

You Can See Everything From Our Windows

Be more aware. A holistic integrated solution for total security management.

SONICWALL CAPTURE SECURITY CENTER IS EASY

with true Single-Sign-On (SSO) and Single-Pane-of-Glass (SPOG) architecture. Watch over your entire security ecosystem with a scalable management solution.

Capture Security Center (CSC) gives you everything you need for comprehensive management, accessible from a single function-packed interface. It touches everything, including analytics and reporting for network, wireless, email, endpoint and cloud security, Risk Meters and asset management.

CSC is a SaaS solution that gives you greater agility with a 360° view of your entire SonicWall security ecosystem. It features functional integration for better efficiency and operational elasticity with a true SPOG interface. Make informed

responses to any threat, quickly, in real time—from any location and any web-enabled device—with detailed reporting and powerful analytics.

CSC supports your broader cyber defense strategy because its design conforms with service level requirements for Security Operation Centers (SOCs). It enables unified security governance, compliance and many other risk management strategies, all from one web-enabled app.



Capture Security Center is a true SPOG application that provides a holistic and integrated management solution. And it's included with most SonicWall firewalls and cloud services.

Management Reports Analytics

Capture Client CAS-Shadow IT CAS-SaaS Security

Email Security Wireless Licensing

Entitlement

CAPTURE SECURITY CENTER

Cloud-delivered unified management, reporting and analytics for network, wireless, switch, endpoint, email and cloud security

LEARN MORE

Gain Greater Efficiencies and Operational Elasticity

Be more effective. Work faster and smarter with less effort.

CAPTURE SECURITY CENTER IS MORE EFFICIENT

Manage more with a SPOG. Touch everything in your security infrastructure and network including architecture, cyber-threats, and compliance issues.

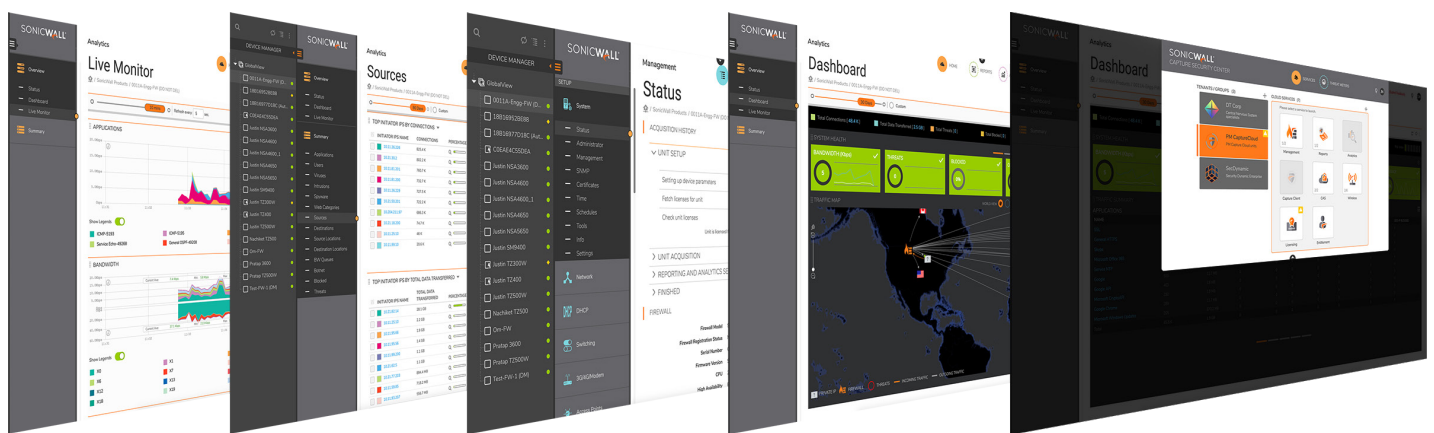
CSC is a productivity management tool with built-in scalability and better management coordination.

SSO opens up every operational aspect of your network—from cloud security to endpoint. Cloud-native design means you have everything you need in a simple, common framework. Every task is easier and more effective.

Reduce time and expense of performing every-day tasks. Eliminate unnecessary security silos and gain

“see-and-click” efficiency for all vital workflows. Acquire new capabilities as soon as they are available.

