SONICWALL CAPTURE SECURITY CENTER

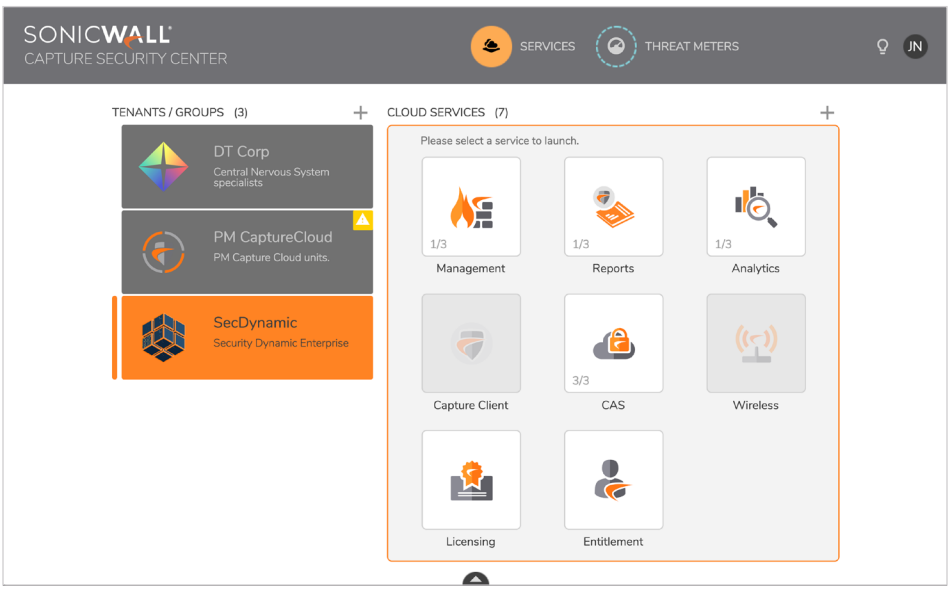
Cloud-delivered single pane of glass unified management, analytics for network, endpoint and cloud security

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 cloud interface that can be accessed from any location and any web-enabled device. 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 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:

- Centrally manage your SonicWall security environment – all from one place
- Reduce security silos with single-pane-of-glass experience
- Improve operational efficiencies with error-free policy management automation
- Ease and speed provisioning of remote firewalls with Zero-Touch Deployment
- Ease compliance reporting for PCI, HIPPA and SOX
- Identify security gaps and risks using detailed, precise analytics
- Respond to risks quickly with time-critical threat information



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.

Managing Cyber Risks

Integrated into Capture Security Center is the SonicWall Risk Meters, a powerful security information and risk management tool. Risk Meters provides personalized threat data and risk scores that reveals gaps in defensive layers, fosters decisive security planning and facilitates actions needed for an optimal cyber defense. This helps bolster network, cloud, web and endpoint defenses while reducing the environment's threat surface and susceptibility to cyberattacks.

Additionally, Risk Meters continuously update computed risk score and threat level based on live threat data relative to existing defense capabilities. These logical scores can then be used to guide security planning, policy and budgeting decisions.

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.

