



Sourcefire IPS™ (Intrusion Prevention System)



Unparalleled Intrusion Detection and Prevention

It's 3 am. A hacker is hard at work trying to break into your network. Not for kicks, but for dollars. Is your network secure? Learn why more organizations depend on SNORT® than any other intrusion prevention technology worldwide, and why thousands of enterprises rely on Sourcefire's award-winning, ICSA-certified IPS to secure networks before, during, and after an attack.

Key Sourcefire IPS Capabilities

- Industry-standard Snort IPS detection engine
- Library of >14,000 Snort rules
- Open rules language—view, edit, & create
- Inline IPS & passive IDS modes
- Reports, alerts, & dashboards
- Multiple default IPS policies
- Third-party integration APIs
- Packet-level forensics
- Sophisticated, customizable workflows
- LDAP & RADIUS support
- Plug-n-Protect features
- High availability features

Plug-n-Protect Features

- Purpose-built IPS appliance
- Easy installation & configuration
- Adaptive IPS (automated IPS tuning)
- Automated VRT rule updates

"I'm convinced RNA was the differentiating factor that made Sourcefire the obvious choice. Even without RNA, the Sourcefire IPS would have been our preference, but the RNA component makes us work much more efficiently."

Greg Clayton, Assistant VP and Network Security Manager, BankersBank Card Services

EMBRACE THE NEXT GENERATION OF INTRUSION PREVENTION

Stop Threats in Their Tracks

Built on Snort, the de facto standard for intrusion detection and prevention (IDS/IPS), the award-winning Sourcefire 3D™ System provides customers with a "Discover, Determine, Defend" framework, enabling you to discover threats accurately as they occur, determine their impact and severity, and defend your network by stopping threats in their tracks. Whether deployed at the perimeter, in the DMZ, in the core, or at critical network segments, and whether placed in inline or passive mode, Sourcefire's IPS appliances protect your network against worms, Trojans, spyware, port scans, buffer overflow attacks, zero-day attacks, and much, much more.

Plug-n-Protect Simplicity

Today's resource-tapped IT organizations must work smarter, not harder, to defend against today's dynamic threat landscape. The plug-n-protect nature of Sourcefire's purpose-built IPS appliances enables customers to easily install and configure their IPS, with minimal effort and training. For customers with limited IT security resources, the process of tuning an IPS can be fully automated to ensure that each IPS is continuously optimized to protect your changing network environment.

Sourcefire's IPS Meets Your Needs—Today and Tomorrow

Most providers offer a "one-size-fits-all" IPS, but Sourcefire is different. Our solution is divided into three simple customer protection phases—IPS, Adaptive IPS, and Enterprise Threat Management (ETM)—with each phase building upon the benefits and features of the previous one, adding capabilities to optimize a company's network protection.

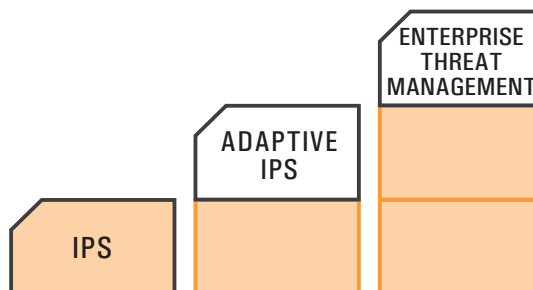


Figure 1. Unlike other IPS vendors that provide a "one-size-fits-all" IPS, Sourcefire's solution is divided into three customer protection phases that scale with your organization's needs.

IPS Key Benefits

- Best-in-class intrusion defense
- Easy to use
- Extensive analytics
- Powerful reporting
- Unrivaled scalability

Snort—the De Facto IPS Standard

- Invented in 1998 by Martin Roesch, Sourcefire Founder & CTO
- Most widely-deployed IPS technology worldwide
- Used by 82% of Fortune 100
- Used by more than half of Fortune 500
- Snort community has become an entire ecosystem:
 - » >3 million downloads
 - » >200,000 registered users
 - » Dozens of Snort books published
 - » Classes taught at colleges & universities
 - » User groups
 - » Discussion lists & forums

Sourcefire Zero-Day Protection Example:

Sourcefire Protects Against Microsoft Animated Cursor Exploit Over Two Years in Advance

