SOURCEfire®

KNOW MORE NETWORK RISKS
NO MORE GUESSING

KNOW MORE

Sourcefire Defense Center™

Sourcefire Defense Center Capabilities

- Store up to 100,000,000 security & host events, including packet data
- Centralized policy & sensor management
  - » Centralized audit logging of configuration & security policy changes
  - » Easy registration of new sensors
  - » Sensor grouping for easy policy management in large enterprises
  - » Secure communication with all sensors
  - » Manage up to 100 Sourcefire 3D Sensors with a single Defense Center
  - » MDC mode for managing up to 10 subordinate DC appliances—manage many hundreds of sensors from one DC
- Centralized health monitoring of all Sourcefire appliances
- Powerful reports, alerts, & dashboards
  - » Generate enterprise- or site-specific reports, graphs, & charts
  - » Create incident reports & bookmarks to direct others to specific events
  - » Report Designer for full report customization
  - » Customized alerts & responses
  - » Customized "dashboard" view of enterprise & event data
  - » Dozens of pre-defined or customized drag-and-drop dashboard widgets
- Detailed packet-level forensics
- Automated event & sensor maintenance tasks
  - » Centralized updating & deployment of security content
- High Availability options
- RADIUS & LDAP-based authentication capability

Centralized and Fully Customizable Management

The Sourcefire Defense Center management console is the "nerve center" of the Sourcefire 3D® System. Defense Center correlates attacks with real-time network and user intelligence and centrally manages network security and operational functions, including event monitoring, incident prioritization, forensic analysis, and reporting, so that you can better protect your business.

CENTRALIZED COMMAND AND CONTROL

Aggregating and Monitoring Intrusion Events

All Sourcefire 3D events are sent securely from Sourcefire 3D Sensors to the Defense Center (DC) for centralized analysis and storage. Designed with enterprise deployments in mind, Defense Center is capable of collecting events from up to 100 sensors and handling a maximum of one hundred million events.

MODEL	DC500	DC1000	DC3000
Management Interfaces (copper)	RJ45	RJ45	RJ45
Memory (RAM)	1GB	2GB	4GB
Maximum Event Storage	2,500,000	10,000,000	100,000,000
Maximum Sensors Managed	3*	25	100

Table 1. Sourcefire Defense Center Appliance Family

*No single sensor larger than Sourcefire 3D2100

Defense Center includes a powerful, yet easy-to-use, Web-based interface for event viewing, reporting, and forensic analysis. Customizable workflows enable users to tailor the interface to fit the way they investigate and analyze security events. Users can choose from dozens of pre-configured event views, making it easy to view large volumes of events by a wide range of criteria. Event views are easily customized and can be stored for later reuse.

Detection Policy Management

With Defense Center, users have complete control of policies and configuration of up to 100 3D Sensors from a single management console. Sourcefire IPS™ and Sourcefire RNA® (Real-time Network Awareness) policies can be pushed down to all sensors, or a number of policies can be created for individual sensors or sensor groups.

- Group sensors logically for easier policy management
- Import/export capabilities for IPS and RNA policies

Sensor Management and Health Monitoring

Depending on the Defense Center appliance model, a maximum of 3, 25, or 100 3D Sensors can be administered from a single DC interface. Once a sensor is assigned to a DC, an Admin can view its connection status, edit sensor properties, delete sensors, and create/manage/edit sensor groups.

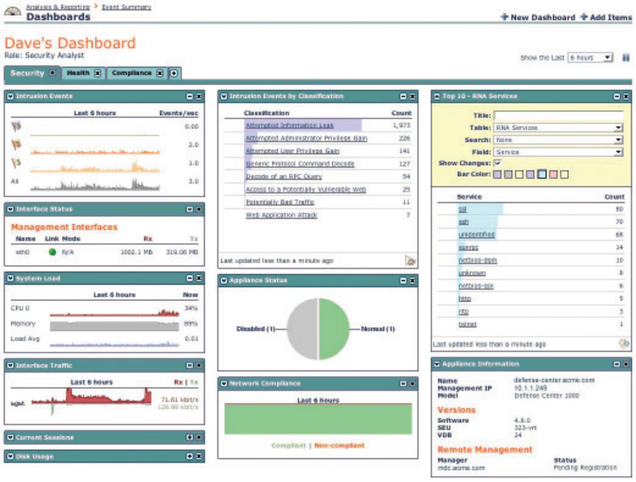
In addition to collecting and taking action on security events, Defense Center provides centralized health monitoring for all sensors. You can be alerted when sensors are offline or overloaded, and the DC can alert users of critical sensor metrics like temperature, CPU utilization, and available disk capacity.

