

The Sourcefire 3D System™

Discover. Determine. Defend.

“Sourcefire’s Real-time Network Awareness Sensor 2000 is like a magic eye that watches everything happening on your network. By combining passive network analysis with a Web-based management system, Sourcefire delivers a powerful tool to IT personnel who need more information about their networks.”

- Network World



6:42 7:08 7:21 7:25 7:49 8:06 8:34 9:02 9:06 9:35 10:04 10:16 10:45 11:03 11:30 11:58 12:01 12:05 12:

System Functionality

IPS/IDS

- Intrusion detection and prevention
- Accurate, powerful and flexible
- Snort-based performance and precision

Vulnerability Management

- Real-time network discovery
- Integrated normalized vulnerability database
- Change detection and management
- Surgical scanning of suspect assets

Security Management

- Identify critical events on your network
- Automated workflows and reporting
- ABC's of Defense – Alert. Block. Correct.

Compliance

- SOX, GLBA, SB1386, HIPAA, FISMA
- Ensure compliance with policy-based alerting and reporting
- Automate compliance reporting

According to CERT, cyber security incidents increased by an average of 85% per year from 2000 to 2003. In 2004, CERT stopped tracking incident reports altogether when they became too commonplace to be meaningful.

Today, not only are the new types of threats and vulnerabilities growing by leaps and bounds; the pace at which they strike has accelerated at an alarming rate.

All the while, networks and network infrastructures are growing larger, more dynamic, more complex and more important.

In a world with an abundance of wireless and mobile computing devices, road warriors and offshore partnerships, the traditional model of perimeter defense is growing increasingly ineffective.

Fact is, organizations are discovering that conventional approaches to network security fall short on all fronts. Active vulnerability scanners are “noisy” and too intermittent – an active scan at 2:00am Sunday morning is largely meaningless, given that few laptop PCs or other mobile devices are even connected at that hour!

Host-based approaches to vulnerability management, while able to do their job in real-time, can be a nightmare to manage. And since they support only updateable platforms running the most popular operating systems, they're incapable of defending all of the assets within diverse networking environments.

There is no silver bullet for network security.

And the challenge doesn't end with security. A myriad of complex regulatory mandates including Sarbanes-Oxley, HIPAA, and FISMA present huge compliance questions and issues.

A new, more effective approach is imperative to address security in the real world.

SOURCEFIRE 3D: A REVOLUTIONARY APPROACH

Growing threats and vulnerabilities demand that security administrators have a more effective, more efficient, truly information-driven process. One that combines real-time network and asset awareness with state of the art threat detection. A solution with the precision to automate otherwise manual processes, and the flexibility to suit the needs of every network regardless of size, topology or composition.

Sourcefire's exclusive, ground-breaking 3D approach brings a patent-pending combination of threat and network discovery, behavioral profiling, and integrated vulnerability management that unifies these technologies to provide the most effective solution for the real world.

This includes:

- Threat detection and vulnerability shielding
- Proactive vulnerability remediation
- Compromise detection and isolation
- Network usage and policy enforcement

Anchored by your security policies, the 3D approach is a proactive process of discovering what's happening on your network ... determining the impact to your business ... and defending your network in real-time.

The power source behind it all is Sourcefire RNA™ (Real-Time Network Awareness) technology. No other solution offers the real-time, persistent insight into every aspect of your network.



SOURCEFIRE RNA™

Security administrators don't need more information; they need more accurate, more *timely* information.

You can have it today, exclusively enabled from Sourcefire RNA.

RNA provides always on, **real-time** visibility into all network assets. The result: you're ready to take action well before a vulnerability becomes a bigger problem. For instance, imagine being able to know that a non-compliant machine has joined your network right when *it happens* – not when it is discovered months later by some network audit or, even worse, after it has been compromised and is already disrupting network operations.