Manage your entire SonicWall security stack from one place. Identify security gaps and risks with Risk Meters and precise analytics. Respond faster with time-critical threat information and situational insights. Simplify management workflow, reduce misconfigurations and human errors, and easily provision remote firewalls, switches and access points at branch locations using Zero-Touch Deployment.



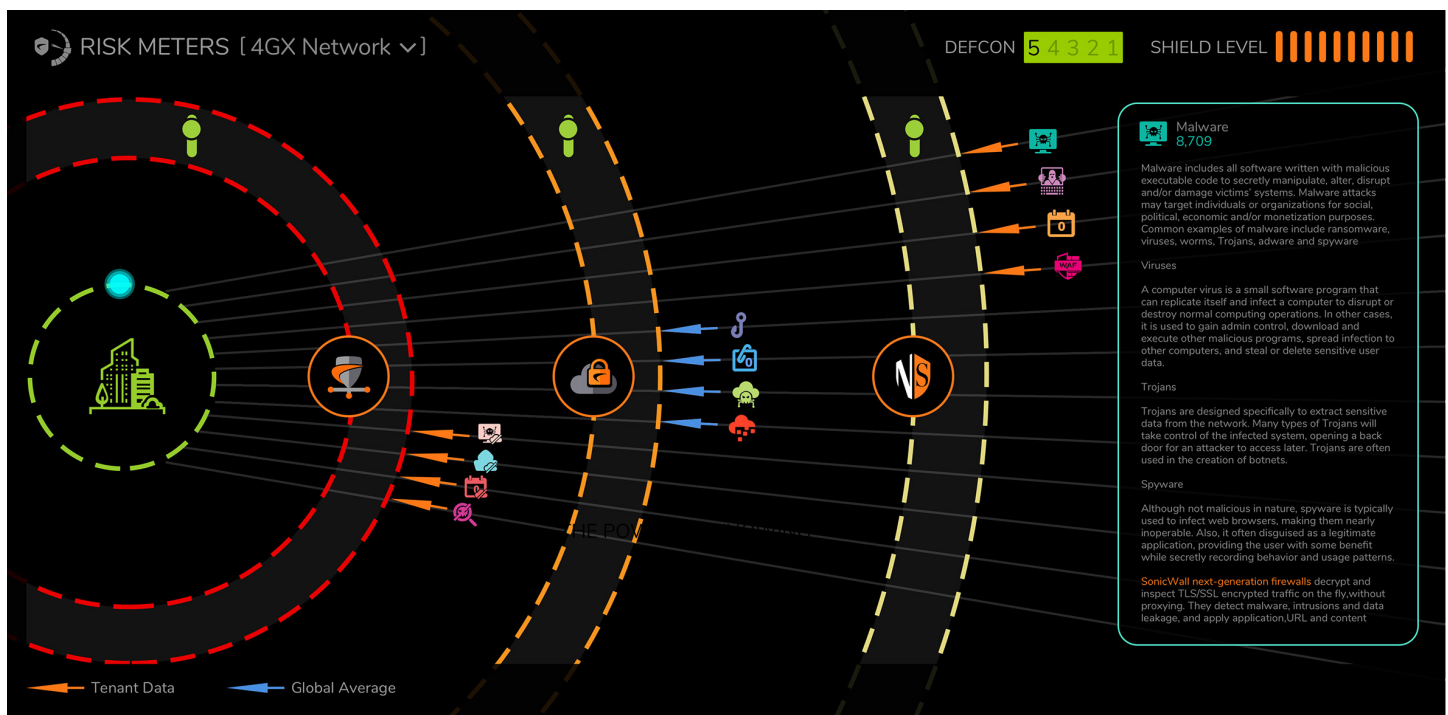
Cloud-native design increases efficiency and operational elasticity. Reduce security silos, increase productivity for the entire security environment—all from one app.

Synchronized Cyberthreat Intelligence for Your Entire Network

Be secure. Study your risks and threats, in real time with real world data.

CAPTURE SECURITY CENTER IS THREAT INTELLIGENT

Merge customized data based on the present condition of your security assets with current cyber-threat intelligence. Defend your network based on real-world risk data—in real time.



Risk Meters automatically show threat data and risk scores based on live threat data compared with your present level of protection. Reveal gaps in defensive layers, and make real-time security decisions. Guide security planning, policy and budgeting decisions based on logical scoring.

