No. 21-

IN THE

Supreme Court of the United States

CENTRIPETAL NETWORKS, INC.,

Petitioner,

v.

CISCO SYSTEMS, INC.,

Respondent.

ON PETITION FOR WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

SUPPLEMENTAL APPENDIX

PAUL J. ANDRE
Counsel of Record
LISA KOBIALKA
JAMES HANNAH
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
(650) 752-1700
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com

Counsel for Petitioner

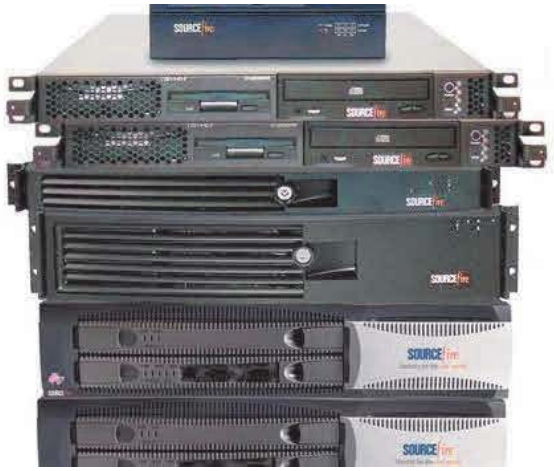
305711

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

TABLE OF CONTENTS

Page

Sourcefire 3D



WRITTEN BY
Ian Murphy

REVIEWS

3 Jan, 2007

Price : £25,000

(Sourcefire 3D Suite starting price), £2,659 (Intrusion Sensors starting price) £20 (RNA per node, falling to £2 for volumes in excess of 131,000 nodes), all exc VAT

Verdict :
Despite Sourcefire's attempts to produce a workable GUI, it is a solution that requires careful planning and significant investment in training to ensure you get the best out of it. Many companies will find that off-putting, yet it is still the most sophisticated security tool I've ever tested and sets a real standard for other vendors to try and match.

Sourcefire is a security company that has built a reputation for providing security across the network. While others focus on just point solutions such as anti-virus, intrusion detection and firewalls, Sourcefire has focused on producing an enterprise-class system that encompasses everything. It can be bought as a single comprehensive solution or you can add components as needed.

3D stands for Discover, Determine and Defend, hence the Sourcefire 3D name. Each of the three components has a specific job. Discover is done by the Intrusion and RNA Sensors, Determine by the Defence Centre and Defence by your existing tools. The Sensors and the Defence Centre are shipped as hardware appliances.

Much depends on what part of the solution you buy and the complexity of your network as to what you get in the box. You can buy all three appliances as a single package or you can buy as separate components. If required, the whole thing can come in a single appliance but for real security you are going to want to deploy and lot of the sensors around your network.

The Defence Centre is a 2U appliance while the Intrusion and RNA Sensors are 1U appliances although the RNA Sensor can be purchased as just a software package and installed on your own hardware.

At first glance this is a complex system to get to grips with. The GUI needs to be reworked and you must have a real understanding of what the components do before deploying. A good knowledge of what you have on your network is always helpful here as it will assist you in understanding what information you get from Sourcefire 3D. Without that, you will find big differences in the type and number of alerts from existing solutions you may have and Sourcefire 3D.

All sensors have their own Gigabit connection to the Defence Centre and use an encrypted SSL (AES 256bit) link. Sourcefire recommends that you place the Defence Centre on a separate LAN or at least use a separate VLAN from the Sensors.

The Intrusion Sensor is a beefed up version of Snort, the software sniffing tool that you can get free. You can configure the Intrusion Sensor in either active or passive mode and this slightly changes its role. In active mode the focus is on intrusion protection, actively monitoring and blocking traffic based on rules. In passive mode it offers intrusion detection using rules to monitor and raise alerts.

What makes the Intrusion Sensor interesting is the use of multiple detection engines all of which work with the main Snort rules engine. This means that whenever a new attack is detected, a single rules update becomes available to all the detection engines.

The RNA Sensor only works in passive mode and there are good reasons for this. Its first job is to identify all the assets on your network and determine what is out there. This has to be done in passive mode as in a critical environment; active mode could interfere with the running of your other equipment. One of the shocking things about the RNA Sensor is the amount of data that it does acquire.

If getting a fairly accurate map of your network was not enough, the RNA Sensor is very smart about how it responds to threats. When a threat is detected, it looks to see what systems you have that are vulnerable to that threat. If there are no vulnerabilities then the threat becomes moot. This is important to understand because you could find yourself caught between different systems giving conflicting data.

An example of this is the Slammer attack. If you have machines running SQL Server that have been patched, any detection of a Slammer attack will be ignored. There is no point in sending alerts for something that isn't real. Compare this with the average firewall which will send an alert because it has detected a Slammer attack but which doesn't know anything about your internal systems.

The result should be a massive reduction in false positives, allowing your security team to concentrate on what they really need to deal with rather than chasing ghosts.

The last element, the Defence Centre is about rules, management and reporting. It acts as a filter engine dealing with the data from the Intrusion and RNA Sensors allowing the operators to manage security from a single point rather than have to touch each sensor constantly.

Most security products look at an alert and simply respond to that. The Defence Centre uses pivot tables to allow you to find correlations between attacks. This is critically important in an age where attacks can easy circumvent your network protection via USB drives, mobile phones, MP3 players and the like.

