Sourcefire® Next-Generation IPS

Agile Security®

Sourcefire Next-Generation IPS sets a new standard for advanced threat protection, integrating real-time contextual awareness, intelligent security automation, and unprecedented performance with industry-leading network intrusion prevention. No other solution offers the visibility, automation, flexibility and scalability to protect today's dynamic environments against increasingly sophisticated threats.

Key NGIPS Capabilities

- Snort IPS detection engine
- Network intelligence
- Impact assessment
- User identification
- Automated policy tuning
- Network behavior analysis
- Packet-level forensics
- File type determination
- Application control
- URL filtering
- Advanced malware protection

True Next-Generation IPS

The Sourcefire Next-Generation Intrusion Prevention System (NGIPS) was built from the ground up to arm security teams with the protection they need in today's rapidly changing environments. Based on core competencies of contextual awareness and automation—recognized by Gartner as key ingredients of a Next-Generation Network IPS—and further fueled by the Sourcefire FirePOWER™ performance platform and sophisticated Sourcefire FireSIGHT™ network intelligence, Sourcefire's NGIPS stands apart, offering:

"Gartner believes that changing threat conditions and changing business and IT processes will drive network security managers to increasingly look for next-generation network IPS capabilities at the next firewall or IPS refresh cycle."[1]

John Pescatore, Gartner
Greg Young, Gartner

- **Real-time Contextual Awareness—See and correlate extensive amounts of event data related to IT environments—applications, users, devices, operating systems, vulnerabilities, services, processes, network behaviors, files and threats**
- **Advanced Threat Protection—Protecting for the latest threats, Sourcefire delivers the best threat prevention that money can buy as validated by independent third-party testing and thousands of satisfied customers around the world**
- **Intelligent Security Automation—Automated event impact assessment, IPS policy tuning, policy management, network behavior analysis, and user identification significantly lower the total cost of ownership and enhance the ability to keep pace with changing environments**

[1]Source: "Defining Next-Generation Network Intrusion Prevention," Gartner, 7 October 2011

- **Unparalleled Performance and Scalability—Purpose-built appliances incorporate a low-latency, single-pass design for unprecedented performance and scalability**
- **Application Control and URL Filtering—Reduce the surface area of attack through optional granular control of over 1200 applications and 100s of millions of URLs in over 80 categories**

In the "real world," threats are constantly evolving. And so is your network. You've got limited resources and a lot on your plate. You need an IPS that is "agile"—one that can protect you today but also grow with your organization tomorrow.

Real-Time Contextual Awareness

You cannot protect what you cannot see. Imagine a U.S. Secret Service agent assigned to protect the President while wearing a blindfold? That's analogous—granted, on a far lesser scale—to a network security device configured with a "default" policy not optimized to protect your unique network environment. It can't properly defend your network because it simply doesn't know what it's protecting.

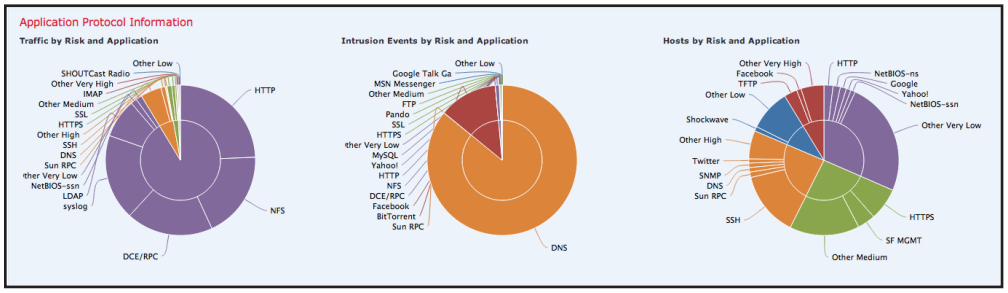
But Sourcefire is different. Since 2003, Sourcefire has been aggregating network intelligence to provide "context" to network security defenses.

- **Worms**
- **Triojans**
- **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**
- **Rate-based threats**
- **Zero-day threats**
- **TCP segmentations and IP fragmentation**

And today, Sourcefire FireSIGHT™ affords users with total network visibility, including physical and virtual hosts, operating systems, applications, users, content, and potential host vulnerabilities.

Powered by Snort®

- Open source, de facto IPS standard
- Invented in 1998 by Martin Roesch, Sourcefire Founder and CTO
- Most widely deployed IPS technology—over 4m downloads
- Used by over half of the world's 100 largest companies
- Used by the 30 largest U.S. government agencies
- Snort community has become an entire ecosystem:
  - » Nearly 400,000 registered users
  - » Dozens of Snort books published
  - » Classes taught at colleges and universities
  - » User groups
  - » Discussion lists and forums



Context Explorer allows you to visualize and explore all of the contextual information that FireSIGHT provides, including top-used applications and hosts.