How can RNA deliver this kind of visibility? Passive discovery methods. With passive discovery, no agents are required, and no superfluous traffic or disruptions to network assets are generated. Just a revolutionary, real-time, all-the-time way to get the information you really need.

A Better View, A Real-Time Network Map

Sourcefire RNA provides continuous, instant, real-time visibility into all network assets:

- Network asset profiles including IP address, OS and version, services and versions, ports
- Asset behavioral profiles including traffic flow, traffic type
- Network profiles including hop count, TTL parameters, security vulnerabilities
- Change events for new assets, changed assets, behaviorally anomalous assets
- All internet peering points

This information, coupled with the RNA vulnerability database, allows you to (1) know all the possible vulnerabilities on your network – in real-time and (2) take the appropriate action – automatically if you choose.

Sourcefire RNA technology is available in three different models: It can be deployed as a Plug-n-Protect dedicated appliance anywhere on your network or, the RNA software can be deployed on a Sourcefire Intrusion Sensor or on Red Hat Linux® servers distributed throughout your environment.

RNA Benefits at a Glance

- Know all the machines on your network – all the time
- Easily detect on the spot if a machine begins to rebroadcast SPAM
- Detect Spyware compromise and quickly quarantine infected machines
- Instantly detect new machines entering your network – if policy dictates, sandbox them until clean
- Detect and shutdown illegal mail servers
- Detect and shutdown rogue desktop applications including desktop web servers
- Enforce corporate policies for P2P restrictions such as Kazaa and instant messaging
- Know if a new device is behaving maliciously despite having passed access controls to check for antivirus and firewall protection
- Maximize network integrity

“With Sourcefire 3D, the promise of the self-defending network is here today.”

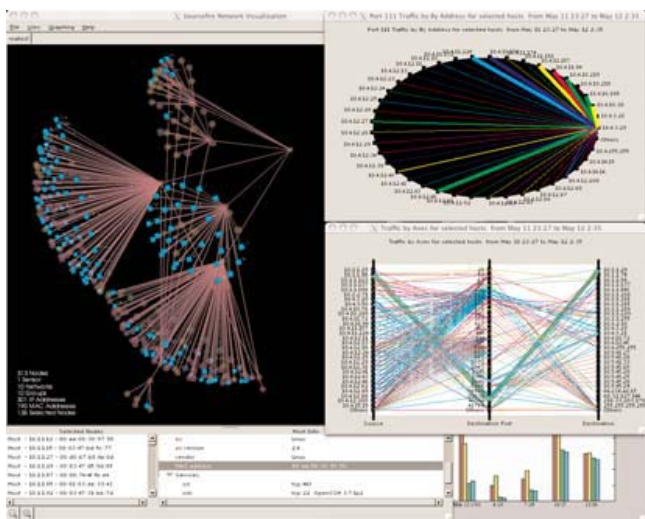
- Martin Roesch, Creator of Snort

Constantly Discovering the Network

Sourcefire RNA continuously discovers and monitors network assets and provides instant notifications of any observed changes, including the introduction of new network assets, services, behaviors, or anomalous traffic patterns and policy violations.

For instance, network environments usually have a set of servers that are statically configured, such as a web server. In the event that the web server is compromised and an attacker establishes a new service on the host like IRC or SSH, use of that service would be immediately noticed and analyzed by RNA, initiating a change event and a host of possible responses as defined by network administrators.

This benefit can also be seen anytime a system is re-configured or rebuilt without the administrator's knowledge, potentially exposing new vulnerabilities or avenues for intellectual property theft. Because RNA is constantly discovering the network, it will notice the system's new configuration and service offerings and automatically associate these changes in network assets with potential vulnerabilities and exploits that may target those vulnerabilities.



The RNA Visualization Module can quickly and easily identify where rogue connection points exist on a network to identify possible leak detection. Any point of interest in the visualization display can be magnified to show whatever level of detail is desired, including the actual host representation. Various highlighting and shape manipulation alternatives promote the visual identification of network groups or assets by any number of criteria – hop count, operating system, service count, vendor, etc. Other features include multi-parameter search and ‘pruning’, allowing for network subsets to be moved to an additional tab. The primary RNA interface is the browser-based display. It’s through this facility that the heavy lifting of analysis, configuration, administration, and reporting is performed.

