

# Cloud Risk Management



## 資安團隊需要全盤掌握才能有效控制風險

今日的雲端環境不僅複雜、而且經常橫跨多家供應商和服務，此時若缺乏整合的可視性，企業將必須面對零散的資安工具、應接不暇的組態設定錯誤警報、有限的環境情境洞見，以及潛藏的雲端曝險，而這一切都會帶來嚴重的資安風險。

Trend Vision One™ Cloud Risk Management 能讓您徹底改變作法，這套全方位解決方案能整合多重雲端環境的可視性，讓團隊從被動移轉至主動式雲端防護，並且為企業提供聰明的風險優先次序判斷與引導式矯正。

## 零散的雲端防護時代已經結束

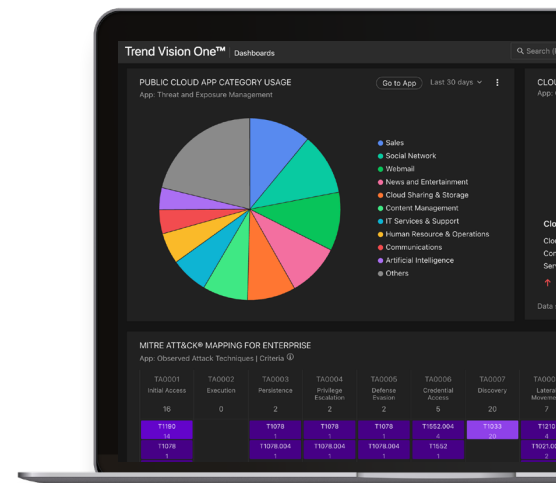
凡是無法在環境當中看到的，雲端團隊就無法為其提供防護，Cloud Risk Management 讓雲端團隊達成以下目標：

- 即時、完整掌握下列項目的可視性：
  - 雲端工作負載
  - AI 資產
  - 組態設定
  - 虛擬機器
  - 身分
  - 資料儲存
  - API
  - 資料庫
  - AI 基礎架構
  - 容器叢集
- 發掘影子資產、漏洞與組態設定錯誤。
- 立即採取行動來改善
- 資安與合規。
- 利用業務情境來量化雲端風險。



## 進一步掌握雲端的狀況

持續發掘、評估及防範雲端風險，縮小攻擊面，強制落實最佳實務原則，並且建立雲端韌性。



## 透過單一解決方案來全盤掌握雲端風險



### 整合式多重雲端可視性與控管

即時掌握雲端資產、組態設定以及身分的情境洞見，涵蓋 AWS、Azure、GCP、Alibaba 和 OCI 環境。



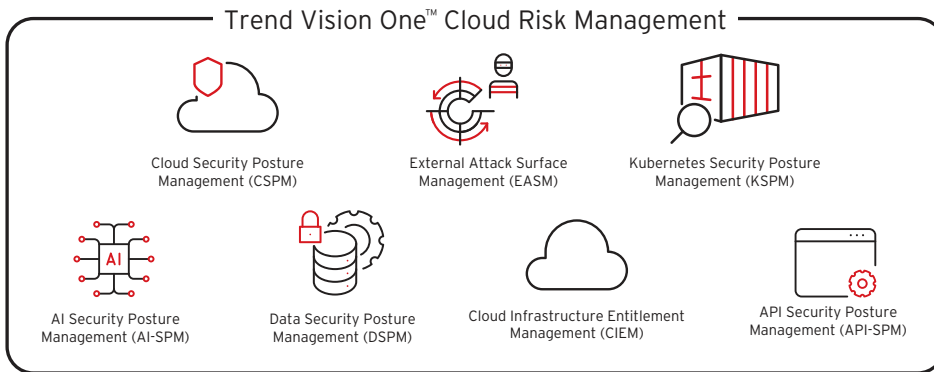
### 以智慧優勢對抗風險

- 以 Trend Cybertron 為後盾 (業界首創的主動式網路資安 AI)
- 全球威脅情報整合
- 1,000 多項資安規則檢查
- 預判式攻擊路徑分析
- 風險導向的優先次序判斷演算法
- 涵蓋所有框架的持續性合規監控



### 領先業界的雲端防護整合

取代多種雲端防護工具：



### 全方位的雲端風險管理方法

將零散的工具與局部的檢視整合成一套強大、容易使用的解決方案。

將以下項目的可視性、風險情報與防範功能整合在一起：

- 多重雲端環境
- 基礎架構程式碼
- 容器工作負載
- 無伺服器功能
- API 閘道
- AI/ML 服務
- 資料儲存庫



雲端態勢工具是協助我們釐清組態設定錯誤的關鍵，也有助於確保我們符合 HIPAA、HITRUST 以及 NIST 網路資安框架的要求。

Andrew Adams 博士  
資訊安全副理，  
Xsolis



獲選為 IDC MarketScape 領導者：全球雲端原生應用程式防護平台 2025 年廠商評估 (Worldwide Cloud-Native Application Protection Platform 2025 Vendor Assessment)



