

# 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

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

The Enterasys SIEM solution portfolio is appliance, based for quick and easy setup. Available hardware components include:

- SIEM Appliance
- Flow Anomaly Processor
- Event Processor
- Behavioral Flow Sensors

## Features

### SIEM Appliances

Enterasys SIEM 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.

Two models are available. The SIEM 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 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 [www.enterasys.com](http://www.enterasys.com).

### Technical Specifications

Technical Specifications for SIEM Appliance Large Enterprise (model DSIMBA7-LU) and SIEM Appliance Small Enterprise (model DSIMBA7-SE) are shown in the table 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 Appliances

Model	DSIMBA7-LU	DSIMBA7-SE
<b>Application</b>	High-performance, scalable Security Information and Event Management	All-in-one Security Information and Event Management
<b>Event Management, Vulnerability Management, and Directed Remediation</b>	Yes	Yes
<b>Expansion Options</b>	Software License Upgrades External Flow Anomaly Processors External Event Processors	The DSIMBA7-SE appliance is designed specifically for smaller enterprise and departmental deployments
<b>Behavioral Flow Sensor</b>	Uses external Behavioral Flow Sensors	Integrated Behavioral Flow Sensor
<b>Maximum # Flows Per Minute (FPM)</b>	400,000 FPM (Unidirectional) 200,000 FPM (Bidirectional)	100,000 FPM (Unidirectional) 50,000 FPM (Bidirectional)
<b>Maximum # Events Per Second (EPS)</b>	5,000/sec	1,000/sec
<b>Processor &amp; Memory</b>	2 x Quad Core Intel® Xeon® Processors at 2.33 GHz 8 GB	2 x Quad Core Intel® Xeon® Processors at 2.33 GHz 8 GB
<b>Hard Disk Drive</b>	6 x 750 GB SATA	6 x 500 GB SATA
<b>Network Interfaces</b>	2 x 10/100/1000 Base-T	1 x 10/100/1000 Base-T for management 3 x 10/100/1000 Base-T for monitoring
<b>Power Supply</b>	Dual redundant 110 V / 220 V auto-sensing	Dual redundant 110 V / 220 V auto-sensing
<b>Form Factor</b>	2U rack-mountable chassis	2U rack-mountable chassis

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 Event Processor

Model	DSIMBA7-EVP
Rated Throughput	5,000 events / second base configuration 10,000 event / second maximum
Connects to	SIEM Appliance DSIMBA7-LU
Processor & Memory	2 x Quad Core Intel® Xeon® Processors at 2.33 GHz 8 GB
Hard Disk Drive	6 x 750 GB SATA
Network Interface	2 x 10/100/1000 Base-T
Power Supply	Dual redundant 110 V / 220 V auto-sensing
Form Factor	2U rack-mountable chassis

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), and a single DSIMBA7-LU appliance supports one or two Flow Anomaly Processors.

## SIEM Flow Anomaly Processor

Model	DSIMBA7-FAP
Rated Throughput	1,200,000 Max FPM (Unidirectional) 600,000 Max FPM (Bidirectional)
Connects to	SIEM Appliance DSIMBA7-LU SIEM Behavioral Flow Sensors DSNBA7-xxx-xx
Processor & Memory	2 x Quad Core Intel® Xeon® Processors at 2.33 GHz 8 GB
Hard Disk Drive	6 x 750 GB SATA
Network Interface	2 x 10/100/1000 Base-T
Power Supply	Dual redundant 110 V / 220 V auto-sensing
Form Factor	2U rack-mountable chassis

## SIEM 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 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 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. Behavioral Flow Sensors interface with the Enterasys SIEM Appliances or the SIEM Flow Anomaly Processor.

## SIEM Behavioral Flow Sensor Appliances

Model	DSNBA7-50-TX	DSNBA7-250-TX	DSNBA7-250-SX	DSNBA7-1G-TX	DSNBA7-1G-SX
<b>Rated Throughput</b>	50 Mbps	200 Mbps	200 Mbps	1 Gbps	1 Gbps
<b>Connects to</b>	SIEM Appliance DSIMBA7-LU SIEM Flow Anomaly Processor DSIMBA7-FAP				
<b>Processor</b>	Xeon 3065 Processor at 2.33 GHz	2 x Quad Core Intel® Xeon® Processors at 2.33 GHz			
<b>Memory</b>	1 GB	2 GB	2 GB	4 GB	4 GB
<b>Hard Disk Drive</b>	160 GB SATA	2 x 80GB SATA			
<b>Network Interface</b>	2 x 10/100/1000 Base-T (on-board) - available in TX only	1 x 10/100/1000 Base-T for management 3 x 10/100/1000 Base-T for monitoring	1 x 10/100/1000 Base-T for management 2 x 1000 Base-SX for monitoring	1 x 10/100/1000 Base-T for management 2 x 10/100/1000 Base-T for monitoring	1 x 10/100/1000 Base-T for management 2 x 1000 Base-SX for monitoring
<b>Power Supply</b>	Dual redundant 110 V / 220 V auto-sensing				
<b>Form Factor</b>	1U rack-mountable chassis				

## Specifications

Environmental and regulatory specifications for Enterasys SIEM DSIMB7-LU, DSIMBA7-SE, DSIMBA7-EVP, DSIMBA7-FAP, and DSNBA7 appliances are listed below.

### 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 Vibration: 0.26 G at 5 Hz to 350 Hz for 2 minutes
- Storage Vibration: 1.54 Grms Random Vibration at 10 Hz to 250 Hz for 15 minutes
- Operating Shock: 1 shock pulse of 41 G for up to 2 ms
- Storage Shock: 6 shock pulses of 71 G for up to 2 ms
- 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)

### Regulatory Specifications

- FCC (U.S. only) Class A
- ICES (Canada) Class A
- CE Mark (EN 55022 Class A, EN55024, EN61000-3-2, EN61000-3-3)
- VCCI (Japan) Class A
- BSMI (Taiwan) Class A
- C-Tick (Australia/New Zealand) Class A
- SABS (South Africa) Class A
- CCC (China) Class A
- MIC (Korea) Class A
- UL 60950-1
- CAN/CSA C22.2 No. 60950-1
- EN 60950-1
- IEC 60950-1

## Ordering Information

Ordering information for SIEM Appliances

Part Number	Description
DSIMBA7-LU	SIEM Appliance for large enterprise deployments
DSIMBA7-SE	SIEM for small enterprise deployments, with integrated Behavioral Flow Sensor
DSIMBA7-EVP	Event Processor
DSIMBA7-FAP	Flow Anomaly Processor
DSNBA7-50-TX	Behavioral Flow Sensor with 50 Mbps rated throughput
DSNBA7-250-TX	Behavioral Flow Sensor with 200 Mbps rated throughput
DSNBA7-250-SX	Behavioral Flow Sensor with 200 Mbps rated throughput and optical interfaces
DSNBA7-1G-TX	Behavioral Flow Sensor Appliance with 1 Gbps rated throughput
DSNBA7-1G-SX	Behavioral Flow Sensor with 1 Gbps rated throughput and optical interfaces

## 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](http://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](http://enterasys.com)



© 2009 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.