Advanced Threat Protection

Sourcefire offers the smartest way to buy the best network threat protection available. Sourcefire helps you fight the latest threats to your network with FirePOWER. IP reputation blacklisting prevents connections to botnets, attackers, spam sources and other malicious IPs. The Network Advanced Malware Subscription, optional for FirePOWER appliances, enables malware detection/blocking, continuous analysis, and retrospective alerting and leverages Sourcefire's vast cloud security intelligence. Simply software-enable these additional protections when you're ready—no need for dedicated malware appliances that add further complexity.

Through a combination of vulnerability-based IPS rules, custom IPS rule creation, security intelligence for IP and file reputation capabilities, Sourcefire. customers have more ways to defend their systems than any other IPS provider. But don't take our word for it.

Sourcefire is the leader in NSS Lab's 2012 Security Value Map for IPS based on security effectiveness and total cost of ownership (TCO). Figure 1 is a summary of our latest test results in comparison to industry averages.

	SOURCEfire	Industry Average
Protection Rate	98.9%	92.76%
Total Cost of Ownership (protected Mbps)	$15.23	$37.82

Figure 1. This table shows protection effectiveness and total cost of ownership in comparison to industry averages based on 2012 NSS Labs Security Value Map for Network IPS.[2]

Sourcefire NGIPS is backed by the esteemed Sourcefire Vulnerability Research Team (VRT), a group of leading security experts that develop and maintain the official Snort rules used by the Sourcefire NGIPS. 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**

[2]Source: NSS Labs 2012 Network IPS Product Analysis Report average from 10 tested vendors

Sourcefire's NGIPS offers the most comprehensive threat prevention in the industry, including:

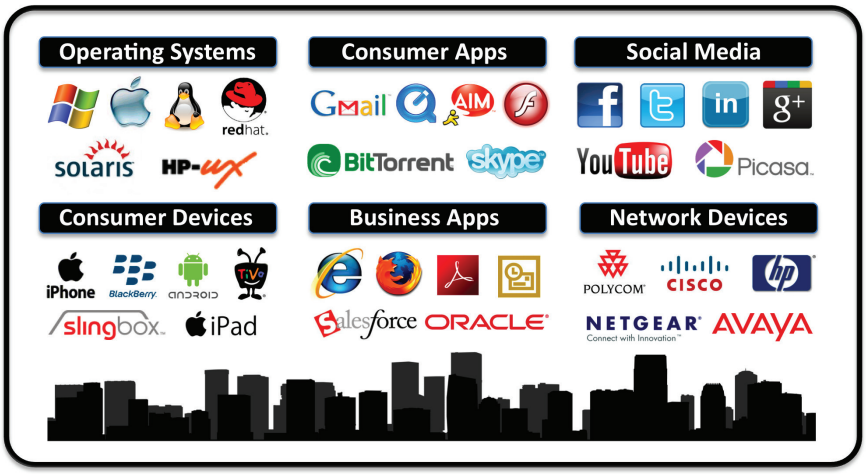


Figure 2. Sample FireSIGHT™ detection.

Intelligent Security Automation

Automation is critical to keep pace with advanced threats despite resource limitations. IT security must constantly strive to work smarter—not harder—to meet business demands. The Sourcefire NGIPS uses contextual awareness to fuel intelligent automation in the following ways:

- Optimize defenses and system performance by automating protection policy updates based on network changes
- Reduce the number of "actionable" security events by up to 99% by correlating threats against target operating systems and applications and their inherent vulnerabilities
- Know instantly who to contact when an internal host is affected by a client-side attack
- Be alerted when a host violates a configuration policy or attempts to access an unauthorized system
- Detect the spread of malware by baselining "normal" network traffic and detecting network anomalies

Sample Automation

- Threat prevention rule and policy updates
- Threat impact assessment
- Linking users to events
- Event correlation of user, device, service and application
- Exporting events to SIEMs
- Generating reports

fireSIGHT®

FireSIGHT™ Detection

- Physical/virtual hosts
- Operating systems
- Applications
- Consumer devices
- Mobile phones
- VoIP phones
- Network printers
- Routers
- Potential vulnerabilities
- Network flow and bandwidth
- Network anomalies
- User identity
- File type and protocol

"Mapping a username to an IP address was taking us away from a backlog of other important tasks. 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

FireSIGHT ensures network protections are deployed appropriately, and maintained automatically, as networks and threats change over time. FireSIGHT enhances the quality of network security while helping to deliver the lowest possible operational expense.

