SONICWALL

# 從我們的窗口您可以盡覽一切

增強意識。實現全面安全管理的整體集成解決方案。

## SONICWALL CAPTURE SECURITY CENTER 易於使用

采用真正的單點登錄(SSO)和單一管理平台(SPOG)體系結構。利用可擴展的管理解決方案來監視您的整個安全生態系統。

**Capture Security Center** (CSC) 為您提供全面管理所需的一切功能，這些功能均可從單個功能豐富的界面訪問。其中涉及到所有方面，包括網絡、無線、電子郵件、端點和雲安全、Risk Meters 和資產管理的分析和報告。

CSC 是一個軟件即服務 (SaaS) 解決方案，通過360度全方位解讀整個 SonicWall 安全生態系統，提高靈活性。它的特點是功能整合，通過真正的 SPOG 接口提高效率和運營彈性。借助詳細的報告和強大的分析功能，可以從任何位置任何可以上網的設備快速、實時地針對任何威脅做出明智的響應。

CSC支持更廣泛的網絡防禦策略，因為其設計符合安全運營中心(SOC)的服務級別要求。它支持統一的安全治理、合規性和許多其他風險管理策略，所有這些都可以從一個可以上網的應用程序完成。

Capture Security Center 是一個真正的 SPOG應用程序，它提供整體和集成的管理解決方案。而且它包含在大多數 SonicWall防火墙和雲服務中。

SONICWALL

# 實現更高的效率和運營彈性

運作效率更高。更快、更智能、更省力地工作。

## Capture Security Center 更高效

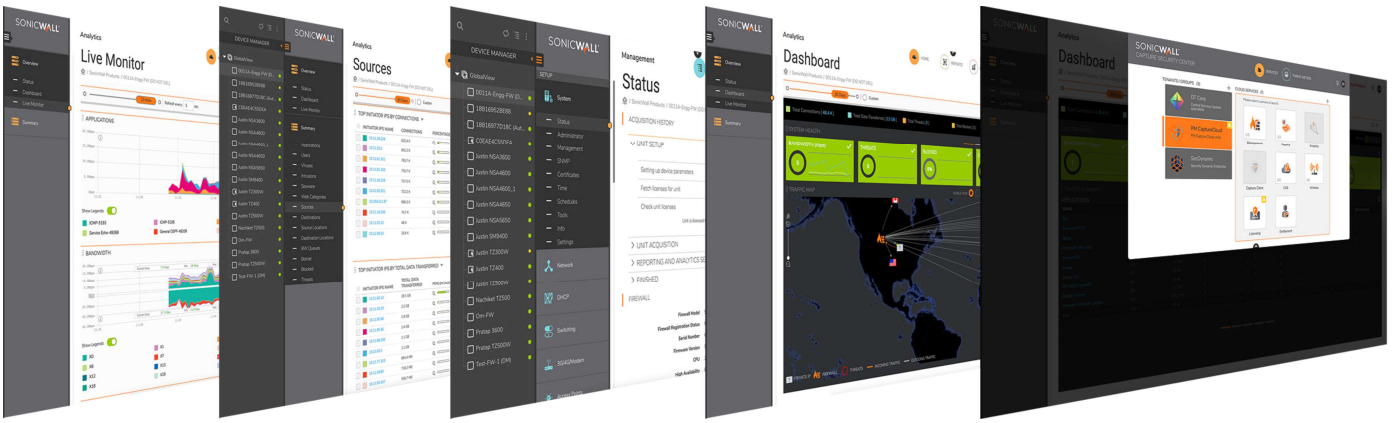
使用 SPOG 管理更多設備。觸及安全基礎設施和網絡中的所有內容，包括體系結構、網絡威脅和合規性問題。

CSC 是一個可以提升生產效率的管理工具，具有內置的可擴展性和更好的管理協調性。

SSO 為您的網絡運營開辟了康莊大道，從雲安全到端點，一切盡在掌控之中。雲原生設計意味著您可以在一個簡單、通通用的框架中擁有所需的一切。每項任務都更簡單、更高效。