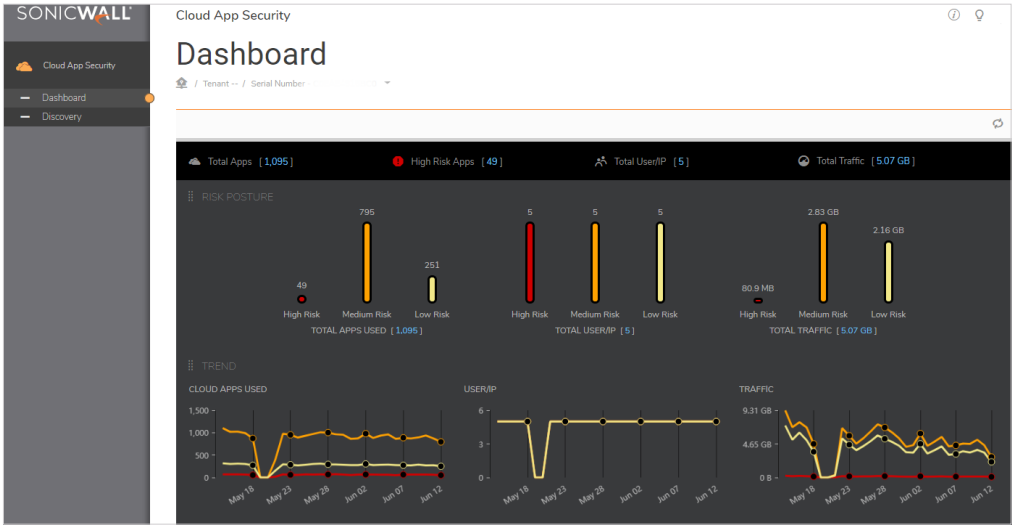
[1] *Web, wireless, email, mobile and IoT security services will be fully integrated into this platform in future product announcements.*

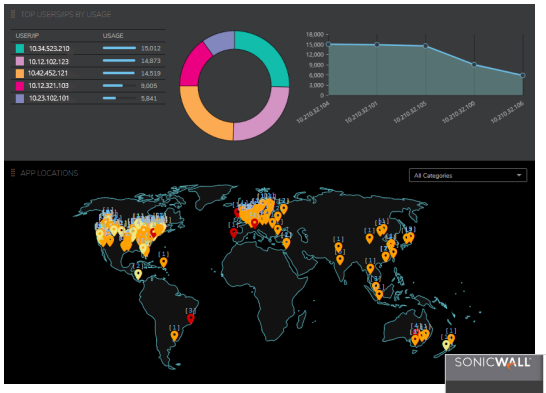
Cloud App Security

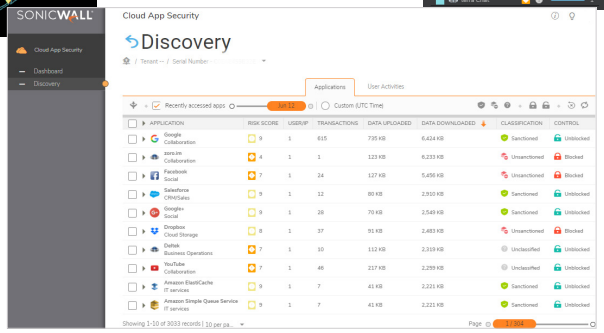
The SonicWall Capture Security Center Analytics subscription bundle empowers customers with shadow IT visibility and control over the usage of cloud applications. SonicWall Cloud App Security provides CASB-like functionality. It enables administrators to discover usage of risky applications, track user 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.







