SONICWALL CAPTURE SECURITY CENTER

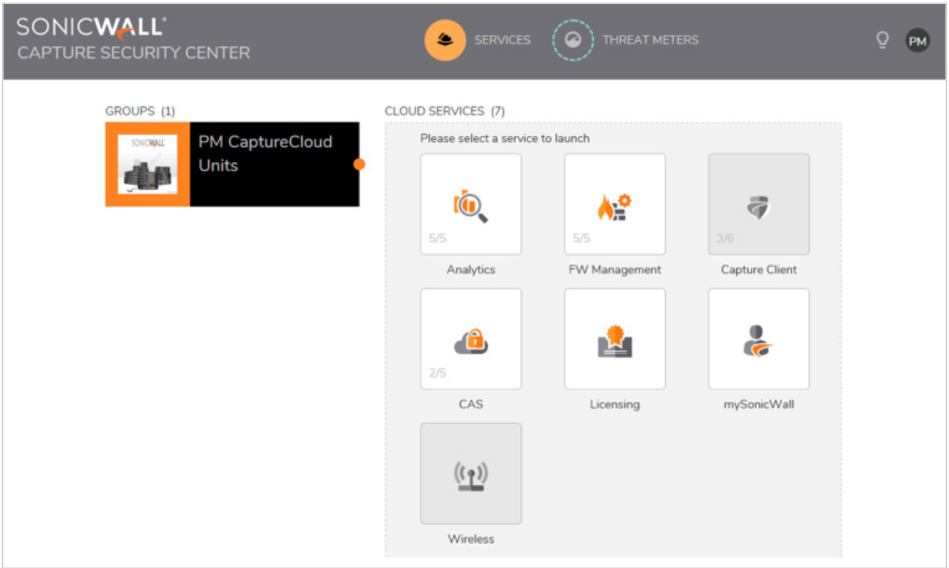
Cloud-delivered unified management, reporting and analytics for network, endpoint and cloud security

SonicWall Capture Security Center is an open, scalable cloud-based security management software delivered as a cost-effective as-a-service offering for organizations and service providers of various sizes and use cases. It offers the ultimate in visibility, agility and capacity to centrally govern the entire SonicWall security ecosystem with greater clarity, precision and speed – all from a single pane of glass. This cloud- and service-oriented architecture unifies and connects SonicWall security services and management tools to help gain better operational efficiencies and elasticity, while supporting a broader cyber defense strategy.

Guided by business processes and service level requirements, Capture Security Center helps Security Operation Centers (SOCs) form the foundation for a unified security governance, compliance and risk management strategy. By establishing a holistic, connected approach to security orchestration, Capture Security Center federates all operational aspects of network, endpoint and cloud security via a simple, common management framework. It simplifies and, in many cases, automates various tasks to promote better security coordination and decision-making, while reducing the complexity, time and expense of performing security operations and administration tasks. These tasks include firewall and endpoint provisioning, configuration, monitoring, reporting, patching, auditing, and traffic and data analytics that is invaluable to the detection and response to security problems before they occur.

Benefits:

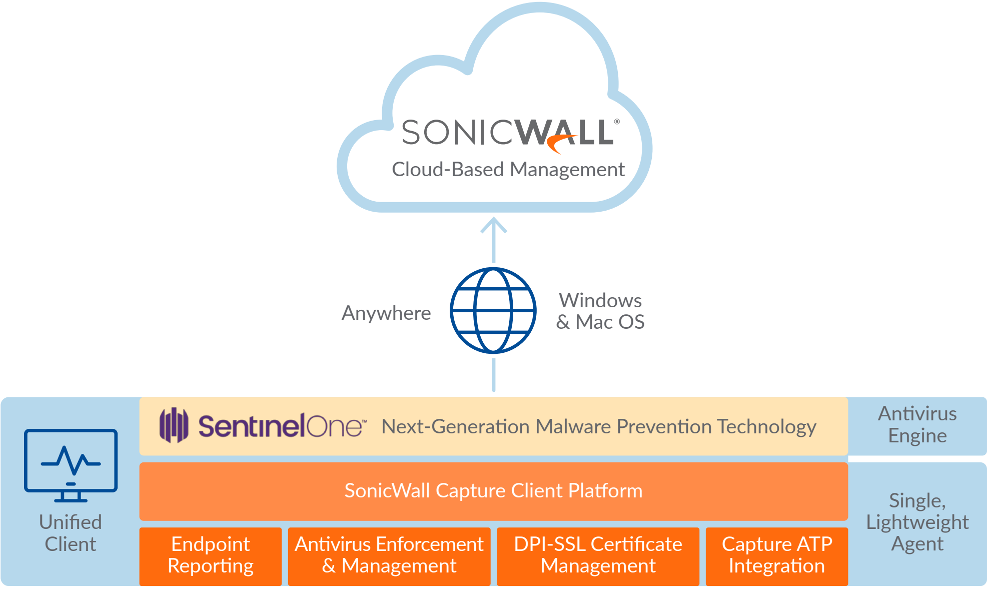
- Unified security governance, compliance and risk management security program
- An integration-friendly management console for all your SonicWall Solutions
- Automated workflows assure security compliance & error-free policy management
- Simple and fast zero-touch remote deployment and provisioning of SonicWall firewalls
- Single-pane visibility and situational awareness of the network security environment
- Deep investigative and forensic analysis of enriched security data
- Reduced incident response time with real-time, actionable threat intelligence



Capture Security Center provides Single Sign-On access to license, provision and manage all your network, endpoint and cloud security services. These services include Firewall Management, Analytics, Capture Client and Cloud Application Security. Our vision of unifying the full breadth of SonicWall security portfolio under one integration-friendly management tool includes web, wireless, email, mobile and IoT security services.[1] The combination of these cloud services delivers layered mission-critical cyber defense, threat intelligence, analysis and collaboration, and common management, reporting and analytics that work synchronously together. With software updates and support included in an active subscription service, access to any latest innovations and enhancements is immediate. This helps manage security risks, help fulfill regulatory obligations, and defend against the newest vulnerabilities and threats in an automated fashion. With limitless scalability and flexibility, Capture Security Center readily adapts to capacity and business changes on demand.

