ThreatDown
Powered by Malwarebytes

DATA SHEET

THREATDOWN ULTIMATE

When "Good Enough" is NOT Enough

企業組織需要的是既使用方便 又能提供絕佳防護的解決方案

網路攻擊事件並未趨緩，在2022年將近85%的企業組織曾經歷過至少一次成功的網路攻擊；將近40%的組織面臨6次以上的攻擊，近七成的組織預估在未來的一年將會受到攻擊。[註1]

70%
企業組織
已受攻擊 [註2]

277天
平均花費
識別並
阻止擴散[註3]

80%
因已知
漏洞而受害 [註4]

62%
IT部門
人手不足 [註5]

『找到，並修復那些漏網之魚』
-寫在Malwarebytes DNA中-

THREATDOWN ULTIMATE 登峰版

專為企業環境設計，了解企業組織的痛點，提供單一端點、全面防護的解決方案。

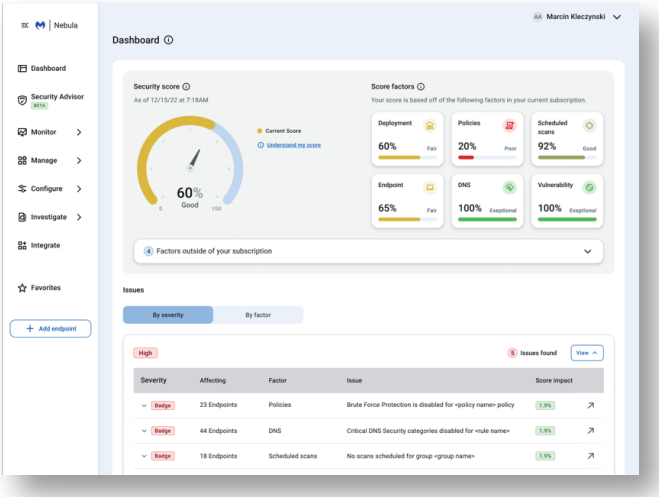
Improve security

- 24 x 7 x 365全年無休持續監控，由專業團隊提供威脅獵捕、鑑識分析與災害復原的豐富經驗。
- 監控可疑行為、威脅誘捕、多層式攻擊偵測技術。
- 透過獨家技術（專利申請中）加快回應速度，持續掃描告警，針對最關鍵的問題優先提供明確的建議方案。
- 單一端點程式可提供多向量保護，無需安裝許多程式影響設備效率。
- 採取阻擋惡意應用程式執行減少攻擊面。

Reduce complexity

- 集中雲端管理平台採用直覺操作介面，單一控管多項防護機制。
- 羽量級端點程式，快速安裝執行。
- Security Advisor提供清晰的色彩區隔，輕易理解目前組織內安全狀況，並提供建議方案
- 獨有的Linking Engine可搜尋並自動修復，自動刪除惡意程式遺留下來的變更與程序修改。
- SOC in box，由專業團隊輔助您的IT團隊。

1 2023 Cyberthreat Defense Report, CyberEdge Group, LLC
2 State of Malware Report 2023, Malwarebytes
3 Cost of a Data Breach Report 2022, Ponemon Institute
4 Cyber Security Report 2021, Check Point
5 Cybersecurity Insights Report 2022, Anomali



Security Advisor

- ◆ 清晰可見企業資安狀況
- ◆ 量化與色彩呈現安全等級
- ◆ 依風險等級排序，高風險優先處理
- ◆ 提供因應措施建議參考

FEATURES

		CORE	ADVANCED	ELITE	ULTIMATE
Endpoint Protection	Endpoint Detection & Response		●	●	●
	Endpoint Protection	●	●	●	●
	Incident Response	●	●	●	●
Services	Managed Threat Hunting		●	●	●
	Managed Detection & Response			●	●
	31-day lookbacks			●	●
Modules	Vulnerability Assessment	●	●	●	●
	Patch Management		●	●	●
	Application Block	●	●	●	●
	Website content filtering				●

ThreatDown提供不同套餐，對應不同規模企業需求，輕鬆符合企業資安規範，達成完整防護目標。

◇ Managed Detection and Response: 24 X 7 X 365由專業團隊監控、分析、回應並修復威脅攻擊。

◇ Endpoint Detection and Response: 提供持續主動式偵測與回應，監控可以活動，雲端沙箱即時檢測、端點隔離、勒索軟體攻擊回復、對應MITRE ATT&CK指標。

◇ Managed Threat Hunting: 主動式自動威脅獵捕，將EDR告警與內外部威脅情資整合分析，針對最緊急的威脅透過清晰的應對步驟說明。

◇ Endpoint Protection: 多層次架構全方位防禦，在滲透發生前阻擋特徵碼比對、無檔案攻擊、零日攻擊等。

◇ Vulnerability Assessment: 排程或自行執行弱點掃描，搜尋OS與應用程式內弱點及漏洞。

◇ Patch Management: 自動執行補丁程序以封鎖潛在的接入點。

◇ Application Block: 簡易封鎖非授權之應用程式，避免惡意攻擊。

◇ Incident Response: 建立於獨有的Linking Engine，不僅是移除惡意程式可執行檔，同時還查找並自動刪除相關的蛛絲馬跡與遺落的殘骸，避免再次感染。

◇ 31-day lookbacks: 由ThreatDown專家們搜尋IOC以阻斷攻擊並優化未來的偵測與告警。

◇ Website content Flitering: 藉由阻擋可疑、已知惡意或不適宜的網站，降低惡意攻擊風險。

RICHS RichSmart Technology Co., Ltd.
代理商 瑞奇數碼股份有限公司
台北市內湖區港華街66號1樓
TEL 02-26581786 | www.richsmt.com