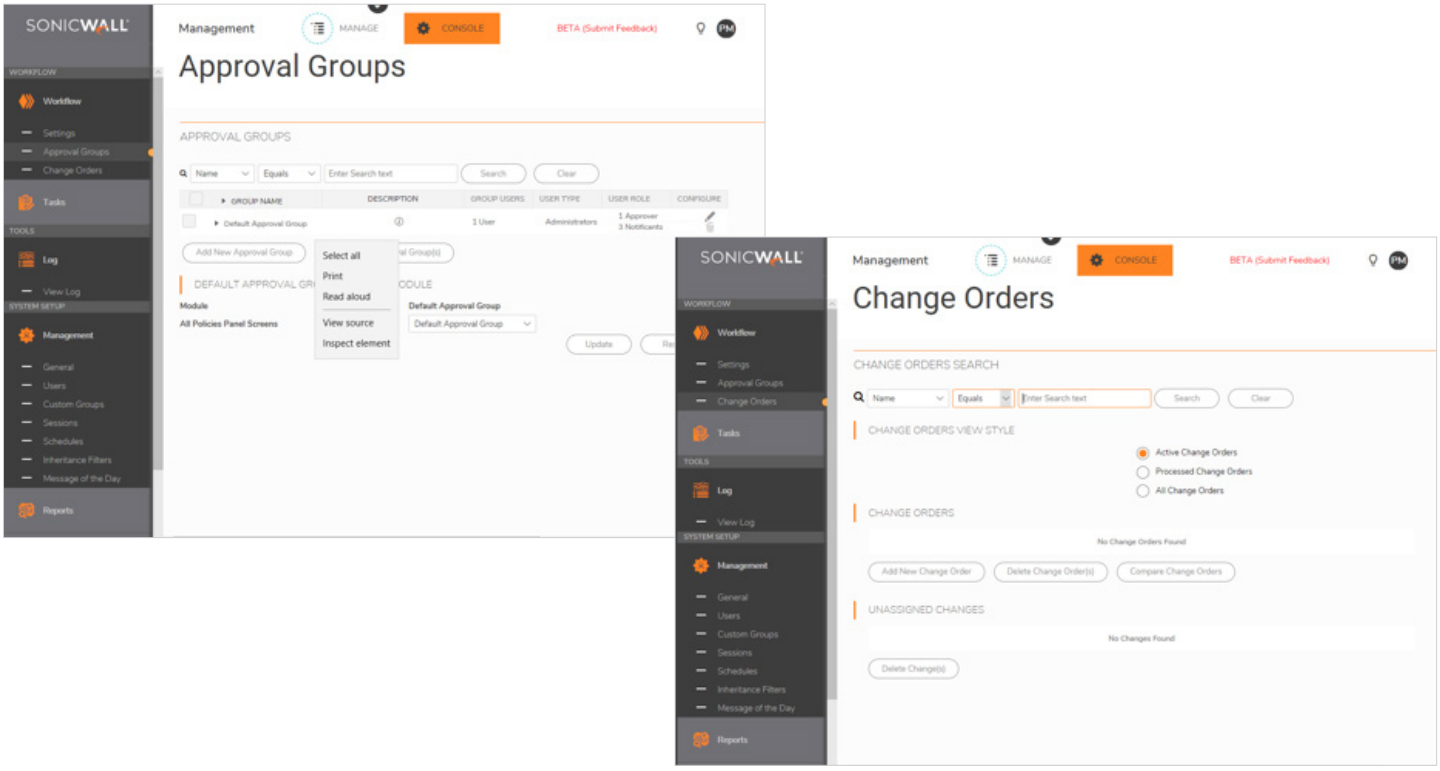
SONICWALL®

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.

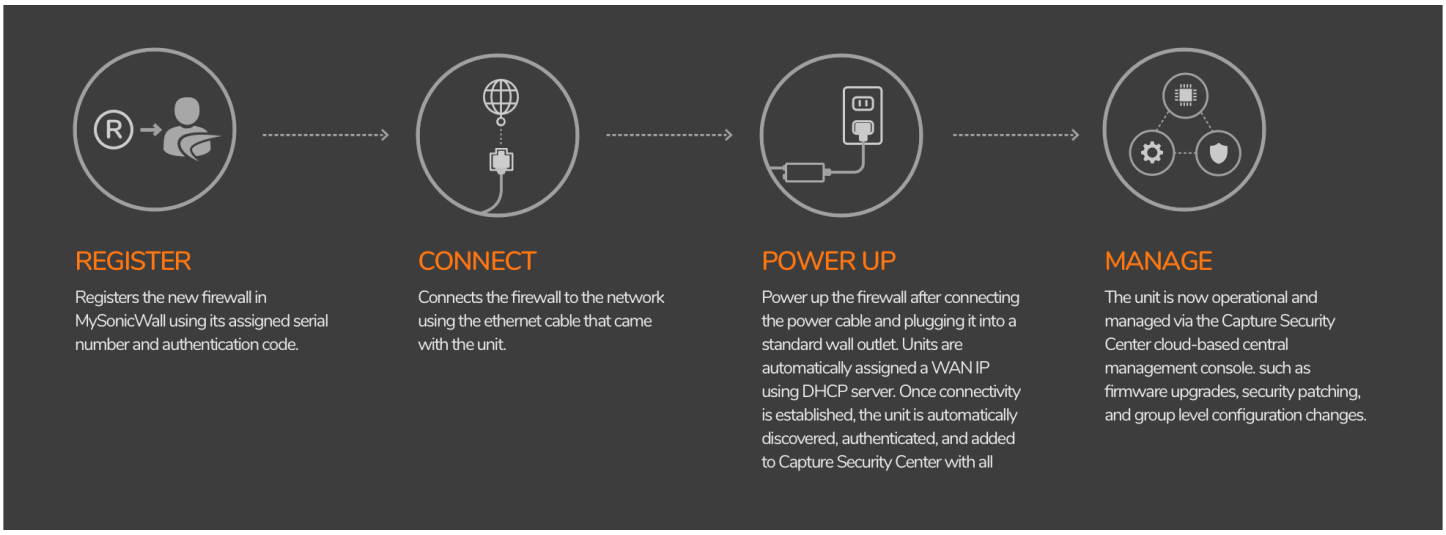
Capture Security Center provides a holistic approach to security governance, compliance and risk management.

