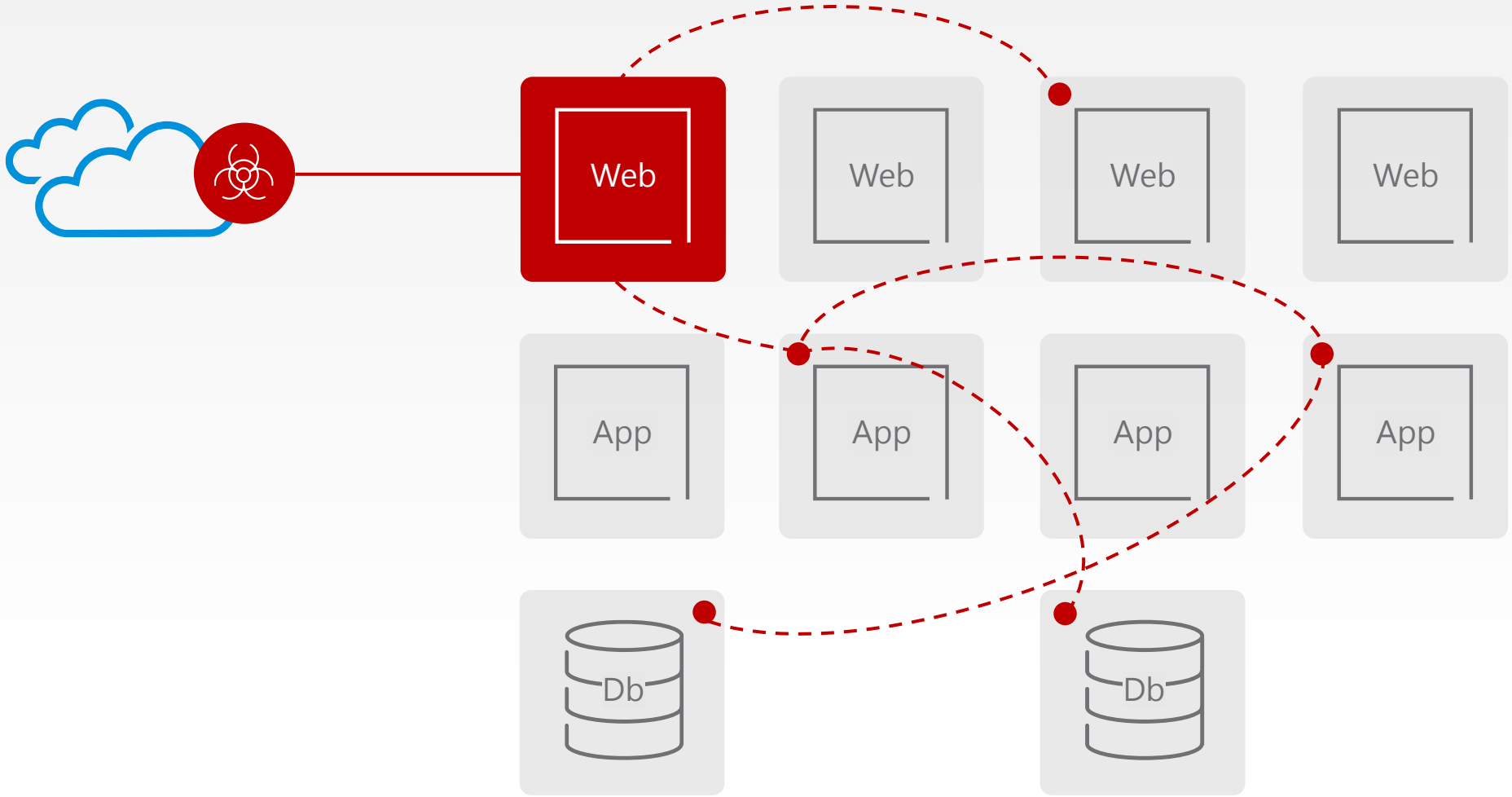
Colin Jao 饒康立
VMware 資深架構師

VMware Zero Trust Architecture 高層架構



資料中心零信任網路聯防六部曲

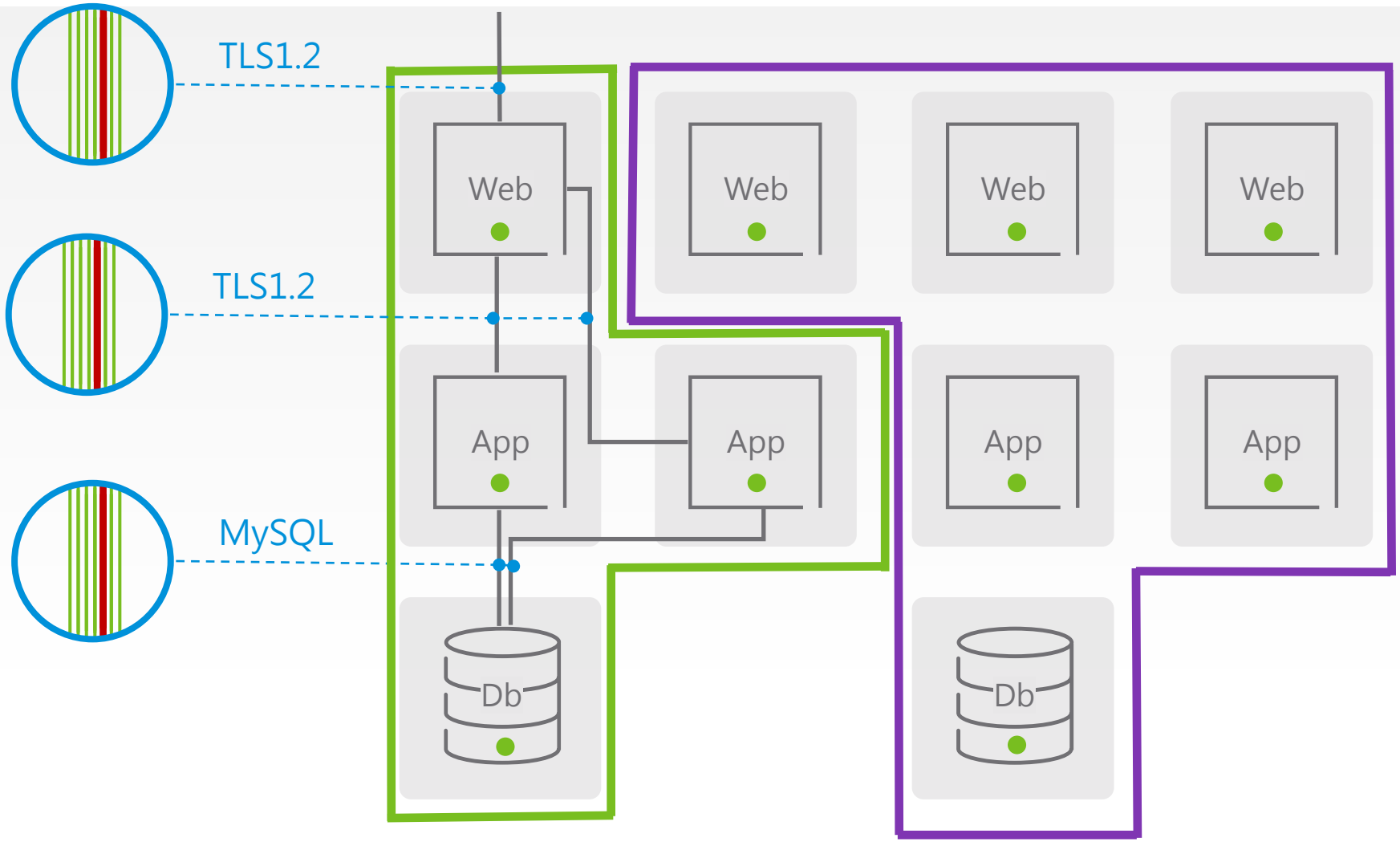
當駭客突破南北向安全機制進入雲平台內之後，如何進行偵測並防禦



一部曲：以微分段防火牆提供租戶、業務、機器阻隔

大幅降低可攻擊範圍，僅限制合法連線

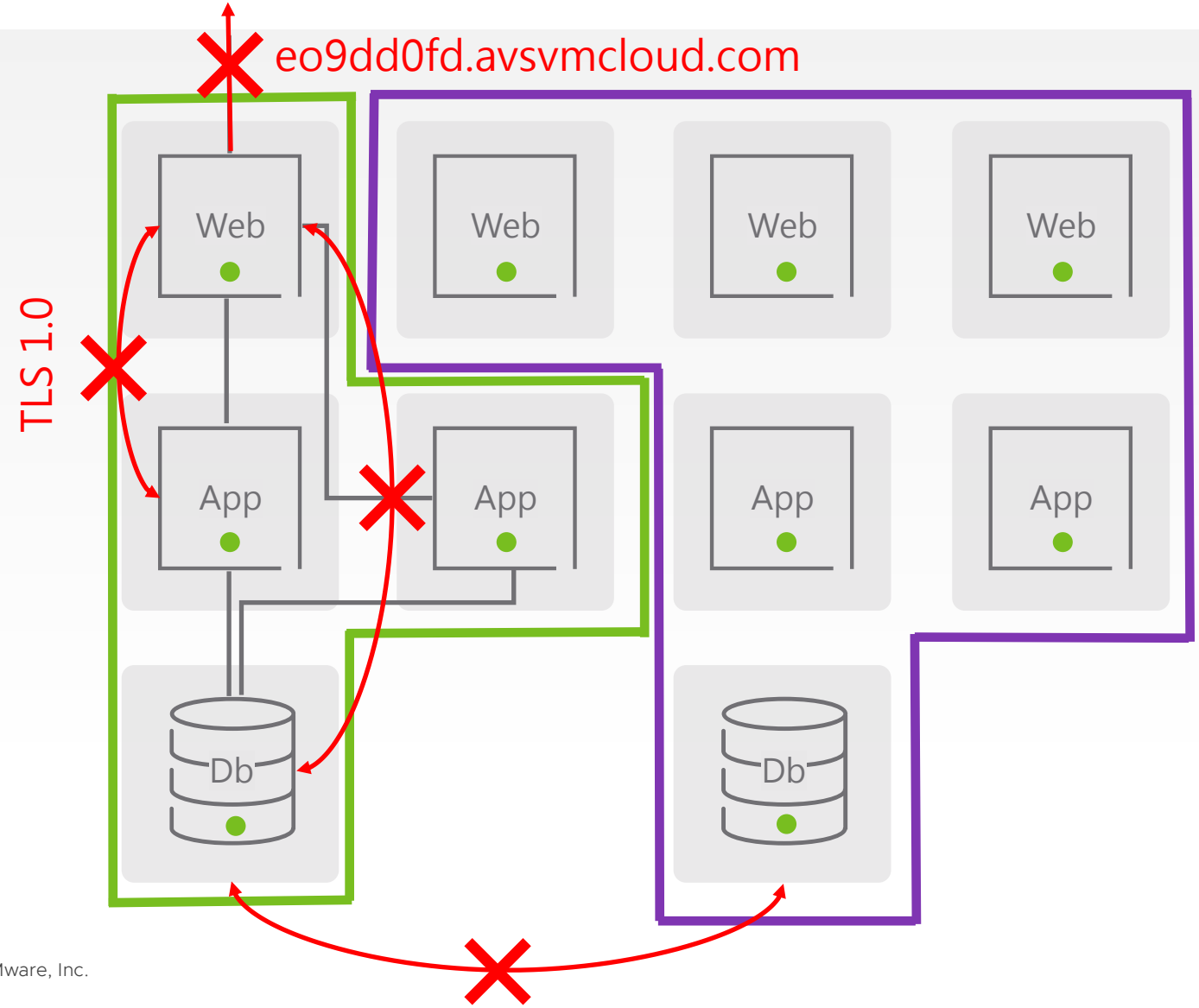
WAF
NDR
NTA
Malware Prevention
IDS/IPS
Segmentation



一部曲：以微分段防火牆提供租戶、業務、機器阻隔

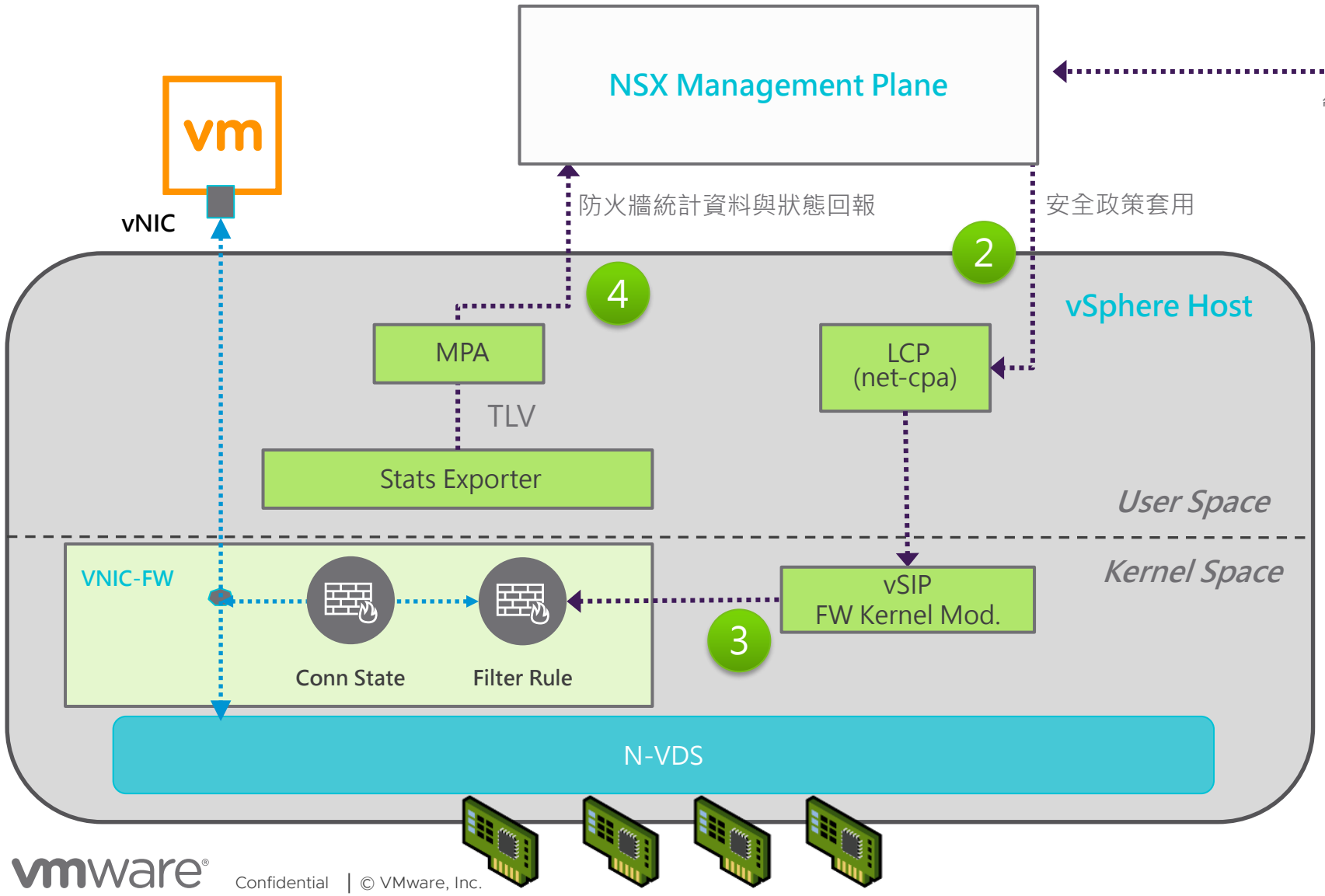
大幅降低可攻擊範圍，僅限制合法連線

WAF
NDR
NTA
Malware Prevention
IDS/IPS
Segmentation



NSX 微分段方案技術架構

直接於 vSphere 內保護每一台虛機，檢視所有網路流

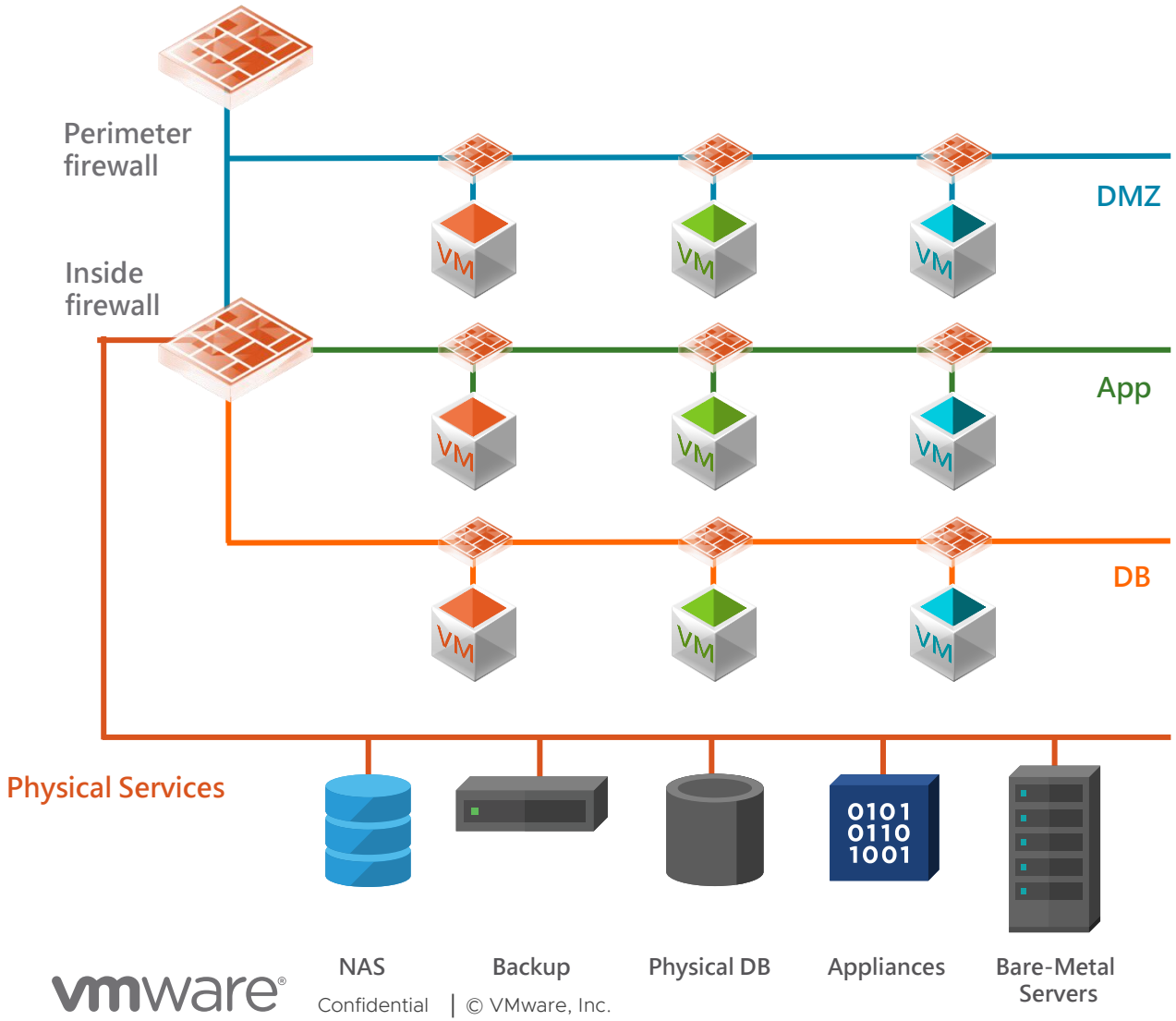


- VM 接在 NSX Logical Switch (Overlay or VLAN 均可) 上，即可受到微分段防護

控制層

資料層

NSX 微分段防火牆機制：
在 vSphere 上，每個虛機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 vSphere Host
- 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）
- 集中單一介面配置

微分段機制採用集中式的網路安全配置，並支援基於群組的政策配置

統合管理、支持 L2~L7，可基於動態群組配置、於虛機前直接提供防護的企業級防火牆

DISTRIBUTED FIREWALL

ACTIONS | REVERT | PUBLISH

ALL RULES | CATEGORY SPECIFIC RULES

ETHERNET (1) | EMERGENCY (0) | INFRASTRUCTURE (3) | ENVIRONMENT (0) | APPLICATION (26)

+ ADD POLICY | + ADD RULE | CLONE | UNDO | DELETE | ...

