



Sourcefire Real-time Network Awareness (RNA)

“Know More” with “All-the-Time/Real-Time” Network Intelligence

With wireless equipment, mobile employees, outsourced workers, and virtual environments, today’s networks are highly dynamic. Hackers have gotten smarter, so threats are constantly evolving and becoming more sophisticated. Static defenses can’t protect today’s dynamic networks against today’s dynamic threats. Learn how Sourcefire RNA™ (Real-time Network Awareness) can help you “know more” about your dynamically changing network and improve your network’s integrity. Know more real threats. Know more about your network composition, changes, and anomalies. Know more compliance policy violations. No more guessing. No more being left in the dark. Dynamic security for a dynamic world.

Sourcefire RNA Benefits—24x7, Passive Network Intelligence

- Contextual Impact Assessment:
 - » Reduces false positives & negatives up to 99%
 - » Prioritizes intrusion events based on the impact to your network
- Adaptive IPS:
 - » Automated IPS tuning
 - » Recommends rules based on your network composition
 - » Dynamic traffic reassembly & non-standard port handling to prevent IPS evasions
- Network Discovery:
 - » Know what hosts you’re protecting on a continuous basis
 - » Identify outdated applications, possibly signifying a rogue system or one rolled back to a previous baseline
- Change Management:
 - » Dynamic knowledge of network changes
 - » Powerful P&R rules allow notification when network changes
 - » Detect rogue devices plugged into your network to collect confidential data
- Network Behavior Analysis:
 - » Detect & quarantine internal threats
 - » Evaluate network bandwidth utilization
 - » Troubleshoot network performance issues
- IT Policy & Regulatory Compliance:
 - » Monitor & enforce IT & regulatory policies
 - » Find hosts using unauthorized applications

Sourcefire RNA is an innovative, passive sensing technology that transforms how organizations defend their networks, providing network and security administrators with unprecedented real-time network visibility. RNA relies on full traffic analysis to monitor network assets in real-time and track their configuration changes and network behavior. RNA enables organizations to confidently protect their dynamic networks through a unique, patented combination of passive network discovery, network flow analysis, and targeted vulnerability assessment technologies. Sourcefire is the only major IPS vendor offering these revolutionary network-sensing capabilities to enable Adaptive IPS with context, accurate network intelligence, and compliance monitoring and enforcement.

ADAPTIVE IPS—“KNOW MORE” REAL THREATS, “NO MORE” MANUAL TUNING

Impact Assessment—“No More” Wild Goose Chases

“I need to know which of the hundreds of intrusion alerts really matter.”

Most network security technologies have little understanding of the assets they are protecting. Firewalls, intrusion prevention systems (IPS), patch management systems, and vulnerability assessment systems often utilize static configurations and operate without real-time information about network composition or high-impact events.

	Sourcefire 3D™ System	Traditional IPS
Amount of Human Intervention Required	HIGHLY AUTOMATED	PEOPLE INTENSIVE
Cost to Operate	LOWER	HIGHER
Number of False Positives	LOWER	HIGHER
Number of False Negatives	LOWER	HIGHER
Potential for Network Downtime	LOWER	HIGHER

Figure 1. Sourcefire RNA adds network context to dramatically reduce the quantity of intrusion events requiring analysis by eliminating both false positives and false negatives.

This lack of visibility into the network and lack of context have significant security implications, especially in today’s dynamic environments. IPSes notice plenty of questionable traffic, but lack contextual information to know which traffic is important and relevant to specific networks. In many real-life deployments,

Sourcefire RNA Performs Impact Assessment & Adaptive IPS

Sourcefire RNA incorporates real-time network intelligence into Sourcefire's 3D System to automatically tune and optimize the Sourcefire IPS. Key IPS capabilities enabled by RNA include:

- Contextual impact analysis displayed as Impact Flags
- Automated IPS tuning
- Non-standard port handling
- Adaptive traffic profiles

at least 90% of the alerts produced by IPS sensors turn out to be “false positives” — alerts that are determined to be irrelevant after investigation. If an attacker has information about specific hosts, IPS deployments without context may also be evaded, a phenomenon known as a “false negative.”

