Symantec
A Division of Broadcom

Product Brief

Security Analytics

Accelerating Incident Response and Improving Network Visibility and Forensics

At a Glance

Security Analytics helps the following:

- **Speed Threat Identification:** Deliver complete visibility into network traffic, with full network traffic analysis and packet capture, classification, deep packet inspection, threat data enrichment, and anomaly detection capabilities.
- **Reduce Incident Response Times and Streamline Forensics:** Provide context around what is happening in the network to support fast incident response and resolution and accelerated post-breach forensics.
- **Deliver Quick Threat Detection to Cyber Security Infrastructure:** Quickly deploy high-performance network traffic analysis and forensics that integrates with the environment to enhance and streamline threat investigation and remediation activities.

Overview

Increasingly sophisticated threats against organizations require increasingly intelligent defenses to enable quick and effective responses. A successful defense requires full visibility into network traffic and insightful security intelligence capable of uncovering breaches, so that they can be quickly contained and remediated. Symantec™ Security Analytics delivers the complete network visibility and forensics required—to conduct comprehensive real-time and retrospective analysis and swiftly react to security issues to protect your workforce, fortify the network, and improve security processes.

A Comprehensive, High-Performance Solution

Symantec Security Analytics appliances are part of our Incident Response and Forensics solutions. These high-performance appliances harness the Symantec Security Analytics software to capture, inspect, index, classify, and enrich all network traffic (including full packets) in real time. This data is stored in an optimized file system for rapid analysis, instant retrieval, and complete reconstruction to support all incident response and remediation activities.

The appliances can be deployed anywhere in the network: at the perimeter, in the core, in a 10GbE backbone, or at a remote link to deliver clear, actionable intelligence for swift incident response and resolution and real-time network forensics. Security Analytics appliance components include:

- **Physical or virtual appliances:** Two server options, both in a 1U condensed form factor, complement available virtualized deployments with highly tuned platforms for network threat detection and forensic workloads of various capacities.
- **Storage modules:** Scale storage capacity as needed to retain days, weeks, or months of network traffic for in-depth investigations. Storage modules are available in a 144 TB (2-rack unit) or 840 TB (5-rack unit), high-density storage solution that supports up to 1.7 PB of raw storage per capture appliance.
- **Central manager:** Security Analytics Central Manager software, running either virtualized or on Security Analytics appliances, allows centrally administered configurations and orchestrated investigations across over 200 Security Analytics forensic appliances, physical, virtual, or in the cloud.

Next-Generation Capabilities for Advanced Protection

Security Analytics appliances are designed to deliver the network traffic analysis, security analytics, and advanced threat protection required to reduce the time it takes to resolve security incidents and conduct swift forensic investigations. Security Analytics enables the following capabilities:

Speed Threat Identification

Symantec Security Analytics enables total visibility into network traffic, from the data center to remote offices, through full network packet analysis, recording, and classification to accelerate the identification of attacks in your environment and shorten your exposure window. The Security Analytics appliances deliver the following:

- **Application classification:** Through powerful deep packet inspection (DPI), more than 3,300 applications and protocols are identified with thousands of descriptive metadata attributes generated, including content types and file names. This detailed metadata accelerates investigation by identifying what traffic is really hiding inside of well-known network channels.
- **Real-time threat intelligence:** Direct access to the latest threat intelligence, via tight integration with Symantec Intelligence Services and the Symantec Global Intelligence Network, delivers a network of thousands of customers and millions of users worldwide, as well as numerous third-party threat and reputation services. Symantec provides real-time, actionable threat intelligence, and URL and file reputation data directly to Security Analytics, enabling confidence in the most up-to-the-minute information on attacks targeting the organization.
- **Anomaly detection:** Performs advanced statistical analysis on captured data to create a baseline of the organization's network traffic and user activity, then detects outliers based on numerical, linguistic, and information density analysis. Security Analytics alerts on anomalous behavior with a pivot to the Anomaly Investigation view to see when the anomaly occurred, how often, and which parts of the network were involved.
- **Emerging, zero-day threat detection:** Automatic brokering of unknown files to Symantec Content Analysis or other 3rd-party sandboxes for detonation and threat scoring helps you incriminate or exonerate suspicious activity in your environment.

