SONICWALL

SonicWall Analytics

Transforming data into decisions and decisions into actions

SonicWall Analytics provides an eagle-eye view into everything that is happening inside the SonicWall network security environment – all through a single pane of glass. At its core is a powerful, intelligence-driven analytic engine that automates the aggregation, normalization and contextualization of security data flowing across all SonicWall firewalls. The application's interactive dashboard uses various forms of semantic graphs, time-use charts and tables to create knowledge representations of the data models.

Analytics presents results in a meaningful, actionable and easily consumable manner.

This empowers security teams, analysts, incident responders, auditors, boards and C-suites to discover, interpret, prioritize, make evidence-based decisions, and take appropriate defensive and corrective actions against risks and threats as they unfold in the discovery process.

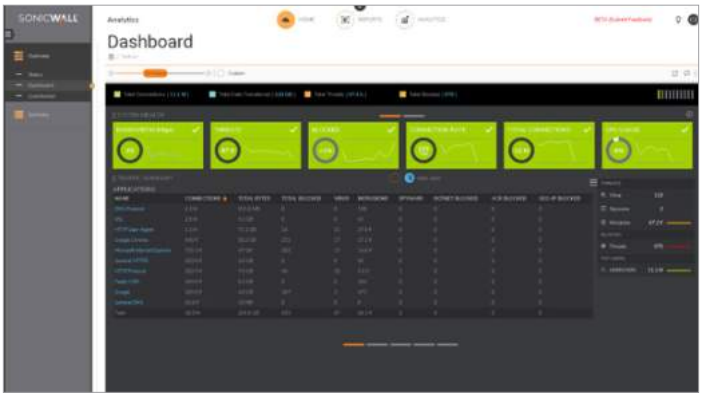
Analytics provides stakeholders with real-time insights and single-pane visibility, authority and flexibility. They can perform deep drill-down investigative and forensic analysis of network traffic, user access, connectivity, applications and utilization, state of security assets, security events, threat profiles and other firewall-related data.

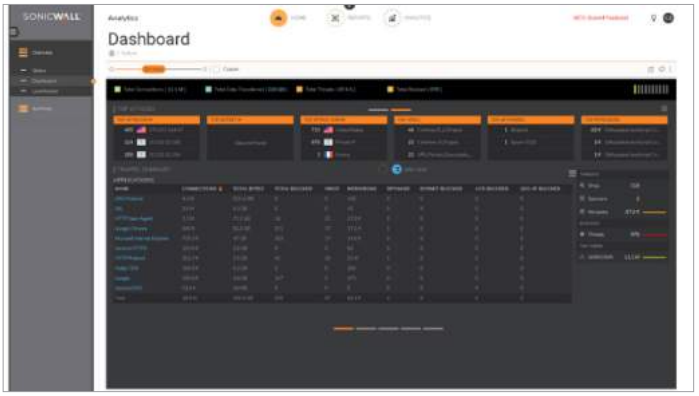
Benefits:

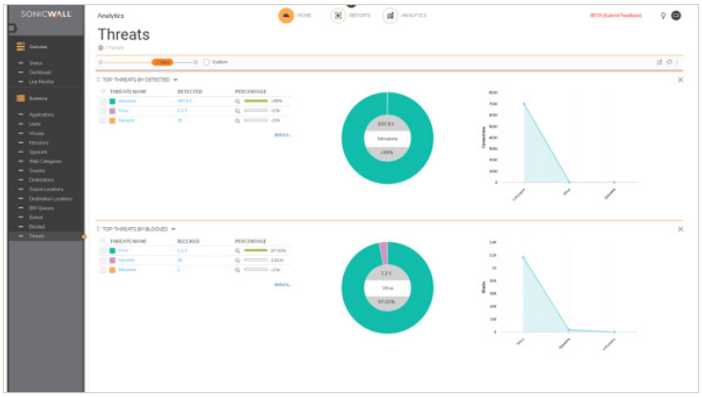
- Get single-pane visibility and complete situational awareness of the network security environment
- Have complete authority and flexibility to perform deep investigative and forensic analysis
- Gain deeper knowledge and understanding of potential and real risks and threats
- Remediate risks with greater clarity, certainty and speed
- Reduce incident response time with real-time, actionable threat intelligence
- Deploys as a cloud service or on-premises as a virtual appliance in VMare or Microsoft Hyper-V private cloud environment