減少執行日常任務的時間和費用。消除不必要的安全孤島，並為所有重要的工作流程提高了 " 查看並點擊 " 效率。一旦有新的功能，能立即獲得。

從一個位置管理整個 SonicWall 安全堆棧。利用 Risk Meters 和精確分析，識別安全缺口和風險。利用時間緊迫的威脅信息和情境洞察，更快地做出響應。使用零接觸部署，簡化管理工作流程，減少配置錯誤和人為錯誤，並在分支位置輕松配置遠程防火墻、交換機和訪問點。




雲原生設計提高了效率和運營彈性。減少安全孤島，提高整個安全環境的生產效率，所有這些都可以從一個應用程序完成。

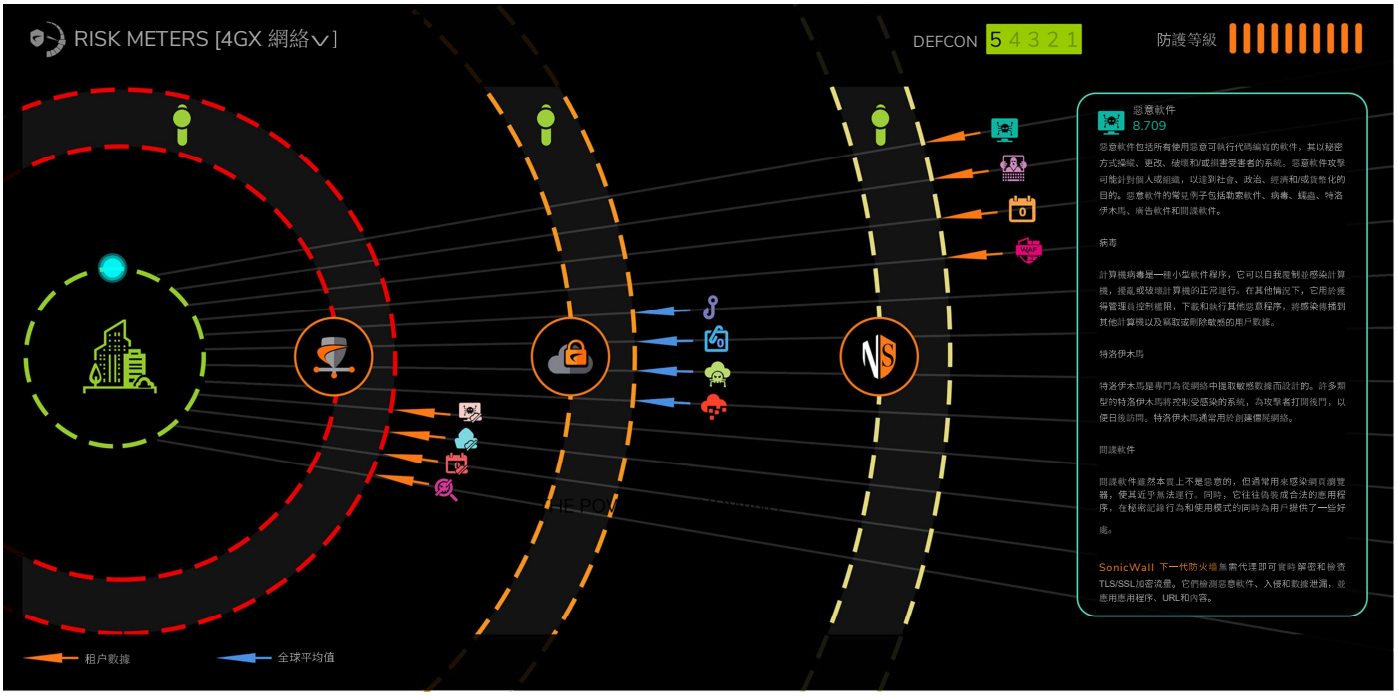
SONICWALL

# 為您的整個網絡提供同步的網絡威脅情報

確保安全。利用真實的數據實時研究您的風險和威脅。

## Capture Security Center 是威脅情報中心

根據您的安全資產的當前狀況與當前的網絡威脅情報合並自定義數據。根據真實的風險數據實時保護您的網絡。




*Risk Meters* 根據實時威脅數據與您當前的保護級別的比較情況，自動顯示威脅數據和風險評分。揭示防禦層的缺口，並做出實時安全決策。根據邏輯評分指導安全規劃、政策和預算決策。

利用 **SonicWall Risk Meters**，您可以根據網絡基礎設施的具體要求，自定義安全評估。通過實時的圖形輔助分析，查看您的網絡面臨的威脅。此內置資源使您的安全團隊可以看到威脅載體，並確定需要采取哪些措施來保護您的網絡。監視從網絡、雲、應用程序、端點、移動設備、數據庫和物聯網(IoT)匯聚到您的網絡上的威脅。直觀呈現潛在的安全缺口，識別入站攻擊，監控所有可能的來源，包括第三方服務，並采取防禦措施。根據實時發生的情況，消除不可預見的攻擊，提高網絡安全態勢。

