Network Insight (Damballa):

自動化入侵防禦

Network Insight (Damballa)

讓資安團隊能夠：

- 確實辨識受害設備
- 迅速處理威脅
- 將最高風險的設備優先進行修復
- 阻斷活動中的入侵程式，直到處理完成
- 改善安全策略，以遏止對手未來成功的攻擊

Core Security 擁有寬廣的威脅偵測視野：

- 保護全球超過 10 億台企業裝置
- 檢視近 50% 的北美行動裝置上網流量
- 每天增加 220 億項資料庫記錄

快速偵測、回應並修復

如今威脅持續演進，防毒軟體、防火牆及沙箱等防禦工具已無法阻止前所未見的威脅。Network Insight (Damballa) 的獨特之處在於它彌補了入侵防禦與回應之間的差距。

Network Insight (Damballa) 是一種自動入侵防禦系統，能夠確實檢測受害設備、終結入侵行動、並提供安全團隊迅速防止損失所需的資源。Network Insight (Damballa) 提供關於已知和未知威脅的可操作資訊，涵蓋設備的受害來源、入口向量或作業系統。依據其提供明確證據，安全團隊能夠快速防止高風險設備發生的損失，同時阻斷其他災害行動。

自動發現進階威脅

威脅行動總有第一步，尤其是針對您的組織。Network Insight (Damballa) 透過以下措施自動發現進階威脅：

- 監控威脅行為和活動的網路流量
- 自動驗證哪些設備已被入侵
- 為每個感染設備設定風險等級
- 終止感染設備與威脅行動間的溝通管道

"為阻斷現今的進階威脅，首先您必須偵測它們。然而傳統的安全控制未能達成此項技術，這也正是 [Network Insight (Damballa)] 存在的理由。"

–某《財富》全球 500 大娛樂企業

遏止威脅取代追蹤告警

防禦裝置是必要的第一層防護。當其失效時，Network Insight (Damballa) 便能發現躲過防禦控制的受感染設備。Network Insight (Damballa) 並非依靠單一的檢測技術，而是透過以下方式確認入侵威脅：

- 瞭解設備的網路行為
- 分析封包內容
- 應用 Core Security 對惡意程式目的地、指令和控制通訊，以及威脅行為分析之智能系統

"被 [Network Insight (Damballa)] 辨識的受感染設備百分之百確實感染。"

–某全球家庭娛樂企業

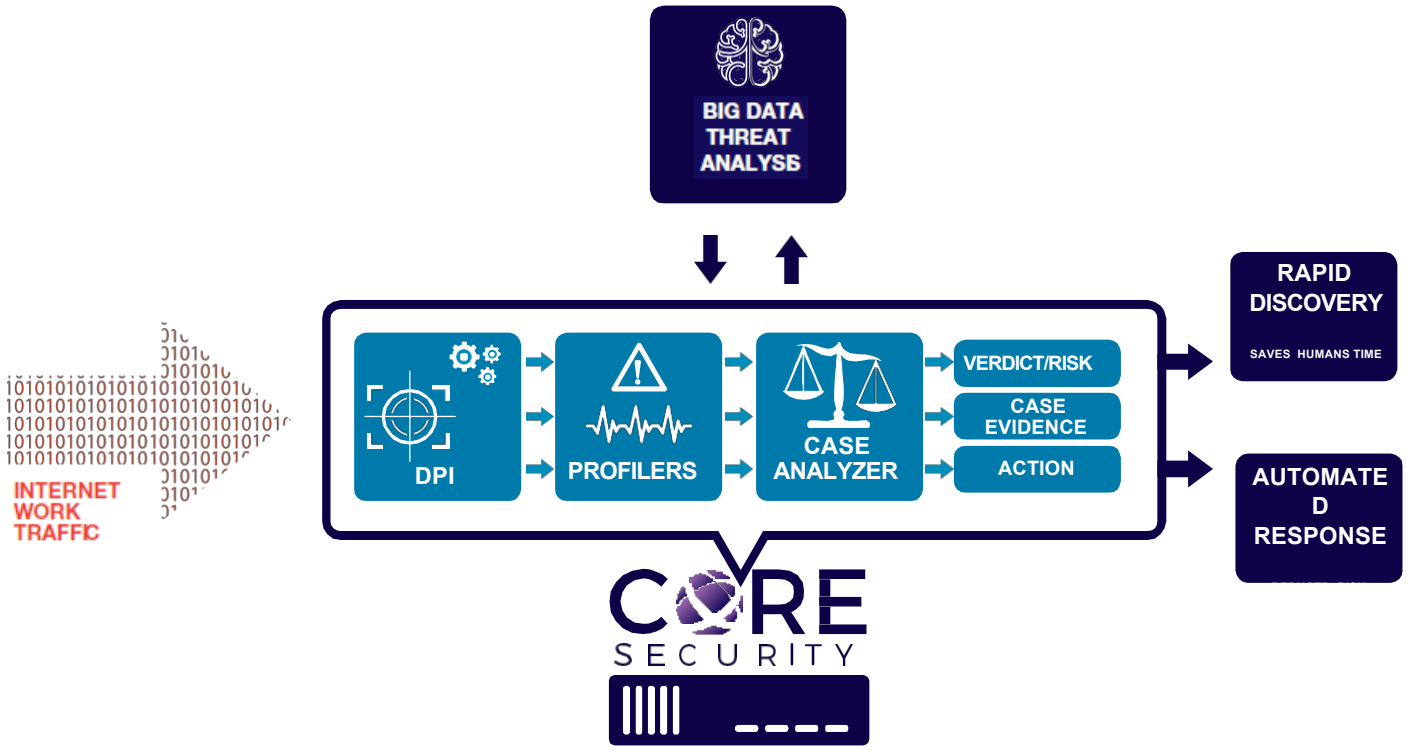
Network Insight (Damballa) 並非依靠任一技術或者快照，取而代之的是透過即時作業並隨時收集證據。Network Insight (Damballa) 採用以下多項技術產生可操作智能：

1. 利用正在申請專利的通信和風險分析器分析網路流量
2. 將訊息傳遞至個案分析系統，確認感染狀態
3. 提供安全團隊關於感染設備及風險等級之明確判決及鑑識證據

"[Network Insight (Damballa)] 已成為組織事件回應的重要工具，原因在於許多威脅是較難偵測的。

[Network Insight (Damballa)] 能準確地檢測惡意行為，讓我們得已有效地採取應對措施。"

–CISO 於坦帕大學



CORE SECURITY 簡介

Core Security 提供企業所需的內部安全隱患資訊。其威脅感知、身份和存取認證、網絡安全和弱點管理等解決方案為管理企業安全風險提供了可實現的洞察力及脈絡，讓客戶獲得企業安全的全面觀點，從而訂定更好的安全修復策略。絕佳的洞察力將使組織能夠為其關鍵資產的保護排定優先順序，儘早採取行動降低存取風險，一旦發生威脅更能迅速回應。

Damballa 於 2016 年 7 月被 Core Security Technologies 收購

欲了解更多資訊請洽力悅資訊股份有限公司（02）2507-1601 或 sales@cyberview.com.tw

力悅資訊股份有限公司 | (02) 2507-1601 | sales@cyberview.com.tw | http://www.cyberview.com.tw/

Cyberview 力悅資訊

CORE SECURITY DAMBALLA