

PROCESSOR

New Products

 [Click To Print](#)

General Information

May 26, 2006 • Vol.28 Issue 21

Page(s) 20 in print issue

Security Management From One Platform

Enterasys Dragon Network Defense Incorporates Compound Intrusion-Detection Technologies



Enterasys Dragon Network Defense

Dragon Security Processor ranges from \$65,000 to \$159,000; Dragon Behavioral Flow Sensors range from \$18,000 to \$45,000

Provides multiple-level security, including network behavioral anomaly detection and signature and event detection, managed from a central Web console

www.enterasys.com

Managing network security gets harder every day as the number and types of threats multiply. Security is also a double-edged sword, and an incorrectly implemented or mismanaged security policy can prevent network commerce and stand in the way of the mission of the enterprise. But if an intruder penetrates the network perimeter, your company's data and reputation could be forever compromised. To ramp up levels of security, network admins are turning to intrusion detection solutions. These packages constantly monitor network traffic, looking for evidence that points to malicious intent and blocking threats before they cross the network boundary.

Enterasys Networks has rolled out Dragon Network Defense, an addition to its existing Dragon Security Suite and Secure Networks product line. The

package runs under the Trustix Secure Linux 2.1 operating system using kernel 2.4.28-11trsmpl. Dragon Network Defense utilizes multiple intrusion-detection technologies to identify threats to the network infrastructure and supports third-party security utilities such as antivirus, antispymware, and network-scanning packages. The package also assists businesses to comply with stringent regulatory issues such as Sarbanes-Oxley.

To help IT staff manage security for even larger enterprises, Dragon Network Defense comes bundled with the Dragon Security Command Console, which lets network administrators configure the package and generate detailed reports. The Dragon Security Command Console's report generator can provide reports for a single department within an organization or for the entire enterprise. The Console is a central security information management tool, providing actionable intelligence and reporting capabilities to protect complex enterprise level IT infrastructures. The console collects and analyzes security information from a broad assortment of security devices and

software, lowering the resources required to effectively manage the security of complex networking environments.

This latest version of Dragon Network Defense now includes network behavioral anomaly detection capabilities. This lets the package identify threats that lack recognizable signatures, increasing the number and types of threats that can be detected and blocked. Behavioral anomaly detection complements Dragon's intrusion prevention and detection capabilities by tracking, analyzing, and recording every network flow, increasing network availability and decreasing the likelihood of expensive outages.

Competitors to the Enterasys Dragon include StealthWatch from Lancope (www.lancope.com), Peakflow from Arbor Networks (www.arbornetworks.com), and Profiler from Mazu Networks (www.mazunetworks.com). According to Enterasys, Dragon Network Defense is unique because of its ability to provide a full complement of Network Behavioral Anomaly Defense technologies with a fully integrated security information manager, the Dragon Security Command Console. ■

by Joe Lazzaro

Copyright © 2006 Sandhills Publishing Company U.S.A. All rights reserved.