

Enterasys Dragon® Intrusion Detection and Prevention

Ensures confidentiality, integrity and availability of business critical resources

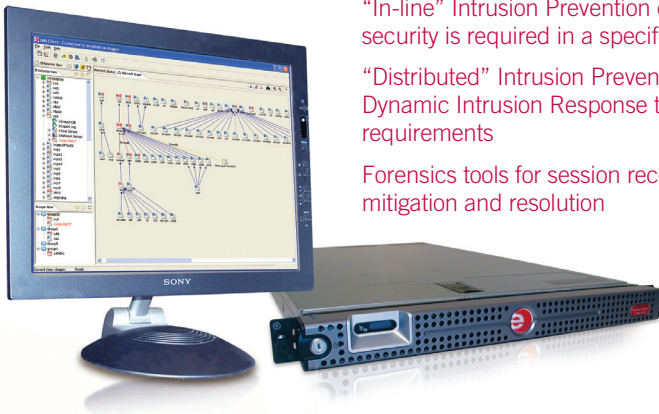
Threat containment that leverages existing network investments

“Out-of-Band” Intrusion Detection deployment that simultaneously utilizes multiple technologies

“In-line” Intrusion Prevention deployment when advanced security is required in a specific location

“Distributed” Intrusion Prevention deployment through Dynamic Intrusion Response to address real-world requirements

Forensics tools for session reconstruction simplify threat mitigation and resolution



Product Overview

Enterasys Dragon® Intrusion Detection, Prevention & Response is unique for its ability to gather evidence of an attacker's activity, remove the attacker's access to the network, undo the damage, and reconfigure the network to resist the attacker's penetration technique. Put simply, Dragon stops attacks at the source of the threat and can proactively protect against future threats and vulnerabilities. Dragon offers an extensive range of detection capabilities, host-based and network-based deployment options, portfolio of IDS/IPS appliances, and seamless integration with the Enterasys Secure Networks™ architecture. 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, Prevention & Response is a core component of the Enterasys' Secure Networks architecture. When deployed in combination with Dragon Security Command Console (DSCC) and NetSight® 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 “out-of-band” **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 “in-line” **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™ policy rules. Dragon's Network IPS leverages the thousands of vulnerability and exploit based signatures in Dragon's threat libraries.

Benefits

Extends IPS protection to Network Edge

- Protect networked resources by removing an attacker's ability to continue an attack or to mount a new attack
- Real-time dynamic attacker containment limits security incident impact
- Works with multi-vendor enterprise edge switching products

Protects Today's and Tomorrow's Next Generation Networks

- Protection against emerging Voice Over IP vulnerabilities, Day Zero threats and advanced Denial of Service attacks
- Library of over 14,000 threat signatures including live signature updates and support for Snort™ signature databases

Industry Leading Intrusion Detection, Prevention & Response

- Unmatched threat detection and containment that leverages sophisticated signature, application, protocol, and behavioral analysis
- Unique host-based and network-based protection deployment options

Leverages your existing infrastructure investments and IT expertise

- Ready to protect “out of the box” with 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

There is nothing more important than our customers.

Dragon's "distributed" **Intrusion Response** threat containment can block attackers at the source physical port for most multi-vendor edge switches. More granular business-oriented visibility and control based on user and application policy is provided when Enterasys Matrix®, SecureStack™ or SecureSwitch™ products are deployed at the network edge. Effective threat containment requires the removal of the attacker's ability to continue the attack or to mount a new attack. The Enterasys Dynamic Intrusion Response (DIR) solution identifies a threat or security event, locates the exact physical source of the event, and mitigates the threat through the use of enforceable bandwidth rate limiting policies, quarantine policies, or other port level controls.

Dragon sensors come ready to use "out of the box" and easily integrate with your existing network infrastructure and security appliances. Dragon 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 Sensors are 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 the 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 integrate with the Access Edge Intrusion Prevention option (see below for details) which extends Intrusion Prevention and threat isolation to the edge of your network or source of the attack.

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. In addition the Dragon 10Gbps IDS/IPS system scales for high performance networks. The system features distributed fault tolerance with no single point of failure for high reliability and address critical business requirements while protecting existing infrastructure investments.