趨勢科技融合了整個攻擊面的主動與被動雲端防護，提供策略性優勢來防範資安威脅。

IDC MarketScape: Worldwide CNAPP, #US53549925 2025 年 6 月



## 主動式雲端防護就從這裡開始

Trend Vision One 是唯一集合下列功能的企業網路資安平台：

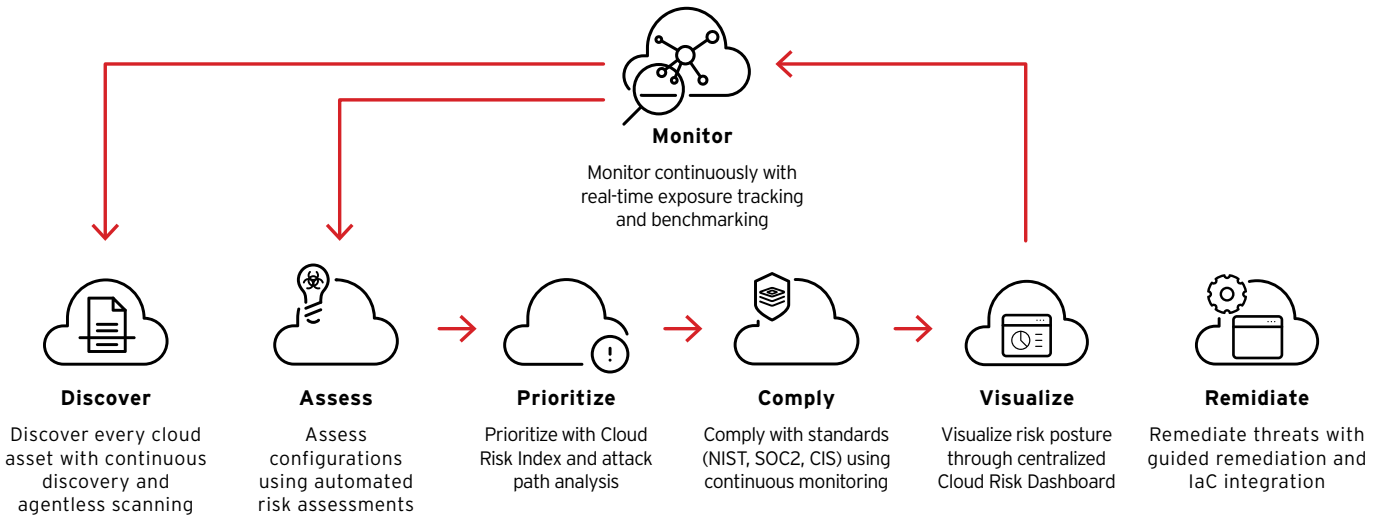
- ✓ 雲端風險管理
- ✓ 資安營運
- ✓ 多層式雲端防護

## Full CNAPP: One platform



Cloud Security = **CREM Cloud Risk Management** + **XDR for Cloud** + **Server & Workload Security** + **Container Security** + **File Security** + **Code Security**

|                          |                                  |       |                             |                          |                             |                                    |
|--------------------------|----------------------------------|-------|-----------------------------|--------------------------|-----------------------------|------------------------------------|
| Hybrid and Multi-Cloud   | ASM                              | XDR   | CWPP                        | <b>Pre-Runtime</b>       | SDK                         | Secret scanning                    |
| 3rd-Party Integrations   | CSPM                             | CDR   | Intrusion Prevention        | Container Image Scanning | Virtual Appliance           | Malware scanning                   |
| Organization Integration | EASM                             | AI-DR | Log Inspection              | Vulnerability Scanning   | Cloud Storage               | IaC / Template Scanning            |
| Terraform Support        | Attack Path Analysis             |       | Integrity Monitoring        | Malware Scanning         | Storage                     | Detect Open-Source Vulnerabilities |
| Trend Companion (GenAI)  | Agentless Vulnerability Scanning |       | Threat Hunting              | Secret Scanning          | Containerized Scanner       | Vulnerability Scanning             |
|                          | Agentless Malware Scanning       |       | Behavior Monitoring         | <b>Runtime</b>           | Predictive Machine Learning |                                    |
|                          | API Risk Visibility              |       | EDR                         | KSPM                     |                             |                                    |
|                          | CIEM                             |       | Anti-Malware Scanning       | Malware Scanning         |                             |                                    |
|                          | AI-SPM                           |       | Predictive Machine Learning | Vulnerability Scanning   |                             |                                    |
|                          | DSPM                             |       | Application Control         | Policy Enforcement       |                             |                                    |
|                          |                                  |       | Device Control              | Container DR             |                             |                                    |
|                          |                                  |       |                             | Runtime Scanning         |                             |                                    |



