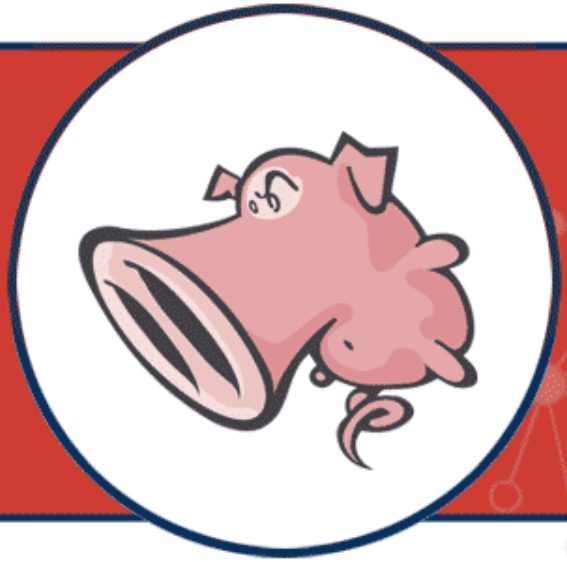
SECURITY for the REAL WORLD.



Sourcefire 3D™ System for Enterprise Threat Management

Mark Ermence
Sr Security Engineer

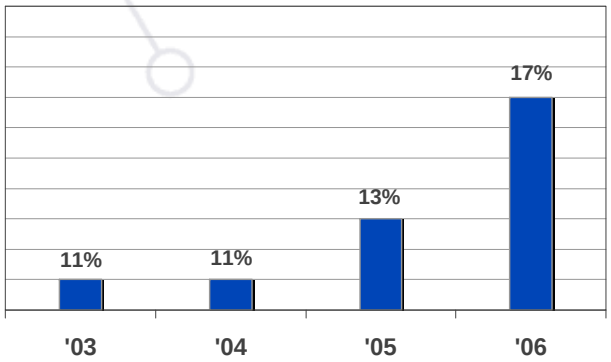
SOURCEfire

The Real Problem to be Solved

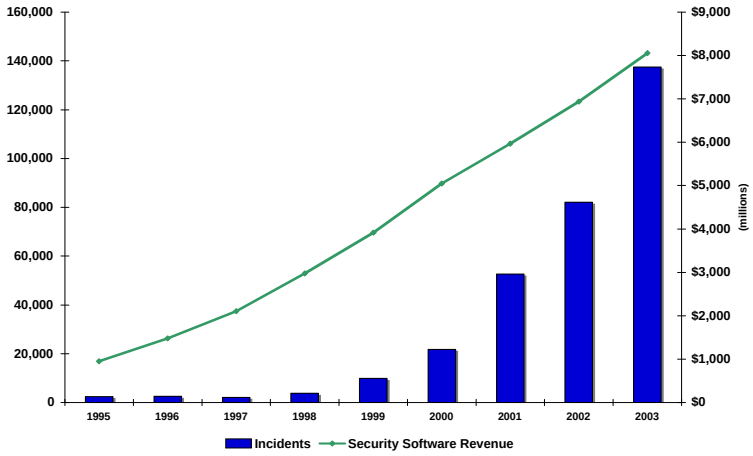
SOURCEfire
Security for the real world.

Reassessing Enterprise Threat Management

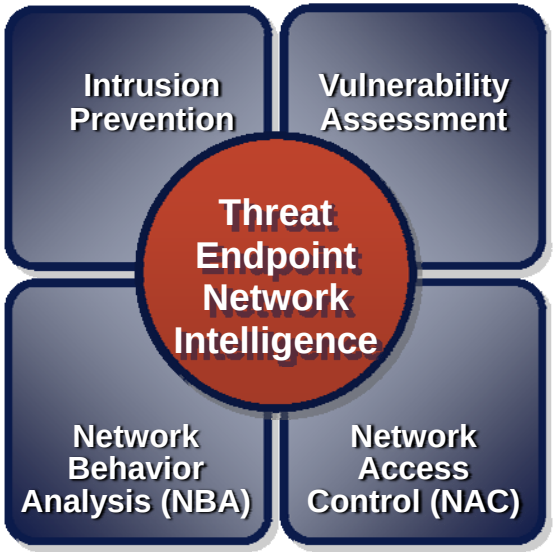
Security spending is dramatically growing as a percentage of the overall IT budget…



Source: 2006 CIO/CSO/PWC State of Info Security Survey



Yet the threats keep coming! A new approach is needed.

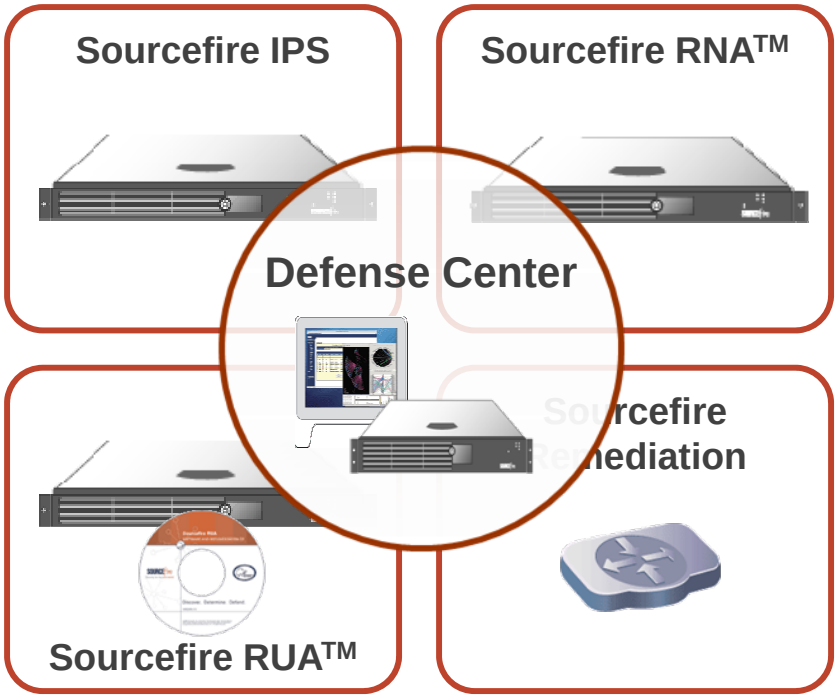


Systems must work more intelligently to solve the core problems

SOURCEfire
Security for the real world.

Introducing the Sourcefire 3D System

- Monitors network traffic
- Leverages Sourcefire VRT Rules to identify malicious traffic
- In-line or passive mode of operation



- Provides network and endpoint intelligence
- Provides passive and active methods of discovery

- Baselines normal behaviour of network devices and alerts on exception
- Maps identity of users to networked computers

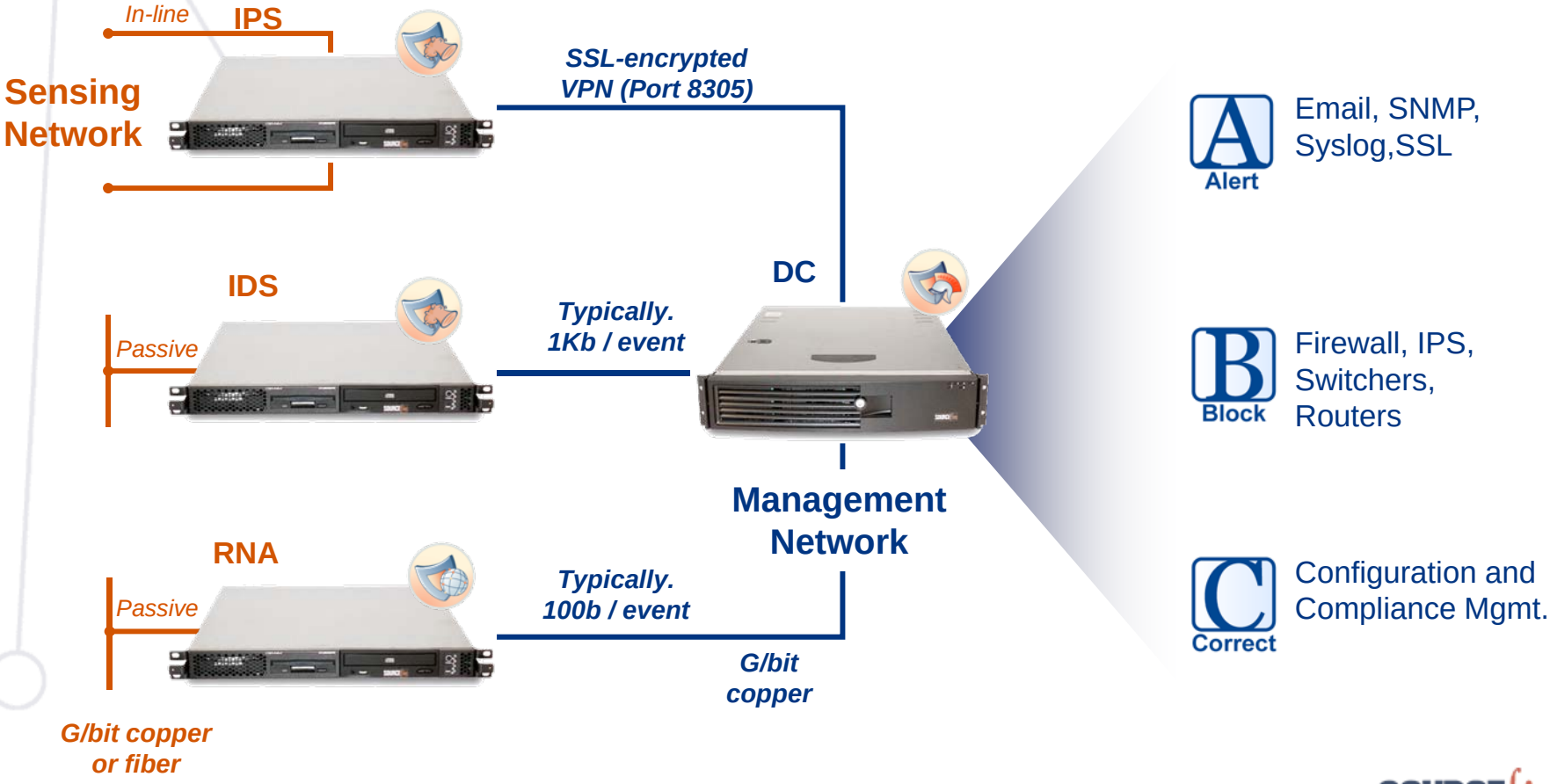
- Automates security response
- Interfaces with your security ecosystem

- Centrally manages, enforces, and reports on security, policy, and compliance
- Correlates and analyzes events
- Provides sensor lifecycle management and system health status

SOURCEfire
Security for the real world.

