容器與微服務資安風險全貌您看清了嗎?

從容器應用生命週期看安全風險與應對策略

蔡均璋 Diamond Tsai

VMware 資深技術顧問 蔡均璋

2022/9/20

vmware Confidential | © VMware, Inc.

"By 2025, more than 85% of global organizations will be running containerized applications in production, which is a significant increase from fewer than 35% in 2019.

GARTNER
"Best Practices for Running Containers and Kubernetes in Production," Published 4 August 2020

Confidential | ©2022 VMware, Inc.

現代化應用轉型帶來新的應用開發與作業模式

對安全性也無疑帶來巨大的改變

微服務架構

負載倍增

DevOps 維運文化

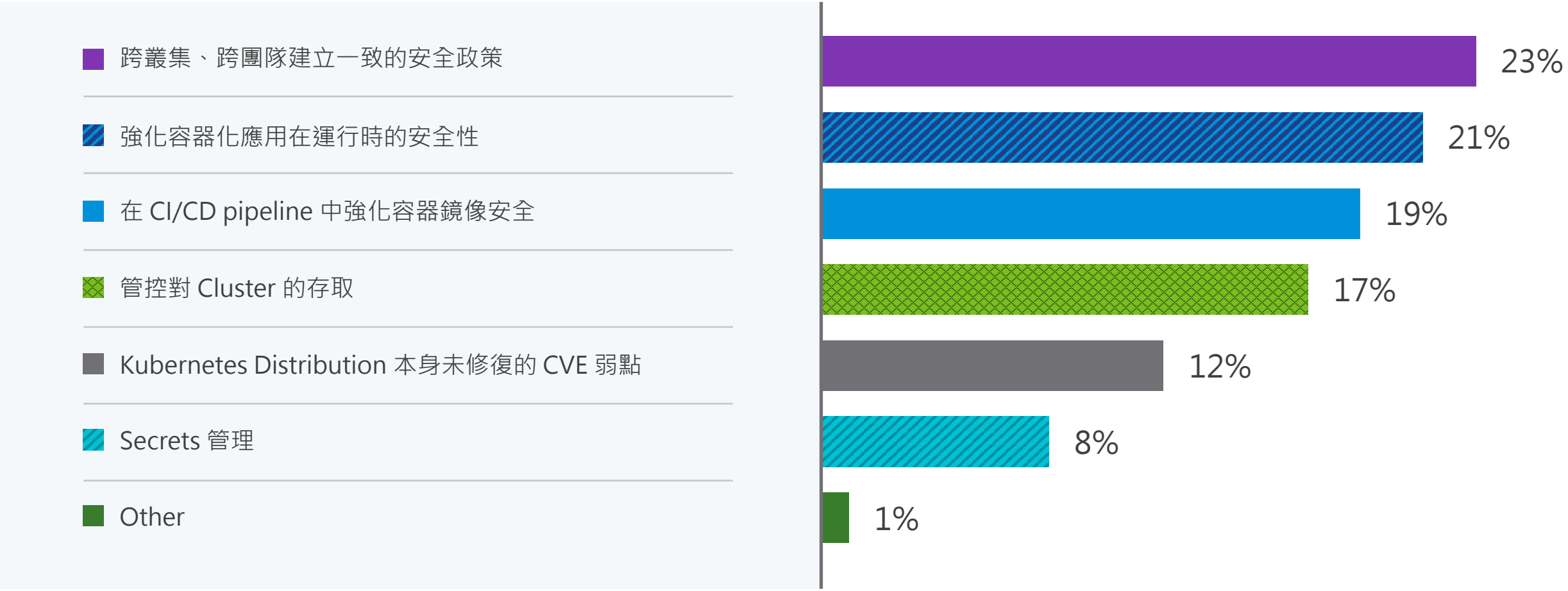
責任改變

持續交付

變動加速

©2022 VMware, Inc.

您對 Kubernetes 的最大安全考量是?



Source: The State of Kubernetes 2021

©2022 VMware, Inc.

從容器/雲原生應用 架構看應該思考的安全問題

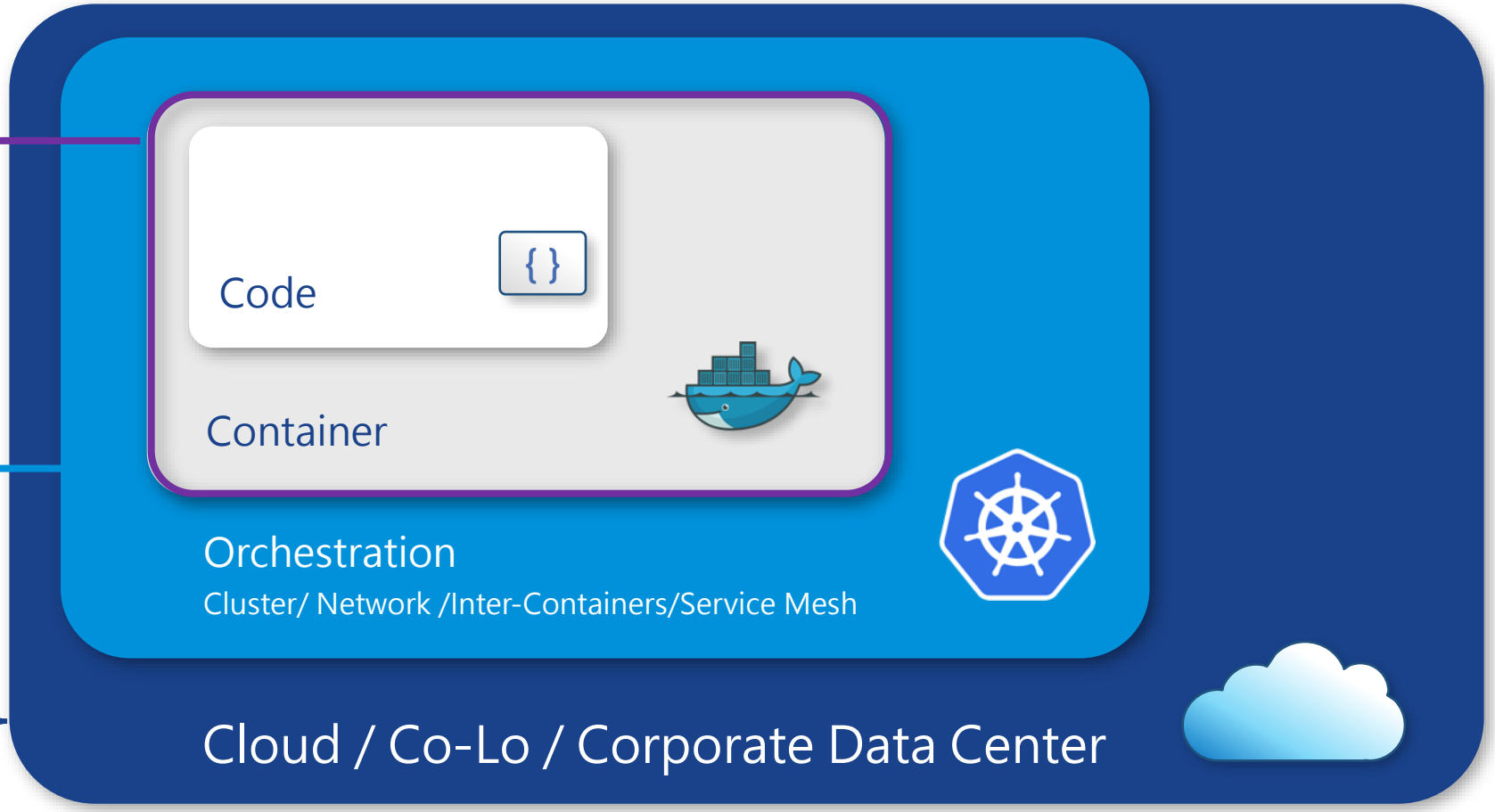
容器本身的安全風險：

- 程式弱點
- 容器鏡像相依組件/基底弱點
- 不明、有漏洞的鏡像誤用

容器運行風險：

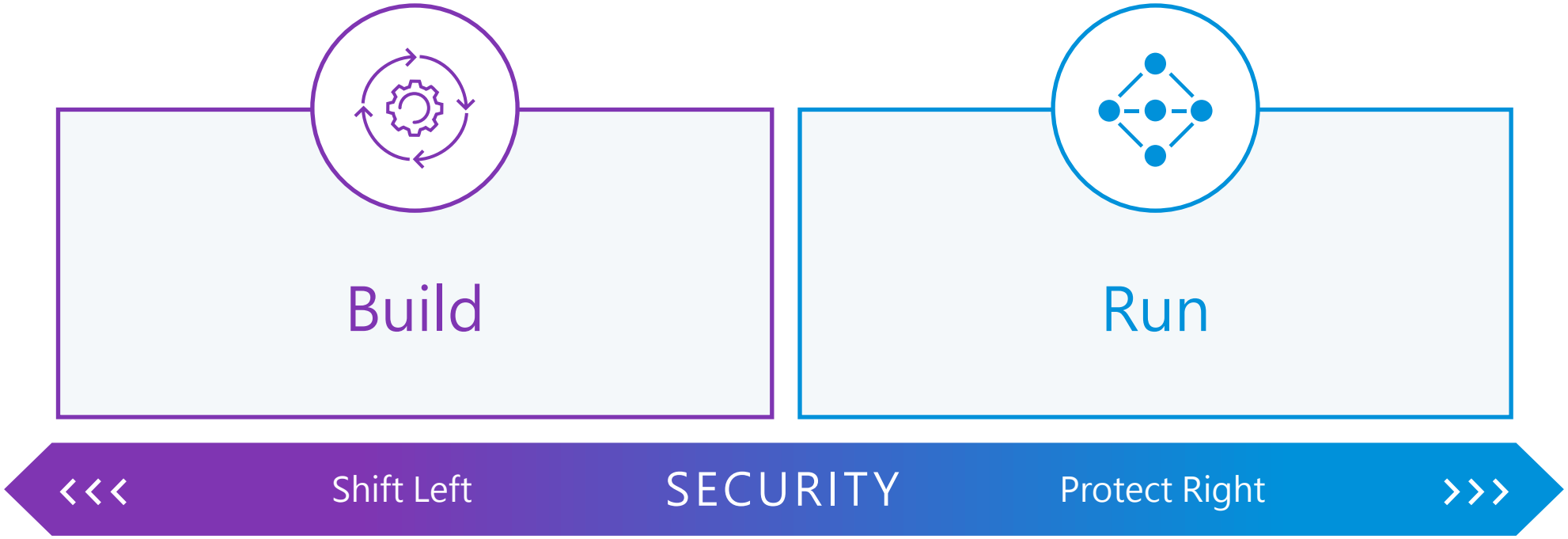
- 容器入侵與異常活動
- 編排控制層之弱點及配置問題
- 對外服務與橫向通訊風險
- 作業系統安全漏洞

雲端與外部環境風險



vmware
©2022 VMware, Inc.