> *"The Sourcefire solution has allowed us to expand the system to monitor seven network segments and manage all from a single Defense Center."*
>
> **Greg Clayton, Assistant VP and Network Security Manager, BankersBank CardServices (BBCS/TIB)**

Reports, Alerts, and Dashboards

Defense Center provides customers with powerful reports, alerts, and dashboards. Customers can leverage a variety of pre-defined report templates or create custom reports to meet the needs of any organization. Reports can be created in PDF, HTML, and CSV formats, which can be automatically e-mailed for easy distribution. Analysts can receive alerts in the form of e-mail messages or SNMP alerts.

Using Defense Center, customers can create fully customized dashboards with dozens of pre-defined or custom drag-and-drop "widgets" that display critical information in the form of tables and graphs. The dashboard appears immediately after the user logs into the DC and becomes the focal point for monitoring security and compliance events generated by the 3D System. Additional dashboard benefits include interactive drill-down to navigate to raw event data or 3D System configuration interfaces, granular administrative privileges for creating different levels of access to data/policy, dashboard sharing among colleagues with similar roles, and dashboard tab cycling at a user-defined time interval to ease the monitoring of security, compliance, and administrative events.



Management Interfaces

Name	Link	Mode	Rx	Tx
eth0	●	N/A	1002.1 MB	319.06 MB

	Last 6 hours	Now
CPU 0		34%
Memory		89%
Load Avg		0.01

Classification	Count
Attempted Information Leak	1,973
Attempted Administrator Privilege Gain	226
Attempted User Privilege Gain	141
Generic Protocol Command Decode	127
Decode of an RPC Query	54
Access to a Potentially Vulnerable Web	25
Potentially Bad Traffic	11
Web Application Attack	7

Title:
Table: RNA Services
Search: None
Field: Service
Show Changes: ☑
Bar Color: □ □ □ □ □ □ □

Service	Count
ssl	80
ssh	70
unidentified	68
sunrpc	14
netbios-dgm	10
unknown	8
netbios-ssn	6
http	5
ntp	3
telnet	1

Name	defense-center.acme.com
Management IP	10.1.1.249
Model	Defense Center 1000

Versions

Software	4.8.0
SEU	323-vrt
VDB	24

Remote Management

Manager	Status
mdc.acme.com	Pending Registration

Figure 1. The Sourcefire Defense Center dashboard is fully customizable and provides numerous drag-and-drop widgets that display critical security, compliance, and health events.

Packet-level Forensics

With Defense Center, customers can easily investigate the source and nature of an attack and what steps to take in response. Defense Center gives users sophisticated, highly customizable, easy-to-use workflows for investigating security events down to the packet level. Unlike most other IPSes, Sourcefire's packet-level forensics are enabled by default and do not affect sensor performance.

Automated System Maintenance

Customers can schedule automated system maintenance tasks to occur at the Defense Center at user-defined intervals, including:

- Performing backups
- Generating reports
- Downloading and applying software updates
- Downloading and applying Snort® rules
- Applying recommendations from RNA-Recommended Rules

Sourcefire Defense Center Enables Automated IPS with Real-Time Network Intelligence

- 24x7, passive network discovery provided by Sourcefire RNA
  - » Know what hosts you're protecting on a continuous basis
  - » Obtain a real-time inventory of all OSes, services, applications, protocols, & potential vulnerabilities on your network
- Impact Flags assessment (powered by RNA) for determining event relevance
  - » Real-time asset tracking & potential vulnerability assessment
  - » Event impact analysis based on your dynamic network
  - » False positive reduction by up to 99%
- Adaptive IPS
  - » RNA-Recommended Rules takes guesswork out of determining which IPS rules to enable & disable
  - » Non-Standard Port Handling helps to prevent possible IPS evasions by inspecting traffic on non-standard ports
  - » Adaptive Traffic Profiles helps to prevent possible IPS evasions attempted through traffic fragmentation

