SE Labs：Symantec Endpoint 安全性能百分百

2023 年 8 月 11 日發布｜專題報導

Adarsh Shetty
Broadcom Inc. Symantec Endpoint Product Manager, Enterprise Endpoint Security Solutions, Broadcom Software

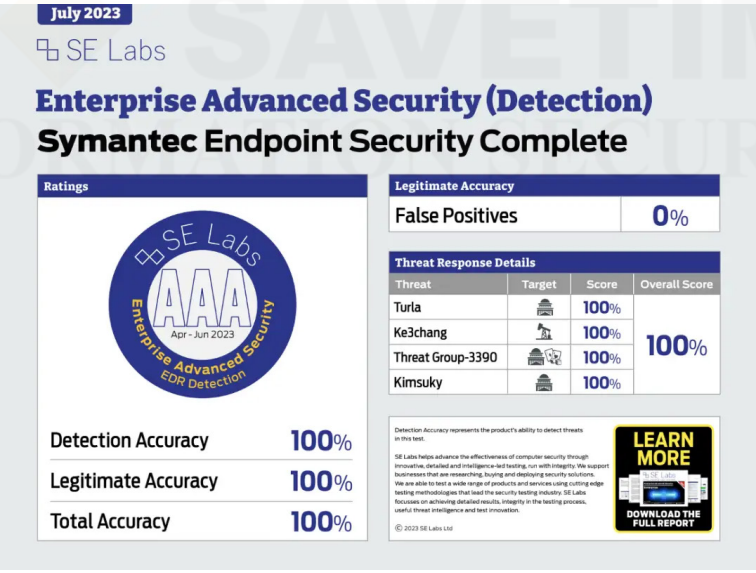
Esther Seguin
Endpoint Marketing Lead, Symantec Endpoint Security

賽門鐵克端點安全完整版的深度縱深防禦和跨控制點可視性脫穎而出

在 SE Labs 的企業進階安全防護的年度評測中，賽門鐵克端點安全完整版 (Symantec Endpoint Security Complete，SES Complete) 連續第二年獲得無懈可擊的滿分成績。

SE Labs 評測是將市面上領導品牌的端點安全產品，暴露在各種漏洞利用、無檔案攻擊和惡意軟體攻擊，是目前所有公開評測中威脅範圍最廣的測試。 測試中的所有攻擊型態都在最近的真實攻擊中出現過。有關該測試的更多詳情，請參閱 SE Labs 2023 年度報告。

SES Complete (賽門鐵克端點安全完整版) 涵蓋所有攻擊鏈不同階段的縱深防禦和跨控制點可視性，增強了賽門鐵克的性能，在測試中脫穎而出並獲得了滿分。



SE Labs 專門從事進階威脅偵測產品的評測，採用 MITRE ATT&CK (對抗策略、技巧和常見知識) 的框架，使用真實世界的攻擊來測試攻擊鏈每一層的威脅反應。因此，全球各地的組織都依賴 SE Labs 的評測來幫助他們選擇端點安全解決方案。

SE Labs 首席執行官 Simon Edwards 表示：「端點偵測與回應 (EDR) 產品不僅僅是防毒軟體。(*EDR 有許多防毒軟體無法提供的高階防護技術、威脅抑制、矯正、調查、回溯等功能與全局可視性)，這就是為何進階測試非常重要的地方。測試人員必須模擬真實的攻擊者，依照攻擊的每一個步驟，才能真正瞭解 EDR 安全產品的功能」。註:(*)為保安資訊補充說明。

Symantec Endpoint Security Complete

Turla

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
1	✓	✓	✓	✓	✓	✓	✓	✓
2	✓	✓	✓	✓	✓	✓	✓	✓
3	✓	✓	✓	✓	✓	✓	✓	✓
4	✓	✓	✓	✓	✓	✓	✓	✓

Ke3chang

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
5	✓	✓	✓	✓	✓	✓	✓	✓
6	✓	✓	✓	✓	✓	✓	✓	✓
7	✓	✓	✓	✓	✓	✓	✓	✓
8	✓	✓	✓	✓	✓	✓	✓	✓

Threat Group-3390

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
9	✓	✓	✓	✓	✓	✓	✓	✓
10	✓	✓	✓	✓	✓	✓	✓	✓
11	✓	✓	✓	✓	✓	✓	✓	✓
12	✓	✓	✓	✓	✓	✓	✓	✓