Network Sonar and Real-time Network Discovery

Submariners long ago recognized the very different characteristics, and the advantages and disadvantages, associated with the two classes of sonar - passive and active. Passive sonar is persistent and stealthy; active sonar can be more precise for certain challenges like determining the exact range to a target.

Over the years the demands for stealth led to incredible advances in the precision of passive sonar. Submarines can routinely, for example, determine the class, type, power, and even the name of a ship just from its acoustic signature.

The demands of real-time network security have led Sourcefire to similar advances in passive network discovery. Like passive sonar, these methods are completely stealthy, are incredibly precise and provide the critical information needed to take real-time action against real-time security threats. Only when those last bits of information are required (like submarine ranging) are active scanning methods ever required.

RNA – always on the job, always alert, always on the lookout for the bad guys.

SOURCEFIRE INTRUSION SENSORS™

Intrusion detection and security monitoring technology provide critical insight into attacks occurring on your network. To achieve the industry’s highest rate of attack detection and prevention, Sourcefire Intrusion Sensors and Agents utilize the popular Snort® rules-based detection engine. Today Snort is the de facto standard in intrusion detection.

“Snort rules are powerful, flexible and relatively easy to write.”

- SearchSecurity.com

Sourcefire Intrusion Sensors use a powerful combination of signature, protocol, and anomaly-based inspection methods to achieve the maximum attack detection and prevention capability.

Every aspect of the Intrusion Sensor can be configured and customized to ensure that users detect and prevent the events most important to them. Flexibility in the rules language and numerous configuration options (port density, interface types, deployment modes), allows users to easily define new ways to identify and prevent threats and enforce policies specific to their individual environment.

Sourcefire Intrusion Sensors can operate “inline” – that is, with direct control over traffic traversing the device. Inline sensors have the ability to simply drop threatening traffic before it can damage network systems or applications. This inline intrusion prevention capability is most appropriate for dealing with attacks that can be identified with a high level of accuracy and confidence. Intrusion Sensors can alternatively send TCP reset commands and ICMP messages to attacking hosts or their targets. This offers more flexibility when responding to ambiguous events – rather than dropping all traffic from a particular IP address (or block of addresses), reset commands can be used to disrupt attacking sessions while leaving normal sessions unmolested. The more cautious response prevents suspicious traffic from reaching its target, while minimizing the potential for disruption of legitimate services.

About Snort



Open source Snort was created by Martin Roesch, the founder and CTO of Sourcefire. Sourcefire owns the Snort IP and controls snort.org. In June 2004, Gartner recognized the mainstream acceptance of Snort in their Open Source Hype Cycle, describing Snort as “widely available. Used by mainstream companies and supported by many vendors.” With over 2 million downloads to date, the Snort community has blossomed into a robust security community with active user groups, multiple sources for training, and widespread support at the university level.



Less Ambiguity, More Clarity and Intelligence

Unless tuned by knowledgeable administrators, traditional IDP has no knowledge of the true context and composition of the network it is responsible for defending. Context brings more meaningful intelligence, more clarity, and eliminates ambiguity and dangerous assumptions. With the context provided by RNA, you now have the smartest intrusion technology on the market.

The inevitable changes to the network mean that the intrusion technology will alert on threats that are not actually relevant to the network and miss, or under-prioritize, threats that are legitimate. Lack of contextual awareness also leaves intrusion technologies guessing in many areas of processing – especially with regard to packet handling. This leaves them ripe for evasion: the attacker can actually know more about the network than the IDP.

With the integration of RNA and intrusion technology all of this guesswork is eliminated. Relevant and non-relevant threats receive the precise priority and attention they deserve. Traffic processing also precisely emulates the behaviors of the target, foiling even the most sophisticated hackers once and for all.

