
THE POWER OF OPEN SOURCE

The Snort open source intrusion detection and prevention system (IDS/IPS) was created in 1998 by Martin Roesch, the founder and CTO of Sourcefire. With its dramatic speed, power and performance, Snort has quickly become the single most widely deployed IDS/IPS technology in the world.

The wide availability of open source brings many advantages. Because the source code is open and non-proprietary, open source development occurs at a markedly accelerated pace compared to proprietary models. The success of the model is due to a vast community of security experts that continually review, test and improve open source code. Simply, users in the open source security community worldwide can detect and respond to bugs and other security threats faster and more efficiently than in a “closed” environment.

With more than 3,000,000 downloads to date, the Snort open source community has achieved a well-earned reputation for extraordinary organization and dedication. Hundreds of thousands of security engineers and specialists the world over contribute Snort rules for new and evolving threats every hour of the day, often in record time.

MANAGING SNORT IN LARGER ENVIRONMENTS

Larger organizations with multiple open source Snort sensors—whether co-located within the same facility or geographically dispersed in different parts of the world—face certain management and scalability challenges that smaller organizations typically don’t experience. First, as events generated by stand-alone Snort sensors are not correlated with endpoint intelligence, Snort administrators lack the ability to prioritize security events. Without the ability to prioritize events by impact, Snort users may find it challenging, or downright confusing, in determining which of the dozens or even hundreds of security events to investigate on a daily basis—especially with limited IT security resources.

Second, as intrusion events are stored on the hard disk of each Snort sensor, security analysts must connect to each sensor to view events. Human analysis is required to identify and assess on-going threats that may be common across different parts of the organization. And when the time comes to produce daily, weekly or monthly reports, Snort users must manually gather statistics from each Snort sensor.

And third, as many open source Snort users place their sensors in passive IDS mode, timely response to critical security events is critical. Time is of the essence, especially when defending mission critical network resources, such as web servers, email servers and CRM/ERP application servers. Open source Snort cannot, by itself, remediate to routers or firewalls to block suspected bad traffic, nor can it generate real-time alerts notifying security analysts of potential high-impact breaches.

Although open source Snort provides a powerful intrusion detection and prevention engine, many Snort users—especially in larger Snort environments—are asking for more.

EXTENDING YOUR SNORT INVESTMENT

Sourcefire is atop the network security industry when it comes to incorporating open source technology into enterprise-class commercial products. Backed by both the open source Snort community and Sourcefire’s global infrastructure of Support, Training and Consulting professionals, Snort users can leverage their existing investments in Snort while extending the manageability, scalability and security of their IDS/IPS solutions.



Introducing the Sourcefire Intrusion Agent for Snort, a Sourcefire software product that installs directly on top of open source Snort sensors. When used in conjunction with a Sourcefire Defense Center™ appliance, the Sourcefire Intrusion Agent affords Snort users with powerful new capabilities, including:

- **Centralized event aggregation and analysis** – Instead of being written to individual, distributed Snort sensor databases, intrusion events generated from each Snort sensor are aggregated to Defense Center's embedded database, vastly simplifying event aggregation and analysis.
- **Powerful event analysis workflows** – Dozens of pre-configured and customizable workflows make it easy to view and process large numbers of Snort events. Events can be organized, prioritized and "drilled into" to uncover additional event details. Viewing capabilities support both identification of long-term trends and packet-level forensic analysis.
- **Real-time alerts** – Administrators no longer have to manually query the Snort sensor event database to discover what's happening in their networks. With Defense Center, automated alerts can be sent to individuals and third-party management systems via syslog, email, SNMP and eStreamer.
- **Automated attack response** – Defense Center's Policy and Response engine can be leveraged to create event-driven rules and actions. Rules can be configured to block threatening or otherwise suspicious traffic at the router or firewall, to trigger a surgical active scan of an endpoint under attack, and to remediate targeted system.
- **Comprehensive reporting** – Both pre-configured and customized reports can be generated with ease to support a full range of operational and strategic objectives. Snort users can create ad-hoc and/or scheduled reports to depict security threat trends over time for a given Snort sensor or for all Snort sensors across the entire organization.
- **Integration with third-party systems** – Sourcefire provides a series of APIs (e.g., Remediation API, Host Input API) and other interfaces (e.g., eStreamer, SNMP, Syslog) to integrate with a wide range of third-party systems, including routers, firewalls, SIEMS, log managers, vulnerability scanners, help desk applications, patch management systems, and network management platforms (e.g., HP OpenView, IBM Tivoli, CA Unicenter, BMC Patrol).