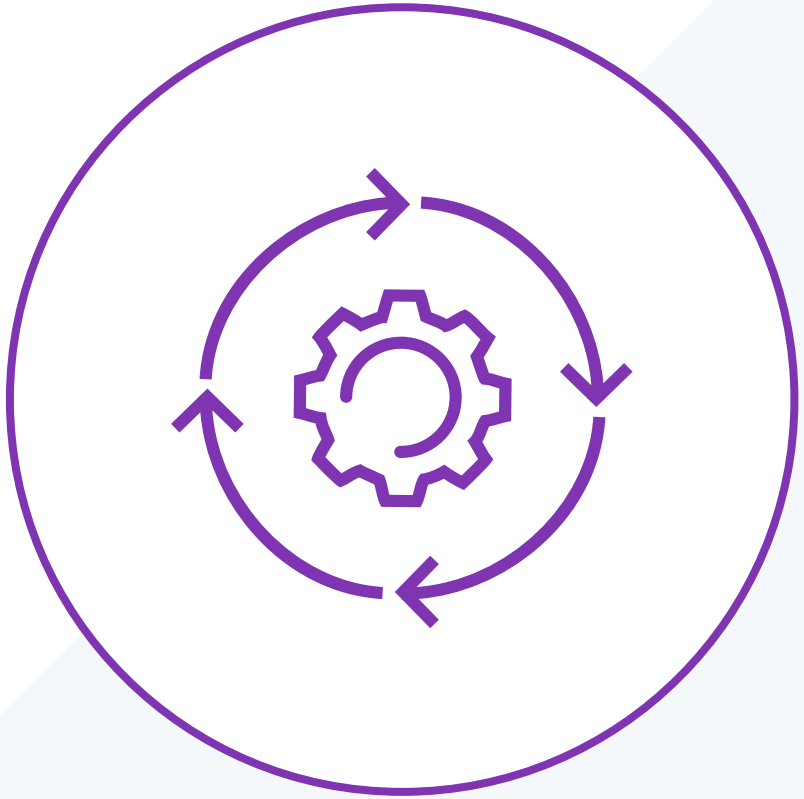
從應用生命週期思考現代化應用的安全策略



©2022 VMware, Inc.

Build

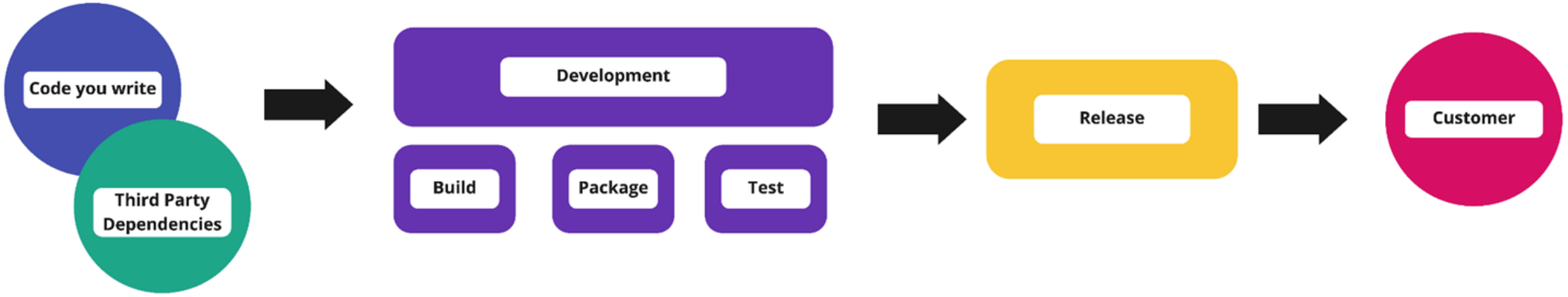
Shifting Security Left
將安全植入到 CI/CD 重要環節，
透過 DevSecOps 組建安全的容器應用



©2022 VMware, Inc.

演進中的軟體供應鏈，帶來新的攻擊表面

除了自製的程式碼，也包含第三方的相依元件，以及從開發到部署過程的相關環境



- 程式漏洞
- 開發工具
- 相依元件安全漏洞

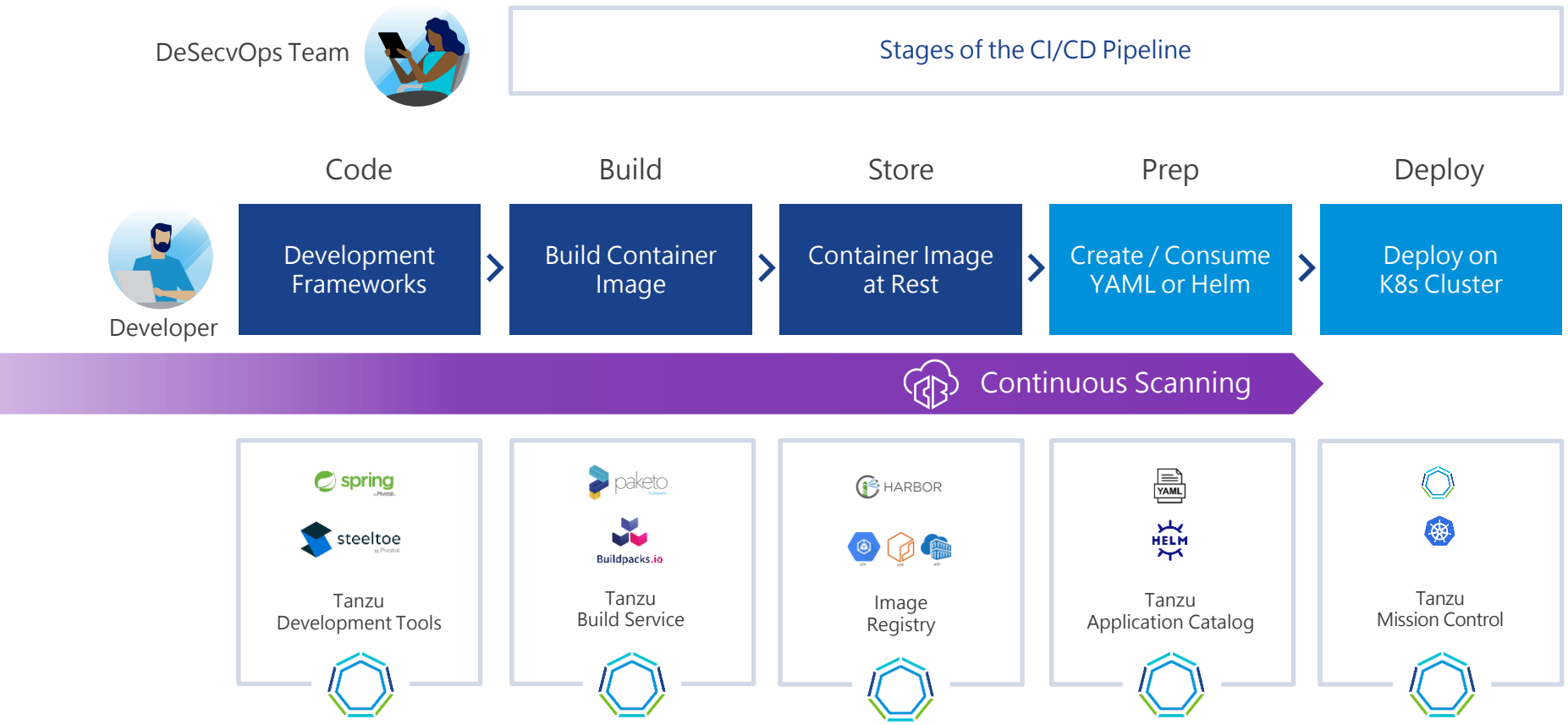
- 組建系統入侵
- 鏡像儲存庫入侵
- 域名劫持/偽造軟體原

- 過時的鏡像
- 鏡像誤用
- SBoM 管理缺陷

- Zero-day 未知弱點
- 特權運行模式
- 不安全的運行環境

©2022 VMware, Inc.

左移策略：將安全植入到 CI/CD 重要環節以組建安全的容器應用



Challenge

- 缺少鏡像弱點檢查工具
- 組建過程夾帶有漏洞的相依組建/鏡像
- 鏡像漏洞過多難以修補
- 誤用老舊、非法、未檢查過的鏡像

VMware Solution

- 提供建議的安全元件及 K8s
- 與 CI/CD 結合自動化進行鏡像安全弱點掃描
- 運用宣告式管理，自動化鏡像安全修補
- 集中管理 K8s 安全政策
- 管制不符合規範的容器運行

©2022 VMware, Inc.