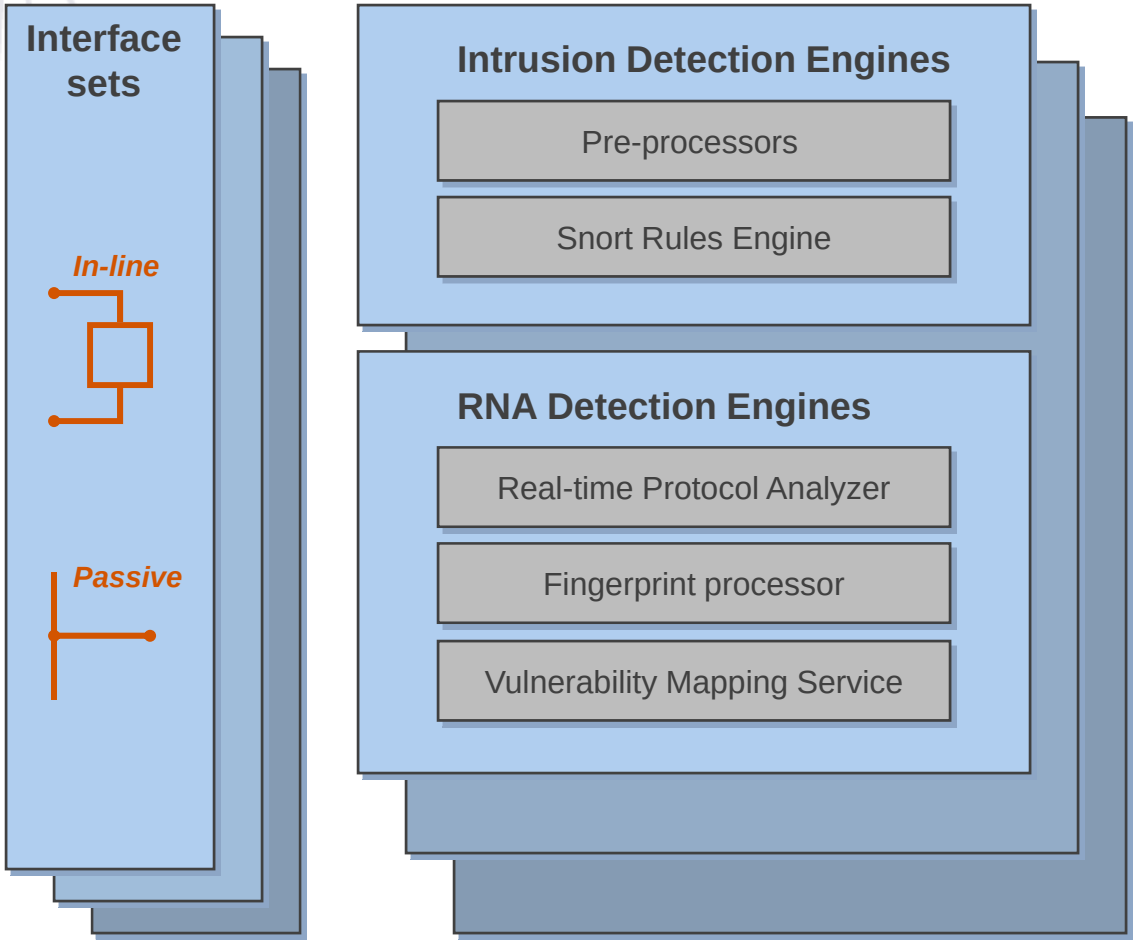
Sourcefire 3D System Components

Discover → **Determine** → **Defend**



SOURCEfire
Security for the real world.

Sensor Architecture



SOURCEfire
Security for the real world.

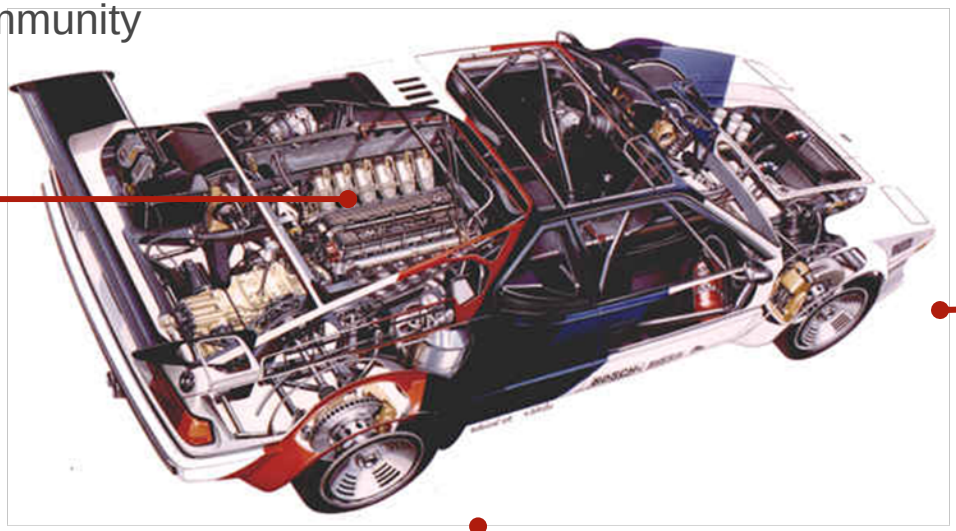
If Sourcefire Made Cars…

Snort®: The Engine

- 80+ OEMs
- Enormous Community

Sourcefire: The Car

- Torque to motion
- Enterprise quality



Snort® Rules: The Fuel

- Open rule set
- Rules, not signatures

SOURCEfire
Security for the real world.

Vulnerability Research Team (VRT)

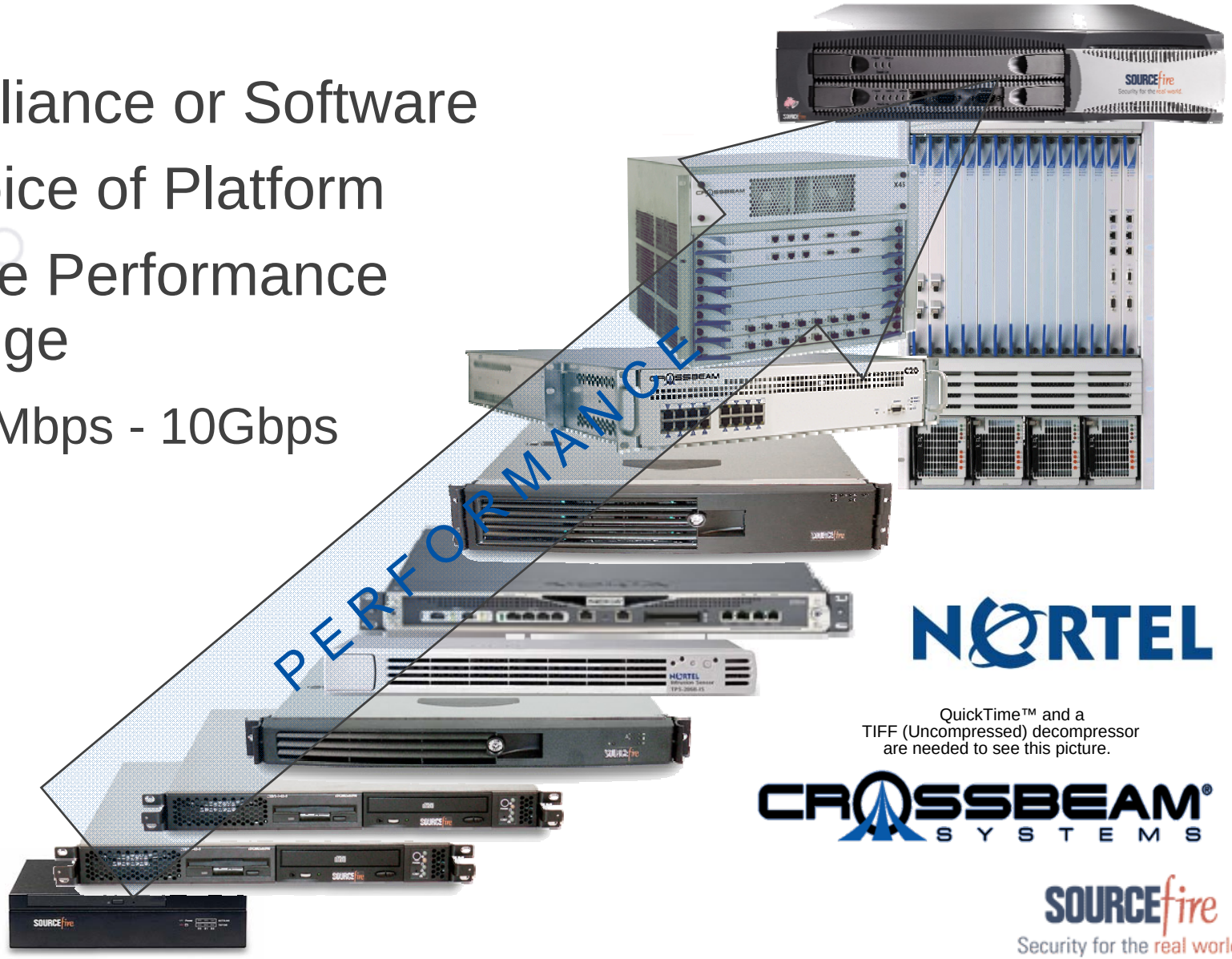
- 10 million dollar investment
  - 200 server regression test facility
- Write rules not signatures
- Full-time team:
  - Analyse vulnerabilities
  - Reverse-engineer patches
- Regular rules updates

VRT Regression Facility, Columbia MD

SOURCEfire
Security for the real world.

