# SonicWall Analytics

Transforming data into information, information into knowledge, knowledge into decisions and decisions into actions

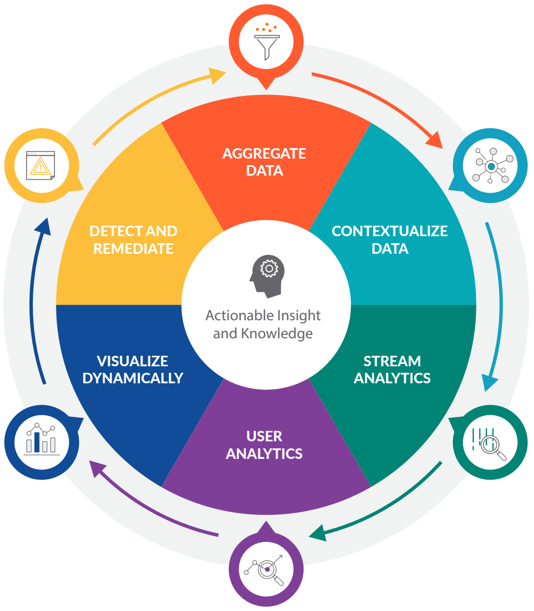
SonicWall Analytics provides an eagle-eye view into everything that is happening inside the SonicWall network security environment – all through a single pane of glass. At its core is a powerful, intelligence-driven analytic engine that automates the aggregation, normalization, correlation and contextualization of security data flowing across all SonicWall firewalls and wireless access points. The application's interactive dashboard uses various forms of 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, 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. As a result, 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



- 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

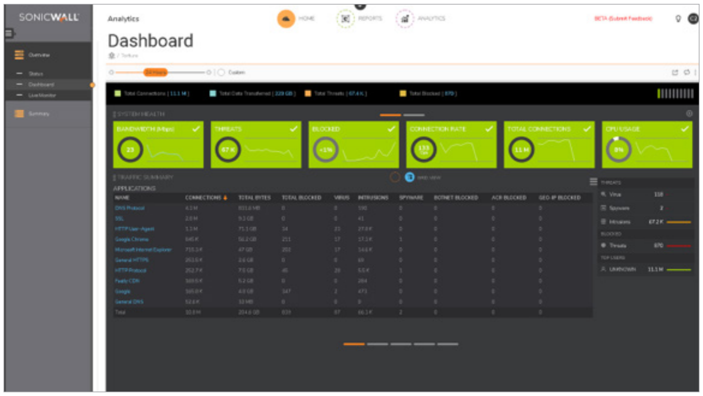
- Calibrate security policies and controls
- Exercise risk-based decision-making and remediation

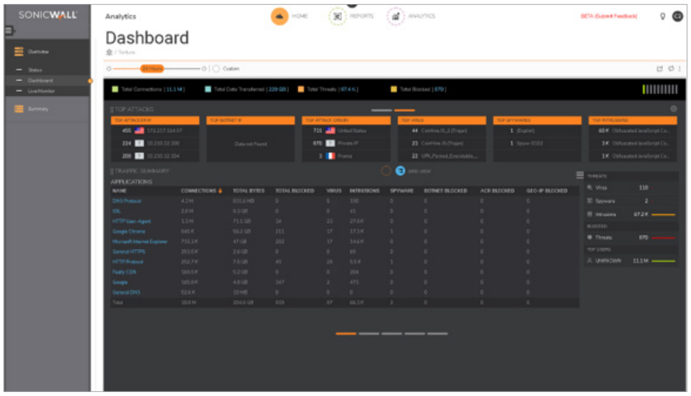
### Partner Enabled Services

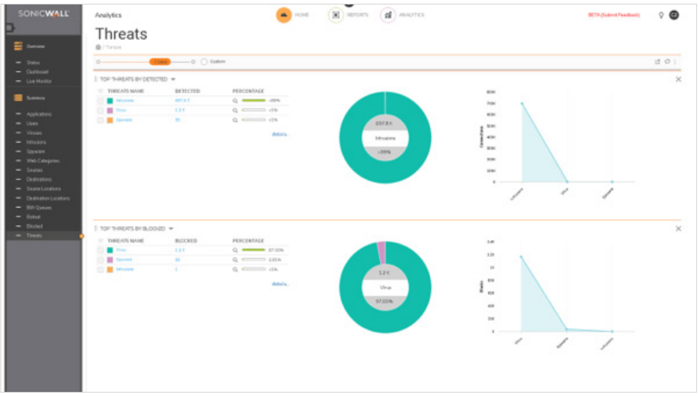
Need help to plan, deploy or optimize your SonicWall solution? SonicWall Advanced Services Partners are trained to provide you with world class professional services. Learn more at www.sonicwall.com/PES.