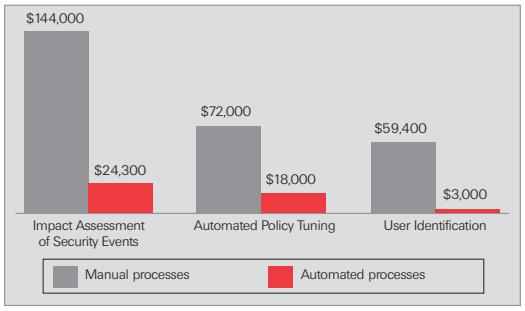


Figure 3. Annual cost of maintenance

Lower TCO Through Automation

Organizations can save tens of thousands of dollars every year by automating common threat prevention functions.

Defense Center Capabilities

- Centralized event monitoring
- Manages physical and virtual Sourcefire FirePOWER appliances
- Customizable dashboards with numerous widgets
- Role-based administration and workflow
- Syslog, email, and SNMP alerts
- Sophisticated and customizable reporting
- Third-party integration APIs
- LDAP, AD and RADIUS support
- Automated threat prevention updates
- Master Defense Center (MDC)

Unparalleled Performance And Scalability

Sourcefire NGIPS takes advantage of the best hardware technology in the industry, providing IPS inspected throughput options ranging from 50Mbps to 40+Gbps. The Sourcefire FirePOWER 8000 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 FirePOWER Series appliances lies breakthrough acceleration technology, providing market-leading performance with greater energy efficiency.

Sourcefire's central management console, called Sourcefire Defense Center®, is the central nervous system of Sourcefire's network security solutions. It's here where all protection and access policies are configured and where all security and compliance events are evaluated. Defense Center also offers a powerful reporting engine with a selection of report templates to meet the needs of any organization. And Sourcefire offers the most customizable dashboard in the business, featuring an intuitive portal-like interface equipped with a library of drag-and-drop widgets for monitoring security and compliance events and the health and performance of your FirePOWER appliances.

But performance and manageability aren't the only aspects that set Sourcefire's NGIPS solution apart. Sourcefire offers unparalleled scalability and ease of management through the Sourcefire Master Defense Center (MDC) capability. This hierarchical approach

allows a MDC to centrally manage up to 10 subordinate DCs. This offers our customers unprecedented scalability, whereas security and compliance events can be filtered up to the MDC, while protection and access policies can be pushed down to subordinate DCs and FirePOWER appliances.

Additional Protection With Application Control & URL Filtering

Sourcefire NGIPS customers can take contextual awareness to the next level with optional Application Control and URL Filtering capabilities. Exploiting applications is one of the most common threat vectors for attackers today. Organizations can go beyond identifying applications to gain even greater protection by granularly controlling application usage and access. Additionally, organizations can mitigate sophisticated client-side attacks—and improve employee productivity—by controlling access to more than 280 million URLs in over 80 categories. Through granular control of applications and web access, organizations can improve their overall network security posture by reducing their surface area of attack.

Seamless Third-Party Integration

Because of its open source flexibility and extensive interfaces (APIs), Sourcefire NGIPS 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**

Protection For Physical & Virtual Environments

Sourcefire offers an impressive line of purpose-built Network Security Appliances with inspected threat prevention throughputs ranging from 50Mbps to 40+Gbps. All Sourcefire Appliances come standard with programmable, fail-open copper and/or fiber interfaces, and most models come equipped with additional fault-tolerant features, including dual power supplies, RAID drives and lights out management (LOM).

Sourcefire also offers security solutions for VMware, Xen and Red Hat virtual platforms. Sourcefire Virtual Sensors provide the capability to inspect VM-to-VM communications, providing the same control and protection as their physical counterparts.

"During our testing, one 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, LA Times

Remove Network Blind Spots Through SSL Decryption

The use of SSL encryption is exploding due to cloud computing and the rise of Web-enabled applications.

The Sourcefire SSL Appliance can decrypt and re-encrypt SSL traffic, allowing unimpeded security inspection that scales in concert with your network performance requirements. It's also easier to centrally manage keys for varying security functions (e.g., IPS, DLP, Network Forensics) within a single appliance deployment.

Sourcefire SSL Appliance 8200

SSL is an easy vehicle for cybersecurity attacks:

- Inbound attacks
- Spyware and malware
- Viruses and worms
- Phishing
- Identity theft
- Information leaks

Take The Next Steps Toward Agile Security

To learn more about Sourcefire's Next-Generation IPS and other solutions that provide Agile Security, contact a member of the Sourcefire Global Security Alliance™ today to view a demonstration, request an onsite evaluation, or schedule a meeting, or visit www.sourcefire.com for more information.

4.13 I REV4B