DATA SHEET

Security Analytics Appliances

Accelerating Your Incident Response and Improving Your Network Forensics

At a glance

The integrated, turnkey Security Analytics Appliances:

- **Speed Threat Identification** – providing complete visibility into your network traffic, with full traffic capture, classification, deep packet inspection, threat data enrichment, and anomaly detection capabilities.
- **Reduce Incident Response Times & Streamline Forensics** – providing context around what is happening in your network to support fast incident response and resolution, and streamlined post-breach forensics.
- **Deliver Quick Time to Value** – offering easy to deploy, turnkey appliances that seamlessly integrate with your environment to enhance and streamline your security activities.

Introduction

With the increasingly sophisticated threats targeting your organization, you need increasingly intelligent defenses that enable you to quickly and effectively respond. This requires full visibility into your network traffic and insightful security intelligence capable of uncovering breaches, so they can be quickly contained and remediated. Symantec Security Analytics Appliances deliver the complete network visibility and forensics you need, out of the box – so you can conduct comprehensive retrospective analysis, and react to security issues in real time to protect your workforce, fortify your network and improve your security processes.

Integrated, Turnkey Solution

Symantec Security Analytics Appliances are part of our Incident Response and Forensics solutions. The turnkey, pre-configured appliances harness the Symantec Security Analytics software to capture, 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 your incident response activities.

The appliances can be deployed anywhere in the network: at the perimeter, in the core, in a 10 GbE 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:

- **2Gbps appliances:** Offering high-performance analytics; massive scalability; and centralized management.
- **10Gbps appliances:** Providing enterprise-proven capabilities via more interfaces, storage and memory.
- **Storage modules:** Extending storage capacity through direct-attach modules or high-densitity, fibre channel modules that support up to 1.5PB of storage per capture appliance.
- **Central Manager:** Manage over 200 Security Analytics appliances or VMs from a central location.

Next-Generation Capabilities for Advanced Protection

The Security Analytics Appliances are the only completely integrated solutions designed to deliver the security analytics and advanced threat protection you need to reduce the time it takes to resolve security incidents and conduct swift forensic investigations. With the Security Analytics Appliances, you can:

- Speed threat identification
- Reduce incident response time and streamline forensics
- Quickly achieve results

Speed Threat Identification

The solution gives you total visibility into your network traffic, from your data center to your remote offices, through full network packet recording and classification to accelerate the identification of attacks in your environment and shorten your exposure window. The Security Analytics Appliances deliver:

- **Application Classification:** Through powerful deep packet inspection (DPI), more than 3,100 applications and thousands of descriptive, metadata attributes, including content types, file names, and more are classified for easy analysis and recall.
- **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 3rd-party threat reputation services. Symantec provides real-time, actionable threat, URL and file reputation data directly to the Security Analytics Appliances, so you can be confident in the most up-to-the-minute information on the attacks targeting your organization.
- **Anomaly Detection:** Performs advanced statistical analysis on your captured data and baseline of your organization's network traffic and user activity. Security Analytics alerts you to anomalous behavior where you can 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

The Security Analytics Appliances give you the insights you need to understand the context of security events in your environment, so you can 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 your applications, files and web content via:

- **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 you have all you need to fully understand the threats in your environment. For example, the Root Cause Explorer uses extracted network objects to reconstruct a timeline of suspect web sessions, emails and chat conversations, so you can find evidence of the full source and scope of a security event.
- **Tight Integration with Security Infrastructure:** The appliances integrate 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 you leverage your existing security investments and improve the effectiveness of established processes and workflows.
- **Context-Aware Security:** Symantec offers you context for all your security alerts, so you can understand what happened, before, during and after an attack. You can 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 with Easy-to-Deploy, Integrated Turnkey Appliances

The durable, certified, thoroughly tested appliances quickly add value to your security operations. The easy-to-deploy, integrated turnkey solutions offer:

- **Security Analytics Appliances** deliver lossless packet capture, indexing and classification that meet the performance demands of your environment. The carrier-class appliances are based on certified, industry standard hardware platforms that provide the high availability and serviceability you require to maximize uptime and performance.
- **Scalability:** Massive storage capacity is able to accommodate extended historical capture windows. Optimized high-density storage, with support for add-on capacity, up to petabytes in size, enables you to meet your fast-changing requirements and growing network traffic demands.
- **Turnkey Deployment:** The appliances come with pre-installed and pre-configured Security Analytics Software for a fast deployment that delivers immediate value. The Security Analytics Central Manager enables you to centrally monitor and manage your distributed Security Analytics appliances from a single pane of glass.

