Malwarebytes

Malwarebytes Endpoint Protection

Malwarebytes 企業防禦惡意軟件和駭客的第一道防線
強大的端點惡意軟件防護，適用於任何規模的企業組織

效能與防護能力並重
快速佈署、有效保護、
提升端點工作效率

精準檢測攻擊點
新世代進階端點保護技術

因應層出不窮的
新型威脅手法
簡單好上手的雲端管理平台

Malwarebytes 核心技術＆特點

Web Protection 網路防護
阻擋使用者訪問惡意網站、惡意廣告、詐騙網路和釣魚網站

Application Hardening 應用程式縱深防禦
阻止漏洞利用攻擊並主動追蹤來源和偵測試圖利用進階攻擊的行為

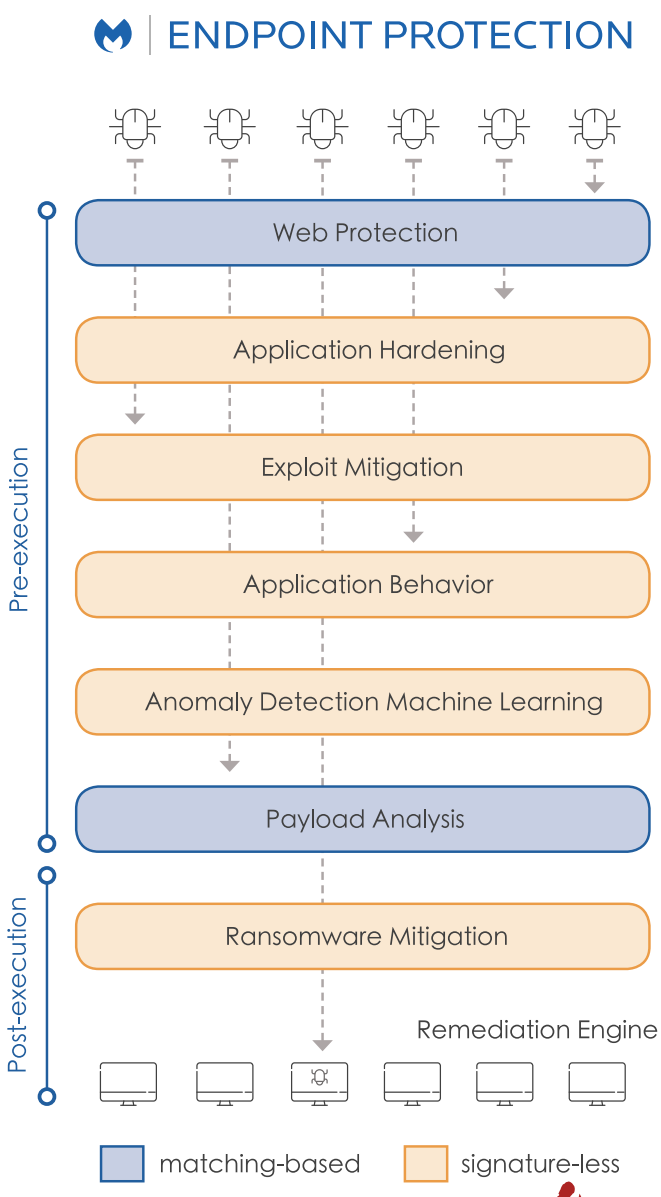
Exploit Mitigation 漏洞防堵
主動檢測及阻擋企圖利用漏洞遠端操控端點執行惡意碼，有效攔截無檔案式攻擊

Application Behavior Protection 應用程式行為保護
防止應用程式被感染利用後造成的橫向擴散感染用戶端

Anomaly Detection Machine Learning 機器學習異常檢測
Malwarebytes 將 Anomaly Detection 專利技術應用在機器學習上，正向表列分析能夠主動識別病毒和惡意軟體，大幅降低誤判並提升偵測效能

Payload Analysis 有效負載分析
使用啓發式 (heuristics) 和行為規則來識別相關惡意軟體家族

Ransomware Mitigation 遠離勒索軟體
無特徵碼的行為監控技術，在勒索軟體發作前偵測並阻擋



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

Malwarebytes 新時代，解決 APT/ 勒索軟體最專業：

來自美國實力雄厚的 Malwarebytes，以修復（Remediation）技術聞名全球，在防禦 Ransomware 有獨到的無特徵碼辨識技術，提供更完整的防勒索防加密保護機制，以及對未知惡意程式的防堵技術與漏洞偵測防禦修補技術，讓企業的資安能加強，提供更完善的安全機制。

Malwarebytes Endpoint Protection 優勢：

多層次偵測技術

綜合無特徵碼和多重比對技術識別和防禦攻擊鏈中所有階段的攻擊（包含發作前與發作後），再加上全方位的感測技術，在感染階段就能提早被偵測到，完善您的資安政策

明確辨識徹底清除

Malwarebytes 提供業界最值得信賴的補救功能 (remediation)，並透過 Linking Engine 技術有效刪除感染並追溯感染源。Malwarebytes 徹底永久刪除感染源，可為一勞永逸的補救措施

