

Security Information & Event Manager (SIEM)

Compliance through Security Information and Event Management, Log Management, and Network Behavioral Analysis



Delivers fast, accurate data about security threats:

- Severity of an attack
- Importance of the affected asset
- Identity of the attacker
- Credibility of data sources
- Identification of abnormal behavior

Product Overview

The Enterasys Security Information and Event Manager (SIEM) product combines best-in-class detection methodologies with behavioral analysis and information from third party vulnerability assessment tools to provide the industry's most intelligent security management solution. Enterasys SIEM delivers actionable information to effectively manage the security posture for organizations of all sizes.

The challenge created by most threat detection systems is the volume of information they generate — making it difficult to determine which vulnerabilities require an immediate, high priority response. The Enterasys SIEM solution addresses this challenge and provides powerful tools that enable the security operations team to proactively manage complex IT security infrastructures.

Enterasys Security Information and Event Manager:

- Goes beyond traditional security information and event managers and network behavioral analysis products to deliver threat management, log management, compliance reporting, and increased operational efficiency
- Collects and combines network activity data, security events, logs, vulnerability data, and external threat data into a powerful management dashboard that intelligently correlates, normalizes, and prioritizes—greatly improving remediation and response times, and greatly enhancing the effectiveness of IT staff
- Baselines normal network behavior by collecting, analyzing, and aggregating network flows from a broad range of networking and security appliances including JFlow, NetFlow, and SFlow records. It then discerns network traffic patterns that deviate from this norm, flagging potential attacks or vulnerabilities—anomalous behavior is captured and reported for correlation and remediation
- Tracks extensive logging and trend information, and generates a broad range of reports for network security, network optimization, and regulatory compliance purposes; report templates are provided for COBIT, GLB, HIPAA, PCI, and Sarbanes Oxley

Benefits

- Enables NOC and SOC staff to focus on actionable information rather than struggle to interpret millions of daily events generated by network security appliances, switches, routers, servers, and applications
- Uses advanced surveillance and forensics analysis to deliver situational awareness of both external and internal threats including inappropriate content, IM file transfers, traffic from undesirable geographies, data theft, and malicious worm infections
- Leverages existing investments in network and security infrastructure while accelerating time to value through out-of-box functionality, rapid deployment, and staff efficiency gains
- Integrates with Enterasys Intrusion Prevention System (IPS), Network Access Control (NAC), and NMS Automated Security Manager solutions to provide a unified, real-time view of the threat landscape and effectively detect, isolate, and automatically remediate threats
- Integrates with a broad array of third party security and network products, including firewalls and routers, for the highest level of visibility and protection
- Virtual Flow Collector allows the analysis of network behavior and enables Layer 7 visibility within virtual infrastructures
- Meets the deployment requirements of the largest enterprises with modular component options and easily deployed high availability functionality

**There is nothing more important
than our customers.**

All SIEM appliances offer High Availability (HA) functionality that ensures availability of SIEM data in the event of a hardware or network failure. HA provides automatic failover and full disk replication between a primary and secondary host. The secondary host maintains the same data as the primary host by either replicating the data on the primary host or accessing a shared external storage. At regular intervals the secondary host sends a heartbeat ping to the primary host to detect hardware or network failure. If the secondary host detects a failure, the secondary host automatically assumes all responsibilities of the primary host. The Enterasys SIEM HA functionality is easily and cost-effectively deployed through appliances and wizards without requiring additional fault management solutions and storage options.

The Enterasys SIEM solution portfolio features appliances for quick and easy setup. The Enterasys SIEM solution complements its appliances with the Virtual Flow (VFlow) Collector. This virtual flow collector

appliance enables application layer traffic monitoring and security intelligence in a virtual infrastructure. Available Enterasys SIEM solution components include:

- SIEM Base Appliance
- Flow Anomaly Processor
- Event Processor
- Network Behavioral Flow Sensors
- Virtual Flow Collector
- SIEM Console Manager
- High Availability options

Features

SIEM Base Appliances

Enterasys SIEM Base Appliances deliver actionable security intelligence in a rack-mount, network-ready platform. They provide on-board event collection and correlation, Layer 7 traffic analysis, aggregation of flow data from multiple network connected devices, and a feature-rich management interface. With pre-installed software and web-based setup, SIEM appliances simplify the deployment and configuration of unified security management.

The SIEM Base Appliance for Small Enterprise (model DSIMBA7-SE) is an all-in-one security information management solution. It is ideal for smaller central site or departmental use, and for fast, easy deployment.