Reduce Incident Response Times and Streamline Forensics

Security Analytics enables the insights required to understand the context of security events in the environment, to quickly contain and remediate the full extent of a security incident, and support post-breach forensics activities. The appliances enable full retrospective analysis and real-time situational awareness, with clear, concise actionable intelligence about the threats to applications, files, and web content through the following:

- **Layer 2 through 7 analytics:** A variety of analytics tools, such as complete session reconstruction, data visualization, Root Cause Explorer, timeline analysis, file and object reconstruction, IP geolocation, trend analysis, and anomaly detection ensure everything is included to fully understand environment threats. For example, the Root Cause Explorer uses extracted network objects to reconstruct a timeline of suspect web sessions, emails, and chat conversations, so that evidence can be collected on the full source and scope of a security event.
- **Tight integration with security infrastructure:** Security Analytics integrates with best-of-breed security technologies, including security information and event management (SIEM) systems, next-generation firewalls (NGFW), intrusion prevention system (IPS), malware sandboxing, and endpoint forensics—to help leverage existing security investments and improve the effectiveness of established processes and workflows.
- **Context-aware security:** Security Analytics offers context for all security alerts to better understand what happened before, during, and after an attack. Pivot directly from any alert or log and obtain the full-payload details to support quick incident resolution and ongoing forensics activities.

Quickly Achieve Results

The enterprise-ready network threat detection and forensics solution quickly adds value to security operations. Easily deployed as a high-performance physical appliance, in a virtual environment, or next to cloud workloads, Security Analytics offers the following:

- **Enterprise-class performance:** Security Analytics delivers packet capture, indexing, and classification that meet the performance needs of the most demanding SOC environments. The hardware appliances are based on certified, industry-standard hardware platforms that provide the high availability and serviceability required to maximize uptime and performance.
- **Scalability:** Massive storage capacity can accommodate extended capture windows for retrospective analysis. Optimized high-density storage with petabytes of capacity enables the ability to meet fast-changing requirements and growing network traffic demands.
- **Flexible deployment:** Security Analytics enterprise licensing enables the option to deploy a high-powered forensics solution when and where it is needed. Deploy unlimited virtual appliances to handle branch or remote locations, add an appliance or additional storage to the data center, or deploy Security Analytics to add complete forensics to cloud workloads. Security Analytics Central Manager enables the ability to centrally monitor and manage distributed Security Analytics appliances from a single pane of glass.

The Intuitive UI makes it easy to get the information required to accelerate incident response and forensics activities.