Filter by Name, Path and more

Name	ID	Sources	Destinations	Services	Profiles	Applied To	Action
terraform-DFW-Sec... (6)	Applied To 1 Groups						Success
Allow SSH and RDP	4167	terraform-exter...	terraform-all-V...	RDP SSH	None	DFW	Allow
Allow HTTPS	4168	Any	terraform-Web-...	HTTPS	None	DFW	Allow
Allow Web to App	4169	terraform-Web-...	terraform-App-...	terraform-app-s...	None	DFW	Allow
Allow App to DB	4170	terraform-App-...	terraform-DB-V...	MySQL	None	DFW	Allow
Allow out	4171	terraform-all-V...	Any	DNS NTP	None	DFW	Allow
Deny ANY	4172	Any	Any	Any	None	DFW	Reject

如同資安友商的產品，VMware NSX 防火牆功能已經取得 ICSA Labs / Common Criteria 認證

ICSA labs
An Independent Division of Verizon

TESTING SERVICES | CERTIF

VMware

vmware

VMware (NYSE: VM
delivers customer-pr
enable more flexible,
transition to cloud co
enabling more efficie

Visit http://www

Technology Program	Vendor	Product Testing Rep
Firewalls	VMware	NSX-T Data Center

National Information Assurance Partnership

Common Criteria Certificate

is awarded to

VMware

for

VMware NSX-T Data Center 3.1

Common Criteria

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 3.1) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Date Issued: 2022-07-22

Validation Report Number: CCEVS-VR-VID11217-2022

CCTL: Acumen Security

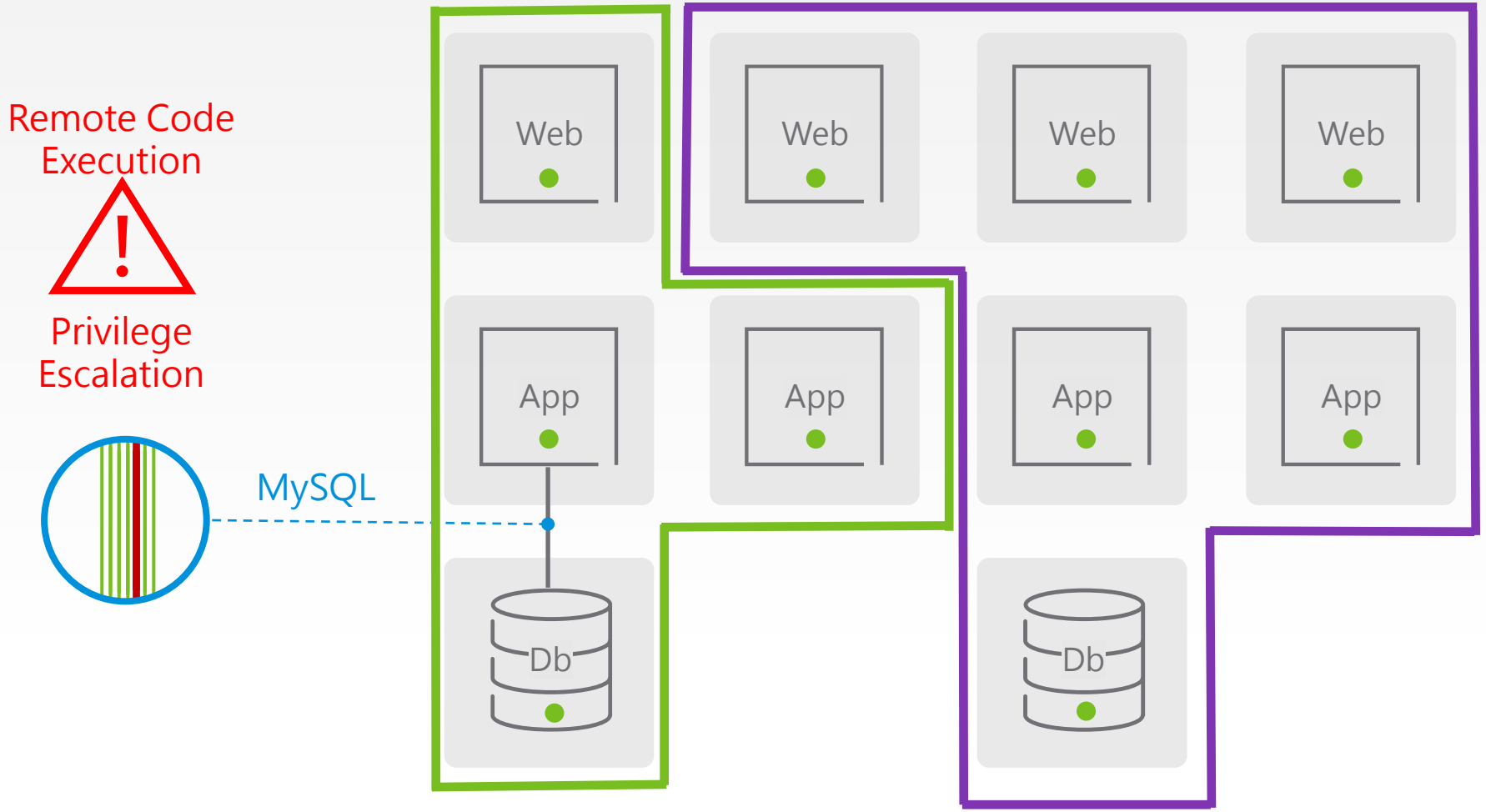
Assurance Level: PP Compliant

Protection Profile Identifier:
collaborative Protection Profile for Network Devices Version 2.2e