Capture Client

Assessible within the Capture Security Center is the SonicWall Capture Client, a unified client platform that delivers multiple endpoint protection capabilities. With a next-generation malware protection engine powered by SentinelOne, Capture Client applies advanced threat protection techniques, such as machine learning and system rollback. This protects against both file-based and fileless malware, while delivering a 360-degree attack view with actionable intelligence relevant for investigations. Combined with SonicWall firewalls, Capture Client also adds visibility into encrypted traffic, through the management of trusted SSL certificates used for Deep Packet Inspection of SSL/TLS traffic.


SONICWALL
Cloud-Based Management
Anywhere
Windows & Mac OS
Unified Client
SentinelOne
Next-Generation Malware Prevention Technology
Antivirus Engine
SonicWall Capture Client Platform
Single, Lightweight Agent
Endpoint Reporting
Antivirus Enforcement & Management
DPI-SSL Certificate Management
Capture ATP Integration

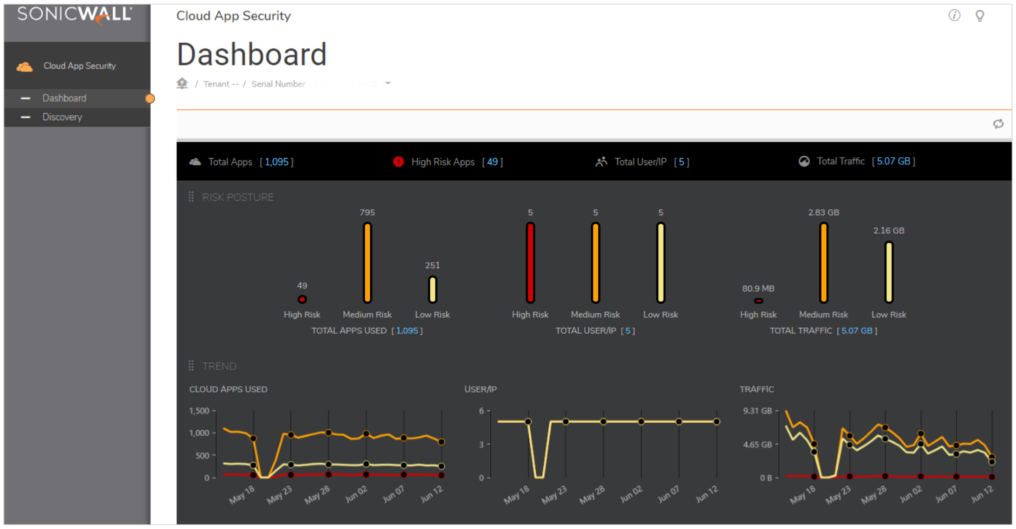
[1] *Web, wireless, email, mobile and IoT security services will be fully integrated into this platform in future product announcements.*

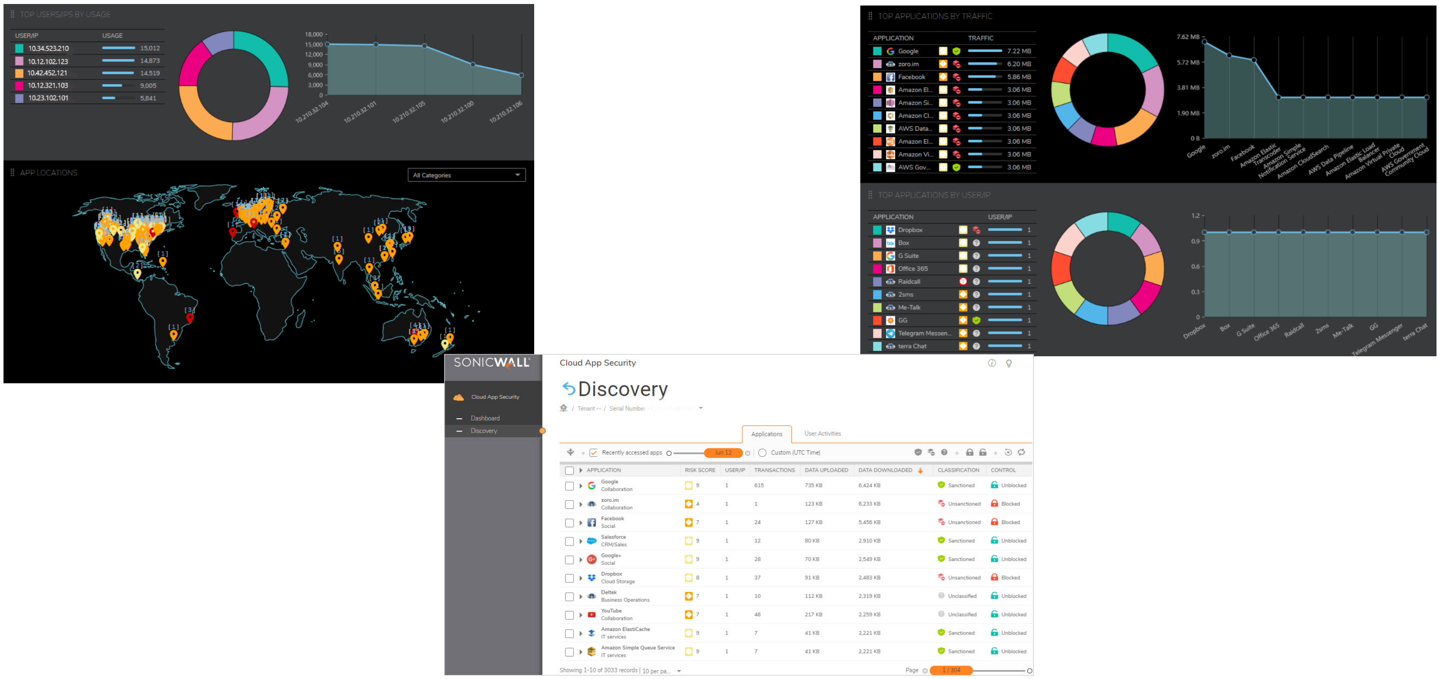
Cloud App Security

The SonicWall Capture Security Center Analytics subscription bundle empowers customers with shadow IT visibility and control over the usage of cloud applications. SonicWall Cloud App Security provides CASB-like functionality. It enables administrators to discover usage of risky applications, track user activity, and set allow/block policies for sanctioned and unsanctioned IT applications on managed firewalls to protect sensitive data.

