SOURCEfire®

Sourcefire RNA® (Real-time Network Awareness)

Continuous Network Intelligence and Network Visibility

Today's networks are highly dynamic. Threats are constantly evolving and becoming more sophisticated. Static defenses can't protect today's dynamic networks against dynamic threats. Learn how Sourcefire RNA® (Real-time Network Awareness) transforms how you defend your organization's networks. Dynamic security for a dynamic world.

Sourcefire RNA Benefits—24x7, Passive Network Intelligence

- Reduce workload in maintaining and tuning an IPS
  - » Know which intrusion events really matter
  - » Optimize staff time by automating IPS tuning
- Detect network configuration changes and traffic anomalies
  - » Gain full network visibility and monitor configuration changes
  - » Identify network anomalies and performance issues
- Monitor and enforce compliance
  - » Act on policy infractions
  - » Facilitate compliance with external regulations

Sourcefire RNA Performs Impact Assessment and Automated IPS Tuning

- Correlation of threats with endpoint intelligence to provide threat impact
- Automated IPS tuning to significantly reduce manual tuning effort

"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

SOURCEFIRE RNA—REAL-TIME PASSIVE NETWORK INTELLIGENCE

Sourcefire RNA is a real-time technology that provides continual network visibility and protects your network against dynamically evolving threats. Deployable on both physical and virtual Sourcefire 3D® Sensors, RNA enables organizations to protect their dynamic networks in a number of ways:

- Reduce workload in maintaining and tuning an Intrusion Prevention System (IPS)
- Detect network configuration changes and traffic anomalies
- Monitor and enforce compliance

REDUCE WORKLOAD IN MAINTAINING AND TUNING AN IPS

Know Which Intrusion Alerts Really Matter by Assessing Impact

"I need to know which of the thousands of intrusion alerts really matter."

Most network security technologies, such as firewalls and IPSes, are statically configured with little understanding of the assets they're protecting. This lack of visibility has significant security implications in today's dynamic environments, especially as virtualization adds complexity. For example, IPSes generate a large quantity of intrusion events because they lack contextual information to know which events are relevant and which are not. It's difficult for any security analyst to discern which events require further investigation.

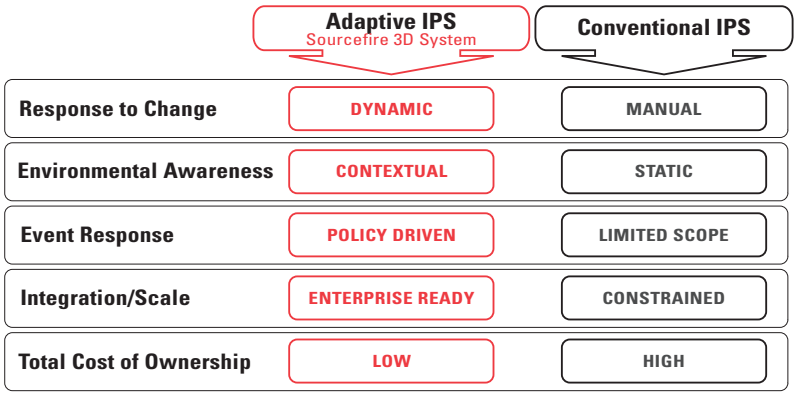

Figure 1. Sourcefire RNA adds network context to dramatically reduce the quantity of intrusion events requiring analysis.

To help address these traditional IPS shortcomings, RNA uses real-time vulnerability data to prioritize intrusion events. The Sourcefire 3D System correlates intrusion events with a host's potential vulnerabilities to assess whether a host is vulnerable to an attack, and each attack is assigned an "impact" value (called an Impact Flag). Security analysts can then focus their attention only on those events that matter most.

"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

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

Network Security Engineer, Major Healthcare Provider

Sourcefire RNA Performs Network Discovery

- When a new host appears, physical or virtual
- What OS and services it's running (e.g., BitTorrent)
- What potential vulnerabilities exist

"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

IMPACT FLAG RATING & COLOR	ADMINISTRATOR ACTION
	Act Immediately, Vulnerable
	Investigate, Potentially Vulnerable
	Good to Know, Currently Not Vulnerable
	Good to Know, Unknown Target
	Good to Know, Unknown Network
	Good to Know, Blocked

Table 1. Sourcefire's Impact Flags allow security analysts to focus their attention on the security events that matter most.