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

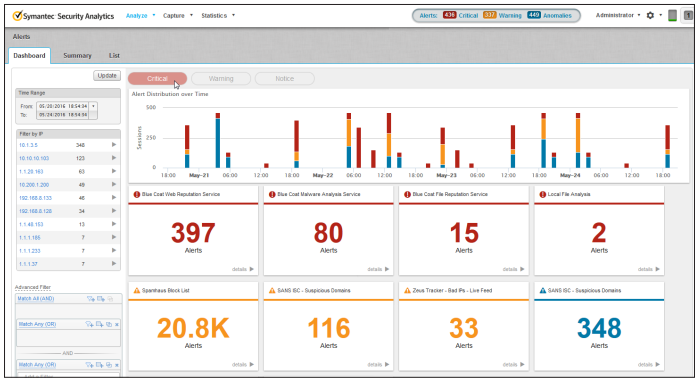

Figure 1. Customized dashboard view for quick analysis

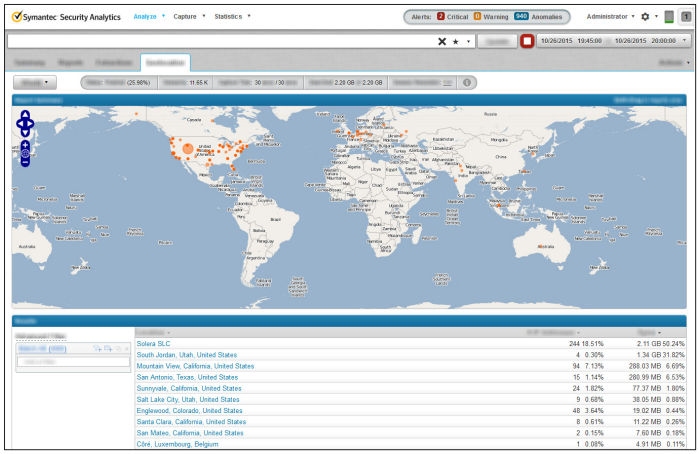

Figure 2. See where all your traffic and threats are coming from

Figure 3. Full packet capture and meta data enrichment

Security Analytics Appliances: Direct-Attached Storage				
	Capture Appliance SA-S500-20-FA	**Capture Appliance SA-S500-40-FA**	**Storage Module SA-J5300-DAS-40T**	**Central Manager SA-S500-10-CM**
Interfaces	6 x 1 GigE Copper (Capture) 1 x 1 GigE Copper (Management)	4 x 1 GigE Copper (Capture) 1 x 1 GigE Copper (Management) 2 x 1/10 GigE DP SFP+ SX/SR (Capture) 4 x SAS connectors	8 x SAS (12 Gb/s)	1 x 1 GigE Copper (Management)
On-Board Storage	12 x 2TB 7.2K NLSAS SED -10TB Raid 5 Capture (6x2TB) -4TB Raid 5 Index (3x2TB) -4TB RAID 5 System (3x2TB)	24 x 2TB 7.2K NLSAS SED -26TB Raid 5 Capture (14x2TB) -8TB Raid 5 Index (5x2TB) -8TB RAID 5 System (5x2TB)	12 SAS 12 Gb/s 4TB 3.5” Self-Encrypting Drives	5 x 2TB 7.2K NLSAS SED -8TB RAID 5 System (5x2TB)
Max Usable Storage	Up to 1 44TB Storage Module- 44TB usable storage	Up to 6 44TB Storage Modules- 264TB useable storage	44TB (44TB Usable / 48TB Raw)	N/A
CPU	2 x E5-2609 v2 (4 core, 2.5 GHz)	2 x E5-2680 v2 (10 core, 2.8 GHz)	---	2 x E5-2609 v2 (4 core, 2.5 GHz)
Memory Capacity	128 GB (8GB x 16 DDR3 RDIMM)	256 GB (16GB x 16 DDR3 RDIMM)	---	128 GB (8GB x 16 DDR3 RDIMM)
Rack Height	2 RU	2 RU	2 RU	2 RU
Rack Depth	812.8mm / 32in	812.8mm / 32in	507mm/19.96 inches	812.8mm / 32in
Chassis Configuration	Up to 12 2.5” Hard Drives	Up to 24 2.5” Hard Drives	12 Drive JBOD Enclosure	Up to 5 2.5” Hard Drives
Power Supplies	Dual, Hot-Plug, Redundant (1+1), 1100W	Dual, Hot-Plug, Redundant (1+1), 1100W	Dual, Hot-plug, Redundant, 595W	Dual, Hot-Plug, Redundant (1+1), 1100W
Power Cords	2x NEMA 5-15P to C13 Wall Plug, 13A, 6FT	2x NEMA 5-15P to C13 Wall Plug, 13A, 6FT	2x SP-305 to IS-14, 10AMP, 6ft, Redundant PSUs	2x NEMA 5-15P to C13 Wall Plug, 13A, 6FT
Rails	Slide Rail Kit	Slide Rail Kit	Rack Rail, 2Us, Static	Slide Rail Kit
Internal Raid Controller	1 x Avago SAS9271-8i	1 x Avago SAS9271-8i	---	1 x Avago SAS9271-8i
External Raid Controller	1 x Avago SAS9380-8e	2 x Avago SAS9380-8e	---	NA
Embedded Management	1G Base-T for BMC MGMT	1G Base-T for BMC MGMT	---	1G Base-T for BMC MGMT
Input Power	Typical 2600 BTU/hr (762 W), Max: 3752 BTU/hr (1100 W)	Typical 2600 BTU/hr (762 W), Max: 3752 BTU/hr (1100 W)	Typical 2763.8 BTU/hr (810 W)	Typical 2600 BTU/hr (762 W), Max: 3752 BTU/hr (1100 W)
Air Flow	29.5 CFM (13.9 l/s)	32.6 CFM (15.4 l/s)	49.3 CFM (23.3 l/s)	23.9 CFM (11.3 l/s)
Total Weight	Approx. 30kg (66.12 lbs) +/- 5%	Approx. 30kg (66.12 lbs) +/- 5%	Approx: 24.8kg (54.7 lbs) +/-5%	Approx. 30kg (66.12 lbs) +/- 5%