ENABLING AUTOMATED IPS WITH REAL-TIME NETWORK INTELLIGENCE

Network Discovery

Defense Center is far more than a management solution. Customers who use Sourcefire RNA can build a complete "network map" of their environment. RNA provides 24x7 network intelligence, storing a real-time inventory of all operating systems (OSes), services, applications, protocols, and potential vulnerabilities that exist on the network. The network map is maintained in real time on the DC, and alerts can be generated when a change occurs or when a new device is installed on the network.

Event Correlation

RNA discovers each asset's OS and its active services, protocols, and client applications, and then determines its potential vulnerabilities. Snort-based security alerts are generated at the sensor and forwarded to the DC. The DC evaluates each threat against RNA's asset data, forming the context from which the "impact" of the attack can be determined. The DC instantly correlates attack relevance based on the nature of the attack and the characteristics of the target asset. The result is real-time impact assessment and prioritization shown via **Impact Flags** to focus security analysts on the relatively small number of events that really matter, saving valuable time and maximizing network protection.

- Real-time asset tracking and change detection
- Event impact analysis
- False positive reduction by up to 99%

Adaptive IPS

We have explained how Defense Center performs event correlation for the Impact Flags feature of Sourcefire's Adaptive IPS strategy, which provides automated impact assessment and IPS tuning. Now let's discuss the DC's role in the remaining Adaptive IPS features—RNA-Recommended Rules, Non-Standard Port Handling, and Adaptive Traffic Profiles.

The **RNA-Recommended Rules (RRR)** feature takes the guesswork out of determining which IPS rules to enable and disable by recommending only those rules that pertain to potential vulnerabilities associated with the host and service information contained in the network map maintained on the DC. As new devices join or leave the network, RRR can prompt policy personnel that new rules are needed or can be disabled. The **Non-Standard Port Handling** feature helps to prevent possible IPS evasions by inspecting traffic on non-standard ports. RNA identifies the ports and services on the hosts it's monitoring and adds this information to the network map. The DC then configures the IPS to dynamically apply the correct rules for any non-standard ports. The **Adaptive Traffic Profiles** feature helps to prevent possible IPS evasions attempted through traffic fragmentation. Via the DC, RNA provides OS data about each host to the 3D Sensor so that the sensor can dynamically adjust the traffic reassembly process in a manner consistent with different target OSes.

None of the aforementioned Adaptive IPS features are possible without the powerful aggregation and correlation capabilities of Defense Center.

TOOLS FOR THE ENTERPRISE

Compliance White Lists and Policy and Response Rules

Compliance "white lists" and Policy and Response (P&R) rules can be used to monitor and enforce IT policy compliance. Armed with the real-time network map powered by RNA, Admins can create compliance white lists of approved host assets by simply checking and un-checking those OSes, services, applications, and protocols that can and/or cannot be used on a particular network. Defense Center will then generate alerts if RNA sees changes that indicate the violation of a compliance policy, such as introduction of unauthorized OSes, services, or applications. These alerts can be used to trigger automated responses including quarantining assets from the network.

Network Behavior Analysis

RNA's built-in RNA Flow capability, and/or the optional Sourcefire NetFlow Analysis module, can be used to perform Network Behavior Analysis (NBA). Sourcefire's NBA solution benefits both Information Security and Network Operations groups. RNA or NetFlow Analysis enables Information Security to guard against attacks that originate from the inside by establishing "normal" traffic baselines and detecting network anomalies. When anomalies are detected, Defense Center can send real-time alerts via e-mail or SNMP. With information from RNA or NetFlow Analysis, the DC also enables Network Operations to monitor bandwidth consumption across the network and troubleshoot network outages and performance degradations.