With **SonicWall Risk Meters**, you can customize your security assessment based on specific requirements of your network infrastructure. See the threats that confront your network projected in a real-time, graphics-assisted analysis. This built-in resource

allows your security teams to see threat vectors and identify what needs to be done to defend your network. Watch threats converge on your network from the web, cloud, applications, endpoints, mobile devices, databases and IoT. Visualize potential security

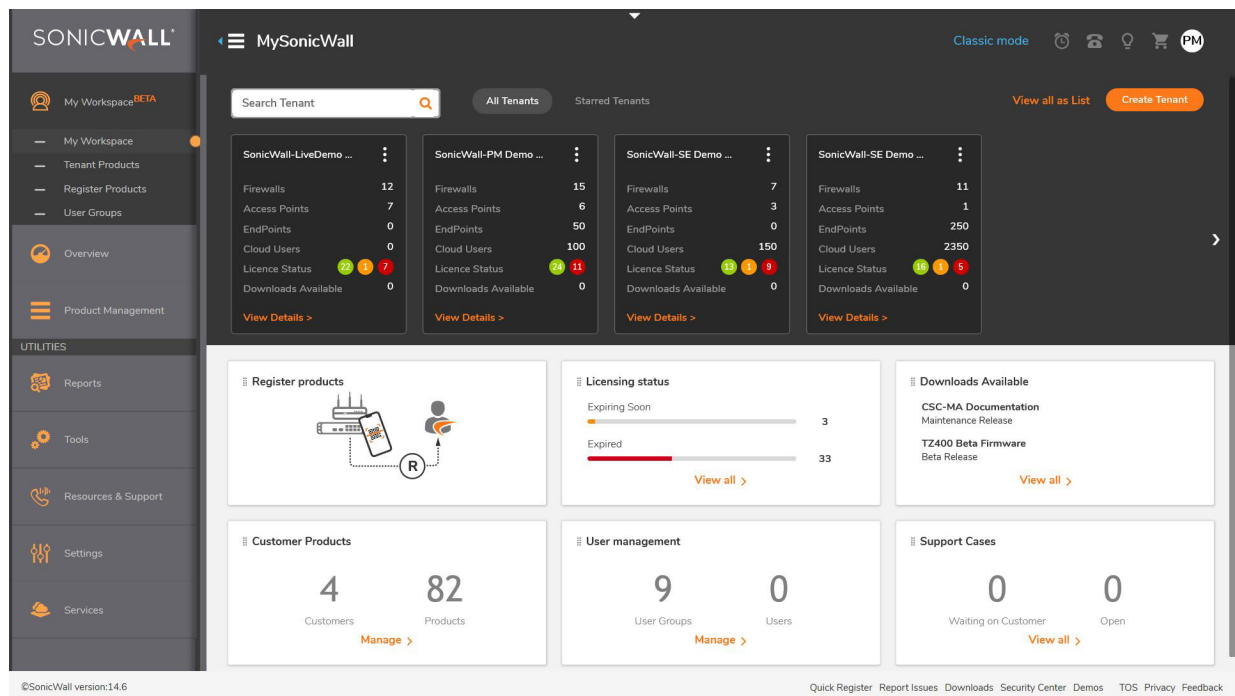
gaps, recognize incoming attacks, monitor all possible sources, including third-party services, and take defensive action. Eliminate unforeseen attacks and boost your network security posture based on what's happening in real time.

Manage Security Without Friction

Be in control. Conduct your security operations from one place.

CAPTURE SECURITY CENTER IS COMPLETENESS

Gain powerful all-at-once viewpoints of your security environments to simplify management and account processes, speed decision-making, improve support and correct security gaps.



Accessible from the Capture Security Center cloud console, My SonicWall's My Workspace lets you to run your complex security operation in a simpler and more efficient way. Its systematic workstreams let you easily and quickly on-board, set-up and manage multiple tenants across campuses, branches or functional

groups, perform bulk product registration, activate licenses and support, and initiate product trials on-demand.

Tenant workflows provide instant access to your security operations teams across organizations, including granular, role-based access control to products managed by the Capture Security

Center. An intuitive dashboard gives you instant visibility and awareness of products that have expiring licenses or products that need software or firmware updates. Engage, collaborate and communicate with tenants and facilitate, track and resolve issues and support cases using a built-in self-service portal.