Figure 1: Customized Dashboard View for Quick Analysis

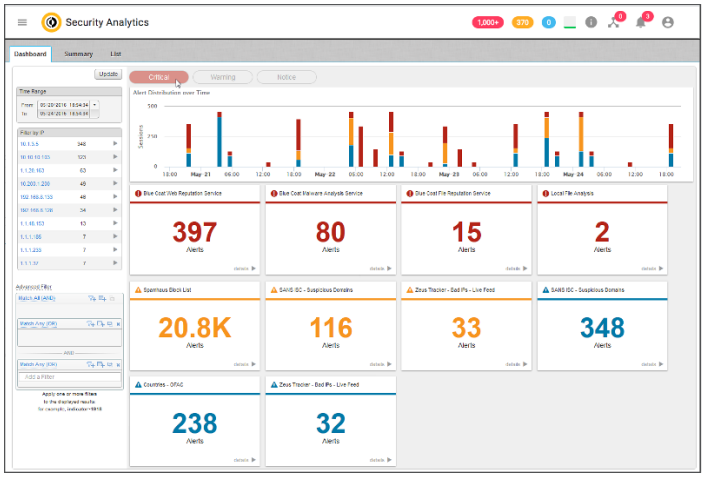

Figure 2: See the Source of Traffic and Threats

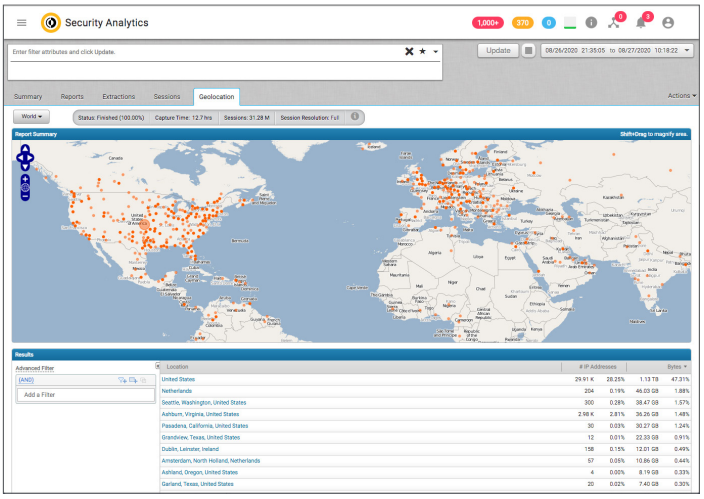

Figure 3. Full Packet Capture and Metadata Enrichment

Security Analytics Capture Appliances

Feature	Capture Appliance SA-SRVG8-20	Capture Appliance SA-SRVG8-40
Interfaces	4x 1GbE/10GbE Copper 2x SFF-8644 HD Mini-SAS Connectors (8x 12 Gb/s SAS lanes)	2x 10GbE/25GbE SR Fiber SFP28 4x 1GbE/10GbE Copper 4x SFF-8644 HD Mini-SAS Connectors (16x 12 Gb/s SAS lanes)
On-Board Storage	5x 2.4 TB 10K RPM Self-Encrypting SAS 12 Gb/s 512e 2.5-in. Hot-Plug Hard Drives	5x 2.4 TB 10K RPM Self-Encrypting SAS 12 Gb/s 512e 2.5-in. Hot-Plug Hard Drives
Max Usable Attached Storage	700 TB	1,400 TB
CPU	2x Intel 4210 2.2G, 10C/20T, 9.6 GT/s, 13.75M Cache, Turbo, HT (85W) DDR4-2400	2x Intel Xeon Gold 6230R 2.1G, 26C/52T, 10.4 GT/s, 35.75M Cache, Turbo, HT (150W) DDR4-2933
Memory Capacity	192 GB (16 GB x12) RDIMM, 2933 MT/s, Dual Rank DDR4	384 GB (16 GB x24) RDIMM, 2933 MT/s, Dual Rank DDR4
Rack Height	1 RU (42.8 mm/1.69 in.)	1 RU (42.8 mm/1.69in.)
Rack Width	482.0 mm/18.98 in.	482.0 mm/18.98 in.
Rack Depth	808.5 mm/31.8 in.	808.5 mm/31.8 in.
Chassis Configuration	Up to five 2.5-in. SAS Hard Drives	Up to five 2.5-in. SAS Hard Drives
Power Supplies	Dual, Hot-plug, Redundant Power Supply (1+1), 750W	Dual, Hot-plug, Redundant Power Supply (1+1), 750W
Power Cords	2x C13 to C14, PDU Style, 12 AMP, 6.5-foot (2m) Power Cord, North America	2 x C13 to C14, PDU Style, 12 AMP, 6.5-foot (2m) Power Cord, North America
Rails	Slide Rail Kit	Slide Rail Kit
Internal Raid Controller	1x PERC H730P RAID Controller, 2GB NV Cache, Mini card	1x PERC H730P RAID Controller, 2GB NV Cache, Mini card
External SAS Controller	1x SAS 12 Gb/s HBA External Controller, LP Adapter	2x SAS 12 Gb/s HBA External Controller, LP Adapter
Embedded Management	iDRAC9 Enterprise	iDRAC9 Enterprise
Input Power	Typical 1218.1 BTU/hr (357 W), Max: 1926.8 BTU/hr (564.7W)	Typical 1264.9.1 BTU/hr (371 W), Max: 1896.8 BTU/hr (555.9W)
Air Flow	42.4 CFM (20 l/s)	43.5 CFM (20.5 l/s)
Total Weight	Approx. 21.9 kg (48.3 lbs.) ±5%	Approx. 21.9 kg (48.3 lbs.) ±5%