Sourcefire RUA—Link User Identity to Security and Compliance Events

Sourcefire is the only IPS provider to link user identity to security and compliance events. Sourcefire RUA™ (Real-time User Awareness) passively detects Active Directory (AD) and LDAP logons, pairs usernames with their corresponding host IP address, and forwards the information to Defense Center. For each username shown on the DC's Table View of Users, the security analyst can see the corresponding IP address and the user's first and last name, department, e-mail address, and phone number. RUA drastically reduces the time and effort to determine users affected by security and compliance events, when time is of the essence.

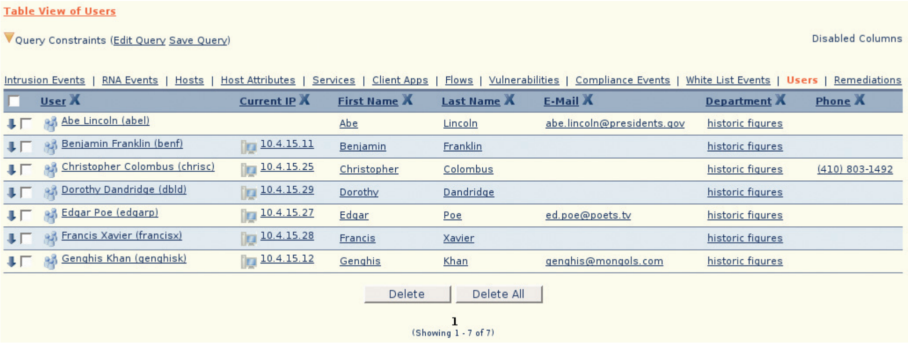


Table View of Users

Query Constraints (Edit Query Save Query)

Disabled Columns
Intrusion Events | RNA Events | Hosts | Host Attributes | Services | Client Apps | Flows | Vulnerabilities | Compliance Events | White List Events | Users | Remediations

User	Current IP	First Name	Last Name	E-Mail	Department	Phone
Abe Lincoln (abel)		Abe	Lincoln	abe.lincoln@presidents.gov	historic figures	
Benjamin Franklin (benf)	10.4.15.11	Benjamin	Franklin		historic figures	
Christopher Colombus (chrisc)	10.4.15.25	Christopher	Colombus		historic figures	(410) 803-1492
Dorothy Dandridge (dbld)	10.4.15.29	Dorothy	Dandridge		historic figures	
Edgar Poe (edgarp)	10.4.15.27	Edgar	Poe	ed.poe@poets.tv	historic figures	
Francis Xavier (francisx)	10.4.15.28	Francis	Xavier		historic figures	
Genghis Khan (genghisk)	10.4.15.12	Genghis	Khan	genghis@mongols.com	historic figures	

(Showing 1 - 7 of 7)

Figure 2. Sourcefire RUA immediately provides full contact information for a username associated with a security or compliance event.

Powerful Integration with Third-Party Systems

Sourcefire offers more ways to integrate with third-party security and network management products than any other IPS vendor. Defense Center provides a number of remediation options, and virtually any kind of event, including IPS events, RNA events, and 3D health alerts, can be used to initiate a number of responses. Responses include the creation of syslog events, SNMP alerts, event logging, or the initiation of a custom response by leveraging the DC's Remediation API. The Remediation API ships with a number of pre-built response modules for passing critical alert data to third-party products, including Cisco routers and PIX firewalls, OPSEC for Check Point's VPN-1/FW-1, NMAP, and Nessus. Admins can build their own modules and achieve additional integration with a variety of other third-party applications, including helpdesk, NAC, and patch management solutions.

Sourcefire Defense Center Enables Numerous Enterprise Tools

- Compliance white lists & P&R rules to monitor & enforce IT policy compliance
- Network Behavior Analysis (NBA)
  - » Detect & quarantine internal threats by establishing traffic baselines & detecting anomalies
  - » Monitor bandwidth consumption across the network
  - » Troubleshoot network outages & performance degradations
- Sourcefire RUA for linking user identity to security & compliance events
  - » Click on username to access full contact info
    - First & last name
    - Department
    - E-mail address
    - Phone number
  - » Support for Active Directory & LDAP
- Third-Party System Integration Options
  - » eStreamer API for offloading host & event data to 3rd-party applications
  - » Remediation API for integrating Sourcefire event data into 3rd-party applications
  - » Direct active scanning instances using NMAP & Nessus
- Sourcefire MDC mode for managing up to 10 subordinate DC appliances