When an attack is detected, you can go back and find the machine that was the zero point. From here you can look at its communication with other computers and see unexpected bursts of traffic or excessive connections. This allows you to map and predict the spread of an attack internally.

You can then start to isolate and stop attacks, clean the network and build a profile of how the incident occurred. This is extremely sophisticated and well ahead of other products in the market.

To make this process easier to see, there is a set of 3D modelling tools so that you can use to see the spread of an attack. This provides more than just security information; it can provide an organisation with an insight as to the relationships and information flow throughout their business. This also pays into the compliance requirements in that it can show how likely it is that information has breach internal safeguards.

While Sourcefire owns the intellectual property for Snort is has kept it free and available to the wider community. Taking that knowledge and then pulling it back with additional features into their Intrusion Sensor is a clever move. It means that there are a number of qualified developers

Popular

1 Def Con developer sells $200 Mac-hacking iPhone cables
SECURITY

2 Massive biometric data breach found in system used by banks and Met police
DATA BREACHES

3 What is HTTP error 503 and how do you fix it?
WEB BROWSER

in the market and the product is widely accessible. As other security companies look to use Snort for their products, it has the added advantage of ensuring that knowledge gained is not knowledge lost should you choose to change security vendor.

Sourcefire takes advantage of the Snort Rules Engine integration with the Detection Engines to simplify the deployment of new rules. This single rule, multiple engines approach is a very fast and simple way to deploy security. It also ensures that when rules are being updated, there is no mismatch between the rules base for each of the different engines, which could open a temporary vulnerability. Sourcefire sends out new rules every two weeks, or sooner should a specific threat emerge.

The GUI is perhaps the most disappointing aspect of the whole system. The problem is that there is so much to do and so many things to work with that the GUI is really fighting against information overload. Sourcefire needs to think about how it can improve this.

Sourcefire could also do a little more in terms of extra wizards and tutorials. It also needs to work a little more on the certified training side and align it with some of the wider industry objectives on security. Despite these criticisms this is the most sophisticated security tool I've ever tested and sets a real standard for other vendors to try and match.

READ MORE ABOUT: FIREWALLS | SECURITY | NETWORK & INTERNET

4 What is GDPR? Everything you need to know, from requirements to fines
POLICY & LEGISLATION

5 UK's tech sector hit by wider economic downturn
STARTUPS

Latest in Firewalls

Decade-old vulnerability found in globally popular office phone
NEWS

NHS anaesthetic machines vulnerable to hackers
NEWS

IT chiefs are compromising security for smoother business operations
NEWS

Flaws in 4G and 5G could allow attackers to launch DoS attacks and track location
NEWS

WatchGuard Firebox M670 review: Dazzling value
REVIEWS

You May Like

May 01, 2006

PRODUCT INFORMATION

Sourcefire 3D IPS1000

Name: Sourcefire 3D IPS1000
Description:
Price: from $4,500 for IS1000; from $1,385 for RNA; from $20,200 for Defense Center

QUICK READ

STRENGTHS: Performs well under normal attack conditions and can work well as a layer of protection for average networks.

WEAKNESS: If the sensor is compromised for any reason, the IPS system leaves the network vulnerable to attack.

VERDICT: Not an IPS star: Sourcefire's rating here does not take into account the suite's full capabilities.

RATING BREAKDOWN

SC Labs Reviews

Reviews from our expert team

Features:

Documentation:

Value for Money:

Performance:

Support:

Ease of Use:

3.00/5

SUMMARY

The Sourcefire box does allthe things an IPS shoulddo. It fits comfortably inthe category of an average IPS,although it must be rememberedthat the Sourcefire 3D Suiteincludes a ton of IDS, scanning,and vulnerability managementcapability which falls outside thecontext of this review. As an IPS,the box has no standout features,and nothing specifically separatesit from other IPSs.

With the management interfacegeared around the suite as a whole,narrowing down IPS functionalitywas difficult. There is no definedprocedure for setting policies ordetermining what types of policiesare needed.

The configuration of the boxitself involves a long navigationthrough a complicated web interface,and setting different policiesand generating the reports weneeded was time-consuming andbecame more difficult the furtherwe progressed.

The box defended againstnormal scans and attacks, but wewere able to compromise thesensor by launching a denial-ofserviceattack and bypassing theIPS. With the sensor disabled, thecomputers on our target networkbecame susceptible to attack byour testing tools. The consolecould flag up a dead sensor, butthat of course will not protect thesystems that are under attack.

The appliance comes with a CDthat contains documentation andrestore information. There aretwo manuals, one is an installationguide and the other is an administratormanual. But the documentationis very long, more than 900pages, and is geared to operatingthe suite as a whole. If the manualis needed to answer specificconfiguration issues or questions,the search for information can bevery time-consuming.

There is a lot of support offeredfrom Sourcefire, including fulltelephone technical support aswell as online help files and emailsupport, as part of an onlinesupport site.

The product comprises threeappliances: the IS 1000; the RNA;and the Defense Center. It is fairlypricey for its abilities but doesrequire reasonably intensivedeployment and management. Butyou would not buy it for the IPS– this is just one component ofthe whole suite, which is a muchmore attractive proposition.

Back to Top ↑

COMPANY INFO

About Us

SC Corporate News

Meet the Team

Advisory Board

Contact Us

PRODUCT REVIEW

About Product Review

Group Tests

FAQ

USER CENTER

Videos

Executive Insight Guidelines

Subscribe

OTHER SC SITES

RiskSec Conference

SC Resource Library

SC Online Events

SC Awards