SONICWALL®

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 networks, 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 scales to almost any size organization and features functional integration for better efficiency. Obtain greater operational elasticity

with a true SPOG interface. Gain immediate access to real-time Risk Meters, Zero-Touch Deployment and federated policy configuration 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	WAF	Wireless
Licensing	Entitlement	

CAPTURE SECURITY CENTER

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

LEARN MORE

SONICWALL®

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. SPOG 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 for wireless, email, mobile, and Internet of Things (IoT) deployments.

Manage firewalls and security applications. Maintain compliance for PCI, HIPAA and SOX. Identify security gaps and risks with precise analytics. Respond faster with time-critical threat information. Speed up provisioning for remote firewalls, eliminate errors and improve management workflows with Zero Touch Deployment.
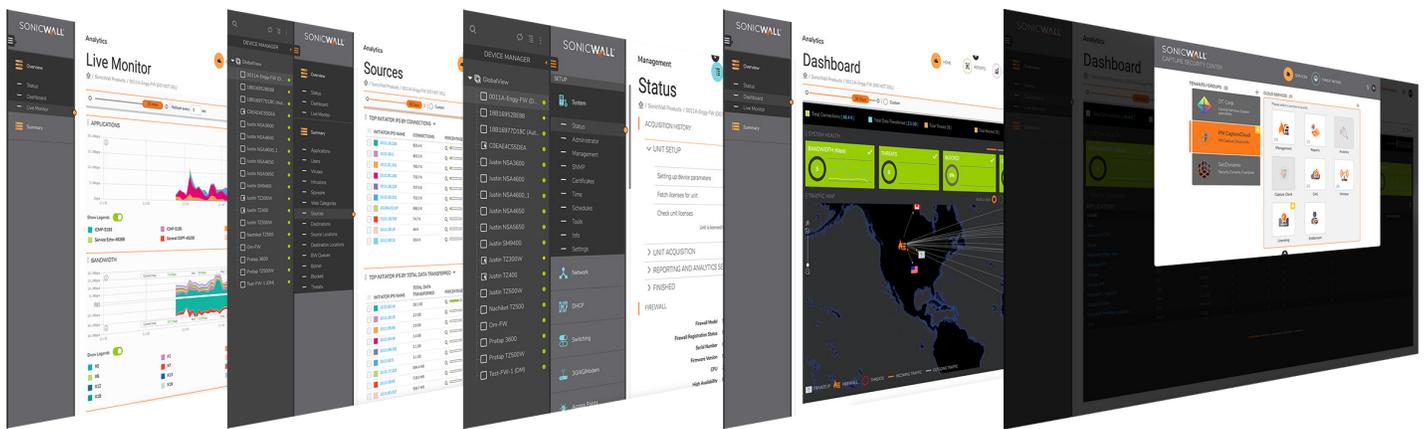

SPOG design increases efficiency and operational elasticity. Reduce security silos, increase productivity for the entire security environment—all from one app.

