SONICWALL

从我们的窗口您可以尽览一切

增强意识。实现全面安全管理的整体集成解决方案。

SONICWALL CAPTURE SECURITY CENTER 易于使用

采用真正的单点登录 (SSO) 和单一管理平台 (SPOG) 体系结构。利用可扩展的管理解决方案来监视您的整个安全生态系统。

Capture Security Center (CSC) 为您提供全面管理所需的一切功能，这些功能均可从单个功能丰富的界面访问。其中涉及到所有方面，包括网络、无线、电子邮件、端点和云安全、Risk Meters 和资产管理的分析和报告。

CSC 是一个软件即服务 (SaaS) 解决方案，通过 360 度全方位解读整个 SonicWall 安全生态系统，提高灵活性。它的特点是功能整合，通过真正的 SPOG 接口提高效率和运营弹性。借助详细的报告和强大的分析功能，可以从任何位置任何可以上网的设备快速、实时地针对任何威胁做出明智的响应。

CSC 支持更广泛的网络防御策略，因为其设计符合安全运营中心 (SOC) 的服务级别要求。它支持统一的安全治理、合规性和许多其他风险管理策略，所有这些都可以从一个可以上网的应用程序完成。

Capture Security Center 是一个真正的 SPOG 应用程序，它提供整体和集成的管理解决方案。而且它包含在大多数 SonicWall 防火墙和云服务中。

SONICWALL

实现更高的效率和运营弹性

运作效率更高。更快、更智能、更省力地工作。

Capture Security Center 更高效

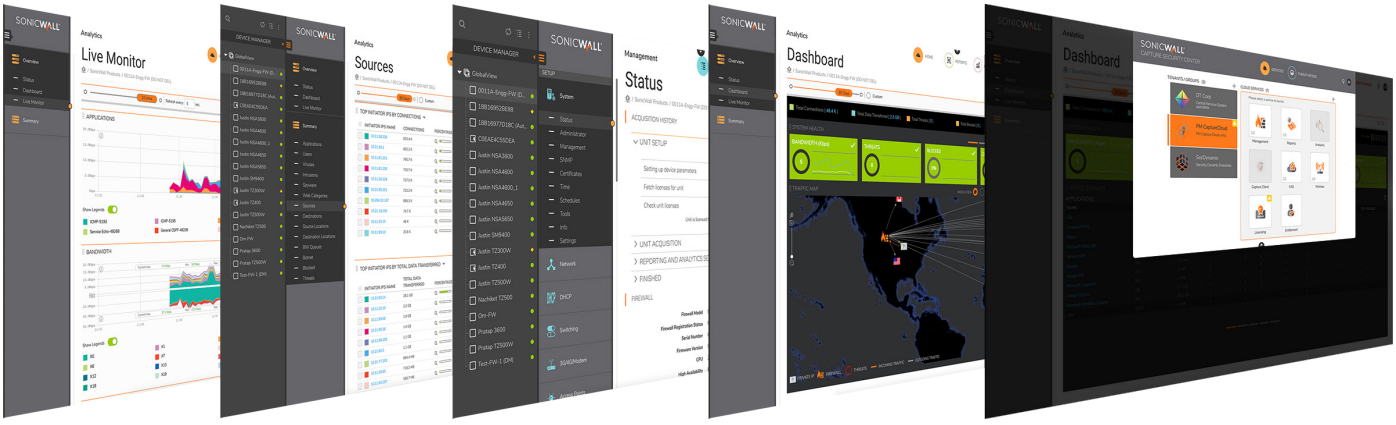
使用 SPOG 管理更多设备。触及安全基础设施和网络中的所有内容，包括体系结构、网络威胁和合规性问题。

CSC 是一个可以提升生产效率的管理工具，具有内置的可扩展性和更好的管理协调性。

SSO 为您的网络运营开辟了康庄大道，从云安全到端点，一切尽在掌控之中。云原生设计意味着您可以在一个简单、通用的框架中拥有所需的一切。每项任务都更简单、更高效。

减少执行日常任务的时间和费用。消除不必要的安全孤岛，并为所有重要的工作流程提高了“查看并点击”效率。一旦有新的功能，能立即获得。

从一个位置管理整个 SonicWall 安全堆栈。利用 Risk Meters 和精确分析，识别安全缺口和风险。利用时间紧迫的威胁信息和情境洞察，更快地做出响应。使用零接触部署，简化管理工作流程，减少配置错误和人为错误，并在分支位置轻松配置远程防火墙、交换机和访问点。