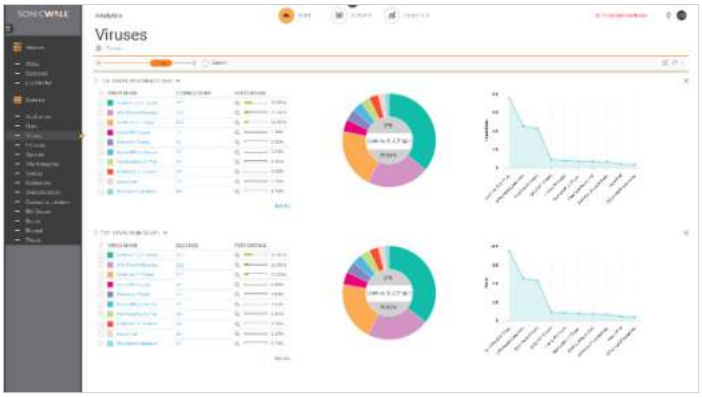
This deep knowledge and understanding of the security environment provides the intelligence and capacity to uncover and orchestrate remediation to security risks, and monitors and tracks the results with greater clarity, certainty and speed.

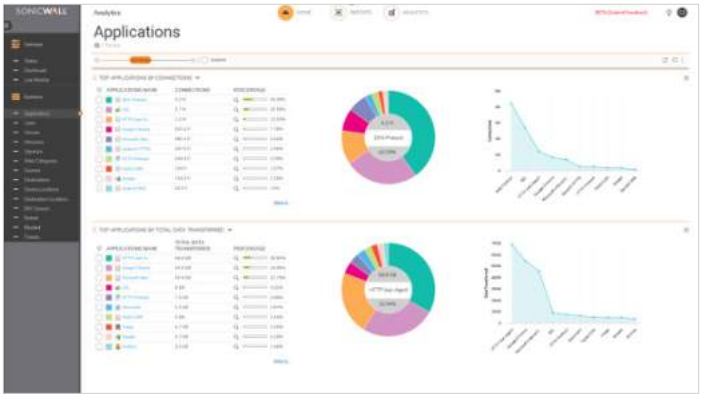
Integrating Analytics into the business process helps operationalize analytics, thus transforming data into knowledge, knowledge into decisions and decisions into actions toward achieving security automation.





