
FORTINET

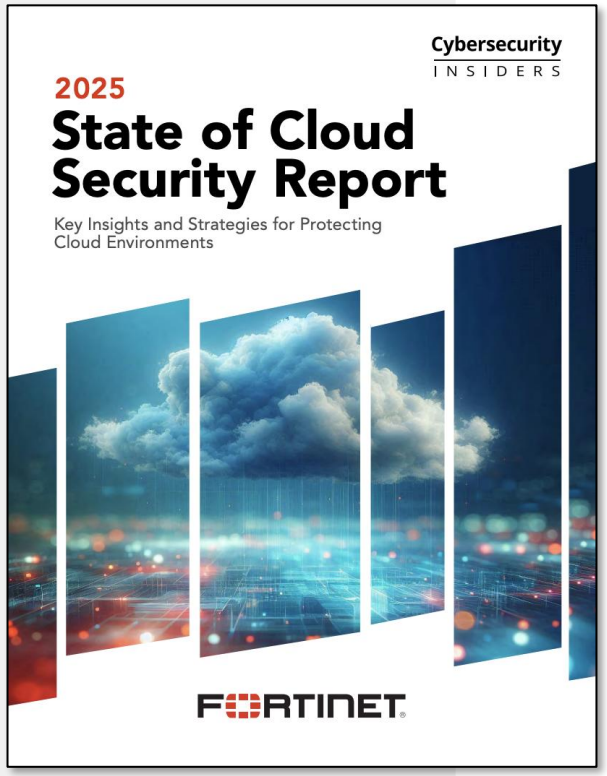
# FortiCNAPP
# AI驅動雲端原生應用程式保護平台

Technical Consultant

James Wang

# 雲端安全前三大挑戰

2025 Cloud Security Report Survey




**64%** 缺少
跨雲威脅及時偵測與回應

**55%** 缺乏
雲端可視化管理

**53%** 不足
雲端安全管理人力與技術

# FortiCNAPP
# AI驅動雲原生應用程式保護平台

# FortiCNAPP 提供企業雲端 開發/佈署/維運 安全方案

## FortiCNAPP AI驅動的雲原生應用程式保護平台

**CSPM**
Cloud Security Posture Management
雲端安全態勢管理

**CDR**
Cloud Detection and Response
雲端偵測及回應

**SOAR**
Security Orchestration, Automation, and Response
安全協助自動化

**KSPM**
Kubernetes Security Posture Management
容器安全態勢管理

**SAST / DAST / SCA**
Secure Application Lifecycle
安全應用生命週期

**CIEM**
Cloud Infrastructure and Entitlement Mgm
雲端基礎架構權限管理

**IaC**
Infrastructure as Code
基礎架構即程式碼

**CWPP**
Cloud Workload Protection Platform
雲端工作負載保護

**NGFW+WAAP**
Cloud Firewall , Web Application and API Protection
雲端網路與應用防火牆

**PaC**
Policy as Code
政策即程式碼

### 安全統一化
- 單一品牌管理
- 單一儀表監控
- 合一多雲管理

### 安全可視化
- Cloud/K8S安全態勢
- Workloads分析監控
- 帳號權限監控

### 安全自動化
- 合規與政策持續檢查
- 軟體與漏洞掃瞄監控
- 威脅偵測與緩解回應

# FortiCNAPP 提供agentless and agent-based 雙效整合

## FortiCNAPP 提供企業最佳整合方式進行

### 檢查雲端帳戶發生甚麼

**Agentless for cloud accounts**

- AWS, Azure, Google Cloud
- Continuous monitoring of cloud configuration
- Compliance checks
- Account threat detection
- Container/host vulnerability assessment
  (software supply chain risk)