云原生设计提高了效率和运营弹性。减少安全孤岛，提高整个安全环境的生产效率，所有这些都可以从一个应用程序完成。

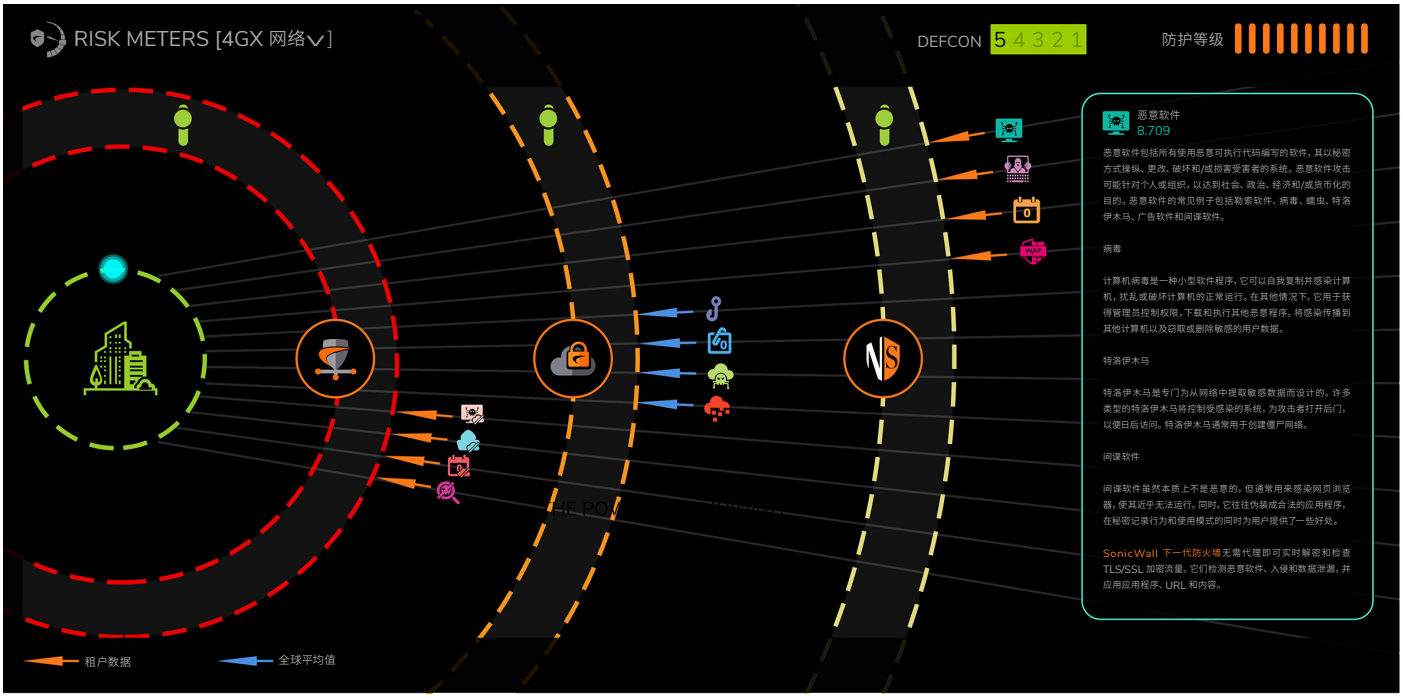
SONICWALL

为您的整个网络提供同步的网络威胁情报

确保安全。利用真实的数据实时研究您的风险和威胁。

Capture Security Center 是威胁情报中心

根据您的安全资产的当前状况与当前的网络威胁情报合并自定义数据。根据真实的风险数据实时保护您的网络。



Risk Meters 根据实时威胁数据与您当前的保护级别的比较情况，自动显示威胁数据和风险评分。揭示防御层的缺口，并做出实时安全决策。根据逻辑评分指导安全规划、政策和预算决策。