SONICWALL®

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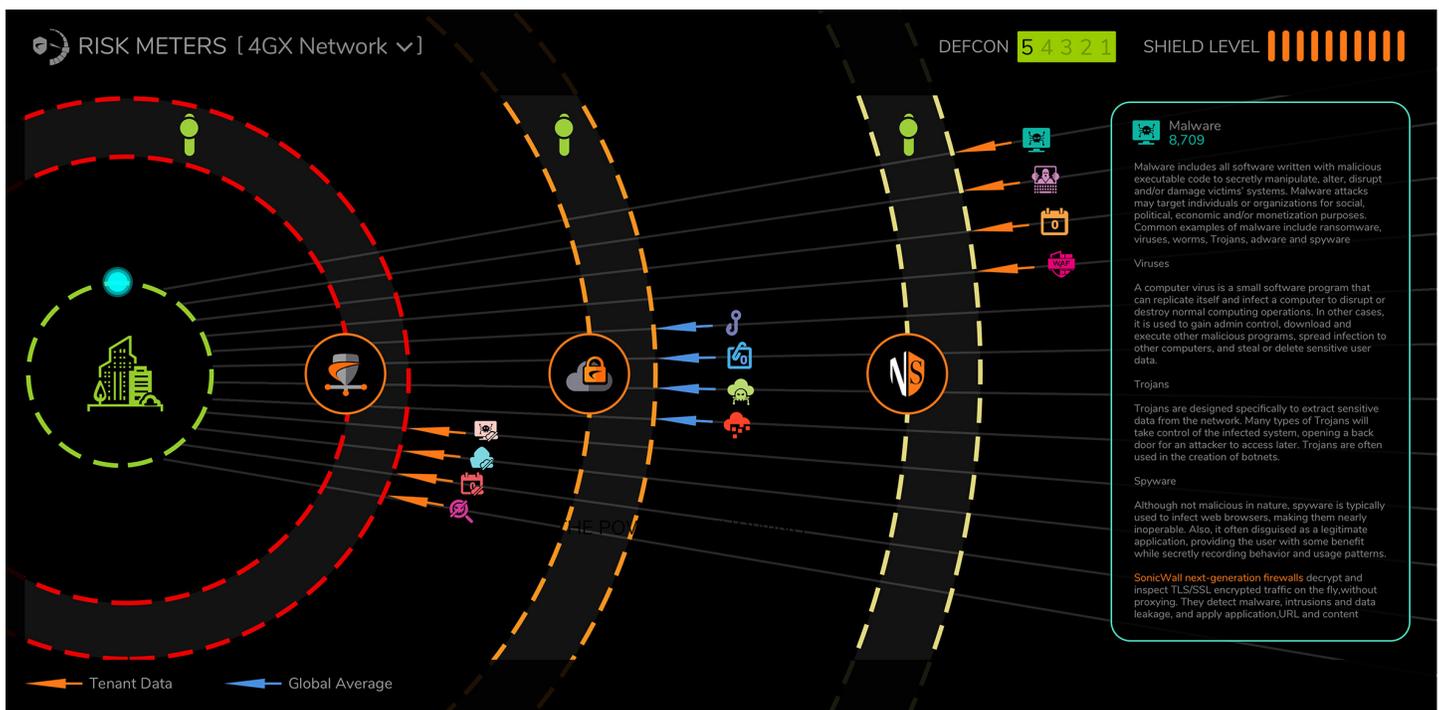
Risk Meters automatically show threat data and risk scores based on live threat data compared with your present level of protection. Reveal gaps in defensive layers, and make real-time security decisions. Guide security planning, policy and budgeting decisions based on logical scoring.