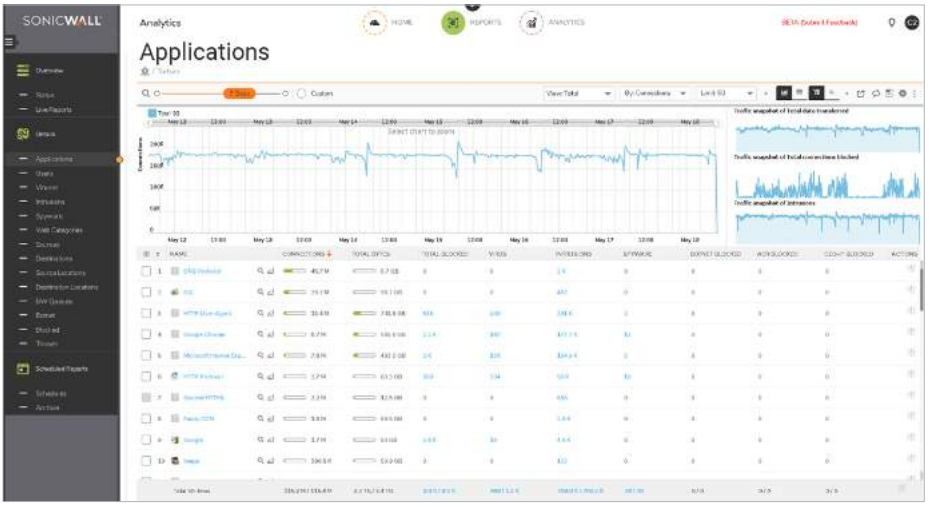






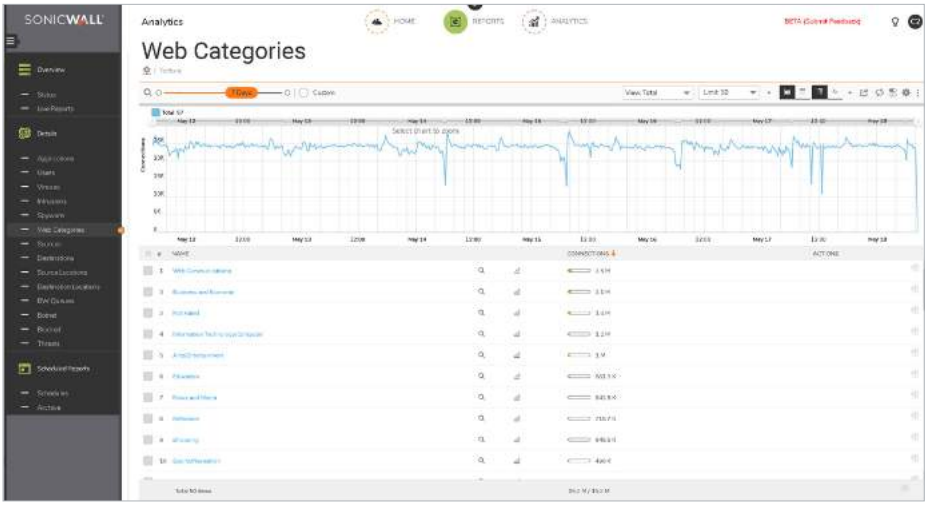
Reporting

Analytics includes a broad range of predefined reports, as well as the flexibility to create custom reports using any combination of auditable data for thorough risk analysis. These reports combined give security analysts detailed insights 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.



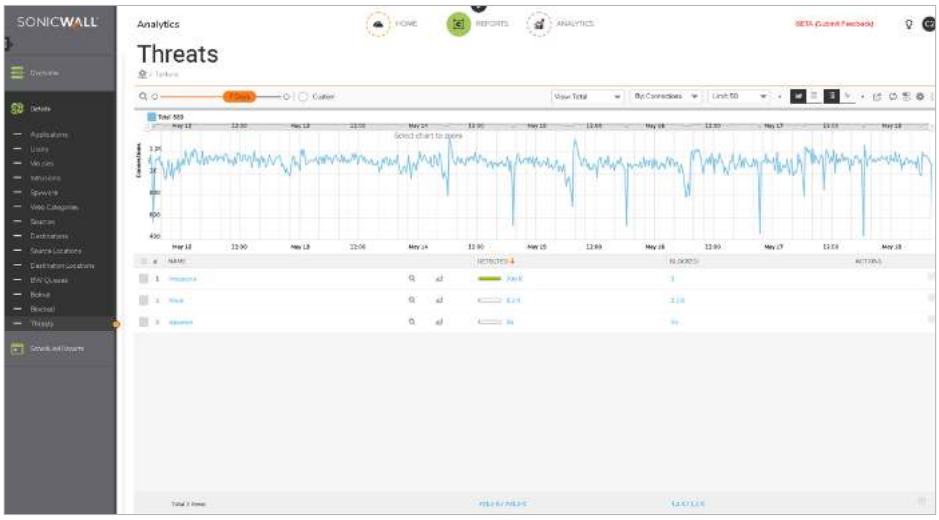
Easily view traffic usage statistics such as top websites visited. Drill-down reporting allows for sorting of data according to granular details, such the site name, IP address, website category and number of connections attempted.

Intuitive graphical reports simplify monitoring of SonicWall appliances and make it easy to identify traffic anomalies based on usage data for a specific timeline, initiator, responder or service. Export reports to a Microsoft® Excel® spreadsheet, PDF file or directly to a printer.



Built-in granular reporting allows for traffic usage data to be displayed according to top applications on the network. Easily identify the top applications detected or blocked according to category, timeline or initiator.

Threat management comes standard with Analytics; easily view the top threats to the network by target, initiator or threat type. Comprehensive threat reporting, such as Gateway Anti-Virus, Intrusion Prevention and Anti-Spyware, are all included.



Deploy via cloud service or virtual appliances

SonicWall Analytics is available in SaaS mode via the SonicWall Capture Security Center and can also be deployed on-premises as software installed on key virtual platforms such as VMware and Hyper-V. When used in conjunction with Capture Security Center, on-premises Analytics can be manage and its reports and data can be accessed and viewed by the Capture Security Center's Analytics console. The flexibility to leverage this product across multiple platforms along with capex or opex based licensing helps ease the financial and operation planning and decision processes. It also enables dynamic upscaling of storage to fulfill the growing data retention requirements from virtually unlimited number of firewall nodes.

Features

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.

Security analytics
Get real-time visibility with rapid threat detection. Enable security analysts and incident responders to hunt, identify and investigate issues.

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 swiftly manage and remediate risks by taking measured actions.

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 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.

