保安資訊 SAVETIME INFORMATION SECURITY

Symantec Endpoint Security 如何保護您

賽門鐵克全球威脅情資

-- 推動世界級的檢測和保護力的重大關鍵

9.0+

PB(1PB=1024TB)
威脅態勢可見性

5,000億
為人工智慧驅動的情資圖譜創造優勢

60億
數位簽章相關特徵

2,200萬
行動裝置相關特徵

20億
可疑檔案

460億
網址記錄

5億
程序行為分類

從數字上來看

-- 無與倫比的可見性、檢測、保護

0.8+

十億
威脅被阻止

45,432,000+
惡意網頁重定向嘗試被阻止

3,706,300+
未知和 0-day 攻擊被阻止

1,887,700+
就地取材威脅被阻止

1,182,800+
勒索軟體 攻擊被阻止

677,100+
Powershell 攻擊被阻止

142,500+
AMSI 事件被阻止

人工智慧驅動的多層次防護

-- 深度防禦

入侵防禦

制敵機先 --
在攻擊到達端點之前阻止攻擊

基於入侵防禦

檔案檢查

透過進階機器學習阻止零日(0-Day)威脅

基於檔案檢查

行為安全

阻止
就地取材威脅

基於行為安全

1 以上數據為2022年4月的數據

保安資訊 SAVETIME INFORMATION SECURITY

Symantec Endpoint Security (SES)

擁有50多項技術，可在整個 MITREATT & CK 規範的攻擊鏈中提供保護和檢測

入侵防禦技術

入侵防禦自動檢測並阻止網路攻擊和瀏覽器攻擊。賽門鐵克的入侵防禦技術是一流的深層封包檢測(DPI；Deep Packet Inspection)引擎，可保護數以千萬計的端點，包括《財星》500大企業和消費者。入侵防禦技術是賽門鐵克緊接在防火牆之後的第一道防線，為用戶端電腦和伺服主機提供保護。

- 每天在威脅獲得初始存取權限和／或執行執行之前，入侵防禦可以保護約**70%到80%**的所有攻擊，從而防止威脅對端點造成的入侵。
- 上個月阻止**513+百萬次**漏洞利用攻擊。
- 超過**2.4+百萬個端點**的**803+百萬次攻擊中有96%**在網路邊界就被阻止，從而防止威脅對端點造成的入侵。其餘**4%**的出埠流量被阻止，切斷與指揮和控制(C&C)的通信。
- 超過**132+千台伺服器**的**105+百萬次攻擊中有93%**在網路邊界被阻止，從而防止威脅對伺服器造成的入侵。其餘**7%**的出埠流量因切斷與指揮和控制的通信而被阻止。

檔案檢查技術

從檔案開始在端點下載的那一刻起，一整個完善的多重技術檔案檢查機制就能檢測和阻止惡意檔案。賽門鐵克密切監控威脅態勢，並採取主動措施來訓練和發布機器學習模型、模擬器和其他內容。該內容為許多威脅家族提供零日預防和啟發式檢測，以及未來可能重新出現的相關威脅。Symantec Endpoint Security能夠運行可攜式可執行檔(PE)和非PE模擬器來處理複雜的封裝工具、混淆程序等，如果允許這些惡意程式在端點的本機上執行，則後續難以遏制其後患無窮的破壞。

- 阻止**3.7+百萬次**威脅~透過經過訓練以防止零日攻擊的進階機器學習(AML)的結果。
- 上個月阻止**70+千個**多個基於x86的混淆惡意軟體的自定義加殼程序（例如：Lokibot）。
- 阻止**142+千個AMSI**事件~代表對終端和最終使用者的資料、應用程式和工作負載的使用者帳戶控制、PowerShell、Office VBA、JavaScript、VBScript和同樣的惡意軟體保護。
- 上個月阻止**691+千次**基於腳本和Powershell的攻擊，例如：Pandex、Emotet和LemonDuck。

行為安全技術

賽門鐵克的行為安全技術會監控端點上所有相關活動，了解正常的應用程序行為模式，並迅速發出警報或阻止偏離規範的行為。攻擊者不再使用通用攻擊工具，而是根據企業環境本身存在的管理或系統工具來定制攻擊。行為技術對命令行檢測、顯示可疑行為的應用程序行為（包括：非PE、DLL和側載）非常有效。

- 上個月，行為安全技術阻止**1.4+百萬個威脅**。
- 來自Conti、Emotet和Ryuk等所有勒索軟體家族的**1.1+百萬次**勒索軟體（和勒索軟體前導程式）活動以及使用Cobalt Strike等工具發起的攻擊都被行為安全技術阻止。
- **1.8+百萬次**被阻止是利用現有工具（例如：PowerShell）的就地取材攻擊。

這對您的企業意味著什麼?

對您的SEP託管端點運行運行狀況檢查，以評估和優化您的安全狀況。