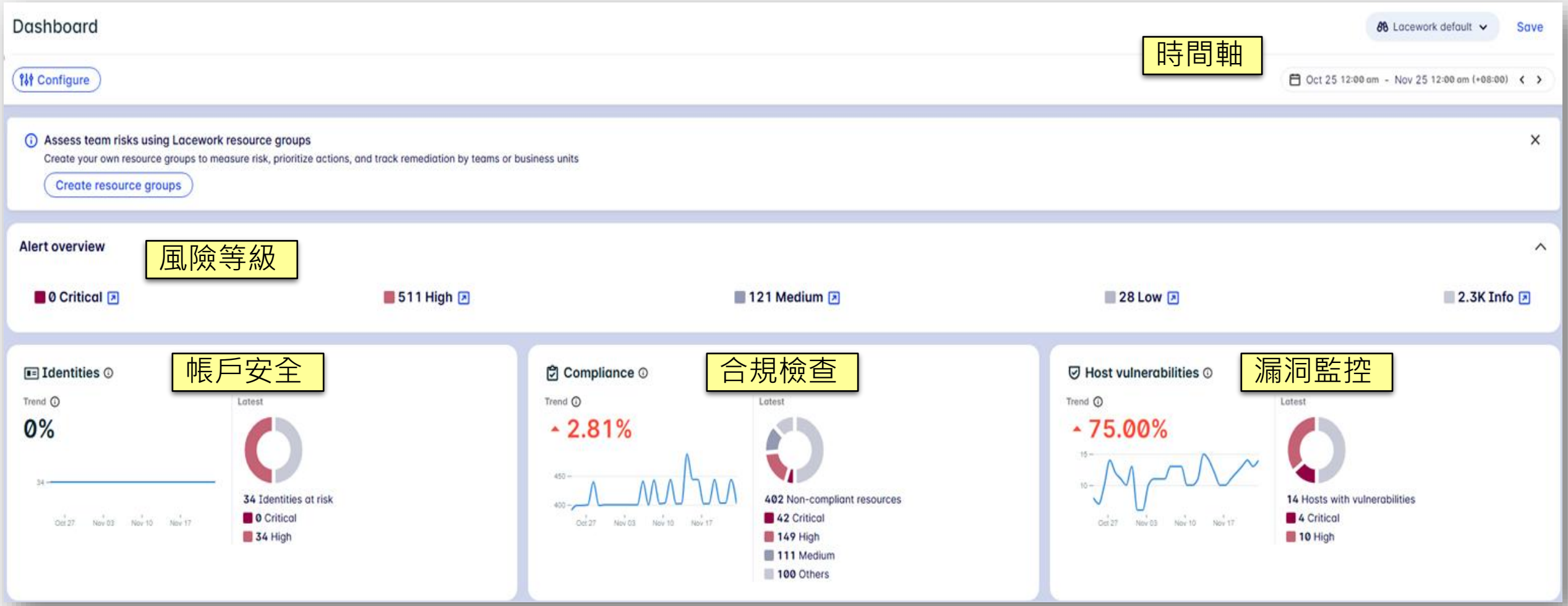
### 檢查雲端系統發生甚麼

**Agent for cloud compute**

- Kubernetes, containers, workloads runtime visibility
- Host intrusion detection
- File integrity monitoring
- User, app, process, and network behavior monitoring
- Container/host vulnerability
  (runtime correlation, CI/CD integration)

# FortiCNAPP 單一安全狀態儀表 (CSPM/KSPM)

## AI驅動全年無休檢查雲端安全風險



# FortiCNAPP 分析Cloud 安全可視化與告警

雲端活動監控

1 - 50 of 20000

| Account | Region | Service | API | Event hour | User name | Source IP | S3 URL | Count | Request parameters | User identity |
|---|---|---|---|---|---|---|---|---|---|---|
| 772035820905 | us-east-1 | ssm.amazonaws.c... | UpdateInstanceInf... | 11/27/2024 10 PM (+... | AssumedRole/772... | 44.203.216.232 | s3://lacework-ct-b... | 1 | | {...} |
| 772035820905 | eu-central-1 | sts.amazonaws.com | AssumeRole | 11/27/2024 10 PM (+... | AWSService/7720... | resource-explorer-2.a... | s3://lacework-ct-b... | 1 | {...} | {...} |
| 772035820905 | us-east-1 | sts.amazonaws.com | AssumeRole | 11/27/2024 10 PM (+... | AWSService/7720... | logs.amazonaws.com | s3://lacework-ct-b... | 1 | {...} | {...} |
| 772035820905 | us-east-2 | ec2.amazonaws.c... | DescribeVpcs | 11/27/2024 10 PM (+... | AssumedRole/772... | ecs.amazonaws.com | s3://lacework-ct-b... | 2 | | {...} |
| 772035820905 | us-west-2 | elasticloadbalanci... | DescribeLoadBala... | 11/27/2024 10 PM (+... | AssumedRole/772... | config.amazonaws.com | s3://lacework-ct-b... | 1 | | {...} |

使用可視化

Account = All Accounts | Caller Account | Service | Source IP | User | Principal ID | Reset

