

TECHNOLOGY BRIEF

EXTENDING YOUR INVESTMENT IN SNORT®

KNOW MORE NETWORK RISKS
NO MORE GUESSING



SOURCEfire®

THE POWER OF SNORT

To date, the SNORT® open source intrusion prevention and detection technology has been downloaded more than 3,000,000 times, making it the most widely deployed IPS technology in the world. Of course, for Snort users this success comes as no surprise.

Powerful, high-performance detection capabilities ensure that Snort can make a valuable contribution to practically any organization's security infrastructure. The fact that Snort is an open source solution also yields significant benefits. Having open, non-proprietary source code introduces an unmatched level of flexibility and spurs development at a markedly accelerated pace compared to typical closed, commercial development models. Indeed, a vast, well-organized community continually develops, reviews, tests, and improves not only the code for Snort's core capabilities, but also the rules for detecting new and evolving threats, and a wide range of complementary open source components (e.g., Barnyard, ACID, BASE, Oinkmaster).

Due to the prevailing conditions associated with the threat, technology, and regulatory landscapes, today's organizations are increasingly looking for more from their security solutions. Overall, they need to achieve significantly greater degrees of efficiency and effectiveness just to keep pace as:

- The diversity, sophistication, and elusiveness of threats to their computing environments and critical information resources continue to increase.
- The proliferation of new technologies and applications ensure a steady, or even growing, population of vulnerabilities that are ripe for exploitation.
- The business-driven adoption of solutions that facilitate greater degrees of user mobility, interconnectivity with remote offices, and third-party access to networked resources introduces more points of entry for threats.
- The emergence and enforcement of a plethora of regulatory and legislative compliance requirements consume a significant percentage of available IT/security resources.

Not surprisingly, the bottom line in this case is that the security challenges confronting today's organizations cannot be addressed with Snort alone.

THE POWER OF SOURCEFIRE'S ETM SOLUTIONS

Founded by Snort creator Martin Roesch, Sourcefire® certainly understands the situation that today's organizations are in and the needs that they have as a result. Accordingly, the goal at Sourcefire has been to build on the powerful and flexible foundation of Snort's technology to create enterprise-class solutions that better and more fully meet these needs. This has led to the development of a solution set that provides capabilities to meet a broad range of enterprise needs.

IT organizations that are not already using Snort can transparently gain the benefits of its robust threat detection and prevention capabilities simply by implementing the Sourcefire 3D™ System, a complete Enterprise Threat Management (ETM) solution (described in detail below).

At the same time, IT groups that have already deployed Snort can easily extend their investment in it. As discussed in the following sections, this is made possible by a handful of Sourcefire product options that are available to open source Snort users. Notably, organizations have the choice of migrating progressively from one option to the next, or just moving directly to the one they want and staying at that stage indefinitely.

Extending Snort with Intrusion Agent and Sourcefire Defense Center™

The first of the potential "upgrades" available to Snort users is the option to implement Sourcefire Intrusion Agents in conjunction with Sourcefire Defense Center, the central management application (i.e., GUI) for the 3D System. Intrusion Agents transmit events generated by open source Snort sensors to Defense Center. This, in turn, enables Snort users to get the benefits of a subset of Defense Center's functionality. In particular, the specific capabilities gained in this case include the following.

- **Centralized event data.** Rather than just being written to individual, distributed databases, the events generated from each open source Snort sensor are aggregated to the embedded database included with Defense Center, vastly simplifying subsequent event processing activities.
- **Real-time alerts.** Administrators no longer have to manually interrogate the event database to discover what's happening in their networks. With Defense Center, automated warnings can be sent to individuals and other management systems via syslog, email, or SNMP.
- **Powerful data analysis.** Dozens of preconfigured and customizable workflows make it easy to view and process large numbers of events. Events can be organized at a high level by one set of criteria (e.g., frequency of occurrence) and then can be "drilled into" to obtain successively granular levels of detail. Viewing capabilities support both identification of long-term trends and packet-level forensic analysis.
- **Real-time attack response.** Defense Center's Policy and Response engine can be used to create event-driven rules and actions. In addition to the aforementioned alerting capabilities, rules can also be configured to block threat-laden or otherwise suspicious traffic, as well as to trigger inspection and/or remediation of targeted systems.
- **Comprehensive reporting.** Preconfigured and customized reports can be generated to support a full range of operational and strategic objectives (e.g., troubleshooting, attack trending, and presentations to management).

- **Integration with third-party tools.** APIs and a range of other supported integration mechanisms can be used to inform or engage other components of the organization's network and security infrastructure (e.g., security information/event management systems, patch or configuration management systems, vulnerability assessment scanners, firewalls, and routers).