Every organization is different, with some network traffic considered legitimate for certain firms, and threatening to others. Sourcefire Intrusion Sensors allow you to enable, disable or modify individual rules so that they are exactly appropriate for your environment and your business. Of course, you can also create custom rules, all without affecting the level of threat coverage provided to the remainder of the network.

SOURCEFIRE INTRUSION AGENTS™

For existing deployments of open source Snort technology, the Sourcefire Intrusion Agent for Snort brings many of the benefits of the Sourcefire 3D approach including Impact Flags for prioritizing events with greater intelligence regarding the enterprise network and vulnerabilities. The Sourcefire Intrusion Agent for Snort is available for Linux and Solaris™.



Intrusion Sensor Rules

Rules are used to examine packets at both the IP protocol level and at the application level and can be set to look for specific occurrences of attacks against a protocol, or set to look for the conditions of an attack. For example, a specific buffer overflow attack can be detected by looking for “/bin/sh” in a packet’s payload ... looking for the overflow condition ... or even looking for the number of bytes in a payload greater than some threshold.

Each rule can be set to not only alert on events, but to drop the packet or replace malicious content with benign. This flexibility in the rules language means critical threats can not only be blocked but also contained or quarantined via techniques such as dropping traffic, disrupting sessions between devices, and integrating with access control devices such as firewalls, routers and switches.

One critical area of rule development relates to the flexibility of the rule itself. Major advances by the Sourcefire Vulnerability Research Team have resulted in rules that look for threats targeting a vulnerability, as opposed to a specific attribute of a known vulnerability exploit. While this may sound like a subtle difference, this approach means dramatically reduced false positives (IDS), reduced potential for disrupting benign traffic (IPS) and the ability to detect mutations of exploits that inevitably emerge.

THE SOURCEFIRE DEFENSE CENTER™

The Sourcefire Defense Center is the nerve center of the 3D solution. It unifies and centrally manages critical network security functions including event monitoring, correlation and prioritization for incident response, forensic analysis, trends analysis, and management reporting.

The Defense Center is turnkey – no third party database required – and it's optimized for real-time processing of security events, regardless of network size. With the Defense Center you can:

- Manage multiple IDP and RNA sensors from a single management console
- Correlate event data from IDP, RNA or open source Snort to get the most comprehensive view of event activity on your network
- Prioritize security events based on relevance, vulnerability, operational importance and other factors
- Define network security policies that are applied to security information in real-time
- Define responses to security events at whatever level of automation you desire, leveraging the ABC's of Defense

The Defense Center interfaces have been designed by security analysts for security analysts with an intuitive layout and efficient presentation. Analysts also have complete power to define their own customized workflows. And because the Sourcefire Defense Center has a built-in, high performance database designed for real-time analysis, you can easily traverse tens of millions of events looking for long-term security trends, while quickly drilling down to in-depth analysis of individual packet payloads.

Centrally Manage Sourcefire Deployments

- Sensor grouping
- Real-time and forensic analysis and reporting
- The Sourcefire Defense Monitor has an open architecture, allowing you to interface with existing management consoles or help desks such as Remedy®, Tivoli® and HP OpenView and integrate with other 3rd party tools such as SIM and network management systems

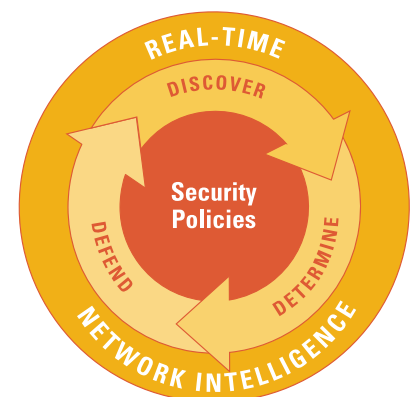
Policy Compliance

Good security is only as good as an enforced security policy. Organizations need not only solid policies, but also an effective way to monitor and enforce those policies.