- **January 11, 2005** – VRT learns of Windows animated cursor vulnerability
- **January 12, 2005** – VRT publishes Snort rule (3079)
- **November 16, 2006** – Malware discovered in the wild
- **March 31, 2007** – Microsoft issues security advisory (935423)
- **April 3, 2007** – Microsoft releases patch (MS07-017)
- **April 3, 2007** – Sourcefire customers protected over 2 years in advance

IPS—THE FOUNDATION OF THE SOURCEFIRE 3D SYSTEM

Snort – the De Facto Standard for Intrusion Prevention



Designed for customers with basic intrusion prevention needs, Sourcefire's IPS phase provides the foundation for all Sourcefire customer protection phases. Built on the legacy of the Snort rules-based detection engine, Sourcefire's IPS uses a powerful combination of vulnerability- and anomaly-based inspection methods to analyze network traffic and prevent critical threats from affecting your network.

The Sourcefire IPS contains multiple default policies for out-of-the box blocking, drawing from a library of more than 14,000 open Snort rules. Open rules allow customers to verify that rules address the vulnerabilities for which coverage is claimed and to create new rules or modify existing ones to protect custom applications and systems. Sourcefire's IPS can be deployed in inline blocking and/or passive alerting modes, and can remediate traffic to external devices, such as firewalls, routers, patch management systems, and more. Powered by the Snort detection engine, Sourcefire IPS excels with detailed packet-level forensics and sophisticated, customizable workflows for investigating security events as they occur.

Snort, created by Sourcefire, is the de facto standard for intrusion prevention with more than 3 million downloads and over 200,000 registered users. More organizations rely on Snort than any other intrusion prevention technology worldwide. Over the past decade, the Snort community has grown to become an entire ecosystem, from user groups, to books, to classes taught at hundreds of colleges and universities. More IT security professionals are familiar with Snort than any other IPS technology in the market. Sourcefire customers benefit from this extensive Snort ecosystem on day one.

Protection Against Known and Unknown Threats

The Sourcefire Vulnerability Research Team (VRT) works around the clock to ensure Sourcefire commercial customers and open source Snort users are protected against both known and unknown threats. The VRT leads the IPS industry in addressing Microsoft Tuesday vulnerabilities on the same day they are announced.

It's often the unknown, zero-day threat that can be the most damaging. That's why Sourcefire publishes vulnerability-based Snort rules. Snort rules offers protection against any possible exploitation of a vulnerability. An IPS that relies primarily on exploit-based signatures provides little-to-no protection against zero-day threats. This was illustrated in 2007 when Sourcefire protected its customers more than two years in advance of a new, zero-day Microsoft Animated Cursor exploit.

Sourcefire's IPS appliances provide comprehensive threat protection against:

- Worms
- Trojans
- Backdoor attacks
- Spyware
- Port scans
- VoIP attacks
- IPv6 attacks
- DoS attacks
- Buffer overflows
- P2P attacks
- Statistical anomalies
- Protocol anomalies
- Application anomalies
- Malformed traffic
- Invalid headers
- Blended threats
- Zero-day threats
- TCP reassembly & IP defragmentation

High Availability Features

- Dual power supplies
- Fail-open ports
- RAID drives
- High availability configuration options



The Industry's First-Shipping 10Gbps IPS

Sourcefire's purpose-built, ICSA-certified 3D Sensors are available with throughputs from 5Mbps up to the industry's first-shipping 10Gbps IPS appliance. Sourcefire 3D Sensors are available with critical fault-tolerant features, such as fail-open copper and fiber ports, dual power supplies, and RAID drives, and each 3D Sensor supports an array of high availability configuration options.













