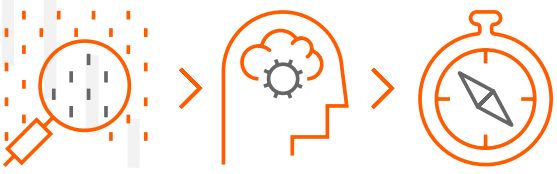
SonicWall Analytics

Transforming data into actionable insights

SonicWall Analytics transforms firewall traffic data into actionable insights across users, applications and networks to help mitigate security risks with greater precision and speed - all through a single interface. Built using high-performance cloud-native architecture, the analytic engine enriches a massive amount of raw data across thousands of firewall nodes at scale to give stakeholders complete visibility and security transparency via an executive dashboard.

Analytics creates knowledge representations of the data models by using various forms of semantic graphs and time-use charts and tables to help reduce dwell time and analyst fatigue. With added drill-down capabilities, security responders can investigate and zero in on critical data points to **expose hidden risks for early intervention** as well as take evidence-backed policy actions against risky user activities as they unfold in the discovery process.

With comprehensive visibility and control, security analysts see everything everywhere to become better risk managers while responders can focus their valuable time and effort on orchestrating rapid response actions across applications and users that matter most instead of reacting to every event. Analytics scales and performs at **cloud-agility and -elasticity** to meet even the most demanding enterprise requirements.



HIGHLIGHTS

Business

- Gain full security transparency
- Get real-time snapshot of the security posture
- Fulfill internal compliance obligations
- Conduct accurate cyber-defense planning and budgeting
- Reduce CAPEX and OPEX

Operational

- Understand security metrics easily at-a-glance
- Spark insights from every network and user events and alerts
- Establish accurate defensive policy actions
- Scale and perform at cloud-agility and -elasticity