Security Analytics Storage Appliances

Feature	Storage Module SA-STAG8-2U144	Storage Expansion Module SA-STXG8-2X144	Storage Module SA-STAG8-5U840
Interfaces	8x SFF-8644 HD Mini-SAS Connectors (32x 12 Gb/s SAS lanes)	8x SFF-8644 HD Mini-SAS Connectors (32x 12 Gb/s SAS lanes)	8x SFF-8644 HD Mini-SAS Connectors (32x 12 Gb/s SAS lanes)
Onboard Storage	12x 12 TB 7.2K RPM Self-Encrypting NLSAS 12 Gb/s 512e 3.5-in. Hotplug	12x 12 TB 7.2K RPM Self-Encrypting NLSAS 12 Gb/s 512e 3.5-in. Hotplug	70x 12 TB 7.2K RPM Self-Encrypting NLSAS 12 Gb/s 512e 3.5-in. Hotplug
Max Usable Storage	144 TB usable storage per module	144 TB usable storage per module	840 TB usable storage per module
CPU	—	—	—
Memory Capacity	—	—	—
Rack Height	2 RU (87.9 mm/3.46 in.)	2 RU (87.9 mm/3.46 in.)	5 RU (222.3 mm/8.75 in.)
Rack Width	483.0 mm/19.01 in.	483.0 mm/19.01 in.	483.0 mm/19.01 in.
Rack Depth	602.9 mm/23.74 in.	602.9 mm/23.74 in.	974.7 mm/38.31 in.
Chassis Configuration	12 Drive Storage Array Enclosure (RBOD)	12 Drive Expansion Enclosure (EBOD)	70 Drive Storage Array Enclosure (RBOD)
Power Supplies	Dual, Hot-plug, Redundant, 580W	Dual, Hot-plug, Redundant, 580W	Dual, Hot-plug, Redundant, 2200W
Power Cords	2x C13 to C14, PDU Style, 12 AMP, 6.5-foot (2m) Power Cord, North America	2 x C13 to C14, PDU Style, 12 AMP, 6.5-foot (2m) Power Cord, North America	C19 to C20, PDU Style, 8.2-foot (2.5m) Power Cord
Rails	Rack Rail, 2Us, Static	Rack Rail, 2Us, Static	Rack Rail, 5Us, Static
Internal Raid Controller	Built-in RAID Support	—	Built-in RAID Support
External SAS Controller	—	—	—
Embedded Management	ME Storage Manager (MESM) HTML5 GUI, CLI	ME Storage Manager (MESM) HTML5 GUI, CLI	ME Storage Manager (MESM) HTML5 GUI, CLI
Input Power	Typical 1204.5 BTU/hr (353W), Max: 1620.8 BTU/hr (475W)	Typical 1057.8 BTU/hr (310W), Max: 1446.7 BTU/hr (424W)	Typical 3818.2 BTU/hr (1119W), Max: 5534.5 BTU/hr (1622W)
Air Flow	6.5 CFM (3.1 l/s)	6.5 CFM (3.1 l/s)	231 CFM (109 l/s)
Total Weight	Approx. 32 kg (70.5 lbs.) ±5%	Approx. 32 kg (70.5 lbs.) ±5%	Approx. 120 kg (264.6 lbs.) ±5%

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

SED-sec-analy-PB100 September 9, 2020