二部曲：以 IDPS 進行合法連線已知弱點防護

在系統尚未進行弱點修補前，提供弱點偵測以及網路層防禦阻擋

WAF
NDR
NTA
Malware Prevention
IDS/IPS
Segmentation



NSX Distributed IDPS 基於分散式架構，完整檢查每個網路流

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

租戶環境區塊阻隔

應用間阻隔

虛機間微分段機制達成零信任架構

具狀態的 L2-L7 防火牆、身份識別防火牆

分散式 IDPS

防護攻擊由合法通道滲透

基於開放特徵庫及 VMware Contexa 專家支持之防護

於每張網卡提供特徵值比對，提供告警及阻擋

完整攻擊稽核軌跡

基於 MITRE ATT&CK / CVE / CVSS 提供分類

每個網卡均取得保護

軟體定義

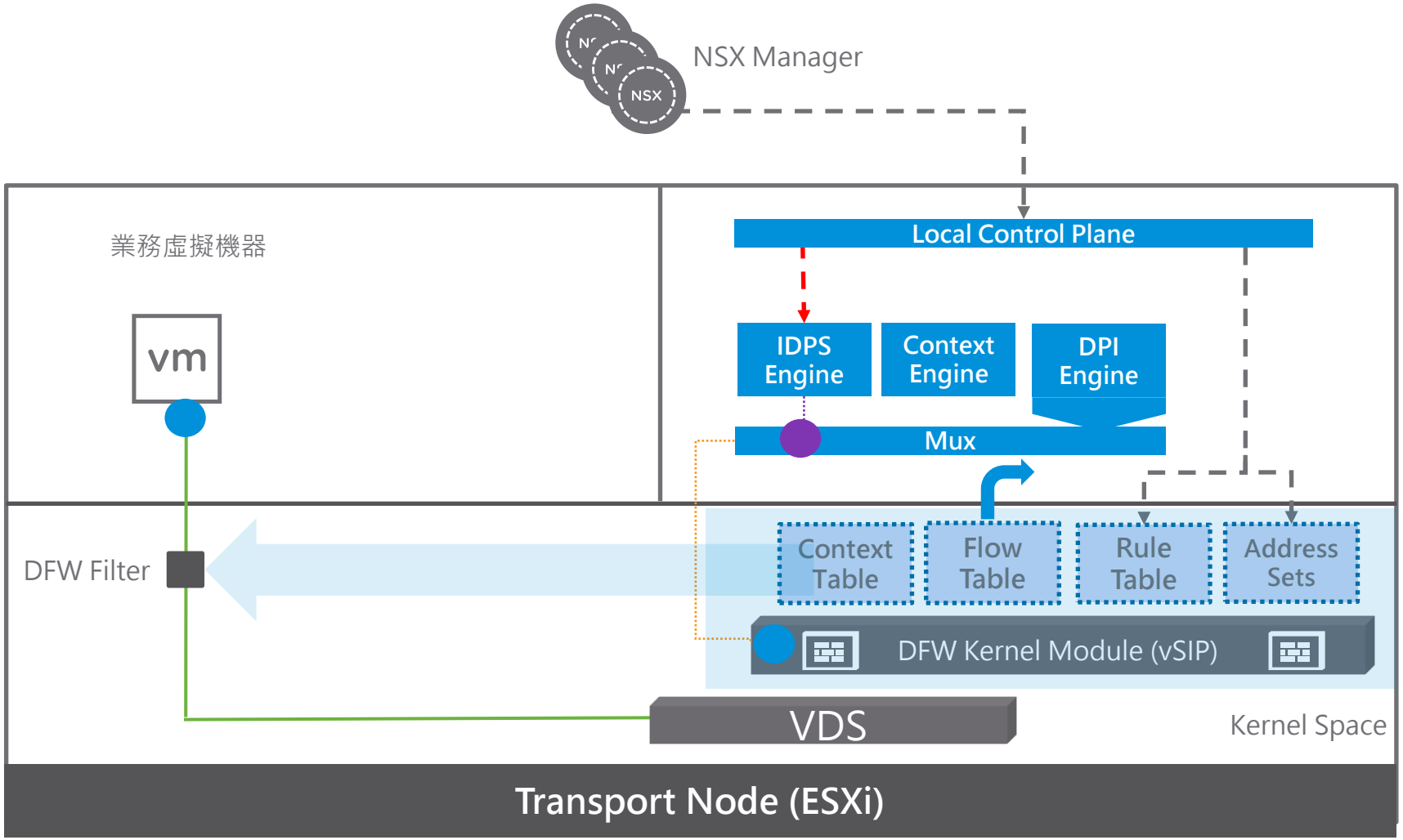
基於群組的管理

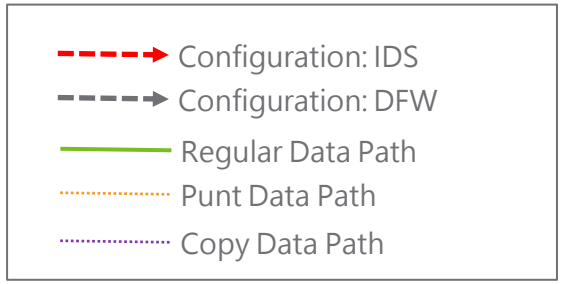
無需更動網路架構

分散式架構
易於橫向擴充

NSX 分散式 IDPS 技術架構

連線封包直接由 NSX Firewall 轉送給 IDPS 檢查

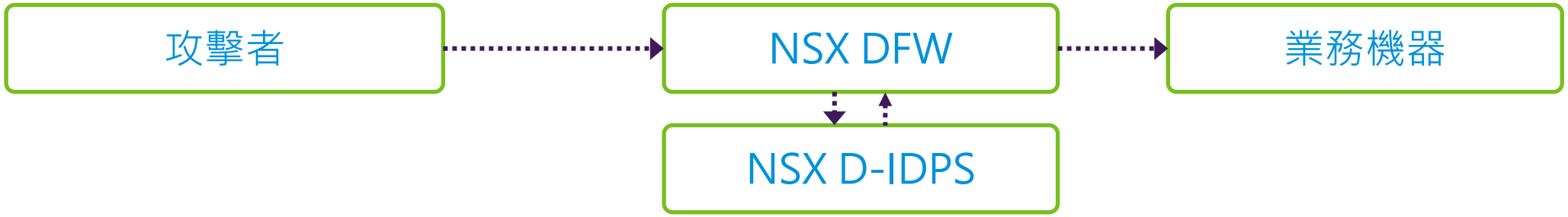




- 運作機制：封包由防火牆攔截後，於 vSphere 內送往 IDPS 引擎做特徵比對，並據以進行告警或阻擋
- 虛機需特別指定要啟用 IDPS 防護

IDPS 採用微分段防護架構討論

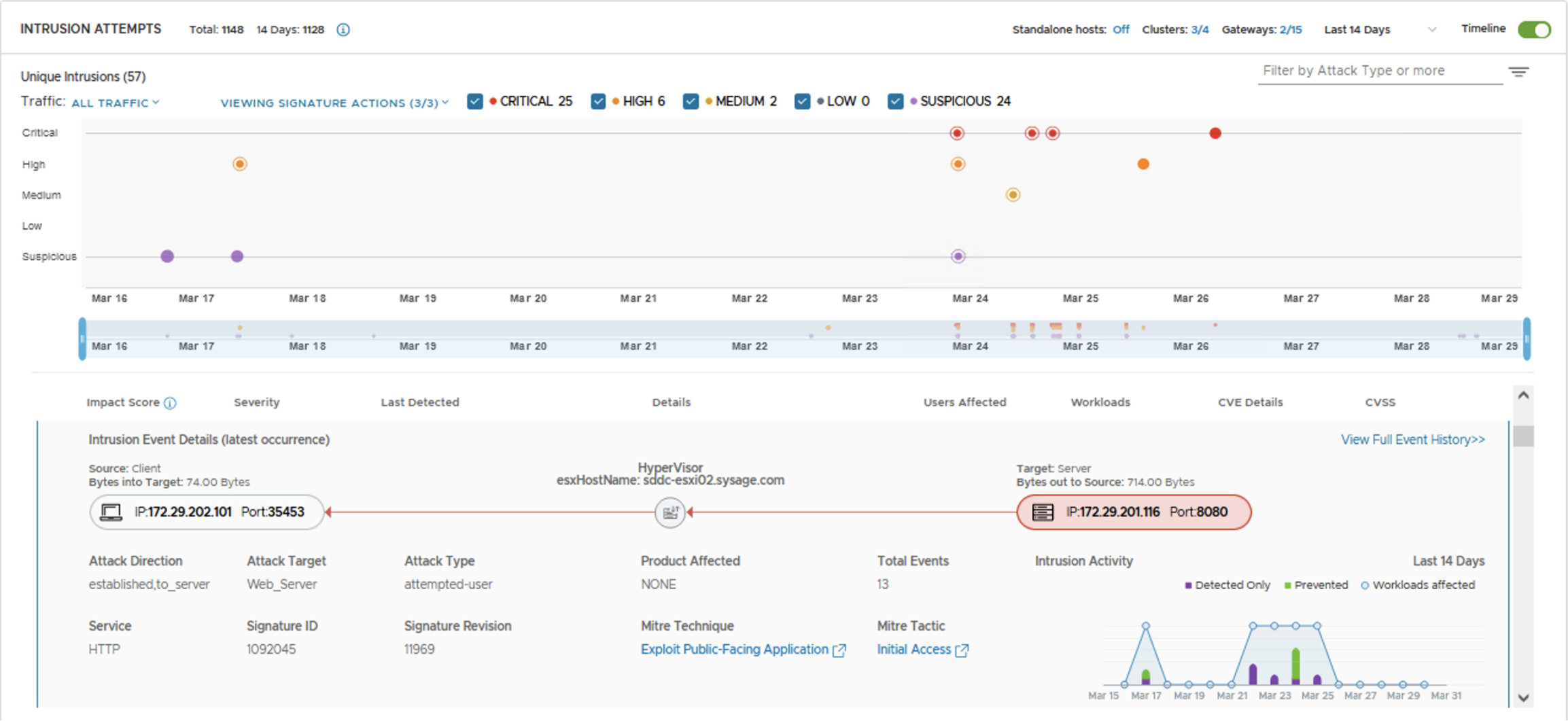
方案架構特性說明



- NSX DFW / IDPS 為虛機前 inline 運作
- 除非 NSX 管理者特別配置，否則每個業務虛機網路流量都會被檢查
- DFW - L2~L7 防護。預設啟用
  IDPS - 惡意攻擊行為特徵比對。手動啟用
- 無論用戶 / 攻擊者 / 檢測者與業務機器是在同網段、同台 vSphere，都無法避開 DFW / IDPS 防護機制