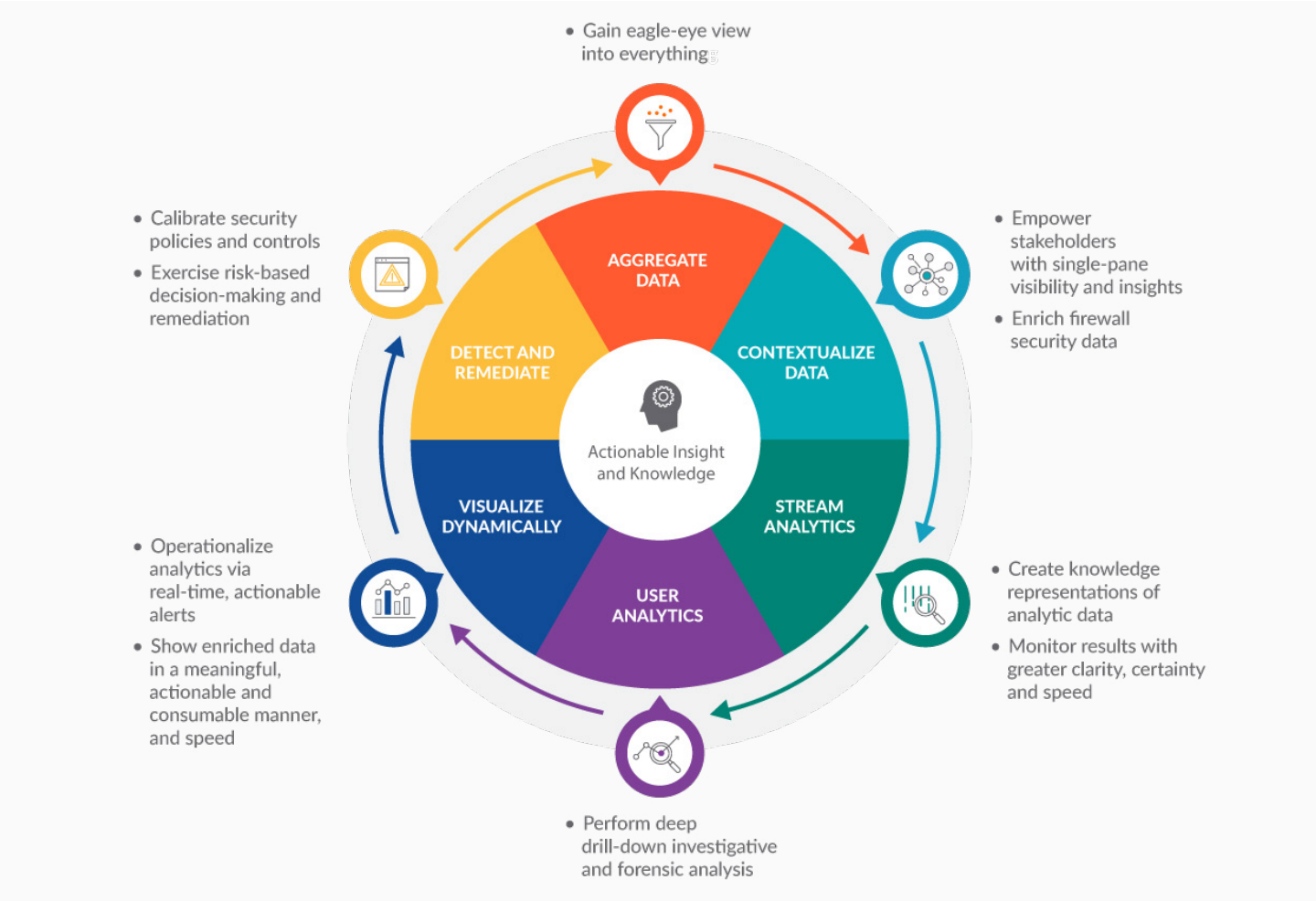
Security

- Uncover hidden risks
- Enable early intervention
- Respond timely to unsafe users' activities
- Help analysts become better risk managers
- Turn responders into better problem solvers

Learn more about SonicWall Analytics

www.sonicwall.com/analytics

DATASHEET



See Everything Everywhere

Analytics gives you a comprehensive view of your entire SonicWall security environment at the tenant, group, or device level. The executive dashboard provides static and near-real-time risk monitoring and analysis of all network traffic and data communication that passes through the firewall ecosystem. All log data is recorded, aggregated, contextualized, and presented in a meaningful and easily consumable way that empowers you to discover, interpret, triage, and take necessary defensive responses based on data-driven insight.

Analytics comes with a broad range of pre-defined reports and the flexibility to create custom reports specific to your desire use or intent using any combination of traffic data and have them delivered on a regular schedule. It presents up to a year of historical records for traffic analysis and security gaps and anomalies discovery to help you track, measure, and run a security-first network and security operation center.

Figure 1.0 Executive Dashboard

Understand Your Risk

Drill-down and pivoting capabilities enable you to further examine specific patterns and trends associated with ingress/egress traffic, application usage, user and device access, threat actions, and more with confidence. Using a mix of endpoint, network, user and application reporting and analytics, you can proactively analyze or respond to

alerts, anomalies, and risky user activities. With full security transparency, you will gain situation-awareness to find security risks, orchestrate policy actions, drive consistent security enforcement and continuously monitor the results across your environment.

Flexible deployment with SaaS, virtual or IaaS options

Analytics gives you flexible deployment choices that will best suit your operational requirements.

For a maintenance-free experience, Analytics is available as a SaaS offering hosted by SonicWall and is accessible over the internet. The SaaS option gives you unlimited elasticity to scale on-demand while lowering your operational cost. The typical cost of hardware and software acquisition, custom installation, regular maintenance and upgrades, asset depreciation, and retirement costs are removed and replaced with one low, predictable yearly subscription cost.

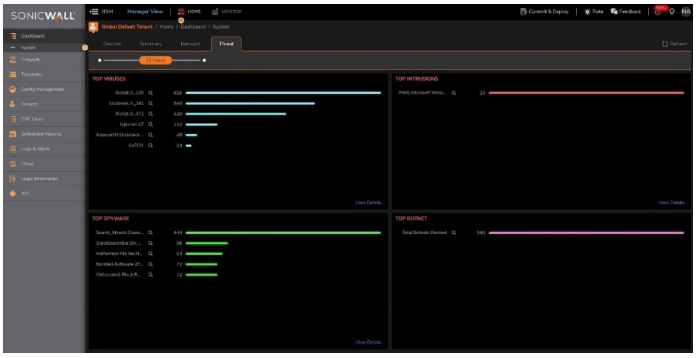


Figure 2.0 Threat Summary

For total system control and compliance, you can deploy Analytics on-prem as software installed on your choice of virtual platform, such as VMWare and Microsoft Hyper-V. You benefit from all the operational and economic benefits of virtualization, including system scalability, speed of system provisioning and cost reduction.

