

Explore the TechTarget Network at SearchTechTarget.com.

Get your FREE subscription today



SUBSCRIBE/RENEW

[HOME](#) | [CURRENT ISSUE](#) | [BACK ISSUES](#) | [BROWSE CONTENT](#) | [ABOUT US](#) | [CONTACT US](#) | [ADVERTISING](#)

Search For: _____ in [TechTarget Security Sites](#)

[ALL HOT PICK & PRODUCT REVIEWS](#)

[MAR '05 TABLE OF CONTENTS](#)

Intrusion Prevention

Issue: [Mar 2005](#)

printer friendly

e-mail a friend

request a reprint

Additional Hot Pick & Product Reviews

- ▣ [Secure Reads](#)
- ▣ [Wireless Firewall](#)
- ▣ [Security Appliances](#)
- ▣ [Configuration Management](#)

>> [SEE ALL HOT PICK & PRODUCT REVIEWS](#)

Features

- ▣ [Invasion Force](#)
- ▣ [Crypto Hazard](#)
- ▣ [Guardians of the Crown Jewels](#)
- ▣ [Double-Check with Routers](#)

>> [SEE ALL FEATURES](#)

Columns

- ▣ [Editor's Desk: Making the Grade](#)
- ▣ [Perspectives: We need technologies that won't impede our Internet use.](#)
- ▣ [Layer 8: Templates can help unskilled users do the work of security pros.](#)
- ▣ [Logoff: Microsoft gave birth to the security economy. It may be responsible for its death, too.](#)

>> [SEE ALL COLUMNS](#)

Dynamic Intrusion Response

[Enterasys Networks](#)

Price: Network IDS starts at \$2,995; host IDS, \$850 per host

Enterasys Networks' development of its Dynamic Intrusion Response (DIR) platform leverages its strength as a network infrastructure products company and its popular IDS, the Dragon Intrusion

Defense System. The result is a powerful, centrally managed intrusion prevention system that enforces security down to the switch level.

DIR isn't a single product, but rather a broad umbrella term used to describe the solution's architecture. DIR's main components are the latest Dragon release (7.0), the NetSight Atlas Automated Security Manager (ASM) and Enterasys' policy-enabled Matrix switches. Enterasys says DIR now integrates with third-party switches, firewalls and routers.

ASM plays a pivotal role by coordinating intrusion detection and response. It translates the data received from Dragon via SNMP traps into policy-based enforcement action on the switches, using Enterasys' proprietary algorithms and network mapping to pinpoint suspect devices.

ASM allows you to define specific responses, such as notifying security managers and isolating the suspect host from the network. We created rules directing ASM to quarantine suspect systems at the switch level in response to a variety of threats. For example, one rule blocked all traffic originating from the switch port occupied by a machine that tried to download the /etc/passwd file from a remote site. Another blocked traffic from ports participating in a DDoS attack.

The configuration process (essentially providing Dragon and ASM with each other's system details) was simple; however, each component uses a separate configuration console, and switching between tools was cumbersome.

Dynamic Intrusion Response



We tested DIR with an Enterasys Matrix E1 switch. Using ASM's policy wizards, you can develop and store custom policies on the switch. This takes the policy processing away from slower software systems and places it closer to the source, minimizing the number of network devices involved and improving response time.

Dragon, one of the best IDSeS on the market, is the heart of DIR. Our Dragon Network Sensor detected everything we threw at it, including buffer-overflow exploits, published OS vulnerabilities and e-mail worms. ASM passed the attack information to the switch, which automatically isolated the offending machines based on our policy.

In addition to Dragon's strong set of preloaded attack signatures, we were able to develop custom signatures through its GUI. Customization can be used for other purposes, such as designing IDS signatures based on keywords for detecting and alerting the unauthorized disclosure of confidential information. In addition to signature-based detection, Dragon uses anomaly detection, pattern matching and protocol decoding.

Dragon 7.0 features an easy-to-use central management GUI, virtual sensors that allow a single network sensor to operate with multiple policies and configurations, and Web server intrusion prevention that protects IIS and Apache from Web-based attacks.

The Dragon sensor is available in a number of different appliance and software versions, supporting bandwidth needs ranging from 100 Mbps to more than 1 Gbps. Dragon has added host-based IDS, which is installable on a wide range of routers, firewalls and servers.

Installation of all the DIR products was fairly straightforward. We simply booted up the IDS appliance and installed the software from a CD. The installation program guided us through the step-by-step process. We had similar ease installing the applications on both Linux and Windows platforms. The Matrix switch required initial configuration through the console port and then cooperated with the other DIR components. We needed about 45 minutes to configure each of the components (IDS, ASM and switch) to get them to communicate with one another--an acceptable amount of time for a product of this complexity.

The DIR architecture combines one of the most popular IDSeS with a powerful security management system and the switching hardware of an established vendor. Overall, it's an intriguing approach that represents a big step toward the full integration of security and network devices.

--Mike Chapple



SUBSCRIBE/RENEW

[HOME](#) | [CURRENT ISSUE](#) | [BACK ISSUES](#) | [BROWSE CONTENT](#) | [ABOUT US](#) | [CONTACT US](#) | [ADVERTISING](#)

Information Security magazine is part of the [TechTarget](#) portfolio of enterprise IT-focused media.

© 2002-2005 TechTarget. All Rights Reserved. [Read our Privacy Statement](#)