

# Enterasys Dragon<sup>®</sup> Intrusion Detection and Prevention

A unique security solution that delivers comprehensive threat analysis, prevention and containment



Dragon<sup>®</sup> Intrusion Detection and Prevention is unique for its extensive range of detection capabilities, host-based and network-based implementations, portfolio of both IDS and IDS/IPS appliances, and seamless integration with Enterasys' Secure Networks<sup>™</sup> solutions. Dragon utilizes a state-of-the-art high-performance, multi-threaded architecture with virtual sensor technology that scales to protect even the largest enterprise networks.

Dragon Intrusion Detection and Prevention is a core component of Enterasys' Secure Networks<sup>™</sup> architecture. When deployed in combination with Dragon Security Command Console (DSCC) and NetSight<sup>®</sup> Automated Security Manager (ASM), it facilitates the automatic identification, location, isolation and remediation of security threats. Dragon IDS / IPS also integrates seamlessly with Enterasys Network Access Control (NAC) for post-connect monitoring of behavior once network access has been granted.

Dragon **Intrusion Detection** is unmatched in detecting and reporting security events, including external intrusions, network misuse, system exploits and virus propagations. It utilizes the industry's most sophisticated multi-method detection technologies by integrating vulnerability pattern matching, protocol analysis and anomaly based detection with specific support for VoIP environments. Application-based event detection detects non-signature-based attacks against commonly targeted applications such as HTTP, RPC and FTP.

Dragon's advanced **Intrusion Prevention** is designed to block attackers, mitigate denial of service attacks, prevent information theft, and ensure the security of VoIP communications - while remaining transparent to the network. Built upon Dragon's award-winning Intrusion Detection technology, Dragon IPS can alert on the attack, drop the offending packets, terminate the session for TCP and UDP based attacks, and dynamically establish firewall or Secure Networks<sup>™</sup> policy rules. Dragon's Network IPS leverages the thousands of vulnerability and exploit based signatures in Dragon's threat libraries.

## Benefits

### Protects you today and ready for next generation networks

- Protection against emerging Voice Over IP vulnerabilities, Day Zero threats and advanced Denial of Service attacks
- Over 6,000 pre-defined threat signatures with live signature updates plus support for the Snort<sup>™</sup> signature library
- Scales to meet the needs of the largest enterprise-class networks

### Industry Leading Intrusion Detection and Prevention

- Unmatched threat detection and reporting that leverages sophisticated signature, application, protocol, and behavioral technologies
- Unique host-based and network-based protection options with simultaneous support for both intrusion detection and prevention
- High performance sensors for wire-speed traffic inspection and rapid response to threats

### Leverages your existing infrastructure investments and IT expertise

- Ready to protect "out of the box" with a powerful configuration tools for customization and advanced control
- No fork lift upgrades – works with your existing network switches, routers, wireless access points, and security appliances
- Rapid deployment with management automation

Dragon sensors come ready to use “out of the box” and easily integrate with your existing network infrastructure and security appliances. Dragon Intrusion Defense ships with a comprehensive set of preinstalled signatures, Voice over IP protocol decoders for SIP and H.323 protocols, and advanced detection of malformed messages to help prevent Denial of Service attacks.

## Dragon Network Sensor

**Dragon Network Sensors** are IDS and IDS/IPS security appliances that offer market leading deep forensics capabilities, including flexible packet capture and complete session reconstruction. Dragon Network Sensors are centrally managed via Dragon Enterprise Management Server (EMS). Dragon EMS provides configuration management, status monitoring, live security updates and a secure encrypted communications channel.

Dragon Network Sensors utilize an adaptive match engine and multithreaded application execution to significantly enhance performance. Sensors support the use of multiple detection algorithms simultaneously, thereby optimizing traffic analysis to match the prevalent traffic type.

Security Administrators have broad flexibility in deploying Dragon Network Sensors. For example a single sensor may operate as multiple “virtual sensors”, each associated with a particular VLAN, Layer 3 network, physical Switch port or TCP / UDP level application. Each virtual sensor can be configured with unique policies that define the analysis techniques used and alerts generated.

Dragon Network Sensors are available at 100 Mbps, 250 Mbps, 500 Mbps and 1 Gbps deep packet inspection throughput rates. All models offer optional Failover and Fail Open redundancy.

