



賽門鐵克勒索軟體防護 適用於不同的情境--解決方案集



INFORMATION SECURITY

業界公認保安資訊--賽門鐵克解決專家

<https://www.savetime.com.tw>

0800-381-500

防範勒索軟體

必須在所有控制點進行深度防禦，才能停止勒索軟體



郵件

*Symantec Email Security.cloud,
Symantec Messaging Gateway*

- 對檔案或檔案中的惡意指標執行靜態分析
- 在電子郵件傳遞和攔截之前，如果有明顯惡意行為跡象在沙箱中引爆潛在的惡意腳本
- 在發送電子郵件之前進行即時連結追蹤，以阻止惡意連結，並在點擊連結後進行分析



網頁

*Symantec Secure Web
Gateway Solutions**

- 阻止惡意網站，包括命令和控制以及加密伺服器
- 使用多層次和即時威脅來源從未知的URL來的檔案進行勒索軟體可疑行為的分析
- 惡意軟體分析會查找特定於勒索軟體的行為，並在傳遞到最終用戶前於沙箱中引爆未知的檔案



端點

*Symantec Endpoint Protection 14,
ATP: Endpoint (EDR)*

- 高級機器學習檢測多變的惡意軟體
- 行為分析揭露勒索軟體的行為時，模擬器會解包逃避性的惡意軟體
- IPS阻止勒索軟體下載加密密鑰的嘗試
- 檢測到勒索軟體時隔離端點，以防止橫向移動
- 在所有端點上搜尋勒索軟體的危害指標 (IoCs)



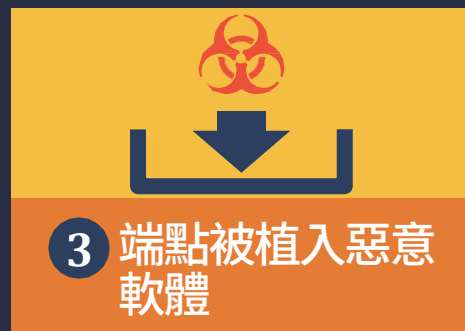
重要主機

*Symantec Data Center Security:
Server Advanced*

- “開箱即用”的IPS規則可以防止勒索軟體執行檔在系統上被植入或執行
- 未使用完整IPS保護的客戶可以部署政策以阻止特定的惡意軟體執行檔
- 可以套用其他規則來阻止所有SMB流入/流出的流量
- 也可以透過將執行檔的哈希值添加到全域黑名單來阻止勒索軟體