CSC Feature Summary

Management

- SPOG Access to Most Functions
- Multiple Concurrent User Sessions
- Centralized Security and Network Management
- Universal Dashboard
- Firewall Management
- SonicWall Switch Management
- Wireless Management
- Federated Policy Configuration
- Define Policy at the Group Level
- Define Policy at the Group Level
- Policy Replication from Device to a Single or Group of Devices
- Change Order Management and Workflow
- Zero-Touch Deployment
- Zero-Touch Pre-Provisioned Device Configurations
- VPN Deployment and Configuration
- Active-Device Monitoring and Alerting
- Application Visualization and Intelligence
- APIs, CLI and SNMP support

- Capture Client Management
- Cloud App Security Management
- Hosted Email Security Management
- MySonicWall and MyWorkspace
- Risk Meters
- Security Center
- Cloud App Security – Shadow IT
- License Management
- Role Based Management (Users, Groups)
- Backup of Preference Files for Firewall Appliance

Monitoring

- Device monitoring and alerting
- IPFIX Data Flows in Real time
- Active Device Monitoring and Alerting
- SNMP Relay Management
- VPN and Firewall Status Monitoring
- Risk Meters

Reporting

- Centralized firewall logging
- Syslog- or IPFIX-based reports
- Custom Scheduled PDF reports
- Multi-threat report
- User-centric report
- Application usage report
- Botnet report
- Geo IP report
- MAC Address report
- Capture ATP report
- Rogue Wireless Access Point report
- Cloud App Security (CAS) report
- Capture Client report
- Bandwidth and Services report per interface

Analytics

- User-based activities
- Application usage
- Cross-product visibility with Capture Client
- Real-Time Dynamic Visualization
- Drill-down and pivoting capabilities

Licensing and packaging

The cloud-based services are available in the following packaging options.

1. CSC Management

This paid subscription option activates full management capabilities including Workflow Automation and Zero-Touch Deployment features.

2. CSC Management and Reporting

This license option is an ideal fit for larger institutions with many firewalls deployed in geographically dispersed locations that are under group-level or tenant-based management. These include mid-market organizations, distributed enterprises, public sector and educational organization with many districts and campuses, and managed service providers (MSPs).

In addition to full management capabilities, this subscription option provides full reporting features to perform periodic or on-demand security and network performance reviews and audits. This can be done using the onscreen interactive universal dashboard with live charts and tables, or off-screen with scheduled exported reports.

3. CSC Analytics

This is a powerful add-on service to all Capture Security Center subscription options. Activating the service provides full access to SonicWall Analytics and SonicWall Cloud App Security tools and services to conduct network forensic and threat hunting using comprehensive drill-down and pivoting capabilities. CSC Analytics also includes 30-days of roll over log storage and 365-days of reporting.

Supported firewall models

Capture Security Center is available to customers with SOHO-W, SOHO 250, SOHO 250W, TZ Series, NSA Series, NSa 2650-6650, and NSv Series firewalls. For SuperMassive 9000 Series, NSa Series and NSsp 12400 to 12800, CSC Management subscription option is automatically activated as part of its corresponding AGSS subscription activation.

CAPTURE SECURITY CENTER

	Management	Reporting ⁴	Analytics ⁴
Entry-level FW	SOHO-W, SOHO 250, SOHO 250W TZ Series, NSv 10-100	SOHO-W, SOHO 250, SOHO 250W, TZ Series, NSv 10-100	SOHO-W, SOHO 250, SOHO 250W, TZ Series, NSv 10-100
Mid-range FW	NSA Series, NSa Series, NSv 200-400	NSA Series, NSa Series, NSv 200-400	NSA Series, NSa Series, NSv 200-400
High-end FW	SuperMassive 9000 series, NSsp 12000 series, NSa 9250-9650, NSv 800-1600	SuperMassive 9000 series, NSsp 12000 series, NSa 9250-9650, NSv 800-1600	SuperMassive 9000 series, NSsp 12000 series, NSa 9250-9650, NSv 800-1600

⁴Support for Reporting and Analytics for High-end FW is available only on On_prem Analytics.

