DATA SHEET

Malwarebytes | HEM 赫盟資訊有限公司 HEM InfoSec, Ltd.

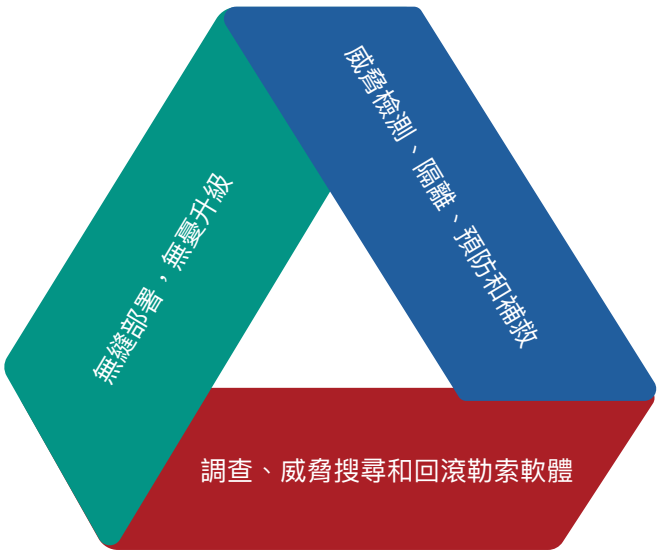
升級到 MALWAREBYTES ENDPOINT DETECTION AND RESPONSE

透過Endpoint Detection And Response提升用戶的網路安全

OVERVIEW

各種規模的企業都是網路攻擊的目標，這使得制定正確的保護和響應計劃變得如此重要。 透過升級至 Malwarebytes 端點檢測和響應 (EDR) 的服務，Malwarebytes 團隊將把用戶的網路安全提升到一個新的水平。
借助 EDR，Malwarebytes 可以提供強大的勒索軟體檢測和響應，更仔細地在用戶環境中尋找威脅，並在不影響用戶工作效率的情況下完成這一切。

Malwarebytes 的首要任務是讓用戶保持高效率和安全性，這就是加入 EDR 作為產品的原因。 Malwarebytes EDR 是一個強大的解決方案，Malwarebytes 團隊能夠在威脅出現時快速並有效地採取行動保護用戶端點不受侵害。 Malwarebytes EDR 是一種比傳統端點保護更全面的安全方案，除了提供複雜的檢測，還可以查明和修復威脅，以及回滾已經觸發的勒索軟體。



KEY BENEFITS

更高的效率：

Malwarebytes EDR 提供高效的解決方案，因此Malwarebytes始終了解用戶端點的安全狀態。 隨著用戶的成長，Malwarebytes 服務的擴展可用相同的服務級別覆蓋所有設備，並提供保護和彈性。

最大化設備可用性：

Malwarebytes EDR 提供多層保護和自動修復，有效保護用戶的端點並確保用戶營運順利進行，不會因勒索軟體或其他攻擊而造成中斷性停機。
用戶可以相信設備是安全的。

在 G2 Crowd Peer Review 網站上可查看其他企業對 Malwarebytes 的評價
https://www.g2.com/products/malwarebytes-for-business/reviews

ENJOY THE ADVANTAGES

勒索軟體回滾

勒索軟體是企業最大體的威脅。 一次成功的攻擊代價高昂，研究表示，企業平均贖金高達 247,000 美元和另外 350,000 美元的恢復成本。
*使用 Malwarebytes EDR，可以通過勒索軟體回滾功能減輕這些風險。 Malwarebytes 使用允許回滾長達 72 小時的技術。 如果用戶端點被感染，Malwarebytes 會簡單地撤銷設備更改並恢復被加密、刪除或修改的文件。

高級威脅搜尋

借助 EDR，Malwarebytes團隊可以主動尋找入侵指標 (IOC) ，在威脅有機會感染和破壞之前就將其消除。

網路安全威脅很複雜，可能會留下殘餘。
Malwarebytes EDR 不僅消除了明顯的威脅，還徹底修復了設備中的每個動態和相關工件，以永久清除病毒。也對潛在有害程式 (PUP) 和潛在有害修改 (PUM) 提供了有效的清理。

網路安全形勢不斷變化。 Malwarebytes EDR 提供關鍵見解，以持續改善用戶的網路資訊安全。

無縫保護

提高企業用戶安全性勢不可擋；
實施升級至 Malwarebytes EDR 是無縫且無中斷的。
Malwarebytes 將在幾分鐘內部署解決方案，讓企業用戶享受高級端點保護，更加安心，並專注於營運增長。

CONTACT US:

HEM 赫盟資訊有限公司

HEM@heminfosec.com

037 - 585552

要了解更多訊息，現在就聯絡赫盟資訊，
用 Malwarebytes 為您的企業阻擋進階式惡意軟體及零日攻擊、漏洞及勒索軟體防護、挽救被感染的檔案;
輕鬆佈署、管理簡易、提升工作效率。

*Source: https://www.propertycasualty360.com/2021/09/28/ransomware-drove-cyber-losses-for-small-medium-businesses