Shadow IT discovery, Real-time visibility, and Application classification & control are the key capabilities of the Cloud App Security service. The service ensures safe adoption of SaaS applications without impacting employee productivity and at a low total cost of ownership.

1. **Shadow IT discovery:** Leverage existing firewall log files to automate cloud discovery to identify applications being used and their risk posture.
2. **Real-time application visibility:** Monitor usage in real-time with an intuitive dashboard view that provides details of applications being used, traffic volume, user activity and location of use.
3. **Application classification and control:** Classify unmanaged cloud applications into Sanctioned Apps (IT approved) or Un-Sanctioned Apps (Not IT approved), and set allow/block policies based on the application risk score.





TOP USERS/IPS BY USAGE

USER/IP	USAGE
🟩 10.34.523.210	15,012
🟪 10.12.102.123	14,873
🟧 10.42.452.121	14,519
🟥 10.12.321.103	9,005
🟦 10.23.102.101	5,841

TOP APPLICATIONS BY TRAFFIC

APPLICATION	TRAFFIC
Google	7.22 MB
zoro.im	6.20 MB
Facebook	5.86 MB
Amazon El...	3.06 MB
Amazon Si...	3.06 MB
Amazon Cl...	3.06 MB
AWS Data...	3.06 MB
Amazon El...	3.06 MB
Amazon Vi...	3.06 MB
AWS Gov...	3.06 MB

TOP APPLICATIONS BY USER/IP

APPLICATION	USER/IP
Dropbox	1
Box	1
G Suite	1
Office 365	1
Raidcall	1
2sms	1
Me-Talk	1
GG	1
Telegram Messen...	1
terra Chat	1

APPLICATION	RISK SCORE	USER/IP	TRANSACTIONS	DATA UPLOADED	DATA DOWNLOADED	CLASSIFICATION	CONTROL
Google Collaboration	9	1	615	735 KB	6,424 KB	Sanctioned	Unblocked
zoro.im Collaboration	4	1	1	123 KB	6,233 KB	Unsanctioned	Blocked
Facebook Social	7	1	24	127 KB	5,456 KB	Unsanctioned	Blocked
Salesforce CRM/Sales	9	1	12	80 KB	2,910 KB	Sanctioned	Unblocked
Google+ Social	9	1	28	70 KB	2,549 KB	Sanctioned	Unblocked
Dropbox Cloud Storage	8	1	37	91 KB	2,483 KB	Unsanctioned	Blocked
Deltek Business Operations	7	1	10	112 KB	2,319 KB	Unclassified	Unblocked
YouTube Collaboration	7	1	46	217 KB	2,259 KB	Unclassified	Unblocked
Amazon ElastiCache IT services	9	1	7	41 KB	2,221 KB	Sanctioned	Unblocked
Amazon Simple Queue Service IT services	9	1	7	41 KB	2,221 KB	Sanctioned	Unblocked

Showing 1-10 of 3033 records | 10 per pa...

Workflow Automation

Employing native workflow automation, Capture Security Center helps SOCs conform to firewall policy change management and auditing requirements of various regulatory laws such as PCI, HIPPA and GDPR. It enables policy changes by applying a series of rigorous procedures for configuring, comparing, validating, reviewing and approving firewall policies prior to deployment. The approval groups are flexible to comply with varying authorization and audit procedures from different types of organizations. Workflow automation programmatically deploys sanctioned security policies to improve operational efficiency, mitigate risks and eliminate errors.

> Capture Security Center provides a holistic approach to security governance, compliance and risk management.

1. CONFIGURE AND COMPARE

Capture Security Center configures policy **change orders** and **color codes** differences for clear comparisons

2. VALIDATE

Capture Security Center performs an integrity **validation of the policy's logic**

3. REVIEW & APPROVE

Capture Security Center emails reviewers and logs an **approval/ disapproval audit trail** of the policy