BENEFITS OF INTRUSION AGENTS FOR SNORT WITH DEFENSE CENTER

- Centralized event aggregation & analysis
- Powerful event analysis
- Real-time alerts
- Automated attack response
- Comprehensive reporting
- Third-party system integration

A SOLUTION THAT GROWS WITH YOU

As your network security requirements grow, Sourcefire is there to grow with you. When you are ready to expand the capabilities of your Snort sensors, or broaden your network security strategy into other Sourcefire Enterprise Threat Management (ETM) solutions, Sourcefire offers a roadmap to take you there.

Once up and running with Sourcefire Intrusion Agents and Defense Center, Sourcefire offers two additional Sourcefire 3D™ System products to strengthen your existing Snort IPS solution and to expand your network security capabilities—Sourcefire RNA™ and Sourcefire RUA™.

Sourcefire RNA (Real-time Network Awareness) provides 24x7, "always-on" passive scanning of your network to identify and catalog endpoints and to uncover potential host vulnerabilities. When RNA is used in conjunction with Intrusion Agents and Defense Center, open source Snort users gain the following key capabilities:

- **Adaptive IPS technology** – Snort users often struggle to determine the optimal selection of Snort rules to enable to effectively and efficiently protect a given network environment. With RNA-Recommended Rules, your Snort sensors can "adapt" to the assets they're protecting by enabling and/or disabling rules recommended by RNA.
- **Security impact assessment** – With Sourcefire RNA, Snort events can be correlated against the profiles of targeted systems virtually eliminating false positives. An "Impact Flag" is assessed and assigned to each Snort event, helping administrators to prioritize investigative efforts. By leveraging Impact Flags, the quantity of actionable Snort events can be reduced by up to 99%.

- **Compliance policy enforcement** – RNA is a key component of Sourcefire’s (post-connect) network access control (NAC) solution. Snort users gain powerful compliance capabilities, helping organizations achieve industry (e.g., PCI) and/or regulatory (e.g., Sarbanes-Oxley, HIPAA) compliance. “White list” policies can be created to enforce usage of approved operating systems, services, ports, protocols and (select) applications. Host access policies can be created to monitor and/or limit access to key network resources.
- **Traffic baselining and anomaly detection** – RNA is a key component of Sourcefire’s network behavior analysis (NBA) solution, enabling Snort users to establish “normal” traffic baselines and detect network anomalies (e.g., worm propagation), thus helping to defend against attacks originating both inside and outside the network.
- **Host vulnerability assessment** – RNA is a key component of Sourcefire’s vulnerability assessment (VA) solution, depicting hosts that are vulnerable and/or potentially vulnerable to today’s emerging threats. Sourcefire customers are afforded the opportunity to “harden” assets (e.g., applying patches, shutting down unnecessary services and ports) before attacks occur.