雲端管理界面

透過雲端平台進行管理，雲端平台讓企業可以輕鬆佈署，同時管理 Malwarebytes Endpoint Protection 與其他 Malwarebytes 解決方案，降低複雜度，更省下特定硬體的購買及後續維護費用

Malwarebytes 解決方案 – 系統要求：

Malwarebytes 雲端控制台

Malwarebytes 雲端控制台，建議使用最新版本的 Google Chrome 瀏覽器

注意：不支持行動裝置瀏覽器

系統要求

1. Malwarebytes Endpoint Protection (EP) 端點保護
2. Endpoint Protection for Servers (EPS) 伺服器端點保護

Windows Server : 2019, 2016, 2012, 2012 R2, SBS 2011, 2008 R2 SP1 , 2008 SP2 , 2008
Windows: 10, 8.1, 8, 7, Vista, XP SP3
Mac: OS X 10.11 El Capitan, macOS 10.12 Sierra, macOS 10.13 High Sierra, macOS 10.14 Mojave, macOS 10.15 Catalina, macOS 11.1, 11.2 Big Sur
Linux: Ubuntu 16 / Debian 9, Ubuntu 18, Debian 8, RHEL7 and for other RPM–based distros

3. Malwarebytes Endpoint Detection and Response (EDR) 端點檢測和響應
4. Endpoint Detection & Response for Servers (EDRS) 伺服器端點檢測和響應

Windows Server : 2019, 2016, 2012, 2012 R2, 2008 R2 SP1
Windows: 10, 8.1, 8, 7 SP1
Mac : macOS 10.13 High Sierra, macOS 10.14 Mojave, macOS 10.15 Catalina, macOS 11.1, 11.2 Big Sur

5. Malwarebytes Incident Response (IR) 事件響應

Windows Server : 2019, 2016, 2012, 2012 R2, SBS 2011, 2008 R2 SP1, 2008 SP2 , 2008
Windows: 10, 8.1, 8, 7, Vista, XP SP3
Mac: OS X 10.11 El Capitan, macOS 10.12 Sierra, macOS 10.13 High Sierra, macOS 10.14 Mojave, macOS 10.15 Catalina, macOS 11.1, 11.2 Big Sur
Linux: Ubuntu 16 / Debian 9, Ubuntu 18, Debian 8, RHEL7 and for other RPM–based distros

技術本位、服務導向 。 專業規劃、最適產品

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。

HEM DM-MBEP-v21007

Malwarebytes

Malwarebytes Endpoint Detection and Response (EDR)

主動威脅檢視與回應，保持端點正常作業

Malwarebytes 核心技術 & 特點

Web Protection 網路防護
阻擋使用者訪問惡意網站、惡意廣告、詐騙網路和釣魚網站

Application Hardening 應用程式縱深防禦
阻止漏洞利用攻擊並主動追蹤來源和偵測試圖利用進階攻擊的行為

Exploit Mitigation 漏洞防堵
主動檢測及阻擋企圖利用漏洞遠端操控端點執行惡意碼，有效攔截無檔案式攻擊

Application Behavior Protection 應用程式行為保護
防止應用程式被感染利用後造成的橫向擴散感染用戶端

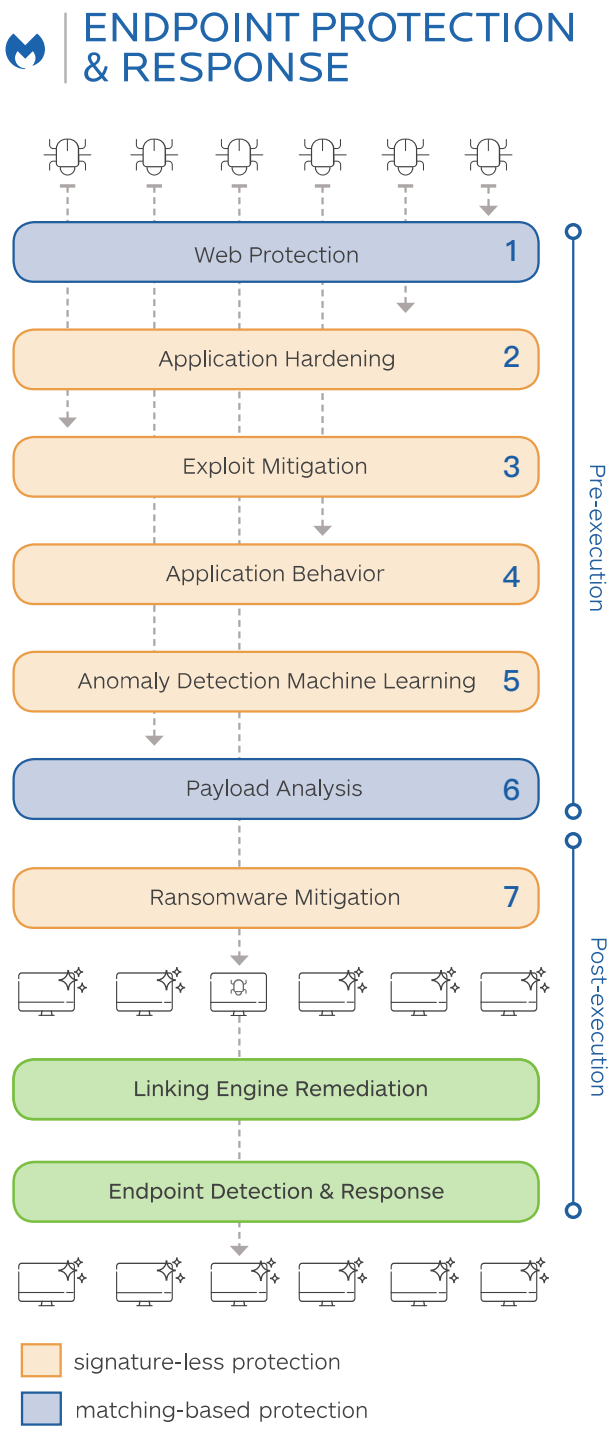
Anomaly Detection Machine Learning 機器學習異常檢測
Malwarebytes 將 Anomaly Detection 專利技術應用在機器學習上，正向表列分析能夠主動識別病毒和惡意軟體，大幅降低誤判並提升偵測效能