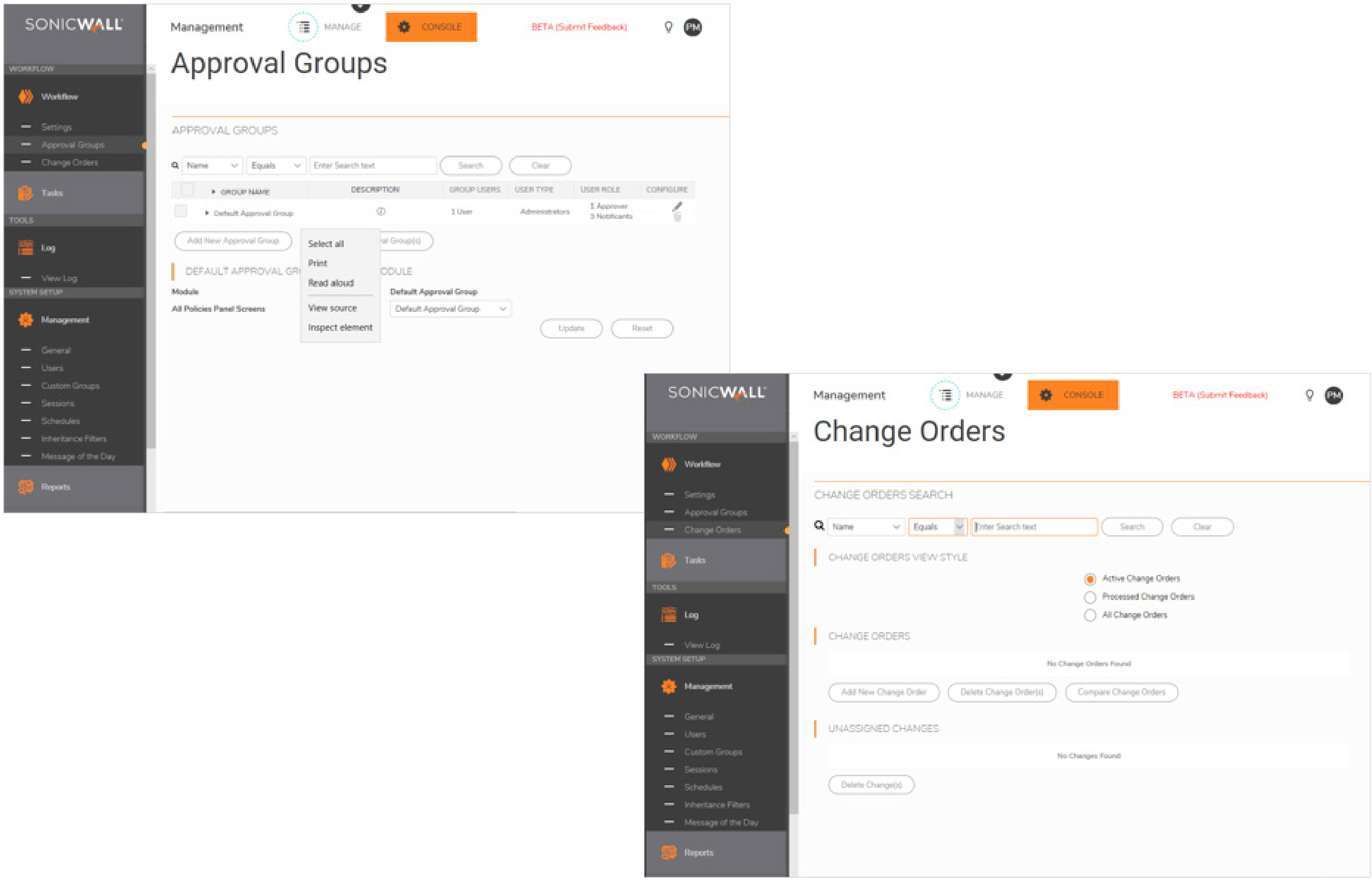
4. DEPLOY

Capture Security Center deploys the policy changes immediately or **on a schedule**

5. AUDIT

The change logs enable accurate policy **auditing** and precise **compliance** data

Workflow Automation: Four steps to error-free policy management



Approval Groups

APPROVAL GROUPS

	GROUP NAME	DESCRIPTION	GROUP USERS	USER TYPE	USER ROLE	CONFIGURE
□	Default Approval Group	ⓘ	1 User	Administrators	1 Approver 3 Notificants	

DEFAULT APPROVAL GR ODULE

Module: All Policies Panel Screens

Default Approval Group: Default Approval Group

Change Orders

CHANGE ORDERS SEARCH

CHANGE ORDERS VIEW STYLE

● Active Change Orders
○ Processed Change Orders
○ All Change Orders

CHANGE ORDERS

No Change Orders Found

UNASSIGNED CHANGES

No Changes Found

Zero-Touch Deployment

Integrated into Capture Security Center is the Zero-Touch Deployment service, which simplifies and speeds the provisioning process for SonicWall firewalls at remote and branch office locations. The process requires minimal user intervention, and is fully automated to operationalize firewalls at scale in four easy deployment steps. This significantly reduces the time, cost and complexity associated with installation and configuration, while security and connectivity occurs instantly and automatically.

STEP 1 **REGISTER THE FIREWALL**
Registers the new firewall in MySonicWall using its assigned seriel number and authentication code.

STEP 2 **CONNECT THE FIREWALL**
Connects the firewall to the network using the ethernet cable that came with the unit.

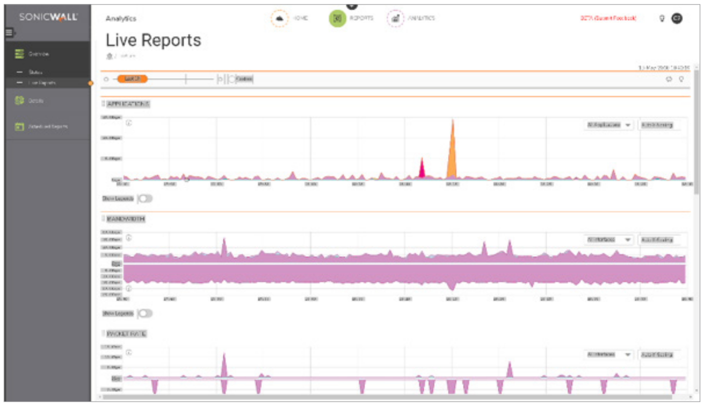
STEP 3 **POWER UP THE FIREWALL**
Power up the firewall after connecting the power cable and plugging it into a standard wall outlet. Units are automatically assigned a WAN IP using DHCP server. Once connectivity is established, the unit is automatically discovered, authenticated, and added to Capture Security Center with all licenses and configurations synchronized with MySonicWall and License Manager.

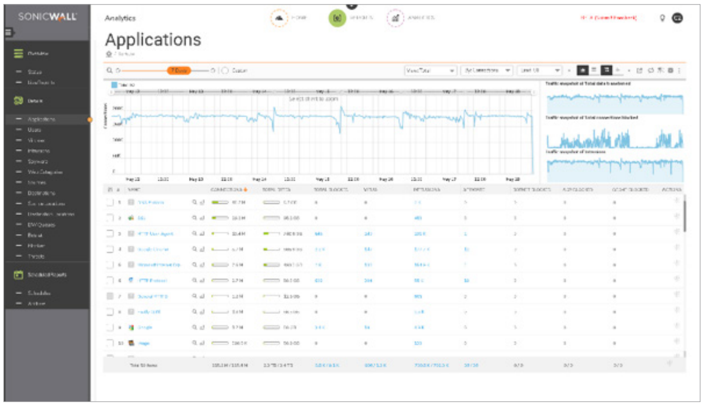
STEP 4 **MANAGE THE FIREWALL**
The unit is now operational and managed via the Capture Security Center cloud-based central management console such as firmware upgrades, security patching, and group level configuration changes.