Workflow Automation: Five steps to error-free policy management



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.

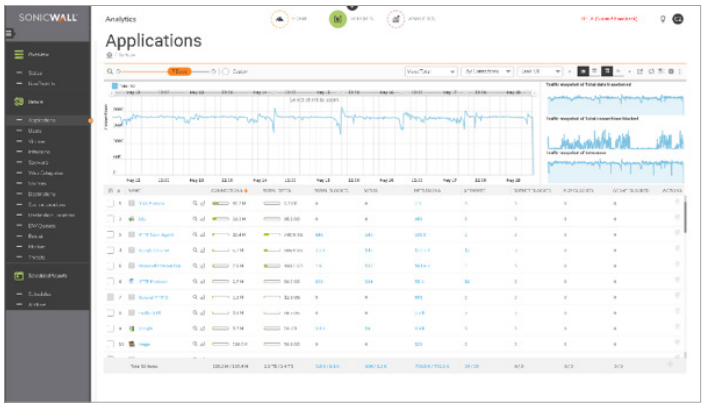


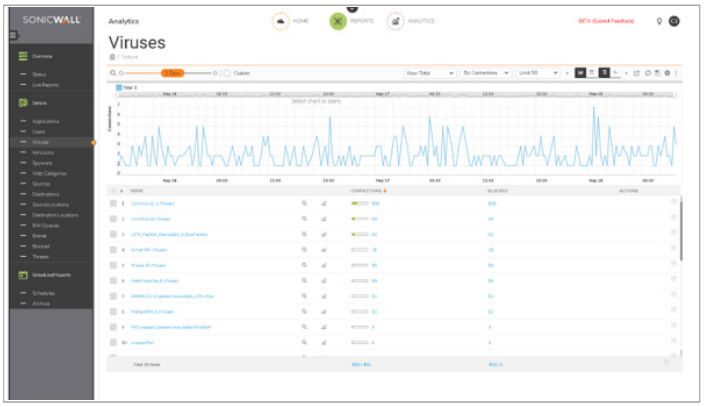
Zero-Touch Deployment: Operationalize firewall in four easy steps