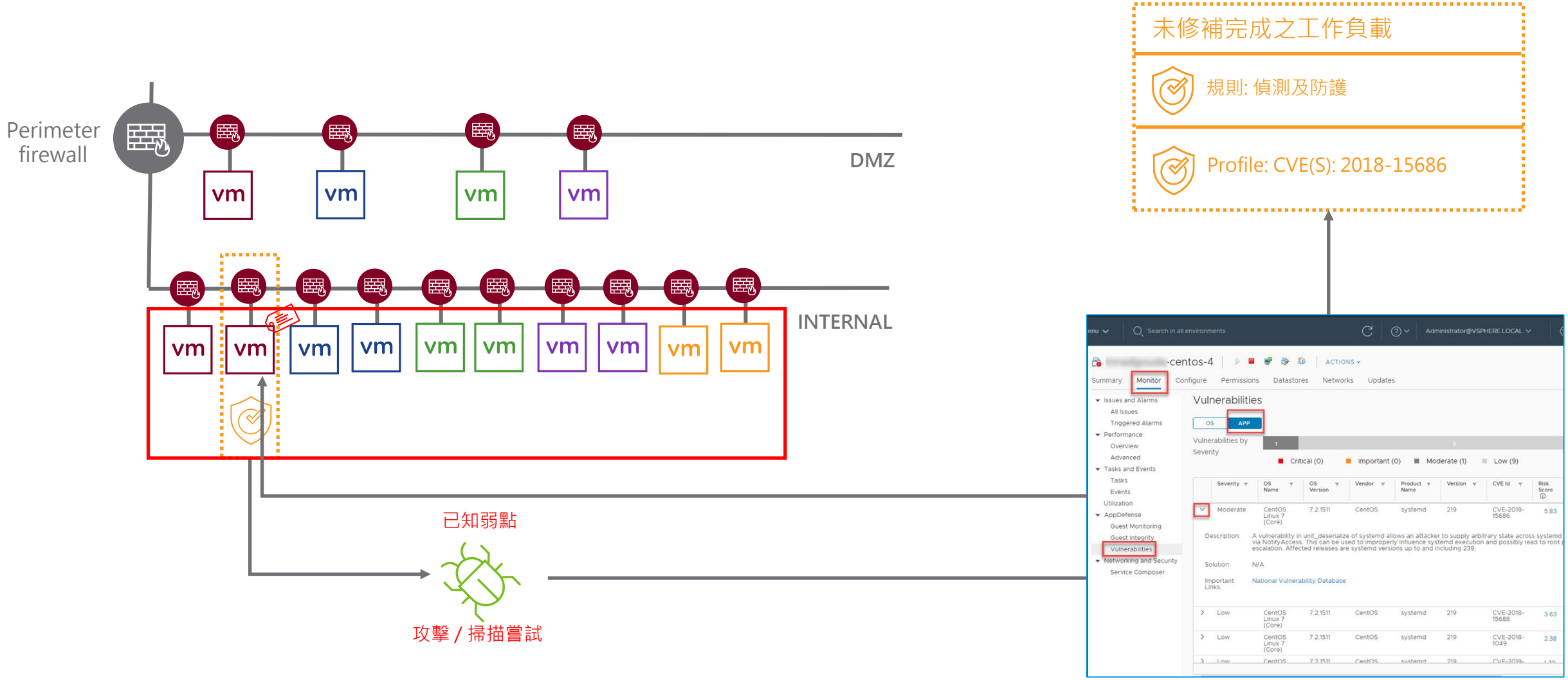
基於 NSX NDR 雲端分析資訊及開放安全特徵庫進行惡意行為比對

就已知惡意行為即時進行檢查及保護



NSX IDPS 可於核心工作負載無法馬上更新時提供 Virtual Patching

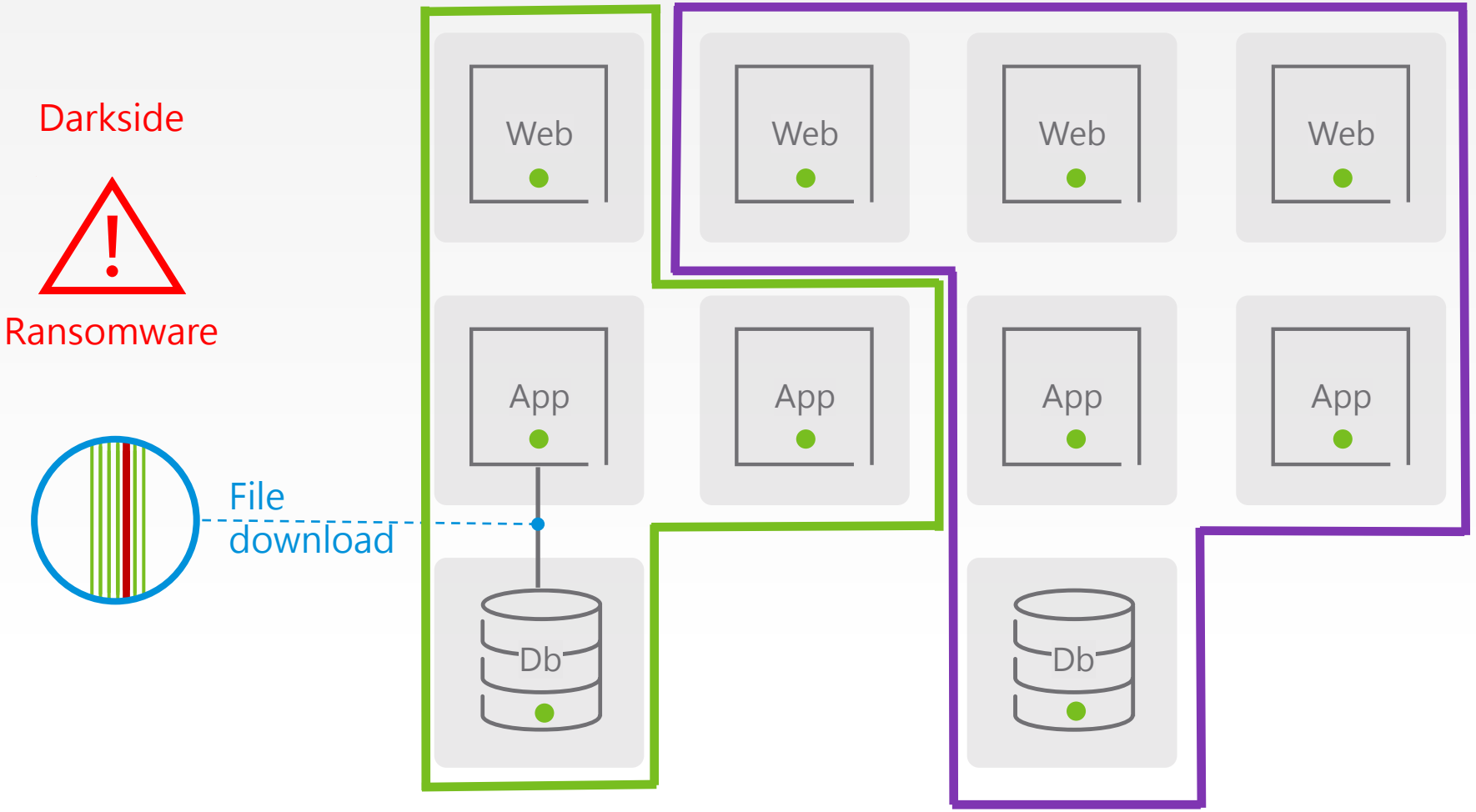
已知攻擊特徵檢視，及工作負載修補前之安全阻擋



三部曲：於系統及閘道端提供異常檔案分析

透過沙箱分析與檔案庫比對，針對異常檔案與附件下載進行保護

WAF
NDR
NTA
Malware Prevention
IDS/IPS
Segmentation



NSX 雲端全系統模擬器沙箱可看到惡意程式的所有行為

針對未知的可疑檔案進行完整分析

可看到惡意程式的迴避掃描技術
- Read Running Processes

可看到鉅細靡遺的勒索軟體行為
- Read Multiple Files
- Write Files back to Disk
- Open Network Connection to Remote Site

行為似乎無害

針對下載之文件、執行檔、Script 代碼、媒體檔案進行 Hash 值比對

未知檔案送往雲端沙箱進行模擬

完整沙箱模擬可看到所有的惡意程式的CPU指令集

更為完整及準確的惡意程式行為偵測，繞過迴避技術

惡意程式分析範例 – 勒索軟體

客戶無意間下載勒索軟體，執行前於沙箱內分析

自動列舉關鍵的惡意行為

已知的勒索軟體

對應的ATT&CK技術手法

ANALYSIS OVERVIEW

Rows to display 25

SEVERITY	TYPE	DESCRIPTION	ATT&CK TACTIC(S)	ATT&CK TECHNIQUE(S)
100	Signature	Identified ransomware code		
100	Family	Ransomware specific behavior	Impact	Data Destruction
60	File	Common ransomware extension usage	Impact	Data Destruction
50	File	Potential file encryption activity (Ransomware)	Impact	Data Destruction
45	Anomaly	AI detected possible malicious code reuse		
30	Stealth	Creating executables masquerading as browser clients	Defense Evasion	Masquerading
25	Autostart	Registering for autostart during Windows boot	Persistence	Registry Run Keys / Startup Folder
20	Steal	Reading browser cookies (Internet Explorer)	Credential Access	Credentials in Files
10	Packer	Confuser .Net Protector		
10	Execution	Ability to execute cryptographic operations		
5	File	Modifying executable in suspicious location of application data directory	Defense Evasion	Masquerading

