

SonicWall Capture Client

勒索軟件和其他基於惡意軟件的攻擊的威脅日益增大，這證明不能僅根據端點合規性來衡量客戶端保護解決方案。傳統防病毒技術采用的是受到長期詬病的基於簽名的方法，這種方法已經無法跟上新出現的惡意軟件和隱蔽技術的步伐。此外，隨著遠程辦公、移動辦公和 BYOD（自帶設備）的湧現，迫切需要隨時隨地為端點提供一致的保護。

SonicWall Capture Client 是一個具有多種保護功能的統一端點產品。借助由 SentinelOne 提供技術支持的下一代惡意軟件防護引擎，Capture Client 應用了先進的威脅防護技術，如機器學習、網絡沙箱集成和系統回滾。通過安裝和管理可信 TLS 證書，Capture Client 還可以利用 SonicWall 防火牆上對加密 TLS 流量的深度檢測（DPI-SSL）。

Capture Client 與 SonicWall Global VPN Client 共存，因此所有產品的策略都可以通過單個雲端管理控制台進行管理。Capture Client 可以通過 Microsoft Active Directory 組策略或任何其他第三方軟件部署技術輕鬆添加到所部署的任何客戶端；也可以通過提供定制 URL 來添加到所部署的任何客戶端，其中客戶端可以靜默地下載並自行安裝，無需任何額外的幹預。此外，與 SonicWall 防火牆集成，Capture Client 可通過可選的強制執行功能在未受保護的客戶端上提供零接觸部署體驗。

功能與好處

持續的端點行為監控有助於獲得文件活動、應用程序和進程活動以及網絡活動的完整概況。這可以防範基於文件和無文件的惡意軟件，並提供全方位的攻擊視圖，其中帶有與調查相關的可操作情報。

多層啟發式保護技術包括雲情報、高級靜態分析和動態行為保護。這些技術有助於防範和清除已知和未知的惡意軟件。

無需定期掃描或定期更新，可隨時提供最高級別的保護，而不會影響用戶的工作效率。Capture Client 在安裝時執行全面掃描，之後持續監控可疑活動。

Capture 高級威脅防護（ATP）集成通過端點無法執行的代碼操作，自動上傳可疑文件進行高級沙箱分析。在更多威脅執行之前阻止它們，例如內置時間延遲的惡意軟件。管理員也可以參考 Capture ATP 的文件裁決數據庫，而無需將文件上傳到雲中進行分析。

獨特的回滾功能還支持相關策略，這些策略不僅可以完全消除威脅，而且還可以將目標客戶端恢復到惡意軟件活動啟動前的狀態。這樣在 Windows 遭遇勒索軟件和類似攻擊的情況下就無需手動恢復。

應用程序漏洞情報使管理員能夠在每個受保護的端點上對每個應用程序以及與之相關的任何風險進行編目。風險基於是否存在任何有通用漏洞披露（CVE）詳細信息的已知漏洞，以及為該版本報告的嚴重性等級，從而為管理員提供可操作的情報以優先安排修補和減小端點的攻擊面。

與 SonicWall 第 6 代及以上防火牆的可選集成可提供零接觸部署和增強的端點合規性。另外，通過向每個端點部署可信證書，該集成還支持執行針對加密流量的深度包檢測（DPI-SSL）。

內容過濾允許組織阻止惡意網站 IP 地址和域，並通過限制帶寬或限制訪問不良或低效網絡內容來提高用戶工作效率。

好處

- 獨立雲端管理
- 與 SonicWall 防火牆協同
- 安全策略執行
- DPI-SSL 證書管理
- 持續行為監控
- 通過機器學習實現高度準確的判斷
- 多層啟發式技術
- 應用程序漏洞情報
- 獨特的回滾功能
- 輕鬆加入白/黑名單
- 用於自動分析惡意軟件的 Capture 高級威脅防護（ATP）雲沙箱
- 免上傳的威脅情報共享，以便手動查文件
- 內容過濾
- 設備控制