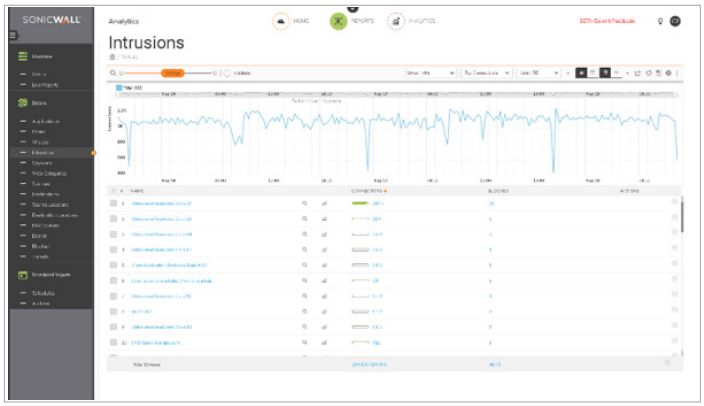
Reporting

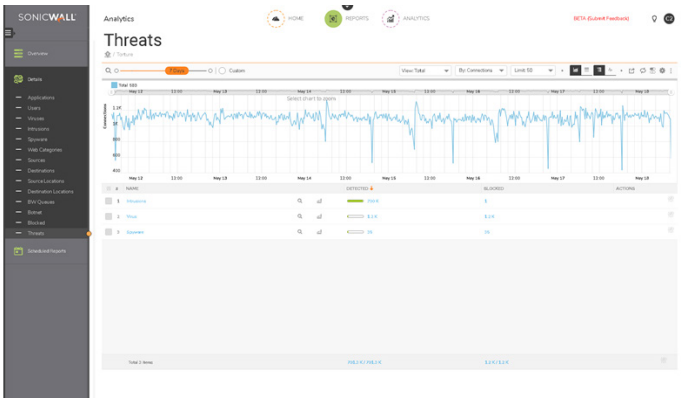
Capture Security Center offers predefined reports, as well as the flexibility to create custom reports using any combination of auditable data to acquire various use-case outcomes.

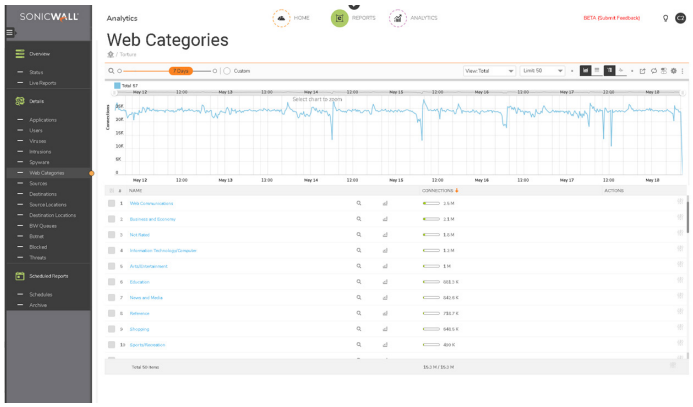
These outcomes include big-picture and detailed awareness of network events, user activities, threats, operational and performance issues, security efficacy, risks and security gaps, compliance readiness, and even post-mortem analysis. Every report is designed with the collective input from many years 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.