VMware Carbon Black Container Security

幫助您提早發現鏡像弱點

鏡像掃描

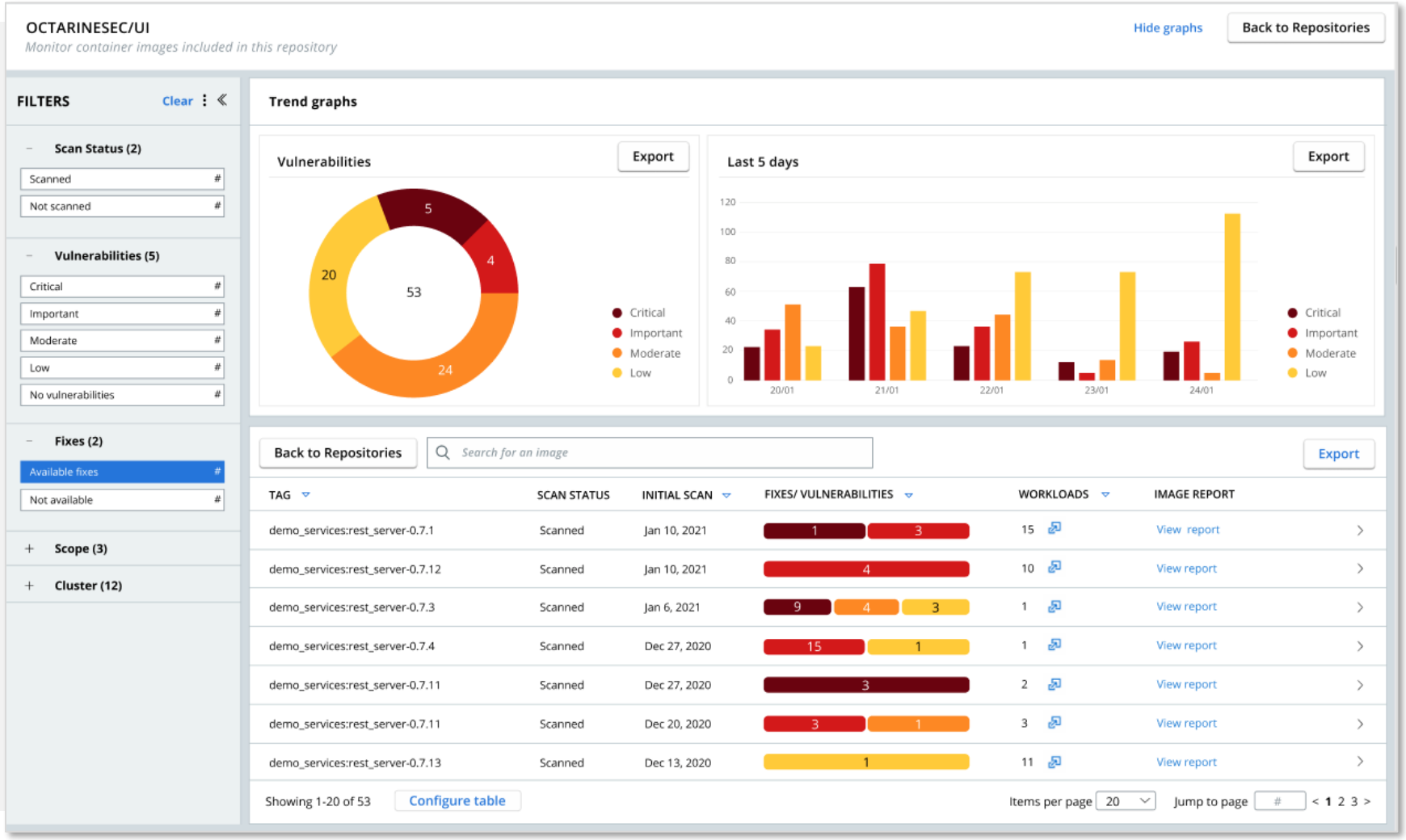
- 確保所有鏡像在執行前都經過檢查
- 辨識弱點
- 確保只有授權的鏡像可以在生產環境使用

弱點評估

- 檢視可能被部署的鏡像的安全狀態
- 根據弱點嚴重程度排序
- 確保只有經過審核的鏡像可以部署在生產環境

鏡像安全強化

- 設定安全及合規的最低門檻
- 依循 CIS Benchmarks 及 K8s 最佳實務
- 產生合規報告



©2022 VMware, Inc.

將鏡像安全掃描與 CICD 整合

cbctl

- 命令列模式，可由開發者透過人工指令操作或是與 CI 整合
- 掃描 images 及 K8s 物件的安全狀態
- 驗證安全政策符合性

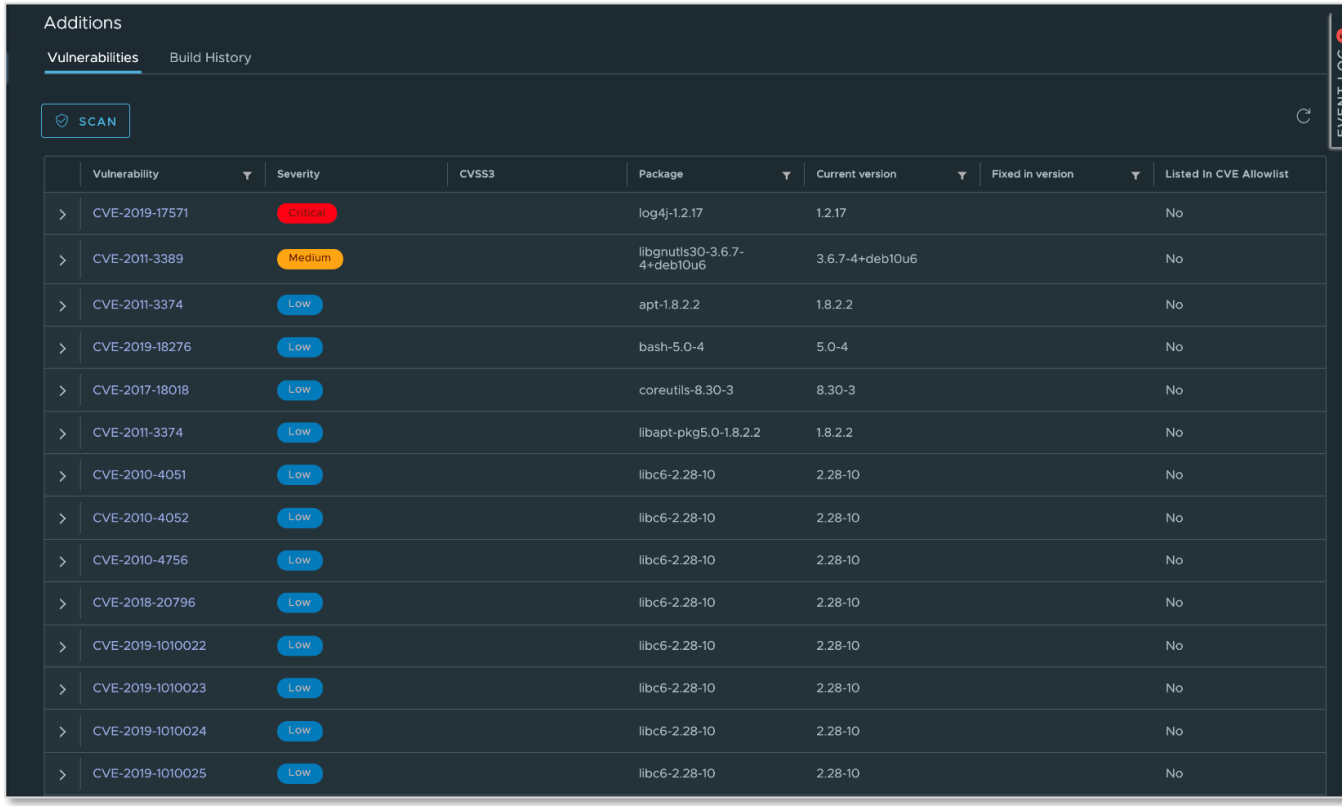
```
 ⠿ Loaded image
 ⠿ Parsed image
 ⠿ Cataloged image  [188 packages]
 ⠿ Scanned image

Scan result for docker.io/octarinesec/guardrails-enforcer:image-scanning ():
+----------------+-----------------------------------+------+----------+-----------------------+---------+---------+
|     VULN ID    |              PACKAGE              | TYPE | SEVERITY |      FIX AVAILABLE    | CVSS V2 | CVSS V3 |
+----------------+-----------------------------------+------+----------+-----------------------+---------+---------+
| CVE-2020-1971  | openssl-1.1.1f-1ubuntu2           | dpkg | HIGH     | 1.1.1f-1ubuntu2.1     |     4.3 |     5.9 |
+----------------+-----------------------------------+------+----------+-----------------------+---------+---------+
| CVE-2021-3449  | openssl-1.1.1f-1ubuntu2           | dpkg | HIGH     | 1.1.1f-1ubuntu2.3     |    -1.0 |    -1.0 |
+----------------+-----------------------------------+------+----------+-----------------------+---------+---------+
| CVE-2021-27365 | linux-libc-dev-5.4.0-56.62        | dpkg | HIGH     | 5.4.0-70.78           |     4.6 |     7.8 |
+----------------+-----------------------------------+------+----------+-----------------------+---------+---------+
| CVE-2020-1971  | libssl1.1-1.1.1f-1ubuntu2         | dpkg | HIGH     | 1.1.1f-1ubuntu2.1     |     4.3 |     5.9 |
+----------------+-----------------------------------+------+----------+-----------------------+---------+---------+
| CVE-2021-3444  | linux-libc-dev-5.4.0-56.62        | dpkg | HIGH     | 5.4.0-70.78           |     4.6 |     7.8 |
+----------------+-----------------------------------+------+----------+-----------------------+---------+---------+
| CVE-2020-27171 | linux-libc-dev-5.4.0-56.62        | dpkg | HIGH     | 5.4.0-70.78           |     2.1 |     5.5 |
+----------------+-----------------------------------+------+----------+-----------------------+---------+---------+
| CVE-2020-28374 | linux-libc-dev-5.4.0-56.62        | dpkg | HIGH     | 5.4.0-62.70           |     5.5 |     8.1 |
+----------------+-----------------------------------+------+----------+-----------------------+---------+---------+
| CVE-2020-27170 | linux-libc-dev-5.4.0-56.62        | dpkg | HIGH     | 5.4.0-70.78           |     2.1 |     5.5 |
+----------------+-----------------------------------+------+----------+-----------------------+---------+---------+
| CVE-2021-3449  | libssl1.1-1.1.1f-1ubuntu2         | dpkg | HIGH     | 1.1.1f-1ubuntu2.3     |    -1.0 |    -1.0 |
+----------------+-----------------------------------+------+----------+-----------------------+---------+---------+
| CVE-2021-23841 | openssl-1.1.1f-1ubuntu2           | dpkg | MEDIUM   | 1.1.1f-1ubuntu2.2     |     4.3 |     5.9 |
+----------------+-----------------------------------+------+----------+-----------------------+---------+---------+
| CVE-2021-27212 | libldap-common-2.4.49+dfsg-2ubuntu1.5 | dpkg | MEDIUM | 2.4.49+dfsg-2ubuntu1.7 |     5.0 |     7.5 |
+----------------+-----------------------------------+------+----------+-----------------------+---------+---------+
| CVE-2020-27673 | linux-libc-dev-5.4.0-56.62        | dpkg | MEDIUM   | 5.4.0-59.65           |     4.9 |     5.5 |
+----------------+-----------------------------------+------+----------+-----------------------+---------+---------+
| CVE-2020-36230 | libldap-2.4-2-2.4.49+dfsg-2ubuntu1.5 | dpkg | MEDIUM | 2.4.49+dfsg-2ubuntu1.6 |     5.0 |     7.5 |
+----------------+-----------------------------------+------+----------+-----------------------+---------+---------+
| CVE-2020-36223 | libldap-2.4-2-2.4.49+dfsg-2ubuntu1.5 | dpkg | MEDIUM | 2.4.49+dfsg-2ubuntu1.6 |     5.0 |     7.5 |
+----------------+-----------------------------------+------+----------+-----------------------+---------+---------+
| CVE-2020-36227 | libldap-common-2.4.49+dfsg-2ubuntu1.5 | dpkg | MEDIUM | 2.4.49+dfsg-2ubuntu1.6 |     5.0 |     7.5 |
+----------------+-----------------------------------+------+----------+-----------------------+---------+---------+
| CVE-2020-36224 | libldap-2.4-2-2.4.49+dfsg-2ubuntu1.5 | dpkg | MEDIUM | 2.4.49+dfsg-2ubuntu1.6 |     5.0 |     7.5 |
+----------------+-----------------------------------+------+----------+-----------------------+---------+---------+
| CVE-2020-36222 | libldap-common-2.4.49+dfsg-2ubuntu1.5 | dpkg | MEDIUM | 2.4.49+dfsg-2ubuntu1.6 |     5.0 |     7.5 |
+----------------+-----------------------------------+------+----------+-----------------------+---------+---------+
| CVE-2021-21300 | git-1:2.25.1-1ubuntu3             | dpkg | MEDIUM   | 1:2.25.1-1ubuntu3.1   |     5.1 |     7.5 |
```

