宏虹
HONGHONG

宏虹電子 ONEKEY

固件安全合規平台

高效管理產品網路安全與合規性

宏虹電子 ONEKEY
固件安全合規平台
高效管理產品網路安全與合規性

引言

在全球數位化浪潮下，嵌入式產品面臨日益嚴峻的安全挑戰。企業既要確保產品符合嚴格的安全合規標準，又要應對軟體物料清單（SBOM）生成與管理的高難度技術壁壘，同時還需持續投入資源進行通用漏洞披露（CVE）匹配和評估。傳統手動測試方式效率低下、成本高昂，加之法規要求不斷升級，使企業陷入資源緊張、成本高企的困境。

為此，ONEKEY 提供了高效解決方案：透過自研固件提取套件自動生成 SBOM，精準掌握軟體組件資訊；採用雙重漏洞匹配模式結合自動化分析，顯著提升漏洞處理效率；其獨有的自動影響評估功能，能基於組件版本和使用情況智能判斷漏洞可利用性，幫助企業優先修復關鍵漏洞，實現資源最優配置。

ONEKEY 平台概述

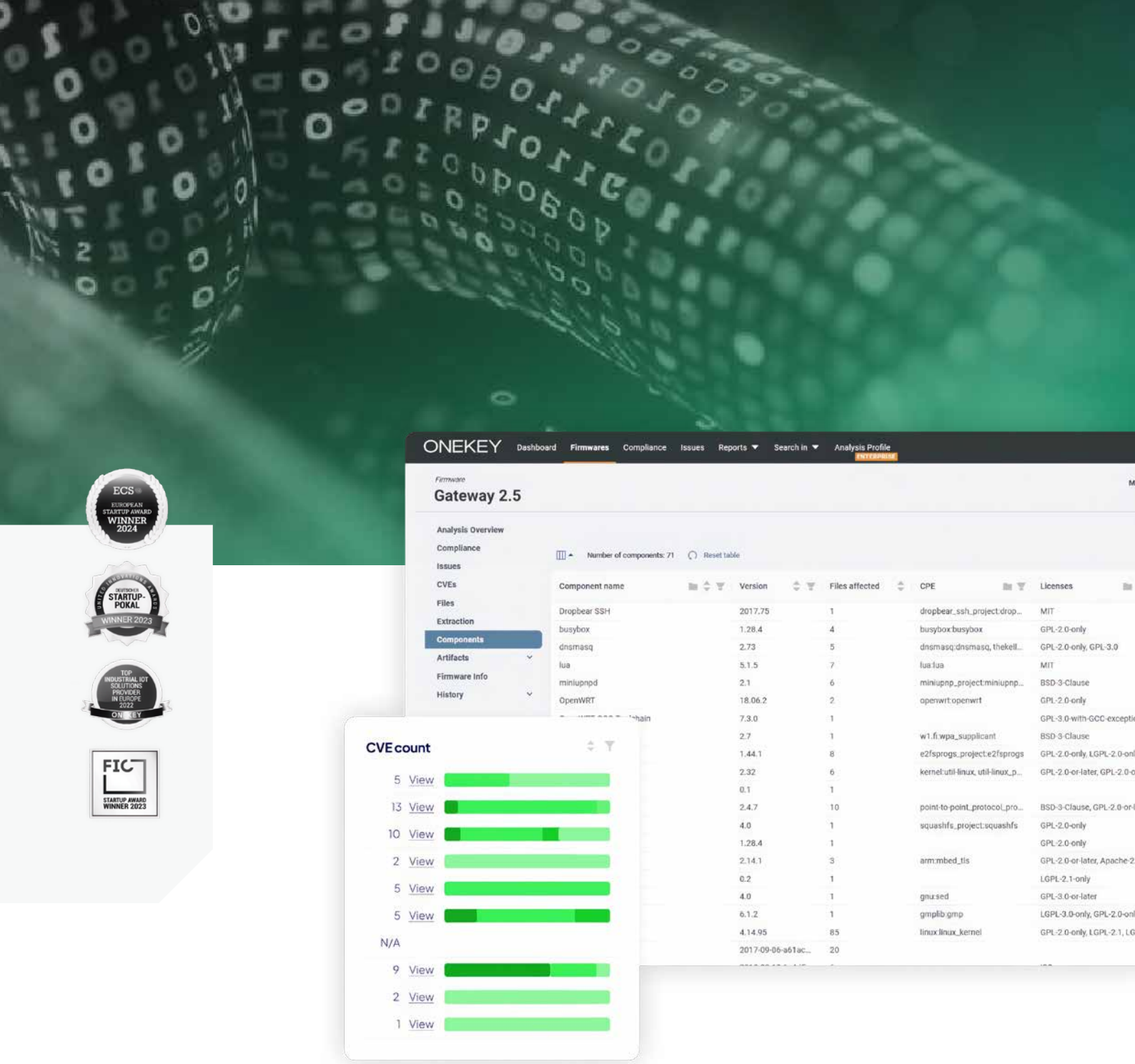
ONEKEY 平台專注於在全產品生命週期內自動化分析設備安全與合規

自動化檢測設備安全

- ✓ 作為市場上高效的自動化固件分析工具之一，具備同類工具中最低的誤報率，為設備安全檢測提供可靠保障

專為快速實現投資回報而設計

- ✓ 為不同角色的使用者提供極具吸引力的工具與服務：向開發者開放 API 介面，便於集成開發；為管理人員配備直觀的儀表板，助力高效決策；為合規部門生成合規報告，滿足合規管理需求
- ✓ 能夠輕鬆檢測任何第三方聯網設備的固件安全狀況，降低安全檢查門檻



全面支持合規

- ✓ 配備歐盟資助的 CRA 合規向導，為企業合規工作提供專業指引
- ✓ 提供全流程合規支持，從設備固件的基礎分析起步，到最終達成 CRA 等國際法規的合規標準，覆蓋合規工作的各個環節

行業領先的技術

- ✓ 擁有一支資深網路安全專家團隊，具備服務大中小企業的豐富經驗，精準應對不同規模企業的安全需求
