DRAGON INTRUSION DETECTION SYSTEM

Total Security for Your Network Infrastructure

Take advantage of Dragon’s flexible, scalable, sophisticated — and cost-effective — intrusion detection systems.

Security and Intrusion Detection for Enterprise Networks

The Internet provides new and exciting opportunities to develop an additional channel for the delivery of products and services. The new global economy, with the Internet as an open network, allows organizations to transcend borders.

At the same time, however, it makes it difficult to ensure that an organization’s most valuable asset—information—is protected, increasing the likelihood that an organization may be a victim of fraud, e-mail eavesdropping, data theft or the intentional corruption of files by unauthorized employees.

That’s where Dragon comes in.

The Dragon Intrusion Detection System is an integral component of Enterasys Networks’ Secure Harbour™ architecture, the industry’s first holistic security architecture for complex enterprise networks. Secure Harbour encompasses a complete range of security solutions designed to “protect and serve” the corporate information ecosystem.

The award-winning Dragon line of intrusion detection products—Dragon Sensor, Dragon Squire and Dragon Server—monitor network, server and firewall activity for signs of suspicious and malicious activity, and offer comprehensive features that bring improved security to your enterprise network.

- Collects forensic data
  - Performs detailed attack analysis to assess the impact of hacker activity
  - Provides time-stamped, chronologically organized data that can be used in court

- Client/server architecture
  - Allows a large number of engines to be controlled from a single server
  - Lowers deployment costs with the use of a single console system

- Powerful, patent-pending, signature format
  - "Out of the box" functionality allows for customization of NIDS and HIDS signatures
  - More than 1,000 updated attack signatures notes; real-time updates of new threats

- Advanced security monitoring
  - Networks can be customized quickly thanks to a scalable signature library
  - Secure shell/secure web access operates from anywhere on the Internet
  - Maximizes productivity while allowing problems to be diagnosed remotely

- Integrated management tools
  - Detects unauthorized network services while allowing customers to quickly secure their network from hackers
  - Detects subtle events while maintaining low false-positive rates
**Dragon Sensor**

**Dragon Sensor** monitors live network packets and looks for signs of computer crime, network attacks, network misuse and anomalies. When it observes an event, the Dragon Sensor can send pages and e-mail messages, and then take action to stop the event and record it for future forensic analysis. Typically, Dragon Sensors are deployed on standalone systems in front of firewalls or at key network choke points.

For signature selection, Dragon administrators can choose from over 1200 signatures located at our support site. Signatures are added weekly and sometimes daily. All Dragon events are categorized into suspicious, probe, attack, compromise, success, failure, virus, collection and maintenance groups. While other NIDS concentrate on attack and probe detection, the Dragon Sensor can usually collect enough evidence to indicate if an attack has succeeded or failed. These groupings are key to reducing false positives and presenting a holistic picture of collected event data.

The performance and efficiency of a Dragon Sensor is such that a dual Pentium III 700 Mhz class computer running Linux can observe network attacks on a 225 Mbps Gigabit Ethernet link. Of course exact performance depends on the signature load, packet size and system hardware, but customers routinely deploy their Dragon Sensors on links faster than 100 Mbps.

Network monitoring can be accomplished through any network interface and does not require the use of a network IP stack. For management, Dragon Sensors have no open ports, which also makes them impenetrable to insider attacks.

- Provides 100 Mbps functionality
- Easy-to-use web GUI with command-line interface
- More than 1,000 easy-to-write signatures
- Offers SNMP and e-mail alerts
- Also available in 2U appliance

**Dragon Sensor Products**

- **Dragon Sensor.** The Dragon Sensor is downloadable. Customers supply their own hardware, harden the boxes to remove security problems and then install the Dragon Sensor software.

- **Dragon Sensor Appliance.** Enterasys offers the Dragon Sensor as an appliance. This system supports dual Pentium III 700 Mhz Intel CPUs, 128MB of memory, a 9 Gb SCSI drive, two 100 Mbps Ethernet cards in a 2U Intel appliance. The system is configured with the FreeBSD operating system and a kernel modified with performance enhancements.

- **Dragon Sensor Workbench.** The Dragon Sensor Workbench is a software product that operates against static network log files instead of a live network feed. Sources of these files may include TCPDUMP or SNOOP (a Solaris-based sniffer). Configuration is identical to Dragon Sensor and operation is controlled from the command line. Analysis may be performed with any of Enterasys’ command line tools or web interfaces.