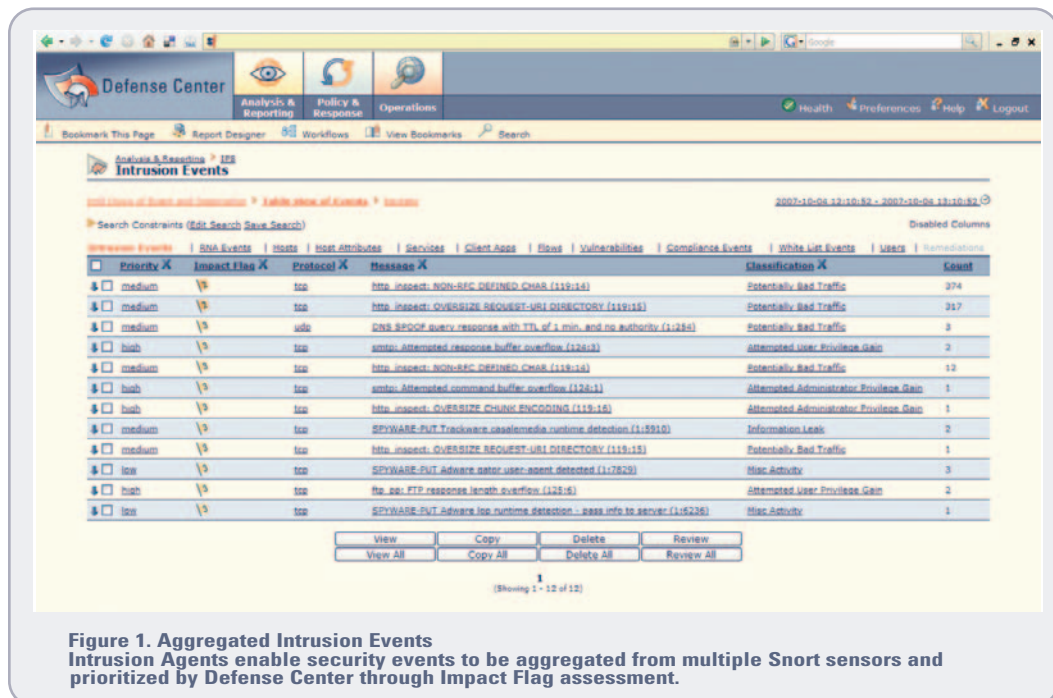


Figure 1. Aggregated Intrusion Events
Intrusion Agents enable security events to be aggregated from multiple Snort sensors and prioritized by Defense Center through Impact Flag assessment.

Sourcefire RUA (Real-time User Awareness) provides user identity tracking capabilities by pairing Active Directory and LDAP usernames with host IP addresses involved in security and compliance events. When RUA is leveraged with Intrusion Agents, Defense Center and RNA, open source Snort users gain the following key capabilities:

- **Quickly identifying owners of compromised hosts** – Snort alone can give you the IP address of a targeted host. But finding the owner of the host under attack can prove difficult, especially in DHCP environments. But with Sourcefire RUA, the Snort administrator can quickly identify the username associated with a host under attack. Additional user information—full name, phone, email and department—is also available at your fingertips. By knowing who to contact, security events can be resolved more quickly than ever—when time is of the essence.
- **Identifying users violating compliance policies** – If a user is using a host with a non-compliant operating system (e.g., Windows 98), or a user is using a non-compliant application (e.g., Skype), you will not only know the IP addresses of non-compliant hosts, but also who to contact in response.
- **Leveraging user identity as a policy constraint** – When configuring compliance and/or remediation policies, user identity can be configured as a restraint. For example, alert on unauthorized access to the company’s payroll application, unless the user is a member of the Finance department. Or block an unauthorized port scan, unless the user is a member of the IT department.



RAPID RETURN ON INVESTMENT

Whether you're an existing open source Snort user looking to improve the manageability and scalability of your Snort sensors through Intrusion Agents and Defense Center, or you're looking to strategically expand your organization's overall network security strategy, Sourcefire commercial ETM solutions provide a rapid return on investment (ROI). By leveraging one or more components within the Sourcefire 3D System, Snort users save time and money by:

- maximizing security through improved IPS protection, real-time alerts, automated responses and through the implementation of an NBA solution to defend against internal threats;
- reducing time spent sifting through Snort event databases, manually creating reports, and locating hosts involved in Snort security events

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			✓	✓
Recommended IDS/IPS policies				✓
Impact flags (prioritization)				✓
Adaptive IPS				✓
Network Behavior Analysis				✓
Vulnerability Assessment				✓
Network Access Control (i.e., monitor/enforce policies)				✓

Figure 2. 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.

Best of all, the investment you've already made in deploying and tuning Snort sensors is fully protected, and the knowledge and experience you've gained along the way is fully transferable to Sourcefire 3D System solutions.

CONTACT SOURCEFIRE TODAY!

Contact Sourcefire or a Sourcefire Channel Partner today to learn more about how Intrusion Agents and Defense Center can improve the manageability and scalability of your Snort investment. For more information on the Intrusion Agent for Snort, Defense Center and other components of the Sourcefire 3D System, connect to the Sourcefire web site at www.sourcefire.com.