HCLSoftware

HCL AppScan On Cloud

Managed On Cloud SaaS Service
Fast, Accurate, Agile
Security Testing

Kevin Chia (CEH / ISO 27001 LA)
Application Security Technical Advisor
Greater China / Japan / ANZ

HCL Software Pillars

We deliver software that fulfils the transformative needs of clients around the world.

Digital Transformation

我們通過技術為您的客戶、員工和利益相關者改變體驗，為您的數字+經濟之旅提供動力

AI & Automation

人性化人工智慧來解決現實世界的問題是業務增長的關鍵。 AI 將有助於在每個企業的 DNA 層面推動智能決策。

Data & Analytics

數據為雄心勃勃的智慧組織提供了動力。 我們讓飛機保持在空中，讓供應鏈保持運轉，每天處理數十億筆交易

Enterprise Security

從應用程式到端點的安全性。 漏洞檢測、緩解和補救——攻擊前、攻擊中和攻擊後

企業安全

從應用程式到端點的安全性。

弱點檢測、弱點修補——攻擊前、攻擊中和攻擊後

100百萬
每天保護端點

98%
更快的弱點修復

100
不同的操作系統
託管

1.5M
每小時掃描的代碼行數

63%
掃描報告高或中漏洞

98%
減少SAST安全測試誤報

2024 安全趨勢

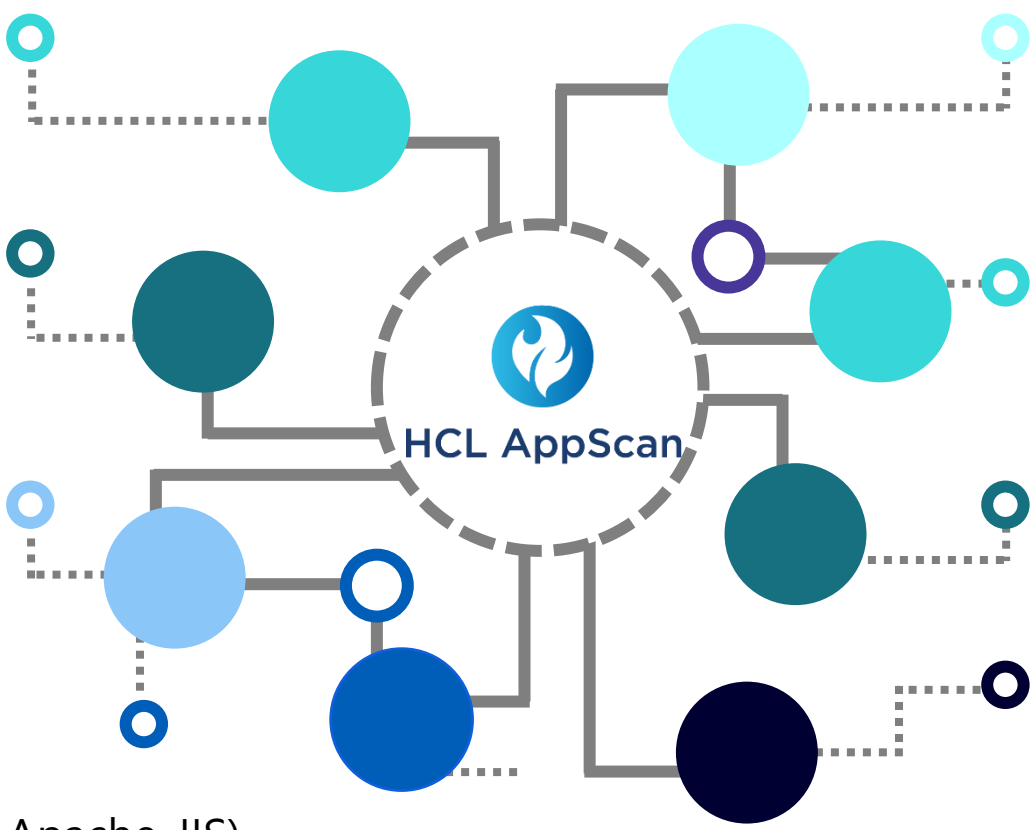
技術

Open API / Graph QL

Container / Docker

開源軟體
(BootStrap, JQuery)