與鏡像倉庫整合

- 讓鏡像倉庫可以自動掃描以取得鏡像安全狀態

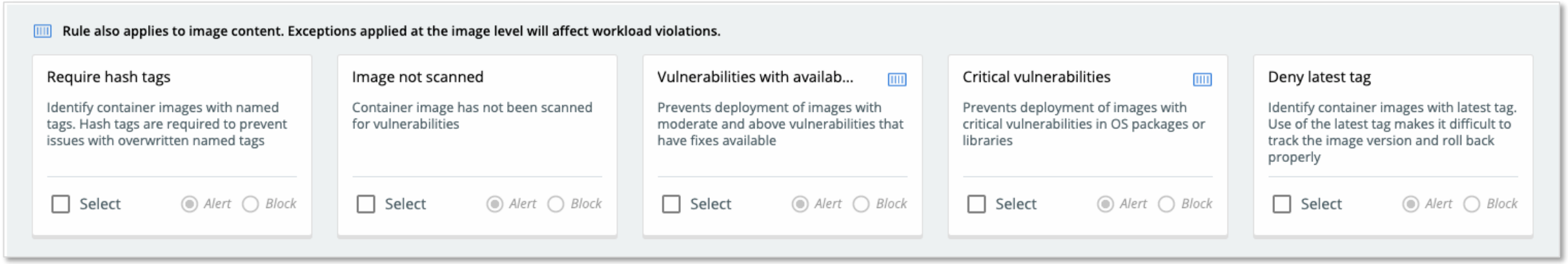
HARBOR

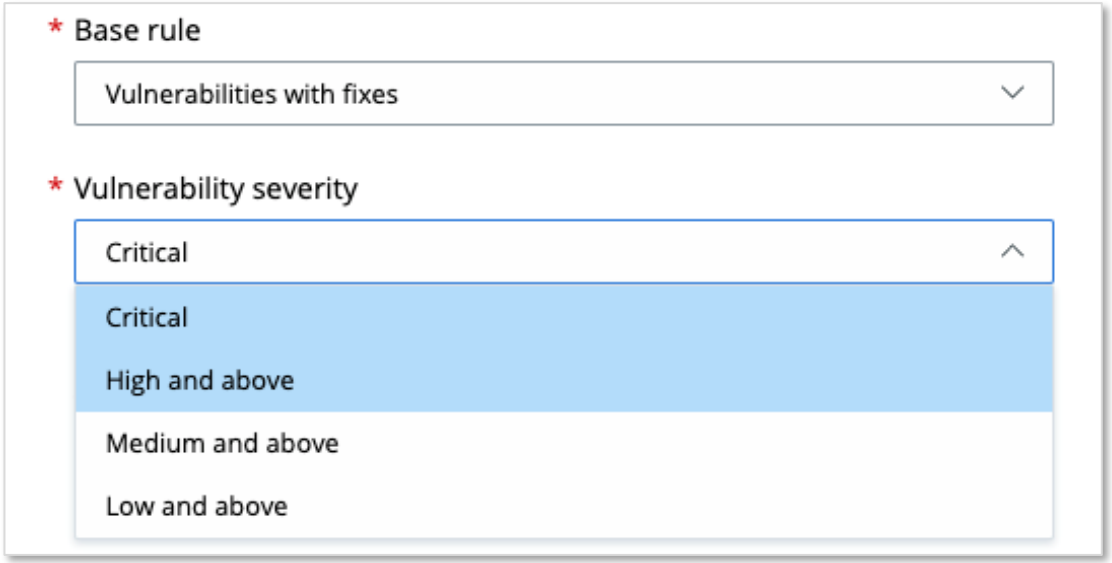


vmware®
©2022 VMware, Inc.

確立鏡像安全政策：預防不合規的鏡像被部署

Image-focused policy rules





New custom rule template

vmware
©2022 VMware, Inc.

鏡像安全修補及管理難題

當開發團隊以不同的方式組建容器鏡像，安全修正及管理複雜度隨即呈指數成長

My app 1

JDK I found

Trusty OS

My app 2

Trusted JDK

ubuntu

My app 3

Trusted JDK

CentOS

Broken Build

Unverified Update

Hard to track and patch CVE

Out of Compliance

挑戰

鏡像管理及更新

難以除錯、修正及維護

安全修補

容器的漏洞修補必須個別進行，耗日費時，難以掌握

容器堆疊稽核

難以一致化的清查及追蹤容器鏡像的相依組建

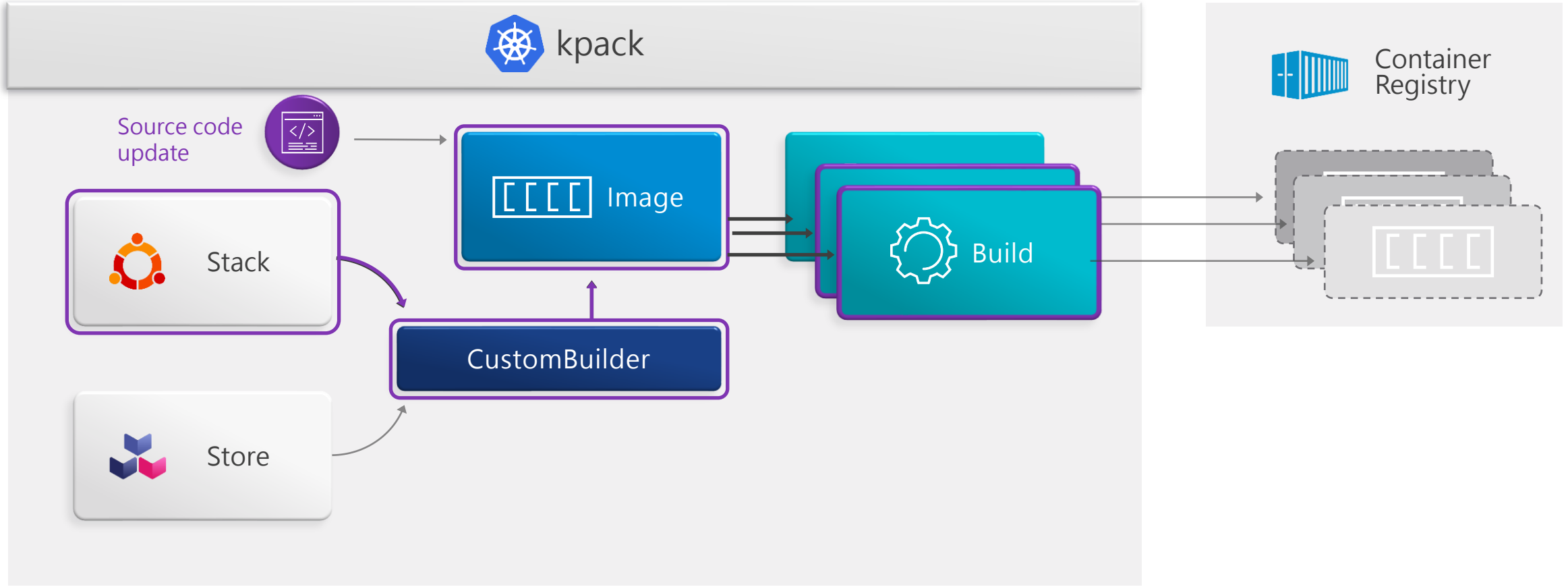
IT 治理

不易達成軟體及安全政策合規

©2022 VMware, Inc.

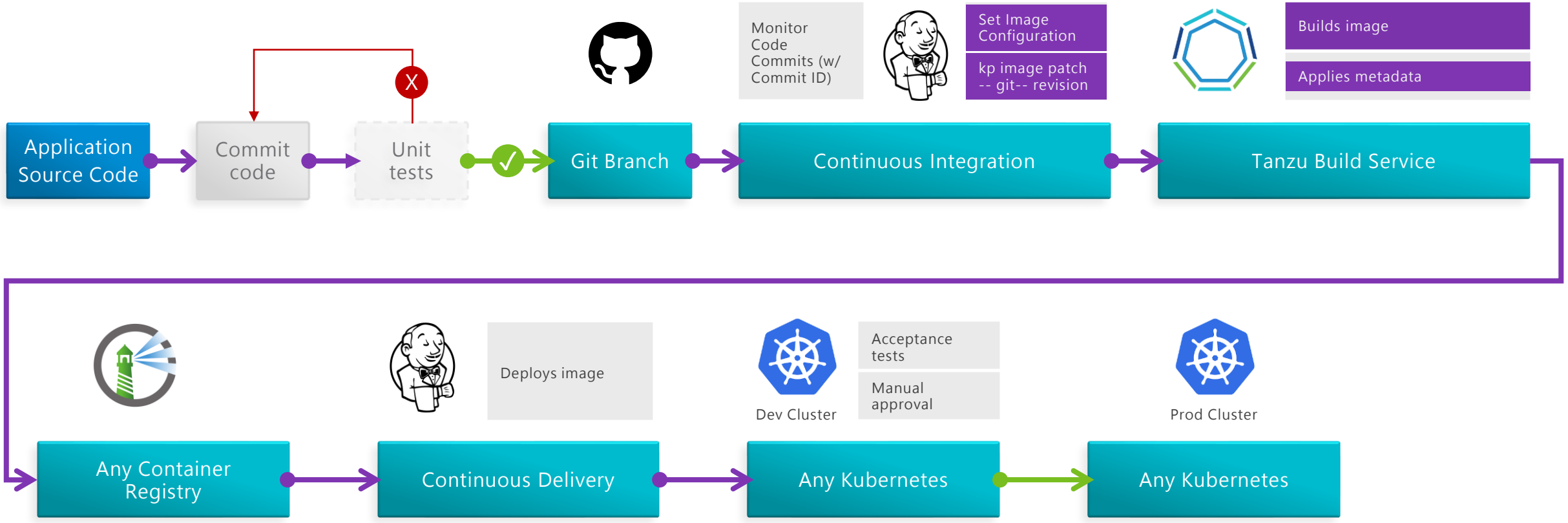
Tanzu Build Service 運用 Buildpacks 自動化配置框架及相依組件

程式碼異動或是相依組件需要更新時，可自動驅動鏡像重建並上傳至鏡像倉庫



©2022 VMware, Inc.

