

Enhancing Security through Continuous Threat Assessment

# EDR 端點威脅偵測系統



**NSGUARD**  
NSGUARD Technology, Inc.

捷睿智能股份有限公司



## 簡介

NSGUARD EDR 是一套布署於端點主機，透過先進的資安鑑識與人工智慧演算法，偵測系統中可疑的檔案、程序。

## 產品效益

- 快速找出受攻擊主機

Windows 版能透過 Activity Directory(AD)進行派送，能在短時間內達到大範圍掃描主機的效益，並且於介面上顯示目前企業/機關內部主機的健康狀況。

- 自動回傳檢測報告

能夠常駐於端點主機中，定期回傳主機的檢測報告，讓管理人員能夠掌握目前企業/機關內部主機的受威脅程度。

## 功能說明

- 監看主機的健康狀態

顯示機關內部主機的健康狀態，監控人員能隨時查詢機關內主機是否存在高風險漏洞。

主機列表	裝置地圖	安全掃描	VANS
10.8. [redacted] 0-6A-B5-1F	Windows 7 Profession...	HMD v.2.5.4936.403	2021-10-14 10:16:17
Malware: 14	Process Monitor: 5	GCB: 792	Event Tracing: 300
VANS: 0			
10.8. [redacted] 54-58-95-81	windows 10	HMD v.2.0.3764.378	
Malware: 23			
172. [redacted] -62-66-82-3C-B8	Windows 7 Profession...	HMD v.2.5.4936.403	2021-10-14 06:30:18
Malware: 5	Process Monitor: 1	GCB: 845	Event Tracing: 71
172.1 [redacted] F6-2A-F4-56	Windows 10 Pro	HMD v.2.5.4936.403	2021-10-14 10:20:44
Malware: 3	Process Monitor: 1	GCB: 785	Event Tracing: 148
VANS: 0			
192.1 [redacted] 5-A7-D1-8A	Windows Server 2008 ...	HMD v.2.5.4936.403	2021-10-14 06:21:07
Malware: 2	Process Monitor: 1	GCB: 637	Event Tracing: 46
VANS: 0			
192.1 [redacted] 6-89-9F-A5	Windows Server 2008 ...	HMD v.2.5.4936.403	2021-10-14 06:16:38
Malware: 4	Process Monitor: 1	VANS: 1	GCB: 637
Event Tracing: 44			

- 威脅快速比對

自動化偵測可疑的程式，有效協助管理人員針對目標主機中受感染的程式進行清除。

主機分析資訊

威脅等級	IP	MAC	主機名稱	使用系統	所屬人員	版本
Emergency	10.8.0		10-PC	Windows 7 Professional	vickeyliao	2.5.4936.403

主機資訊

Dashboard | Yara Scan | **Malware** | GCB | IR | File Integrity | Event Tracing | Process Monitor | VANS | EDR | 設定

重新載入 檢測時間: 2021-10-14 03:28:32 重新檢測

檢測時間: 2021-10-14 03:28:32 回應時間: 2021-10-14 04:20:40 可疑檔案數: 14 疑檔檔案

可疑檔案路徑

路徑: C:\Windows\TEMP\tmp38EA.tmp.exe	加入白名單
路徑: C:\Windows\TEMP\tmp5E35.tmp.exe	加入白名單
路徑: C:\Windows\TEMP\tmp75CC.tmp.exe	加入白名單
路徑: C:\Windows\TEMP\tmp7863.tmp.exe	加入白名單
路徑: C:\Windows\TEMP\tmpE56.tmp.exe	加入白名單
路徑: C:\Windows\TEMP\tmpEA99.tmp.exe	加入白名單
路徑: C:\Windows\Temp\tmp5E35.tmp.exe	加入白名單
路徑: C:\Windows\Temp\tmpEA99.tmp.exe	加入白名單
路徑: C:\Windows\Temp\tmp75CC.tmp.exe	加入白名單

匯出 關閉

## 應用場景

- 大規模部屬於企業/機關環境

Windows 版可透過 Activity Directory(AD)的方式能夠進行大範圍部屬，並且支援在 DMZ、伺服器區與 OA 區域，自動化的進行檢測與威脅掃描，

## 系統需求

### 系統規格

Windows 支援作業系統

Windows 7 / 8.1 / 10

Windows Server 2008R2 / 2012R2 / 2016 / 2019

系統需求

記憶體: 4GB 以上

硬碟空間: 5GB 以上

Linux 支援作業系統

CentOS 6 / 7 / 8

Ubuntu 14.04 / 16.04 / 18.04 / 19.04 / 20.04

系統需求

記憶體: 2GB 以上

硬碟空間: 5GB 以上



**NSGUARD**  
NSGUARD Technology, Inc.