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.
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.

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.

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.

Malware
Malware includes all software written with malicious executable code to secretly manipulate. After disrupt system behavior and gain elevation or access to sensitive data, it may target individuals or organizations for social, political, economic or informational purposes. Common examples of malware include backdoors, viruses, worms, Trojans, adware and spyware.

Viruses
A computer virus is a small software program that can replicate itself and infect connected or directly normal computing operations. In other uses, it is used to gain access, control, surveillance or execute other malicious programs. Malicious code can spread by normal operations or propagate on the computer, spreading or data transfer via e-mail attachments.

Trojans
Trojans are designed specifically to extract sensitive data from the network. Many types of Trojans will take advantage of the infected system, triggering a key-down or other activity. They can take the form of a program, a web page, or an email attachment. Trojans are often used in the creation of worms.

Spyware
Although software in nature, spyware is typically installed on a user's computer without his or her knowledge or intent. Once installed, spyware typically monitors the user with some harm, possibly recording behavior and taking pictures.

SonicWall next-generation Firewalls disrupt and eliminate attacks targeting critical network positions. They detect malware, intrusions and data leakage, and deny applications, URL and content.
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 Basic Management (Lite)
This version is best suited for Backup/Restore of firewall system or preferences, and for firmware upgrade. Any firewall with AGSS or CGSS subscription can have this basic management functionality activated to help administer firewalls.

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

3. 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.

4. 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.

<table>
<thead>
<tr>
<th>CAPTURE SECURITY CENTER</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management</strong></td>
</tr>
<tr>
<td>Mid-range FW</td>
</tr>
<tr>
<td>High-end FW</td>
</tr>
</tbody>
</table>

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

\(^1\) 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

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

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.