**Dragon Squire**

**Dragon Squire** is a host-based intrusion detection and firewall monitoring system that looks at system logs for evidence of malicious or suspicious application activity, and monitors key system files for evidence of tampering in real time. Dragon Squire has been tuned to prevent high load levels and minimize any negative system impact to a server’s performance. Besides being an excellent system security tool, Dragon Squire can also analyze firewall logs, router events and just about anything that can speak SNMP or SYSLOG.

Dragon Squire’s signature library includes suspicious events from a wide variety of operating systems. These events check for suspicious file transfers, denied login attempts, physical messages (like an Ethernet interface
set to promiscuous mode) and system reboots. The library also includes security messages from many applications and services such as Secure Shell, Sendmail, Qmail, Bind and Apache Web servers.

Dragon Squire is an excellent complement to the Dragon Sensor network IDS. There are many network attacks (such as web attacks sent over an SSL connection) which the Dragon Sensor (or any other NIDS) cannot observe. Correlating these host and network events (along with firewall information) is accomplished at the Dragon Server.

- Provides log analysis and file integrity checking
- An enterprise console
- Offers low-server overhead
- Uses flexible signature language

**Dragon Server**

Designed to provide engine management, event alerting, analysis and correlation, **Dragon Server** facilitates secure management of all Dragon Sensors and Dragon Squires. It also aggregates all alerts into one central database so that disparate attack information can be correlated. The Dragon Server includes a variety of reporting and analysis tools as well as the ability to customize alerts via e-mail, SNMP or SYSLOG messages.

- Operates Dragon Sensor and Dragon Squire engines
- Correlates events from multiple engines
- SNMP trap server accepts firewall alerts
- Provides 3D/2D visualization
- Offers live signature updates
- Web-based management interface

**Dragon Server: Web Interfaces** The Dragon Server includes three web-based analysis tools that provide unique views of collected event data. These views are real time, forensic and trending in nature. They support all phases of IDS operation and support events from Dragon Sensor and Dragon Squire, which also includes firewall events.

**Dragon Console.** The real-time web tool is named “Dragon Console.” This tool consists of a program which holds up to 1,000,000 events in memory and a set of Perl and Java programs which analyze the data in memory to produce graphs, score attacks and organize events by group. The tool is available to customers today, but more advanced 2D and 3D visualization applets are under development and will be available in the near future. The tool also supports a ‘shell’ which Dragon administrators can connect to and generate data from the command line.

**Dragon Fire.** Dragon Fire is a web interface tool which analyzes collected events with a variety of different reporting functions. Events can be categorized via groups, by IP address, by CIDR block, by time and by the success or failure of an event. Other tools within Dragon Fire allow for session reconstruction, scoring of each IP address by a heuristic which identifies suspicious anomalies and false positives, analysis of suspicious ICMP traffic payloads and reporting events by time distribution.

**Sorcerer.** Sorcerer is the long-term trending tool which stores all event information. It can answer questions about how often certain attacks occur, if a certain IP address has probed your networks before and which combination of attacks have occurred on similar days.
DRAGON SENSOR OPERATING SYSTEMS
Linux
OpenBSD
Free BSD
Solaris x86
Solaris Sparc
HP-UX

NETWORK INTERFACES
Gigabit Ethernet
ATM 100Base-T
10Base-T
Token Ring
FDDI

DRAGON SQUIRE OPERATING SYSTEMS
Linux
OpenBSD
Free BSD
Solaris x86
Solaris Sparc
HP-UX
Windows NT 4.0
Windows 2000

COMMERCIAL FIREWALL SUPPORT
CheckPoint/Nokia
Cisco PIX
Raptor
NetScreen

OPEN SOURCE FIREWALL SUPPORT
Ipfilter
Ipchains

ORDERING INFORMATION
DS001
Dragon Sensor Software
DS002
Dragon Workbench Software
DS003
Dragon Sensor Appliance
DS004
Dragon Server Software
DS005
Dragon Squire Software
DS006
Dragon Server Appliance

Dragon is a trademark or registered trademark of Enterasys Networks, a Cabletron Systems Company. All other products or services mentioned 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. © Enterasys Networks, Inc. All rights reserved.