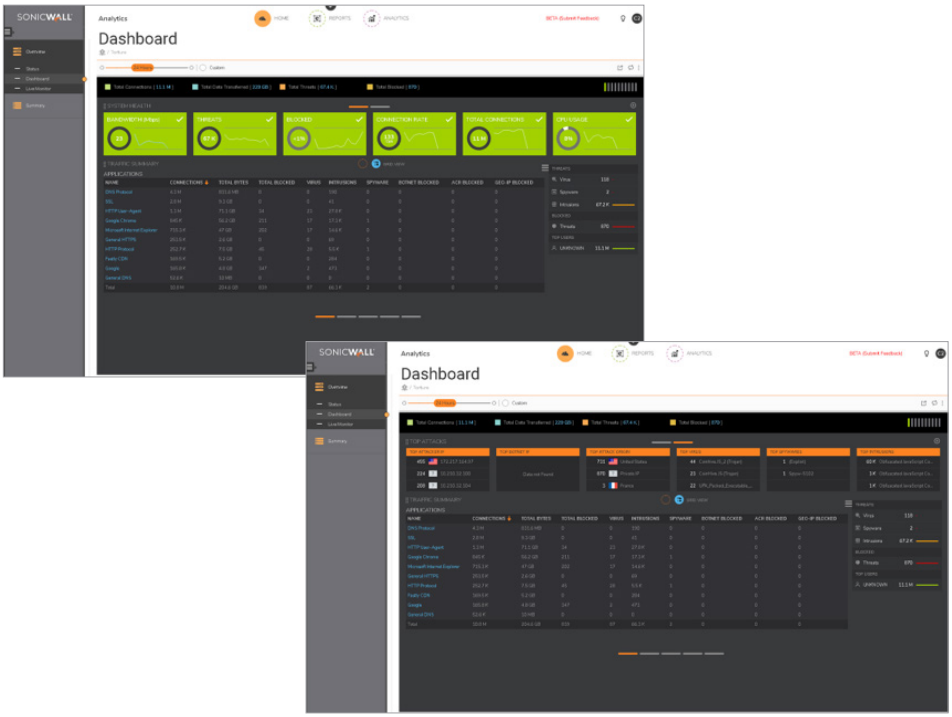


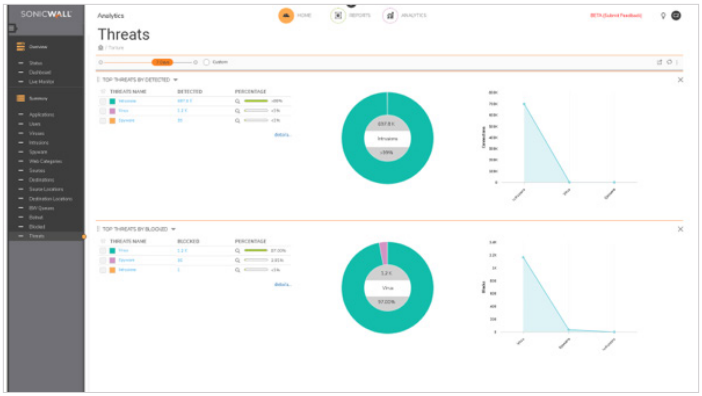


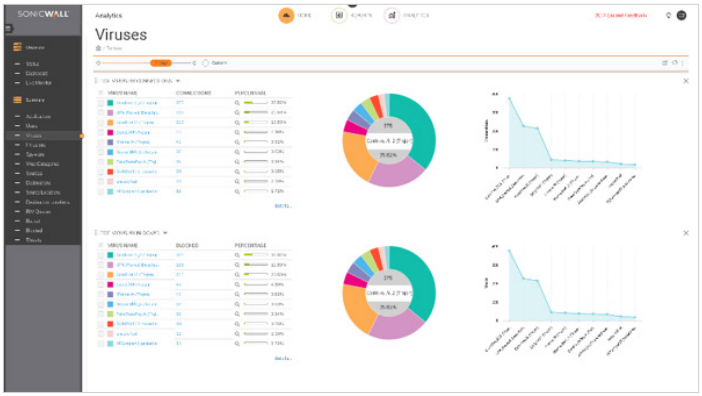
Analytics

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.

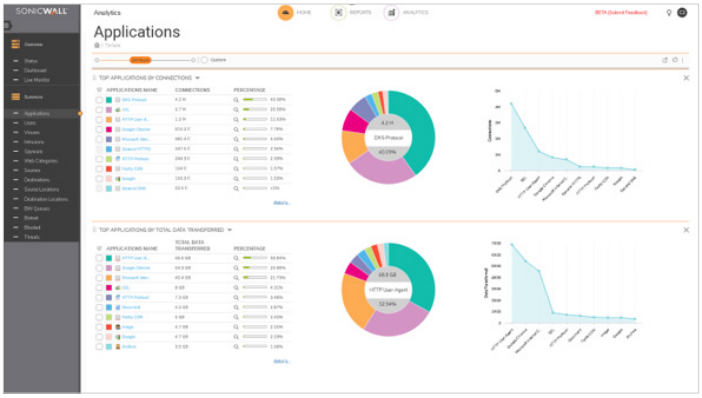
Analytics presents real-time visualization, monitoring and alerting of enriched security data through a single pane of glass. It comes with powerful tools that give customers complete authority, agility and flexibility to perform extensive drill-down investigative analysis of network traffic, user activities, 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.

