COMODO

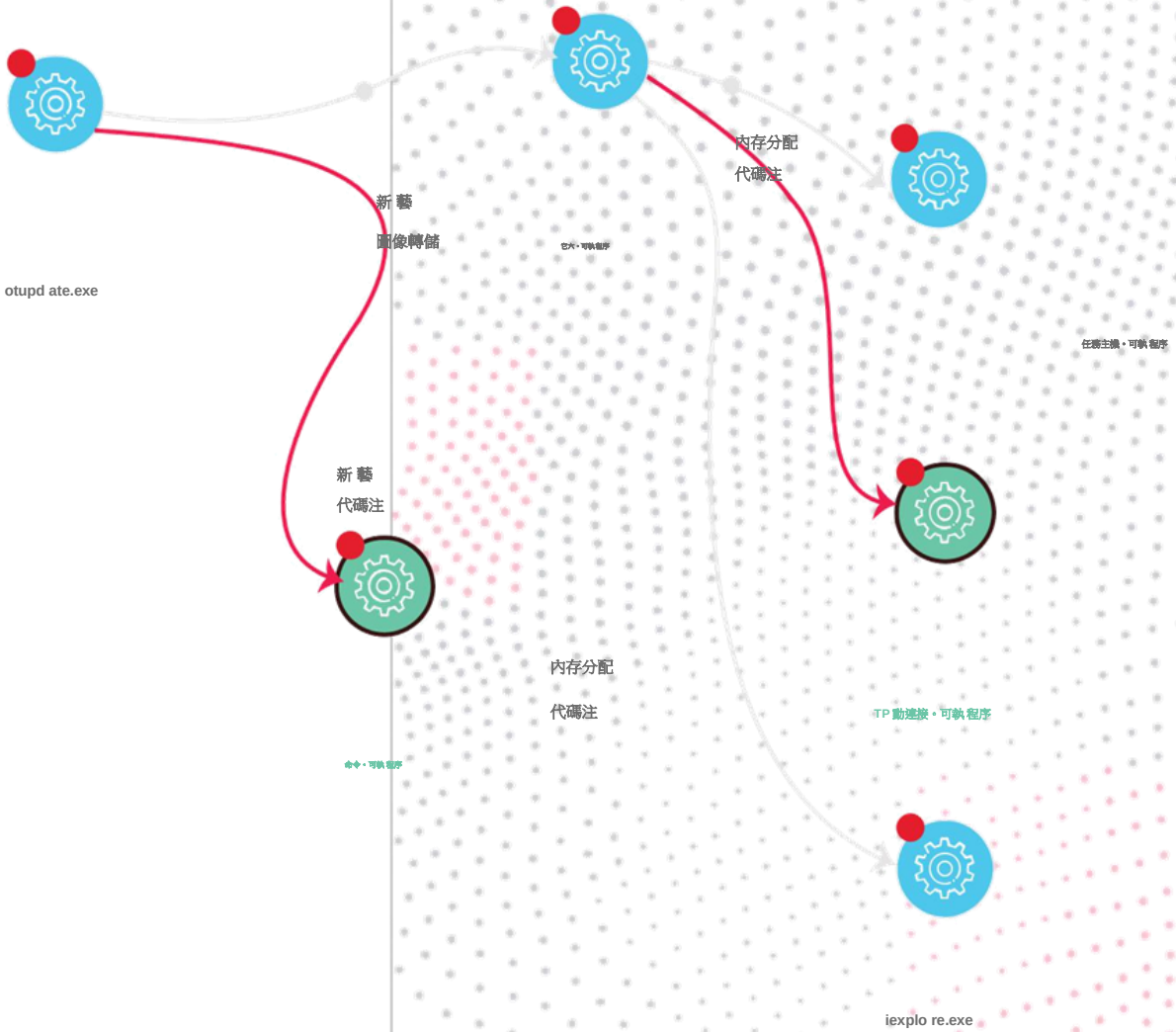
電話：+[illegible]
話：[illegible]