To help address these traditional IPS shortcomings, Sourcefire RNA leverages a vulnerability database to generate a list of an asset's potential vulnerabilities. RNA uses this vulnerability data to make its impact analysis more accurate. The Sourcefire Defense Center™, a central management console that provides event aggregation, asset monitoring, and Sourcefire 3D™ Sensor management, can correlate security event data with a target's operating system (OS), services, applications, and potential vulnerabilities in real time. By comparing attacks to the attributes of the hosts under attack, the Sourcefire 3D System can assign an “impact” value to the attack and visually represent this impact with a prioritized **Impact Flag** on the Defense Center dashboard. By determining the relevance and impact of each intrusion attack on your network, security analysts can focus their attention only on those events that matter most.







IMPACT FLAG RATING & COLOR	IMPACT FLAG SUMMARY	IMPACT FLAG MEANING
	Act Immediately, Vulnerable	Indicating that the targeted host is in the RNA network map and a vulnerability is mapped to that host.
	Investigate, Potentially Vulnerable	Indicating that either the source or the destination host is in RNA's network map and one of the following is true: <ul style="list-style-type: none"> • for port-oriented traffic, the port is running a service • for non-port-oriented traffic, the host uses the protocol
	Good to Know, Currently Not Vulnerable	Indicating that either the source or the destination host is in RNA's network map and one of the following is true: <ul style="list-style-type: none"> • for port-oriented traffic (for example, TCP or UDP), the port is not open • for non-port-oriented traffic (for example, ICMP), the host does not use the protocol
	Good to Know, Unknown Target	Indicating that either the source or destination host is on a monitored network, but there is no entry for the host in RNA's network map.
	Good to Know, Unknown Network	Indicating that neither the source nor the destination host is on a network that is monitored by RNA.
	Good to Know, Blocked	Indicating in the Inline Result field that the rule state for the rule that generates this event is set to Drop, and the packet was dropped.

Table 1. Sourcefire's Impact Flags drastically reduce the number of “actionable” security events.

For example, a Linux exploit targeting a Microsoft Windows server would generate a low impact rating because it has no chance of actually succeeding. Conversely, an exploit targeting a server that may be vulnerable to that exploit would have a more serious impact. This impact analysis allows administrators to focus only on the events that can affect their networks, allowing security resources to be used more efficiently.

Automated IPS Tuning—“No More” Wasted Effort

“I want to automate the time-consuming process of tuning my IPS.”

RNA uses a feature known as **RNA-Recommended Rules (RRR)** to optimize IPS performance and maximize protection by recommending that only Snort® rules pertaining to a network's operating systems and services be enabled. For example, if RNA determines that a protected network segment is only running Linux systems supporting Web services and NIS, then RNA can recommend disabling any rules pertaining to Windows hosts and services, such as IIS. RRR is designed to maximize protection and sensor performance and significantly reduce, or virtually eliminate, the manual effort required to tune Sourcefire IPS™ sensors. Rule recommendations made by RRR can be implemented with or without human intervention.

“RNA is amazing. It reduces the number of false positives in the network. That really frees up time to deal with bigger, more pressing issues.”

Gregory Henry, CISSP, IT Security Consultant for GraceKennedy

“We went from 110,000 alerts a week to 42,000 just by enabling RNA-Recommended Rules.”

Network Security Engineer, Major Healthcare Provider

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

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

Sourcefire RNA Performs Network Discovery to Know

- When a new host appears, whether physical or virtual
- What OS and services it's running (e.g., BitTorrent)
- What ports are open
- What protocols it's using
- What its potential vulnerabilities are

“Network discovery is passive for Sourcefire RNA. It can tell what OS version is on a server, what services it's running, and the specific versions of each service. With the information from RNA, I can correlate events to determine any impact.”

**John Abella, Senior Network Engineer,
Retail Decisions**

Another automated IPS tuning feature, **non-standard port handling**, helps to prevent possible IPS evasions by inspecting traffic on non-standard ports. For example, nothing precludes the use of HTTP traffic on TCP port 8888 instead of the standard TCP port 80. Traditional IPS implementations can detect this traffic, but the result is usually sub-optimal performance or requires manual configuration of rules for non-standard ports. Sourcefire's non-standard port handling capability accounts for such scenarios. RNA identifies the ports and services on the hosts it's monitoring and configures the IPS to dynamically apply the correct rules for any non-standard ports.