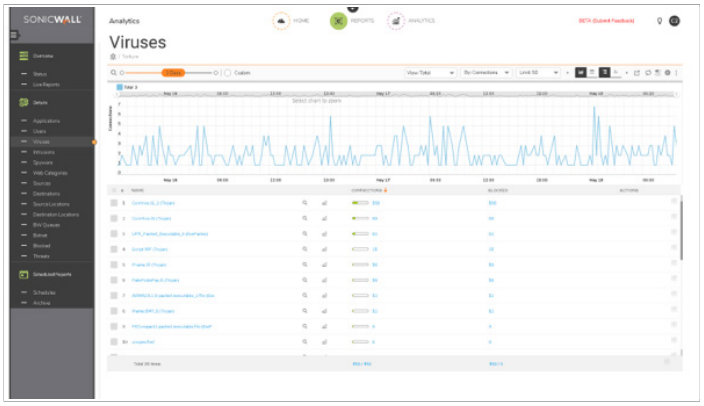
Zero-Touch Deployment: Operationalize firewall in four easy steps

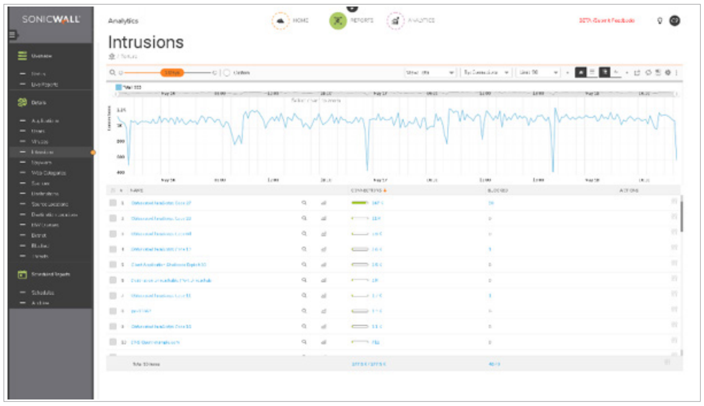
Reporting

Capture Security Center offers over 140 predefined reports, as well as the flexibility to create custom reports using any combination of auditable data to acquire various use-case outcomes. These outcomes include big-picture and detailed awareness of network events, user activities, threats, operational and performance issues, security efficacy, risks and security gaps, compliance readiness, and even post-mortem analysis. Every report is designed with the collective input from many years of SonicWall customer and partner collaborations. This provides the deep granularity, scope and knowledge of syslog and IPFIX/NetFlow data SOCs need to track, measure and run an effective network and security operation.





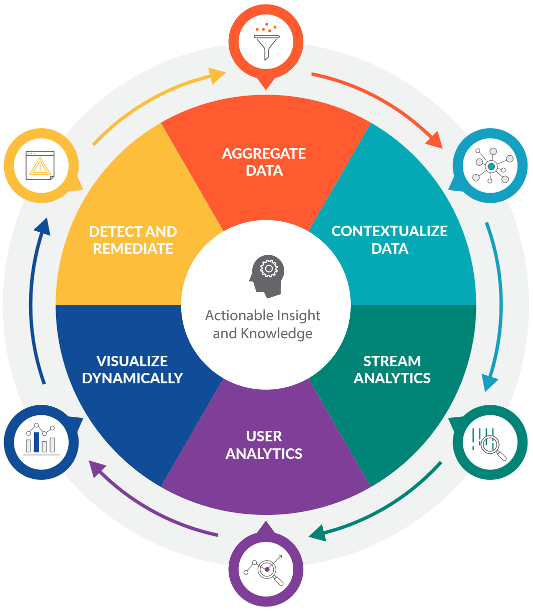




Analytics

SonicWall Analytics is an intelligence-driven big data analysis engine that automates the aggregation, normalization, correlation, and contextualization of security data flowing through all managed firewalls. It gives organizations real-time insight into everything that is happening across their networks. The results, presented in a structured, meaningful, actionable and easily consumable way, empower security team, analysts, auditors, boards, C-Suites and stakeholders to discover, interpret, prioritize, make decisions and take appropriate defensive and corrective actions.

Analytics presents real-time visualization, monitoring and alerting of enriched security data through a single pane of glass. It comes with powerful tools that give customers complete authority, agility and flexibility to perform extensive drill-down investigative analysis of network traffic, user activities, security events, threat profile, application utilization, and a myriad of other contextual firewall data. This deep visibility, knowledge and understanding of the security environment gives customers valuable insight and the capacity to not only uncover security risks, but also orchestrate remediation, while monitoring and tracking the results with greater clarity and speed. Analytics enables customers to operationalize security analysis and integrate it into business processes to transform data into information, information into knowledge, and knowledge into decisions that enable achieving full security automation.



- Gain eagle-eye view into everything

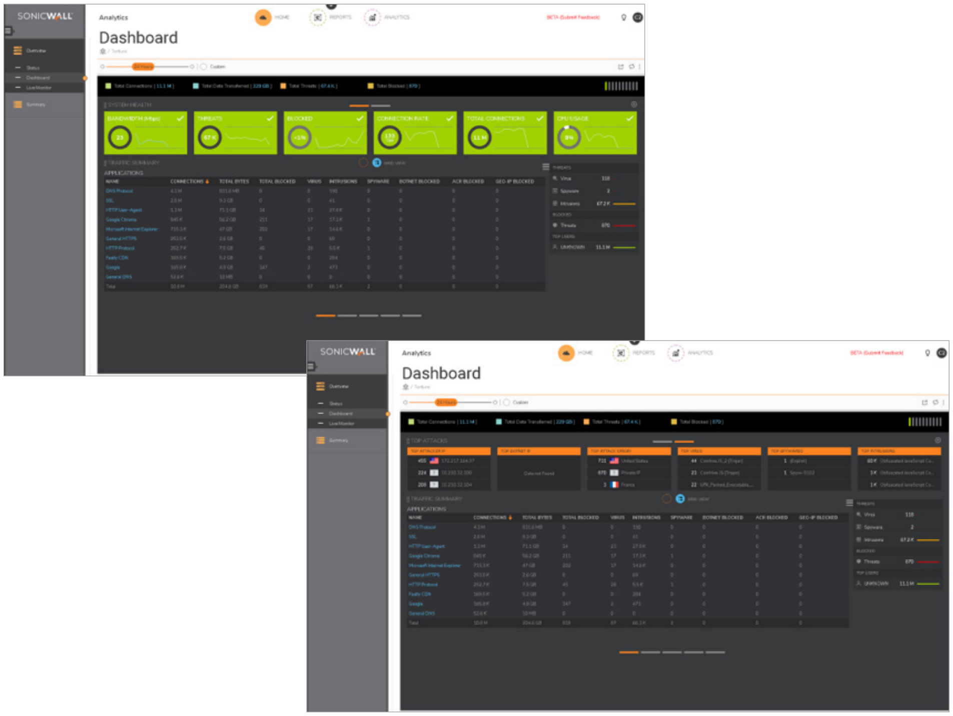
- Empower stakeholders with single-pane visibility and insights
- Enrich firewall security data

