



Sourcefire® Solutions Overview

Headlines constantly remind us that network threats are growing at an alarming rate and attacks are becoming more sophisticated. What's less obvious is what to do about it. Every network is unique, and you need technology and solutions that meet your specific needs. Look no further.

Sourcefire is a world leader in intelligent cybersecurity solutions. Our flagship family of intrusion detection and prevention systems (IDS/IPS) lies at the heart of our security solutions portfolio. We offer a range of IPS solutions as well as several complementary products to protect your network.

WHY SOURCEFIRE?

We offer the best protection—period. As the creator of Snort®, the de facto standard for intrusion detection and prevention, our roots are in security. More organizations rely on Sourcefire IPS technology than any other technology on the market. Don't just take our word for it, here's proof from the industry:

- Best detection in the Network IPS Comparative Group Test conducted by NSS Labs
- Leader in the Gartner Magic Quadrant for Network IPS Appliances
- Best IDS/IPS from *SC Magazine*
- ICASA Labs Certified



IPS SOLUTIONS PORTFOLIO

Your network is unique, which is why Sourcefire offers three distinct IPS solutions designed to address your security needs. For large networks with dedicated security teams, Sourcefire Next-Generation IPS (NGIPS) includes network, application, behavior, and identity awareness for improved visibility and automation. For security teams that need robust protection features without awareness, we offer Sourcefire IPS™. And for network administrators and IT generalists, Sourcefire IPSx™ is designed to secure networks and meet compliance mandates with minimal administrative attention.

Choose the IPS that Meets Your Needs:

Features	IPSx	IPS	NGIPS
IPS Detection & Blocking	✓	✓	✓
Snort Rules & SEUs	✓	✓	✓
Reporting & Dashboard	✓	✓	✓
Policy Management	✓	✓	✓
Advanced Policy Management		✓	✓
Snort Rule Editing		✓	✓
Custom Workflows & Tables		✓	✓
Impact Assessment			✓
Automated Tuning			✓
Host Profiles & Network Map			✓
Network Behavior Analysis			✓
Application Monitoring			✓
User Identity Tracking			✓

All Sourcefire IPS Solutions Offer the Following Benefits

Powered by Snort



Created by Martin Roesch, the founder of Sourcefire, Snort is the single most widely deployed intrusion detection and prevention technology in the world. With nearly 4 million downloads and over 326,000 registered users, the Snort community is a security ecosystem of user groups, books, and classes taught at colleges and universities worldwide. Each commercial Sourcefire IPS integrates the power of Snort:

- Open architecture provides the ability to view, edit, and create Snort rules
- Advanced threat intelligence leveraging the collaboration of the Snort community
- Built-in Data Leakage Prevention (DLP) helps you to identify unauthorized transmission of sensitive data, including credit card numbers, social security numbers, and more

Backed by Sourcefire Vulnerability Research Team™ (VRT)



The Sourcefire VRT is a group of leading security experts that maintain the open source community rule set and develop the official Snort rules used by the Sourcefire IPS solutions. The Sourcefire VRT:

- Discovers, assesses, and responds to the latest trends in hacking activities, intrusion attempts, and vulnerabilities to stay ahead of threats
- Develops vulnerability-based rules to protect you before exploits are in the wild
- Delivers same-day protection for critical Microsoft vulnerabilities

Seamless Third-party Integration

Because of its open source flexibility, the Sourcefire IPS solutions integrate quickly and easily with a variety of third-party technologies including vulnerability management systems, security information and event management (SIEM) applications, network access control (NAC), network forensics, and more. System interoperability provides numerous benefits:

- Extends your investment without major effort or upgrades
- Simplifies your security deployment and planning activities
- Provides the flexibility to interoperate security in any IT environment

Sampling of Threat Detection Provided by All Sourcefire IPS Solutions

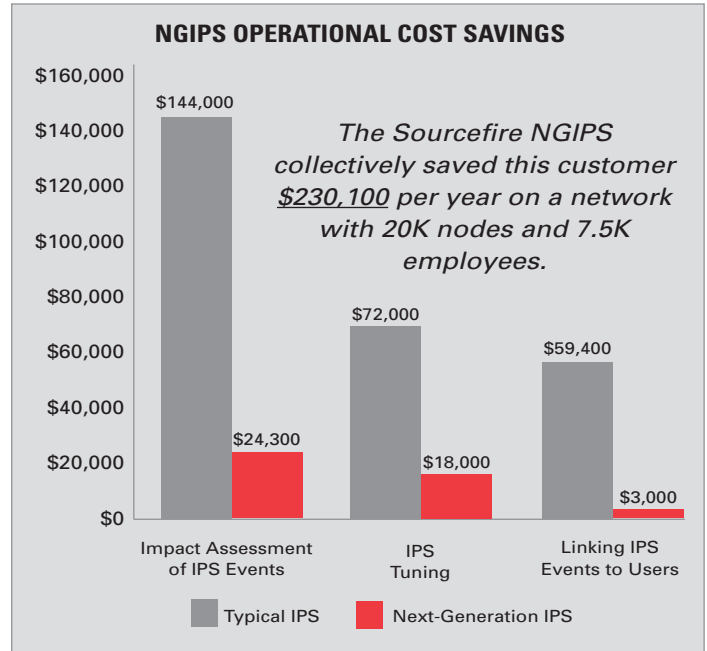
- DoS attacks
- Buffer overflows
- P2P attacks
- Worms
- Trojans
- Backdoor attacks
- Spyware
- Invalid headers
- Blended threats
- Rate-based attacks
- Zero-day threats
- Port scans
- VoIP attacks
- IPv6 attacks
- Statistical anomalies
- Protocol anomalies
- Application anomalies
- Malformed traffic
- TCP segmentation and IP fragmentation