					
MODEL	3D500	3D1000	3D2000	3D2100	3D2500
Supported Line Speed (IDS/IPS)	5Mbps	45Mbps	100Mbps	250Mbps	500Mbps
					
MODEL	3D3500	3D3800	3D4500	3D5800	3D9800
Supported Line Speed (IDS/IPS)	1Gbps	1.5Gbps	2Gbps	4Gbps (3Gbps inline)	up to 10Gbps

Table 1. Sourcefire 3D Sensor Product Family

Sourcefire Defense Center Key Capabilities

- Centralized event monitoring & sensor management
- Customizable dashboards with numerous widgets
- Email & SNMP alerts
- Sophisticated & customizable reporting
- Automated VRT rules updates
- Master Defense Center (MDC) scalability

Centralized Event Aggregation and Analysis

Sourcefire's IPS phase is intended for customers with multiple Sourcefire 3D Sensors that require centralized event aggregation and analysis. Using the feature-rich, yet easy-to-use Sourcefire Defense Center™ (DC) management console, customers can analyze events, configure and push IPS policies, automatically download and apply Snort rule updates, and more. For larger deployments, customers can leverage Sourcefire's Master Defense Center (MDC) technology to manage multiple DCs and hundreds of 3D Sensors across their entire organization.

Powerful Reports, Alerts, and Dashboards

Sourcefire Defense Center provides customers with powerful reports, alerts, and dashboards. Customers can leverage a variety of pre-defined report templates or create custom reports to meet the needs of any organization. They can receive alerts in the form of email messages or SNMP alerts. And customers can create fully customized dashboards with dozens of drag-n-drop "widgets" that display critical information in the form of tables and graphs.

“During our testing, we threw lots of different types of traffic at a couple of leading IPS vendors. One IPS vendor produced alerts on 80% of the traffic we threw at it, but Sourcefire didn’t produce a single alert. We brought the Sourcefire engineer in because we thought it wasn’t working, but he said that it wasn’t producing alerts because the boxes being attacked in the test weren’t vulnerable to what was being thrown at it...he showed me proof that it was working, which was nice.”

**Jeremy Pratt, Network Manager,
L.A. Times**

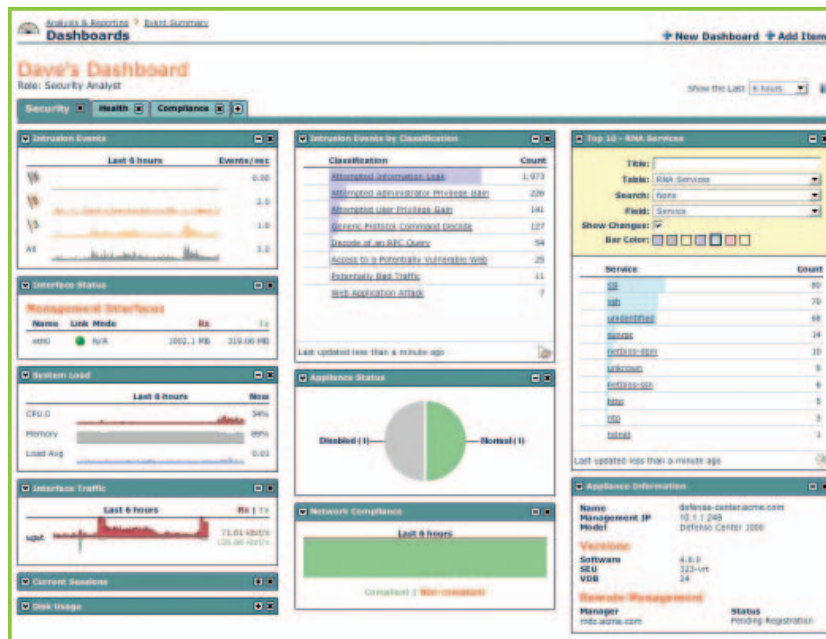


Figure 2. The Sourcefire Defense Center dashboard is fully customizable and provides numerous drag-n-drop widgets that display critical security event information.