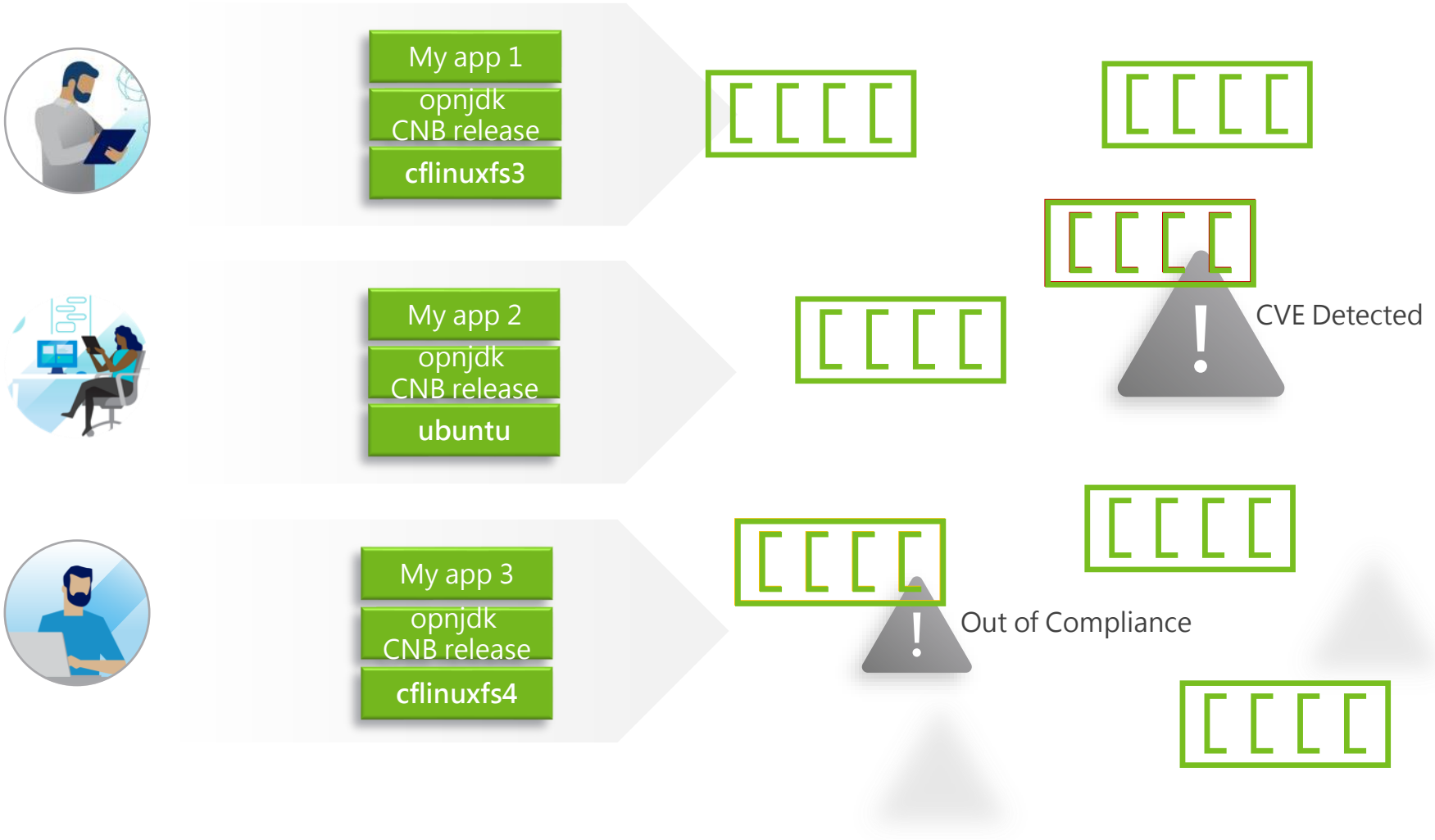
Tanzu Build Service 可無縫整合到 CI / CD 流程



©2022 VMware, Inc.

Tanzu Build Service 解決容器鏡像組建及維運難題

將鏡像的組建與配置透過管理框架，搭配自動化更新機制大幅簡化修補及維運



解決方案

自動化鏡像更新

依 code commit、相依組件及 OS 更新自動化組建新的容器鏡像

提升鏡像安全

簡化鏡像之安全修補及追蹤

強化容器堆疊稽核

完整的容器組建堆疊元數據，讓稽核輕易達成

增強 IT 治理敏捷性

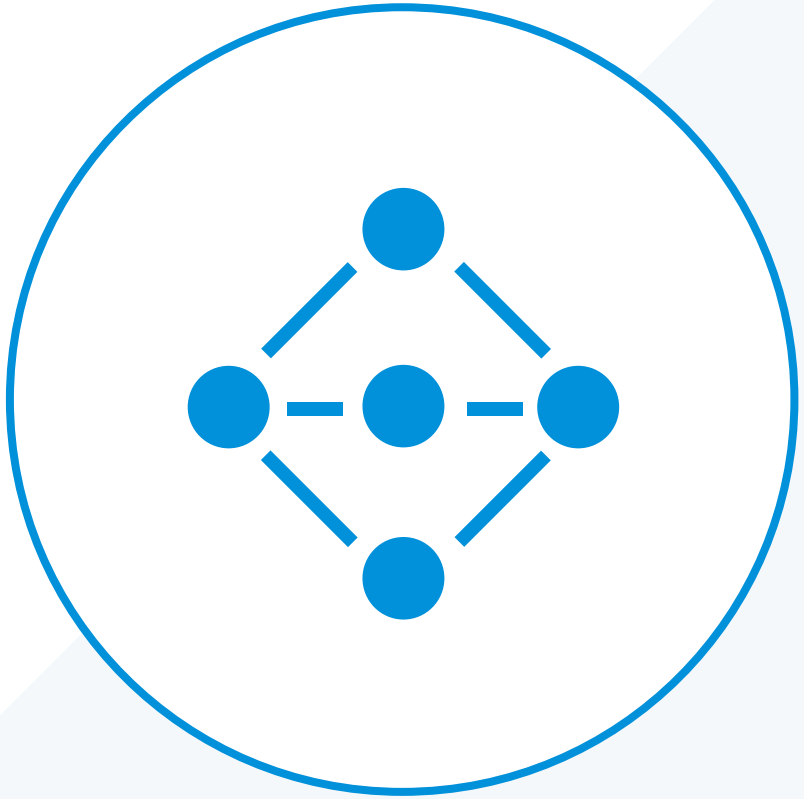
讓政策的符合性更容易檢驗及查核

©2022 VMware, Inc.

Run

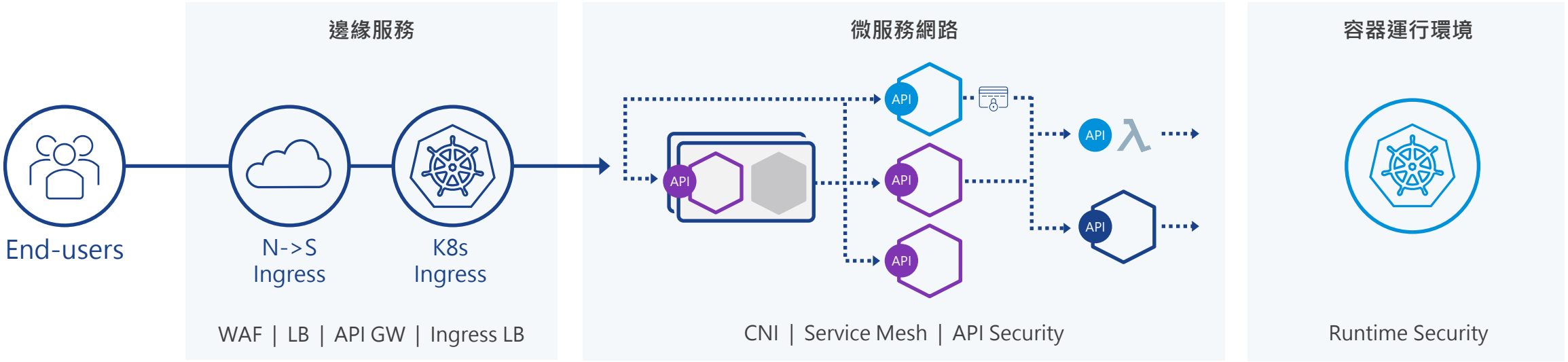
Protect Security Right

為容器的運行環境與交互通訊
做好正確的安全防護



©2022 VMware, Inc.

容器化應用在運行階段可能面臨的安全挑戰



At the Edge

如何確保只有合法流量可以接取容器應用?

E-W Security

如何確保微服務間僅有正確的資料流可以互相溝通?

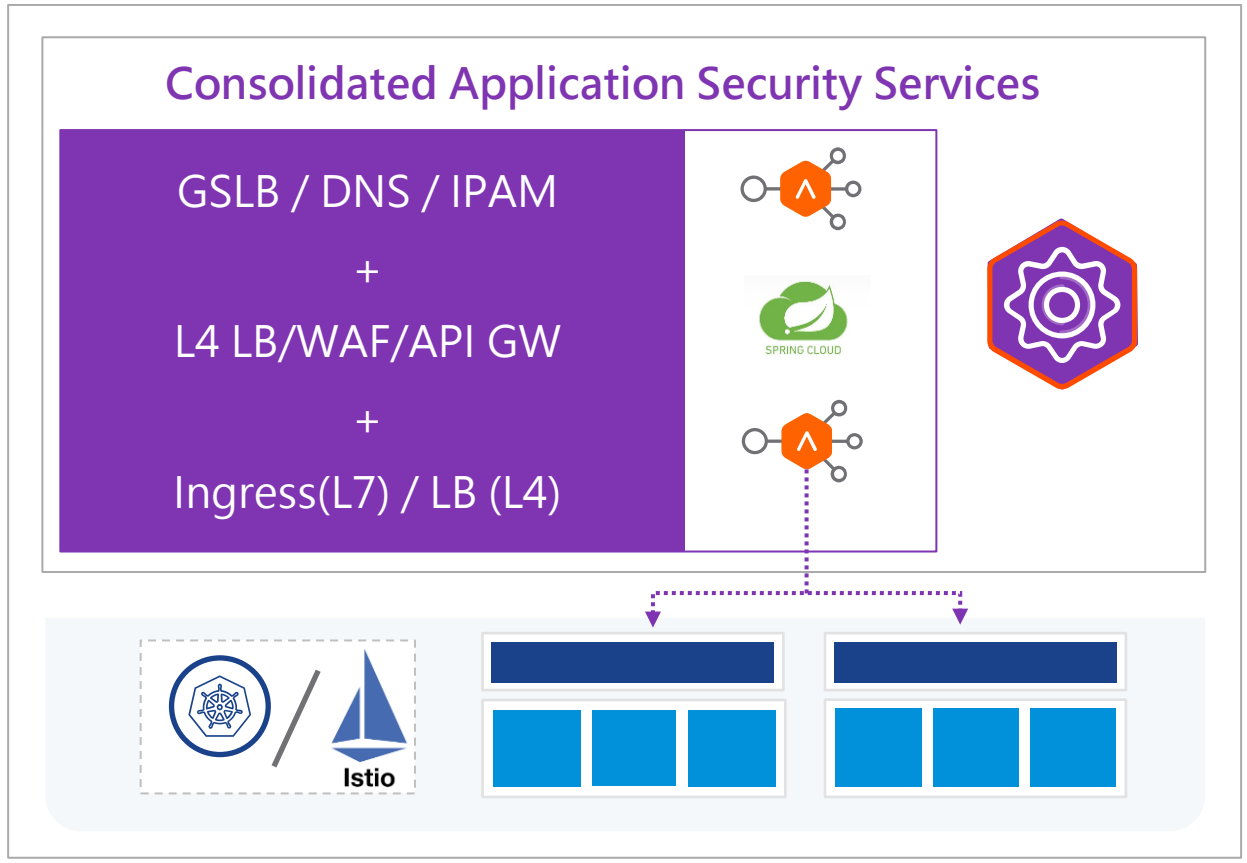
The Container Runtime

如何確保容器在運行環境以預期的狀態運行並得到應有防護？

©2022 VMware, Inc.