- GIG Dragon Network Sensors are IDS/IPS appliances for high performance data centers. They support 1 Gbps data rates and include 2 onboard ports plus 2 dual-port fiber or 2 dual-port 10/100/1000 copper LAN interfaces.

- GE500 Dragon Network Sensors are IDS/IPS appliances for data centers. They support 500 Mbps data rates and include 2 onboard ports plus 1 dual-port fiber or 1 dual-port 10/100/1000 copper LAN interfaces.
- GE250 Dragon Network Sensors are IDS/IPS appliances for regional office and similar locations. They support 250 Mbps data rates and include 2 onboard ports plus 1 dual-port fiber or 1 dual-port 10/100/1000 copper LAN interfaces.
- FE Dragon Network Sensors are IDS/IPS appliances for branch office and similar locations. They support 100 Mbps data rates and include 2 onboard ports plus 1 dual-port 10/100/1000 copper LAN interface.

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.

Dragon Enterprise Management Server (EMS) is the centralized configuration, monitoring, and control application for Dragon Intrusion Detection & Prevention. 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.

Dragon Event Flow Processor

Dragon Event Flow Processor (EFP) is a security appliance used to scale Dragon Intrusion Detection, Prevention & Response 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.

Specifications

Dragon IDS/IPS 1U Appliances

Chassis

Form Factor: 1U Rack
Height: 1.68" (4.27 cm)
Width: 17.60" (44.70 cm)
Depth: 21.50" (54.61 cm)
Weight: ~ 26.0 lbs. (11.80kg)

Power

Single power supply (345W)

Environmental

Operating Temperature: 10° to 35°C (50° to 95°F)
Operating Relative Humidity: 20% to 80% (noncondensing) with a maximum humidity gradation of 10% per hour
Operating Maximum Vibration: 0.25 G's 0-Peak, 3-200 HZ sweep @ 1/2 Octaves/minute
Operating Maximum Shock: 31G, 2.6ms, 20inch/sec, bottom side
Operating Altitude: -16 to 3048 m (-50 to 10,000 ft.)
Storage Temperature: -40° to 65°C (-40° to 149°F)
Storage Relative Humidity: 5% to 95% (noncondensing)
Storage Maximum Vibration: 1.54 GRMS - 6 sides @ 15 min/side
Storage Maximum Shock: 71G, 2ms, 35inch/sec, 6 sides; 32G, 2ms, 270inch/sec, 6 sides
Storage Altitude: -16 to 10,600 m (-50 to 35,000 ft.)

Regulatory

FCC Part 15 Class A
EN61000-3-2, A1, A2: Current Harmonics
EN61000-3-3: Voltage Flicker
EN55022: 1998 and CISPR 22: 1997 Class A
VCCI Class 1
MIC Class A
BSMI
EN55024: 1998 and CISPR 24: 1997
IEC 61000-4-2: Electrostatic Discharge specification
IEC 61000-4-3: Radiated Immunity
IEC 61000-4-4: EFT/Bursts Immunity
IEC 61000-4-5: Surge Immunity
IEC 61000-4-6: Conducted Immunity 0.15-80MHz
IEC 61000-4-8: Power Frequency H-Field
IEC 61000-4-11: Voltage Dips/Interrupts/Variations
EN60950-1, First Edition: Standard for Information Technology Equipment - Safety-Part 1: General Requirements
IEC 60950-1, First Edition (2001)
UL/CSA 60950-1, First Edition: Standard for Information Technology Equipment -Safety-Part 1: General Requirements
EK1-ITB 2000:2003 : Ergonomics
ISO 9241 : VDT Ergonomic Requirements
ZH1/618:GS-VW-SG7:1997 :Ergonomics
ISO 13406-2 : Ergonomic requirements for work with visual displays based on flat panels
ISO 7779 : Sound Pressure at Operator Position (Acoustics)
MsanPiN 001-96: Interstate Sanitary rules and norms (Acoustics)

Dragon IDS/IPS 2U Appliances

Chassis

Form Factor: 2U Rack
Height: 3.4" (8.64cm)
Width: 17.5" (44.43cm)
Depth: 29.31" (74.4cm)
Weight: 50.71 lbs (23 Kg), maximum configuration