*ProxySG, WSS, GIN, Content and Malware Analysis, Security Analytics, SSLV

勒索軟體的攻擊流程



Symantec Email Security.cloud

賽門鐵克郵件安全雲端服務

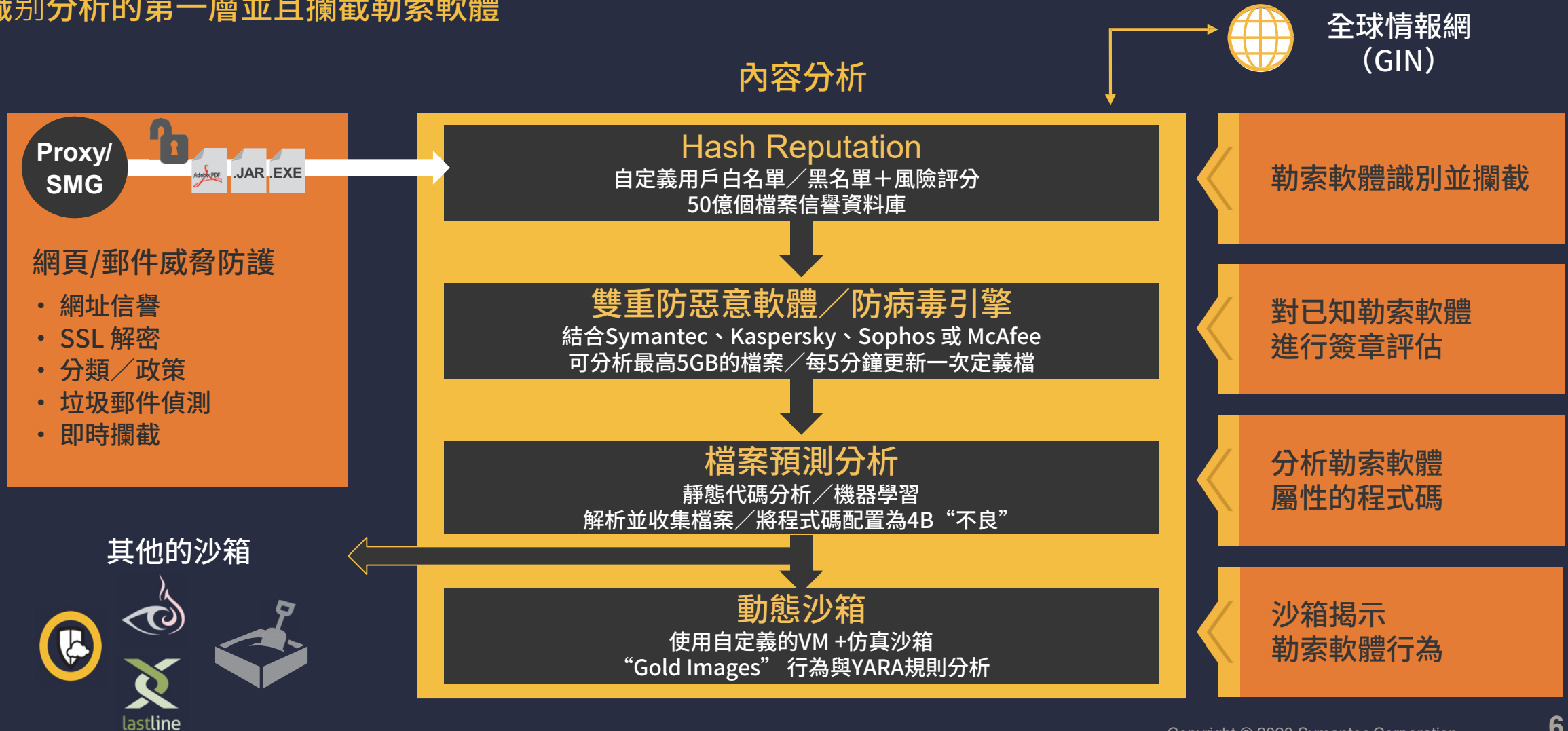


SMG郵件安全閘道的勒索病毒防護



Symantec Content Analysis : APT識別與攔截勒索軟體

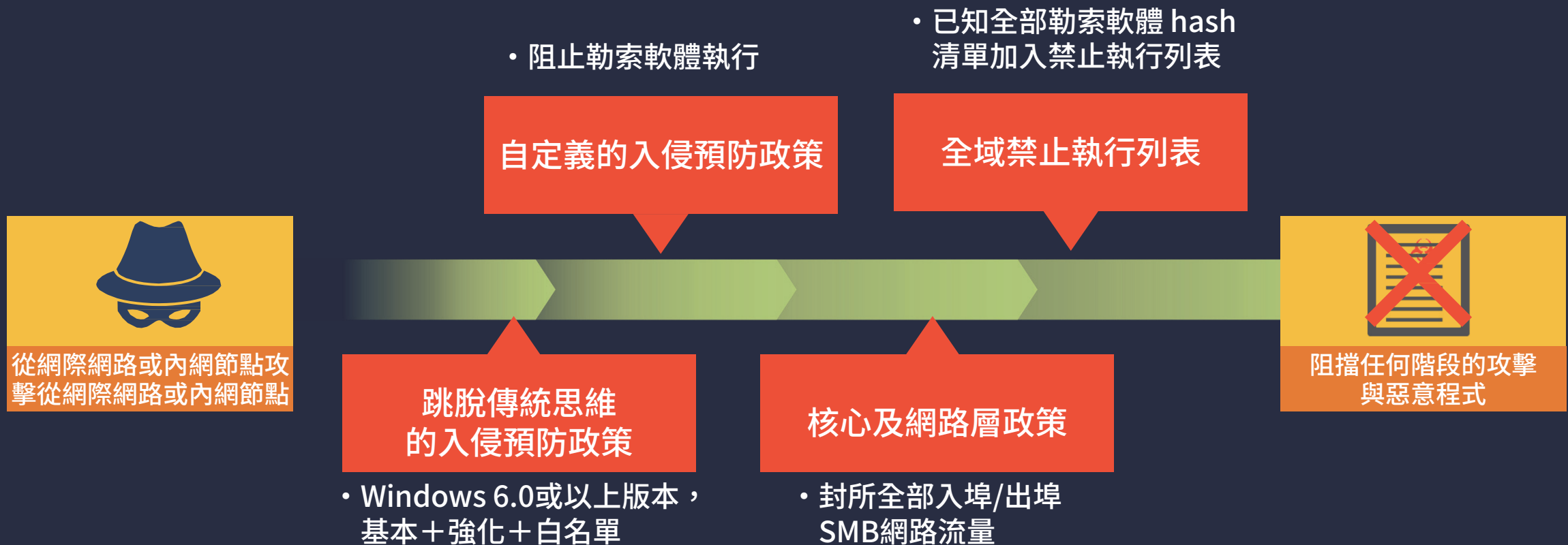
識別分析的第一層並且攔截勒索軟體



SEP 14 端點防護：勒索軟體防護



Data Center Security: 重要主機進階勒索軟體防護



IT Management Suite : 阻止勒索軟體



Cyber Security Services

精準可靠的威脅情資、持續性的威脅監控、針對事件快速回應



Actionable Intelligence

Symantec DeepSight 情資服務

- 在有**攻擊威脅活動**前預先警告
- 排定**修補漏洞**評比／警告的**優先權**以防止勒索軟體
- 深度利用各種威脅情報、動機等……**採取對策**以阻擋攻擊

Continuous Monitoring

Symantec 安全託管服務

- 持續監控勒索軟體傳播度以將受衝擊最小化