For example, a Linux-only 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 cause a more serious impact rating.

Optimize Staff Time by Automating IPS Tuning

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

RNA-Recommended Rules (RRR) recommends which Snort® rules to enable and disable on the IPS. 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 various Windows-specific services. RRR is designed to maximize protection and sensor performance and significantly reduce, or virtually eliminate, the manual effort required to tune Sourcefire IPS™. Rule recommendations made by RRR can be implemented with or without human intervention.

DETECT NETWORK CONFIGURATION CHANGES AND TRAFFIC ANOMALIES

Gain Full Visibility into Network Assets

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

RNA provides full visibility into your assets (both physical and virtual), network composition, and network risks. RNA passively analyzes your network to tell you what is actually going on, as opposed to what you think is going on.

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 consume bandwidth or potentially harm network infrastructure
- Provides a network view that's 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
- Doesn't rely on endpoint agents that require management—unknown or rogue devices are always visible

Organizations can 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. RUA therefore provides much more visibility into specific user activity in enterprise networks.

Receive Alerts about New or Altered Hosts

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

Information Security (IS) or Network Operations (NO) can use RNA's powerful compliance engine to learn when a new host appears on the network and/or when an existing host has changed its approved configuration. In addition, organizations can use Sourcefire's Remediation API to integrate the 3D System with direct external devices and systems to help enforce policies and/or take corrective actions.

Users can also use Sourcefire's Host Input API to augment RNA's host database with information from other tools. For example, they can add vulnerability data from a third-party scanner to increase the effectiveness of RNA's impact analysis.

Sourcefire RNA Enables Network Behavior Analysis

- Detect network changes in real time
- Detect internal malware and quarantine before it spreads
- Evaluate bandwidth provisioning against baselined traffic
- Troubleshoot network outages and degradations

Identify Network Anomalies

"Whose computer is propagating malware within our organization?"

RNA's network behavior analysis (NBA) capabilities analyze network traffic and detect traffic surges or other anomalies. NBA solves daily challenges faced by both IS and NO groups. First, RNA enables IS to detect and quarantine internal threats by establishing "normal" traffic baselines and detecting network anomalies. Second, RNA enables NO to monitor bandwidth consumption across the network and to troubleshoot network outages and performance degradations.

MONITOR AND ENFORCE COMPLIANCE

Key Sourcefire RNA Compliance Capabilities

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

Act on IT Policy Infractions

"I want to know if employees are using Skype, which is against our company's IT policy."

Sourcefire makes it easy to monitor and enforce IT policy compliance. RNA continuously discovers and monitors physical and virtual network assets. Administrators can create "compliance white lists" for the proper use of assets. Sourcefire Defense Center® can then generate alerts and take appropriate action if RNA sees changes that could indicate the violation of a compliance policy, such as the introduction of unauthorized applications.

RNA's business criticality features can also assist with compliance monitoring. Hosts can be prioritized based on the business value to the organization, such as critical finance servers with highly sensitive data. RNA's compliance engine can use this data to trigger a different response for hosts with different criticalities.

Facilitate Compliance with External Regulations

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

Monitoring and enforcing compliance with company IT policies should facilitate 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 and charts showing the percentage of compliant hosts, help organizations achieve regulatory, as well as internal, compliance. Admins can monitor compliance progress in a dashboard and generate 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.

"Not knowing what's on your network is going to continue to be the biggest problem for most security practitioners."

Marcus Ranum, CSO Magazine

TAKE THE NEXT STEP TO PROTECT YOUR NETWORK

Sourcefire RNA is a real-time technology that provides continual network visibility and protects your network against dynamically evolving threats. RNA greatly improves and automates your network security, allowing your security resources to work more efficiently—saving you time and money.

- RNA provides real-time intelligence about 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 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 us at www.sourcefire.com or contact Sourcefire or a member of the Sourcefire Global Security Alliance today.