EDR

銓眾資安有限公司

原廠授權台灣經銷商

端點檢測和響應



全球挑戰

勒索軟件是 項複雜的業務。

新惡意軟件
300,000
每 創建

新的贖
11 秒
PE RI NC ID ENT

受害者 MS PA ID
3.5 億美元
贖

EDR 還不夠
99% 檢測
當前的安全解決 案依賴於檢測才能預防。檢測有效率還不夠好。

信譽服務
不可預料的
第三 情報服務為檢測世界提供了動 ，但仍然過於緩慢和低效，無法 直依賴

不 的
專業知識
有限的網絡培訓、 學習曲線和有限數量的可 專家來解決您的 險

科莫多 區別

只有科摩多可以維護 100% 有效性防 勒索軟件和零 漏洞造成傷害！

網絡安全
100 %
效

端點
零
已感染

網絡安全
100 %
可擴展性

贖
零
有薪酬的

解決 案

基於雲的端點檢測和響應

毫無疑問，您需要部署專為保護 構建的端點安全 具和平台。但這還不夠。攻擊者很聰明。他們了解這些解決 案是如何 作的，並且他們不斷開發技術以躲避他們的注意。您還需要實時、持續的可 性，以便識別零 攻擊和無 件攻擊，並且這種可 性必須引導您進 準確的根本原因分析以進 有效的補救。

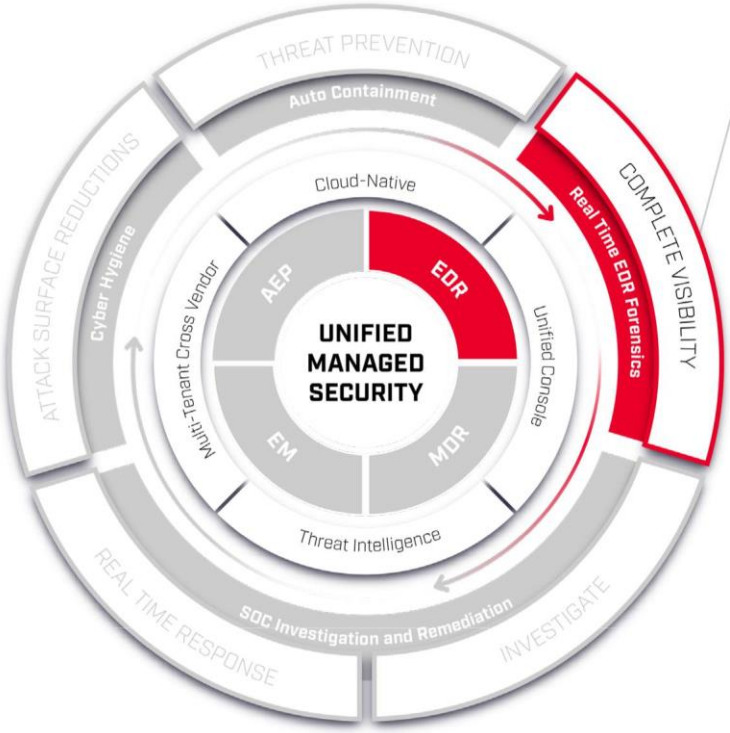
EDR 允許您在基本事件級別分析整個環境中正在發 的事情。這種粒度可以實現更快、更有效的補救所需的準確根本原因分析。流程層次可視化已被證明是傳達此類信息的最佳 式，它提供的不僅僅是數據，它們還提供可操作的知識。易於導航的菜單可以輕鬆獲取有關端點、哈希以及基本和 級事件的詳細信息。您可以獲得詳細的 件和設備軌跡信息，並且可以導航單個事件以發現可能危及您的系統的更 問題。

級端點 保護

端點檢測 和響應

端點 經理

託管檢測 和響應



結果

消除威脅並解決重複事件

EDR 不斷從您的端點收集事件，將它們集中在我們利 **Comodo Threat Laboratories** 情報和 **Comodo** 推薦安全策略的威脅雲中。我們基於雲的沙盒使 **Valkyrie** 件判斷系統來隔離試圖在端點上運 的未知 件並返回快速的好/壞判斷。

您會根據可 定義的安全策略獲得即時警報，以通知您有關可能代表勒索軟件、內存利 、**PowerShell** 濫 和許多其他威脅的可疑活動。當違反 **Comodo** 推薦的安全策略時，也會觸發警報。惡意 為是由 **PowerShell** 和 **Regedit** 等簽名和受信任的應 程序執 的，傳統的端點 具不會標記它——這正是攻擊者使 這種 法的原因。如果沒有 **EDR**，威脅可能會被忽視，從 使攻擊者能夠竊取公司的所有機密數據。