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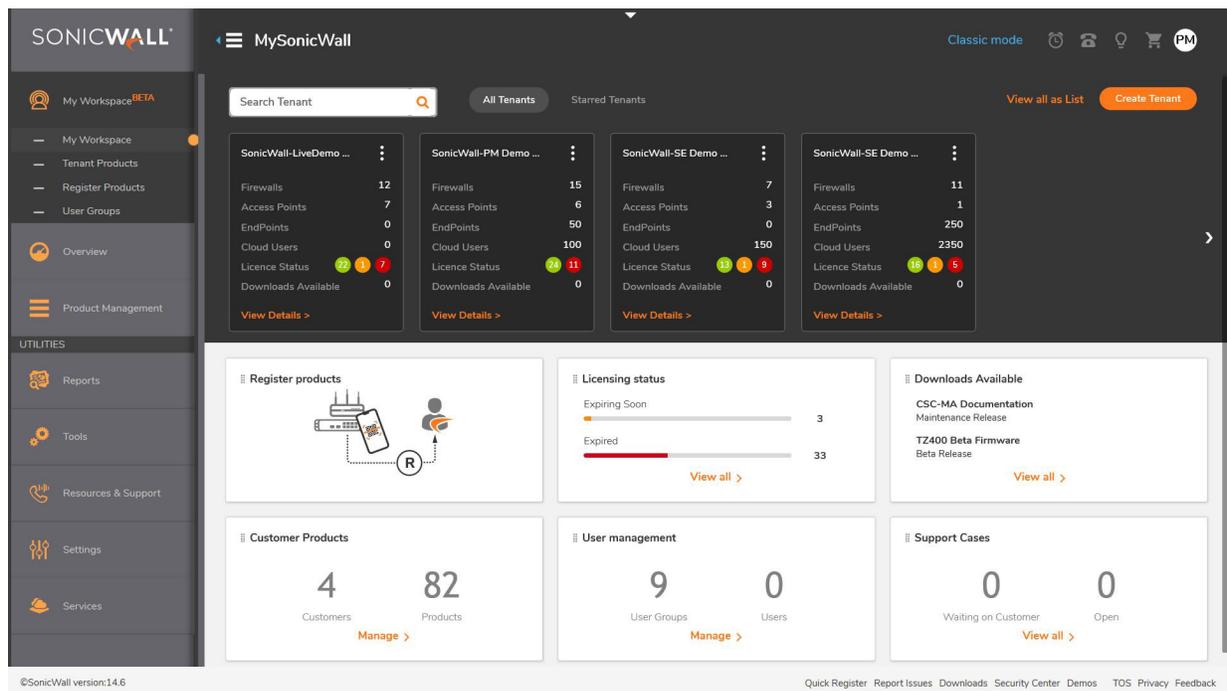
Accessible from the Capture Security Center cloud console, My SonicWall's My Workspace lets you to run your complex security operation in a simpler and more efficient way. Its systematic workstreams let you easily and quickly on-board, set-up and manage multiple tenants across campuses, branches or functional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

SonicWall Capture Security Center

CSC SECURITY MANAGEMENT AND MONITORING FEATURES

Feature	Description
Single Pane of Glass Management	Unified security management enables single sign-on access and monitoring of all key assets. Increases productivity from one app.
Centralized Security and Network Management	Helps administrators deploy, manage and monitor a distributed network security environment.
Federated Policy Configuration	Easily sets policies for thousands of SonicWall firewalls, wireless access and switches from a central location.
Change Order Management and Workflow	Assures compliance with policy changes by enforcing configuration process that includes comparing, validating, reviewing, and approving policies prior to deployment. Approval groups are user-configurable to enforce company security policy and regulatory requirements. Establish firewall policy for regulatory compliance requirements. Policy changes logged for audit-trail. Historically preserves granular details for compliance and troubleshooting research.
Zero-Touch Deployment	Simplifies and speeds the deployment and provisioning of SonicWall firewalls remotely using the cloud. Pushes policies; performs firmware upgrades; and synchronizes licenses.
Zero-Touch Pre-Provisioned Configurations	Operationalize large number of firewalls with ease by centrally pushing custom configurations to all zero-touch deployed appliances at multiple sites globally.
Sophisticated VPN Deployment and Configuration	Dell X-Series switches can now be managed easily within TZ, NSa and SuperMassive series firewalls to offer single-pane-of-glass management of the entire network security infrastructure.
Offline Management	Simplifies and speeds the deployment and provisioning of SonicWall firewalls remotely using the cloud. Automatically pushes policies; performs firmware upgrades; and synchronizes licenses.
Streamlined License Management	Simplifies the enablement of VPN connectivity, and consolidates thousands of security policies.
Universal dashboard	Features customizable widgets, geographic maps and user-centric reporting.
Active-Device Monitoring and Alerting	Provides real-time alerts with integrated monitoring capabilities, and facilitates troubleshooting efforts, thus allowing administrators to take preventative action and deliver immediate remediation.
Application Visualization and Intelligence	Shows historic and real-time reports of what applications are being used, and by which users. Reports are completely customizable using intuitive filtering and drill-down capabilities.
Rich Integration Options	Provides application programming interface (API) for web services, command line interface (CLI) support for most functions, and SNMP trap support for both service providers and enterprises.
Dell Networking X-Series Switch Management	Dell X-Series switches can now be managed easily within TZ, NSa and SuperMassive series firewalls to offer SPOG management of the entire network security infrastructure.
Risk Meters	Displays live attacks in real-time, with detailed graphs and charts that capture malicious activities at the specific defense layer. • Categorize attackers' malicious actions at the specific defense layer. • Restrict the focus on incoming attacks to a specific environment. • Real-time computed risk score and threat level. • Real-time analysis of threat data relative to existing defense capabilities. • Highlight current security gaps; see preventable threats get through missing defenses. • Promote immediate defensive actions - prevent all incoming threats .