**Events**
MAX: 11.2K AVG/HR: 4.91K


**Alerts**
MAX: 2 AVG/HR: 1.02


**Unique usernames**
MAX: 48 AVG/HR: 41.1


**Unique APIs**
MAX: 413 AVG/HR: 173

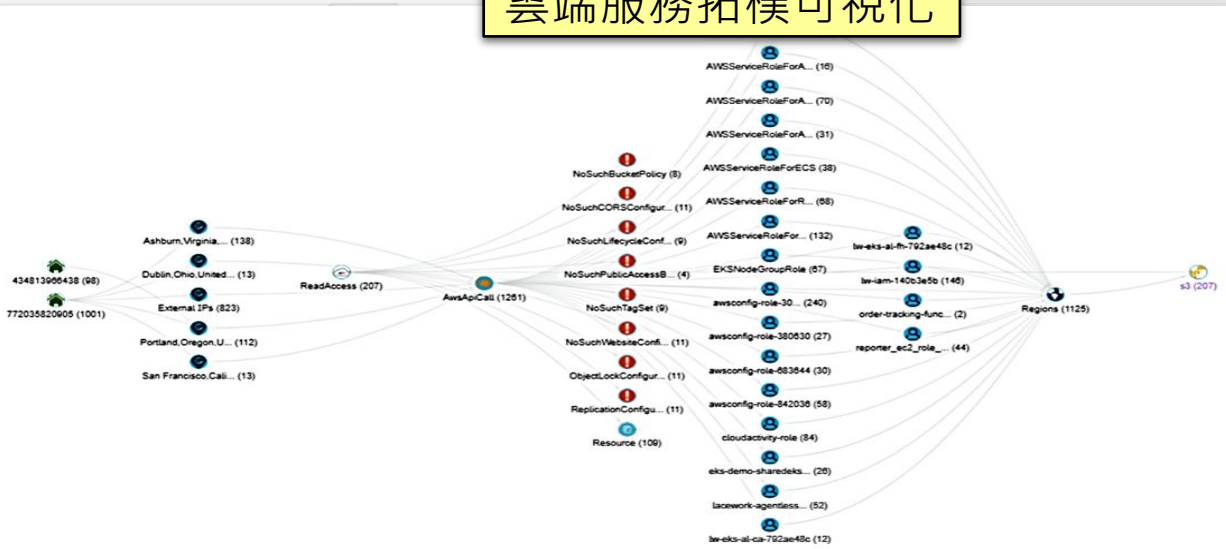

自動分析告警

**Alerts**

1 - 2 of 2

| Alert name | Severity | Event activity |
|---|---|---|
| New service | Medium | 11/20/2024 at 10:00 PM +08:00 to 11:00 PM +08:00 |

雲端服務拓樸可視化

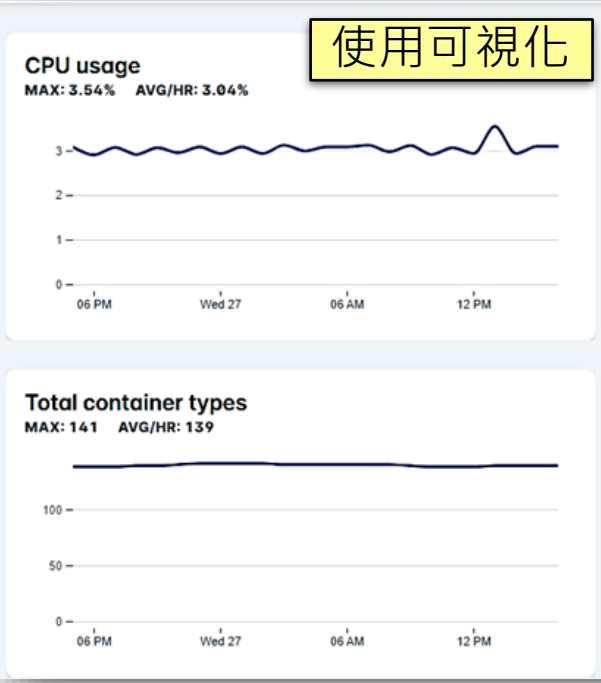


# FortiCNAPP 分析Workloads 安全可視化與告警

工作活動監控

| Container ID | Pod name | Pod namespace | Kubernetes cluster | | Start time | Hostname | PID | Vulnerabilities |
|---|---|---|---|---|---|---|---|---|
| 5630b2a546dfb0c115b2a0d... | aws-node-j5ft2 | kube-system | eks-demo-sharedeks | 602401143452.dkr.ecr.us-ea... | 10/8/2024 4:16 AM (+08:00) | ip-10-0-3-9.ec2.internal | 4524 | 7 High 49 Fixable View Repo |
| a833e87ae4f0202899abb06... | cloud-node-manager-5v... | kube-system | aks-demo-sharedaks-aks | mcr.microsoft.com/oss/kub... | 11/25/2024 8:56 AM (+08:00) | aks-default-42392653-vmss... | 4381 | |
| 990b34c5956854a81231fa5a... | lacework-agent-fc2p9 | lacework | aks-demo-sharedaks-aks | docker.io/lacework/datacoll... | 11/25/2024 8:57 AM (+08:00) | aks-default-42392653-vmss... | 6659 | 4 Medium 0 Fixable View Re |