With Sourcefire, you can set security policies specifically for your network and know immediately when those policies are violated.

For example, easily prevent unauthorized servers, P2P applications such as Kazaa, and rogue applications such as web servers running on desktops.

With Sourcefire, policy can drive remediation. Bottom line: you can enforce, manage, enhance and tune your security policies with confidence; and your management will be better able to document compliance with Sarbanes-Oxley, HIPAA, and others.



ACTING ON THE ABC'S OF DEFENSE

The Sourcefire Defense Center prioritizes the millions of security events to determine the most critical events to your organization's business, and takes the appropriate actions, all based on your policies and your chosen remediations.

These actions allow users to leverage the ABC's of Defense – Alert, Block, and Correct – all in real-time, against all network threats.

Alert: Ensure Attack Warnings are Rapidly Addressed

Alert responses let the Sourcefire Defense Center inform individuals, as well as network and systems management infrastructure, about attacks and threatening activity. The Defense Center supports several standard notification methods. All can be invoked in response to individual intrusion and RNA events, as well as policy violations. They include:

- General event logging, sending network discovery events to the Defense Center database. By default, all events are logged to the Defense Center databases.
- SYSLOG notification, which forwards events to the system log of a specified host. SYSLOG notification is particularly useful if a SIM is being used.
- Email notification can be used to keep individuals and systems (help desk) properly informed of selected events, or to draw the attention of an analyst to a significant threat. Email can also be used to page individuals.
- SNMP notification forwards events in the form of an SNMP trap to a specified network and systems management frameworks like Tivoli, CA Unicenter, and HP OpenView.

Block Attackers in Their Tracks

Blocking actions can be invoked in response to a variety of events – individual intrusion or RNA Sensor alerts, combinations of events, and explicit policy violations. Blocking actions can be undertaken by Sourcefire Intrusion Sensors directly, or coordinated by the Sourcefire Defense Center with other networking devices like firewalls, routers and switches.

Networks already operate devices designed to intercept inappropriate or unwanted traffic – firewalls, routers, and switches. The Sourcefire Defense Center interacts with those devices through a sophisticated Remediation API. Security analysts specify standard actions to be taken by Cisco PIX and Check Point® firewalls or Cisco Routers.

Correct Faster and Smarter to Eliminate Possible Exploitation

Responding to new vulnerabilities and threats often means interaction with the full security and management infrastructure of an organization. To make this easier, the Sourcefire Remediation API supports interaction with a broad range of applications and systems – virtually any system that supports programmatic integration including active scanners if a “surgical scan” is needed, patch management systems, and configuration management systems.

The most significant benefit from this integration comes from the ability to enforce configuration management policy by invoking patch management systems, like Citadel, Shavlik, PatchLink™ or BigFix®, to update potentially vulnerable systems discovered by Sourcefire RNA. Since so many security threats are directly related to configuration errors (leaving unneeded ports open, systems unpatched, or unnecessary services operating), the power to automatically issue commands to rectify these potential vulnerabilities helps prevent problems before they occur.

SOURCEFIRE 3D — THE POWER OF AUTOMATION

How can you immediately and dramatically improve security without adding a single headcount?

Leverage the power of automation inside Sourcefire. You can easily and quickly customize your workflows and reports. They'll be generated automatically and emailed and/or posted to your intranet, for example, on a daily basis.

Management of security policies can be enforced automatically. In addition, compliance reports can automatically be generated and emailed to your auditors.

Minimize IDS and IPS tuning through RNA context intelligence.

You also benefit from automated responses that are policy-based. See a change occurring on your network, such as an unauthorized desktop application? You can fully automate your response according to your exact policy specifications, using the ABC's of Defense – real-time responses for real-time risks.

Enterprise Ready

Sourcefire offers a highly scalable solution, providing all the features you need for large scale, enterprise deployments. In fact, Sourcefire received the highest score of "Exceptional" from Network World for scalability.