伺服器
(Tomcat, Apache, IIS)



管理

Secure DevOps

API Secret

生命開發週期(SDLC)

法令法規遵循
ISO 27001:2022
GDPR
NIST
OWASP Top 10
CWE Top 25

HCL AppScan

具有 360° 可視性的完整 AppSec 平臺

靈活的體驗

- 開發人員
- DevOps人員
- 資安人員

生態系統

- IDE
- CI/CD
- DTS
- SCM
- Robust API

部屬方式

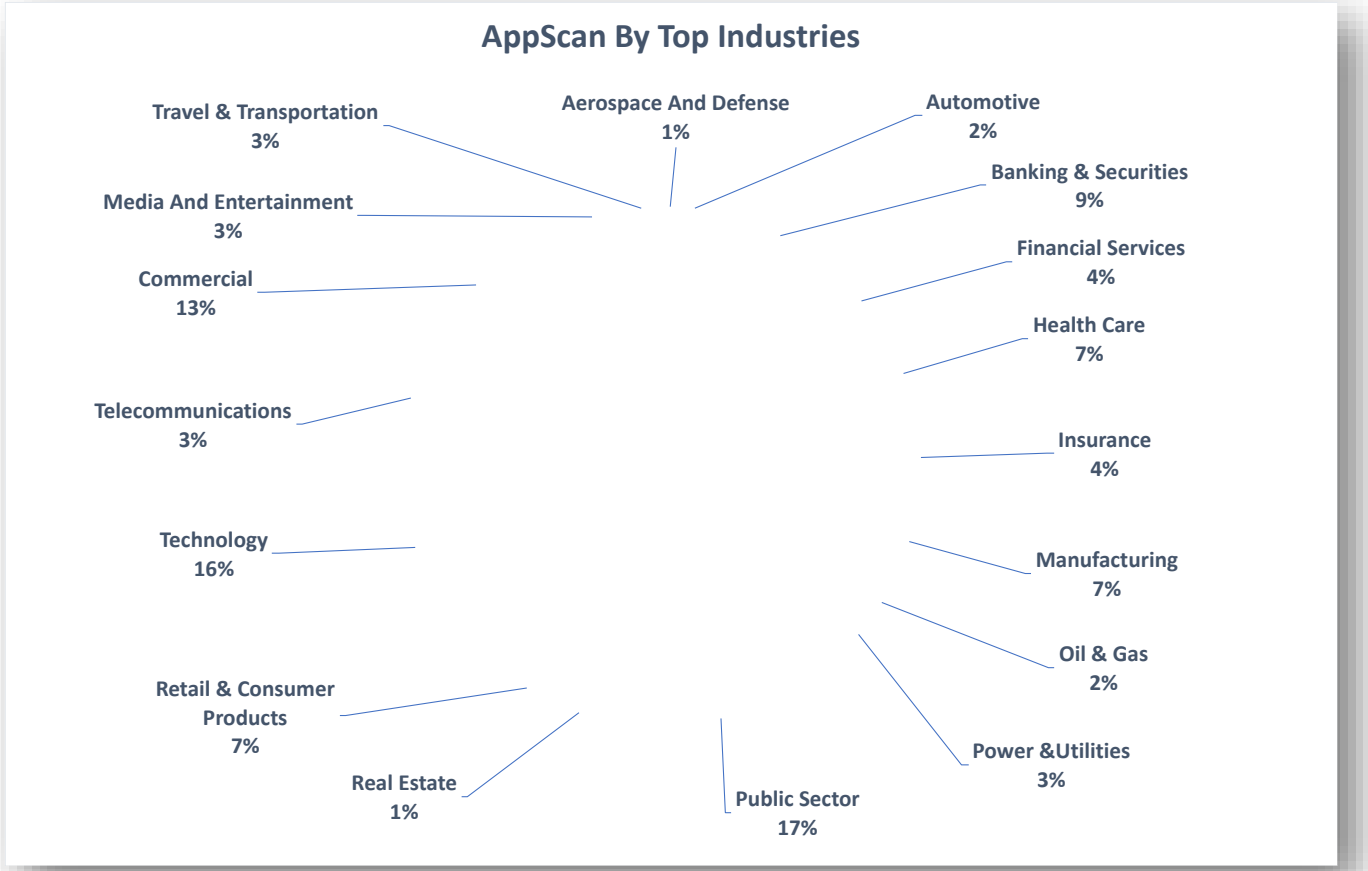
- 雲端 (SaaS)
- 地端
- 混合Hybrid
- MSP

服務

- **AppScan for You**
  個人化諮詢服務
- **Advanced Technical Services**
  工作坊、培訓和顧問服務
- **AppScan On Demand**
  全面託管服務

HCL AppScan: The Difference It Makes

自 AppScan 成為 HCL 的一部分以來，已有 250 多個新客戶選擇我們的產品



“它 (AppScan) 使我們能夠確保我們的開發人員多年來通過培訓克服的安全開發挑戰真正應用於我們的應用程式.”

IT Security Domain Architect at Progressive Insurance

HCL AppScan 被 6000 多個客戶和 80 多個行業使用

HCL AppScan 的優勢

痛點

- ❑ 在開發生命週期中無法保護跨越不同環境的大規模應用程式，導致部署延遲和成本增加。