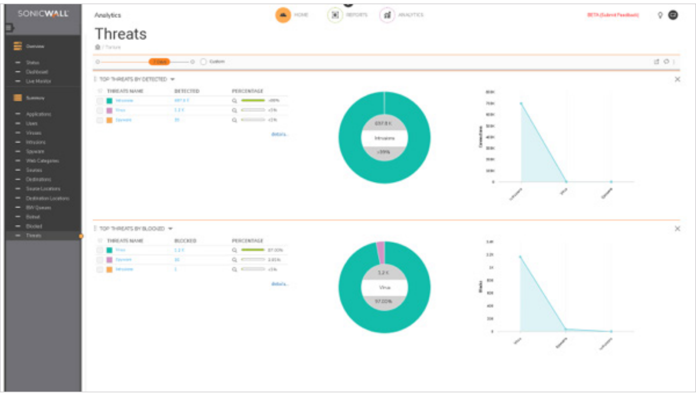
- Create knowledge representations of analytic data
- Monitor results with greater clarity, certainty and speed

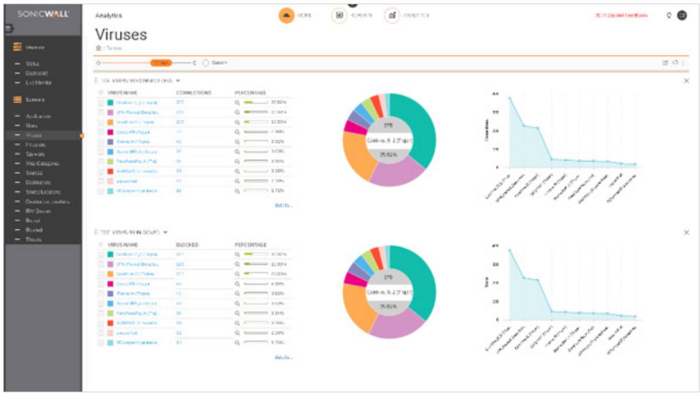
- Perform deep drill-down investigative and forensic analysis

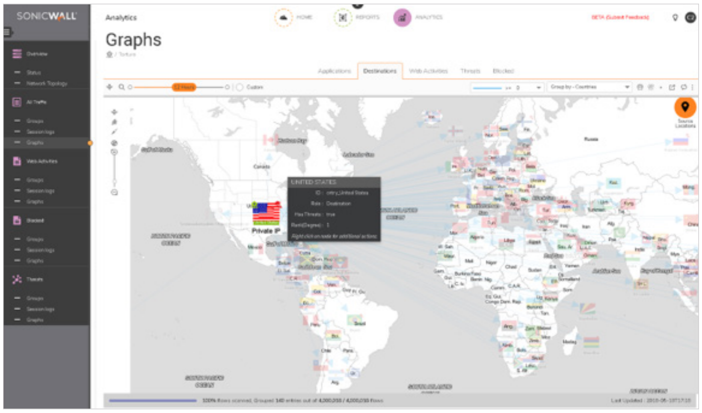
- Operationalize analytics via real-time, actionable alerts
- Show enriched data in a meaningful, actionable and consumable manner, and speed

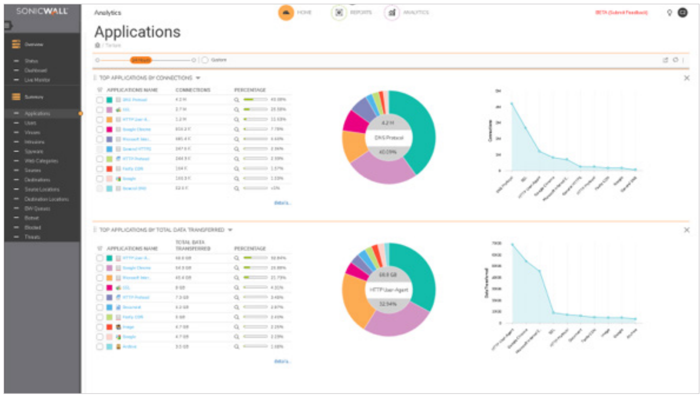
- Calibrate security policies and controls
- Exercise risk-based decision-making and remediation




SONICWALL
Analytics
Threats
HOME
REPORTS
ANALYTICS
TOP THREATS BY DETECTED
TOP THREATS BY BLOCKED
THREATS NAME
DETECTED
BLOCKED
PERCENTAGE
Intrusions
Virus