The Sourcefire Defense Center provides automated failover support by offering a high availability mode that allows two Defense Centers to manage the same sensor or group of sensors. In this case, one would act as the primary and one as the secondary Defense Center.

In addition, Sourcefire offers dynamic load balancing across Intrusion Sensors that are deployed on the same network segment. Administrators can easily create groups and apply common policies across the sensor group. Together, these features bring a high degree of continuity of operations across the enterprise.

Given that enterprises often have large, disperse security teams, Sourcefire offers several levels of user-specific access to allow you to determine exactly what access to allow including maintenance access, data access, restricted data access, rule access, and admin access.

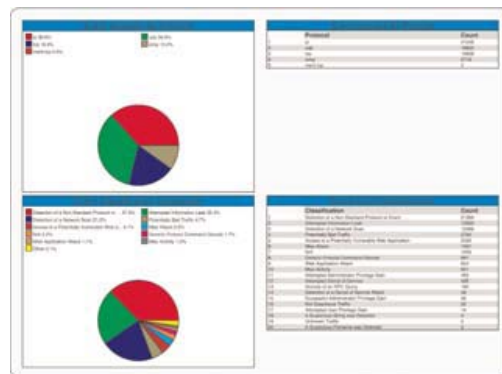
Plug-n-Protect

All Sourcefire appliances come preconfigured, designed to be up and running in less than 15 minutes. No software installation is required. These 'Plug-n-Protect' appliances come with built-in data management and hardened operating systems. The user interfaces have been designed by security engineers for security engineers. To start, simply connect to the network and boot. And going forward, you're assured of low overhead and the best TCO in network security.

AUTOMATED, FLEXIBLE REPORTING MEETS REAL WORLD DEMANDS

The Sourcefire 3D System offers a highly flexible and customized reporting system, providing users with complete control over each report's contents and display of the data.

This flexibility enables administrators to define templates for management reports, compliance reports, analyst reports, etc. Reports can be easily created from custom workflows as well. Once created, reports can be named, saved and scheduled to run for any time interval or relative time interval. Report outputs include CSV, HTML, PDF and text reports. What's more, reports can be fully automated to go direct to one or multiple recipients.



A NEW WORLD, A NEW DEFINITION OF SECURITY

We live in a new world. A new type of security is necessary.

Today's most dynamic, forward-looking organizations realize the dissolving perimeter and the shortfalls of traditional network security methods mandate a new, more effective approach.

Sourcefire, with its revolutionary 3D approach, (Discover, Determine and Defend) and RNA technology, is driving a new definition of network security, delivering an innovative solution that would not have been possible even a few short years ago.

By tightly integrating and correlating the threat information provided by Sourcefire Intrusion Sensors and Agents with the network intelligence provided by Sourcefire RNA Sensors, the Sourcefire Defense Center easily prioritizes millions of security events to determine those most critical to your organization, and takes the appropriate action.

With real-time network defense, potential network weaknesses are proactively identified and risks are removed well before they are exploited ... and attack and threat management solutions are poised to quickly respond, mitigate, and remediate attacks from all threat vectors.

Bottom line: only Sourcefire addresses the entire real-time network defense challenge, providing all the benefits of the most complete, end-to-end network security solution for the real world.

For more information

Contact your local Sourcefire Representative, visit www.sourcefire.com, or call 800.501.6008.



www.sourcefire.com

Corporate Headquarters
 9212 Berger Road
 Suite 200
 Columbia, MD 21046
 800.501.6008 | 410.290.1616
 fax 410.290.0024

European Headquarters
 400 Thames Valley Park Drive
 Thames Valley Park
 Reading, RG6 1PT
 +44 (0) 118 965 3555
 +44 (0) 118 965 3554 fax



supplied and supported by

Phoenix Datacom
www.phoenixdatacom.com
01296 397711
info@phoenixdatacom.com