Feature Summary

Feature	Description
Data aggregation	Automate the aggregation and normalization of security data flowing through all firewalls.
Data contextualization	Process and enrich firewall data and present it in a structured, meaningful and easily consumable way, empowering the security team, analyst and stakeholders to discover, interpret, prioritize, make decisions and take appropriate defensive actions.
Streaming analytics	Stream of network security data is continuously processed and loaded in real-time and the results are illustrated in a dynamic, interactive visual dashboard.
User analytics	Show a comprehensive view of the workforce's web application and internet usage via an executive dashboard. It lets you granularly drill-down on historical records to establish evidence-backed policy-controlled measures against risky user web activities.
Application traffic analytics	Provide organizations with powerful insight into application traffic, bandwidth utilization and security threats, while providing powerful troubleshooting and forensics capabilities.
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 analysts can perform deep drill-down investigative and forensic analysis of security data with greater precision and speed.
Rapid detection and remediation	Investigative capabilities to chase down unsafe activities and to swiftly manage and remediate risks by taking measured actions.
Productivity Reports	Provide insights into the organization's internet resource utilizations. It generates powerful snapshots and drill-down reports on users' internet access behavior. These reports collect data about the website address and the date of access users visited and calculate the amount of time that users spent on each site and whether the time spent on those sites happened during office or non-office hours. Productivity reports classify users' web activities into productivity groups such as productive, unproductive, acceptable, unacceptable or custom-defined groups to help the organization better understand internet usage patterns and optimize workforce productivity. For example, with information about the duration users spent on non-business-related websites, department leaders in HR can manage and respond to potential employees' Code of Conduct policy violations. A similar use case can apply to all other functional groups.

Feature	Description
VPN Reports	Summarize what company resources are being used in the VPN tunnel, how much bandwidth they are consuming and who (i.e., username and IP address) uses that traffic. Network admins can leverage this information for monitoring business-critical applications, controlling or shaping traffic and planning for capacity growth.
Flow analytics and reports	Provide 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 additional flow attribute tabs • A Flow Analytics screen with powerful correlation and pivoting features • A Session Viewer for deep drill-down of individual sessions and packets
Comprehensive graphical reports	Provide visibility into firewall threats, bandwidth usage, employee productivity, suspicious network activity and application traffic analysis.
Syslog reporting	Streamline 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.
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 analysts.
At-a-glance reporting	Offer 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.
Multi-threat reporting	Collect information on 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 security services.
New Attack intelligence	Report on specific types of attacks, intrusion attempts and the source address of the attack to enable administrators to respond quickly to ongoing threats.
Rogue Wireless Access Point Reporting	Show 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	Provide an at-a-glance threat analysis dashboard and reports, which detail the analysis results for files sent to the service, including source, destination and a summary plus details of malware action once detonated.
Botnet Report	Include four report types: Attempts, Targets, Initiators, and Timeline containing attack vector contexts such as Botnet ID, IP Addresses, Countries, Hosts, Ports, Interfaces, Initiator/Target, Source/Destination, and User.
Geo IP Report	Contain 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	Show 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.
Cloud-Native Architecture	Collect, combine, process, reprocess, extract, correlate and load massive amount of queried data from tens of thousands of firewall nodes at cloud-speed and -elasticity.

Licensing and Packaging

	Features	SaaS Analytics	On-premises Analytics
Management	Backup/Restore – firewall system	Yes	Yes*
	Reporting (Netflow/IPFIX based)	Yes	Yes*
	Analytics (Netflow/IPFIX based)	From local file only	From local file only
Technical Support	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	1 Year
Technical Support		24x7 support	24x7 support**

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

Minimum System Requirements

For SonicWall Analytics in SaaS mode via Network Security Manager:

Supported SonicWall appliances include:

- SonicWall Network Security Appliances: E-Class NSA, NS*a* Series, TZ Series appliances, SOHO-W, SOHO 250, SOHO 250W
- SonicWall Network Security Virtual Appliances: NS*v* 10 to NS*v* 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, NS*a* Series, TZ Series appliances, SOHO-W, SOHO 250, SOHO 250W
- SonicWall Network Security Virtual Appliances: NS*v* Series

Learn more about SonicWall Analytics

www.sonicwall.com/analytics

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. 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-COG-3948