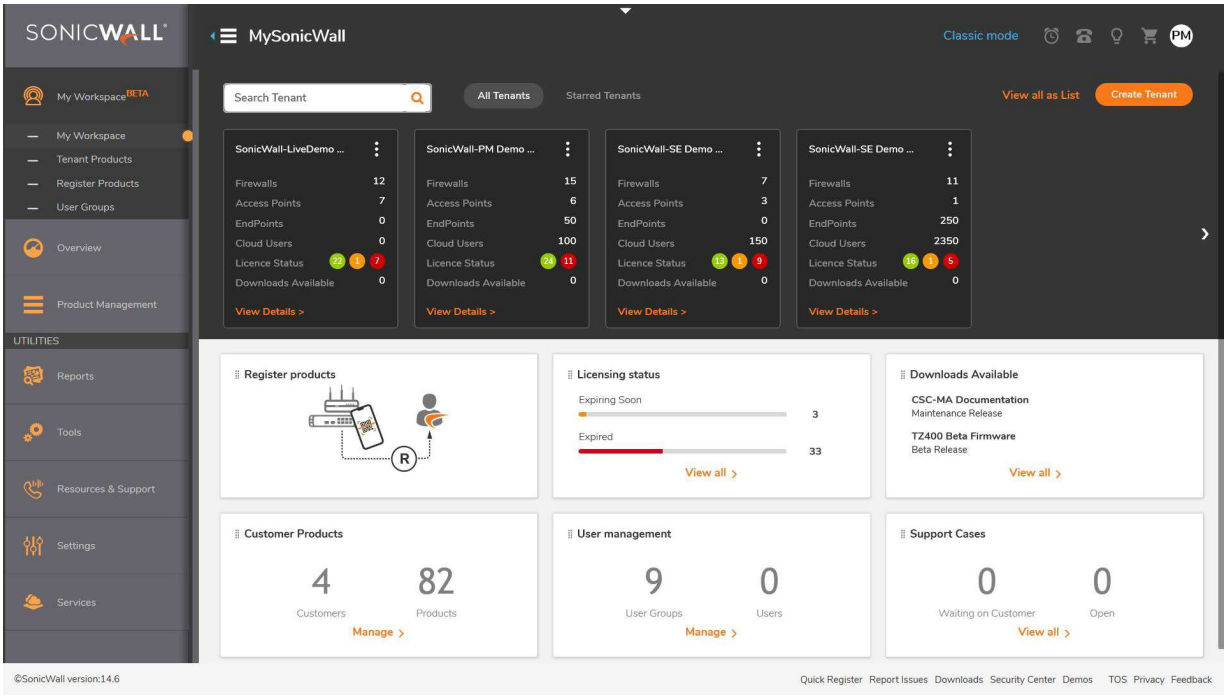
SONICWALL

# 無摩擦地管理安全

掌控一切。從一個位置執行安全操作。

## Capture Security Center 系統而全面

通過單一管理平台全面而深入地了解您的安全環境，以簡化管理和帳戶流程，加快決策制定，改善支持並彌補安全缺口。




My SonicWall 的 My Workspace 可從 Capture Security Center 雲控制台訪問，讓您以更簡單、更高效的方式運行覆雜的安全操作。其系統化的工作流讓您可以輕松快速地加入、設置和管理跨園區、分支機構或職能組的多個租戶，執行批量產品注冊，激活许可证和支持，並按需啟動產品試用。

租戶工作流程為您的安全運營團隊提供跨組織 的即時訪問，包括對Capture Security Center管理的產品進行基於角色的精細訪問控制。直觀的儀表板讓您可以即時查看和了解許可證到期的產品或需要更新軟件或固件的產品。與租戶互動、協作和溝通，並使用內置的自助服務門戶推進、跟蹤和解決問題以及支持案例。

# CSC 功能摘要

## 管理

- SPOG 可訪問大多數功能
- 多個並行用戶會話
- 集中式安全和網絡管理
- 通用儀表板
- 防火墙管理
- SonicWall 交換機管理
- 無線管理
- 聯合策略配置
- 在組級定義策略
- 從設備到單個設備或一組設備的策略覆制
- 更改訂單管理和工作流程
- 零接觸部署
- 零接觸預配置設備配置
- VPN 部署和配置
- 活動設備監控和警報
- 應用程序可視化和情報
- API、CLI 和 SNMP 支持
- Capture Client 管理
- Cloud App Security 管理
- 托管電子郵件安全管理
- MySonicWall 和 MyWorkspace
- Risk Meters
- Security Center