- GIG Dragon Network Sensors are IDS or IDS/IPS appliances for high performance data centers. They support 1 Gbps data rates and include 2 x 10/100/1000 plus 4 x 1Gbps Fiber or 4 x 1Gbps Copper LAN interfaces.
- GE500 Dragon Network Sensors are IDS or IDS/IPS appliances for data centers. They support 500 Mbps data rates and include 2 x 10/100/1000 plus 2 x 1Gbps Fiber or 2 x 1Gbps Copper LAN interfaces.
- GE250 Dragon Network Sensors are IDS or IDS/IPS appliances for regional office and similar locations. They support 250 Mbps data rates and include 2 x 10/100/1000 plus 1 x 1Gbps Fiber or 1 x 1Gbps Copper LAN interfaces.
- FE Dragon Network Sensors are IDS or IDS/IPS appliances for branch office and similar locations. They support 100 Mbps data rates and include 2 x 10/100 plus 1 x 10/100/1000 LAN interfaces.

## Product Specifications

### Environmental Specifications

Operating Temperature: -10° C to +35° C (50° F to 95° F)  
Maximum temperature change not to exceed +10° C per hour)  
Non-operating temperature: -40° C to +70° C (-40° F to 158° F)

### Industry Certifications

Common Criteria EAL2 Certified  
Argentina: IRAM Certificate  
Australia/New Zealand: ACA/MED (FE100 only)  
Belarus: Bellis Certificate (FE100 only)  
Canada: UL 60950 – CSA 60950 (UL and cUL)  
China: CNCA (FE100 only), GB4943 (CCC certification)  
Europe / CE Mark: EN60950 (complies with 73/23/EEC)  
Germany: GS License  
International: IEC60950 (CB Report and Certificate)  
Nordic Countries: EMKO – TSE (74-SEC) 207/94 (excluding FE100)  
Russia GOST 50377-92  
US: UL60950 – CSA 60950 (UL and cUL)

### Electromagnetic Compatibility

US: FCC, Part 15  
Australia/New Zealand: AS/NZS 3548 (based on CISPR 22)  
Canada: ICES-003  
China: GB 9254 and GB 17625 (CCC certification)  
Europe/CE Mark: EN55022, EN55024 and EN61000 -3-2 -3-3 (complies with 89/336/EEC)  
International: CISPR 22  
Japan: VCCI  
Korea: RRL, MIC 1997-41 and 1997-42  
Russia: GOST 29216-91 and 50628-95  
Taiwan: CNS13438 (excluding FE100), BSMI RPC (FE 100 only)

### Power Consumption

4.96A at 115V, 2.48A at 220V

### Physical Dimensions

FE100 versions: 1U rack-mount for EIA standard 310-D racks, 4.32 cm (1.7”) H x 42.9 cm (16.9”) W x 67.2 cm (26.5”) D  
GE250 / GE500 / GIG versions: 1U rack-mount for EIA standard 310-D racks, 4.32 cm (1.7”) H x 42.9 cm (16.9”) W x 60.71cm (23.9”) D

## Dragon Host Sensor

**Dragon Host Sensors** are security applications used to detect attacks on network endpoints in real time. Host Intrusion Defense is particularly valuable in environments where AES, SSL, IPSec or other encryption schemes are deployed because the sensor analyzes the decrypted data. Dragon Host Sensors deploy advanced techniques to identify rootkits and buffer overflows via a kernel monitoring module. This module traps and analyzes all calls to the kernel to detect the existence of kernel level rootkits.

The optional Dragon Host Sensor Web Intrusion Prevention System module helps avert attacks on web servers running Microsoft IIS or Apache HTTP Servers - providing maximum protection while operating with minimal overhead on the system.

### System Requirements

Dragon Intrusion Defense Host Based Sensors support Microsoft® Windows 2000, Windows XP Professional, Windows Server 2003, Linux, AIX, Solaris, and HP-UX operating systems.

Web Intrusion Prevention supports WebIPS for Apache with Linux and Solaris servers, plus WebIPS for Microsoft IIS 5 and IIS 6 for Microsoft Windows 2000, Windows XP and Windows 2003 server.

## Dragon Enterprise Management Server

Dragon Enterprise Management Server (EMS) is the centralized configuration, monitoring and control application for Dragon Intrusion Defense. Dragon EMS utilizes a client-server architecture for effective enterprise-wide management of Dragon deployments. It uses group policy rules to simplify the configuration of network and host sensors. Dragon EMS Alarm Tool aggregates event reporting from individual network and host sensors. It can execute firewall rule changes, switch / router reconfigurations or other mitigation actions in response to attacks.

Dragon EMS provides in-depth reporting and archiving of security event and network activity. This information may be used for regulatory compliance, audit trail analysis, forensics and real-time trending. Dragon EMS seamlessly integrates with Dragon Security Command Console.