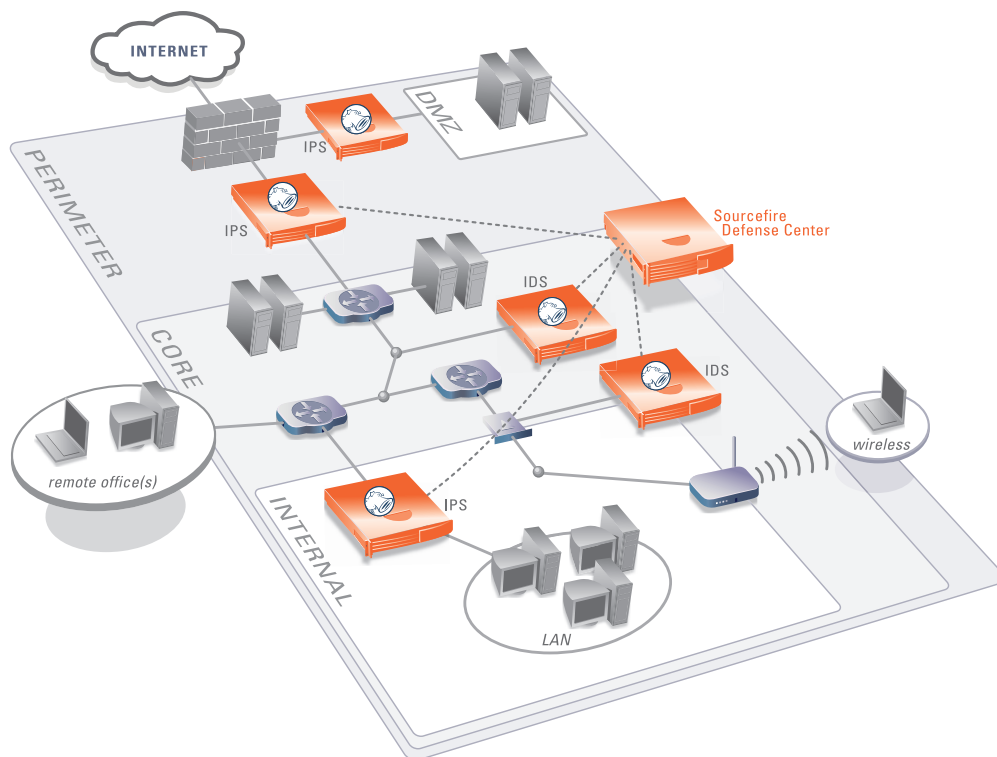


Figure 3. Sourcefire fully supports a Defense-in-Depth intrusion prevention strategy by allowing Sourcefire 3D Sensors to be positioned at the perimeter, in the DMZ, in the core, and at critical internal network segments. Sourcefire Defense Center orchestrates all event aggregation, analysis, and IPS policy management.

Adaptive IPS Key Benefits

- Know what's on your network—in real time, all the time
- Save time by significantly reducing quantity of “actionable” security events
- Reduce risk by ensuring IPS is always optimized to protect your dynamically changing network
- Helps organizations with small network security staffs effectively protect their networks

Sourcefire RNA Key Capabilities

- 24x7, passive, real-time network intelligence
- Provides real-time network/device, state & behavior context to IPS
- Contributes to automated impact assessment
- Supports automated IPS tuning
- Contributes to IT policy compliance

“Events requiring manual reviews have been reduced from over 20,000,000 per month down to approximately 2,000 per month. By using the Sourcefire IPS, we have been able to reduce the time and number of staff who are dedicated to analyzing IDS data, re-utilizing these SOC resources for other activities.”

**Network Security Analyst,
Global 500 Software Provider**

ADAPTIVE IPS—DYNAMIC DEFENSES FOR DYNAMIC NETWORKS

Sourcefire RNA™—Real-Time Passive Network Intelligence

Although Sourcefire’s IPS phase provides exceptional network threat protection, the Adaptive IPS phase is where Sourcefire surpasses all other IPS systems. Sourcefire’s Adaptive IPS phase is designed to help IT organizations perform more optimally and is ideal for companies with small IT security staffs. IT security professionals don’t have time to constantly “tune” their IPSes as their networks change. And they don’t have time to sift through hundreds or thousands of security events each day to try to figure out which events matter most. IT security organizations need dynamic, intelligent network defenses to defend their highly dynamic networks against today’s dynamic threats.

The technology that provides context to the Sourcefire IPS is called Sourcefire RNA (Real-time Network Awareness). Analogous to passive SONAR on a ship, RNA provides 24x7 passive network intelligence and presents a real-time inventory of all operating systems (OSes), services, protocols, and potential vulnerabilities that exist on your network. By adding the RNA module to your 3D Sensors, real-time/all-the-time network intelligence is incorporated into the IPS, and the process of tuning the IPS and assessing security events can be fully automated.