利用 **SonicWall Risk Meters**，您可以根据网络基础设施的具体要求，自定义安全评估。通过实时的图形辅助分析，查看您的网络面临的威胁。此内置资源使您的安全团队可以看到威胁载体，并确定需要采取哪些措施来保护您的网络。监视从网络、云、应用程序、端点、移动设备、数据库和物联网 (IoT) 汇聚到您的网络上的威胁。直观呈现潜在的安全缺口，识别入站攻击，监控所有可能的来源，包括第三方服务，并采取防御措施。根据实时发生的情况，消除不可预见的攻击，提高网络安全态势。

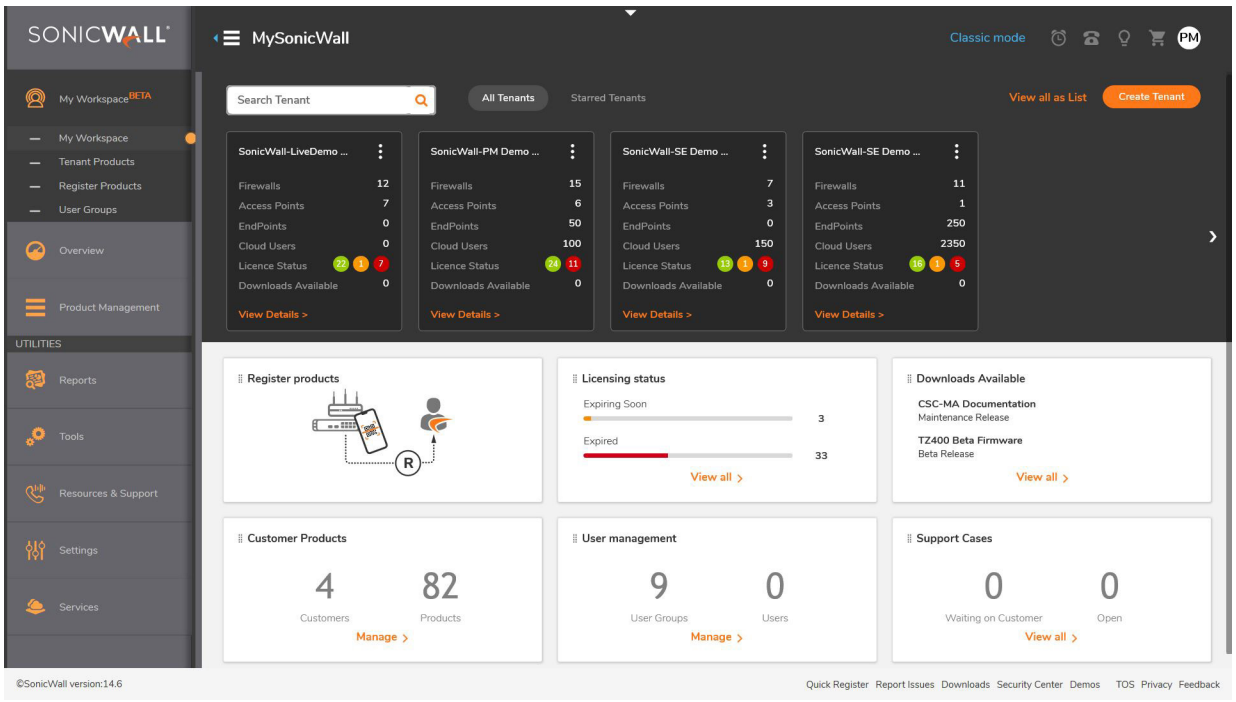
SONICWALL

无摩擦地管理安全

掌控一切。从一个位置执行安全操作。

Capture Security Center 系统而全面

通过单一管理平台全面而深入地了解您的安全环境，以简化管理和帐户流程，加快决策制定，改善支持并弥补安全缺口。



My SonicWall 的 My Workspace 可从 Capture Security Center 云控制台访问，让您以更简单、更高效的方式运行复杂的安全操作。其系统化的工作流让您可以轻松快速地加入、设置和管理跨园区、分支机构或职能组的多个租户，执行批量产品注册，激活许可证和支持，并按需启动产品试用。