Features	CSC Management Lite	CSC Management	CSC Management and Reporting	SaaS Analytics	On Premises Analytics
Management	Backup/Restore – firewall system	Yes	Yes	Yes	Yes ²
	Backup/Restore – firewall preferences	Yes	Yes	Yes	Yes ²
	Firmware upgrade	From local file only	From local file only or MySonicWall	Yes	From local file only ³
	Task scheduling	-	Yes	Yes	-
	Group firewall management	-	Yes	Yes	-
	Inheritance – forward/reverse	-	Yes	Yes	-
	Zero touch deployment ¹	-	Yes	Yes	-
	Offline firewall signature downloads	-	Yes	Yes	-
	Workflow	-	Yes	Yes	-
	Pooled Licenses – Search, Sharing, Used Activation Code Inventory	-	Yes	Yes	-
Reporting (Netflow/IPFIX based)	Schedule reports, Live monitor, Summary dashboards	-	-	Yes	Yes
	Download Reports: Applications, Threats, CFS, Users, Traffic, Source/Destination (1-year flow reporting)	-	-	Yes	Yes
Analytics (Netflow/IPFIX based)	Network forensic and threat hunting using drill-down and pivots	-	-	-	Yes
	Cloud App Security - Shadow IT	-	-	-	Yes
	Data Retention	-	-	-	30-day traffic 1 Year
Technical Support	Web Cases Only	24x7 support	24x7 support	24x7 support	24x7 support

¹ Supported for SOHO-W with firmware 6.5.2+; TZ, NSA series and NSa 2650-6650 with firmware 6.5.1.1+.
Not supported for SOHO or NSv series.

² Requires AGSS/CGSS service or any paid Capture Security Center service

³ Requires a 24x7 support license

Ordering information

Product	SKU
SonicWall Capture Security Center Management for TZ Series, SOHO-W, SOHO 250, SOHO 250W, NSv 10 to 100 1Yr	01-SSC-3664
SonicWall Capture Security Center Management for TZ Series, SOHO-W, SOHO 250, SOHO 250W NSv 10 to 100 2Yr	01-SSC-9151
SonicWall Capture Security Center Management for TZ Series, SOHO-W, SOHO 250, SOHO 250W NSv 10 to 100 3Yr	01-SSC-9152
SonicWall Capture Security Center Management for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 1Yr	01-SSC-3665
SonicWall Capture Security Center Management for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 2Yr	01-SSC-9214
SonicWall Capture Security Center Management for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 3Yr	01-SSC-9215
SonicWall Capture Security Center Management and Reporting for TZ Series, SOHO-W, SOHO 250, SOHO250W, NSv 10 to 100 1Yr	01-SSC-3435
SonicWall Capture Security Center Management and Reporting for TZ Series, SOHO-W, SOHO 250, SOHO250W, NSv 10 to 100 2Yr	01-SSC-9148
SonicWall Capture Security Center Management and Reporting for TZ Series, SOHO-W, SOHO 250, SOHO250W, NSv 10 to 100 3Yr	01-SSC-9149
SonicWall Capture Security Center Management and Reporting for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 1Yr	01-SSC-3879
SonicWall Capture Security Center Management and Reporting for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 2Yr	01-SSC-9154
SonicWall Capture Security Center Management and Reporting for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 3Yr	01-SSC-9202
SonicWall Capture Security Center Analytics for SOHO-W, SOHO 250, SOHO250W, TZ Series, NSv 10 to 100 1Yr	02-SSC-0171
SonicWall Capture Security Center Analytics for NSA 2600 to 6600, NSa 2650 to 6650 and NSv 200 to 400 1Yr	02-SSC-0391

Internet Browsers

- Microsoft® Internet Explorer 11.0 or higher (do not use compatibility mode)
- Mozilla Firefox 37.0 or higher
- Google Chrome 42.0 or higher
- Safari (latest version)

Supported SonicWall appliances managed by Capture Security Center

- SonicWall Network Security Appliances: SuperMassive E10000 and 9000 Series, E-Class NSA, NSsp Series, NSa Series, TZ Series, SOHO-W, SOHO 250, SOHO 250W
- SonicWall Network Security Virtual Appliances: NSv Series
- SonicWall Endpoint Security – Capture Client
- SonicWall Cloud Security – Cloud App Security (CAS)
- SonicWall Email Security
- SonicWall Web Application Firewall
- SonicWall Secure Mobile Access: SMA 100 Series

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.