Intrusion Sensor Capabilities

- Appliance or Software
- Choice of Platform
- Wide Performance Range
  - 5Mbps - 10Gbps



NORTEL

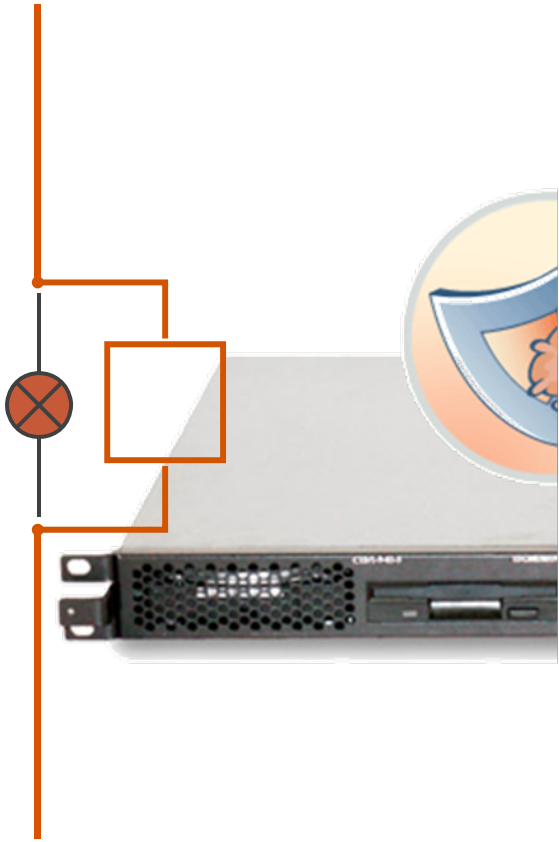
QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

CROSSBEAM SYSTEMS

SOURCEfire
Security for the real world.

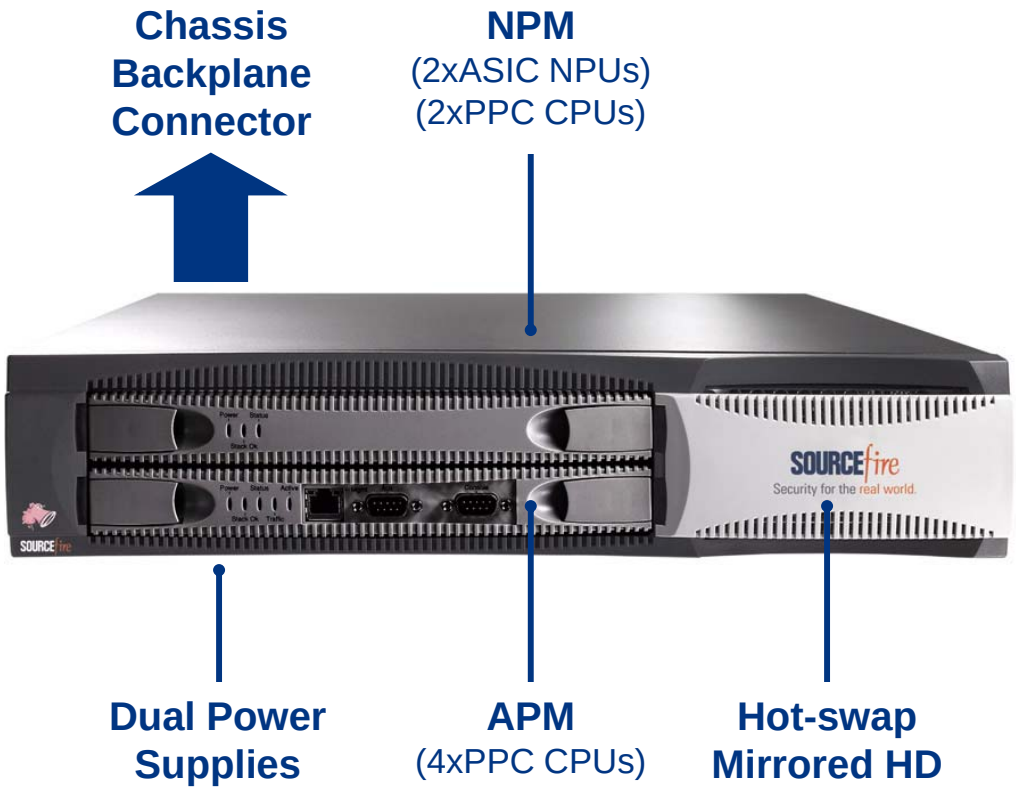
In-line Sensor Failover

- Intrusion sensors use a special failover NIC
- NIC failover circuitry enters bridge mode on the following conditions
  - Sensor loses power
  - Sensor suffers software failure
  - Sensor intentionally shut down
- Change is instant



Ultimate Performance IS-5800

- Hybrid ASIC/PowerPC (G5) architecture
- ‘Stackable’ chassis enables scalable performance
  - 8/4 Ports (IDS/IPS) per chassis
- Line speeds of 3.5/4 or 7/8 Gbps (IPS/IDS)
- Unsurpassed protection for VoIP technology
- Fault Tolerant design



SOURCEfire
Security for the real world.

Breaking the 10G Barrier
Sourcefire 3D9800 Sensor

- Aggregate throughput of 10Gbps
- Up to 2 Network Interface Modules (NIMS)
  - 12 ports @ 1Gbps copper / NIM
  - 6 ports @ 1 Gbps fiber / NIM
  - 2 ports @ 10 Gbps fiber / NIM
- All with bypass

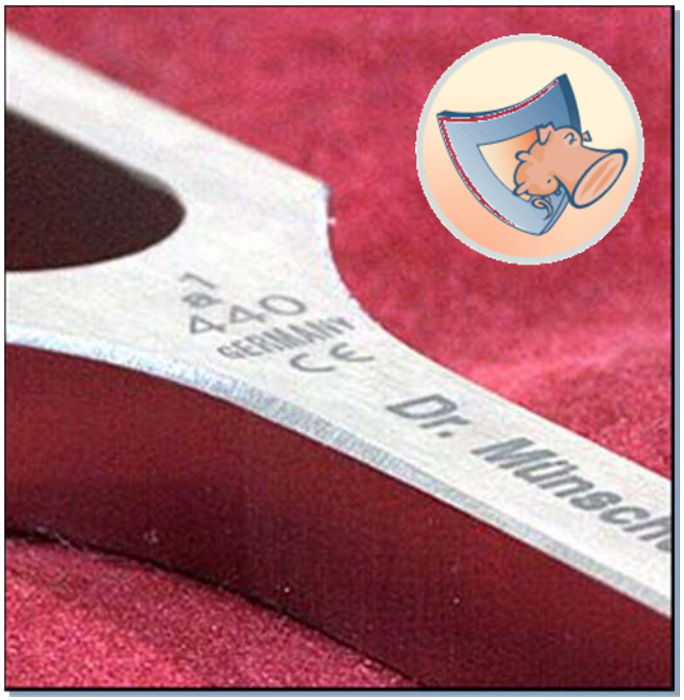
SOURCEfire
Security for the real world.

Intrusion Sensor Enhancements
Version 4.7

- Default IPS Policies
  - Three levels:
    - Conservative
    - Moderate
    - Aggressive
- Port lists
  - HTTP_SERVERS=[80,8080,3128]
- Conservative default search algorithm
  - Ac-bnfa
- Latency Capping

Tuning Sensors

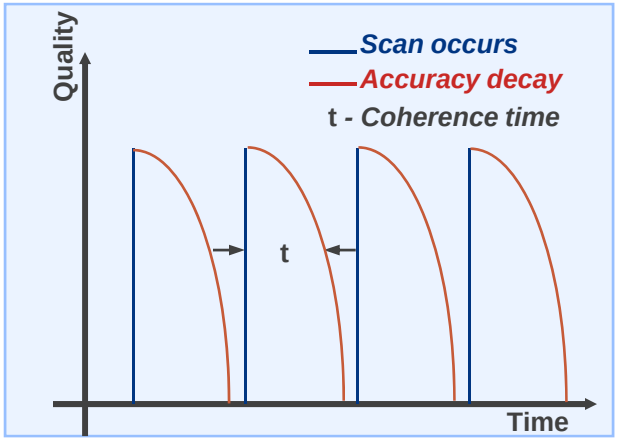
- Sensor tuning is important for performance and alert validity
  - Statistical data from intrusion sensors can be easily used for tuning
  - In v4.7, RNA can auto-tune the intrusion sensor, reducing or eliminating tuning burden.
- Biggest impact on event reduction comes from correlation of passive discovery and intrusion event data



Why Passive Network Discovery?

Your active scan of the oil refinery SCADA network corrupts control systems data and causes a life-threatening failure of the plant.

Your active scan of the medical imager re-boots the liquid helium controller. Imager down for 2 days due to temperature instability

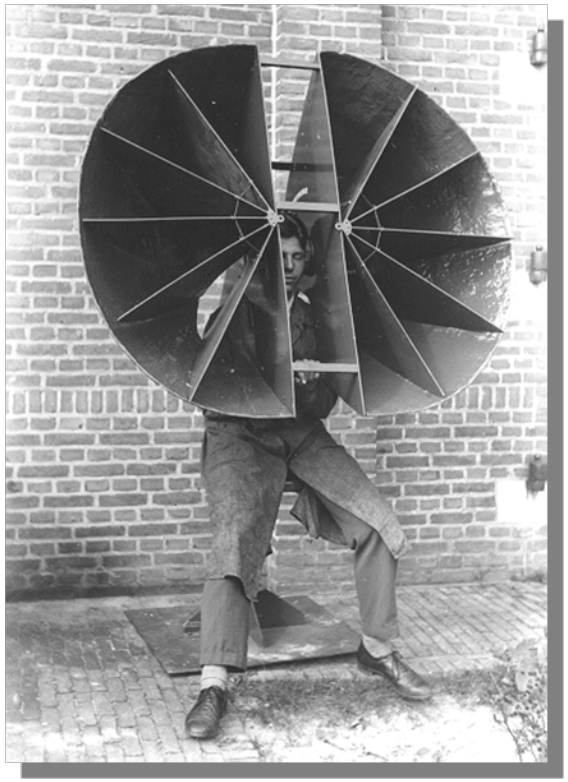


Your active scans never seem to reflect reality for very long

SOURCEfire
Security for the real world.