VMware 提供統合的邊緣安全服務

NSX Advanced Load Balancer



在邊緣節點提供整合的
應用層級安全及流量管理能力

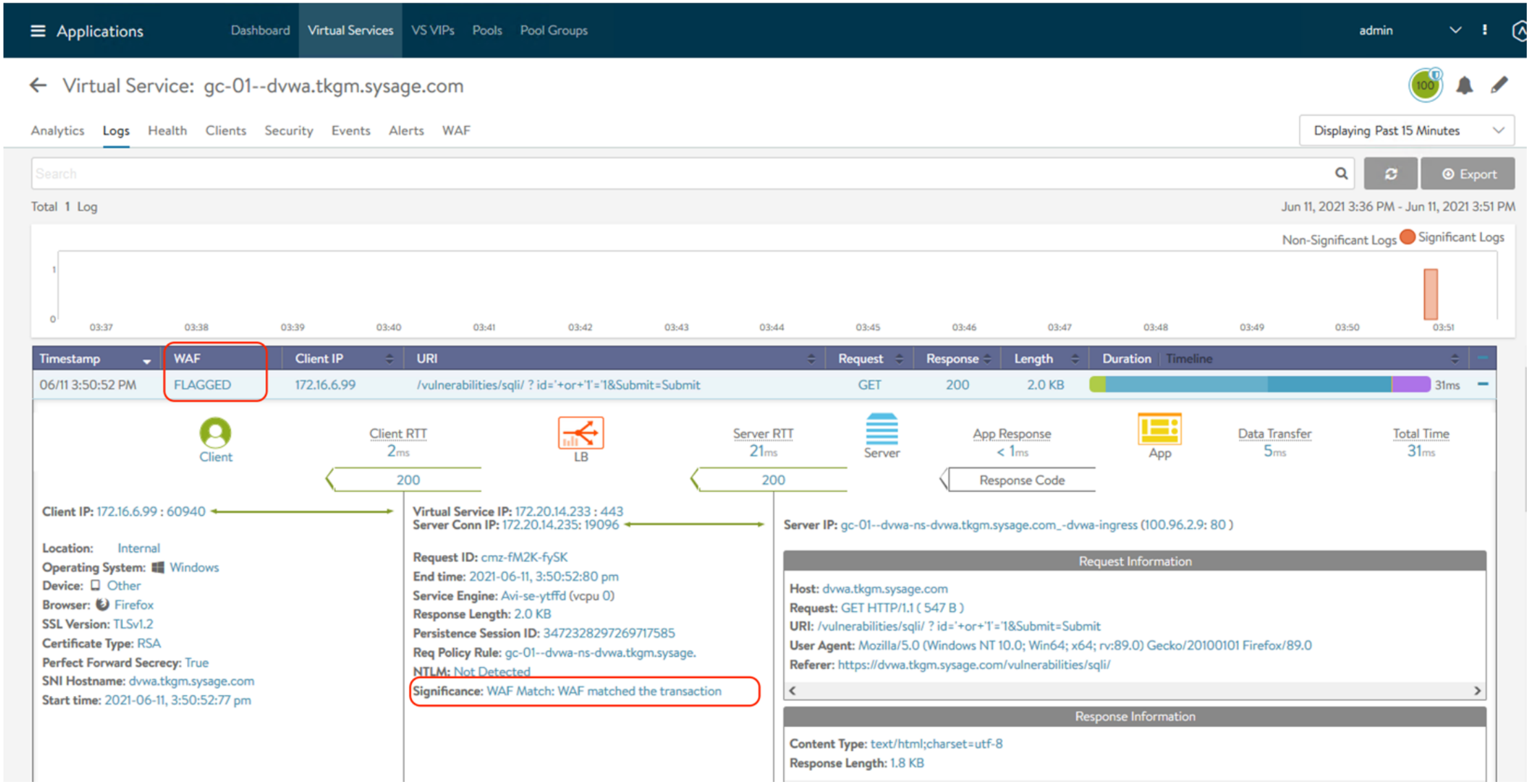
與雲原生應用集成
的自動化服務及節點部署

豐富的可視性及分析能力

大幅簡化維運及部署

©2022 VMware, Inc.

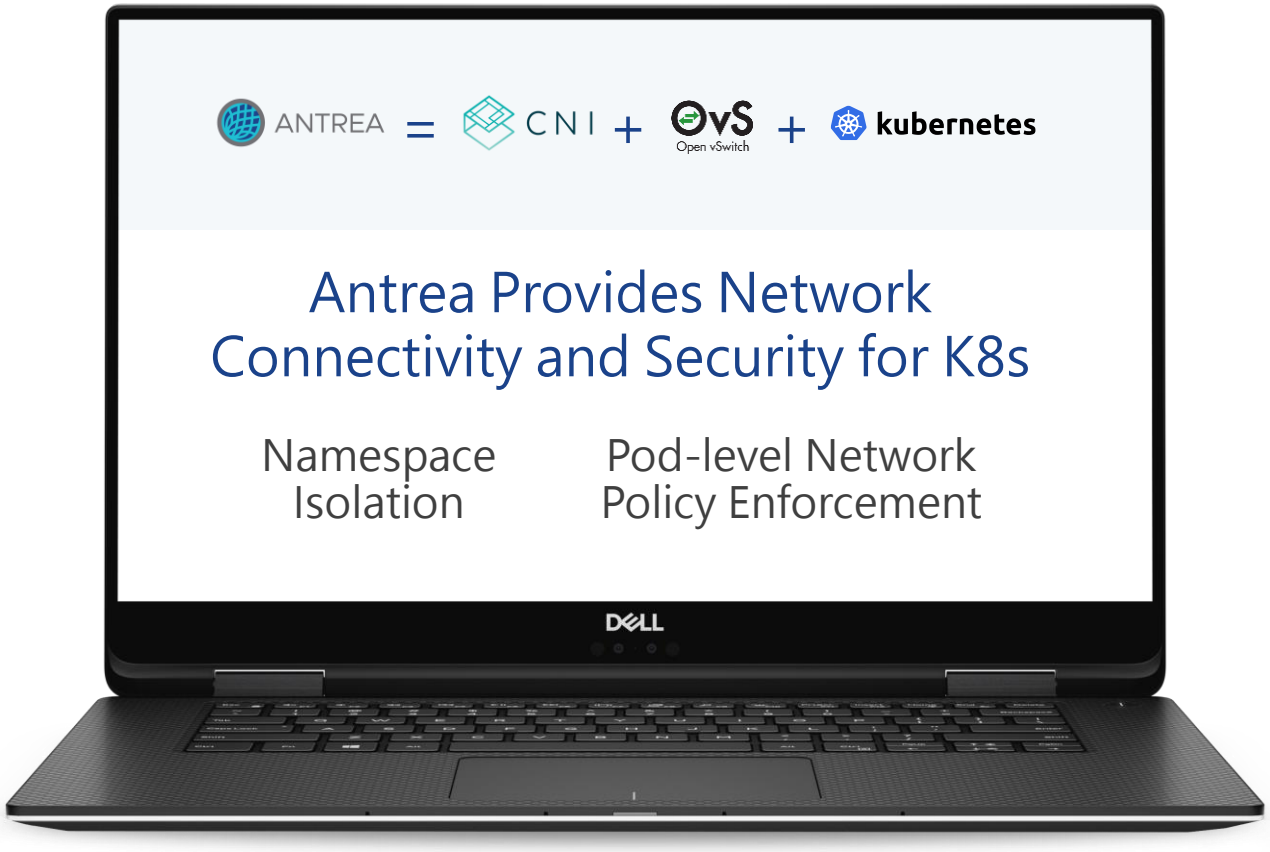
NSX ALB 簡化容器服務部署，帶來更佳的安全性(WAF)及可視性



©2022 VMware, Inc.