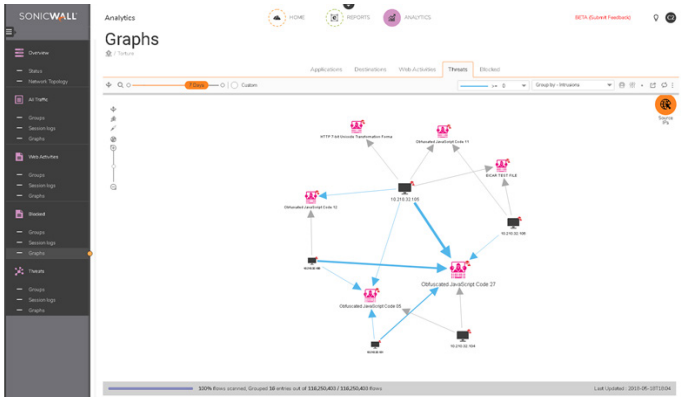


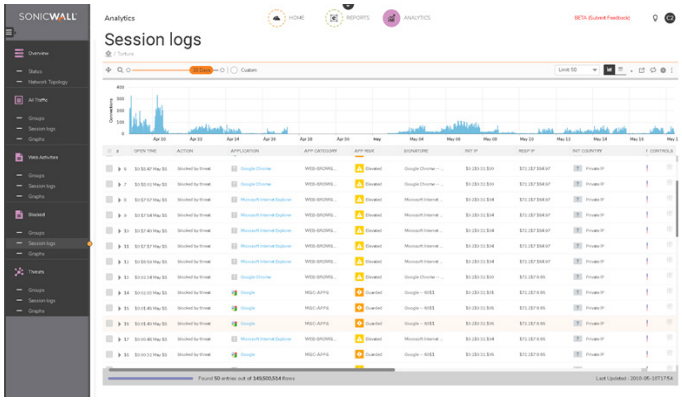

Analytics
Threats


Analytics
Viruses


Analytics
Graphs


Analytics
Applications


Analytics
Graphs

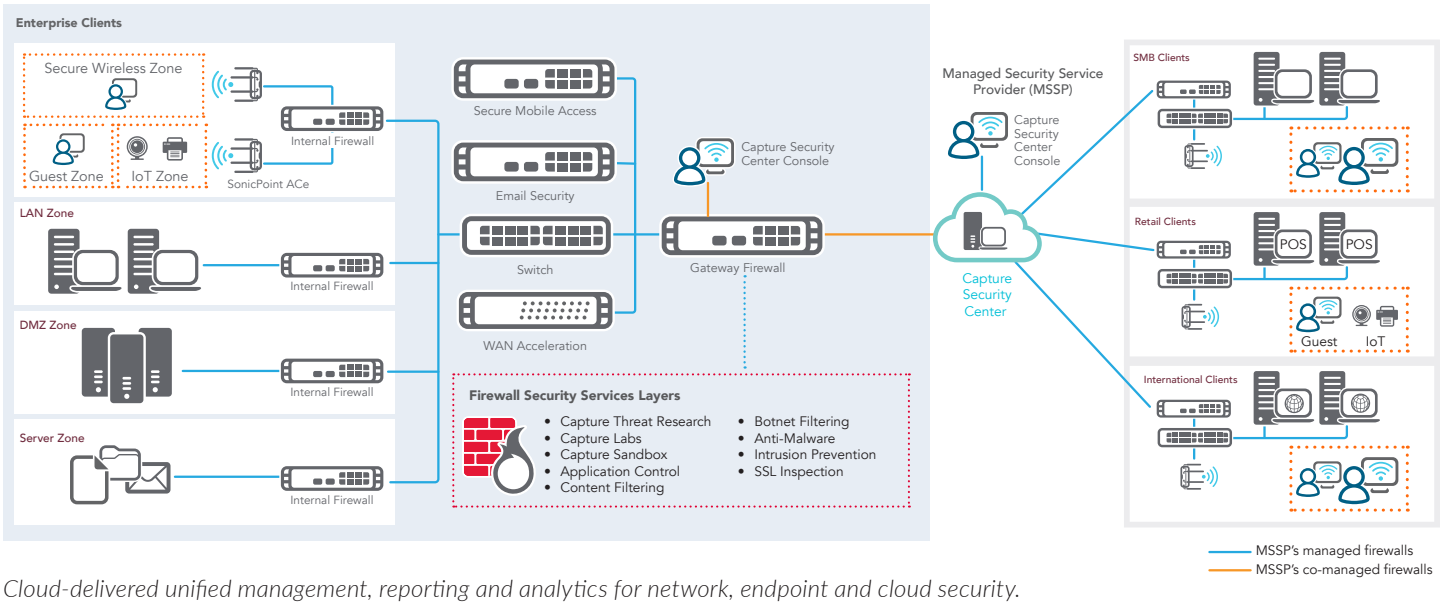

Analytics
Session logs

SONICWALL®

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.

Features

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.

Security management and monitoring features (continued)	
Feature	Description
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.
Risk Meters	Display live attacks in real-time, coupled 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 in a specific environment • Update computed risk score and threat level based on live threat data relative to existing defense capabilities • Underscore current security gaps where preventable threats get through due to missing defenses • Promote immediate defensive actions in response to prevent all incoming threats
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 (continued)	
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
- Risk Meters

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

The cloud-based services of CSC Management, Reporting, Analytics and CAS are available in below 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 on-screen 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 the SonicWall Analytics and SonicWall Cloud App Security tools and services to conduct network forensic and threat hunting using comprehensive drill-down and pivoting capabilities.

	Features	CSC Management Lite	CSC Management	CSC Management and Reporting	CSC Analytics
Management	Backup/Restore – firewall system	Yes	Yes	Yes	Yes
	Backup/Restore – firewall preferences	Yes	Yes	Yes	Yes
	Firmware upgrade	From local file only	From local file only or MySonicWall	Yes	From local file only
	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	–	–	–	Yes
	30-day traffic data retention	–	–	–	Yes
Technical Support		Web Cases only	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.*