You Can Learn More By Listening…

- Machines reveal a great deal about themselves:
  - Operating system(s), vendor, version
  - Services, vendors, versions
  - Ports and protocols
  - MAC and IP address(s)
  - Vulnerabilities
  - User data
  - Behavioral information
- Passive discovery is the basis of Sourcefire Real-Time Network Awareness (RNA™)



SOURCEfire
Security for the real world.

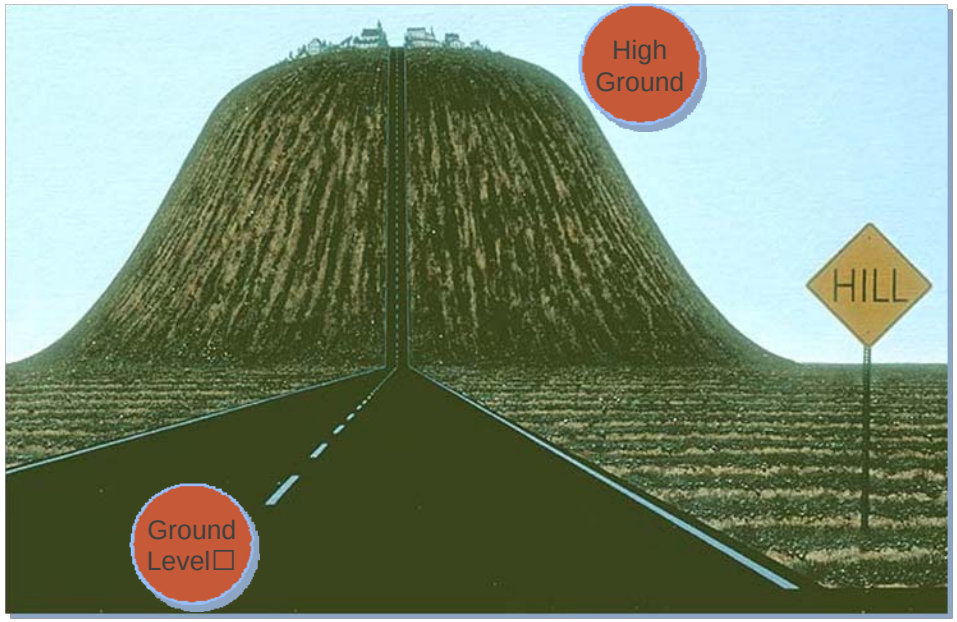
What does RNA Capture?

- Information on Hosts
  - Client/server/bridge
- Information on Services
  - ftp, telnet, ssh …
- Information on Flows
  - Who talked with whom
  - Which protocol, which ports
- RNA continuously computes an error margin and reflects this in a confidence figure.
- From this data, network maps are constructed and vulnerability tables computed.

SOURCEfire
Security for the real world.

RNA Placement Strategy

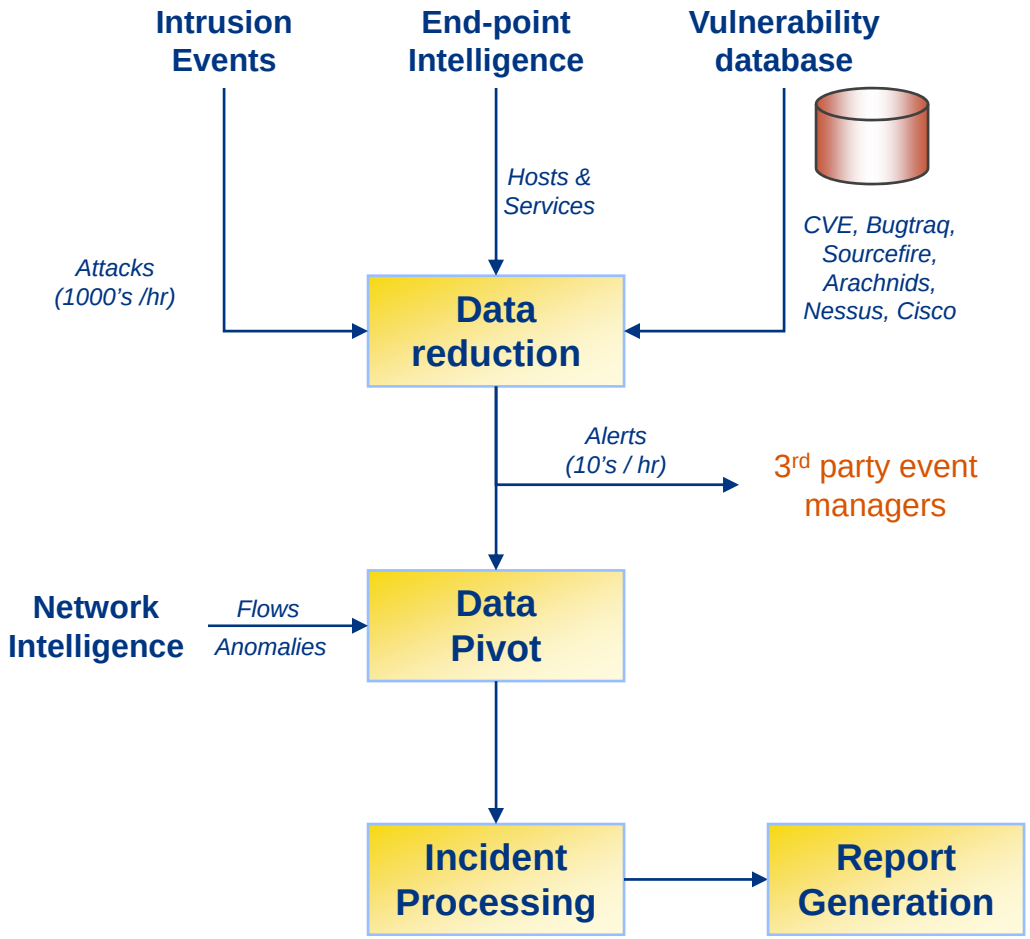
- **On 3D Sensors**
  - RNA pre-installed
  - Often, better to place RNA in different location to intrusion sensor
- "**Ground Level**" - high resolution (on broadcast domain)
  - Good for servers
- "**High Ground**" - high visibility (by DNS, mail servers)
  - Good for workstations
- Most companies mix methods to optimise coverage



SOURCEfire
Security for the real world.

Putting RNA and Intrusion Data to Work
Finding The Events That Matter with The Sourcefire DC

- Defense Center provides powerful data reduction, pivoting and correlation services
- Web-based or optional 3D visualization clients
- Incident management subsystem included
- Easy interface to your existing security ecosystem



SOURCEfire
Security for the real world.

The Power of the Pivot

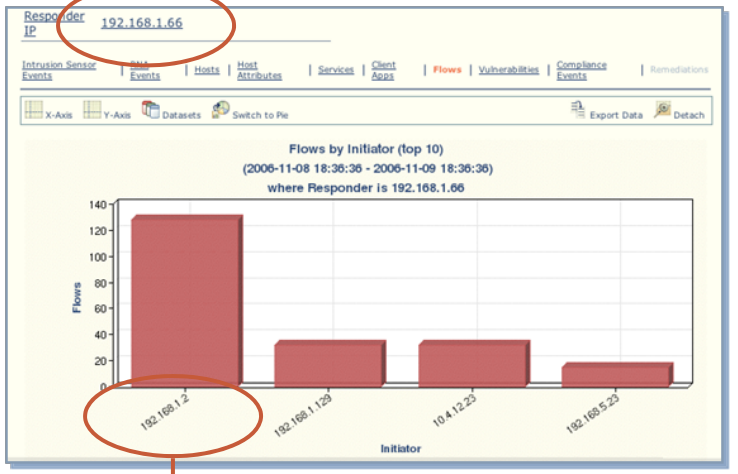
Selection

Suspect candidates

Intrusion Events

on Sensor Events | RNA Events | Hosts | Host Attributes | Services | Client Apps | Flows | Vulnerabilities | Compliance Events

Time	Source IP	Destination IP	Message
2006-11-09 18:15:45	192.168.1.129	192.168.1.66	NETBIOS SMB lsass DsRolerUpgradeDownlevelServer unicode little endian overflow attempt (1:5228)
2006-11-09 18:15:45	192.168.1.129	192.168.1.66	NETBIOS SMB lsass DsRolerUpgradeDownlevelServer WriteAndX unicode little endian overflow attempt (1:2514)
2006-11-09 18:15:45	192.168.1.129	192.168.1.66	NETBIOS SMB IPC$ unicode share access (1:538)
2006-11-09 18:15:24	192.168.1.2	192.168.1.66	NETBIOS DCERPC ISystemActivator path overflow attempt little endian unicode (1:2351)



Other possible victims

Pivot

Drill-down

Initiator IP 192.168.1.2

Intrusion Sensor Events | RNA Events | Hosts | Host Attributes | Services | Client Apps

Initiator IP	Responder IP
192.168.1.2	192.168.1.1
192.168.1.2	192.168.1.66
192.168.1.2	192.168.1.67
192.168.1.2	192.168.1.122
192.168.1.2	192.168.1.120
192.168.1.2	239.255.255.253
192.168.1.2	224.0.0.251

Query Constraints (Edit Query Save Query)