The SIEM Base Appliance for Large Enterprise (model DSIMBA7-LU) is designed for large and geographically dispersed organizations. It is ideal for users that demand a scalable, enterprise-class solution that can be easily upgraded to support additional flow and event monitoring capacity as required.

Both SIEM platforms capture event and flow data from a broad range of networked devices including application servers, web servers, workstations, routers, switches, firewalls, VPN tunnel servers, and IDS/IPS appliances. For an up-to-date listing of supported devices please refer to the SIEM product information at http://www.enterasys.com/company/literature/Enterasys_SIEM_Supported_DSIMs.pdf.

SIEM Flow Anomaly Processor

The SIEM Flow Anomaly Processor (model DSIMBA7-FAP) is an expansion unit for Enterasys SIEM. It offloads and enhances the processing of flow data from the DSIMBA7-LU appliance and interfaces with Behavioral Flow Sensors to collect IP traffic flow information from a broad range of devices. Each SIEM Flow Anomaly Processor can process up to 1,200,000 flows per minute (unidirectional).

SIEM Event Processor

The SIEM Event Processor (model DSIMBA7-EVP) is an expansion unit for Enterasys SIEM. It offloads and enhances processing of event data from the DSIMBA7-LU appliance. Status events are collected from a broad array

of network and security devices—including router syslogs, SNMP events, and firewall events. Each SIEM Event Processor can process up to 10,000 events per second and, for added flexibility, multiple Event Processors may be connected to a single DSIMBA7-LU appliance.

SIEM Network Behavioral Flow Sensors

A network traffic flow is a sequence of packets that share common characteristics—such as source/destination IP address, source/destination TCP port, and IP protocol used. SIEM Network Behavioral Flow Sensors are deployed at strategic points in the network to collect IP traffic flow information from a broad range of networked devices—including switches, routers, security appliances, servers, and applications. SIEM Network Behavioral Flow Sensors go beyond traditional flow-based data sources to enable application-layer (L1-L7) flow analysis and anomaly detection. Deep packet and content inspection capabilities identify threats tunneled over standard protocols and ports. Network Behavioral Flow Sensors interface with the Enterasys SIEM Base Appliances or the SIEM Flow Anomaly Processor.

SIEM Virtual Flow Collectors

Gain the same visibility and functionality that SIEM Network Behavioral Flow Sensors provide for the physical environment for the virtual network infrastructure. A SIEM Virtual Flow Collector is a virtual appliance that enables the analysis of network behavior and Layer 7 visibility within the enterprise's virtual infrastructure. SIEM Virtual Flow Collectors support up to 10,000 flows per minute and monitoring of three virtual interfaces with one additional switch designated as the management interface.

SIEM Console Manager

For large deployments, the SIEM Console Manager distributes the collection and processing of flows and logs while maintaining a global view of the entire network. Console Manager requires a minimum of one Processor Appliance (Event Processor and/or Flow Processor). NBAD sensors are required for Layer 7 monitoring.

Specifications*

Technical Specifications for all SIEM appliances are shown in the tables below. All appliances support RAID 10 for high availability and redundancy of OS and storage. Enterasys SIEM appliances support external storage options including iSCSI SAN and NAS.

SIEM Base Appliances

Model	DSIMBA7-LU / DSIMBA7-LU-HA	DSIMBA7-SE / DSIMBA7-SE-HA
Application	High-performance, scalable Security Information and Event Management	All-in-one Security Information and Event Management
Event Management, Vulnerability Management, and Directed Remediation	Yes	Yes
Expansion Options	Software License Upgrades External Flow Anomaly Processors External Event Processors	The DSIMBA7-SE appliance is designed specifically for smaller enterprise and departmental deployments
Behavioral Flow Sensor	Uses external Behavioral Flow Sensors	Integrated Behavioral Flow Sensor
Maximum # Flows Per Minute (FPM)	400,000 FPM (Unidirectional) 200,000 FPM (Bidirectional)	100,000 FPM (Unidirectional) 50,000 FPM (Bidirectional)
Maximum # Events Per Second (EPS)	5,000 EPS	1,000 EPS
Processor & Memory	2 X Quad Core Intel® Xeon® Processors at 2.4 Ghz 24 GB	2 X Quad Core Intel® Xeon® Processors at 2.4 Ghz 12 GB
Hard Disk Drive	6 X 750 GB SATA	6 X 500 GB SATA
Network Interfaces	4 X 10/100/1000 Base-T (on board)	4 X 10/100/1000 Base-T (on board)
Power Supply	Dual redundant 570 W	Dual redundant 570 W
Form Factor	2U rack-mountable chassis	2U rack-mountable chassis