設備控制允許組織通過細粒度的白名單策略來阻止可能受感染的設備連接到端點。

集中的管理和客戶端保護報告SonicWall雲端管理控制台作為單一管理平台工作以管理所有客戶端策略，包括下一代惡意軟件防護、DPI-SSL證書管理和內容過濾。

該管理控制台是一個免費提供的多租戶雲端平台。它提供客戶端保護報告和策略管理，支持細粒度訪問控制策略，包括基於Microsoft Active Directory屬性分配策略的能力。這使托管服務提供商（MSP）能夠管理和報告多個客戶的客戶端。同時，其中每個客戶只能管理和報告自己的客戶端。

該管理控制台還充當一個調查平台，可以幫助確定所檢測到的惡意軟件威脅的根源，並提供有關如何防止此類威脅再次發生的可操作情報。例如，管理員可以輕鬆查看哪些應用程序在客戶端上運行。這反過來又可以幫助確定可能在運行易受攻擊或未經授權的軟件的機器。

產品版本和平台支持

SonicWall Capture Client 具有兩種產品版本：

SonicWall Capture Client Basic 提供所有 SonicWall 下一代惡意軟件防護和修復功能，以及DPI-SSL支持功能。

SonicWall Capture Client Advanced提供上面針對Basic版本列出的所有功能，另外還有高級回滾功能、CaptureATP集成、攻擊可視化、應用程序漏洞情報和內容過濾。

兩個版本均可用於Windows 7及更高版本以及Mac OSX。



功能特性比較		
功能特性	Basic	Advanced
雲管理、報告和分析 (CSC)	✓	✓
一體化網絡安全		
端點監視	✓	✓
DPI-SSL 證書部署	✓	✓
內容過濾	–	✓
高級威脅防護		
下一代反惡意軟件	✓	✓
Capture高級威脅防護 (ATP) 沙箱	–	✓
端點檢測和響應		
攻擊可視化	–	✓
回滾和修復	–	✓
設備控制	–	✓
應用程序漏洞和情報	–	✓

系統要求	
操作系統	
Windows7 及更高版本	
Windows Server 2008 R2 及更高版本	
Mac OS/OSX 10.10 及更高版本	
硬件	
1 GHz雙核 CPU 或更高	
1 GB RAM 或更高 (如果操作系統需要) (推薦 2 GB)	
2 GB 可用磁盤空間	