關鍵能

攻擊鏈可視化

攻擊向量顯 在儀表板上，當與 件軌跡和流程層次結構可視化相結合時，有助於調查。基於流程的事件以樹視圖結構顯 ，以幫助分析師更好地理解流程 為。

推薦的安全策略

每個 **EDR** 許可證都附帶安全策略，可根據您的個 需求進 定制。我們的銷售 程團隊可與您 起根據您的要求定制策略，包括特定於端點的策略。

可疑活動警報

獲取有關無 件攻擊、 級持續威脅 **(APT)** 和權限提升嘗試等活動的通知。分析師可以在採取反制措施時更改警報狀態，從 顯著簡化後續 作。

事件調查

事件搜索屏幕允許分析師運 查詢以返回基本事件級別粒度的任何詳細信息。聚合表是可點擊的，讓調查 員可以輕鬆深 了解特定事件或設備。

基於雲的架構

EDR 使 輕量級代理來收集進程、網絡、註冊表、下載、上傳、 件系統、外圍設備訪問和瀏覽器事件，並使您能夠以基本事件級別的粒度深 了解事件。

VALKYRIE 判決引擎

在 動遏制中運 時，未知 件會上傳到全球威脅雲進 實時分析，並在 **45** 秒內對 **95%** 的提交 件做出判斷。

無 件惡意軟件檢測

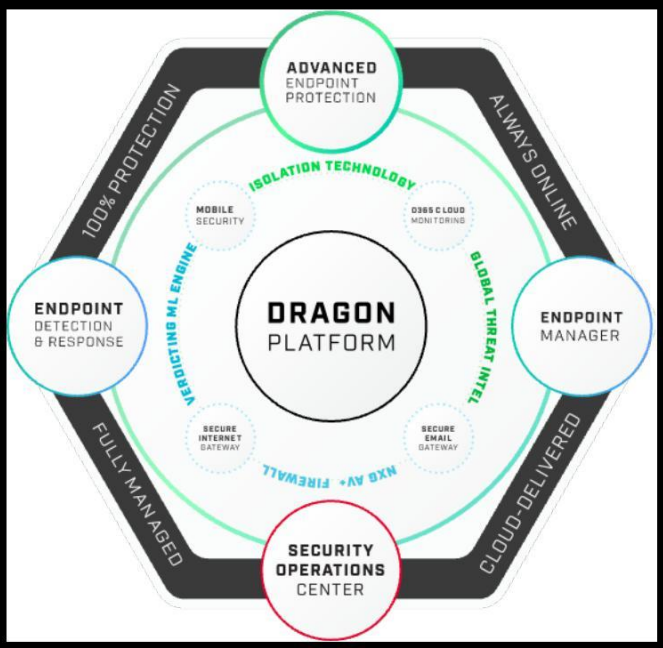
並 所有惡意軟件都是平等的。 些惡意軟件不需要您執 件，它內置在端點的基於內存的構件中，例如 **RAM**。**Comodo EDR** 可以在此威脅出現之前對其進 檢測。

與 動遏制兼容

請求運 時權限的未知可執 件和其他 件會 動在 **Comodo** 的專利虛擬容器中運 ，該容器無法訪問主機系統的資源或 數據。

企業級和 **MSP** 就緒

無論您是擁有數千個端點的企業還是為數百個客 提供服務的 **MSP**，**EDR** 代理都可以通過組策略對像或 **Comodo ITSM** 即時部署，並在每次發佈時 動更新。



級端點保護

使 **Auto Containment™** 從檢測轉向預防，以隔離勒索軟件和未知威脅等感染。

端點檢測和響應

獲取完整的攻擊背景，以了解 客如何試圖破壞您的網絡。

端點管理器

通過識別應 程序、了解漏洞和修復補丁來練習網絡衛 以減少攻擊 。

託管服務

通過 **24·7·365 SOC** 調查和修復，您的漏洞是由於缺乏資源、流程以及可能缺乏維護所有這些技術的技術。

關於科莫多

Comodo 總部位於新澤西州布盧姆菲爾德，其使命是通過突破性的隔離技術幫助客 避免違規 為，該技術可以完全消除勒索軟件、零 惡意軟件和其他安全提供商無法做到的網絡攻擊。我們通過獲得專利的 動遏制技術提供主動違規預防。我們的統 端點將此技術與我們 度評價的 級端點保護、端點檢測和響應以及端點管理等關鍵組件相集成，以提供單 的雲可訪問的主動違規保護解決 案。**Comodo** 的 **SOC** 即服務團隊使該解決 案成為 種無摩擦、 安全性的實施。欲了解更多信息，請訪問區台灣經銷商銓重安信有限公司。

:https://www.omnisecutek.com/