- Cloud App Security – Shadow IT
- 許可證管理
- 基於角色的管理（用户、組）
- 防火墙設備的首選項文件備份

## 監控

- 設備監控和警報
- IPFIX 實時數據流
- 活動設備監控和警報
- SNMP中繼管理
- VPN和防火墙狀態監控
- Risk Meter

## 報告

- 集中式防火墙日志記錄
- 基於 Syslog 或 IPFIX的報告
- 自定義預定的 PDF報告
- 多威脅報告
- 以用戶為中心的報告
- 應用程序使用報告
- 僵屍網絡報告
- Geo IP報告
- MAC 地址報告
- Capture ATP 報告
- 惡意無線接入點報告
- Cloud App Security (CAS) 報告
- Capture Client 報告
- 每個接口的帶寬和服務報告

## 分析

- 基於用戶的活動
- 應用程序使用
- 利用 Capture Client 實現跨產品可見性
- 實時動態可視化
- 向下鑽取和透視功能

# 許可和組合

基於雲的服務有以下幾種組合可供選擇。

### 1. CSC 基本管理 (精簡版)

此版本最適合防火墻系統或首選項的備份/還原以及固件升級。訂閱了 AGSS 或 CGSS的任何防火墻都可以激活此基本管理功能，以幫助管理防火墻。

### 2.CSC 管理

該付費訂閱選項可激活全部管理功能，包括工作流自動化和零接觸部署功能。

### 3.CSC管理與報告

該許可證選項非常適合大型機構，這些機構在組級或基於租戶的管理中在地理位置分散的位置部署了許多防火墻。其中包括具有許多分區和園區的中型市場組織、分布式企業、公共部门和教育组织，以及托管服务提供商 (MSP)。

除了完整的管理功能之外，此訂閱選項還提供完整的報告功能，以執行定期或按需的安全性以及網絡性能檢查和審核。可以使用屏幕上帶有實時圖表和表格的交互式通用儀表板，或在屏幕外使用預定導出的報告來完成。