- ❑ 手動弱點檢測，延遲項目部署和開發發布週期。
- ❑ 當前的安全軟體是一種通用的解決方案。 無法依據合規性法規進行增長、擴展和發展，從而導致潛在的弱點。
- ❑ 團隊之間缺乏跨職能協作導致政策制定和測試延遲。

AppScan 如何提供幫助

- ✓ **通過敏捷的應用程式安全測試，在開發生命週期的每個階段檢測和修復應用程式弱點。**
- ✓ **HCL AppScan 是一套應用程式安全掃描解決方案，有助於加快 DevSecOps 並縮短修補時間。**
- ✓ **通過風險管理儀表板提供可擴展的應用程式安全測試，從而實現對風險和合規性的可見性。**
- ✓ **使安全和開發團隊能夠在整個應用程式生命週期內協作、制定策略和擴展測試。**

應用程式安全趨勢

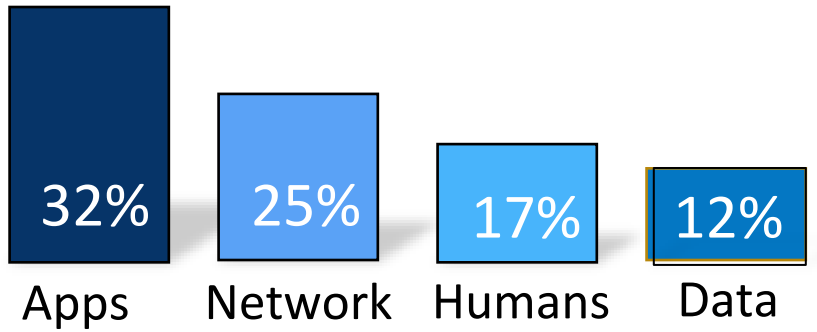
98% 的應用程式至少有 1 個 CVE [1]

修復對外服務的弱點的平均時間（天）[2] **85**

63% 安全性漏洞是由於技術不足和過時造成的 [3]

應用程式安全支出的年增長率 [4] **25%**

- 應用程式序安全是 CISO 關注的第一大領域
  （接受調查的 630 家公司）



- 應用程式外洩平均造成 3.6億新台幣的損失，外加聲譽/品牌損失 [5]

2 | Ponemon Institute Report pg32 3 | Ponemon Institute Report pg31 4 | Ponemon Institute Report pg20 5 | Ponemon Institute Report pg2