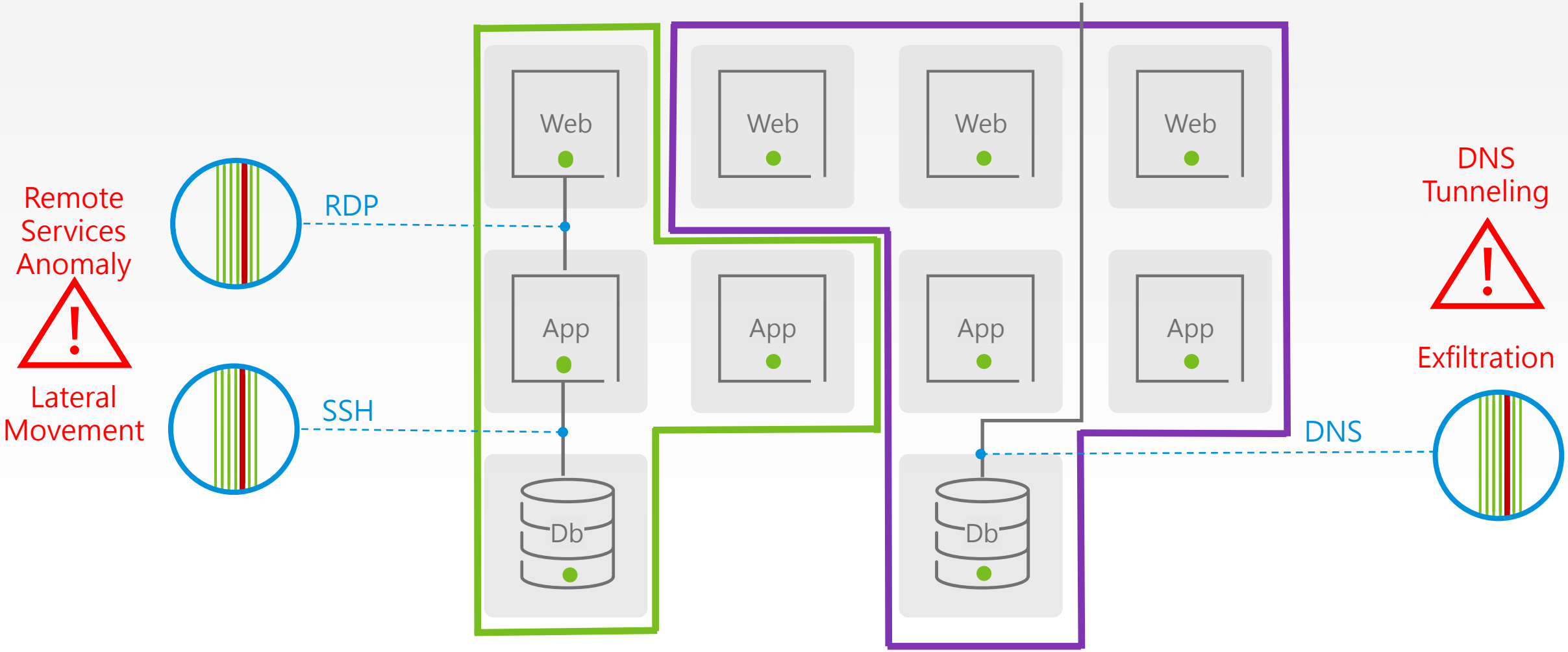
對應的ATT&CK戰略階段

嘗試隱匿

四部曲：對應未知的異常網路流分析

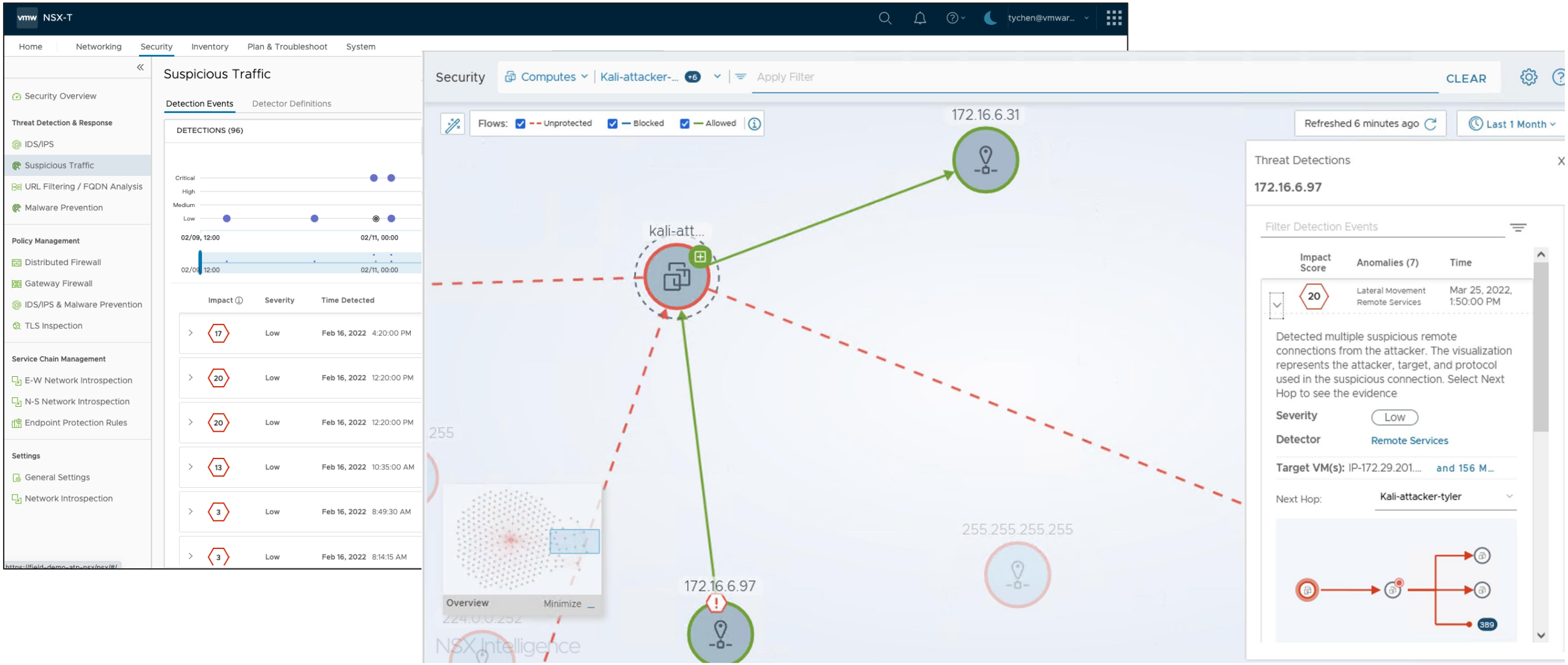
透過網路流數據收集、常態行為分析及雲端資料比對，找出異常之網路流

WAF
NDR
NTA
Malware Prevention
IDS/IPS
Segmentation



NTA所學習到的可疑行為

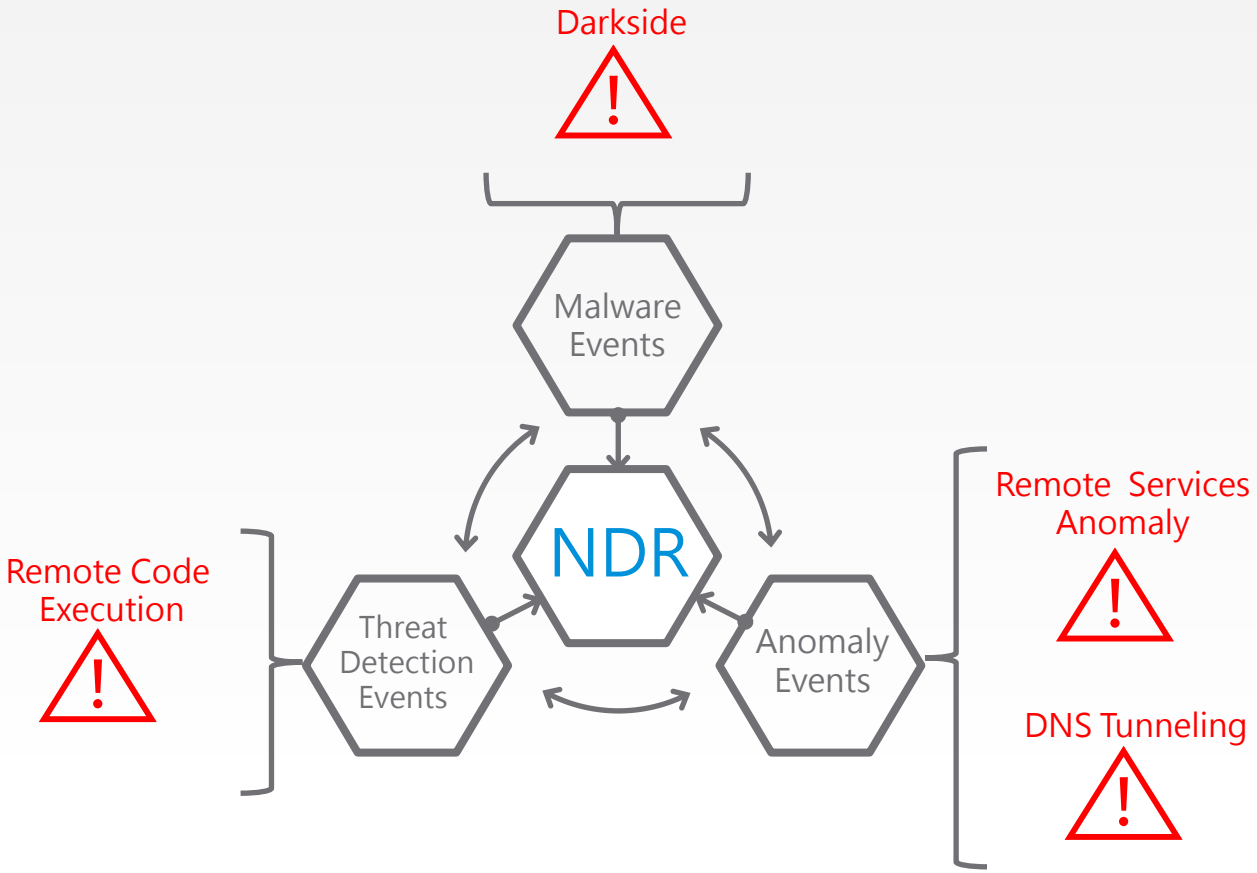
透過 Intelligence 收集到完整網路流資訊進行學習分析，針對異常行為提供告警