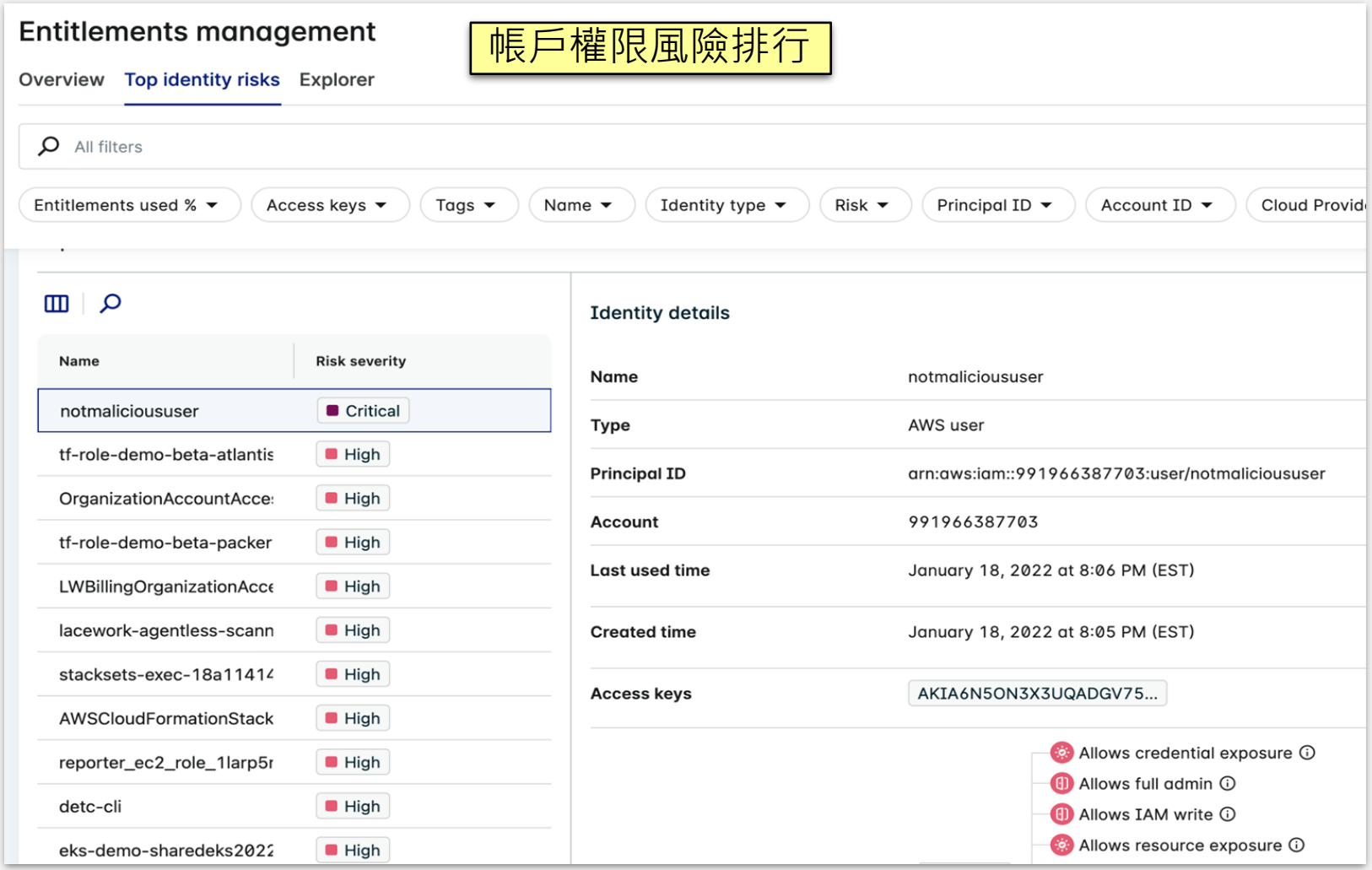
使用可視化




自動分析告警


服務拓樸可視化分析

# FortiCNAPP 分析Account/Group/Role權限



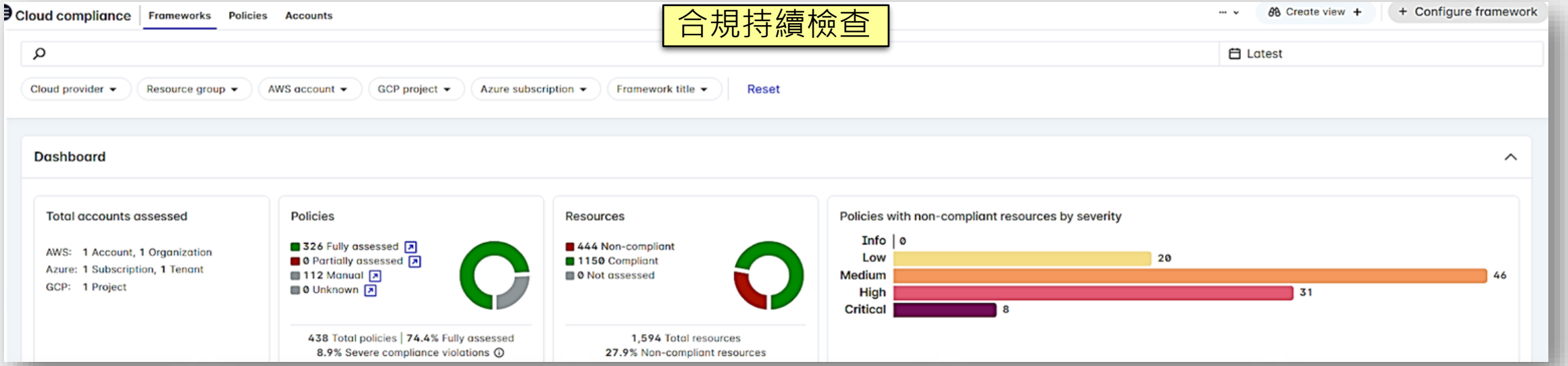

## 帳戶權限檢查

- 雲端使用者、群組和角色身份和權限清單。
- 識別並修正權限過高的角色。

## 服務權限檢視

- 持續監控雲端使用者、資源、群組和角色身分及其相關的網路有效權限
- 持續與活動資料進行比較，以驗證授予的權限與存取的權限

# FortiCNAPP 彈性Compliance引擎 自動檢查規則與安全風險等級




AWS

| Framework Name |
|---|
| AWS Cloud Security Alliance Cloud Control Matrix (CSA CCM) v4.0.5 |
| AWS Cyber Essentials 2.2 Report |
| AWS ISO/IEC 27002:2022 |
| AWS Cybersecurity Maturity Model Certification (CMMC) v1.02 |
| AWS HIPAA Report |
| AWS ISO 27001:2013 Report |
| AWS NIST 800-171 rev2 Report |
| AWS NIST 800-53 rev5 Report |
| AWS NIST CSF |
| AWS PCI DSS 3.2.1 Report |
| AWS SOC 2 Report |
| AWS PCI DSS 4.0.0 Report |
| Lacework FortiCNAPP AWS Security Addendum 1.0 |
| AWS FSBP Standard |

GCP

| Framework Name |
|---|