常見客戶問題

合規

外部法規和內部政策要求

- 我的業務風險在哪裡？
- 如何訂製應用程式安全的內部規範要求？
- 我的私人/敏感資料是否被應用程式洩漏？
- 如何檢查和證明應用程式合規性？

創新

應用程式

版本和技術的快速增長

- 我們如何在不減慢流程/業務的情況下，在快速 DevOps/Agile 中測試應用程式的安全性？
- 我們如何降低成本並在生命週期的早期發現安全問題？

資源

小型安全團隊

大量應用程式

- 我們如何為我擁有的資源確定工作的優先順序？
- 我們應該測試什麼以及我們如何測試？
- 我們如何配置員工並提高技能和意識？

AppScan 進行應用程式安全測試的類型

您的AppSec 程式能完成哪些？

靜態掃描 原碼檢測
Static Analysis (SAST)

WHAT: 程式碼

WHY: 快速、早期發現

動態掃描 網站弱掃
Dynamic Analysis (DAST)

WHAT: 網頁應用程式

WHY: 低誤判,發送實際攻擊

軟體成分分析
Software Composition Analysis (SCA)

WHAT: 協力廠商開源套件(ASoC)

WHY: 識別具有弱點之協力廠商套件

互動式分析
Interactive Analysis (IAST)

WHAT: 即時監控應用程式

WHY: 部屬簡單, 即時顯示弱點

保護您的開發與應用 – HCL AppScan

HCLSoftware

使用AI測試應用程式從開發到營運的安全弱點

SCA: 開源軟體
Software Composition Analysis

搜尋並分析您使用的開源和第三方軟體

SAST: 源碼檢測
Static Application Security Test

在開發、實作和編譯的每個階段分析應用程式程式碼

IAST: 交互式分析
Interactive Application Security Test

監控和分析 Web 應用程式 在 QA 測試和預發布生產環境測試中執行

DAST: 網頁弱掃
Dynamic Application Security Test

分析在即時和營運生產環境中進行的 Web 應用程式 QA 測試、預發布生產環境測試

小團隊

源碼檢測

網頁弱點掃描

HCL AppScan Source

HCL AppScan Standard

地端部屬

CI/CD integration

HCL AppScan Source For Automation

HCL AppScan Enterprise

全企業

HCL AppScan on Cloud

雲端部屬

使用 AI 向左偏移 守護資訊安全與開發安全

ICA (Intelligent code analytics)

確定新 API 和框架的安全影響

IFA (Intelligent findings analytics)

顯著減少（分類）SAST 中出現的許多誤報、噪音和誤報

自動關聯性群組

將 IAST 中檢測到的問題與 SAST 和 DAST 問題進行匹配，以識別相關性

弱點群組化

提供可以覆蓋多個漏洞的修復程序

AppScan的技術能力 (DAST)

動態掃描 網站弱掃 Dynamic Analysis (DAST)

Dynamic application security testing (DAST)

技術在測試或運行階段分析應用程式的動態運行狀態。

它模擬駭客行為對應用程式進行動態攻擊，分析應用程式的反應，從而確定該Web應用是否易受攻擊。

產品:

ASE

AppScan Standard

ASoC

AppScan的技術能力 (SAST)

靜態掃描 原碼檢測 Static Analysis (SAST)

Static application security testing (SAST)

技術通常在編碼階段分析應用程式的原始碼或二進位檔的語法、結構、過程、介面等來發現程式代碼存在的安全性漏洞。

產品:

AppScan Source

ASoC

AppScan的技術能力 (IAST)

互動式分析 Interactive Analysis (IAST)