Responder IP 192.168.1.66

Initiator IP 192.168.1.2

Intrusion Sensor Events | RNA Events | Hosts | Host Attributes | Services

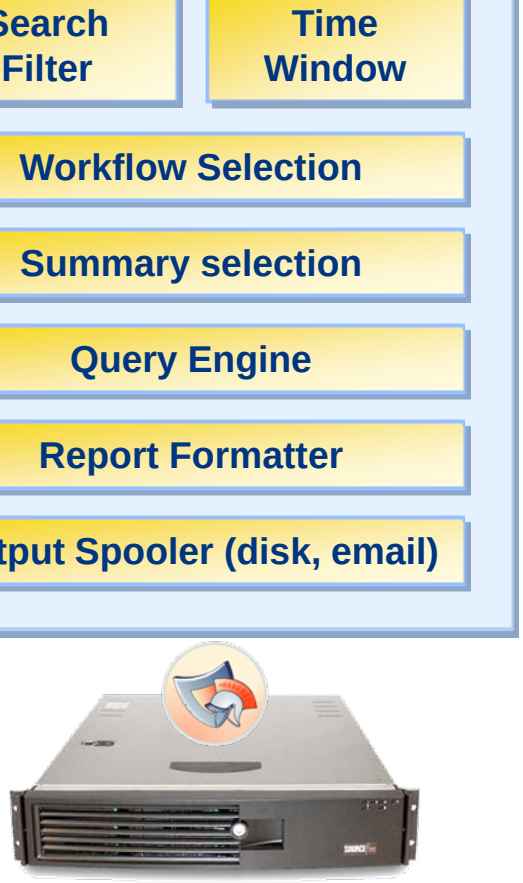
First Packet	Last Packet	Initiator IP	Responder IP
2006-11-09 18:15:40	2006-11-09 18:15:40	192.168.1.2	192.168.1.66
2006-11-09 18:15:24	2006-11-09 18:15:24	192.168.1.2	192.168.1.66
2006-11-09 16:44:26	2006-11-09 16:44:26	192.168.1.2	192.168.1.66
2006-11-09 16:44:10	2006-11-09 16:44:10	192.168.1.2	192.168.1.66
2006-11-09 15:13:12	2006-11-09 15:13:12	192.168.1.2	192.168.1.66
2006-11-09 15:12:56	2006-11-09 15:12:56	192.168.1.2	192.168.1.66
2006-11-09 13:41:57	2006-11-09 13:41:57	192.168.1.2	192.168.1.66

Suspect - victim Conversation

SOURCEfire
Security for the real world.

Powerful Reporting

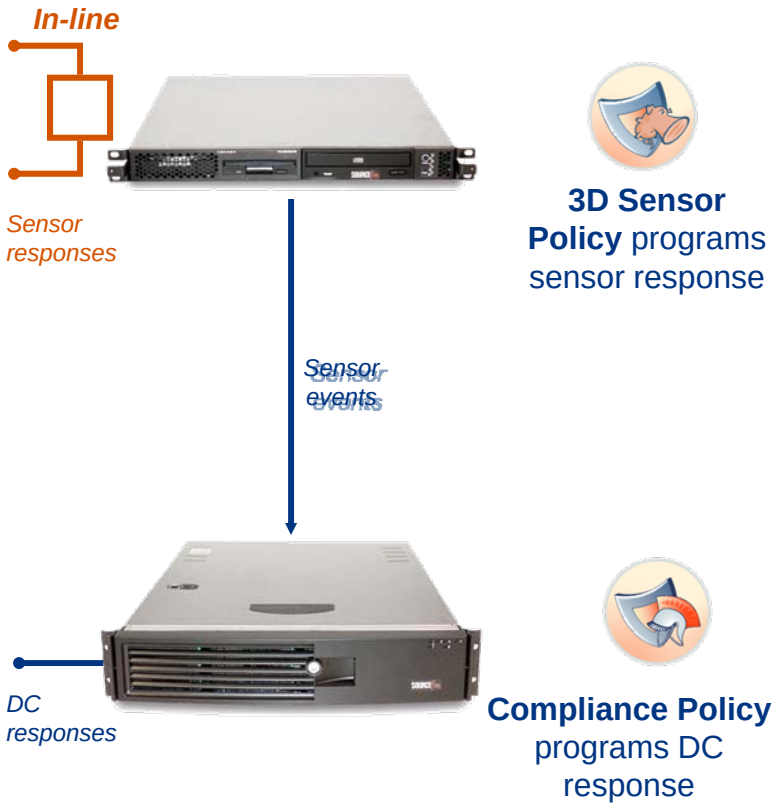
- Tailor reports on your most critical assets
- Automate compliance reporting
  - Schedule tailored reports to be emailed to your compliance managers
- Multiple formats
  - PDF, HTML or Excel
- Stream reporting to 3rd party applications



SOURCEfire
Security for the real world.

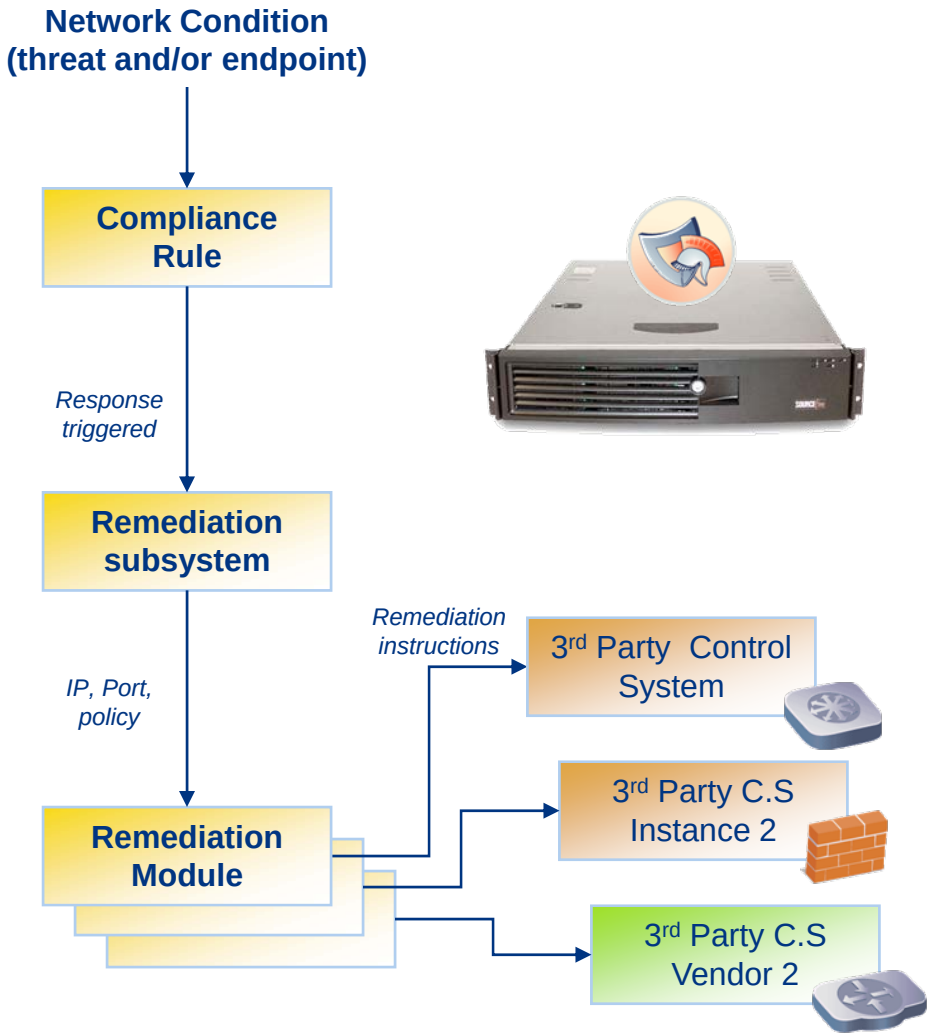
Responding to Network Events
Can Operate At Two Levels

- At 3D Sensor:
  - Drop, Replace, Reset
- At Defense Center:
  - Higher level rule processor operates on intrusion, host, service or flow events
  - Response processor triggers **remediation event**
  - Used for **compliance rules**



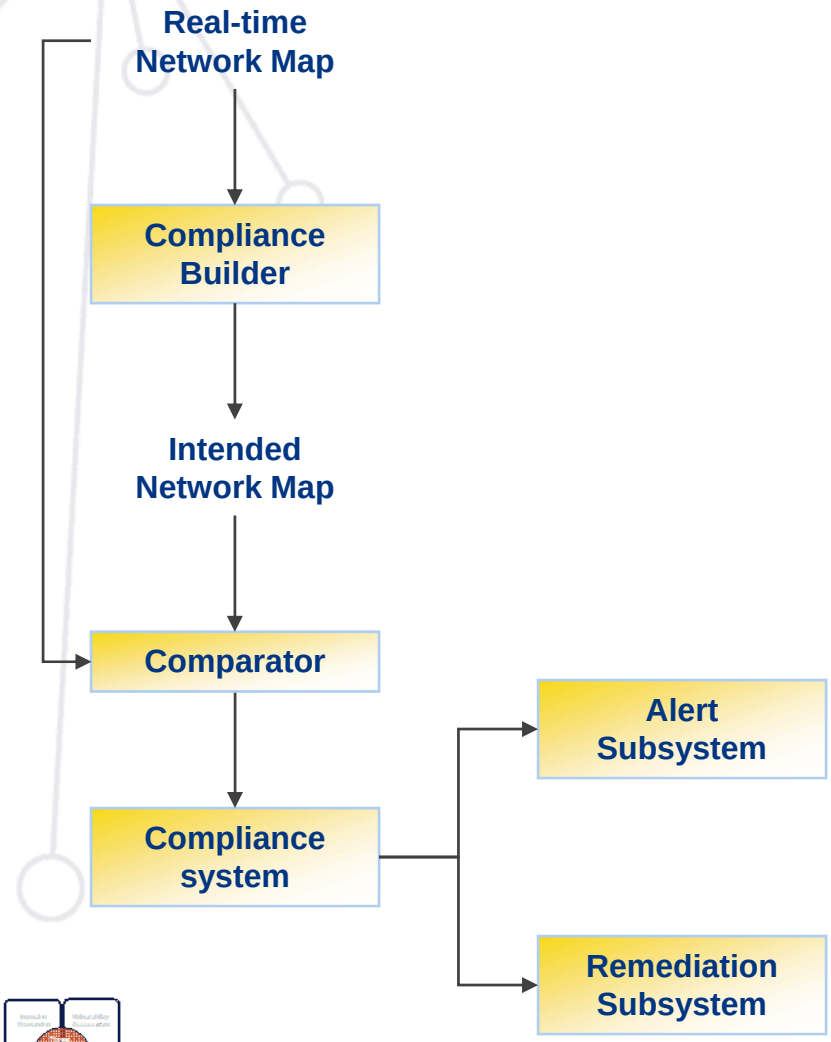
Responding to Network Events
Remediation Subsystem