Kimsuky

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
13	✓	✓	✓	✓	✓	✓	✓	✓
14	✓	✓	✓	✓	✓	✓	✓	✓
15	✓	✓	✓	✓	✓	✓	✓	✓
16	✓	✓	✓	✓	✓	✓	✓	✓

Response Details

Attacker/ APT Group	Number of Incidents	Attacks Detected	Delivery/ Execution	Action	Privilege Escalation/ Action	Lateral Movement/ Action
Turla	4	4	4	4	4	4
Ke3chang	4	4	4	4	4	4
Threat Group-3390	4	4	4	4	4	4
Kimsuky	4	4	4	4	4	4
Total	**16**	**16**	**16**	**16**	**16**	**16**

This data shows how the product handled different group stages of each APT. The Detection and Attacks Detected columns show the basic level of detection.

Detection Accuracy Rating Details

Attacker/ APT Group	Number of Incidents	Attacks Detected	Group Detections	Detection Rating
Turla	4	4	16	160
Ke3chang	4	4	16	160
Threat Group-3390	4	4	16	160
Kimsuky	4	4	16	160
Total	**16**	**16**	**64**	**640**

Different levels of detection, and failure to detect, are used to calculate the Detection Rating.

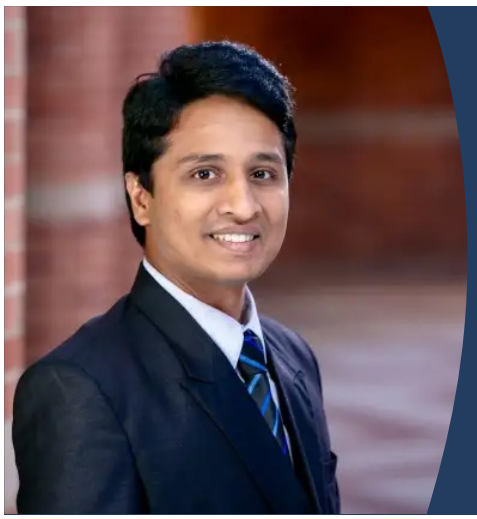
Group Detections

We record detections in groups, as described above in Understanding Detection Groups. To get an overview of how a product handled the entire set of threats we then combine these detections into 'Group Detections'.

In a test with four incidents and four detection groups (Delivery/Execution; Action; Escalation/ PE Action; and Lateral Movement/ Lateral Action) the maximum score would be 16. This is because for each of the four threats a product that detects everything would score 4.

Our overall Detection Rating is based on the number of Detection Groups achieved.

賽門鐵克致力於與 SE Labs 以及 MRG、MITRE 和 AV-Test 等機構進行嚴密的實際測試。SE Labs的企業端點安全 (偵測) 等評測，證明我們在廣泛的數據整合和檢測能力的優勢，並為我們的客戶帶來價值。點擊此處可參考更詳細的 SES Complete 賽門鐵克端點安全版資訊。

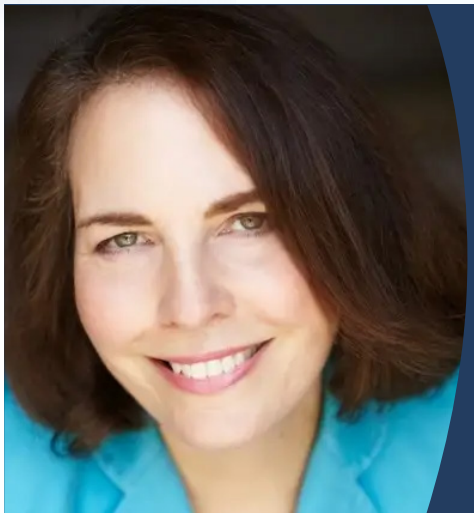


關於作者

Adarsh Shetty
Product Manager, Enterprise Endpoint Security Solutions, Broadcom Software

Adarsh 是 Broadcom 軟體公司 Symantec 的產品經理，主要負責防護成效、資料平臺和威脅情報。他熱衷於資料分析匯整並整合產品，以強化安全解決方案並提高客戶參與度。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/feature-stories/se-labs-says-symantec-endpoint-security-performance-100



關於作者

Esther Seguin
Endpoint Marketing Lead, Symantec Endpoint Security

Esther 為 Symantec Endpoint Security 客戶提供有關當今不斷變化的威脅的見解，以及透過我們的端點安全解決方案擊敗這些威脅的方法。 20 多年來，她致力於幫助企業了解和解決組織中的風險。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力於賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶環境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。保安資訊連絡電話：**0800-381-500**。