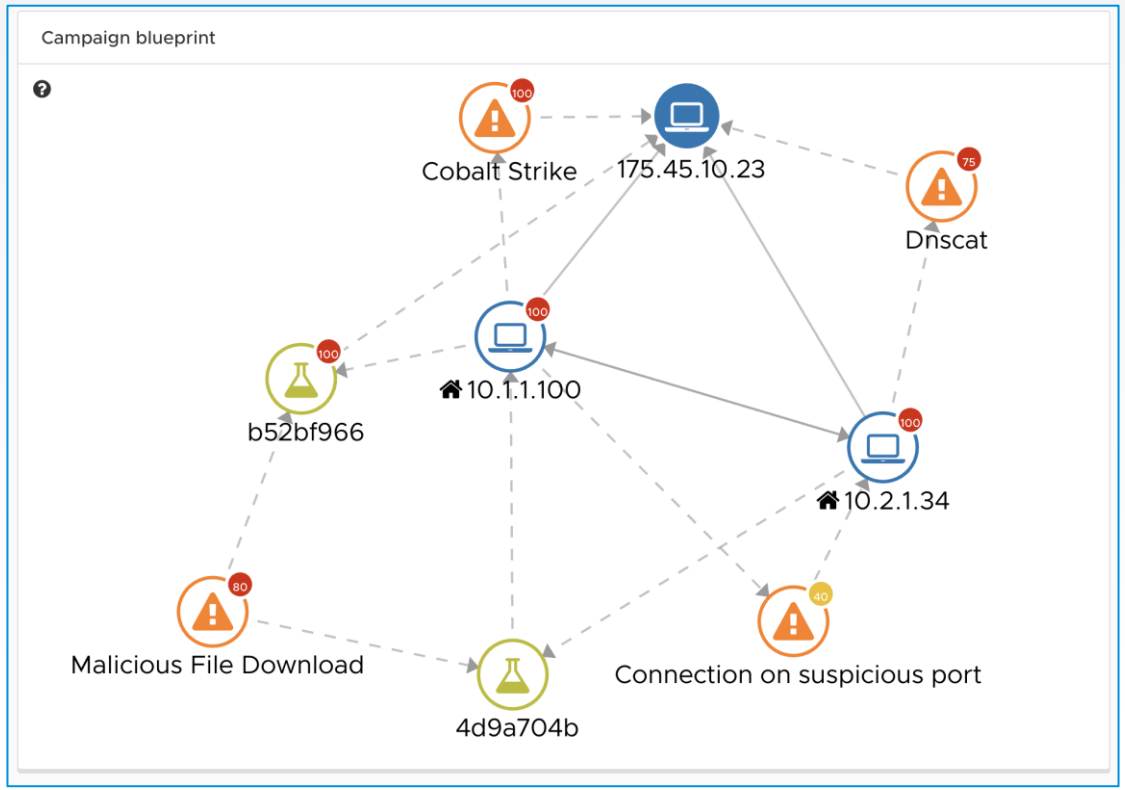


五部曲：提供完整攻擊軌跡

整合不同偵測手法及事件來源，還原攻擊軌跡

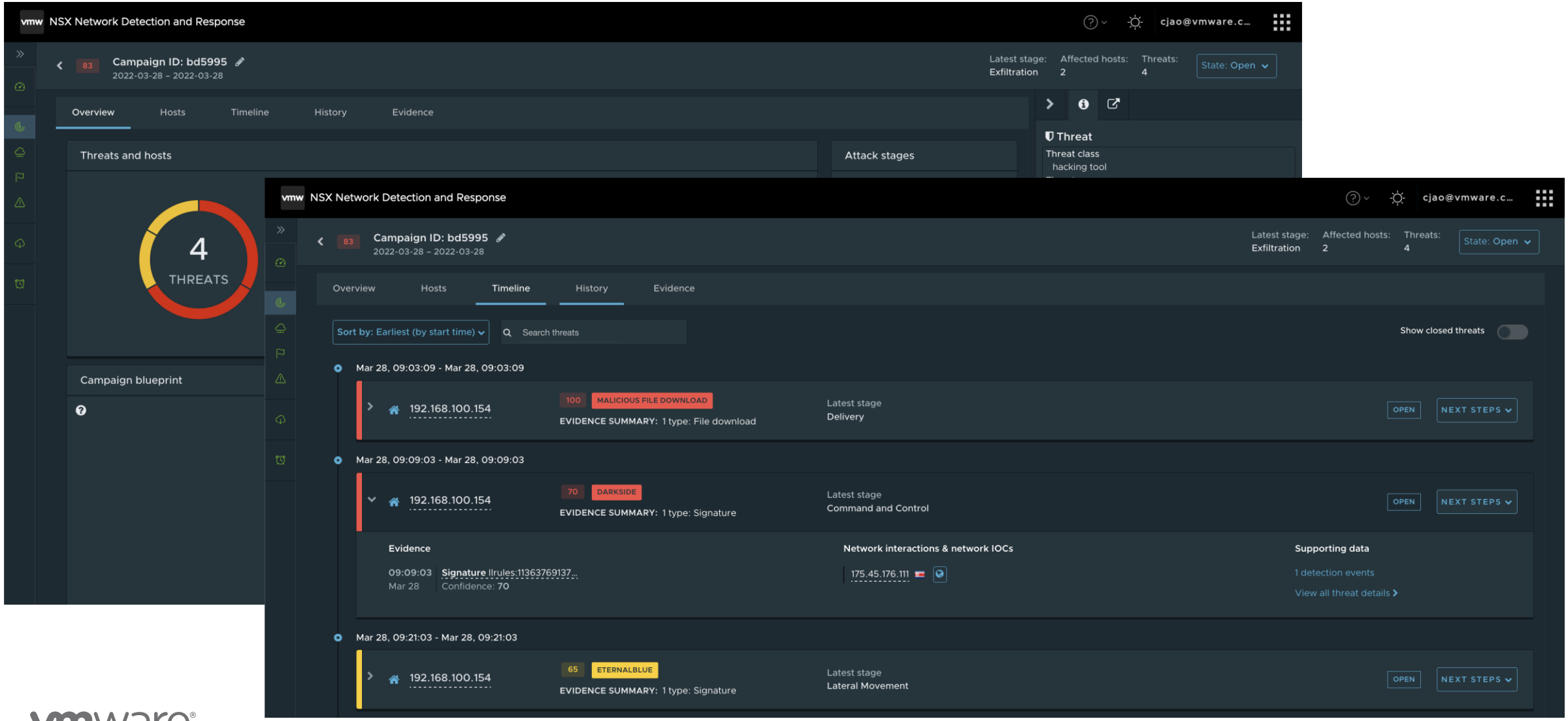
- WAF
- NDR
- NTA
- Malware Prevention
- IDS/IPS
- Segmentation





NSX NDR 以視覺化方式還原完整攻擊軌跡

並提供攻擊階段敘述及事件 Timeline ，協助客戶瞭解可能的威脅影響程度



NSX NDR 榮獲 SE Labs 評比為第一個 AAA 評價的NDR解決方案

SE Labs
INTELLIGENCE-LED TESTING
BEST
Network Detection & Response
WINNER 2021

VMware

vmware®

SE Labs

SE Labs Breach Response Detection Test

VMware NSX Network Detection and Response

August 2021

RATINGS

SE Labs AAA Network Detection & Response AUGUST 2021

Total Rating	100%
Detection Accuracy	100%
Legitimate Accuracy	100%

LEGITIMATE ACCURACY

False Positives	0%

THREAT RESPONSE DETAILS

Threat	Target	Score	Overall Score
FIN7 & Carbanak		100%	100%
OilRig		100%	
APT3		100%	
APT29		100%	

This is a summary of the full test report available selabs.uk/vmware.

Detection scores represent the product's behaviour when encountering network-specific threat techniques.

SE Labs helps advance the effectiveness of computer security through innovative, detailed and intelligence-led testing, run with integrity. We support businesses that are researching, buying and deploying security solutions. We are able to test a wide range of products and services using cutting-edge testing methodologies that lead the security testing industry. SE Labs focusses on achieving detailed results, integrity in the testing process, useful threat intelligence and test innovation.

Licensed for republication by VMware, Inc

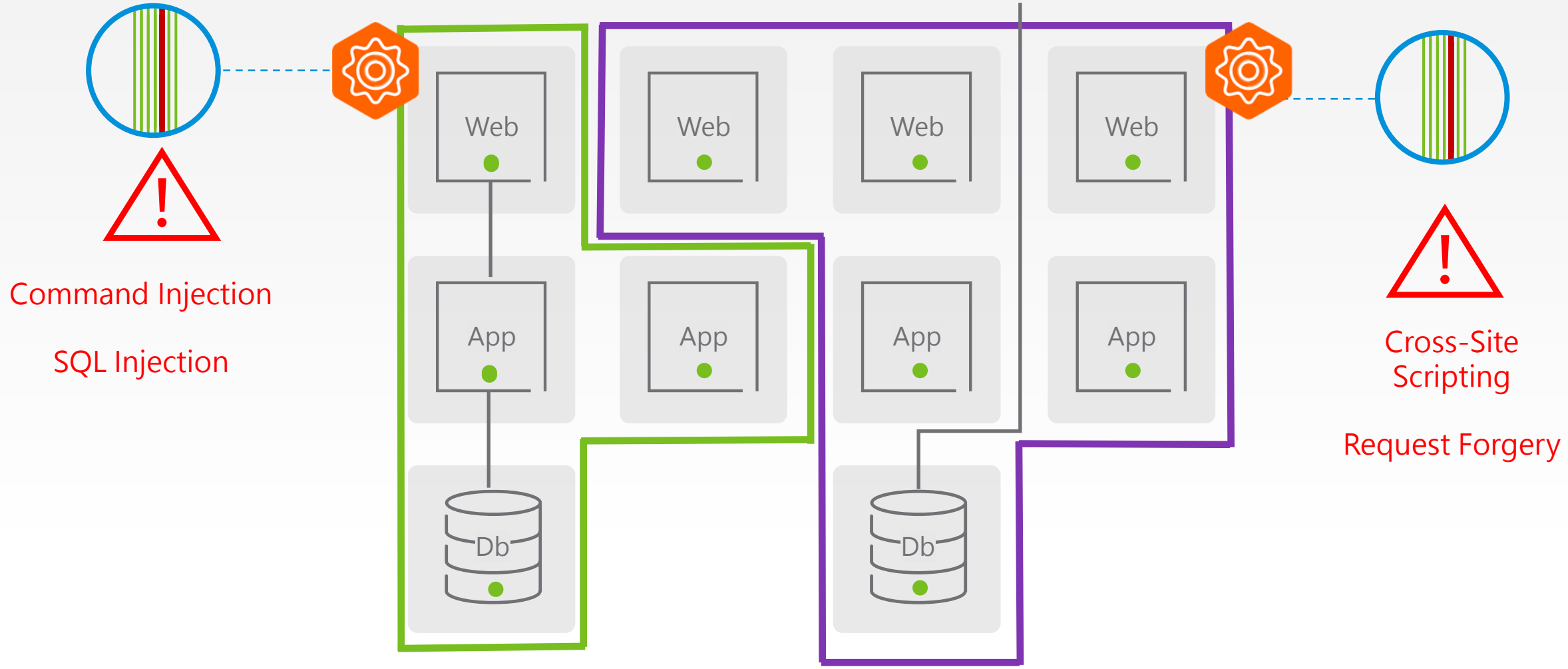
© 2021 SE Labs Ltd

https://blogs.vmware.com/networkvirtualization/2021/10/vmware-achieves-industry-first-aaa-rating-for-network-detection-response-from-se-labs.html/