SIEM Event Processor

Model	DSIMBA7-EVP / DSIMBA7-EVP-HA
Rated Throughput	5,000 EPS (base configuration) 10,000 EPS (maximum configuration)
Connects to	SIEM Base Appliance DSIMBA7-LU
Processor & Memory	2 X Quad Core Intel® Xeon® Processors at 2.4 GHz 12 GB
Hard Disk Drive	6 X 750 GB SATA
Network Interface	4 X 10/100/1000 Base-T (on board)
Power Supply	Dual redundant 570 W
Form Factor	2U rack-mountable chassis

SIEM Flow Anomaly Processor

Model	DSIMBA7-FAP / DSIMBA7-FAP-HA
Rated Throughput	1,200,000 Max FPM (Unidirectional) 600,000 Max FPM (Bidirectional)
Connects to	SIEM Base Appliance DSIMBA7-LU DSIMBA7-FAP is compatible with
Processor & Memory	2 X Quad Core Intel® Xeon® Processors at 2.4 GHz 12 GB
Hard Disk Drive	6 X 750 GB SATA
Network Interface	4 X 10/100/1000 Base-T (on board)
Power Supply	Dual redundant 570 W
Form Factor	2U rack-mountable chassis

*Specifications refer to Enterasys appliance revision 6A or higher unless otherwise noted. Enterasys reserves the right to substitute alternative hardware that meets or exceeds the specifications in this datasheet.

SIEM Console Appliance

Model	DSIMBA7-CON/DSIMBA7-CON-HA
Maximum # Flows per minute (FPM)	N/A; Flow Anomaly Processor (DSIMBA7-FAP) required
Maximum # Events Per Second (EPS)	N/A; Event Processor (DSIMBA7-EVP) required
Processor & Memory	2 X Quad Core Intel® Xeon® Processors at 2.4 Ghz
Hard Disk Drive	6 X 750 GB SATA
Network Interfaces	4 X 10/100/1000 Base-T (on board)
Power Supply	Dual redundant 570 W
Form Factor	2U rack-mountable chassis

SIEM Network Behavioral Flow Sensor Appliances

Model	DSNBA7-50-TX** / DSNBA7-50-TX-HA**	DSNBA7-250-TX / DSNBA7-250-TX-HA	DSNBA7-250-SX / DSNBA7-250-SX-HA	DSNBA7-1G-TX / DSNBA7-1G-TX-HA	DSNBA7-1G-SX / DSNBA7-1G-SX-HA
Rated Throughput	50 Mbps	250 Mbps	250 Mbps	1 Gbps	1 Gbps
Connects to	SIEM Base Appliance DSIMBA7-LU SIEM Flow Anomaly Processor DSIMBA7-FAP				
Processor	Quad Core Intel Xeon Processor at 2.4 GHz (X3220)	Quad Core Intel Xeon Processor at 2.4 GHz (E5530)			
Memory	1 GB	6 GB	6 GB	6 GB	6 GB
Hard Disk Drive	160 GB SATA	2 x 80GB SATA			
Network Interface	2 X 10/100/1000 Base-T (on-board) - available in TX only	4 X 10/100/1000 Base-T (on board)	4 X 10/100/1000 Base-T (on board) One 2 X 1000 Base-SX	4 X 10/100/1000 Base-T (on board) One 4 X 10/100/1000 Base-T	4 X 10/100/1000 Base-T (on board) One 4 X 1000 Base-SX
Power Supply	Dual redundant 110 V / 220 V auto-sensing	90-264 VAC, autoranging, 47-63 Hz, 570 W			
Form Factor	1U rack-mountable chassis				

**Revision 5x appliances

Environmental Specifications

- Operating Temperature: 10° C to 35° C (50° F to 95° F)
- Storage Temperature: -40° C to 65° C (-40° F to 149° F)
- Operating Relative Humidity: 20% to 80% non-condensing
- Storage Relative Humidity: 5% to 95% non-condensing
- Maximum Humidity Gradient: 10% per hour, operational and non-operational
- Operating Altitude: -16 m to 3,048 m (-50 ft to 10,000 ft)
- Storage Altitude: -16 m to 10,600 m (-50 ft to 35,000 ft)