- **Full support.** Finally, the change from open source Snort to 3D Sensors also brings with it a change from the ad-hoc, volunteer community support model associated with open source projects to a more efficient, dedicated support offering provided by Sourcefire.

Taking Advantage of Sourcefire 3D™ Sensors

A second upgrade option entails supplementing, or perhaps even replacing, open source Snort sensors with Sourcefire 3D Sensors. The first aspect of this scenario that needs to be highlighted is that 3D Sensors are based on Snort and, therefore, employ the same core detection technology. Of course, it is also necessary to acknowledge the capabilities and benefits that are gained in this case. Assuming, again, that Defense Center is employed, these include all of the items listed for the previous option, plus the following additional benefits.

- **Pre-packaged hardware.** Sourcefire's 3D Sensors are offered as a family of appliances. With throughput options from 5 Mbps up to 10 Gbps and the ability to be deployed in both inline and/or passive modes, they easily support a full range of deployment needs. As prepackaged solutions, they also significantly reduce the effort associated with initial implementation. Organizations need not commit precious time to "spec-ing" hardware, selecting and hardening an operating system, and installing and configuring the Snort code and associated management utilities.
- **Centralized sensor management.** For the upgrade option involving Intrusion Agents, only a subset of the Defense Center capabilities would be enabled. That is true once again, but in this case because of bi-directional communication between 3D Sensors and Defense Center, additional capabilities are enabled. One significant benefit is that security administrators can now centrally manage policies and configurations for up to 100 sensors from a single Defense Center console.
- **Backup and restore for configuration data.** Along similar lines, Defense Center also provides a centralized mechanism for backup and restore of configuration settings for an organization's 3D Sensors. In contrast, achieving a similar capability with Snort typically involves manually backing up and restoring the configuration file for each sensor.
- **"Zero-touch" upgrades for sensors.** With Snort, taking advantage of newly developed features and detection capabilities typically entails a "forklift" upgrade. In other words, a whole new install, essentially requiring an administrator to manually regenerate configuration files and rebuild all of the sensors. But with 3D Sensors, software updates are implemented in a far more transparent manner. They are simply scheduled at the Defense Center, and then the software is automatically downloaded and installed.

Embracing the Full Sourcefire 3D System

As discussed previously, the Sourcefire 3D System is a complete Enterprise Threat Management (ETM) solution. To clarify what this means, ETM is an approach that (a) combines complementary threat and vulnerability management technologies, (b) enhances them by taking advantage of shared intelligence, and (c) further improves overall efficiency and effectiveness by coordinating and fully managing them with a single management system. The primary technologies involved are intrusion prevention (IPS) and network behavior analysis (NBA).

In terms of the 3D System, the ETM approach is achieved by bringing Sourcefire RNA™ (Real-time Network Awareness) into the mix, in conjunction with Defense Center and 3D Sensors and/or Snort sensors equipped with Intrusion Agents. At a high level, the role of RNA is to passively monitor network activity and to extract various types of "intelligence" from what it observes, including detailed information about individual endpoints (e.g., operating system, services, applications, and potential vulnerabilities) and how the network is being used, or, for that matter, misused. Optionally, Sourcefire RUA™ (Real-time User Awareness) can be implemented to provide intelligence on the "who" dimension of observed activities. In any event, it is these passive monitoring capabilities, associated analysis and inference engines, and resulting intelligence that either enable or enhance each of the main components of the 3D System. Specific benefits and capabilities that are obtained by embracing RNA and the full 3D System include the following.

- **Centralized management.** The Sourcefire Defense Center dashboard is the focal point for monitoring and managing security and compliance events generated by the Sourcefire 3D System. The fully customizable dashboard contains a library of interactive "widgets" that can be dragged and dropped from one column to another, much like a Google, Yahoo, or Microsoft SharePoint portal. Configured dashboards can be saved and made available to colleagues with similar roles in the organization.
- **Event correlation and prioritization.** By correlating detected events against the profiles of targeted systems, not only can false positives be virtually eliminated, but Impact Flags can be automatically assessed to prioritize the efforts of administrators responsible for investigating and responding to potential threats.

- **Automated IPS Tuning.** The RNA-Recommended Rules (RRR) and Non-Standard Port Handling features of RNA automate the time-consuming process of tuning your IPS. RRR optimizes IPS performance and maximizes protection by recommending that only Snort rules pertaining to a network’s operating systems and services be enabled. RNA’s Non-Standard Port Handling feature identifies the ports and services on the hosts it’s monitoring and enables the IPS to dynamically apply the correct rules for any non-standard ports. This feature helps to prevent possible IPS evasions when sending traffic on non-standard ports.