Another technique for malicious attackers to possibly evade IPS inspection is to fragment attacks, thus taking advantage of the fact that operating systems reassemble traffic fragments differently. For example, if the target host is a Windows system, but the IPS reassembles traffic in the same manner as Linux, then the IPS may not detect a certain fragmented-traffic exploit that has its desired effect on Windows systems (a false negative). **RNA's adaptive traffic profiles** feature prevents this type of IPS evasion by providing OS data about each host to the 3D Sensor. No other IPS product provides this real-time host information. The 3D Sensor can dynamically adjust the traffic reassembly process in a manner consistent with different target OSes.

NETWORK INTELLIGENCE—“NO MORE” GUESSING OR SURPRISES

Network Discovery—“No More” Being Left in the Dark

“I want to know how many servers and workstations are on my network, plus the configuration and status of each one.”

Despite spending more money on security, you're still not sleeping at night, threats are not going away, and uncertainty remains. Since Sourcefire RNA is watching all the time, in real time, it will help you “know more” about your assets, network composition, and network risks, and protect against both internal threats and external attacks. With RNA, you will discover things running on your network that you never dreamed possible — “no more” being left in the dark.

RNA provides 24x7, passive network intelligence, storing a real-time inventory of all operating systems, services, applications, protocols, and potential vulnerabilities that exist on the network. RNA's key differentiator lies in its ability to collect this intelligence in a completely passive manner, while seamlessly integrating the intelligence within the Sourcefire 3D System. Combine RNA's real-time network visibility with Sourcefire RUA™ (Real-time User Awareness), a technology that links user identity to security and compliance events, and organizations have enterprise-wide intelligence on their dynamic networks and users.

Because RNA is passive, it avoids the numerous and substantial pitfalls of traditional network monitoring technologies that rely on active scanning or host-based agents.

- Generates no traffic that can either consume bandwidth or potentially harm network infrastructure
- Provides a real-time network view that is continually updated as devices produce traffic — data never becomes “stale” or dependent on periodic scans
- Detects application traffic on all ports, not just well-known ports
- Does not rely on endpoint agents that require management — unknown or rogue devices are always visible

With Sourcefire RNA's real-time network intelligence, you will know exactly what is happening on your network.

"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**

Sourcefire RNA Enables Network Behavior Analysis

- Detect internal malware & quarantine before it spreads
- Monitor contractors & guests
- Evaluate bandwidth provisioning against baselined traffic
- Troubleshoot network outages & degradations
- Monitor network resource usage
- Detect network changes in real-time

"A \$100,000 IPS can easily be defeated with a laptop and a comfortable pair of shoes."

**Martin Roesch,
Sourcefire Founder and CTO**

Change Management—"Know More" About New or Altered Hosts

"I want to be alerted when a new host appears on my network or if an existing host changes its approved configuration."

How do you become aware, in real time, of changes to the network baseline established by RNA? With RNA's change management capability and powerful Policy and Response (P&R) engine, Information Security or Network Operations can be notified the moment a new host appears on the network and/or when an existing host has changed its approved configuration (e.g., OS upgrade, new service). In addition, Sourcefire's Remediation API enables the 3D System to direct external devices and systems to help enforce policies and/or take corrective actions, such as quarantining connections at the firewall or router.

Although passive discovery is RNA's primary means of gathering network intelligence, RNA's host database can be augmented with information gathered by active discovery tools. For example, RNA's detection of a new host can trigger an active scan of that host by using the Remediation API to call a third-party vulnerability assessment tool. Sourcefire's Host Input API enables the 3D System to obtain additional endpoint asset and vulnerability intelligence from a variety of third-party tools, and it integrates the active scan results into the RNA host database to increase the accuracy of RNA's impact analysis.

NETWORK BEHAVIOR ANALYSIS—"KNOW MORE" NETWORK ANOMALIES

"Whose computer is propagating malware within our organization?"

Network Behavior Analysis (NBA) solves daily challenges faced by both Information Security and Network Operations groups. First, Sourcefire RNA enables Information Security to detect and quarantine internal threats by establishing "normal" traffic baselines and detecting network anomalies. Security analysts can receive real-time alerts via e-mail, SNMP, or through a third-party SIEM (Security Information & Event Management) using the Sourcefire eStreamer™ capability. Endpoints accessing unauthorized resources or propagating malware can be quarantined at the router or firewall using the Remediation API. RNA can also help to secure the "unmanaged" devices used by contractors and guests, and IT can be alerted any time a new host appears or attempts to access an unauthorized network resource.