SONICWALL®

CSC REPORTING FEATURES

Feature	Description
Botnet Report	Four report types: Attempts, Targets, Initiators, and Timeline containing attack vector context such as Botnet ID, IP Addresses, Countries, Hosts, Ports, Interfaces, Initiator/Target, Source/Destination, and User.
Geo IP Report	Contains information on blocked traffic based on the traffic country of origin/destination. Includes four report types: Attempts, Targets, Initiators, and Timeline containing attack vector context such as Botnet ID, IP Addresses, Countries, Hosts, Ports, Interfaces, Initiator/Target, Source/Destination, and User
MAC Address Report	Shows the Media Access Control (MAC) address on the report page. Includes device-specific information (Initiator MAC and Responder MAC) in five report types: • Data Usage > Initiators • Data Usage > Responders • Data Usage > Details • User Activity > Details • Web Activity > Initiators
Capture ATP Report	Gives detail threat behavior information to respond to a threat or infection.
HIPAA, PCI and SOX reports	Pre-defined PCI, HIPAA and SOX report templates help satisfy security compliance audits.
Rogue Wireless Access Point Reporting	Shows all wireless devices in use as well as rogue behavior from ad-hoc or peer-to-peer networking between hosts and accidental associations for users connecting to neighboring rogue networks.
Intelligent reporting and activity visualization	Provides comprehensive management and graphical reports for SonicWall firewalls, email security and secure mobile access devices. Enables greater insight into usage trends and security events while delivering a cohesive branding for service providers.
Centralized logging	As a central location for consolidating security events and logs for thousands of appliances, provides a single point to conduct network forensics.
Real-time and Historic Next Generation Syslog Reporting	Innovative architectural enhancement streamlines time-consuming summarization process. Allows near real-time reporting on incoming syslog messages; ability to drill down into data with extensive customization.
Universal Scheduled Reports	Schedule automatic reports and distribute to authorized recipients across multiple appliances of various types.

SONICWALL®

CSC ANALYTICS FEATURES

Feature	Description
Data Aggregation	Automatic aggregation of security activity flowing through all firewalls with deep normalization, correlation, and contextualization of data points.
Data Contextualization	Contextualized analytics, restructured for quick analysis and interpretation; designed for quick interpretation and prioritization.
User Analytics	Reduce security risk and optimize network performance by monitoring, discovering and managing all users' unsafe internet and application activities, malware and intrusion attacks, and resource utilization, access, and connections across the entire network.
Cross-Product Visibility and Insights	Manage and respond to security risks and issues using enhanced data correlation between endpoint and network traffic information associated with users or IP addresses.
Streaming Analytics	Analytics fed by real-time data streams of network security data. Results feed into SPOG management dashboard where data is dynamically illustrated, visually interactive.
Real-Time Dynamic Visualization	Augments SPOG management capability for deep drill-down investigative and forensic analysis of security data with precision, clarity, and speed.
Rapid Detection and Remediation	Additional investigative power to chase down unsafe activities; quickly manage and remediate risks.
Application Traffic Analytics	Provides organizations with powerful insight into application traffic, bandwidth utilization and security threats, while providing powerful troubleshooting and forensics capabilities.