Attackers can also possibly evade IPS inspection by fragmenting attacks and taking advantage of the fact that operating systems reassemble traffic fragments differently. RNA’s Adaptive Traffic Profiles feature prevents this type of IPS evasion by providing operating system data about each host to the 3D Sensor. The 3D Sensor can dynamically adjust the traffic reassembly process in a manner consistent with different target OSes.

- **Network Behavior Analysis.** The fundamental technique that lies at the heart of network behavior analysis (NBA), network flow analysis, can be applied in a number of ways. The most recognizable of these is using it to identify attacks for which the corresponding threats and/or vulnerabilities have not yet been widely disclosed and defined—which in the past was commonly referred to as network behavior anomaly detection, or NBAD. However, NBA is actually intended to encompass much more. For example, it also enables the detection of unauthorized hosts and communications. In addition, it facilitates both security and network operations by supplying invaluable contextual information pertaining to network composition, specific events, and overall usage patterns.

CAPABILITY	OPEN SOURCE SNORT WITH INTRUSION AGENT	ADD SOURCEFIRE DEFENSE CENTER	ADD SOURCEFIRE 3D SENSOR	FULL SOURCEFIRE 3D SYSTEM**
Leading IDS/IPS capabilities	✓	✓	✓	✓
Inline and passive options	✓	✓	✓	✓
Sourcefire VRT rules	✓*	✓	✓	✓
Real-time alerts		✓	✓	✓
Centralized event data		✓	✓	✓
Powerful data analysis		✓	✓	✓
Real-time attack response		✓	✓	✓
Comprehensive reporting		✓	✓	✓
Integration w/ 3rd-party tools		✓	✓	✓
Pre-packaged appliance (up to 10 Gbps)			✓	✓
Centralized sensor management			✓	✓
Backup & restore of configuration data			✓	✓
Full support and “zero-touch” upgrades for sensors			✓	✓
Adaptive IPS: - Impact Flags (prioritization) - RNA-Recommended Rules - Non-Standard Port Handling - Adaptive Traffic Profiles				✓ ✓ ✓ ✓
Network Behavior Analysis				✓
Vulnerability Assessment				✓
Network Access Control (i.e., IT policy compliance monitoring)				✓

Figure 1. Capabilities comparison between open source Snort and Sourcefire commercial product offerings.

*Sourcefire VRT rules are available on a 30-day delayed basis at no charge. Open source Snort users may purchase Sourcefire VRT Subscriptions on a per-sensor basis. Sourcefire commercial customers receive Sourcefire VRT Subscriptions as part of a standard Sourcefire Support Agreement.

**The Sourcefire 3D System is comprised of Defense Center and 3D Sensor appliances. Sourcefire 3D Sensors include Sourcefire IPS and RNA software. (RNA Host Licenses are required for monitored hosts.) Sourcefire RUA is recommended, but not required.

THE BEST OF BOTH WORLDS

Figure 1 summarizes the capabilities that can be gained by IT organizations that elect to extend their investment in Snort by taking advantage of one or more components of the Sourcefire 3D System. Overall, it should be clear that what Sourcefire provides with its solutions is a combination of the best features of both a commercial model of operation and a tremendously successful open source project. The net result is a compelling set of benefits that enable organizations to work smarter, not harder, when it comes to protecting their computing systems and critical information resources.

- **Operational efficiency is improved.** Enhanced management capabilities, shared intelligence, integration with other components, and increased levels of automation enable overtaxed security administrators and analysts to spend fewer cycles managing the IPS and more cycles tackling other problems (e.g., figuring out a security model for web services, or virtualization).
- **Security effectiveness is improved.** Not only are additional threat protection technologies brought into the mix, but enhanced management capabilities also enable tighter, more consistent control in the first place—not to mention faster response to any events or attacks that happen to materialize.
- **Compliance status and readiness is improved.** This is due, in part, to being able to take advantage of granular policy enforcement and compliance reporting capabilities. But there is also value in being able to show auditors that the organization has implemented a more comprehensive approach to threat management.
- **Costs remain the same, or less.** Sourcefire commercial products offer a rapid return on investment (ROI). The cost of acquiring Sourcefire Defense Center, Intrusion Agents, and/or 3D Sensors typically offsets the existing costs associated with managing open source Snort environments. Time that would have been spent managing Snort sensors, monitoring un-prioritized events, and creating manual reports can now be spent on more pressing IT security concerns.

- **The investment in Snort is maintained.** Expertise acquired with open source Snort is fully transferable to Sourcefire commercial offerings. Snort users maintain the ability to view, edit, and create Snort rules while gaining improved manageability, scalability, and performance only found within Sourcefire 3D System components.

For more information about Sourcefire Intrusion Agents, Sourcefire Defense Center, Sourcefire 3D Sensors, or the entire Sourcefire 3D System, visit Sourcefire's web site at www.sourcefire.com, or contact Sourcefire today.