- ✓ 憑藉深厚的技術積累，在行業內形成領先優勢，為企業提供高品質的安全解決方案

典型應用場景

設備製造商應用場景

1. 設計階段
對第三方二進位元組件開展全面安全與合規核查

2. 開發階段
整合原始碼、構建及部署環節的 SBOM，校驗形成完整統一的物料清單；針對已編譯的預發布軟體持續實施安全性與合規性檢測，為 SBOM 驗證及漏洞評估提供支撐

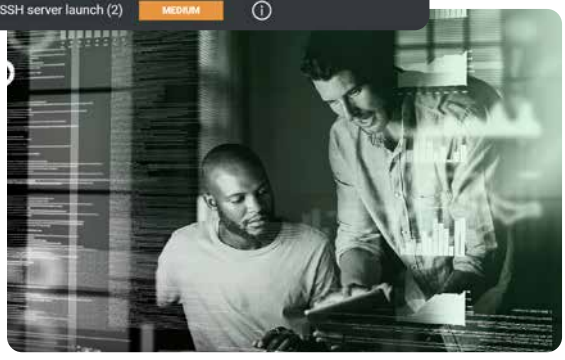
3. 生產階段
支持開展自我評估或申請相關認證

4. 終止階段
在產品全生命周期內，為PSIRT（產品安全事件響應團隊）提供 7×24小時不間斷的漏洞與合規監測服務；為已達生命周期終點（EOL）的產品提供風險及漏洞狀態資訊，助力企業降低 EOL 產品的法律責任風險

關鍵功能模組解析

SBOM 生成與管理

- ✓ 支援一鍵生成詳盡的軟體物料清單（SBOM）概覽，兼容從二進位映像到 CycloneDX、SPDX 等主流格式，滿足多樣化的格式需求
- ✓ 可從原始碼及構建過程中導入 SBOM 並完成驗證，同時具備對 SBOM 的編輯、合併、豐富及校正功能，確保 SBOM 的準確性與完整性
- ✓ 能夠驗證第三方提供的 SBOM，將原始碼、構建及部署階段的 SBOM 整合校驗為完整統一的物料清單，同時實現對 SBOM 的全自動漏洞監控，提升漏洞管理效率



設備採購者應用場景

1. 採購階段

在採購環節或整合至自身基礎設施前，提前對含軟體的產品及組件進行預防性安全與合規檢查，實現對供應商網路安全與合規水平的量化評分

2. 生產階段

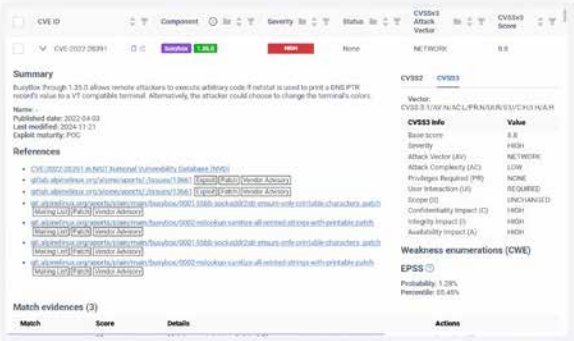
確保軟體構成資訊（SBOM）的透明性與即時更新，即便第三方提供的二進位檔案也能被全面覆蓋；針對固件實施符合 CERT 標準的 7×24 小時預防性漏洞監控，覆蓋設備全生命周期