SONICWALL
Analytics
Viruses
HOME
REPORTS
ANALYTICS
VIRUS NAME
CONNECTIONS
BLOCKED
PERCENTAGE

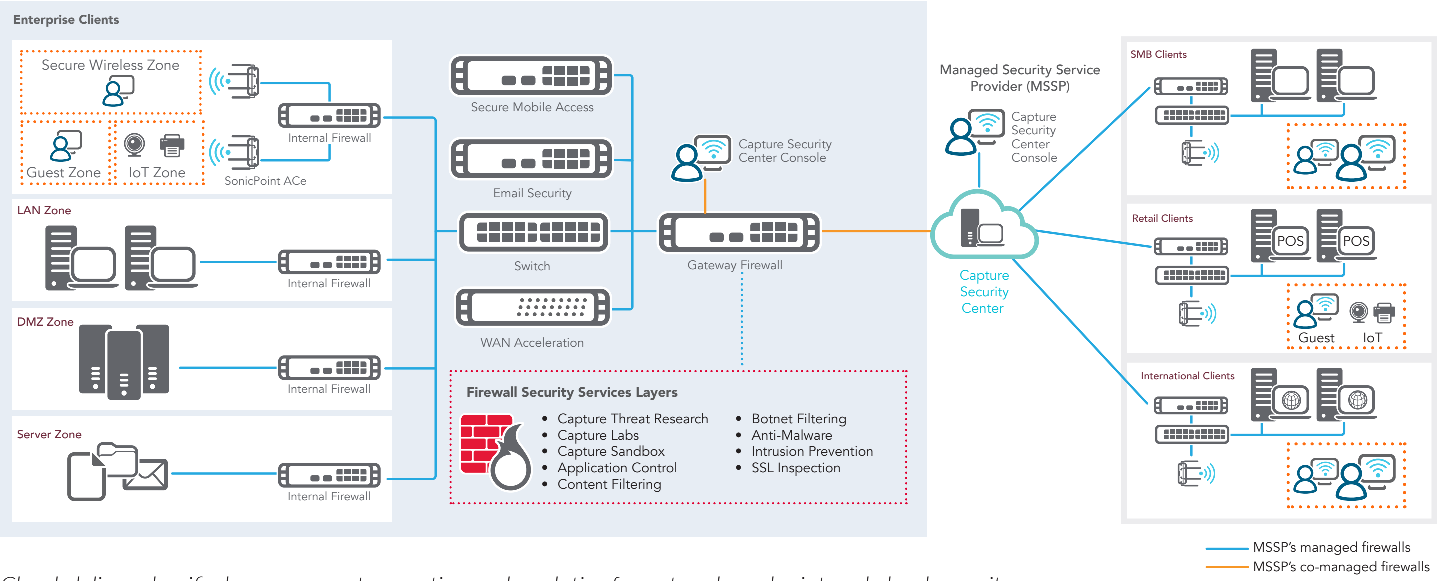

SONICWALL
Analytics
Graphs
HOME
REPORTS
ANALYTICS
Applications
Destinations
Web Activities
Threats
Blocked
Group by - Countries
UNITED STATES
Private IP
Russia
Canada
Brazil


SONICWALL
Analytics
Applications
HOME
REPORTS
ANALYTICS
TOP APPLICATIONS BY CONNECTIONS
TOP APPLICATIONS BY TOTAL DATA TRANSFERRED
APPLICATIONS NAME
CONNECTIONS
TOTAL DATA TRANSFERRED
PERCENTAGE
DNS Protocol
HTTP User-Agent

Scalable cloud architecture

Capture Security Center distributed architecture facilitates limitless system availability and scalability. Supporting small to large enterprises, telecoms, carriers and service providers with a massive multi-tenant ecosystem, Capture Security Center can scale on-demand to support thousands of SonicWall security devices under its management, regardless of location. At the customer-facing level is its highly interactive universal dashboards loaded with real-time monitoring, reporting, and analytics data to help guide smart security policy decisions, and drive collaboration, communication and knowledge across the shared security framework. With an enterprise-wide view of the security environment and real-time security intelligence reaching the right people in the organization, accurate security policies and controls actions can be made towards a stronger adaptive security posture.

Capture Security Center provides a complete and scalable security management, analytic and reporting platform for distributed organizations and service providers (i.e. carriers, telecoms, and MSPs).



Cloud-delivered unified management, reporting and analytics for network, endpoint and cloud security.

Security management and monitoring features

Feature	Description
Centralized security and network management	Helps administrators deploy, manage and monitor a distributed network security environment.
Federate policy configuration	Easily sets policies for thousands of SonicWall firewalls, wireless access points, email security, secure remote access devices and switches from a central location.
Change Order Management and Work Flow	Assures the correctness and compliance of policy changes by enforcing a process for configuring, comparing, validating, reviewing and approving policies prior to deployment. The approval groups are user-configurable for adherence to company security policy. All policy changes are logged in an auditable form that ensures the firewall complies with regulatory requirements. All granular details of any changes made are historically preserved to help with compliance, audit trailing, and troubleshooting.
Zero-Touch Deployment	Simplifies and speeds the deployment and provisioning of SonicWall firewalls remotely using the cloud. Automatically pushes policies; performs firmware upgrades; and synchronizes licenses.
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.
SNMP support	Provides powerful, real-time traps for all Transmission Control Protocol/Internet Protocol (TCP/IP) and SNMP-enabled devices and applications, greatly enhancing troubleshooting efforts to pinpoint and respond to critical network events.
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 the majority of 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 single-pane-of-glass management of the entire network security infrastructure.

Reporting

Feature	Description
Botnet Report	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.
Geo IP Report	Contains information on blocked traffic that is based on the traffic's country of origin or 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	Shows detail threat behavior information to respond to a threat or infection.
HIPPA, PCI and SOX reports	Includes pre-defined PCI, HIPAA and SOX report templates to satisfy security compliance audits.

Reporting con't	
Feature	Description
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	Offers a central location for consolidating security events and logs for thousands of appliances, providing a single point to conduct network forensics.
Real-time and historic next-generation syslog reporting	Through a revolutionary enhancement in architecture, streamlines the time-consuming summarization process, allowing for near real-time reporting on incoming syslog messages. Also provides the ability to drill down into data and customize reports extensively.
Universal scheduled reports	Schedules reports that are automatically created and mailed out across multiple appliances of various types to authorized recipients.