| CIS Google Cloud Benchmark 2.0.0 |
| GCP Cybersecurity Maturity Model Certification (CMMC) v1.02 |
| GCP HIPAA (2013) Report |
| GCP ISO 27001:2013 Report |
| GCP NIST 800-171 rev2 Report |
| GCP NIST 800-53 rev5 Report |
| GCP NIST CSF Report |
| GCP PCI DSS 3.2.1 Report |
| GCP SOC 2 Report |
| GCP PCI DSS 4.0.0 Report |
| GCP Cloud Security Alliance Cloud Control Matrix (CSA CCM) v4.0.5 |

Azure

| Framework Name |
|---|
| Azure HIPAA Report |
| Azure ISO 27001:2013 Report |
| Azure NIST 800-171 rev2 Report |
| Azure NIST 800-53 rev5 Report |
| Azure NIST CSF Report |
| Azure PCI DSS 3.2.1 Report |
| Azure SOC 2 Report |
| Azure PCI DSS 4.0.0 Report |
| Azure Cloud Security Alliance Cloud Control Matrix (CSA CCM) v4.0.5 |

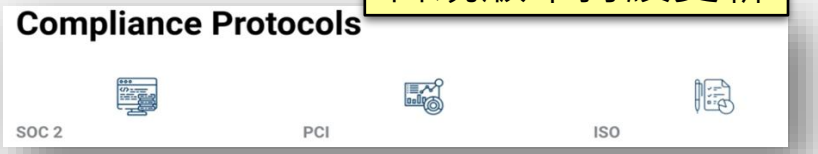
OCI

| Framework Name |
|---|
| Oracle Cloud Infrastructure Configuration (OCI CFG) Detector Rules |