租户工作流程为您的安全运营团队提供跨组织的即时访问，包括对 Capture Security Center 管理的产品进行基于角色的精细访问控制。直观的仪表板让您可以即时查看和了解许可证到期的产品或需要更新软件或固件的产品。与租户互动、协作和沟通，并使用内置的自助服务门户推进、跟踪和解决问题以及支持案例。

CSC 功能摘要

管理

- SPOG 可访问大多数功能
- 多个并行用户会话
- 集中式安全和网络管理
- 通用仪表板
- 防火墙管理
- SonicWall 交换机管理
- 无线管理
- 联合策略配置
- 在组级定义策略
- 从设备到单个设备或一组设备的策略复制
- 更改订单管理和工作流程
- 零接触部署
- 零接触预配置设备配置
- VPN 部署和配置
- 活动设备监控和警报
- 应用程序可视化和情报
- API、CLI 和 SNMP 支持
- Capture Client 管理
- Cloud App Security 管理
- 托管电子邮件安全管理
- MySonicWall 和 MyWorkspace
- Risk Meters
- Security Center
- Cloud App Security – Shadow IT
- 许可证管理
- 基于角色的管理（用户、组）
- 防火墙设备的首选项文件备份

监控

- 设备监控和警报
- IPFIX 实时数据流
- 活动设备监控和警报
- SNMP 中继管理
- VPN 和防火墙状态监控
- Risk Meters

报告

- 集中式防火墙日志记录
- 基于 Syslog 或 IPFIX 的报告
- 自定义预定的 PDF 报告
- 多威胁报告
- 以用户为中心的报告
- 应用程序使用报告
- 僵尸网络报告
- Geo IP 报告
- MAC 地址报告
- Capture ATP 报告
- 恶意无线接入点报告
- Cloud App Security (CAS) 报告
- Capture Client 报告
- 每个接口的带宽和服务报告

分析

- 基于用户的活动
- 应用程序使用
- 利用 Capture Client 实现跨产品可见性
- 实时动态可视化
- 向下钻取和透视功能

许可和组合

基于云的服务有以下几种组合可供选择。

1. CSC 基本管理 (精简版)

此版本最适合防火墙系统或首选项的备份/还原以及固件升级。订阅了 AGSS 或 CGSS 的任何防火墙都可以激活此基本管理功能，以帮助管理防火墙。

2.CSC 管理

该付费订阅选项可激活全部管理功能，包括工作流自动化和零接触部署功能。

3.CSC 管理与报告

该许可证选项非常适合大型机构，这些机构在组级或基于租户的管理中在地理位置分散的位置部署了许多防火墙。其中包括具有许多分区和园区的中型市场组织、分布式企业、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，此订阅选项还提供完整的报告功能，以执行定期或按需的安全性以及网络性能检查和审核。可以使用屏幕上带有实时图表和表格的交互式通用仪表板，或在屏幕外使用预定导出的报告来完成。

4.CSC 分析

这是所有 Capture Security Center 订阅选项的功能强大的附加服务。激活该服务可完全访问 SonicWall Analytics 和 SonicWall Cloud App Security 工具和服务，以使用全面的向下钻取和透视功能进行网络取证和威胁搜寻。CSC Analytics 还包括 30 天的回滚日志存储和 365 天的报告。

支持的防火墙型号

Capture Security Center 适用于使用 SOHO-W、SOHO 250、SOHO 250W、TZ 系列、NSA 系列、NSa 2650-6650 和 NSv 系列防火墙的客户。对于 SuperMassive 9000 系列、NSa 系列和 NSsp 12400 至 12800，CSC 管理订阅选项将作为其相应 AGSS 订阅激活的一部分自动激活。

CAPTURE SECURITY CENTER			
	管理	报告[4]	分析[4]
入门级固件	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] *仅 On_prem Analytics 上提供对高端固件的报告和分析的支持。*