- Remediation subsystem called when compliance rule conditions are triggered
- Remediation modules simple to write in Bash ,Perl or C
- Remediation modules typically interface to 3rd party control systems
- Pre-written modules:
  - Perform Cisco IOS Null Route, PIX ACL
  - Add temporary Check Point firewall block rule
  - Initiate “surgical scan”

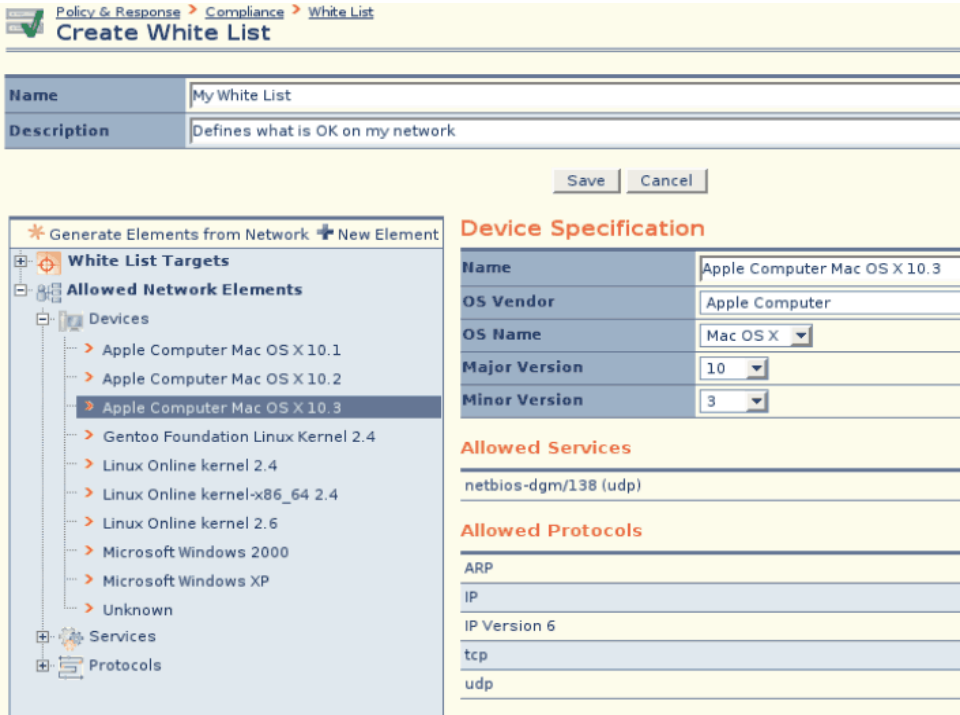


SOURCEfire
Security for the real world.

One-Click Compliance

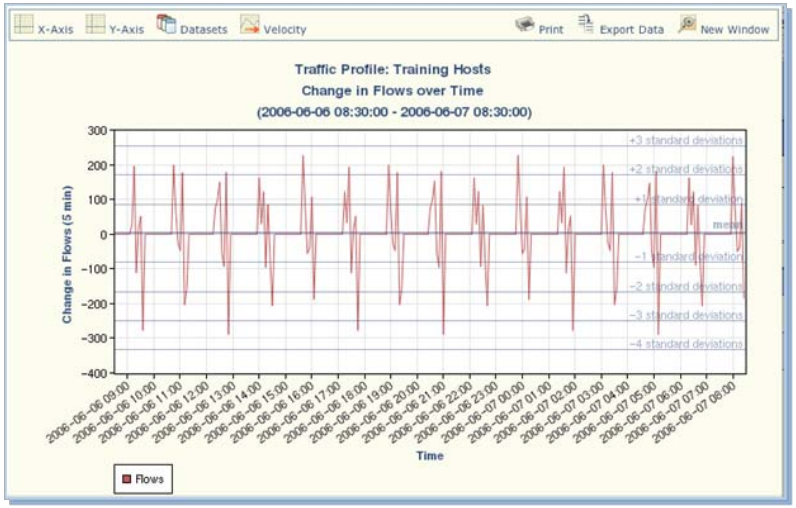


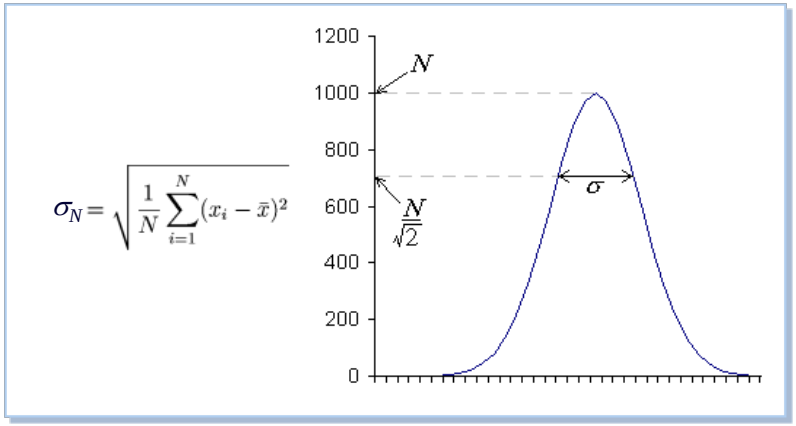
- Maps “what is” to “what should be”
- Facilitates white listing of hosts OS, services and detected applications



Trend Analysis and NBA

- DC can sample flows and perform sophisticated statistical analysis
- Network behaviour is learned over a training period. Any departure triggers an alert
  - Absolute value, derivative (velocity) standard deviation (sigma, σ)
- Many quantities can be sampled

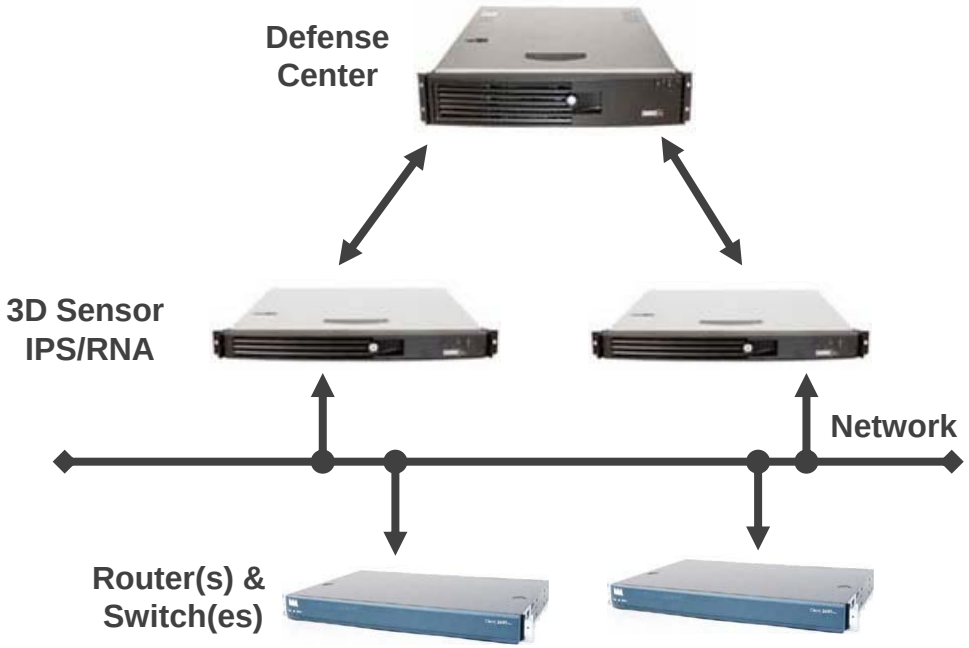




SOURCEfire
Security for the real world.

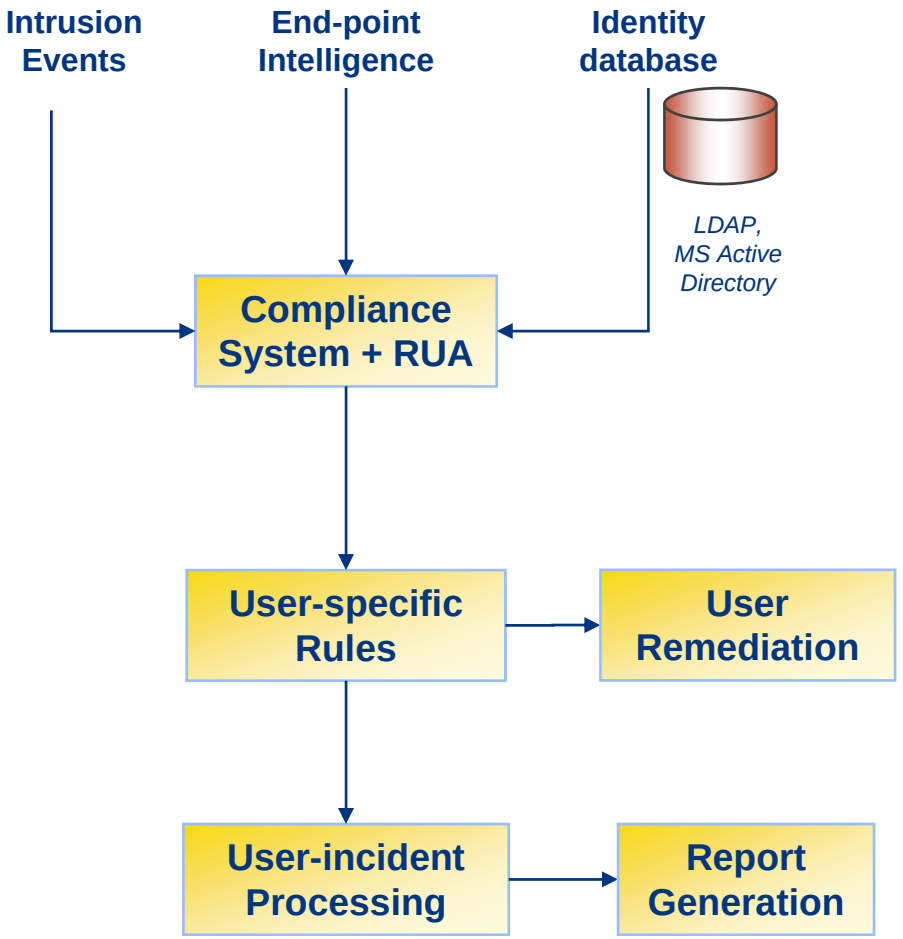
Flow Analysis Enhancements
Version 4.7

- Support for Netflow (v5) collection
  - Configure 3D Sensors to collect Netflow from one or more Netflow sources
  - Combine with RNA native flow data.
  - Extends reach to those areas of the network not monitored by RNA
- Network Map & Topology Improvements
- Flow chunking on native RNA flow data
  - Compression of approximately 5:1



Identity Mapping
Sourcefire Real-time User Awareness (RUA™)

- Maps a user to an IP addresses within the Sourcefire 3D System
- With RUA:
  - Easier to determine physical location of exploited hosts
  - Easier to identify employees hacking into internal systems
  - Easier to set up per-user compliance
- Available in v4.7



SOURCEfire
Security for the real world.