透過 Project Antrea 為容器網路做好防護

Antrea 搭配 NSX 可以圖形化管理安全性，建立容器網路可視性、東西向防護及網路流追蹤



Runs K8s Everywhere

vmware Tanzu™ · Amazon EKS · Azure · OPENSHIFT

Open and Community Driven

aws · Google · IBM · intel · NVIDIA · vmware

1.1k GitHub stars

212 GitHub forks

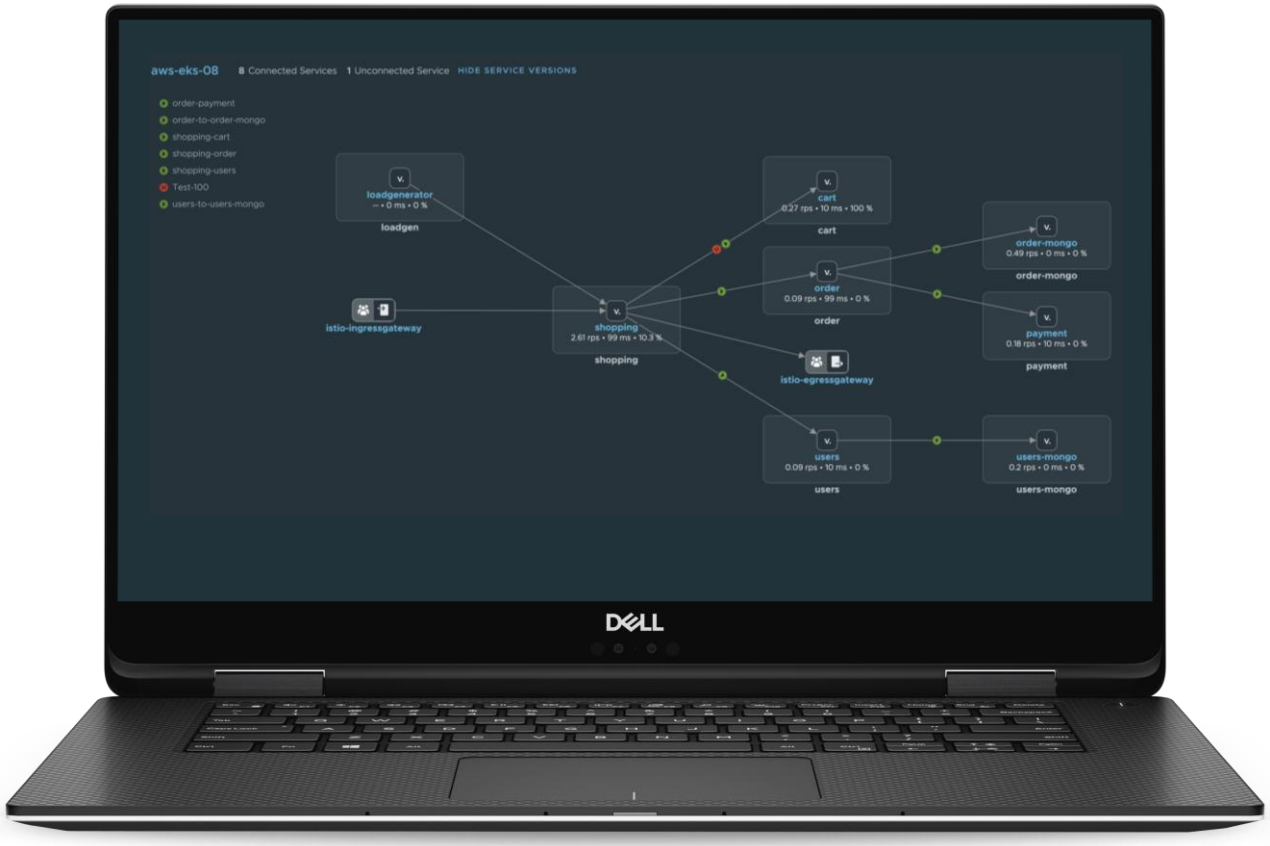
80 Contributors

vmware ©2022 VMware, Inc.

NSX 為容器網路提供企業等級，圖形化的安全管理能力

©2022 VMware, Inc.

Service Mesh: 為應用提供跨雲、跨叢集的服務串連及安全



Service Mesh 概念

- 為現代化應用提供端到端的應用/微服務串連及安全
- 以開源的 Istio 及 Envoy 專案為基礎

應用案例

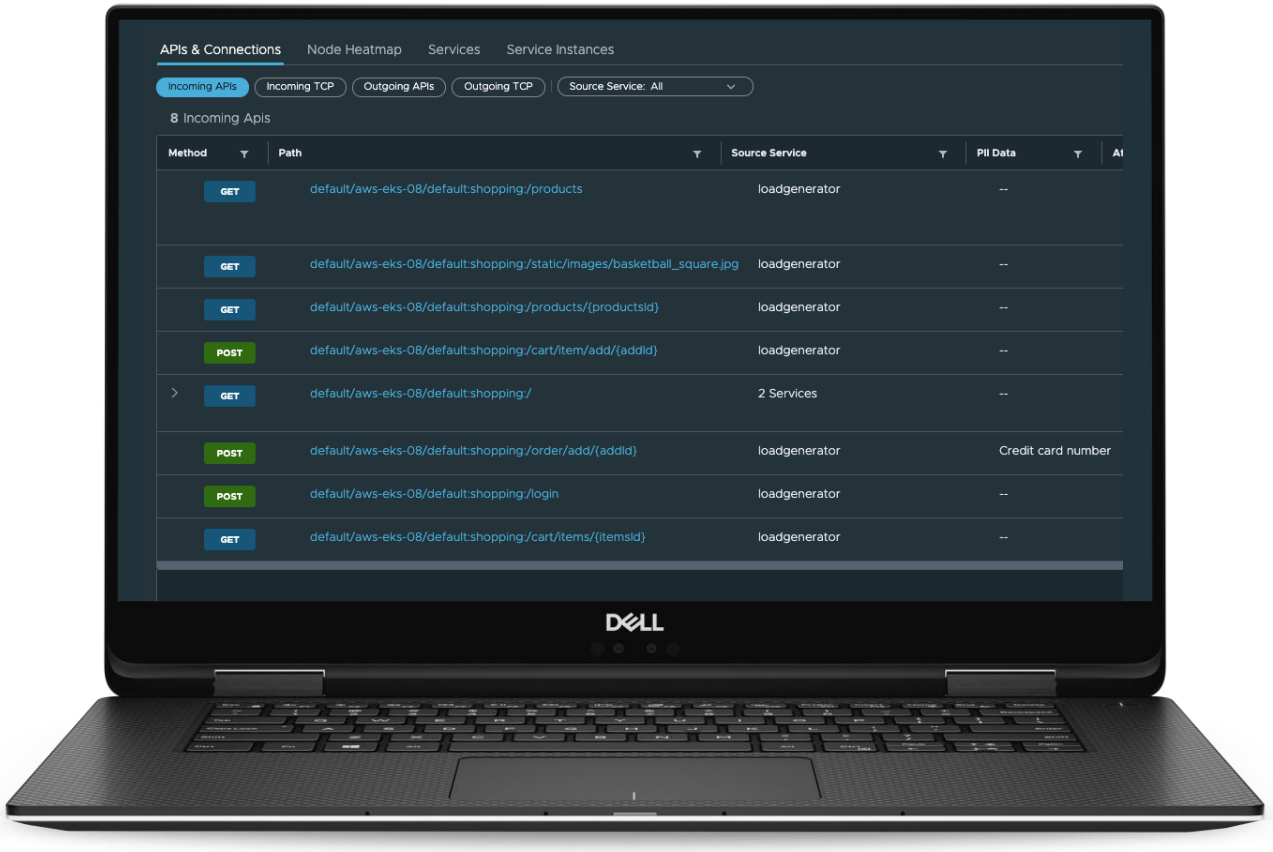
流量管理 | 安全 | 可視性

Tanzu Service Mesh 提供的安全能力

- 跨雲、跨叢集微服務串連
- 容器-容器(服務與服務)間的資料通訊加密
- 存取控制政策及稽核
- API 可視性、安全及合規

©2022 VMware, Inc.

保護應用的新端點: API

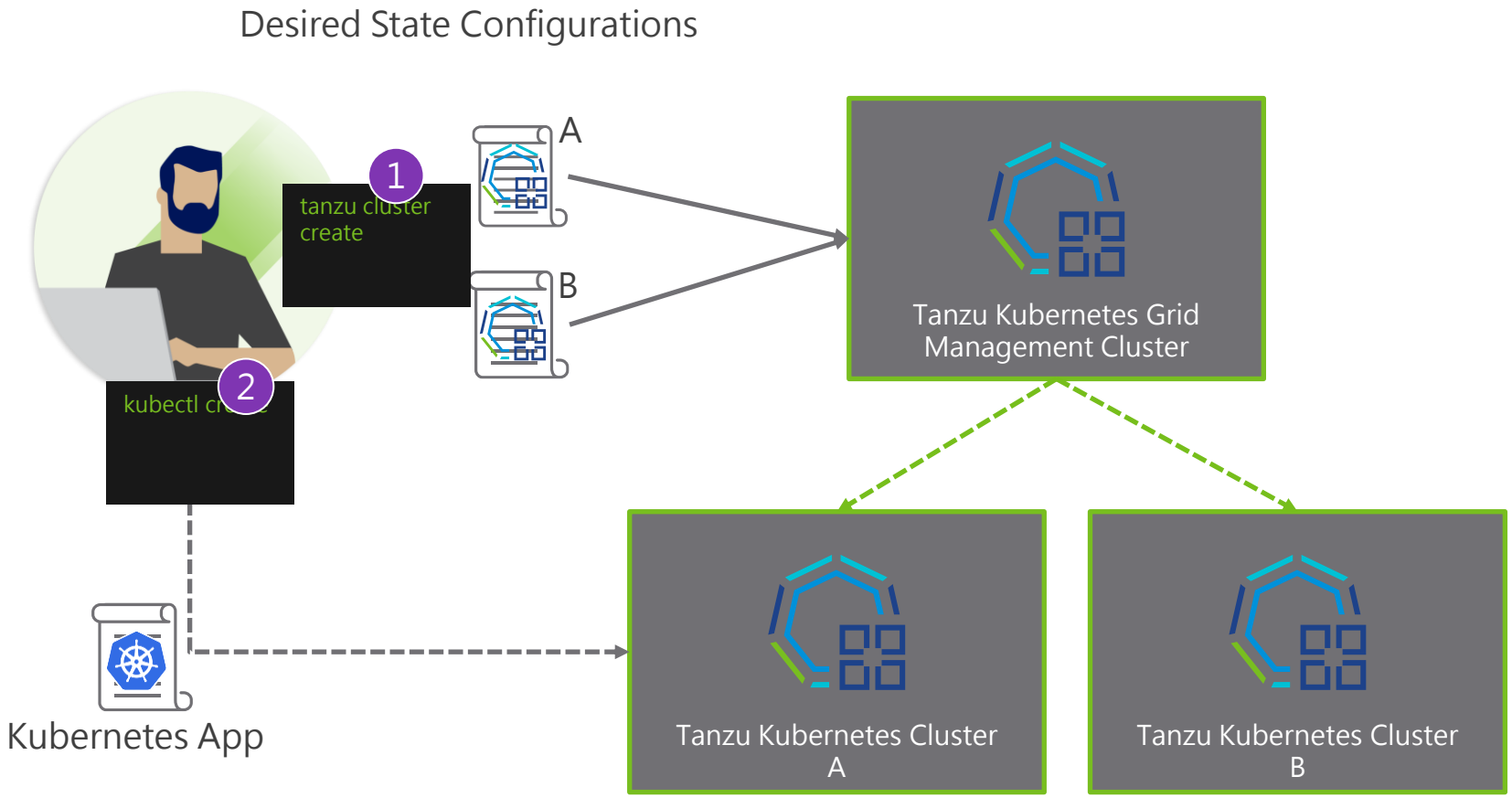


- API 探索
- 對應通訊特徵
- 為正常的活動建立基準線
- 偵測異常的行為

©2022 VMware, Inc.