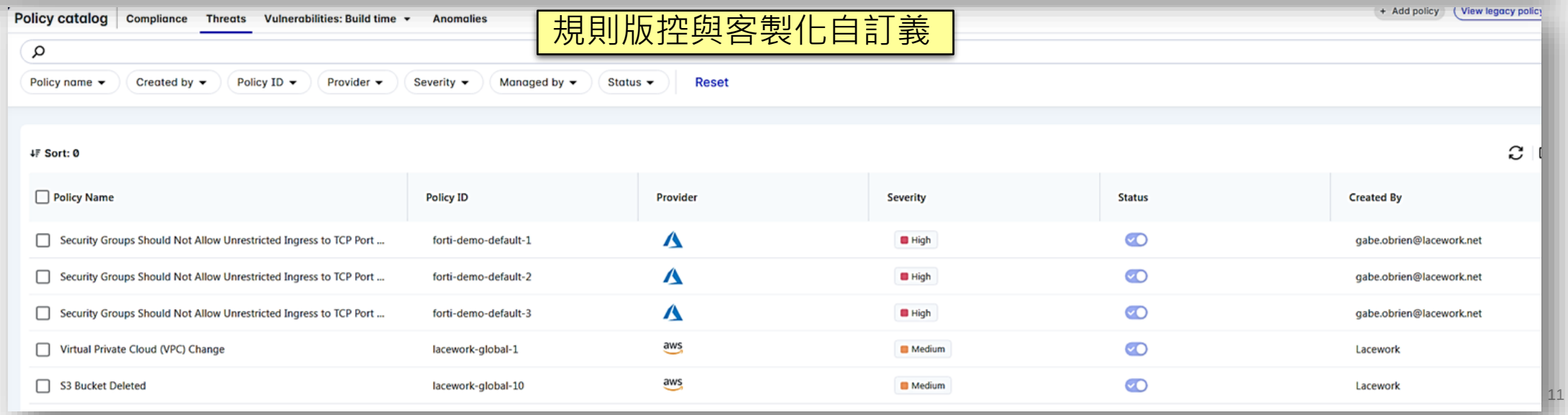
K8S

| Framework Name |
|---|
| CIS Google Kubernetes Engine (GKE) Benchmark v1.4.0 |

合規版本持續更新



# FortiCNAPP 使用Threats引擎 自動檢查規則與告警

# FortiCNAPP Path Investigation AI分析潛藏威脅路徑

持續潛藏威脅分析

Path investigation

Lacework default

Sav

| Name | Cloud provider | Account/Project/Subscripti | Resource type | Path severity | Vulnerabilities | Secrets | Compliance violations |
|---|---|---|---|---|---|---|---|
| reporter_ec2_role_y... | AWS | 991966387703 | AWS IAM role | Info | 2 Critical | 0 | 4 |
| reporter_ec2_role_y... | AWS | 991966387703 | AWS IAM role | Info | 2 Critical | 1 | 4 |

**風險持續探勘**

- 設定錯誤
- 權限疏失
- 軟體漏洞

EXPOSURE POLYGRAPH

**reporter_ec2_role_yenjfgcjnw**

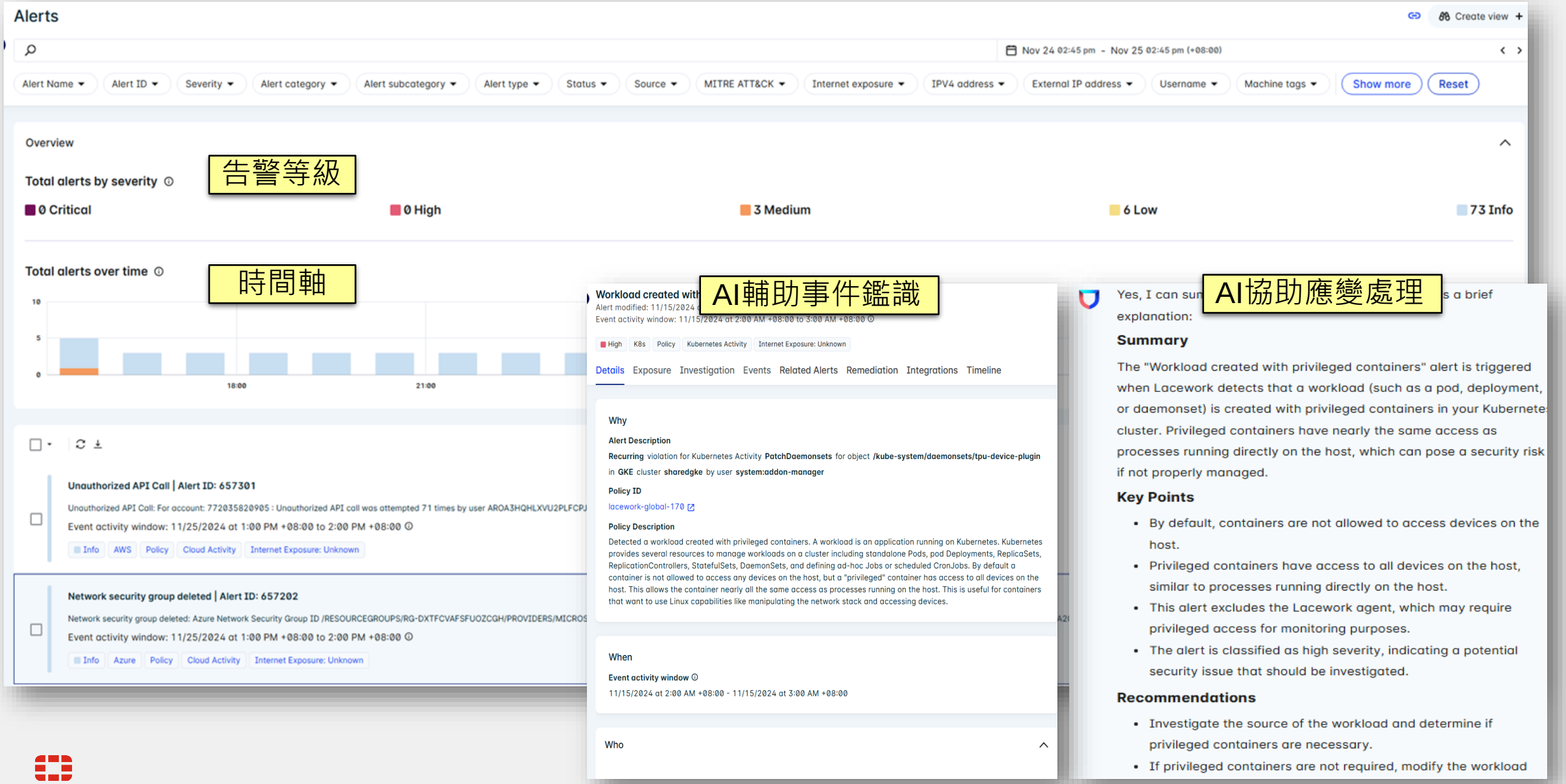
Last updated on 4/19/2024 2:00 AM (EDT)