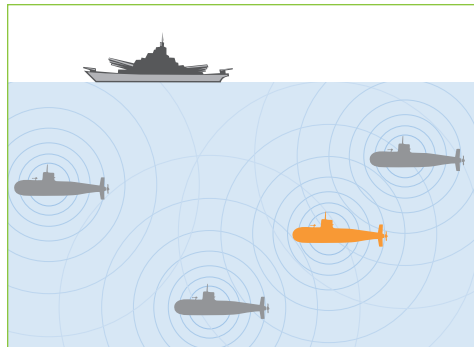


Figure 4. Sourcefire RNA works like passive SONAR on a ship, enabling you to identify friendly and non-friendly network behavior through passive network discovery 24 hours a day, seven days a week.

Automated IPS Tuning and Optimization

Sourcefire is the only network security provider to offer an Adaptive IPS solution, which is why the company is regularly depicted by leading market research analysts as the most visionary leader in the IPS industry. The following table depicts key capabilities found in Sourcefire’s Adaptive IPS phase:

Impact Flag Assessments	Threat intelligence is automatically correlated against real-time target host intelligence to determine the relevance and impact of the attack. Actionable events are typically reduced by 99% or more.
RNA-Recommended Rules	As your network evolves, Sourcefire takes the guesswork out of determining which Snort rules to enable and disable. RNA recommends relevant Snort rules based on the network it’s protecting. Snort rules can be enabled with or without human intervention.
Adaptive Traffic Profiling	Prevents IPS evasions by enabling the IPS to model segmented and fragmented traffic in the same manner the host OS would see it.
Non-Standard Port Handling	If traffic using a non-standard port is detected, such as HTTP on port 8080 (rather than port 80), applicable Snort rules will automatically be re-configured to monitor related traffic using both standard and non-standard ports.

Table 2. Sourcefire’s Adaptive IPS phase incorporates real-time network intelligence to prioritize security events and automate the process of tuning your IPS.

The use of Sourcefire's Adaptive IPS results in massive elimination of false positives and false negatives, less manual event investigation and IPS tuning by your IT security staff, lower potential for network downtime, and lower cost of operations. By having real-time knowledge of what's running on your network, the 3D System saves you time and effort and maximizes protection of your dynamically changing network.

ETM Key Benefits

- Quickly link users to security & compliance events
- Easily monitor & enforce IT policy compliance with compliance white lists
- Detect internal anomalies to baselined "normal" traffic
- Monitor bandwidth consumption
- Troubleshoot network outages & performance degradations

Sourcefire RUA Key Capabilities

- Links users to security & compliance events
- Support for Active Directory & LDAP
- Provides full names, contact info, & more
- Resolve incidents in a fraction of the time

ENTERPRISE THREAT MANAGEMENT (ETM)—FULL DEFENSE BEFORE, DURING, AND AFTER THE ATTACK

ETM—A Fully Integrated Approach for Complete Protection

Sourcefire's Enterprise Threat Management (ETM) solution provides full functionality to defend your network before, during, and after an attack. ETM is the combination of the world's most powerful attack detection engine, enhanced by real-time network intelligence provided by RNA, completed by a system that gives you round-the-clock knowledge of any behavioral change of your critical systems. ETM allows the Sourcefire IPS to filter out the noise and tune itself so you can quickly react to network changes and compromises. Just enable certain RNA features and add Sourcefire RUA™ (Real-time User Awareness) to your 3D Sensors, and you have a complete solution to protect your network at any point of the attack continuum.

Sourcefire RUA—Link User Identity to Security and Compliance Events

Sourcefire is the only IPS provider to link user identity to security and compliance events. Rather than sifting through Active Directory, LDAP, and DHCP log files to determine the owner of a host under attack, Sourcefire RUA links both Active Directory and LDAP usernames to IP addresses involved in security and compliance events. By clicking on the username, the security analyst is presented with the user's full name, department, and contact information. By leveraging Sourcefire's ETM approach, RUA enables incidents to be resolved in a fraction of the time it would take with an IP address alone.