以更安全、簡易的方式創建 K8s 運行環境

Tanzu Kubernetes Grid



宣告式管理、自動化部署

- 可自定義叢集規格、透過自助式服務
- 一鍵式完成叢集之部署、版本更新、規格變更等生命週期管理

企業級驗證及支援、符合 CNCF

- 經測試、打包、簽認，相容於 upstream 的發行版本
- 降低自行安裝、設定 OS、修正程式、K8s 相關套件所需之負擔及安全風險

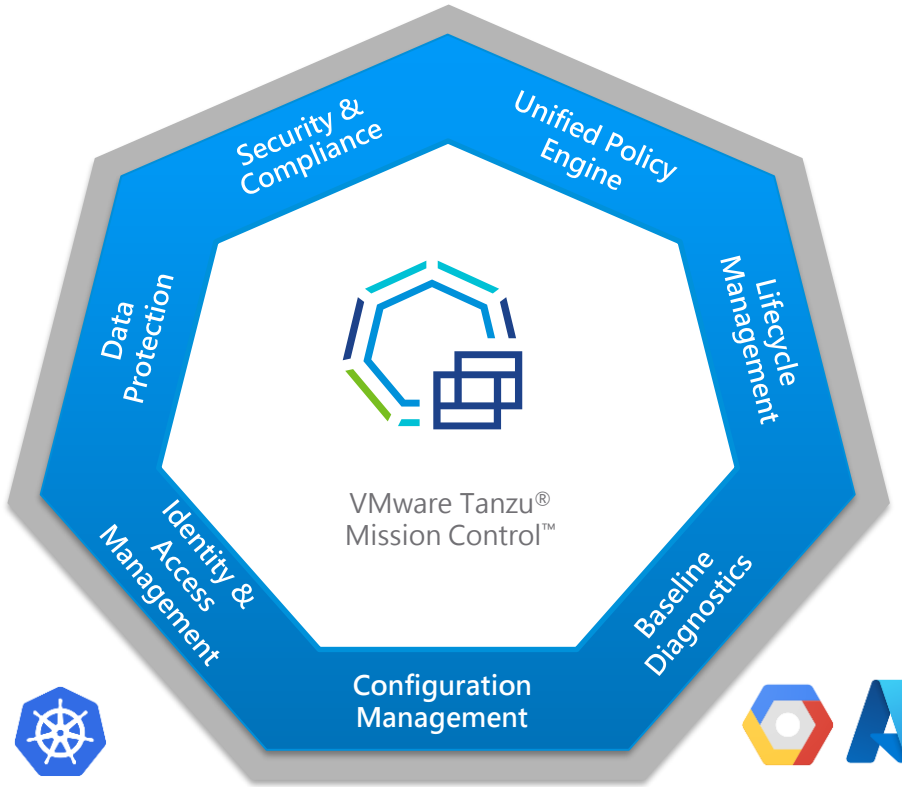
支援多叢集多版本，有效隔離環境

- 可依業務、開發階段、部門有效區隔
- 提升測試可靠度及有效區隔風險

©2022 VMware, Inc.

為容器運行環境提供更好的管控

Tanzu Mission Control



Any Kubernetes cluster anywhere

On-premises Public Cloud Edge

跨叢集、跨雲管理，提高 K8s 運行環境及安全可視性

集中管理安全政策、帳戶及權限、網路及配額配置

檢查與標準 K8s/CIS Benchmark 等最佳實務之符合性

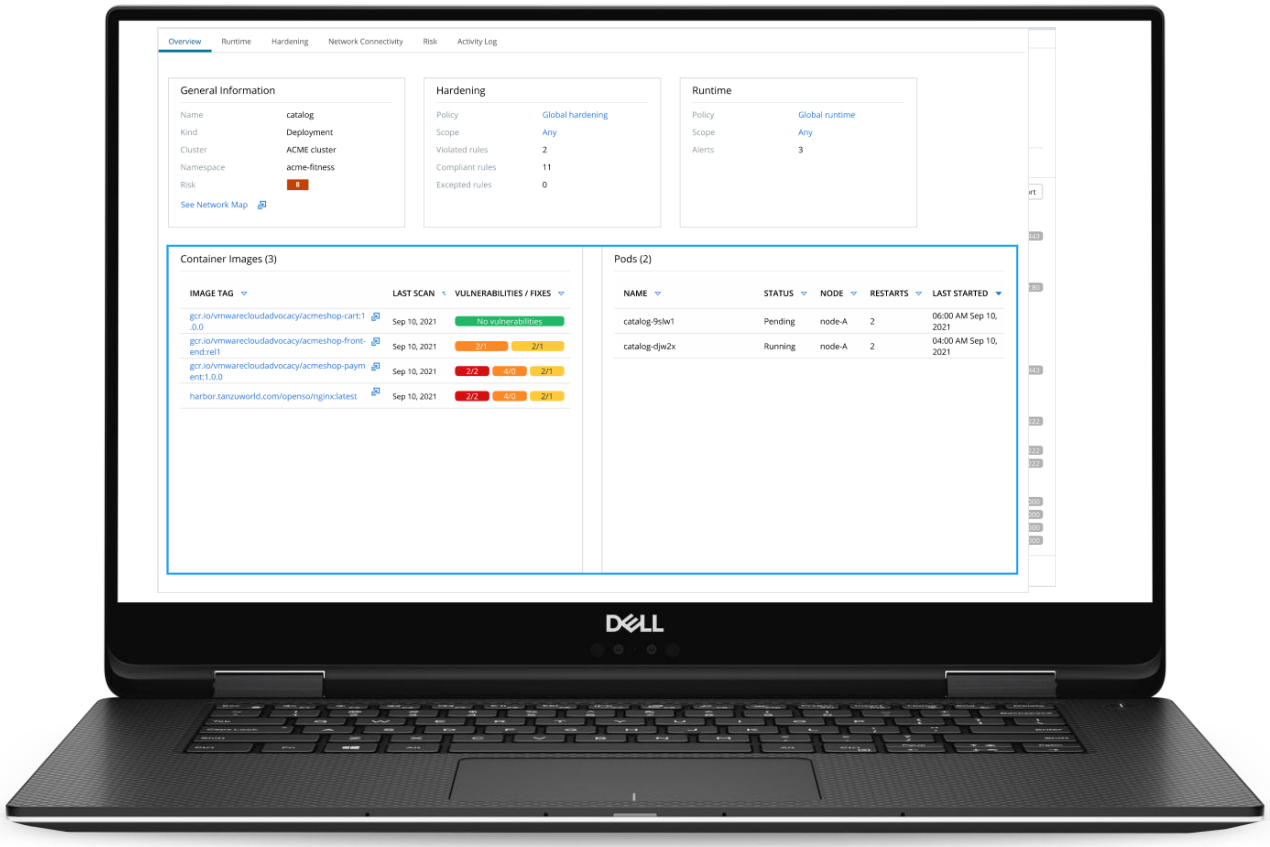
簡化 K8s 部署、套件管理及容器備份

vmware

©2022 VMware, Inc.

為容器負載提供執行階段之安全性

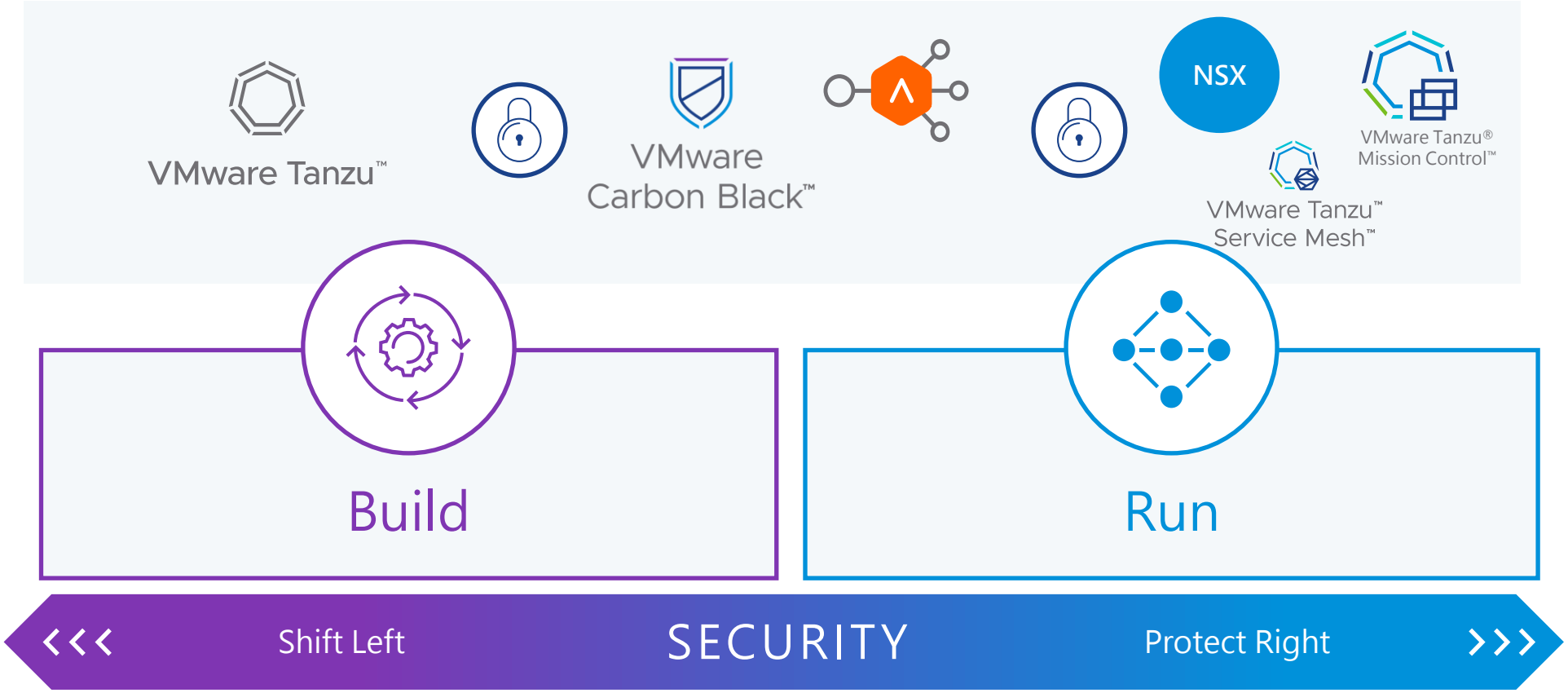
Carbon Black Container Security Advanced



- 提供容器網路、負載及加密狀態之可視性
- 分析及管理 Egress 存取
- 容器及網路異常活動偵測
- 惡意活動偵測

vmware®
©2022 VMware, Inc.
The image is for illustrations purposes only.
The information in this presentation is for informational purposes only and may not be incorporated into any contract. There is no commitment or obligation to deliver any items presented herein.

VMware 現代化應用安全方案為您從應用的組建到運行做好把關



©2022 VMware, Inc.

Thank You

vmware® Confidential | © VMware, Inc.