- 我們的SOC全天候**24x7**監控全球情報來辨識威脅並**優先**採取行動
- 應用進階的分析和機器學習鑑識從前未知的**風險指標**和**隱形攻擊**

Rapid Response

Symantec 事件快速回應服務

- **快速回應**能抑制現有攻擊，以及減輕未來的攻擊
- 能記錄並重現攻擊鍊過程以確定“**原始感染源**”以及判斷資料是否被加密，刪除或被洩漏
- 用智慧型**取證**工具和**專家**分析尋找進階威脅

相關解決方案型錄下載

- ◆ 端點安全完整版(包含以下元件)：
端點防護、EDR、AD 防護、安全連線……更多
- ◆ SEP 14 端點防護
- ◆ EDR：端點偵測與回應
- ◆ SMG 郵件安全閘道
- ◆ AD 防護
- ◆ DCS 重要主機進階防護
- ◆ CAS 內容分析與沙箱
- ◆ Web Isolation 網頁隔離，遠端瀏覽技術
- ◆ 賽門鐵克郵件安全雲端服務
- ◆ IT Management Suite

- ◆ 新版 Veritas 備份解決方案：
已強化**加密勒索防護**

備份是加密勒索的最後一道防線，如果連備份主機都被加密了，就只能乖乖付贖金，加上拜拜、禱告、祈禱--因為常常付了贖金，也救不回資料。

Veritas Backup Exec 20.4 版之後就將勒索防護功能包含在內，保護備份主機不受勒索威脅，更在 **21 版**強化該功能。

相關簡報檔請[由此下載](#) 。