Abstract

Ideally, comprehensive security analytics extend beyond mere management and reporting. An intelligence-driven analytics engine should feature real-time data presented in a structured, meaningful, actionable and easily consumable manner. Security stakeholders should be able to monitor, record, analyze and report security data for deep forensic analysis across the entire security ecosystem, including multiple firewalls and wireless access points.

Introduction

Today's business-driven IT initiatives — such as mobility, BYOD, wireless, cloud and IoT — inadvertently create new vectors for cyberattack. Organizations often do not have deep, actionable insight into the behaviors, actions and traffic generated by new technologies over wired, wireless and mobile networks.

This lack of insight hampers the effectiveness of network security and compliance teams to plan and implement a viable defense. As a result, organizations must take a comprehensive approach to network security analysis across all networking vectors.

Best practices for comprehensive analytics

The goal of a comprehensive analytics solution should be to empower security teams, analysts, auditors, boards, C-suites and stakeholders to discover, interpret, prioritize and take appropriate defensive actions against security risks and threats. The end goal is the ability to make smarter decisions faster.

Best practices for comprehensive network security analytics require real-time visualization, monitoring and alerting of correlated security data through a single pane of glass. An effective solution requires powerful analytic tools to give
security teams the complete authority, agility and flexibility to perform deep drill-down investigative analysis.

Areas for analysis should include network traffic, user access, user connectivity, application utilization, state of security assets, security events, threat profile and other firewall-related data.

The resulting deep knowledge and understanding of the security environment should give security teams the full visibility and capacity needed to uncover security risks and orchestrate remediation. It should enable them to monitor and track results with clarity, certainty and speed.

Ultimately, effective network security analytics enable organizations to operationalize the analytics and integrate it into their business processes as a cornerstone in their journey toward achieving full security automation.

**Criteria requirements**

When considering a comprehensive network security analytics solution, selection criteria should include:

1. **Data aggregation**: An intelligence-driven analytic engine should be able to automate the aggregation, normalization, correlation and contextualization of security data flowing through all firewalls.

2. **Data contextualization**: Actionable analytics should be presented in a structured, meaningful and easily consumable way. This helps empower security teams, analysts and stakeholders to discover, interpret, prioritize, make decisions and take appropriate defensive actions.

3. **Streaming analytics**: Streams of network security data should be continuously processed, correlated and analyzed in real time, and the results should be illustrated in a dynamic, interactive visual dashboard.

4. **User analytics**: The capability to perform deep analysis of user activity trends can provide full visibility into their utilization, access and connections across the entire network.

5. **Real-time dynamic visualization**: Security teams should be able to perform deep drill-down investigative and forensic analysis of security data with precision, clarity and speed — all through a single-pane-of-glass.

6. **Real-time detection and remediation**: The analytics solution should include investigative capabilities to enable security teams to identify and investigate unsafe activities, and to quickly manage and remediate risks as they unfold in the discovery process.

**Conclusion**

A comprehensive network security analysis solution should provide deep security analytics that both aggregates and correlates network security data thoroughly. It should make those results meaningful, actionable and easily consumable for network security teams and stakeholders to interpret, prioritize, make decisions upon and take appropriate defensive actions.

A sound network security analysis solution should also be capable of weaving into the business process to help operationalize analytics by automating real-time, actionable alerts; orchestrating security policies and controls in a proactive and automated fashion; and monitoring the results for security assurance.

[Learn more](https://www.sonicwall.com/capture-security-center) about how SonicWall can provide your organization with in-depth, comprehensive network security analytics.
SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com