> *"Once inside the manager—in this case, the Sourcefire Defense Center—we can view more details about the alert and even start packet captures, if necessary. Packet captures are very beneficial tools that we used as part of this pilot which are not always available on other products."*
>
> **Tristan Morel L'Horset, Director of Managed Security Services, Unisys Federal Government Group**

In addition, all IPS, RNA, and 3D Sensor health events on the DC can be forwarded via the eStreamer™ API to other applications, such as SIEM and network management platforms. The eStreamer API includes a "reference client" that allows customers to format and integrate precisely the data from Sourcefire 3D that they need. eStreamer can also be queried by third-party applications to provide host data stored in the DC's network map.

Sourcefire Master Defense Center—Enterprise Scalability

For very large organizations or organizations with distributed IT personnel, a single DC3000 can be configured in Master Defense Center (MDC) mode to manage up to 10 subordinate DCs, effectively allowing the management of many hundreds of sensors from a single management console. Sourcefire is the only IPS vendor to offer this powerful management capability.

Subordinate DCs can forward and aggregate selected events to the MDC for further analysis and alerting. IPS, RNA, system, and health policies can also be pushed down from the MDC to subordinate DCs and/or sensors from one centralized MDC console.

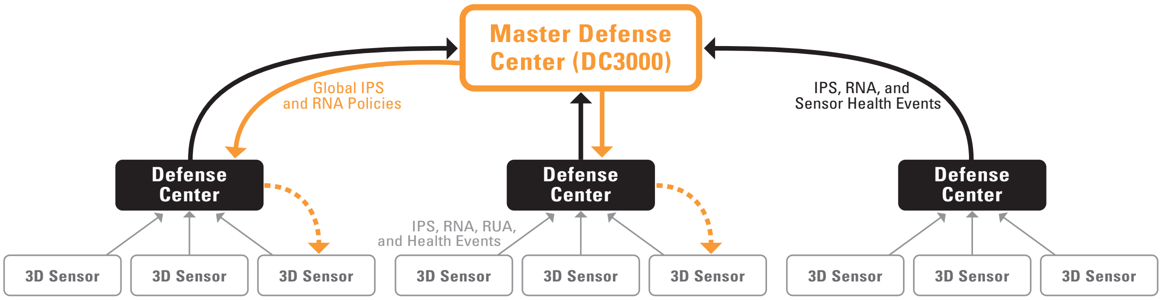

Master Defense Center (DC3000)
Global IPS and RNA Policies
IPS, RNA, and Sensor Health Events
Defense Center
Defense Center
Defense Center
IPS, RNA, RUA, and Health Events
3D Sensor
3D Sensor
3D Sensor
3D Sensor
3D Sensor
3D Sensor
3D Sensor
3D Sensor
3D Sensor

Figure 3. Sourcefire's Master Defense Center (MDC) capability allows management of up to 10 subordinate DC appliances.

With the MDC capability, enterprises of all shapes and sizes can reduce operating costs and achieve economies of scale when multiple DC appliances are spread throughout their organization.

TAKE THE NEXT STEP TO PROTECT YOUR NETWORK

Sourcefire Defense Center is a highly customizable centralized management console for basic security and operational tasks, but it also does so much more. Below is a summary of Defense Center's key capabilities.

- Centralized event monitoring and sensor management
- Customizable dashboards with numerous drag-and-drop widgets
- Sophisticated and customizable reporting
- E-mail and SNMP alerts
- Automated Sourcefire VRT rules updates
- Enables real-time network intelligence, automated impact assessment, automated IPS tuning, IT policy compliance, NBA, and user identification
- Store up to 100,000,000 events and manage up to 100 3D Sensors from a single DC
- Master Defense Center (MDC) capability for managing up to 10 subordinate DC appliances

To learn more about Sourcefire Defense Center, visit our Web site at www.sourcefire.com or contact Sourcefire or a member of the Sourcefire Solutions Network™ today.