SOLUTION BRIEF

Malwarebytes for Business

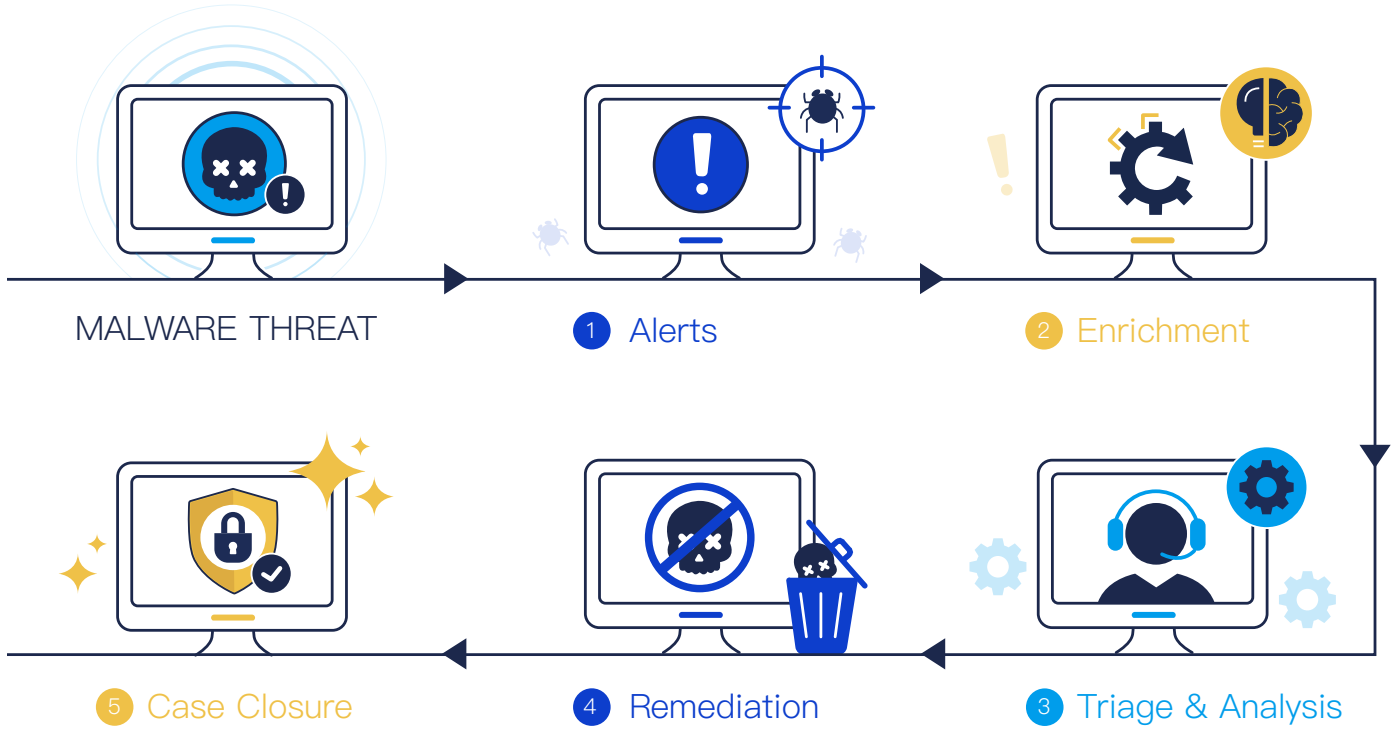
MALWAREBYTES MANAGED DETECTION AND RESPONSE (MDR)

Unlocking effective and fast threat detection and remediation

HOW IT WORKS

Malwarebytes MDR 提供強大的威脅檢測和補救措施，由Malwarebytes 的頂級安全分析師提供 24x7x365 監控和調查。 由強大的技術和一流的安全專家結合，企業組織將通過 MDR 服務獲得網路彈性，加速威脅檢測並精確地執行事件響應。

從最初的威脅警報到調查結束，我們的專家專注於提供高質量的服務。
下圖顯示了我們為快速處理您環境中的威脅警報而遵循的流程。



1 ALERTS

通過在使用者的環境中部署 Malwarebytes Endpoint Detection and Response (EDR)，使用者將獲得強大的第一道防線來抵禦企業組織面臨的威脅。 該解決方案在第三方評估中名列前茅，包括 MITRE Engenuity Evaluations、MRG Effitas 和 AV-TEST.org，包括七層保護、多模式隔離、72 小時勒索軟件回滾等全面的端點保護和檢測功能。

Malwarebytes 的安全專家團隊利用 Malwarebytes EDR 對使用者的端點進行 24x7 全天候監控，以發現對企業組織的威脅。 Malwarebytes 將始終如一地評估 EDR 數據，以尋找指示可疑活動、檢測到的威脅或妥協指標 (IOC) 的警報。

2 ENRICHMENT

為了更深入地分析 Malwarebytes EDR 威脅檢測及其對使用者的企業組織構成的風險級別，使用者的 EDR 遙測數據會自動引入我們的後端安全編排、自動化和響應 (SOAR) 平台。 SOAR 平台還從多個來源獲取威脅情報源，這些來源共同提供 EDR 警報的相關和上下文分析。

這為使用者的安全操作增加了強大的 SOAR 功能，由Malwarebytes 的 MDR 團隊維護，並由 MDR 分析師提供有關使用者環境中正在發生的事情和更多信息與見解，使他們能夠快速輕鬆地了解威脅及其潛在影響。 有了這些信息， MDR 分析師可以迅速就最佳行動方案做出明智的決定。

3 TRIAGE & ANALYSIS

一些 MDR 提供商僅依賴其 SOAR 平台進行分析，這可能會產生偏差並導致錯誤診斷。 Malwarebytes MDR 不是這種情況。 Malwarebytes 的後端 SOAR 自動執行瑣碎的任務和相關性，而 MDR 分析師提供對威脅行為的必要的實際分析。 他們全面調查警報中的遙測數據上下文，以有效評估它是真正的威脅還是誤報。

Malwarebytes 的方法提供了更高的準確性並捕獲了更多的威脅，其中包括以下步驟：

- 在警報分析期間，MDR 分析師審查特定的工件以找到需要更深入檢查的工件。
- 為每個需要分類的工件打開一個案例。
- MDR 分析師通力合作，從各個角度審視威脅並確定最佳行動方案。
- MDR 分析師所做的所有步驟和決策都在 MDR 門戶中進行跟踪，讓客戶了解每一步的信息。

4 REMEDIATION

當警報被確認為威脅時，就會競相遏制和補救它。我們了解企業組織的資安團隊可能會發生變化，因此企業組織可以靈活地選擇最適合補救方法。使用以下選項決定如何將響應應用於端點：

- Malwarebytes managed：
  MDR 分析師代管補救威脅，通知企業資安團隊在端點上採取的所有操作。

- 客戶管理：
  MDR 分析師提供有關建議操作的指導，企業資安團隊可以採取這些操作來有效地補救威脅。

5 CASE CLOSURE

一旦威脅得到補救，Malwarebytes 將結案，包括有關來自 SOAR 平台的安全事件和詳細的分析文檔都保存在 MDR 門戶中，供使用者訪問或報告，便於參考管理、合規性和其他需求。

申請試用

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

www.heminfosec.com HEM@heminfosec.com Tel : 037 - 585552
赫盟資訊有限公司