Second, Sourcefire RNA enables Network Operations to monitor bandwidth consumption across the network and to troubleshoot network outages and performance degradations. Using RNA's built-in RNA Flow capability, or Sourcefire's optional NetFlow Analysis Module, Network Operations professionals can leverage RNA to ensure ample bandwidth is provisioned to remote offices. Flow analysis is also useful during periods of network slowdowns and to analyze traffic just prior to a network outage. For example, a network may slow to a crawl at noon each day. By leveraging flow analysis, it can be determined that a backup system was misconfigured to begin its backup procedure at noon rather than at midnight.

Key Sourcefire RNA Compliance Capabilities

- Internal IT policy compliance features:
 - » Custom rules
 - » White lists
 - » Reports
 - » Alerts
 - » Dashboards
- Facilitates compliance with external regulations:
 - » PCI DSS
 - » SOX
 - » HIPAA
 - » FISMA
 - » Basel II
 - » GLBA
 - » NERC

“Without Sourcefire, we would have never passed the [PCI] audits, which could have led to regulatory fines or loss of business with our partners.”

Michael Morgan, Network Security Administrator, BankersBank

MEETING COMPLIANCE—“KNOW MORE” POLICY VIOLATIONS

IT Policy Compliance—“Know More” IT Policy Infractions

“I want to know if my employees are using Skype, which is against our company’s IT policy.”

The Verizon Business 2008 Data Breach Investigations Report found that 79% of the studied companies failed to actually enact their established security policies.¹ Sourcefire helps customers to overcome this challenge by making it easy to monitor and enforce IT policy compliance.

Sourcefire RNA continuously discovers and monitors network assets and maintains an updated inventory of OSEs, services, client applications, and protocols. Administrators can work with this inventory to create “compliance white lists” for the proper use of assets. The Defense Center will then generate alerts if RNA sees changes that could indicate the violation of a compliance policy, such as the introduction of new network assets or new services, such as IRC or SSH. These alerts can be used to trigger a number of automated responses, including removal of assets from the network through integration with network infrastructures capable of performing network access control.

RNA’s business criticality features can assist with compliance monitoring. Hosts in the Sourcefire 3D database can be prioritized based on the business value to the organization. This setting can be used to differentiate between a finance server with highly sensitive data and a test server sitting in a lab. RNA’s compliance engine can use this data to build powerful compliance rules that trigger a different response or remediation for hosts with different criticalities.

Regulatory Compliance—“No More” Penalties

“I want to demonstrate that my company meets the requirements for PCI DSS compliance.”

Oftentimes, monitoring and enforcing compliance with company IT policies facilitates compliance with external regulations, such as PCI DSS, HIPAA, SOX, FISMA, Basel II, GLBA, and NERC. Numerous 3D System compliance features, such as white lists, graphs showing user compliance events over time, and pie charts showing percentage of hosts in compliance with white lists, help organizations achieve regulatory, as well as internal, compliance. Admins can monitor compliance progress within the Defense Center dashboard and generate standard or customized compliance reports that show assets and users that are out of compliance. By tracking these metrics over time, admins can demonstrate progress towards compliance goals and provide auditors with data proving enforcement of configuration and network usage policies.

¹Verizon Business RISK Team, 2008 Data Breach Investigations Report, June 2008

TAKE THE NEXT STEP TO PROTECT YOUR NETWORK—“KNOW MORE” NOW

Sourcefire RNA helps you “know more” about your dynamic network in real time and strengthens its integrity through contextual impact assessment, Adaptive IPS tuning, network discovery, change management, network behavior analysis, and IT policy and regulatory compliance monitoring and enforcement — improving your network security, allowing your network security team to work more efficiently, and saving you time and money.

- RNA provides real-time intelligence about the targets on your dynamic network and enables the correlation of attacks and target assets — drastically reducing the noise and allowing security teams of all sizes to more efficiently defend their networks.
- RNA’s “all-the-time/real-time” network visibility monitors for behavior or configuration changes, giving your network security team the intelligence to know when a system on the network has been compromised.
- RNA’s compliance capabilities, such as compliance white lists and custom Policy and Response rules, help to achieve company IT and regulatory compliance.

To learn more about Sourcefire RNA, visit www.sourcefire.com or contact a member of the Sourcefire Solutions Network™ today.