Supported firewall models

Capture Security Center is available to customers with SOHO-W, TZ Series, NSA Series, NS*a* 2650-6650, and NS*v* Series firewalls. For SuperMassive 9000 Series, NS*a* 9250 to 9650 and NS*sp* 12400 to 12800, CSC Management subscription option is automatically activated as part of its corresponding AGSS subscription activation.

Capture Security Center			
	Management	Reporting	Analytics
Entry-level FW	SOHO-W, TZ Series, NSv 10-100	TZ Series, NSv 10-100	TZ Series, NSv 10-100
Mid-range FW	NSA Series, NS*a* 2650-6650, NSv 200-400	NSA Series, NS*a* 2650-6650, NSv 200-400	NSA Series, NS*a* 2650-6650, NSv 200-400
High-end FW	SuperMassive 9000 series, NS*sp* 12000 series, NS*a* 9250-9650, NSv 800-1600		

Ordering information

Product	SKU
SonicWall Capture Security Center Management for TZ Series, SOHO-W, NSv 10 to 100 1Yr	01-SSC-3664
SonicWall Capture Security Center Management for TZ Series, SOHO-W, NSv 10 to 100 2Yr	01-SSC-9151
SonicWall Capture Security Center Management for TZ Series, SOHO-W, 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, NSv 10 to 100 1Yr	01-SSC-3435
SonicWall Capture Security Center Management and Reporting for TZ Series, NSv 10 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 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 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: NS*a* 2600 to NS*a* 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 cybercriminal industry for over 27 years, defending small, medium-sized businesses and enterprises worldwide. Our combination of products and partners has enabled an automated real-time breach detection and prevention solution tuned to the specific needs of the more than 500,000 organizations in over 215 countries and territories, so you can do more business with less fear. For more information, visit **www.sonicwall.com** or follow us on Twitter, LinkedIn, Facebook and Instagram.

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

DataSheet-CaptureSecurityCenter-US-VG-MKTG4731