## 主要應用情境

### 攻擊路徑預測

發掘組態設錯誤或漏洞，將外部入侵點到關鍵內部資產的潛在攻擊路徑視覺化，例如：權限過度寬鬆的 IAM。

### 無代理程式的漏洞與威脅偵測

發掘並評估您整個雲端基礎架構的資安風險，無須花費力氣在每一套系統上部署及管理代理程式。避免對營運系統造成效能衝擊，確保所有動態環境都獲得一致的防護。

### 以智慧優勢對抗風險

獨家取得 Zero Day Initiative (ZDI) 漏洞懸賞計畫的研究與漏洞情報，在攻擊管道遭到廣泛利用之前預先掌握，實現主動式防禦策略，對整個雲端環境做出明智的資安決策。

### 整合多重雲端的防護管理

藉由單一平台來整合 AWS、Azure、GCP、Alibaba 及 OCI (即將推出) 環境的可視性與控管，消除管理多重雲端防護工具的複雜性，為所有雲端廠商提供一致的防護政策。

### 加速雲端合規

達成並維持產業標準合規狀態 (NIST、SOC2、CIS、GDPR)，透過持續監控、自動化合規報表，以及即時的矯正指引來縮短稽核準備時間並確保持續遵守規範。

### 保護雲端轉型計畫

將資安融入 CI/CD 流程、掃描基礎架構程式碼範本，讓開發人員在部署之前獲得立即的回饋來掌握資安風險，進而實現安全的 DevOps 實務。

### 管理雲端身分與存取風險

在各雲端環境實施最低授權的存取原則，發掘過度授權的身分、未用到的權限，以及可能導致資料外洩或未授權資源存取的危險存取模式。

### 保護 AI 和資料資產

採用特化的防護狀況管理解決方案來保護 AI/ML 工作負載和敏感的資料儲存庫，偵測雲端環境當中的組態設定錯誤、資料曝險，以及 AI 特有的資安漏洞。

### 超越雲端：整合式資安風險管理

Trend Vision One™ Cyber Risk Exposure Management 提供了一套完整的資安風險管理方法，包括：持續發掘資產、利用 AI 預測威脅、在情境中量化風險、整合漏洞情報、合規自動化，以及聯合矯正，讓資安團隊有能力管理整個攻擊面的風險。

| 功能                 | 說明  |
|--------------------|---|
| 雲端資安態勢管理 (CSPM)    | 監控、保護及維持多重雲端環境的合規狀態。                            |
| 外部攻擊面管理 (EASM)     | 發掘並監控暴露在外的雲端資產與影子資源。                            |
| 雲端基礎架構權限管理 (CIEM)  | 管理身分與權限，強制實施最低授權存取。                             |
| AI 資安態勢管理 (AI-SPM) | 保護 AI 基礎架構並偵測 AI 相關的組態設定錯誤。                     |
| 資料資安態勢管理 (DSPM)    | 保護雲端環境與 AI 工作流程的敏感資料。                           |
| API 資安態勢管理         | 評估 API 的風險，包括認證與授權漏洞。                           |
| 基礎架構程式碼 (IaC) 掃描   | 分析 CI/CD 流程中的範本來發掘資安風險。                         |
| 攻擊路徑分析             | 尋找雲端各層次可利用的攻擊路徑，並判斷其優先次序。                       |
| 無代理程式的漏洞與惡意程式偵測    | 無須在資源上安裝代理程式即可偵測漏洞和惡意程式，而且不影響效能。                |
| 專案檢視               | 透過集中化檢視來查看雲端專案以及所有相關的雲端風險，包括：資料、身分、API 和 AI 資產。 |
| 合規監控               | 針對各種合規框架建立自動化控管。                                |
| 風險導向的優先次序判斷        | 根據業務衝擊與可攻擊性來智慧評分。                               |
| 多重雲端資產盤點           | 取得 AWS、Azure 及 GCP 的全方位可視性。                     |
| 即時曝險監控             | 持續追蹤防護狀況的變化。                                    |
| 引導式矯正              | 取得逐步的指引來修正已發現的風險。                               |

## 關於趨勢科技

趨勢科技為網路資安全球領導廠商，致力建立一個安全的資訊交換世界。憑藉著數十年的資安專業、全球威脅研究以及持續不斷的創新，Trend Vision One 企業網路資安平台運用 AI 來保護全球數十萬家企業機構及數百萬一般使用者，涵蓋雲端、網路、裝置及端點。[TrendMicro.com](https://www.trendmicro.com)

©2025 年版權所有。趨勢科技股份有限公司保留所有權利。Trend Micro、Trend Micro 標誌、t 字球形標誌及 Trend Vision One 是趨勢科技股份有限公司的商標或註冊商標。所有其他公司和產品名稱為該公司的商標或註冊商標。本文件之內容若有變動，恕不另行通知。Trend Micro、Trend Micro 標誌與 t 字球形標誌註冊於美國專利與商標局。[SB00\_Solution Brief\_Cloud Risk Management\_250829TW]

如需有關我們蒐集哪些個人資料的詳細內容和理由，請參閱我們的網站上的「隱私權聲明」：[trendmicro.com/privacy](https://www.trendmicro.com/privacy)

申請免費 30 天試用  
[TrendMicro.com/trial](https://www.trendmicro.com/trial)