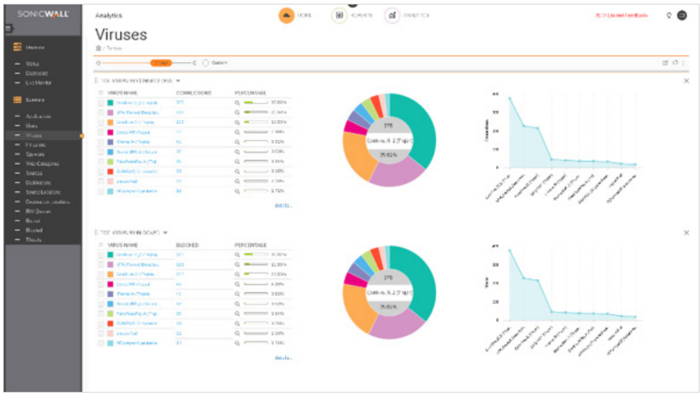
This deep knowledge and understanding of the security environment provides the intelligence and capacity to uncover and orchestrate remediation to security risks, and monitors and tracks the results with greater clarity, certainty and speed.

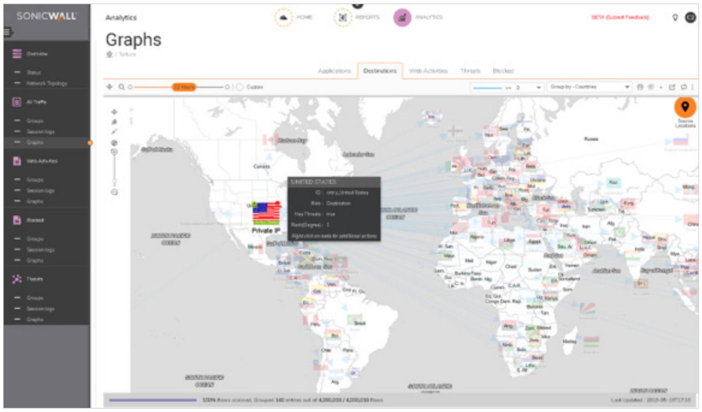
Integrating Analytics into the business process helps operationalize analytics, thus transforming data into information, information into knowledge and knowledge into decisions toward achieving security automation.

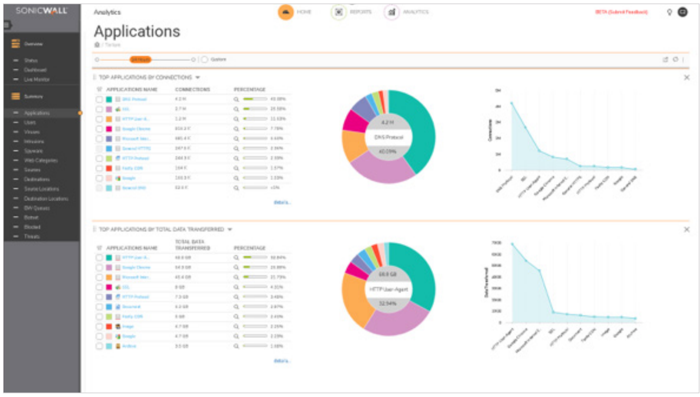












### Analytics features

| 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.<br>• A Real-Time Viewer with drag and drop customization<br>• A Real-Time Report screen with one-click filtering<br>• A Top Flows Dashboard with one-click View By buttons<br>• A Flow Reports screen with five additional flow attribute tabs<br>• A Flow Analytics screen with powerful correlation and pivoting features<br>• 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. |

## 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

### 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 | 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.*

## 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, 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 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: NS*a* 2600 to NS*a* 6650, and TZ Series appliances
- SonicWall Network Security Virtual Appliances: NS*v* 10 to NS*v* 400

## 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

SONICWALL®