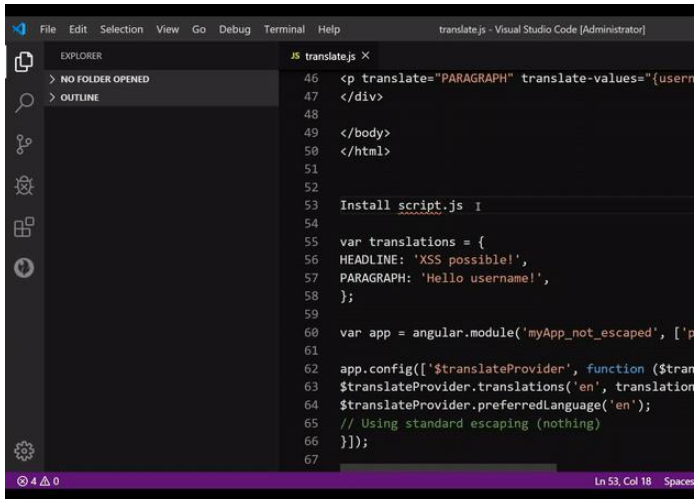
Interactive application security testing (IAST)
通過代理、VPN或者在服務端部署Agent程式，收集、監控Web應用程式運行時函數執行、數據傳輸，並與掃描器端進行實時交互，高效、準確的識別安全缺陷及漏洞，同時可準確確定漏洞所在的代碼檔、行數、函數及參數。IAST相當於是DAST和SAST結合的一種互相關聯運行時安全檢測技術。

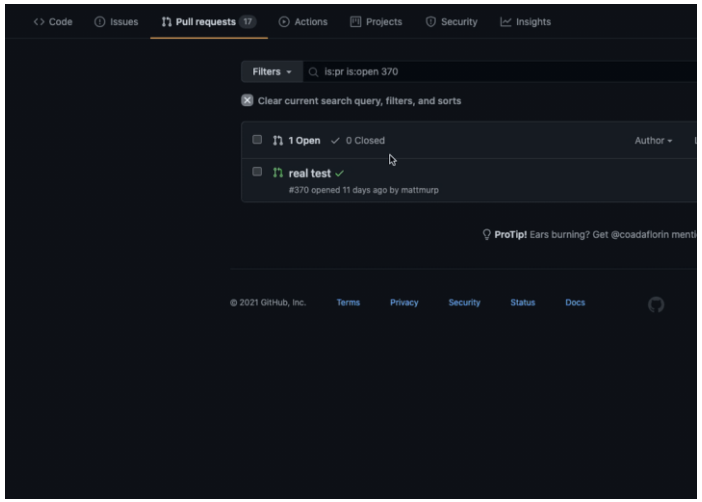
產品:

ASE　ASoC

HCL AppScan: For Developers

"Shift Left" with CodeSweep





IDE 中的安全性

輕鬆瀏覽資訊安全資訊

——即使是在編寫代碼時

修復建議 – 在上下文中

在代碼更改的同時提供修復

開發人員充滿信心地交付專案

提交前掃描，解決問題並更好地確保安全交付

誰從 HCL AppScan 中受益

	開發人員	Build Engr/ DevOps	QA	資訊安全	維運
地端 **AppScan Standard** DAST				DAST • Point-& Shoot Scans • Auto explore/crawl • Smart Scans • Actions-based Scans • Penetration Testing	
地端 **AppScan Source** SAST **AppScan CodeSweep**	SAST • CodeSweep • IDE Scans • Incremental Scans	SAST • Automation • Build Integration		SAST • Deep Code Audit • Tool assisted review	
地端 **AppScan Enterprise** DAST, IAST	DAST • Smart Scans • Actions-based Scans	DAST • Automation plug-ins • Smart Scans • Point-& Shoot Scans • Auto explore/crawl	DAST IAST • Functional Testing Scans • Action-based Scans	DAST • Point-& Shoot Scans • Auto explore/crawl • Smart Scans • Actions-based Scans	IAST • Security Telemetry
雲端 **AppScan on Cloud(ASoC)** DAST, SAST, SCA, IAST	SAST DAST SCA Open Source	SAST DAST SCA Open Source	IAST DAST	SAST DAST SCA Open Source	IAST • Security Telemetry

30+ Supported Code Languages & Growing

我們投資於您的成功。

HCL AppScan 在應用程式安全行業擁有超過 20 年的經驗，提供應用程式安全市場中最大的支援語言列表之一。

HCL AppScan

hcltechsw.com/AppScan