Power

Dual power supplies (750W)

Environmental

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 (non-condensing twmax=29C): 20% to 80% non-condensing
Maximum humidity gradient: 10% per hour, operational and non-operational conditions.
Storage Relative Humidity: 5% to 95% non-condensing (twmax=38C)
Operating Vibration: 0.26G at 5Hz to 350Hz for 2 minutes
Storage Vibration: 1.54Grms Random Vibration at 10Hz to 250Hz for 15 minutes
Operating Shock: 1 shock pulse of 41G for up to 2ms
Storage Shock: 6 shock pulses of 71G for up to 2ms
Operating Altitude: -16 to 3,048m (-50 ft to 10,000 ft) Storage Altitude: -16m to 10,600m (-50 ft to 35,000 ft)

Regulatory

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

Dragon EMS Appliance with dual power

Chassis

Form Factor: 1U Rack
Height: 1.67" (4.26cm)
Width: 16.7" (42.6cm)
Depth: 30.4" (77.2cm)
Weight: 35.8 lbs (16.3 Kg), maximum configuration

Power

Dual power supplies (670W)

Environmental

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 (non-condensing twmax=29C): 20% to 80% non-condensing

Maximum humidity gradient: 10% per hour, operational and non-operational conditions.

Storage Relative Humidity: 5% to 95% non-condensing (twmax=38C)

Operating Vibration: 0.26G at 5Hz to 350Hz for 2 minutes

Storage Vibration: 1.54Grms Random Vibration at 10Hz to 250Hz for 15 minutes

Operating Shock: 1 shock pulse of 41G for up to 2ms

Storage Shock: 6 shock pulses of 71G for up to 2ms

Operating Altitude: -16 to 3,048m (-50 ft to 10,000 ft)

Storage Altitude: -16m to 10,600m (-50 ft to 35,000 ft)

Regulatory

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

Dragon IDS / IPS Network Sensors

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

Dragon IDS Network Sensors

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

Dragon Host Sensor

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 servers.

Dragon Enterprise Management Server

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 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
DEMA-ME	Dragon Enterprise Management Server Appliance - Medium Enterprise, manages up to 25 nodes
DEMA-LE	Dragon Enterprise Management Server Appliance - Large Enterprise, manages up to 100 nodes
DEMA-U	Dragon Enterprise Management Server Appliance - Unlimited managed nodes
DEPA	Dragon Event Flow Processor Appliance
DISA-TX	Integrated Network Sensor/Server (Copper NIC), 250Mbps, contains management server for up to 2 nodes
DISA-SX	Integrated Network Sensor/Server (Fiber NIC), 250Mbps, contains management server for up to 2 nodes

Dynamic Intrusion Response

Part Number	Description
NS-AB-50	NetSight Advanced Bundle 50-devices (50 device Console license for 1 server plus 3 concurrent users with Policy Manager, Policy Control Console, Automated Security Manager, Inventory Manager, and NAC Manager)
NS-AB-50FT	NetSight Advanced Bundle 50-devices FT (50 device Console license for 1 server plus 3 concurrent users, Policy Manager, Policy Control Console, Automated Security Manager, Inventory Manager, NAC Manager, a redundant NetSight license for fault tolerance (manual failover), Includes Lab License)
NS-AB-U	NetSight Advanced Bundle Unrestricted (Unrestricted device Console license for 1 server plus 25 concurrent users with Policy Manager, Policy Control Console, Automated Security Manager, Inventory Manager, and NAC Manager)
NS-AB-UFT	NetSight Advanced Bundle Unrestricted FT (Unrestricted device Console license for 1 server plus 25 concurrent users, Policy Manager, Policy Control Console, Automated Security Manager, Inventory Manager, and NAC Manager, a redundant NetSight license for fault tolerance (manual failover), includes Lab License)

Warranty

Dragon comes with a one year hardware warranty. There is also a 90-day software and firmware warranty to cover patches, bug fixes, and feature upgrades with 8 x 5 telephone support. For full warranty terms and conditions please go to <http://www.enterasys.com/support/warranty.aspx>. 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 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



© 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.