Comprehensive graphical reports
Provide visibility into firewall threats, bandwidth usage, employee productivity, suspicious network activity and application traffic analysis.

Next-generation syslog reporting
Revolutionary architecture streamlines data summarization, allowing for near real-time reporting of incoming syslog messages. Direct access to the underlying raw data further facilitates extensive granular capabilities and highly customizable reporting

Universal scheduled reports
Provide a single entry point for all scheduled reports. One report can combine charts and tables for multiple units. Reports can be scheduled and sent out in various formats to one or more email addresses.

At-a-glance reporting
Offers customizable views to illustrate multiple summary reports on a single page. Users can easily navigate through vital network metrics to analyze data quickly across a variety of reports.

Compliance reporting
Enables administrators to generate reports that fulfill compliance requirements on an ad-hoc and scheduled basis for specific regulatory mandates such as PCI, HIPPA and SOX.

Multi-threat reporting
Collects information on thwarted attacks, providing instant access to threat activities detected by SonicWall firewalls using the SonicWall Capture ATP, Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Intelligence and Control Service.

User-based reporting
Tracks individual user activities locally or on remote network sites. Provides greater insight into traffic usage across the entire network and, more specifically, application usage, websites visited, backup activity and VPN connections per user.

Ubiquitous access
Simplifies reporting to provide administrators with analysis of any location using only a standard web browser.

New attack intelligence
Offers granular reporting on specific types of attacks, intrusion attempts and the source address of the attack to enable administrators to react quickly to incoming threats.

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.

Capture ATP Report
Shows detail threat behavior information to respond to a threat or infection.

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.

Features cont'd

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:

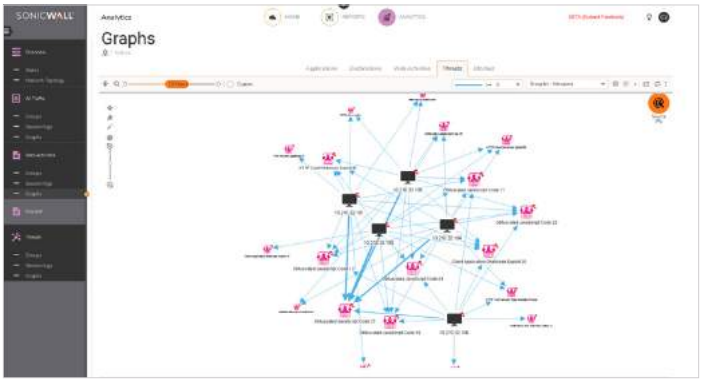
- Data Usage > Initiators
- Data Usage > Responders
- Data Usage > Details
- User Activity > Details
- Web Activity > Initiators

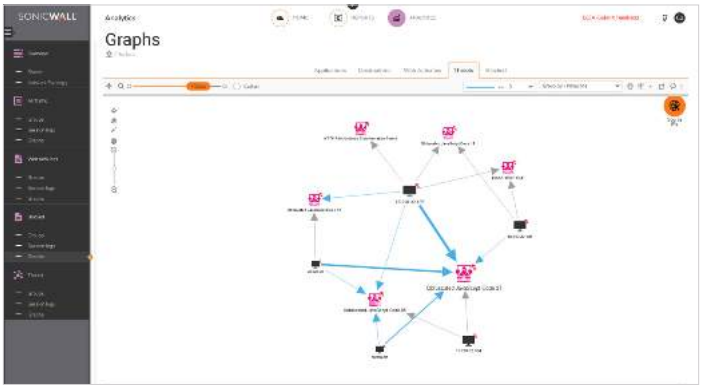
Centralized logging

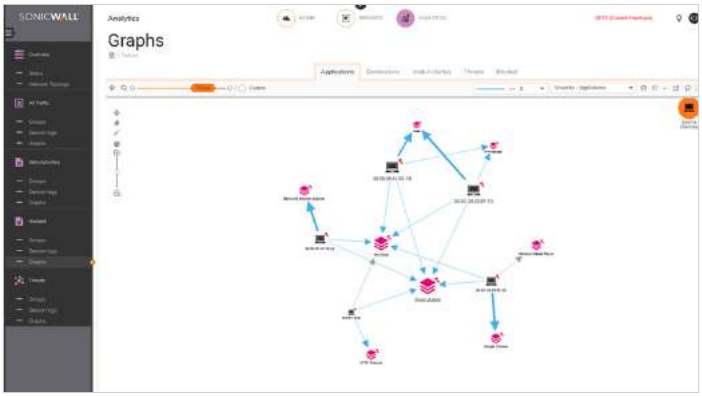
Offers a central location for consolidating security events and logs of all managed appliances, providing a single point to conduct network forensics.