Agency and Regulatory Standard Specifications

- Safety: UL 60950-1, CSA 22.1 60950, EN 60950-1, and IEC 60950-1, NOM
- EMC: FCC Part 15 (Class A), ICES-003 (Class A), BSMI, KCC, VCCI V-3, AS/NZS CISPR 22 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, EN 61000-3-3

SIEM Virtual Flow Collector System Requirements

(VFlow Collector 7.6.3.1)

- VMware ESXi 4.0
- VMware Infrastructure Client installed on the desktop system (VMware server applications are bundled with client software)
- VMware host requires 512 MB of free memory
- VMware host requires 36 GB of free disk space
- Enterasys SIEM Console version 7.6.3.1

Ordering Information

Ordering information for SIEM Appliances

Part Number	Description
SIEM Base Unit	
DSIMBA7-LU	SIEM Appliance for large enterprise deployments
DSIMBA7-SE	SIEM Appliance for small enterprise deployments, with integrated Behavioral Flow Sensor
SIEM Event & Flow Processor	
DSIMBA7-EVP	Event Processor
DSIMBA7-FAP	Flow Anomaly Processor
SIEM Virtual Flow Collector	
DSIMBS7-VFLOW	Virtual Flow Collector
SIEM Network Behavior Flow Sensor	
DSNBA7-50-TX	Behavioral Flow Sensor with 50Mbps rated throughput (copper interfaces)
DSNBA7-250-TX	Behavioral Flow Sensor with 250Mbps rated throughput (copper interfaces)
DSNBA7-250-SX	Behavioral Flow Sensor with 250Mbps rated throughput (fiber interfaces)
DSNBA7-1G-TX	Behavioral Flow Sensor with 1Gbps rated throughput (copper interfaces)
DSNBA7-1G-SX	Behavioral Flow Sensor with 1Gbps rated throughput (fiber interfaces)
SIEM Console Manager	
DSIMBA7-CON	SIEM Console Manager (Requires Event Processor and/or Flow Processor)
SIEM Additional Log Sources	
DSIMBA7-DEV	SIEM Additional 1 Log Source
DSIMBA7-DEV-50	SIEM Additional 50 Log Sources
DSIMBA7-DEV-500	SIEM Additional 500 Log Sources
DSIMBA7-DEV-1K	SIEM Additional 1K Log Sources
DSIMBA7-DEV-5K	SIEM Additional 5K Log Sources
DSIMBA7-DEV-10K	SIEM Additional 10K Log Sources
SIEM High Availability	
DSIMBA7-LU-HA	SIEM high availability for DSIMBA7-LU
DSIMBA7-SE-HA	SIEM high availability for DSIMBA7-SE
DSIMBA7-EVP-HA	SIEM high availability for DSIMBA7-EVP
DSIMBA7-FAP-HA	SIEM high availability for DSIMBA7-FAP
DSNBA7-50-TX-HA	SIEM high availability for DSNBA7-50-TX
DSNBA7-250-TX-HA	SIEM high availability for DSNBA7-250-TX
DSNBA7-250-SX-HA	SIEM high availability for DSNBA7-250-SX
DSNBA7-1G-TX-HA	SIEM high availability for DSNBA7-1G-TX
DSNBA7-1G-SX-HA	SIEM high availability for DSNBA7-1G-SX
DSIMBA7-CON-HA	SIEM high availability for DSIMBA7-CON
Upgrades	
DSLUS7-UP	Add additional Flow and Event processing to the DSIMBA7-LU SIEM Base Appliance
DSES7-UP	Add additional Flow processing to the DSIMBA7-SE Base Appliance
DSEVPS7-UP	Add additional event processing to DSIMBA7-EVP Appliance
DSFAPS7-UP	Add additional flow processing to DSIMBA7-FAP Appliance

Warranty

As a customer-centric company, Enterasys is committed to providing quality products and solutions. In the event that one of our products fails due to a defect, we have developed a comprehensive warranty that protects you and provides a simple way to get your products repaired or media replaced as soon as possible.

Enterasys SIEM comes with a one-year warranty against manufacturing defects. For full warranty terms and conditions please go to:

www.enterasys.com/support/warranty.aspx.

Service and Support

Enterasys Networks provides comprehensive service offerings that range from Professional Services to design, deploy and optimize customer networks, customized technical training, to service and support tailored to individual customer needs. Please contact your Enterasys account executive for more information about Enterasys Service and Support.

Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or **+1-978-684-1000** and visit us on the Web at enterasys.com



Thought Leadership
Patented Innovation

© 2010 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications. Please visit <http://www.enterasys.com/company/trademarks.aspx> for trademark information.