Analytics	
Feature	Description
Data aggregation	Intelligence-driven analytic engine automates the aggregation, normalization, correlation, and contextualization of security data flowing through all firewalls.
Data contextualization	Actionable analytics, presented in a structured, meaningful and easily consumable way, empower security team, analyst and stakeholders to discover, interpret, prioritize, make decisions and take appropriate defensive actions.
Streaming analytics	Streams of network security data are continuously processed, correlated and analyzed in real-time and the results are illustrated in a dynamic, interactive visual dashboard.
User analytics	Deep analysis of users' activity trends to gain full visibility into their utilization, access, and connections across the entire network.
Real-time dynamic visualization	Through a single-pane-of glass, security team can perform deep drill-down investigative and forensic analysis of security data with greater precision, clarity and speed.
Rapid detection and remediation	Investigative capabilities to chase down unsafe activities and to quickly manage and remediate risks.
Flow analytics and reports	Provides a flow reporting agent for application traffic analytics and usage data through IPFIX or NetFlow protocols for real-time and historical monitoring. Offers administrators an effective and efficient interface to visually monitor their network in real-time, providing the ability to identify applications and websites with high bandwidth demands, view application usage per user and anticipate attacks and threats encountered by the network. • A Real-Time Viewer with drag and drop customization • A Real-Time Report screen with one-click filtering • A Top Flows Dashboard with one-click View By buttons • A Flow Reports screen with five additional flow attribute tabs • A Flow Analytics screen with powerful correlation and pivoting features • A Session Viewer for deep drill-downs of individual sessions and packets.
Application traffic analytics	Provides organizations with powerful insight into application traffic, bandwidth utilization and security threats, while providing powerful troubleshooting and forensics capabilities.

Cloud App Security	
Feature	Description
Real-Time Dashboard	Get real-time, visual representation of applications being used, traffic volume, user activity and location of use.
App Discovery	Automate cloud application discovery by leveraging your SonicWall firewall log files to identify shadow IT activities on the network.
App Risk Assessment	Make informed decisions to block/unblock applications based on the risk assessment.
App Classification and Control	Classify applications into Sanctioned or Unsanctioned apps, and set policies to block risky applications.

Feature summary

Management

- Ubiquitous Access
- Alerts and Notifications
- Diagnostic Tools
- Multiple Concurrent User Sessions
- Offline Management and Scheduling
- Management of Security Firewall Policies
- Management of Security VPN Policies
- Management of Email Security Policies
- Management of Secure Remote Access/SSL VPN Policies
- Management of Value Added Security Services
- Define Policy Templates 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
- Command Line Interface (CLI)
- Web Services Application Programming Interface (API)
- Role Based Management (Users, Groups)
- Universal Dashboard
- Backup of preference files for firewall appliances

Monitoring

- IPFIX Data Flows in Real time
- SNMP Support
- Active Device Monitoring and Alerting
- SNMP Relay Management
- VPN and Firewall Status Monitoring
- Live Syslog Monitoring and Alerting

Reporting

- Comprehensive Set of Graphical Reports
- Compliance Reporting
- Customizable Reporting with Drill Down Capabilities
- 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
- Reporting for SonicWall SRA SSL VPN Appliances
- Universal Scheduled Reports
- Next-generation Syslog and IPFIX Reporting
- Flexible and Granular Near Real-Time Reporting
- Per User Bandwidth Reporting
- Client VPN Activity Reporting
- Detailed Summary of Services over VPN Report
- 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
- Streaming analytics
- User analytics
- Real-time dynamic visualization
- Rapid detection and remediation

Licensing and Packaging

Capture Security Center (CSC)		License Tier			
		CSC Management Lite	CSC Management	CSC Management and Reporting	CSC Analytics
Licensing requirement	Available to customers with active AGSS/CGSS subscription	AGSS/CGSS	AGSS/CGSS	AGSS/CGSS	AGSS/CGSS
Management	Single Pane of Glass	✓	✓	✓	
	Backup/Restore	✓	✓	✓	
	Task scheduling		✓	✓	
	Group firewall management		✓	✓	
	Inheritance - forward/reverse		✓	✓	
	Zero touch		✓	✓	
	Offline firewall signature downloads		✓	✓	
	Workflow		✓	✓	
Reporting	Live monitor, Summary dashboards			✓	
	Download Reports: Applications, Threats, CFS, Users, Traffic, etc.			✓	
	Scheduled reporting			✓	
Analytics	Analytics (30-day retention)				✓
	Cloud App Security(30-day retention)				✓

Capture Security Center ordering information

Product	SKU
SonicWall Capture Security Center Management for TZ Series, NSv 10 to 100 1Yr	01-SSC-3664
SonicWall Capture Security Center Management for TZ Series, NSv 10 to 100 2Yr	01-SSC-9151
SonicWall Capture Security Center Management for TZ Series, NSv 10 to 100 3Yr	01-SSC-9152
SonicWall Capture Security Center Management for NSA 2600 to 6650 and NSv 200 to 400 1Yr	01-SSC-3665
SonicWall Capture Security Center Management for NSA 2600 to 6650 and NSv 200 to 400 2Yr	01-SSC-9214
SonicWall Capture Security Center Management for NSA 2600 to 6650 and NSv 200 to 400 3Yr	01-SSC-9215
SonicWall Capture Security Center Management and Reporting for TZ Series, NSv 10 to 100 1Yr	01-SSC-3435
SonicWall Capture Security Center Management and Reporting for TZ Series, NSv10 to 100 2Yr	01-SSC-9148
SonicWall Capture Security Center Management and Reporting for TZ Series, NSv 10 to 100 3Yr	01-SSC-9149
SonicWall Capture Security Center Management and Reporting for NSA 2600 to 6650 and NSv 200 to 400 1Yr	01-SSC-3879
SonicWall Capture Security Center Management and Reporting for NSA 2600 to 6650 and NSv 200 to 400 2Yr	01-SSC-9154
SonicWall Capture Security Center Management and Reporting for NSA 2600 to 6650 and NSv 200 to 400 3Yr	01-SSC-9202
SonicWall Capture Security Center Analytics for TZ Series, NSv 10 to 100 1Yr	02-SSC-0171
SonicWall Capture Security Center Analytics for NSA 2600 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: NSa 2600 to NSa 6650, and TZ Series appliances
- SonicWall Network Security Virtual Appliances: NSv 10 to NSv 400
- SonicWall Endpoint Security- Capture Client
- SonicWall Cloud Security – Cloud App Security (CAS)

About Us

SonicWall has been fighting the cyber-criminal industry for over 26 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com