Reduce Risk Before the Attack

With the ETM phase, customers can reduce the risk in multiple ways before the attack occurs. First, with RNA's change management capability and powerful Policy and Response (P&R) engine, IT can be notified when a new host appears on the network and/or when an existing host changes its approved configuration. Second, once RNA has inventoried network assets into its Network Map, users can create compliance white lists of approved host assets by indicating the OSes, services, applications, and protocols that can and/or cannot be used on a particular network, plus create custom compliance rules to monitor and enforce your IT acceptable-use policies. And last, by narrowing the list of approved applications and attributes, IT can better defend against both known and unknown attacks. By leveraging Sourcefire's compliance capabilities, fueled by RNA, IT can harden network assets by shutting down unapproved systems, turning off unnecessary ports, and by applying key patches and service packs before the attack occurs.

Improve Network Security and Protect Your Organization

Not all threats pass through your network's perimeter. Some threats are hand-carried on laptops right through the front door of your building. An IPS can only protect what it can see. By leveraging RNA to baseline "normal" traffic on your network, you can leverage Sourcefire to detect anomalies, such as malware propagating from host to host. ETM also enables customers to monitor bandwidth consumption and troubleshoot network outages and performance degradations.

"Mapping a username to an IP address was taking us away from a backlog of other important tasks. By using Sourcefire RUA, what used to take up to an hour now takes just a second or two. I feel much better knowing that I can contact a user immediately in the event they are affected by a network attack."

**Tamara Fisher, Security Engineer,
AutoTrader.com**

Sourcefire 3D System Components

- Sourcefire 3D Sensor
 - » Sourcefire IPS Module
 - » Sourcefire RNA Module
 - » Sourcefire RUA Module
- Sourcefire Defense Center

"Sourcefire's 3D System offers a highly sophisticated intrusion protection solution, which we found particularly easy to install and deploy. We were very impressed with the extensive policy-based responses on offer and the remarkable amount of information it is capable of gathering about internal and external systems."

**Dave Mitchell, Product Reviewer,
Computing Security Magazine
Product Review**

TAKE THE NEXT STEP TO PROTECT YOUR NETWORK

Sourcefire is the only IPS provider offering dynamic defenses against the dynamic threats aimed at your dynamic network. Sourcefire's unique capabilities include:

- A three-phased customer protection solution (IPS, Adaptive IPS, and Enterprise Threat Management) that scales with the needs of your company's requirements
- Best-in-class intrusion defense
- 24x7, passive network intelligence through Sourcefire RNA
- Real-time, automated intrusion event impact assessment
- Automated IPS tuning based on actual network assets protected through Adaptive IPS
- User identity tracking through Sourcefire RUA
- An integrated system managed from a single, easy-to-use Sourcefire Defense Center management console
- "Manager of managers" enterprise-class scalability through Sourcefire's Master Defense Center technology

IPS	ADAPTIVE IPS	ETM
<ul style="list-style-type: none"> • Best-in-class intrusion defense • Easy to use for both novice & experienced users • Extensive packet-level forensics • Fully customizable reports, alerts, & dashboards 	<p>All IPS benefits, plus:</p> <ul style="list-style-type: none"> • Know what's on your network—in real time, all the time • Save time by significantly reducing quantity of "actionable" events • Reduce risk by ensuring IPS is always optimized to protect your dynamically changing network 	<p>All Adaptive IPS benefits, plus:</p> <ul style="list-style-type: none"> • Quickly link users to security & compliance events • Easily monitor & enforce IT policy compliance with compliance white lists • Detect internal anomalies to baselined "normal" traffic, monitor bandwidth consumption, & troubleshoot network outages & performance degradations

Table 3. Sourcefire Customer Protection Phase Benefits. Sourcefire's solution is available in three protection phases, with each phase adding capabilities to optimize a company's network protection.

To learn more about Sourcefire's award-winning IPS solutions, visit our Web site at www.sourcefire.com or contact Sourcefire or a member of the Sourcefire Solutions Network™ today.



KNOW MORE

©2008 Sourcefire, Inc. All rights reserved. SOURCEFIRE®, SNORT®, the Sourcefire logo, the Snort and Pig logo, SECURITY FOR THE REAL WORLD™, SOURCEFIRE DEFENSE CENTER™, SOURCEFIRE 3D™, SOURCEFIRE RNA™, SOURCEFIRE RUA™, DAEMONLOGGER™, CLAMAV™, SOURCEFIRE SOLUTIONS NETWORK™, and certain other trademarks and logos are trademarks or registered trademarks of Sourcefire, Inc. in the United States and other countries. Other company, product and service names may be trademarks or service marks of others.