Security Analytics Appliances: High-Density SAN Storage		
	10G HD Appliance SA-S500-30-FA	**300TB Storage Array SA-E5660-ISA-300T**
Interfaces	4 x 1 GigE Copper (Capture) 1 x 1 GigE Copper (Management) 2 x 1/10 GigE DP SFP+ SX/SR (Capture) 4 x Fibre Channel HBA	N/A
On-Board Storage	5 x 2TB 7.2K NLSAS SED -8TB RAID 5 System (5x2TB)	360TB (60x6TB 7.2K FIPS 140-2 Self-Encrypting NLSAS 3.5in Hot-plug Hard Drives)
Max Usable Storage	Up to 5 312TB Storage Modules- Each module consists of: 2 R5 (4+1) index partitions = 48TB 2 R5 (11+1) capture partitions = 256TB 1.3PB maximum useable storage	312TB 2 R5 (4+1) index partitions = 48TB 4 R5 (11+1) capture partitions = 264TB 2 Hot Spares
CPU	2 x E5-2680 v2 (10 core, 2.8 GHz)	N/A
Memory Capacity	256 GB (16GB x 16 DDR3 RDIMM)	N/A
Rack Height	2RU	7”
Rack Depth	812.8mm / 32in	32.5”
Chassis Configuration	Up to 5 2.5” Hard Drives	4U
Power Supplies	Dual, Hot-Plug, Redundant (1+1), 1100W	Dual hot-plug power supplies
Power Cords	2x NEMA 5-15P to C13 Wall Plug, 13A, 6FT	2 x Power Cord, C20 to C19, PDU Style, 250V, 16A, 2ft (0.6m)
Rails	Slide Rail Kit	Static rails
Server Raid Controller	1 x Avago SAS9271-8i	N/A
External Raid Controller	NA	N/A
Storage Network Interface	2 x Avago LPe16002B	2 x 8GB Caching Controller with 16 Gb/s Fibre Channel support
Embedded Management	1G Base-T for BMC MGMT	SANtricity Storage Manager
Heat Dissipation	1563 BTU/hr	5159 BTU/hr
Input Voltage	Typical 2600 BTU/hr (762 W), Max: 3752 BTU/hr (1100 W)	200 - 240V AC, auto ranging, 50Hz/60Hz
Total Weight	Approx. 30kg (66.12 lbs) +/- 5%	Approx: 109.2kg (240.7 lb) +/-5%
Air Flow	33.8 CFM	231 CFM
Power Consumption	458 W	1512 W

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world’s leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec’s Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world’s largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit **www.symantec.com** or connect with us on **Facebook**, **Twitter**, and **LinkedIn**.

Symantec™ 350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | **www.symantec.com**

18D157064_ds_Security_Analytics_Appliance-EN