Payload Analysis 有效負載分析
使用啓發式 (heuristics) 和行為規則來識別相關惡意軟體家族

Ransomware Mitigation 遠離勒索軟體
無特徵碼的行為監控技術，在勒索軟體發作前偵測並阻擋

Linking Engine and Remediation 鏈接引擎和修復技術
提供完整的修復與追蹤感染源全面清除惡意軟件

Endpoint Detection and Response (EDR) 端點檢測和回應
針對端點防護執行中的異常行為，提供分析與鑑識。降低零日攻擊的停留時間。



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

資料的遺失無可避免，因此即時修補更是不可少的一環！

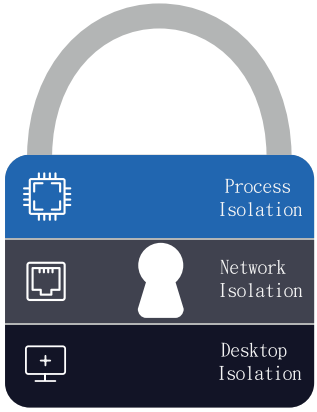
Malwarebytes Endpoint Protection and Response (EDR) 端點檢測和回應
提供您除了告警與重灌之外的解決方案：

可疑活動監視
持續關注及檢視端點文件、事件、執行中的程式及惡意註冊碼的活動

個別端點隔離
網路、執行作業及桌面的隔離，可以阻止惡意程式呼叫遠端惡意主機並阻擋遠端駭客行為

雲端沙箱整合
觀察可疑檔案的行為模式、機器學習端點異常檢測

備份 – 加密後回溯
勒索事件發生後，協助回復正常文件，備份文件保留時間可回溯至 72 小時



Malwarebytes 解決方案 – 系統要求：

Malwarebytes 雲端控制台
Malwarebytes 雲端控制台，建議使用最新版本的 Google Chrome 瀏覽器
注意：不支持行動裝置瀏覽器

系統要求

1. Malwarebytes Endpoint Protection (EP) 端點保護
2. Endpoint Protection for Servers (EPS) 伺服器端點保護
Windows Server : 2019, 2016, 2012, 2012 R2, SBS 2011, 2008 R2 SP1 , 2008 SP2 , 2008
Windows: 10, 8.1, 8, 7, Vista, XP SP3
Mac: OS X 10.11 El Capitan, macOS 10.12 Sierra, macOS 10.13 High Sierra, macOS 10.14 Mojave, macOS 10.15 Catalina, macOS 11.1, 11.2 Big Sur
Linux: Ubuntu 16 / Debian 9, Ubuntu 18, Debian 8, RHEL7 and for other RPM–based distros

3. Malwarebytes Endpoint Detection and Response (EDR) 端點檢測和響應
4. Endpoint Detection & Response for Servers (EDRS) 伺服器端點檢測和響應
Windows Server : 2019, 2016, 2012, 2012 R2, 2008 R2 SP1
Windows: 10, 8.1, 8, 7 SP1
Mac : macOS 10.13 High Sierra, macOS 10.14 Mojave, macOS 10.15 Catalina, macOS 11.1, 11.2 Big Sur

5. Malwarebytes Incident Response (IR) 事件響應
Windows Server : 2019, 2016, 2012, 2012 R2, SBS 2011, 2008 R2 SP1, 2008 SP2 , 2008
Windows: 10, 8.1, 8, 7, Vista, XP SP3
Mac: OS X 10.11 El Capitan, macOS 10.12 Sierra, macOS 10.13 High Sierra, macOS 10.14 Mojave, macOS 10.15 Catalina, macOS 11.1, 11.2 Big Sur
Linux: Ubuntu 16 / Debian 9, Ubuntu 18, Debian 8, RHEL7 and for other RPM–based distros

技術本位、服務導向 。 專業規劃、最適產品

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。

HEM DM-MBEDR-v21007

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