

未知型惡意程式偵測系統： *eDetector*

*eDetector*為具有全中文化之遠端惡意程式資安鑑識機制，中央管理系統派送agent程式偵測遠端電腦是否感染惡意程式。

*eDetector*在欲進行分析的遠端電腦部署agent後，系統管理者便可透過中央控管的方式，對已部署畢的電腦進行記憶體內之執行程序與相關檔案進行鑑識分析，並在不影響目標電腦運作的情況下，結合*Metadefender OPSWAT* 最新多合一整合知識庫，進行任何已知或未知惡意程式偵測分析。

最優質的資安鑑識分析計畫，從 *eDetector* 開始

The screenshot displays the *eDetector* web interface. On the left, there's a sidebar with navigation options like '用戶端檢視' (Client View) and '處理程序檢視' (Process View). The main area shows a list of monitored devices with columns for IP address, device name, and status. One device, '00-0C-29-4B-1D-96: 192.168.10.112', is selected. The right pane shows a detailed view of this device, including a list of running processes (e.g., [System Process], System, smss.exe, csrss.exe) and a file system tree (e.g., \$Extend, \$Recycle.Bin, PerfLogs, Program Files).

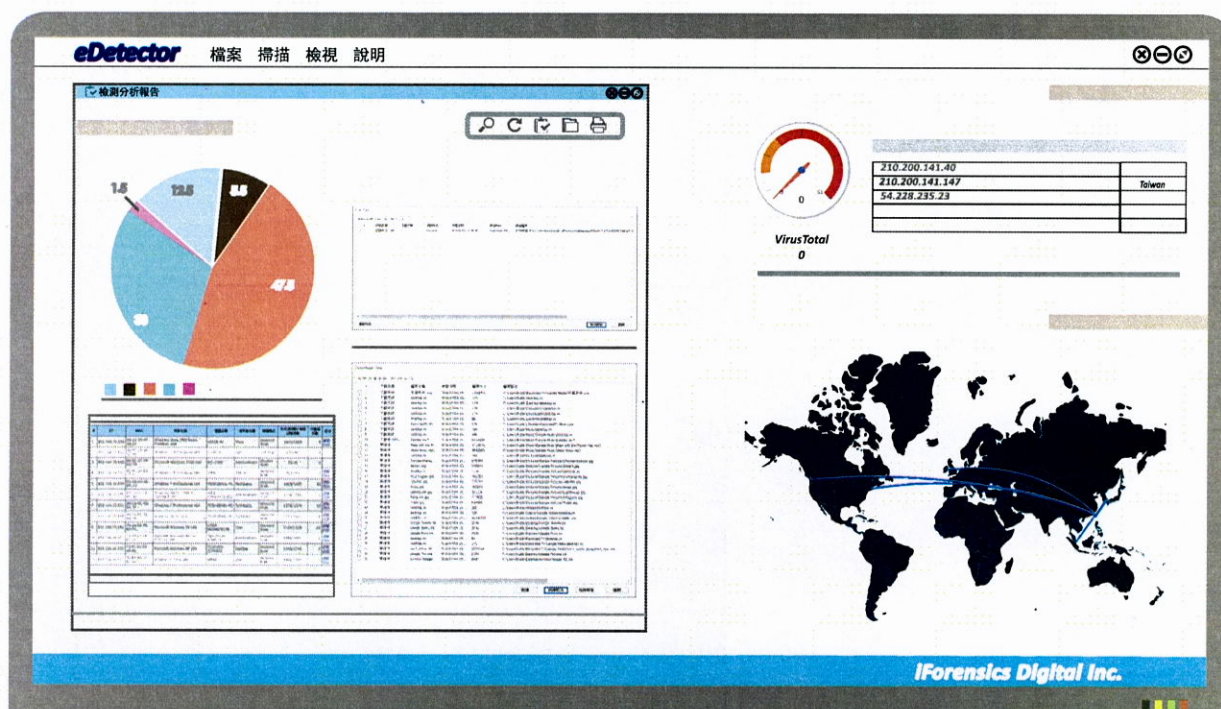
您不再需要上傳Virus Total即可擁有40合1整合知識庫！

This section shows another part of the *eDetector* interface. On the left, there's a calendar view showing scan results for various dates from January to December. The right pane shows a detailed report for a specific device, including a table with columns for '掃描引擎' (Scan Engine), '掃描引擎版本' (Scan Engine Version), '掃描引擎名稱' (Scan Engine Name), and '掃描引擎狀態' (Scan Engine Status). The report also includes a table for '掃描引擎' (Scan Engine) with columns for '引擎名稱' (Engine Name), '引擎版本' (Engine Version), '引擎狀態' (Engine Status), and '引擎描述' (Engine Description).

資安鑑識服務：

TAF認證的**App**檢測實驗室，可檢測行動平台**App**的惡意程式行為，透過**eDetector**可進一步與本公司研發及代理(**Vmray**)之沙箱進行惡意程式樣本分析。

鑒真數位深耕數位鑑識領域 提供您資訊安全的最佳對策



鑒真數位有限公司
iForensics Digital Inc.

臺北市中山區松江路309號11樓之5

TEL: (02) 2517 2532

FAX: (02) 2517 1097

e-mail: service@iforensics.com.tw

<http://www.iforensics.com.tw/>

facebook 搜尋：鑒真數位