3. 維護階段

在對現有設備進行更新前，對產品及其帶軟體的組件開展預防性安全與合規檢查，從而避免不必要的更新操作，減少設備停機時間

4. 終止階段

提供產品生命周期終止後的風險與漏洞狀態資訊，降低 EOL 產品的運營責任風險

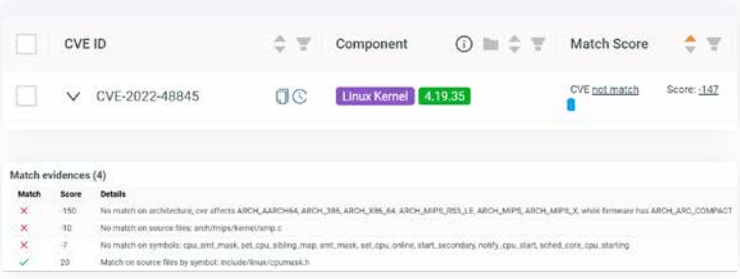


漏洞管理

- ✓ 基於 AI 的漏洞檢測，能在幾分鐘內完成二進位檔案的漏洞檢測
- ✓ 利用 SBOM 對二進位軟體組件進行分析，快速發現已知 / 未知漏洞
- ✓ 持續掌握 CVE 和零日漏洞的影響評估，幫助企業快速緩解風險，避免安全事故

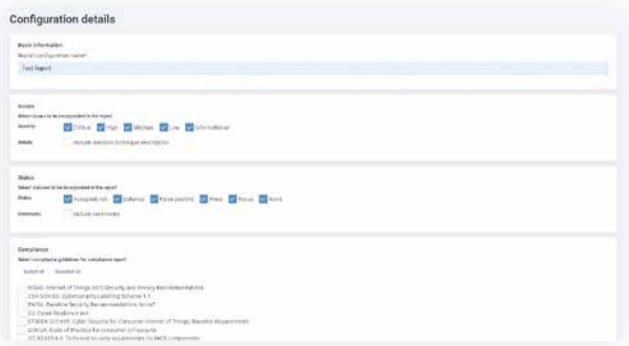
自動化影響評估

- ✓ 對 CVE 及零日漏洞進行自動分流，對關鍵威脅進行透明評分和優先級排序，減少超過 60% 的無影響漏洞，聚焦最關鍵的問題，節省時間和資源
- ✓ 自動掃描覆蓋 license、雲端存儲、攻擊向量、可利用性和依賴關係，提供附帶緩解策略的嚴重性報告



合規管理及報告生成

- ✓ 配備專利級虛擬助手，可實現合規檢查與自動化文件支持。該助手內建法規導航功能，能精準對接多項國際標準，包括歐盟《網路韌性法案》、IEC 62443、ETSI 303 645 等，為企業合規工作提供有力指引
- ✓ Compliance Wizard 將產品網路安全合規管理整合於統一平台，可實現固件合規性的自動化檢查，整個過程僅需數秒。同時，它能引導使用者應對複雜法規要求，為合規的每個環節提供證據支持與專業建議，顯著節省企業在合規、文件編制、自我證明及第三方認證等方面投入的時間與資源
- ✓ 支援靈活定制報告，使用者可根據需求自主選擇報告中需包含的問題嚴重級別，以及想要達成的合規標準，滿足多樣化的報告需求



不同版本參數對比

功能	專業訂閱	企業訂閱
基礎分析	✓	✓
軟體物料清單	✓	✓
漏洞管理	✓	✓
單點登錄	可選	✓

功能	專業訂閱	企業訂閱
配置文件分析	可選	✓
API Token	可選	✓
二進制零日漏洞分析	可選	✓
多域访问	不可選	✓

我們的客戶

部署方式

ONEKEY 提供兩種部署選項供使用者選擇：

- 若選擇訪問 ONEKEY 雲平台，服務將由位於德國、通過 ISO27001 認證的資料中心提供支援，確保資料安全與合規
- 針對具有高安全性需求的場景，ONEKEY 同樣提供本地部署方案，滿足使用者對資料本地化及更高安全級別的要求

客户案例

swisscom

初始情況

- Swisscom，瑞士的重要電信公司、最大的 IT 服務提供商之一，需求是確保客戶使用的物聯網設備的安全性
- 超過 180 萬台設備正在使用，並且需要進行韌體更新以確保安全
- 由於產品生命周期短且供應鏈複雜，物聯網設備製造商常常忽視安全性問題

ONEKEY 解決方案

- ✓ 將自動化的安全性和合規性分析整合到 Swisscom 的韌體測試流程中，每年分析超過 80 個韌體映像
- ✓ 及早發現關鍵漏洞，提供詳細的安全洞察和合規性檢查
- ✓ 透過揭示先前未知的安全問題，提高供應鏈的透明度

Swisscom 的收益

投資回報率（ROI）
防止帶有關鍵漏洞的韌體發布，每次避免的事件可節省高達 40 萬美元

加強供應商關係
透過基於事實的安全數據，提升與供應商的談判地位

運營效率
透過在發布前識別問題，降低維修和維護成本