### 4.CSC 分析

這是所有 Capture Security Center訂閱選項的功能強大的附加服務。激活該服務可完全訪問 SonicWall Analytics 和 SonicWall Cloud App Security 工具和服務，以使用全面的向下鑽取和透視功能進行網絡取證和威脅搜尋。CSC Analytics 還包括30天的回滾日志存儲和365天的報告。

# 支持的防火墻型號

Capture Security Center 適用於使用 SOHO-W、SOHO 250、SOHO 250W、TZ 系列、NSA 系列、NSa 2650-6650 和 NSv 系列防火墻的客戶。對於 SuperMassive 9000 系列、NSa 系列和 NSsp 12400 至 12800，CSC 管理訂閱選項將作為其相應 AGSS 訂閱激活的一部分自動激活。

| CAPTURE SECURITY CENTER | | | |
|---|---|---|---|
| | 管理 | 報告[4] | 分析[4] |
| 入門級固件 | SOHO-W、SOHO 250、SOHO 250W TZ 系列、NSv 10-100 | SOHO-W、SOHO 250、SOHO 250W、TZ 系列、NSv 10-100 | SOHO-W、SOHO 250、SOHO 250W、TZ 系列、NSv 10-100 |
| 中端固件 | NSA 系列、NSa 系列、NSv 200-400 | NSA 系列、NSa 系列、NSv 200-400 | NSA 系列、NSa 系列、NSv 200-400 |
| 高端固件 | SuperMassive 9000 系列、NSsp 12000 系列、NSa 9250-9650、NSv 800-1600 | SuperMassive 9000 系列、NSsp 12000 系列、NSa 9250-9650、NSv 800-1600 | SuperMassive 9000 系列、NSsp 12000 系列、NSa 9250-9650、NSv 800-1600 |

[4] 僅 On_prem Analytics 上提供對高端固件的報告和分析的支持。

| | 特色 | CSC 管理（精簡版） | CSC 管理 | CSC 管理與報告 | SaaS 分析 | 內部分析 |
|---|---|---|---|---|---|---|
| 管理 | 備份/還原 – 防火墙系统 | 是 | 是 | 是 | 是 | 是[2] |
| | 備份/還原 – 防火墙首选项 | 是 | 是 | 是 | 是 | 是[2] |
| | 固件升級 | 僅來自本地文件 | 僅來自本地文件或 MySonicWall | 是 | 僅來自本地文件 | 僅來自本地文件[3] |
| | 任務計劃 | - | 是 | 是 | - | - |
| | 組防火墙管理 | - | 是 | 是 | - | - |
| | 繼承 – 正向/反向 | - | 是 | 是 | - | - |
| | 零接觸部署1 | - | 是 | 是 | - | - |
| | 離線防火墙簽名下載 | - | 是 | 是 | - | - |
| | 工作流程 | - | 是 | 是 | - | - |
| | 匯集的許可證 – 搜索、共享使用的激活碼清單 | - | 是 | 是 | - | - |
| 報告 (基於 Netflow/ IPFIX) | 計劃報告、實時監控器、摘要儀表板 | - | - | 是 | 是 | 是 |
| | 下載報告：應用程序、威脅、CFS、用户、流量、源/目標（1 年流量報告） | - | - | 是 | 是 | 是 |
| 分析 (基於 Netflow/ IPFIX) | 使用向下鉆取和透視進行網絡取證和威脅搜尋 | - | - | - | 是 | 是 |
| | Cloud App Security – Shadow IT | - | - | - | 是 | 否 |
| | 數據保留 | - | - | - | 30 天流量 | 1 年 |
| 技術支持 | | 僅限網絡案例 | 全天候支持 | 全天候支持 | 全天候支持 | 全天候支持 |