RUA Example
Real-time Network User Lists

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

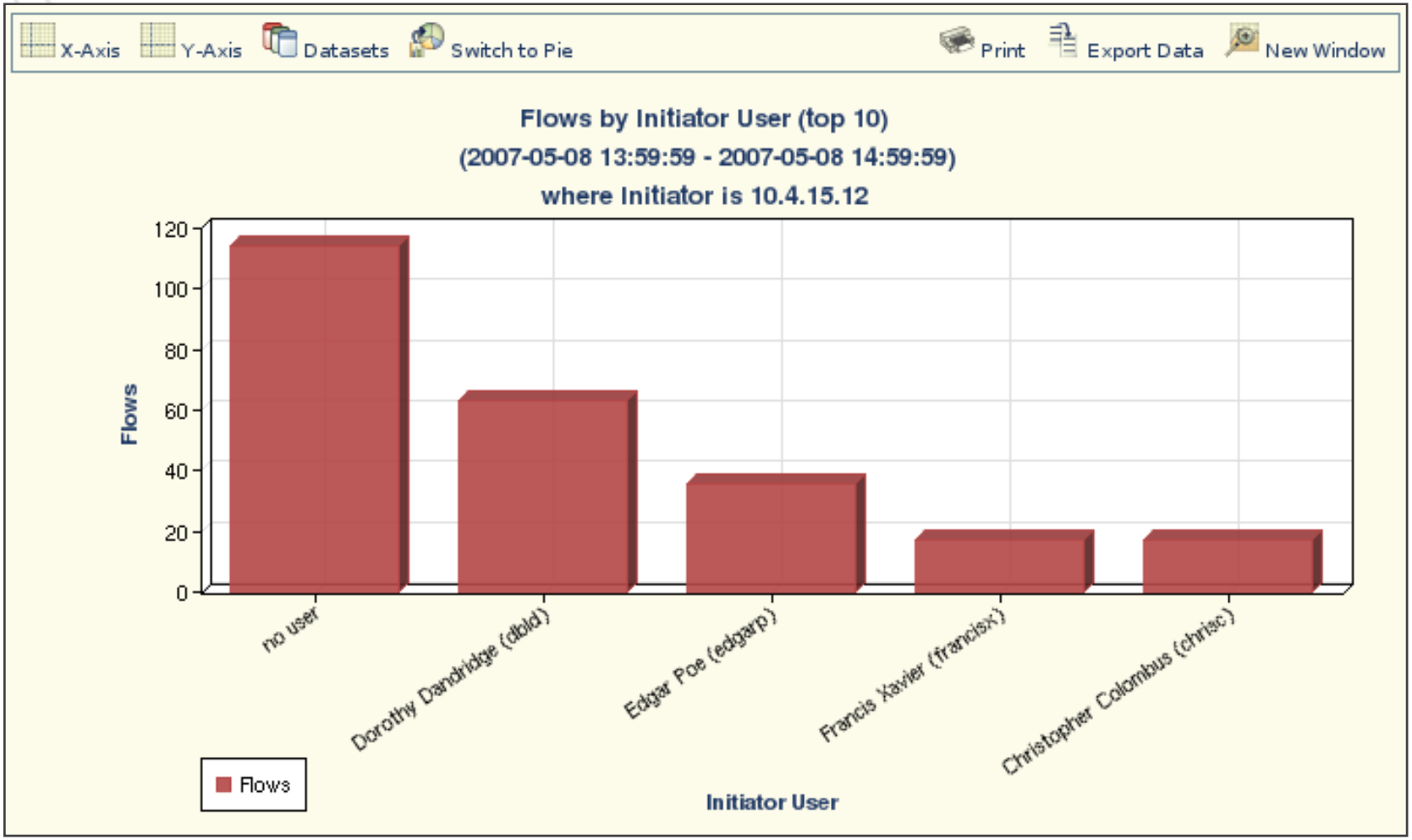
User	Current IP	First Name	Last Name	E-Mail	Department	Phone
Abe Lincoln (abel)		Abe	Lincoln	abe.lincoln@presidents.gov	historic figures	
Benjamin Franklin (benf)	10.4.15.11	Benjamin	Franklin		historic figures	
Christopher Colombus (chrisc)	10.4.15.25	Christopher	Colombus		historic figures	(410) 803-1492
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	

Delete Delete All

1
(Showing 1 - 7 of 7)

SOURCEfire
Security for the real world.

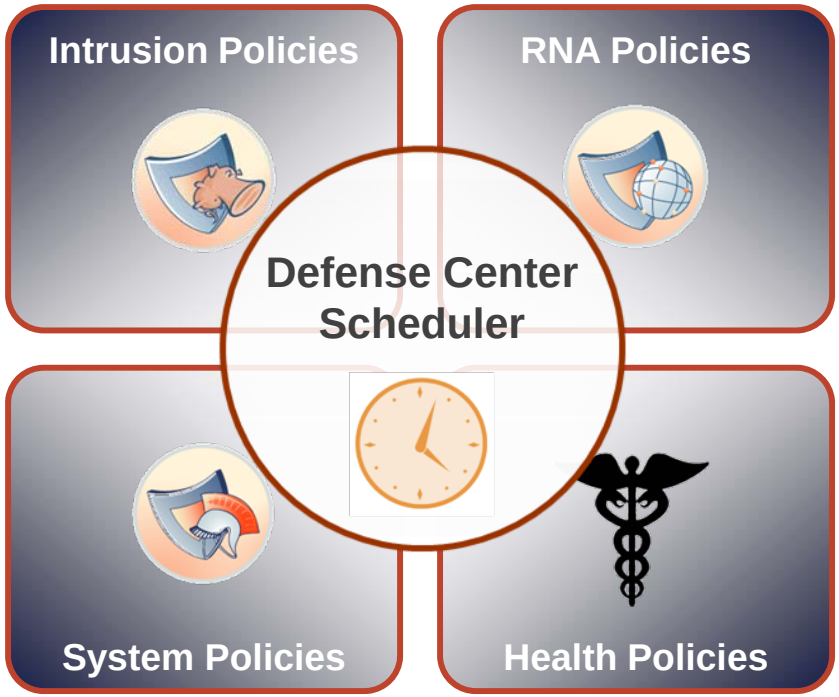
RUA Example
Real-time User Flows



SOURCEfire
Security for the real world.

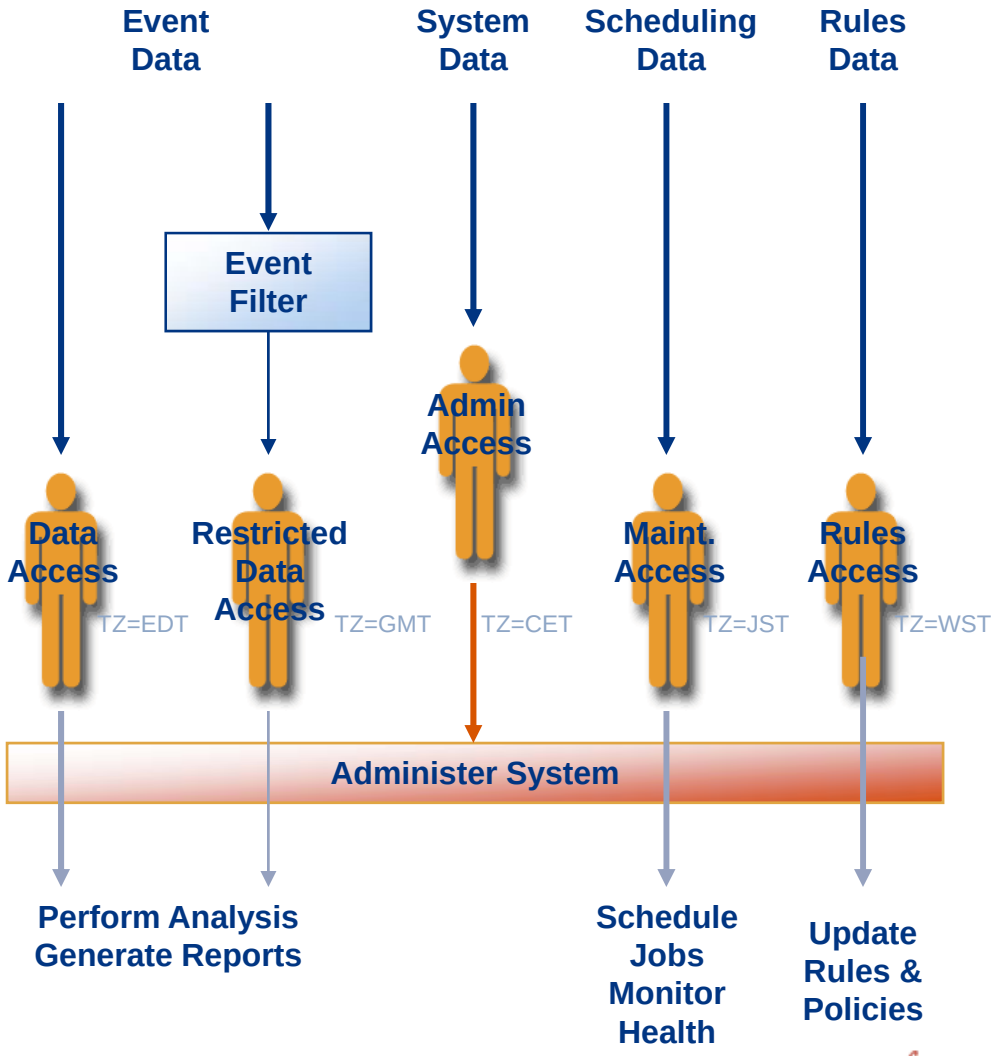
System Management

- All sensors managed via *policies*:
- System Scheduler
  - Download and push rule updates
  - Apply policy changes during quiet periods
  - Download and apply software and rule updates
  - Generate reports
  - Perform backups