六部曲：核心網頁應用防護

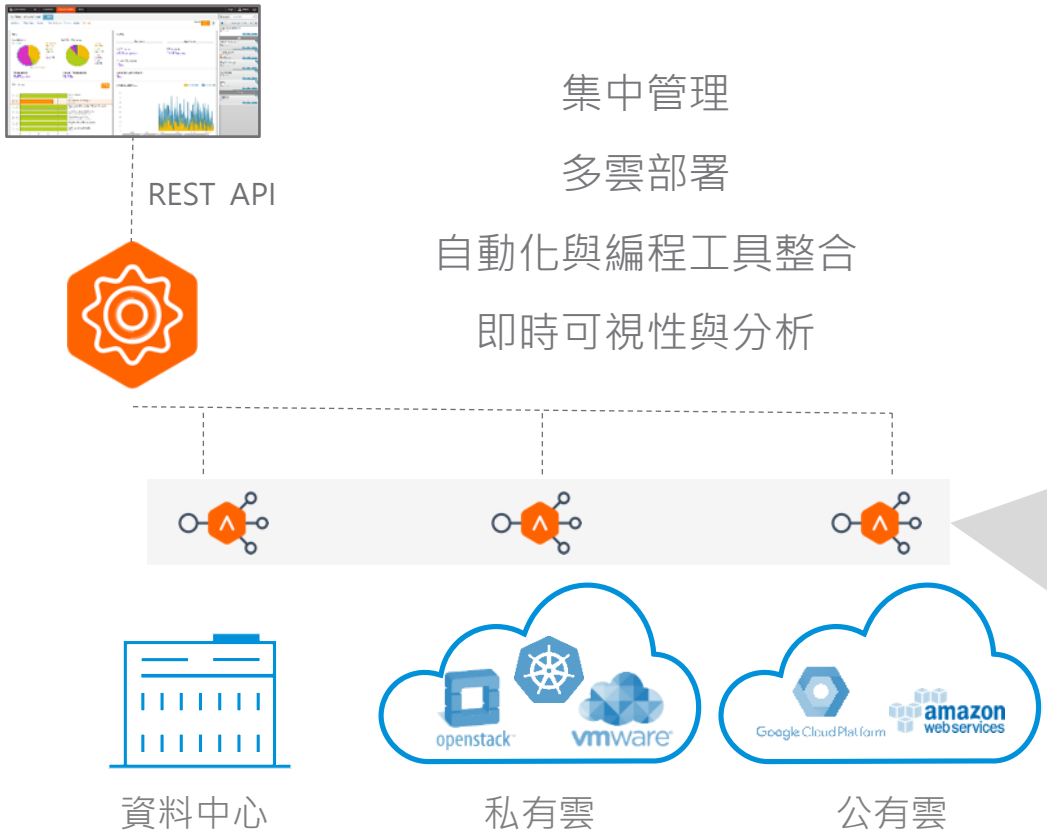
藉由 Web Application Firewall 機制進行核心業務前端保護

WAF
NDR
NTA
Malware Prevention
IDS/IPS
Segmentation



NSX ALB 安全防禦機制：應用安全及網頁應用防火牆

廣泛、多層的核心網頁前端安全防護機制



集中管理

多雲部署

自動化與編程工具整合

即時可視性與分析

網頁應用防火牆
OWASP TOP 10, Application protection, Attack Analytics

應用連線限制
Control and restrict by application or tenants

DDoS 防護
DDoS detection and mitigation with elastic scaling

基於 URL 的防火牆規則
Content (URI) based security rules

加密
SSL/TLS

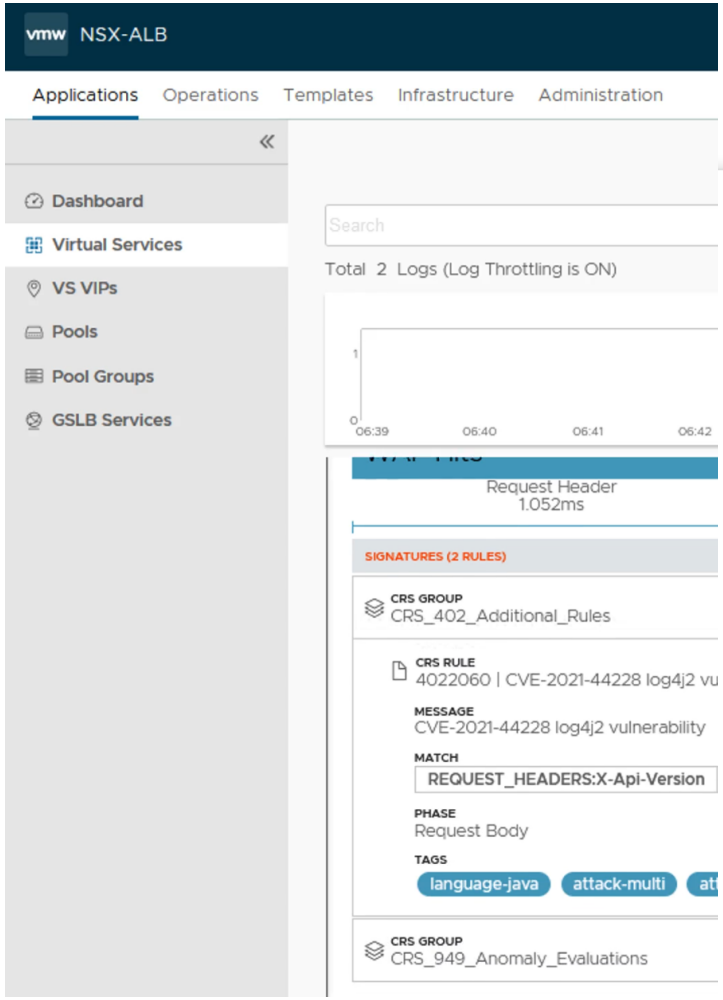
基於 IP/Port 的防火牆規則
IP-Port based Security Rules

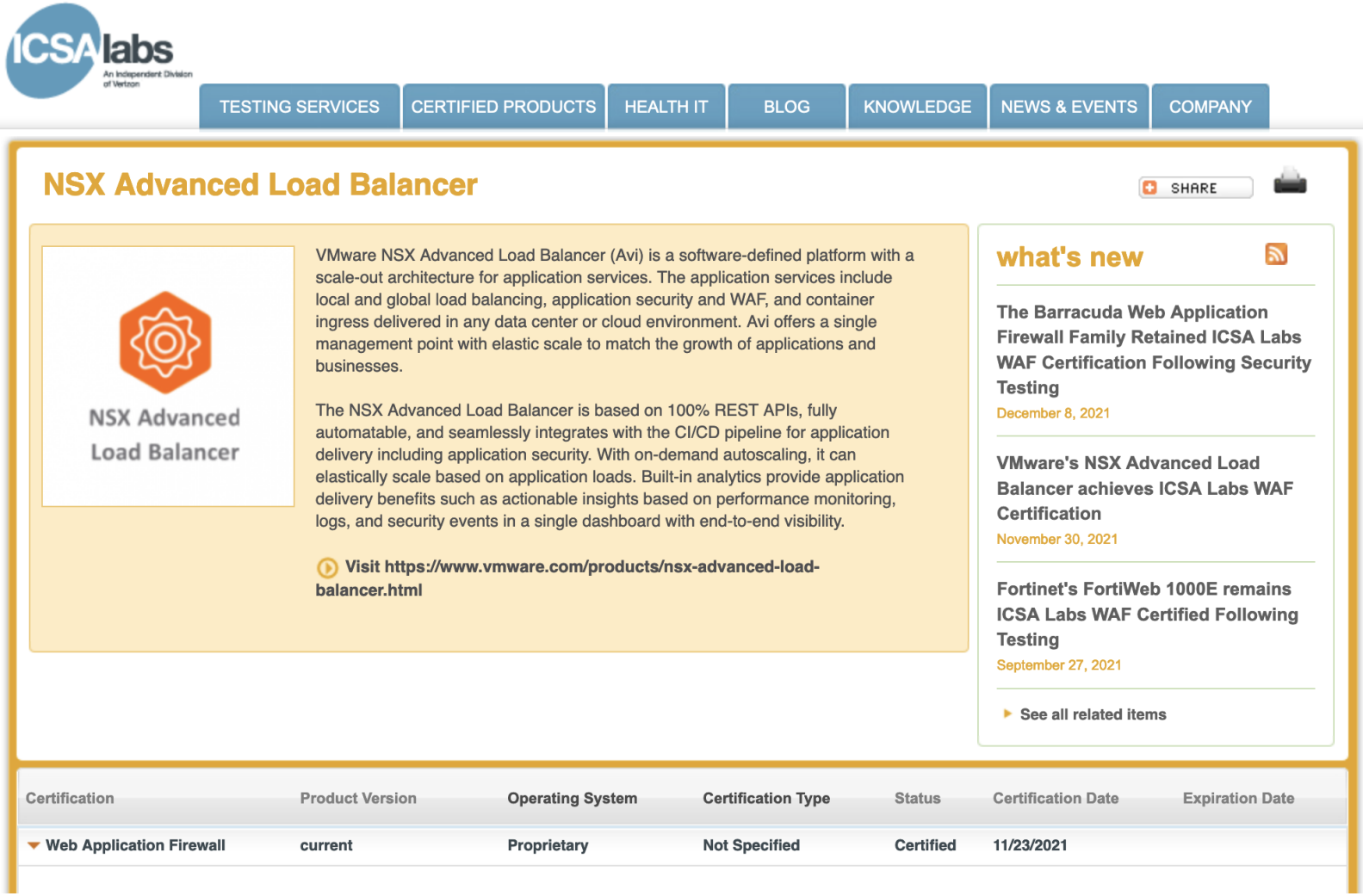
安全狀態檢視

Security score
Attack insights
SSL Insights
WAF analytics

企業等級並取得正式認證之網頁應用防護方案

針對包含 Log4j 在內，對應 OWASP 發布各種網頁攻擊手法防禦





VMware 網路防護技術完整對應 MITRE ATT&CK 戰術

實現零信任架構內的完整資料中心防護

MITRE ATT&CK Tactics （戰術）	Firewall 防火牆	WAF 網頁應用防火牆	NDR / NTA 網路偵測及回應	IDPS 入侵偵測及防護	Sandbox 沙箱暨惡意程式偵測
Initial Access 初始訪問	●	●		●	●
Execution 執行					●
Persistence 維持			●	●	●
Privilege Escalation 權限提升	●	●	●	●	●
Defense Evasion 防禦規避	●	●		●	●
Credential Access 權限訪問		●	●	●	●
Discovery 探索	●		●	●	●
Lateral Movement 橫向移動	●		●	●	●
Collection 收集			●	●	●
Command and Control 命令與控制			●	●	●
Exfiltration 滲透			●		
Impact 影響			●	●	●