

ENTERASYS NETWORKS ANNOUNCES NEW RELEASE OF AWARD-WINNING DRAGON INTRUSION DETECTION SYSTEM

Submitted by: MCC International Ltd

Monday, 22 October 2001

Dragon 5 Provides Intrusion Detection Across The Entire Enterprise, From Firewall To Web Server, Reducing The Threat Of Hackers, Worms And Cyber Crime

October 22, 2001 – Continuing its commitment to network security, Enterasys Networks Inc., a leader in secure, available, and mobile enterprise networking solutions, announced the latest version of its award-winning Dragon Intrusion Detection System (IDS) line with a new release. Dragon 5 introduces more scalability, availability, and flexibility into its underlying architecture to enhance the security of enterprise networks. By working closely with its managed security service providers and customers, Enterasys designed an architecture ideal for today's large-scale IDS implementations.

“Since its introduction, users have benefited from Dragon's flexibility by customising the monitoring of their complex network applications, as well as Dragon's ability to monitor at 100 Megabit and Gigabit speeds,” said Ron Gula, vice president of Intrusion Detection Systems at Enterasys Networks. “Through working closely with our managed security service provider partners, we have developed a unique architecture for Dragon 5 that can scale to several hundred monitored networks and nodes, making it ideal for large enterprises and MSPs.”

Dragon leverages its leading architecture to provide customers the most complete enterprise-wide intrusion detection capability on the market. The Dragon product line not only provides integrated network and host-based intrusion detection, (Dragon Sensor and Dragon Squire) but extends the detection boundary through its capability of monitoring firewalls, routers, and third party intrusion detection systems. In addition, Dragon (Squire) provides leading detection capability of attacks against commonly targeted applications such as mail servers, FTP servers, and web servers. This capability allowed Dragon customers to detect and protect against the recent Code-red and NIMDA worms.

“With Dragon, Enterasys has an intrusion detection system capable of meeting the security monitoring needs of large corporations with high-bandwidth networks while simultaneously providing a centralized and scalable product for the rapidly expanding MSSP (managed security solution provider) market. While ambitious, such a strategy means that Enterasys can gain from the growth of security monitoring solutions in both the insourced and outsourced models. The future release of a medium-end IDS product will increase the size of Enterasys' target client audience significantly, and should allow them to become an increasingly important player in the IDS market,” said Ian Williams, eSecurity analyst at Datamonitor.

Most recently, Dragon's integrated host and network-based approach enabled customers to detect and

respond to the recent Code-Red and NIMDA worms. Via Dragon Sensor, these worms were detected as they travelled across the network in search of the next victim host. When attacking a host, Dragon Squire was able to detect and record the results of the attack. When correlated in Dragon Server, customers were able to identify targeted and infected hosts on their network, allowing them to determine which systems had been compromised and which had not been affected. This provided the critical information required in organising their incident response process, resulting in a tremendous time and cost savings to the organisation.

The Dragon line consists of three products, Dragon Sensor, Dragon Squire, and Dragon Server.

§ Dragon Sensor, a high-speed network-based intrusion detection system that was recently awarded Network Computing's Editors Choice award, is a proven solution for detecting attacks across high-speed networks. For the Network Computing review, Dragon was the only network-based IDS to detect every attack.

§ Dragon Squire, a host-based intrusion detection system, detects attacks on the local host. It supports Windows and UNIX based operating systems, and detects attacks by analysing the audit and system logs as well as monitoring the integrity of key system files using MD5. Dragon Squire also supports monitoring of firewalls, routers and third-party intrusion detection systems via SNMP and SYSLOG log forwarding. Squire also detects attacks against often targeted and commonly vulnerable applications such as mail servers, FTP servers and web servers – including Microsoft Internet Information Server.

§ Dragon Server ties together Dragon's capabilities through its centralised and secure management and reporting capabilities. The Dragon Policy Manager provides group-based maintenance of Sensor's and Squires providing efficient configuration and signature deployments across the enterprise. For monitoring, Dragon Server provides centralised analysis, reporting, and correlation of security activity across the entire infrastructure. Dragon's powerful analysis consoles allow events to be correlated against known vulnerabilities, known attackers, and attack destination, source, and time. This provides organisations the information they need to make informed decisions regarding the escalation and mobilization of incident response teams.

A cornerstone of Enterasys' Secure Harbour architecture, Dragon offers a complete intrusion detection solution providing the detective measures required for protecting today's business-critical IT infrastructure. Secure Harbour is the industry's first holistic security architecture for enterprise networks, encompassing a complete range of security solutions designed to "protect and serve" corporate information.

About Enterasys Networks

Enterasys Networks (NYSE: ETS) is a new type of company that combines a single market focus with a strong technology heritage to provide communications infrastructures for enterprise-class customers. Enterasys' networking hardware and software offerings deliver the innovative security, availability and mobility solutions required by Global 2000 organizations coupled with the industry's strongest service and support. Based in Rochester, New Hampshire, Enterasys was named a "Company to Watch in 2001" by CIO Magazine.

For more information, visit <http://www.enterasys.com>

This release may contain projections or other forward-looking statements regarding the future financial performance of the company or other future events and circumstances. Such forward-looking statements by their nature involve risks and uncertainties, and actual results or events could differ materially. Risks that could cause actual events or results to differ materially from those described in the forward-looking statements include business disruption and market perceptions associated with the company's emergence as an independent public company, as well as risks associated with competitive conditions, pricing and margin pressures as a result of product shifts and changes in market dynamics, greater use of, and expenses associated with, distributors and resellers, limited management resources, the company's acquisition strategy, volatility in the stock markets and market valuations being placed on communications infrastructure and service companies, technological changes, intellectual property protection and related issues, dependence on suppliers and contract manufacturers, and potential volatility in operating results, among others. For a more detailed discussion of these and other risks and uncertainties related to the company's business, please refer to Cabletron Systems, Inc.'s most recent filings with the Securities and Exchange Commission, including the its most recent annual report on Form 10-K, and its other more recent reports on Form 10-Q and Form 8-K.

Editorial Contacts:

Annmarie Dickson
Enterasys Networks
Tel: +44 1635 810723
E: adickson@enterasys.com

Martin Brindley
MCC International
Tel: +44 1962 888100
E. martin.brindley@mccint.com