### System Requirements

Linux on Intel platforms: 2 GHz Pentium 4 processor, 2 GB RAM, 36 GB HDD space minimum, Intel based Network Interface Card

Solaris (ver 9 and 10) on Sparc platform: 1 GHz Sparc Processor, 2 GB RAM, 36 GB HDD space minimum, Broadcom or Intel based Network Interface Card

### Dragon Event Flow Processor

Dragon Event Flow Processor (EFP) is a security appliance used to scale Dragon Intrusion Defense deployments for very large networks. Event Flow Processors are strategically placed on the network to aggregate event data from multiple network and host sensors, and report to the centralized Dragon Enterprise Management Server. This is particularly useful for organizations with multiple high traffic remote sites.

## Ordering Information

### Dragon IDS / IPS Network Sensors

Part Number	Description
DSIPA7-GIG-TX	Dragon Network GIG IPS Appliance - includes two 2 port Copper Fail-safe bypass NICs
DSIPA7-GIG-SX	Dragon Network GIG IPS Appliance - includes two 2 port Fiber Fail-safe bypass NICs
DSIPA7-GE500-TX	Dragon Network GE500 IPS Appliance - includes 2 port Copper Fail-safe bypass NIC
DSIPA7-GE500-SX	Dragon Network GE500 IPS Appliance - includes 2 port Fiber Fail-safe bypass NIC
DSIPA7-GE250-TX	Dragon Network GE250 IPS Appliance - includes 2 port Copper Fail-safe bypass NIC
DSIPA7-GE250-SX	Dragon Network GE250 IPS Appliance - includes 2 port Fiber Fail-safe bypass NIC
DSIPA7-FE-TX	Dragon Network Intrusion Prevention Appliance - Fast Ethernet

### Dragon IDS Network Sensors

Part Number	Description
DSNSA7-GIG-TX	Dragon Gig Network Sensor Appliance (Copper NIC)
DSNSA7-GIG-SX	Dragon Gig Network Sensor Appliance (Fiber NIC)
DSNSA7-GE500-TX	Dragon GE500 Network Sensor Appliance (Copper NIC)
DSNSA7-GE500-SX	Dragon GE500 Network Sensor Appliance (Fiber NIC)
DSNSA7-GE250-TX	Dragon GE250 Network Sensor Appliance (Copper NIC)
DSNSA7-GE250-SX	Dragon GE250 Network Sensor Appliance (Fiber NIC)
DSNSA7-FE-TX	Dragon Network IDS Appliance, Fast Ethernet

## Dragon IDS Host Sensors

Part Number	Description
DSHSS7-100-LIC	Dragon Host Sensor Software License (100 pack)
DSHSS7-1-LIC	Dragon Host Sensor Software License (Single)
DSHSS7-25-LIC	Dragon Host Sensor Software License (25 pack)
DSHSS7-500-LIC	Dragon Host Sensor Software License (500 pack)
DSHSS7-WEBIPS	Dragon Host Sensor Software for Web IPS

## Dragon Enterprise Management Server

Part Number	Description
DSEMS7-SE	Dragon Enterprise Management Server Software - Small Enterprise, manages up to 2 nodes
DSEMS7-ME	Dragon Enterprise Management Server Software - Medium Enterprise, manages up to 25 nodes
DSEMS7-LE	Dragon Enterprise Management Server Software - Large Enterprise, manages up to 100 nodes
DSEMS7-U	Dragon Enterprise Management Server Software - Unlimited, manages unlimited nodes
DSEMA7-ME	Dragon Enterprise Management Server Appliance - Medium Enterprise, manages up to 25 nodes
DSEMA7-LE	Dragon Enterprise Management Server Appliance - Unlimited managed nodes
DSEMA7-U	Dragon Network IDS Appliance, Fast Ethernet
DSEPA7	Dragon Event Flow Processor Appliance
DSISA7-TX	Integrated Network Sensor/Server (Copper NIC), 250Mbps, contains management server for up to 2 nodes
DSISA7-SX	Integrated Network Sensor/Server (Fiber NIC), 250Mbps, contains management server for up to 2 nodes

## Warranty

As a customer-centric company, Enterasys is committed to providing the best possible workmanship and design in our product set. In the event that one of our products fails due to a defect in one of these factors, we have developed a comprehensive warranty that protects you and provides a simple way to get your products repaired as soon as possible.

## Service and Support

Enterasys understands that superior service and support is a critical component of Secure Networks™. The Enterasys SupportNet Portfolio—a suite of innovative and flexible service and support offerings—completes the Enterasys solution. SupportNet offers all the post-implementation support services you need—online, onsite, or over the phone—to maintain your network availability and performance.

## 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)



© 2007 Enterasys Networks, Inc. All rights reserved. Enterasys is a registered trademark. Secure Networks is a trademark of Enterasys Networks. All other products or services referenced herein are identified by the trademarks or service marks of their respective companies or organizations. NOTE: Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications.

000000 8/07



Delivering on our promises. On-time. On-budget.