	特色	CSC 管理（精简版）	CSC 管理	CSC 管理与报告	SaaS 分析	内部分析
管理	备份/还原 – 防火墙系统	是	是	是	是	是[2]
	备份/还原 – 防火墙首选项	是	是	是	是	是[2]
	固件升级	仅来自本地文件	仅来自本地文件或 MySonicWall	是	仅来自本地文件	仅来自本地文件[3]
	任务计划	-	是	是	-	-
	组防火墙管理	-	是	是	-	-
	继承 – 正向/反向	-	是	是	-	-
	零接触部署[1]	-	是	是	-	-
	离线防火墙签名下载	-	是	是	-	-
	工作流程	-	是	是	-	-
	汇集的许可证 – 搜索、共享、使用的激活码清单	-	是	是	-	-
报告（基于 Netflow/IPFIX）	计划报告、实时监控器、摘要仪表板	-	-	是	是	是
	下载报告：应用程序、威胁、CFS、用户、流量、源/目标（1 年流量报告）	-	-	是	是	是
分析（基于 Netflow/IPFIX）	使用向下钻取和透视进行网络取证和威胁搜寻	-	-	-	是	是
	Cloud App Security – Shadow IT	-	-	-	是	否
	数据保留	-	-	-	30 天流量	1 年
技术支持		仅限网络案例	全天候支持	全天候支持	全天候支持	全天候支持

[1] *支持带有固件 6.5.2+ 的 SOHO-W；TZ、NSA 系列和带有固件 6.5.1.1+ 的 NSa 2650-6650。不支持 SOHO 或 NSv 系列。*
[2] *需要 AGSS/CGSS 服务或任何付费的 Capture Security Center 服务*
[3] *需要全天候支持许可证*

订购信息

产品	SKU
SonicWall Capture Security Center Management，适用于 TZ 系列、SOHO-W、SOHO 250、SOHO 250W、NSv 10 到 100 1 年	01-SSC-3664
SonicWall Capture Security Center Management，适用于 TZ 系列、SOHO-W、SOHO 250、SOHO 250W NSv 10 到 100 2 年	01-SSC-9151
SonicWall Capture Security Center Management，适用于 TZ 系列、SOHO-W、SOHO 250、SOHO 250W NSv 10 到 100 3 年	01-SSC-9152
SonicWall Capture Security Center Management，适用于 NSA 2600 到 6600、NSa 2650 到 6650 和 NSv 200 到 400 1 年	01-SSC-3665
SonicWall Capture Security Center Management，适用于 NSA 2600 到 6600、NSa 2650 到 6650 和 NSv 200 到 400 2 年	01-SSC-9214
SonicWall Capture Security Center Management，适用于 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，适用于 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，适用于 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，适用于 TZ 系列、SOHO-W、SOHO 250、SOHO 250W NSv 10 到 100 3 年	01-SSC-9149
SonicWall Capture Security Center Management and Reporting，适用于 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，适用于 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，适用于 NSA 2600 到 6600、NSa 2650 到 6650 和 NSv 200 到 400 3 年	01-SSC-9202
SonicWall Capture Security Center Analytics，适用于 SOHO-W、SOHO 250、SOHO 250W、TZ 系列、NSv 10 到 100 1 年	02-SSC-0171
SonicWall Capture Security Center Analytics，适用于 NSA 2600 到 6600、NSa 2650 到 6650 和 NSv 200 到 400 1 年	02-SSC-0391

互联网浏览器

- 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 设备

- SonicWall 网络安全设备：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 设备：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 AccessSMA 100 系列

关于 SonicWall

SonicWall 为超分布式时代和每个人都远程办公、每个人都移动办公、每个人都不太安全的工作现实提供了 Boundless Cybersecurity。通过了解未知、提供实时可见性并实现经济学突破，SonicWall 为世界各地的大型企业、政府和中小企业弥补了网络安全业务缺口。有关详情，请访问 www.sonicwall.com。

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
有关详情，请访问我们的网站。
www.sonicwall.com

Datasheet-CaptureSecurityCenter-US-COG-2315