1 支持帶有固件 6.5.2+ 的 SOHO-W；TZ、NSA 系列和帶有固件 6.5.1.1+ 的 NSa 2650-6650。不支持 SOHO 或 NSv 系列。
2 需要 AGSS/CGSS 服務或任何付費的 Capture Security Center 服務
3 需要全天候支持許可證

# 訂購信息

## 產品

| | SKU |
|---|---|
| SonicWall Capture Security Center Management，適用於 TZ 系列、SOHO-W、SOHO 250、SOHO 250W、NSv 10 到 100 1 年 | 01-SSC-3664 |
| SonicWall Capture Security Center Management，適用於 TZ 系列、SOHO-W、SOHO 250、SOHO 250W NSv 10 到 100 2 年 | 01-SSC-9151 |
| SonicWall Capture Security Center Management，適用於 TZ 系列、SOHO-W、SOHO 250、SOHO 250W NSv 10 到 100 3 年 | 01-SSC-9152 |
| SonicWall Capture Security Center Management，適用於 NSA 2600 到 6600、NSa 2650 到 6650 和 NSv 200 到 400 1 年 | 01-SSC-3665 |
| SonicWall Capture Security Center Management，適用於 NSA 2600 到 6600、NSa 2650 到 6650 和 NSv 200 到 400 2 年 | 01-SSC-9214 |
| SonicWall Capture Security Center Management，適用於 NSA 2600 到 6600、NSa 2650 到 6650 和 NSv 200 到 400 3 年 | 01-SSC-9215 |
| SonicWall Capture Security Center Management and Reporting，適用於 TZ 系列、SOHO-W、SOHO 250、SOHO 250W、NSv 10 到 100 1 年 | 01-SSC-3435 |
| SonicWall Capture Security Center Management and Reporting，適用於 TZ 系列、SOHO-W、SOHO 250、SOHO 250W、NSv 10 到 100 2 年 | 01-SSC-9148 |
| SonicWall Capture Security Center Management and Reporting，適用於 TZ 系列、SOHO-W、SOHO 250、SOHO 250WNSv 10 到 100 3 年 | 01- C-9149 |
| SonicWall Capture Security Center Management and Reporting，適用於 NSA 2600 到 6600、NSa 2650 到 6650 和NSv 200 到 400 1 年 | 01-SSC-3879 |
| SonicWall Capture Security Center Management and Reporting，適用於 NSA 2600 到 6600、NSa 2650 到 6650 和NSv 200 到 400 2 年 | 01-SSC-9154 |
| SonicWall Capture Security Center Management and Reporting，適用於 NSA 2600 到 6600、NSa 2650 到 6650 和NSv 200 到 400 3 年 | 01-SSC-9202 |
| SonicWall Capture Security Center Analytics，適用於 SOHO-W、SOHO 250、SOHO 250W、TZ 系列、NSv 10 到 100 1 年 | 02-SSC-0171 |
| SonicWall Capture Security Center Analytics，適用於 NSA 2600 到 6600、NSa 2650 到 6650 和 NSv 200 到 400 1 年 | 02-SSC-0391 |

## 互聯網瀏覽器

- Microsoft® Internet Explorer 11.0 或更高版本（不使用兼容模式）
- Mozilla Firefox 37.0 或更高版本
- Google Chrome 42.0 或更高版本
- Safari（最新版本）

## 由 Capture Security Center 管理的支持的 SonicWall 設備

- SonicWall網絡安全設備: SuperMassive E10000 和 9000 系列、E-Class NSA、NSsp 系列、NSa 系列、TZ 系列、SOHO-W、SOHO 250、SOHO 250W
- SonicWall Network Security Virtual 設備: NSv 系列
- SonicWall Endpoint Security – Capture Client
- SonicWall Cloud Security – Cloud App Security (CAS)
- SonicWall Email Security
- SonicWall Web Application Firewall
- SonicWall Secure Mobile Access 系列

## 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

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas CA 95035
有關詳情，請訪問我們的網站。
www.sonicwall.com


Datasheet-CaptureSecurityCenter-US-COG-2315