A Closer Look at NGIPS

Sourcefire Next-Generation IPS raises the bar for IPS technology by integrating real-time contextual awareness into its inspection. The system gathers information about network and host configurations, applications and operating systems, user identity, and network behavior and traffic baselines. By having the utmost visibility into what's running on your network, NGIPS offers event impact assessment, automated IPS tuning, and user identification to significantly lower the total cost of ownership.

Sampling of Application Awareness Provided by NGIPS

- AIM
- Clarizen
- eHarmony.com
- eTrade
- Facebook
- Gmail
- Jabber
- Lotus
- Match.com
- Myspace.com
- NetBotz
- Oracle
- Outlook
- Salesforce.com
- Scottrade
- Skype
- Twitter
- WebEx
- Windows Messenger
- Yahoo Mail



Source: Data from Appendix A of SANS White Paper, "Calculating TCO on Intrusion Prevention Technology." March 2010

HOW THE NGIPS USES CONTEXTUAL AWARENESS TO FUEL INTELLIGENT AUTOMATION

Network Awareness

Continual network visibility, including new hosts entering the network, network and host configuration changes, and IT policy compliance.

Automated Tuning & Impact Assessment Reduces Costs

Automatically determine threat relevancy, threat severity, and self-tune to defend against attacks; increasing security, maximizing throughput, and reducing operational costs.

Application Awareness

Identify application traffic that is traversing the network to define application policies and management.

Application Policy Management Improves Visibility

Control your acceptable use policy (AUP) by automatically identifying the types of applications on your network and recognizing policy violations.

Identity Awareness

Improve audit controls and regulatory compliance by linking events directly to individual users.

User Identity Tracking Speeds Incident Resolution

Automatically link Active Directory and LDAP users to events so you know exactly who to contact when time is of the essence.

Behavior Awareness

Detect and quarantine internal threats by establishing "normal" traffic baselines and detecting network anomalies.

Network Behavior Analysis Increases Network Visibility

Monitor bandwidth consumption, troubleshoot network performance degradation, and automatically quarantine internal hosts with malware before it spreads.

IPS and NGIPS Hardware and Technology

Sourcefire IPS and NGIPS solutions take advantage of the best hardware technology in the industry, providing IPS inspected throughput options ranging from 20Gbps down to 5Mbps. Upgrading Sourcefire IPS to NGIPS is as easy as adding a license to your software.

The new Sourcefire 3D8000 Series appliances, our highest-throughput sensors, offer interface modularity, expandability, and scalability. Modularity provides a low entry-price and enables you to choose the number of ports and media type for your network and swap out interface types as needed. Expandability gives you the option to pay for network interfaces as you grow. Scalability enables you to add additional processing power through appliance stacking.



At the heart of the new 3D8000 Series appliances lies the breakthrough FirePOWER™ acceleration technology, providing market-leading performance with greater energy efficiency.

A Closer Look at IPSx

If your organization doesn't have dedicated security personnel and you need to meet compliance requirements, IPSx is for you. IPSx makes implementing and managing an IPS simple through its intuitive GUI. Installing the system takes just minutes, and ongoing administration is simple through dashboards, security event details, and reporting. Available in 250Mbps, 500Mbps, and 1Gbps, the simplicity of IPSx is backed by industry-leading Sourcefire detection at an attractive price point.

COMPLEMENTARY SOURCEFIRE PRODUCTS

Centralized Management

The Sourcefire Defense Center® centrally manages Sourcefire IPS sensors and enables you to categorize events, generate recurring reports, schedule automated Snort rule updates, configure policies, and display customizable dashboards to quickly communicate sensor feedback.

Security for Virtualized Environments

The Sourcefire Virtual IPS™ and Sourcefire Virtual Defense Center™ are available for VMware and XEN platforms. These virtual appliances enable you to inspect traffic between virtual machines (VMs) and simplify your deployment and management of sensors at remote sites where resources may be limited. Plus, you can mix and match physical and virtual Defense Centers and sensors to fit your needs.

SSL Inspection

Sourcefire SSL Appliances enable existing security appliances to effectively inspect SSL traffic through SSL traffic decryption. The SSL Appliance operates transparently on the network and supports both passive and inline network configurations.



Anti-malware

Most anti-malware products slow down an endpoint and require large downloads of the latest detection. Immunet™ provides accurate, lightweight end-point protection by moving detection and analysis to the cloud for true, real-time protection. Try Immunet today alone or run it alongside your existing antivirus or anti-malware solution.

To learn more, visit us at www.sourcefire.com or contact Sourcefire or a member of the Sourcefire Global Security Alliance today.

©2011 Sourcefire, Inc. All rights reserved. Sourcefire, the Sourcefire logo, Snort, the Snort and Pig logo, ClamAV, Immunet 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.