用於企業基礎設施的供應鏈安全方案_

信任您的技術

大多數組織預設信任 IT 產品會以安全的方式開發和交付。然而，事實是您的 IT 基礎設施的每個部分都依賴於極其複雜的供應鏈。每個硬體、韌體和軟體元件都可能包含漏洞，甚至存在惡意的低階程式碼。

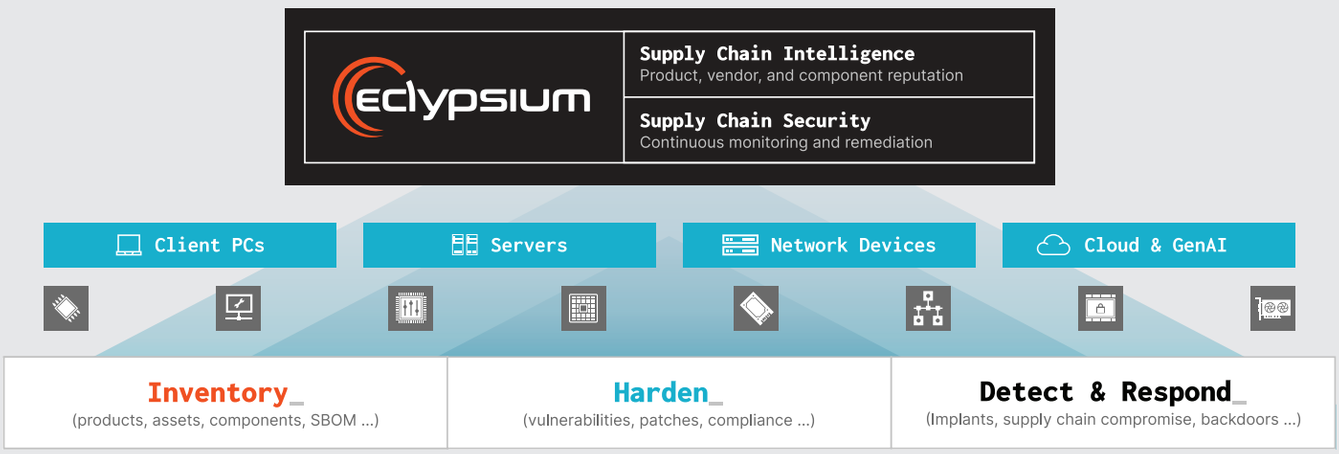
攻擊者利用供應鏈的複雜性，針對硬體、韌體和軟體元件中的漏洞發動攻擊。這類威脅能夠繞過端點偵測與回應 (EDR) 系統，並在修補漏洞或重新啟動後仍能保持持續性，最終可能導致嚴重的安全事件。

在購買 IT 產品之前，如何了解這些風險？接收到產品後，如何驗證所收到的產品是否與預期相符？一旦進入生產環境，如何持續監控並修復這些低階組件的風險？

> “鞏固您對IT的信任 基礎架構至關重要，但往往難以檢視且缺乏足夠的理解。Eclypsium 的供應鏈安全解決方案以簡便的方式有效解決了這些關鍵問題。”
>
> **Tim Lisko**, 安全工程資深總監
> DigitalOcean

用於企業基礎設施的供應鏈安全方案_

Eclypsium 供應鏈安全平台專注於保護硬體、韌體及軟體組件。透過 Eclypsium，您的 IT 團隊可以高效且便捷地部署關鍵安全控管，全面防禦底層威脅，包括資產盤點、漏洞管理及威脅偵測。



資產清單

動態資產清單管理 - 建立企業 IT 基礎架構的完整資產清單，涵蓋硬體、韌體和軟體層級的每個組件。

隨選生成 SBOM - 根據需求生成軟體物料清單 (SBOM)，包括設備的硬體和韌體元件。

評估產品風險 - 讓安全和採購團隊在購買前瞭解產品中固有的風險。

加強鞏固

優先處理基礎架構漏洞 - 深入了解硬體、韌體和軟體元件中的低階漏洞。

簡化合規性管理 - 追蹤硬體和韌體層級的問題，符合 NIST 800-53 等合規框架要求。

自動化韌體更新 - 設定排程並自動應用關鍵的韌體補丁。

偵測與回應

偵測繞過 EDR 的威脅 - 當發現植入程式及其他低階組件的攻擊跡象時發出警報，識別可能的不正當獲取。

防禦篡改與仿冒元件 - 驗證資產是否遭篡改，確保組件為正品，防範假冒或未授權的硬體和韌體。

與其他數據關聯 - 將警報發送至 SIEM (安全資訊與事件管理) 及 SOAR (安全自動化與回應) 系統，提供分析師更多的關聯資訊，以便做出更精確的反應。

AUTOMATA 二進制分析系統_

Eclypsium 平台搭載市場上最先進的二進制分析系統。Eclypsium Automata 承載了我們專業安全研究團隊的領域專業知識與逆向工程技術。重要的是，Automata 保持24/7 持續運行，並分析客戶環境中 100% 新的二進位檔案，有效防範先前未知的威脅、漏洞及錯誤配置。它採用了多種方法和機器學習模型，並具備擴展性，能夠處理數百萬個韌體和軟體二進位檔案，且不需要客戶進行任何操作。

用於企業基礎設施的供應鏈安全方案_

保護生產資產
在最基礎層次上改善企業 IT 的偵測平均時間 (MTTD) 並強化安全防護。

降低數位化供應鏈風險
協助企業做出更明智的 IT 採購決策，並迅速評估供應鏈威脅的影響。

降低硬體成本
透過基準化並偵測低階元件的變更，延長設備的使用壽命。

合規性管理
輕鬆實施設備完整性與韌體安全的安全控制措施，符合相關法規要求。

關於 ECLYPSIUM_

Eclypsium 的雲端平台為企業基礎設施中的關鍵軟體、韌體和硬體提供數位化供應鏈安全。Eclypsium 協助企業和政府機構降低複雜技術供應鏈對其基礎設施造成的風險。欲了解更多信息，請訪問 eclypsium.com。