CAPTURE CLIENT SKU		
產品	有效期	SKU
ADVANCED		
SONICWALL CAPTURE CLIENT ADVANCED, 5-24 個端點, 含全天候支持	3 年	02-SSC-1518
SONICWALL CAPTURE CLIENT ADVANCED, 5-24 個端點, 含全天候支持	1 年	02-SSC-1519
SONICWALL CAPTURE CLIENT ADVANCED, 25-49 個端點, 含全天候支持	3 年	02-SSC-1520
SONICWALL CAPTURE CLIENT ADVANCED, 25-49 個端點, 含全天候支持	1 年	02-SSC-1521
SONICWALL CAPTURE CLIENT ADVANCED, 50-99 個端點, 含全天候支持	3 年	02-SSC-1522
SONICWALL CAPTURE CLIENT ADVANCED, 50-99 個端點, 含全天候支持	1 年	02-SSC-1523
SONICWALL CAPTURE CLIENT ADVANCED, 100-249 個端點, 含全天候支持	3 年	02-SSC-1524
SONICWALL CAPTURE CLIENT ADVANCED, 100-249 個端點, 含全天候支持	1 年	02-SSC-1525
SONICWALL CAPTURE CLIENT ADVANCED, 250-499 個端點, 含全天候支持	3 年	02-SSC-1454
SONICWALL CAPTURE CLIENT ADVANCED, 250-499 個端點, 含全天候支持	1 年	02-SSC-1455
SONICWALL CAPTURE CLIENT ADVANCED, 500-999 個端點, 含全天候支持	3 年	02-SSC-1456
SONICWALL CAPTURE CLIENT ADVANCED, 500-999 個端點, 含全天候支持	1 年	02-SSC-1457
SONICWALL CAPTURE CLIENT ADVANCED, 1,000-4,999 個端點, 含全天候支持	3 年	02-SSC-1458
SONICWALL CAPTURE CLIENT ADVANCED, 1,000-4,999 個端點, 含全天候支持	1 年	02-SSC-1459
SONICWALL CAPTURE CLIENT ADVANCED, 5,000-9,999 個端點, 含全天候支持	3 年	02-SSC-1460
SONICWALL CAPTURE CLIENT ADVANCED, 5,000-9,999 個端點, 含全天候支持	1 年	02-SSC-1461
SONICWALL CAPTURE CLIENT ADVANCED, 10,000 個端點以上, 含全天候支持	3 年	02-SSC-1462
SONICWALL CAPTURE CLIENT ADVANCED, 10,000 個端點以上, 含全天候支持	1 年	02-SSC-1463
BASIC		
SONICWALL CAPTURE CLIENT BASIC, 5-24 個端點, 含全天候支持	3 年	02-SSC-1510
SONICWALL CAPTURE CLIENT BASIC, 5-24 個端點, 含全天候支持	1 年	02-SSC-1511
SONICWALL CAPTURE CLIENT BASIC, 25-49 個端點, 含全天候支持	3 年	02-SSC-1512
SONICWALL CAPTURE CLIENT BASIC, 25-49 個端點, 含全天候支持	1 年	02-SSC-1513
SONICWALL CAPTURE CLIENT BASIC, 50-99 個端點, 含全天候支持	3 年	02-SSC-1514
SONICWALL CAPTURE CLIENT BASIC, 50-99 個端點, 含全天候支持	1 年	02-SSC-1515
SONICWALL CAPTURE CLIENT BASIC, 100-249 個端點, 含全天候支持	3 年	02-SSC-1516
SONICWALL CAPTURE CLIENT BASIC, 100-249 個端點, 含全天候支持	1 年	02-SSC-1517
SONICWALL CAPTURE CLIENT BASIC, 250-499 個端點, 含全天候支持	3 年	02-SSC-1444
SONICWALL CAPTURE CLIENT BASIC, 250-499 個端點, 含全天候支持	1 年	02-SSC-1445
SONICWALL CAPTURE CLIENT BASIC, 500-999 個端點, 含全天候支持	3 年	02-SSC-1446
SONICWALL CAPTURE CLIENT BASIC, 500-999 個端點, 含全天候支持	1 年	02-SSC-1447
SONICWALL CAPTURE CLIENT BASIC, 1,000-4,999 個端點, 含全天候支持	3 年	02-SSC-1448
SONICWALL CAPTURE CLIENT BASIC, 1,000-4,999 個端點, 含全天候支持	1 年	02-SSC-1449
SONICWALL CAPTURE CLIENT BASIC, 5,000-9,999 個端點, 含全天候支持	3 年	02-SSC-1450
SONICWALL CAPTURE CLIENT BASIC, 5,000-9,999 個端點, 含全天候支持	1 年	02-SSC-1451
SONICWALL CAPTURE CLIENT BASIC, 10,000 個端點以上, 含全天候支持	3 年	02-SSC-1452
SONICWALL CAPTURE CLIENT BASIC, 10,000 個端點以上, 含全天候支持	1 年	02-SSC-1453

關於 SonicWall

SonicWall 為超分布式時代和每個人都遠程辦公、每個人都移動辦公、每個人都不太安全的工作現實提供了 Boundless Cybersecurity。通過了解未知、提供實時可見性並實現經濟學突破，SonicWall 為世界各地的大型企業、政府和中小企業彌補了網絡安全業務缺口。有關詳情，請訪問 www.sonicwall.com