**Description**

Internet accessible ip-172-16-1-213.us-east-2.compute.internal with critical vulnerabilities. EC2 ip-172-16-1-213.us-east-2.compute.internal instance has access to admin privilege IAM Role reporter_ec2_role_yenjfgcjnw.

潛藏威脅分析可視化

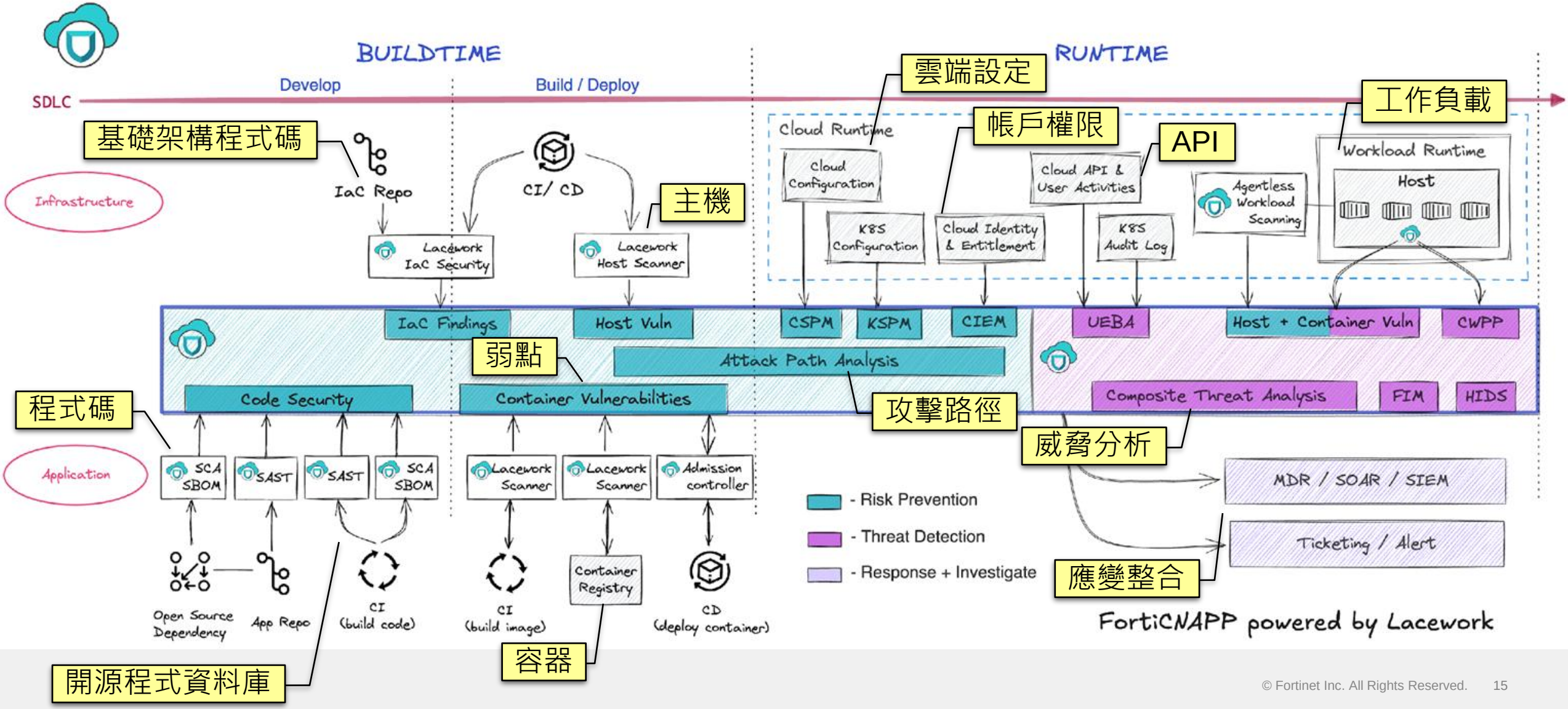
# FortiCNAPP 透過AI協助告警應變與緩解



# 為什麼選擇FortiCNAPP

# FortiCNAPP 提供雲端安全 事前預警 事中告警 事後分析應變

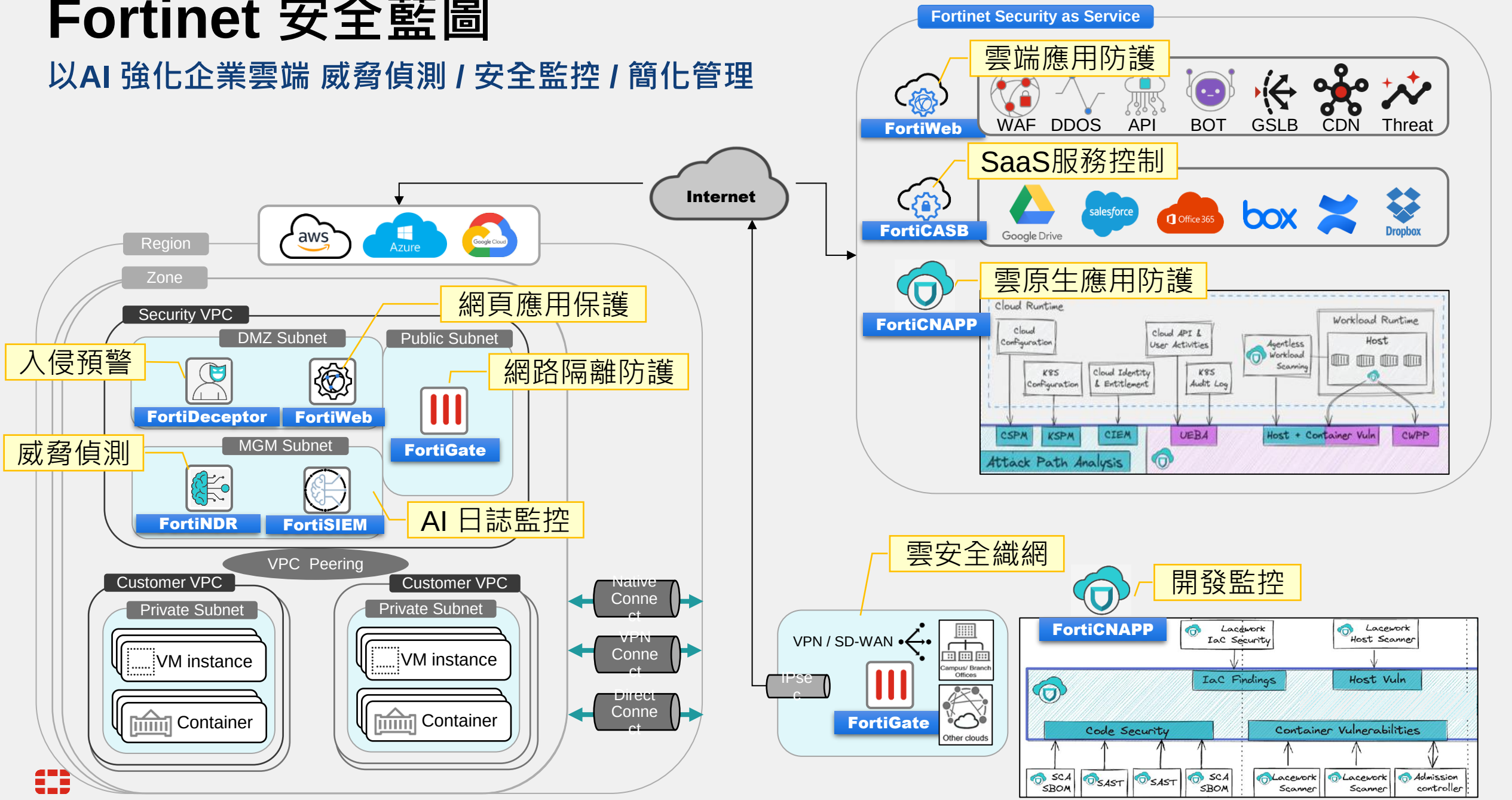
## 協助企業降低雲端安全風險



# Fortinet 安全藍圖

## 以AI 強化企業雲端 威脅偵測 / 安全監控 / 簡化管理




FORTINET