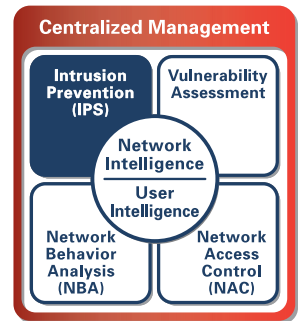


## Sourcefire IPS™

### Intrusion Prevention for Enterprise Threat Management (ETM)

By integrating Intrusion Prevention System (IPS), Network Behavior Analysis (NBA), Network Access Control (NAC), and Vulnerability Assessment technologies – all under one management console – ETM is drawing the praises of risk, compliance, and security professionals who are finding it to be a more effective and efficient approach. Within Sourcefire's ETM solution, the unsurpassed network protection Sourcefire IPS™ delivers is correlated and unified with network and user intelligence to ensure full, continuous protection.



#### Sourcefire IPS at a glance:

- Powered by Snort®<sup>®</sup>, the industry-standard IPS detection engine
- Inline and passive deployments
- High performance at throughputs and line speeds up to 10 Gbps
- Comprehensive, accurate protection against threats
- Multiple default IPS policies covering more than 3,000 rules for out-of-the-box blocking
- Adaptive IPS, which leverages network intelligence for automatic tuning
- Detailed forensics providing powerful event analysis
- Sophisticated and customizable reporting system
- Open rules language – view, edit, and create rules

#### EMBRACE THE NEXT GENERATION OF INTRUSION PREVENTION

Whether deployed at the perimeter, the core, or remote offices, Sourcefire IPS™ appliances protect against spyware, worms, Trojans, port scans, buffer overflow attacks, protocol anomalies, malformed traffic, invalid headers, zero-day attacks, and more. Sourcefire IPS delivers the capabilities you need to efficiently and effectively protect your network, including:

- ▶ IPS appliances with high performance and scalability, from 5 Mbps up to 10 Gbps throughputs
- ▶ Out-of-the-box blocking, with recommended IPS rule sets covering more than 3,000 rules
- ▶ Adaptive IPS, which uses network intelligence to stop evasions and reduce false positives
- ▶ IPv6 support, including protection against attacks in IPv6 traffic

#### STOP THREATS IN THEIR TRACKS

Built on the legacy of the award-winning Snort® rules-based detection engine created by Sourcefire®, Sourcefire IPS uses a powerful combination of vulnerability-based, protocol, and anomaly-based inspection methods – at throughputs up to 10 gigabits per second – to stop threats before they impact your network. Deployable in inline and/or passive modes, Sourcefire IPS analyzes network traffic and prevents critical threats from affecting your network, and integrates with the Sourcefire 3D System to contain threats by remediating to other devices, including firewalls and routers.

#### DRAMATICALLY REDUCE RISK AND FALSE ALARMS

Worried about the next network threat? It's time to find out what many Fortune 100 companies already know – Sourcefire IPS can eliminate the need to investigate events that do not impact customer networks. Sourcefire IPS, a cornerstone of the Sourcefire 3D System, leverages network intelligence collected by the 3D System to enable accurate blocking decisions while preventing false positives and negatives.

#### TAKE ADVANTAGE OF 10 GIGABIT THROUGHPUT



Sourcefire 3D9800 - intrusion prevention at 10Gbps

Sourcefire offers intrusion prevention at line speeds and throughputs up to 10 Gbps to handle today's bandwidth requirements at the core. In high-traffic, latency-sensitive environments, Sourcefire IPS lets you monitor multiple networks from one central core, reducing the effort and complexity of threat management. The 10 Gbps Sourcefire 3D9800 supports both copper and fiber networks, with high port density and a highly redundant, scalable architecture.



## Sourcefire IPS protects against:

- Worms
- Trojans
- Port scans
- Buffer overflow attacks
- Denial-of-service attacks
- Spyware
- Protocol anomalies
- Malformed traffic
- Invalid headers
- VoIP attacks
- IPv6 attacks
- Fragmentation attacks and evasions
- Zero-day attacks

## USE ADAPTIVE IPS FOR MORE ACCURATE INTRUSION PREVENTION

As part of Sourcefire's ETM approach, Sourcefire IPS can use Sourcefire RNA™ to automatically provide a set of recommended rules based on the operating systems and services actually seen in customer environments. This approach leverages RNA intelligence to eliminate the effort of manual tuning.



**Adaptive IPS and RNA Recommended Rules help users to easily tune detection policies for their specific environments.**

## COMPLY WITH IPV6 REQUIREMENTS

"Events requiring manual reviews have been reduced from over 20,000,000 per month down to approximately 2,000 per month. 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**

Sourcefire's commitment to IPv6, the newest version of the Internet Protocol, enables you to extend the intrusion prevention capabilities of Sourcefire IPS into next-generation networks. Support for IPv6 traffic includes full packet analysis of regular and tunneled attacks, as well as features to stop evasions and normalize traffic in IPv6 networks.

## RELY ON SOURCEFIRE FOR UP-TO-DATE PROTECTION

The Sourcefire Vulnerability Research Team (VRT) – a group of seasoned industry experts providing coverage and rules in advance of actual threats – works to discover, assess, and respond to the latest trends in hacking activity, worm outbreaks, and vulnerabilities. Customers depend on the VRT to provide an up-to-date, recommended rule set that offers full protection against the very latest reported vulnerabilities.

## DEPLOY EASILY AND MANAGE CENTRALLY

Sourcefire IPS appliances can be used in both small and large deployments, from single sensors to enterprise management across large, distributed networks. Sourcefire Defense Centers can collect events and centrally manage hundreds of IPS appliances from one central location, and their policy management and reporting capabilities make administration painless. Installing and deploying sensors is simple thanks to Sourcefire's easy-to-use setup wizards and Adaptive IPS self-tuning technology.

## TAKE THE NEXT STEP TO PROTECT YOUR NETWORK

For more information about the Sourcefire 3D System, including Sourcefire IPS, contact your Sourcefire sales representative or call 1.800.501.6008.

[www.sourcefire.com](http://www.sourcefire.com)

SOURCEFIRE®, SNORT®, the Sourcefire logo, the Snort and Pig logo, SECURITY FOR THE REAL WORLD™, SOURCEFIRE 3D™, SOURCEFIRE DEFENSE CENTER™, SOURCEFIRE IPS™, SOURCEFIRE MASTER DEFENSE CENTER™, ESTREAMER™, SOURCEFIRE RNA™, SOURCEFIRE RUA™, DAEMONLOGGER™, OFFICECAT™ NETWORK USAGE CONTROL™ (NUC) and certain other trademarks and logos are trademarks or registered trademarks of Sourcefire, Inc. in the United States and other countries.