

# 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 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 visual and knowledge representations of the data datasets by using various forms of semantic graphs and time-use charts and tables to help reduce data silos 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](http://www.sonicwall.com/analytics)



## 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 that can be delivered on-demand or on a regular schedule. It also allows you the flexibility to custom-build reports with values and metrics chosen from an extensive library of firewall data types, allowing you to assemble and logically extract valuable insights from specific devices across selected groups or tenants. Custom reports help declutter data funnels, giving decision-makers and responders clearer



Figure 1.0 Executive Dashboard

visibility and actionable intel from smaller but more quality data sets for traffic analysis and security gaps and anomalies discovery. They can now zoom to the right analytics, make informed decisions, and take timely policy actions based on reliable data.

## 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.

## Optimize Workforce Productivity

User Analytics gives a broad and transparent view of your workforce's web application and internet usage activities. Drill-down capabilities enable analysts to pivot and investigate data points of interest and establish evidence-backed policy-controlled measures for risky users and applications as they unfold in the discovery process. In addition, Productivity Reports provide insights into employees' internet utilization and behavior over a specified period. It generates powerful snapshots or detailed reports that classify users' web activities into productivity groups such as productive, unproductive, acceptable, unacceptable, or custom-defined groups, helping organizations better understand and control internet usage.

## 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 integrated into SonicWall's Network Security Manager (NSM) 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 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.

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



Figure 2.0 Threat Summary

## Feature Summary

Feature	Description
User analytics	Show a comprehensive view of the workforce's network, application and threat activities via an interactive 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.
Custom reports	Self-guided workflow to custom-build reports with selected values and metrics chosen from a library of firewall data types.

Feature	Description
Tenant- and Group-level reports	Allow users to view pre-defined or custom reports at the device-group or tenant level.
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	<p>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.</p> <ul style="list-style-type: none"> <li>• A Real-Time Report screen with one-click filtering</li> <li>• A Top Flows Dashboard with one-click View By buttons</li> <li>• A Flow Reports screen with additional flow attribute tabs</li> <li>• A Flow Analytics screen with powerful correlation and pivoting features</li> <li>• A Session Viewer for deep drill-down of individual sessions and packets</li> </ul>
Comprehensive graphical reports	Provide visibility into firewall threats, bandwidth usage, employee productivity, suspicious network activity and application traffic analysis.
Syslog reporting (Only for Analytics 2.5)	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.
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

### Reporting

Features	SaaS Analytics for NSM Essential	SaaS Analytics for NSM Advanced	On-premises Analytics	On-premises Analytics
Log Protocol	Proprietary <sup>1</sup>	Netflow/IPFIX based <sup>1</sup>	Netflow/IPFIX based <sup>1</sup>	Syslog based <sup>1</sup>
Group/Tenant Level Dashboard	Yes	Yes	No	No
Capture ATP (Device Level)	Yes	Yes	Yes	Yes
Capture Threat Assessment (CTA) - Device Level	Yes	Yes	Yes	No
Productivity Reports <sup>3</sup>	No	Yes	No	No
VPN Reports	No	Yes	No	Yes
Custom Report	No	Yes	Yes	Yes
Schedule Report (Flow, Syslog, CTA or Management)	Yes (exclude Flow)	Yes	Yes	Yes
Days of reporting data	7 days (basic reporting)	365 days (complete reporting)	As per log rate, disk size and license <sup>4</sup>	Up to 36 months <sup>5</sup>

### Analytics

Days of analytics data	No	30 days	As per log rate, disk size and license <sup>4</sup>	Up to 36 months <sup>5</sup>
User-based analytic	No	Yes	Yes	Yes
Application analytics	No	Yes	Yes	Yes
Network forensic and threat hunting using drill-down and pivots	No	Yes	Yes	Yes
Technical Support	24x7 support	24x7 support	24x7 support <sup>2</sup>	24x7 support <sup>2</sup>

<sup>1</sup> Requires AGSS/CGSS service or any paid Capture Security Center service

<sup>2</sup> Requires a 24x7 support license

<sup>3</sup> Requires AGSS/CGSS license enabled on Generation 6/6.5 Firewalls, Essential Protection license on Generation 7 Firewalls

<sup>4</sup> Analytics and reporting data stored on system depends on aggregated log rate, available disk space and applied license

<sup>5</sup> Maximum number of days are user configurable

## Minimum System Requirements

### For SonicWall Analytics in SaaS mode via Network Security Manager:

#### Supported SonicWall appliances include:

- SonicWall Network Security Appliances: NSA Series, 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 firmware

- SonicWall SonicOS 6.0 or higher

#### Supported SonicWall appliances include:

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



# Learn more about SonicWall Analytics

[www.sonicwall.com/analytics](http://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](http://www.sonicwall.com).



**SonicWall, Inc.**  
1033 McCarthy Boulevard | Milpitas, CA 95035  
Refer to our website for additional information.  
[www.sonicwall.com](http://www.sonicwall.com)



© 2023 SonicWall Inc. ALL RIGHTS RESERVED.  
SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. Except as set forth in the terms and conditions as specified in the license agreement for this product, SonicWall and/or its affiliates assume no liability whatsoever and disclaims any express, implied or statutory warranty relating to its products including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose, or non-infringement. In no event shall SonicWall and/or its affiliates be liable for any direct, indirect, consequential, punitive, special or incidental damages (including, without limitation, damages for loss of profits, business interruption or loss of information) arising out of the use or inability to use this document, even if SonicWall and/or its affiliates have been advised of the possibility of such damages. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.