CSC CLOUD APP SECURITY

Feature	Description
Real-Time Dashboard	Real-time SPOG management, with visual representation of applications being used, traffic volume, user activity and location of use.
App Discovery	Automates cloud application discovery by leveraging SonicWall firewall log files to identify shadow IT activities on the network.
App Risk Assessment	Quickly block or unblock applications based on the risk assessment.
App Classification and Control	Classify applications as Sanctioned or Unsanctioned. Set policies to block risky applications.

SONICWALL®

CSC Feature Summary

Management

- SPOG Access to Most Functions
- Multiple Concurrent User Sessions
- Offline Management and Scheduling
- Management of Security Firewall Policies
- Management of Security VPN Policies
- Management of SD-WAN
- Management of Hosted Email Security Policies
- Management of Value Added Security Services
- Define Policy at the Group Level
- Policy Replication from Device to a Group of Devices
- Policy Replication from Group Level to a Single Device
- Redundancy and High Availability
- Provisioning Management
- Scalable and Distributed Architecture
- Dynamic Management Views
- Unified License Manager
- Web Services Application Programming Interface (API)
- Role Based Management (Users, Groups)

- Universal Dashboard
- Backup of Preference Files for Firewall Appliance
- SSO to Managing Capture Client
- SSO to Managing Cloud App Security (CAS)
- SSO to Manage Secure Wireless
- SSO to Managing Web Application Firewall (WAF)
- SSO to WiFI Planner
- SSO to MySonicWall and My Workspace

Monitoring

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

Reporting

- Comprehensive Set of Graphical Reports
- Centralized Logging
- Multi-Threat Reporting
- User-Centric Reporting
- Application Usage Reporting
- Granular Services Reporting
- New Attack Intelligence

- Bandwidth and Services Report per Interface
- Reporting for SonicWall UTM Firewall Appliances
- Universal Scheduled Reports
- Next-Generation Syslog and IPFIX Reporting
- Flexible and Granular Near Real-Time Reporting
- Per User Bandwidth Reporting
- Rogue Wireless Access Point Reporting
- SRA SMB Web Application Firewall (WAF) Reporting
- Cloud App Security (CAS) reporting
- Capture Client Reporting

Analytics

- Data Aggregation
- Data Contextualization
- User Analytics
- Cross-Product Visibility and Insights
- Streaming Analytics
- User Analytics
- Real-Time Dynamic Visualization
- Rapid Detection and Remediation
- Data Exploration with Drill-Down Capabilities

SONICWALL®

Licensing and packaging

The cloud-based services of CSC Management, Reporting, Analytics and CAS 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.

SONICWALL®

	Features	CSC Management Lite	CSC Management	CSC Management and Reporting	SaaS Analytics	On Premises Analytics
Management	Backup/Restore – firewall system	Yes	Yes	Yes	Yes	Yes[2]
	Backup/Restore – firewall preferences	Yes	Yes	Yes	Yes	Yes[2]
	Firmware upgrade	From local file only	From local file only or MySonicWall	Yes	From local file only	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	Yes
	Download Reports: Applications, Threats, CFS, Users, Traffic, Source/ Destination (1-year flow reporting)	-	-	Yes	Yes	Yes
Analytics (Netflow/ IPFIX based)	Network forensic and threat hunting using drill-down and pivots	-	-	-	Yes	Yes
	Cloud App Security - Shadow IT	-	-	-	Yes	No
	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*

SONICWALL®

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

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

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

SONIC**WALL**®

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 has been fighting the cybercriminal industry for over 28 years defending small and medium businesses, enterprises and government agencies worldwide. Backed by research from SonicWall Capture Labs, our award- winning, real-time breach detection and prevention solutions secure more than a million networks, and their emails, applications and data, in over 215 countries and territories. These organizations run more effectively and fear less about security. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

SONICWALL®