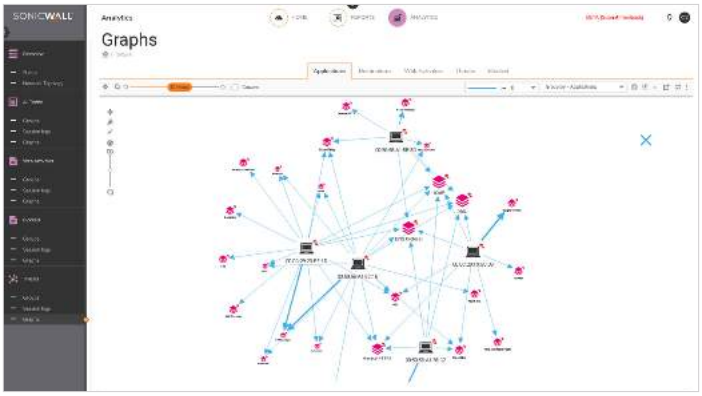
Partner Enabled Services

Need help to plan, deploy or optimize your SonicWall solution? SonicWall Advanced Services Partners are trained to provide you with world class professional services. Learn more at www.sonicwall.com/PES.









Analytics feature summary

Summary Dashboard with visualizations and charts

- Bandwidth rate
- CPU utilization
- Connection count
- Connection rate per second
- Risk index (scale 1-10)
- Block percentage
- Total connections
- Total data transferred
- Top applications
- Top intrusions
- Top URL categories
- Top viruses
- Number of viruses, intrusions, spyware, botnets

Live Monitor streaming with area/bar charts

- Applications
- Interface ingress/egress, average, min, peak
  - Bandwidth
  - Packet rate
  - Packet size
  - Connection rate
- Usage
  - Connection count
  - Multi-core monitor

Top Summary Dashboards with drill-downs

- Applications
- Users
- Viruses
- Intrusions
- Spyware
- Web categories
- Sources
- Destinations
- Source locations
- Destination locations
- BW queues
- Botnet

Reports with drill-downs, export to pdf/csv, and scheduled emailing

- Applications / Users / Sources / Destinations
  - Connections
  - Total connections blocked
  - Connections blocked by access rule
  - Connections blocked by threat
  - Connections blocked by botnet filter
  - Connections blocked by GeoIP filter
  - Connections blocked by Content Filtering Service
  - Virus
  - Intrusions
  - Spyware
  - Total data transferred
  - Data sent
  - Data received
- Viruses / Intrusions / Spyware / Web categories / Source locations / Destination locations / BW queues
  - Connections
  - Total data transferred
  - Data sent
  - Data received
- Botnet
  - Connections
- Export
  - .pdf
  - .csv
- Scheduled Reports
  - Flow Reporting
  - Capture Threat Assessment (SWARM)
  - Daily / Weekly / Monthly
  - Archive / Email / PDF

Analytics Session Viewer with drill-downs, filtering, export of individual session data

- Traffic analytics on any combination of:
  - Application
  - App Category
  - App Risk
  - Signature
  - Action
  - Initiator/responder IP
  - Initiator/responder country
  - Initiator/responder port
  - Initiator/responder bytes
  - Initiator/responder interface
  - Initiator/responder index
  - Initiator/responder gateway
  - Initiator/responder MAC
  - Protocol
  - Rate (kbps)
  - Flow ID
  - Intrusion
  - Virus
  - Spyware
  - Botnet
- Threats / Blocked analytics on any combination of:
  - Threat name
  - Threat type
  - Threat ID
  - Application
  - App category
  - App risk
  - Signature
  - Action
  - Initiator/responder IP
  - Initiator/responder country
  - Initiator/responder port
  - Initiator/responder bytes
  - Initiator/responder interface
  - Initiator/responder index
  - Initiator/responder Gateway
  - Initiator/responder MAC
  - Protocol
  - Rate (kbps)
  - Flow ID
  - Intrusion
  - Virus
  - Spyware
  - Botnet

Analytics feature summary cont'd

URL / Blocked analytics on any combination of:

