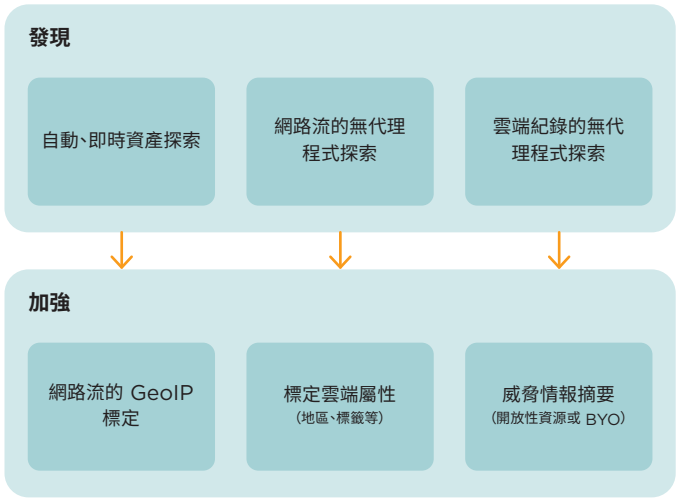
FIREEYE™

產品型錄

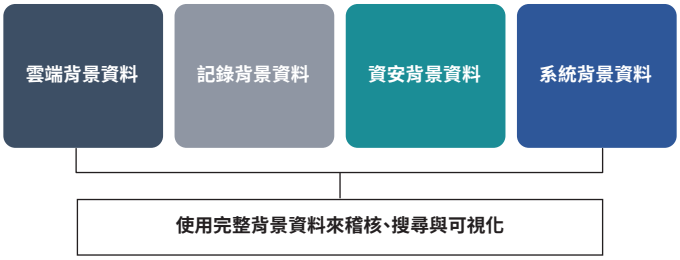
Cloudvisory

透過深度可視性、持續合規性和情報管理，提供多雲端工作負載資安性



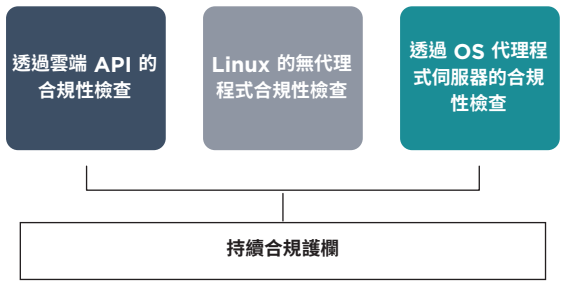
可視性

持續發掘與定位在公共與私人雲端間的企業資產、資安控制和資安事件。機器學習利用語境來發現風險和威脅



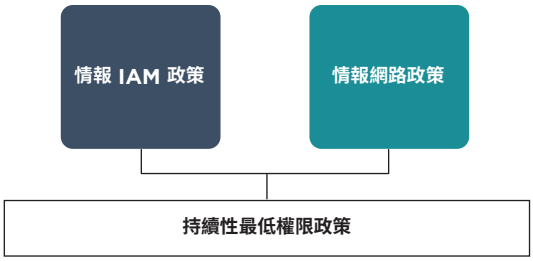
法規遵循

自動監測資安的合規性，內置 1300 多項檢查。最佳實踐、定制政策和框架的治理如 CIS、GDPR、HIPAA、NIST、PCI DSS 等。



管理

透過機器情報增加管理實踐。透過有效學習、測試、以及部署任何規模的情報最低權限政策，來減少攻擊面和防止入侵的能力。



公用雲端—Azure

可視性

帳戶,IAM 使用者/群組/角色,地區,資源群組,服務,訂閱,子網路。

已探索之工作負載

AKS Pod、應用程式服務、應用程式服務環境、Cosmos、DB 帳戶、DNS 區域、功能、負載平衡器、Redis Cache、服務架構叢集、儲存帳戶、虛擬機台等……

公用雲端—AWS

可視性

帳戶、IAM 使用者/群組/角色、地區、服務、子網路、VPC。

已探索之工作負載

EC2 執行個體、EFS 系統檔案、EKS Pods、彈性負載平衡器、Kineses 串流、Lambda 功能、NAT 網閘、RDS 叢集、Route53 代管區、S3 容器、SNS 標題等……

私人雲端—OpenStack

可視性

叢集、執行個體、Keystone 控制閥件、網路、項目(租用戶)、地區服務。

為 OpenStack(Nova)執行個體和 Kubernetes Pods 探索、分析和管理網路資安群組。監控網路流量,近乎實時地檢測威脅。

私人雲端—Kubernetes

可視性

叢集、部署、識別使用者/群組/角色、Namespaces、網路、Pods。

傳統資料中心

作業系統

- Ubuntu Linux
- Redhat
- CentOS

自動整合

外部(第三方)系統

自動化、可配置的警示、資安事件的紀錄分析(如:SIEM、Elasticsearch)、API 啓動/以事件為主的合規性掃描與回報、記錄日誌以獲取其他資安事件來源(如:傳統網路裝置、身分提供商)。

Gartner Cool Vendor 2018

在《2018 年網路資安性》中,Cloudvisory 被提名為 Gartner Cool Vendor。

CIO APPLICATIONS TOP 25 AMAZON SOLUTION PROVIDERS-2017

Cloudvisory 被 CIO Applications 評為亞馬遜解決方案供應商 25 強之一。

AICPA SOC

Cloudvisory-SaaS 獲得 SOC2 獨立認證。

若要瞭解更多有關 Cloudvisory 的內容,請參閱: **www.FireEye.com/cloudvisory**

FireEye Taiwan | 台灣火眼有限公司
| 10683 台北市信義路四段 6 號 6 樓
+886 2 5551 1268 | FIREEYE |
taiwan@FireEye.com

關於 FireEye, Inc.

FireEye 是一間情報主導的資安公司。作為客戶資安監控的無縫、可擴充的延伸,FireEye 提供單一平台,將創新的資安技術、國家級別的威脅情報和世界知名的 Mandiant® 諮詢融合在一起。藉由此方法,FireEye 為那些正在努力準備、預防和應對網路攻擊的組織,消除資安機制的複雜性和重擔。

FIREEYE™