- URL
- URL category
- URL domain
- Application
- App category
- App risk
- Signature
- Action
- Initiator/responder IP
- Initiator/responder country
- Initiator/responder port
- Initiator/responder bytes
- Initiator/responder interface
- Initiator/responder index
- Initiator/responder gateway
- Initiator/responder MAC
- Protocol
  - Rate (kbps)
  - Flow ID
  - Intrusion
  - Virus
  - Spyware
  - Botnet

Analytics Flow Monitor – drill-down and pivot on flow parameters

- Applications
  - Names
  - Categories
  - Signatures
- Users
  - Name
  - IP Address
  - Domain names
  - Authentication types
- Web activities
  - Websites
  - Web categories
  - URLs
- Sources
  - IP addresses
  - Interfaces
  - Countries
- Destinations
  - IP addresses
  - Interfaces
  - Countries
- Threats
  - Intrusions
  - Viruses
  - Spyware
  - Spam
  - Botnets
- VoIP
  - Media types
  - Caller IDs
- Devices
  - IP addresses
  - Interfaces
  - Names
- Contents
  - Email addresses
  - File types
- Bandwidth management
  - Inbound
  - Outbound
  - All
  - URL
  - Sessions
  - Total packets
  - Total bytes
  - Threats

Star Graphs – point-to-point visualizations, drill-downs, and pivoting

- Sources / Users / Locations / Devices
  - To/from
    - Destinations
    - Applications
    - Web activities
    - Threats
  - Filtered by
    - Number of connections
    - Data transferred
    - Packets exchanged
    - Number of threats
  - Halo highlighting for
    - Threats
    - Data > 1 MB
    - Connections >1000
    - Packets >1000

Licensing and Packaging

	Features	SaaS Analytics	On-premises Analytics
Management	Backup/Restore – firewall system	Yes	Yes*
	Backup/Restore – firewall preferences	Yes	Yes*
	Firmware upgrade	From local file only	From local file only**
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	Yes
	Cloud App Security - Shadow IT Discovery	Yes	No
	Data retention	30 Days	Unlimited
Technical Support		24x7 support	24x7 support**

Requires AGSS/CGSS service or any paid Capture Security Center service
*** Requires a 24x7 support license*

Analytics ordering information

Product	SKU
SonicWall Capture Security Center Analytics for TZ Series, SOHO-W, SOHO 250, SOHO250W, 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
SonicWall Analytics on prem 500 GB storage license	02-SSC-1503
24X7 Support for Analytics on prem 500 GB storage 1yr	02-SSC-1504
SonicWall Analytics on prem 1 TB storage license	02-SSC-1526
24X7 Support for Analytics on prem 1 TB storage 1yr	02-SSC-1527
SonicWall Analytics on prem 5 TB storage license	02-SSC-1530
24X7 Support for Analytics on prem 5 TB storage 1yr	02-SSC-1533
SonicWall Analytics on prem 10 TB storage license	02-SSC-1531
24X7 Support for Analytics on prem 10 TB storage 1yr	02-SSC-1536
SonicWall Analytics on prem unlimited storage license	02-SSC-1532
24X7 Support for Analytics on prem unlimited storage 1yr	02-SSC-1539

Minimum system requirements

For SonicWall Analytics in SaaS mode via the SonicWall Capture Security Center:

Supported SonicWall appliances include:

- SonicWall Network Security Appliances: E-Class NSA, NSa Series, TZ Series appliances, SOHO-W, SOHO 250, SOHO 250W
- SonicWall Network Security Virtual Appliances: NSv 10 to NSv 400

Supported SonicWall firmware

- SonicWall SonicOS 6.0 or higher

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)

For SonicWall Analytics on-premises deployment:

Virtual appliance

- Hypervisor: VMware ESXi v5.5 / v6.0 / v6.5 / v6.7, Microsoft Hyper-V Win 2016
- Recommended RAM: Unlimited (8 GB minimum)
- HardDisk: Base OVA 65 GB need external mount
- vCPU: 4/unlimited
- Network Interface: 1
- VMware Compatibility Guide

Supported SonicWall appliances include:

- SonicWall Network Security Appliances: SuperMassive E10000 and 9000 Series, E-Class NSA, NSa Series, TZ Series appliances, SOHO-W, SOHO 250, SOHO 250W
- SonicWall Network Security Virtual Appliances: NSv Series

Supported SonicWall firmware

- SonicWall SonicOS 6.0 or higher

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)

About SonicWall

SonicWall has been fighting the cybercriminal industry for over 27 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, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

Datasheet-Analytics-US-VG-343