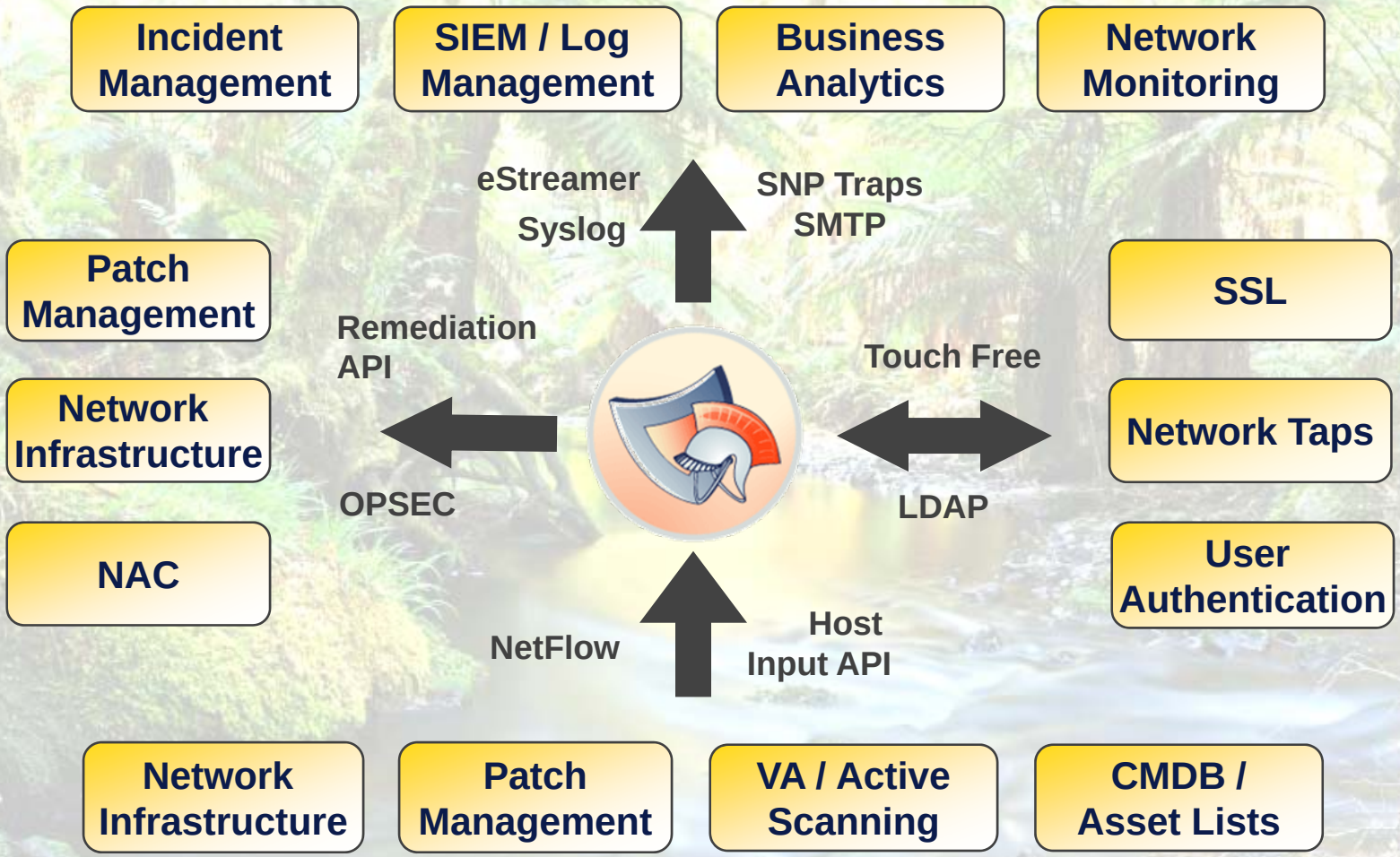
Access Security

- 5 Levels of user privilege
- User-specific environment
  - Local time zone support
  - Per-user ‘skins’ (workflow, address resolution, refresh interval, etc.)
- IP-based access security



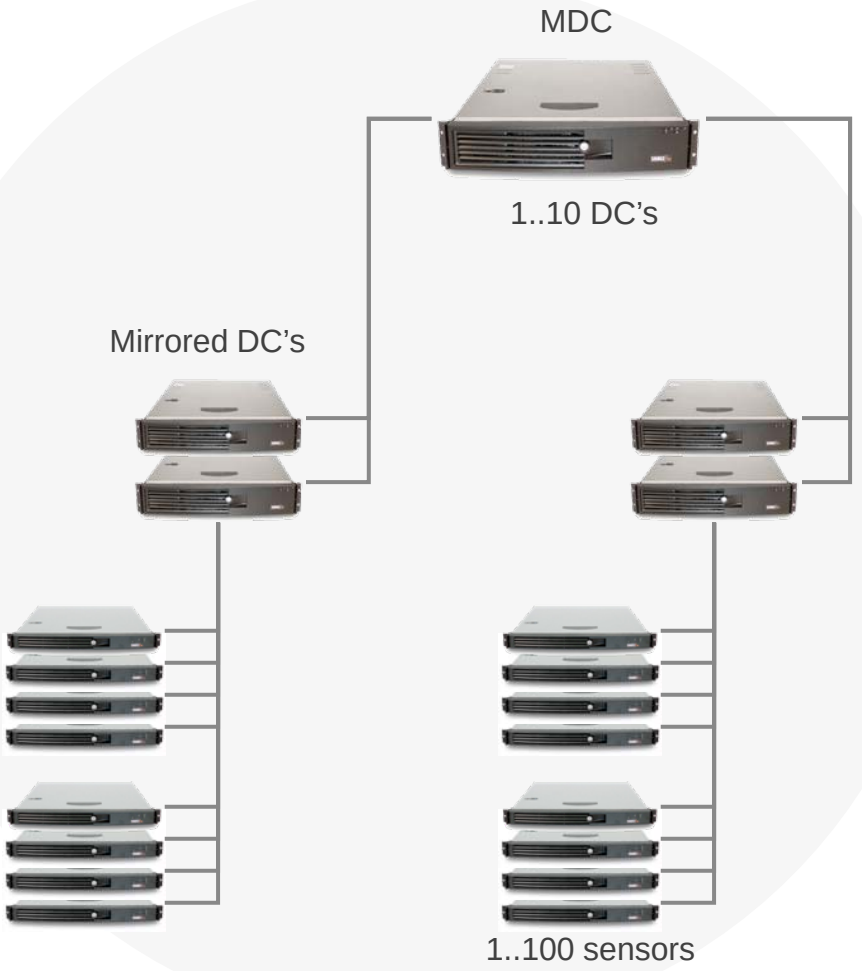
SOURCEfire
Security for the real world.

Integrating With Your Security Ecosystem



Scaling the Global Enterprise

- DC3000
  - 100 sensors
  - 400GB, 100 million events
- DC High Availability
- Master Defense Center
  - Cascade events from 10 DC's for global overview



SOURCEfire
Security for the real world.

DC Enhancements
Version 4.7

- Master Defense Center Phase II
  - Subordinate policy management
  - Mirroring support for MDC and subordinate DC's.
- Host Input API
  - Incorporate external asset information into RNA
- Miscellaneous Improvements
  - Internet Explorer 7
  - Streamlined communications protocols
  - Right mouse actions
  - Improved network map
  - Impact rating of blocked events
  - Prohibit packet capture
  - Snooze health monitoring during maintenance

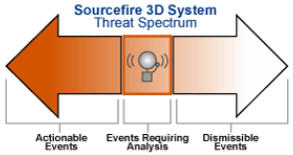
ROA “Return On Analysis”

Threat data

Target data

Central management
Global view

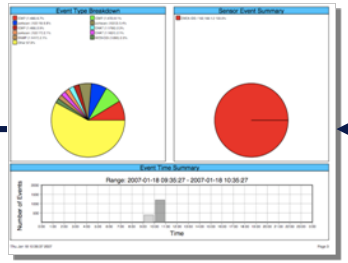
Open Rules
Reliable, auditable decisions



Event Reduction
Save time, reduce operational cost

Build compliance Policy
Discover problem systems in real-time

Automatic Response
Mitigate future risk



Report on Event
Proving compliance

Event Pivoting
Decreasing incident response effort

Target Analysis
Real-time change discovery

SOURCEfire
Security for the real world.

Demonstration: Sourcefire 3D System

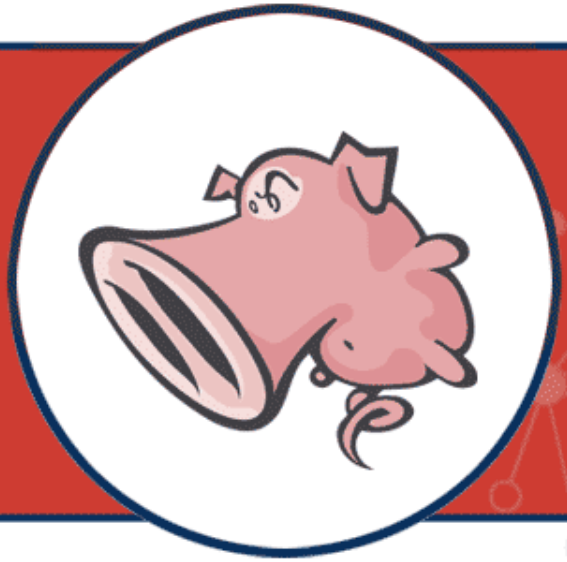
Sourcefire's live system of IPS, RNA and Defense Center

SOURCEfire
Security for the real world.

Summary

- Sourcefire Solutions provide *practical answers* to problems with current intrusion prevention
- End-point correlation *saves time* by reducing the number of alerts and reducing the time spent on dealing with them
- Sourcefire remediation enables you to *enforce* a wide range of security policies on your network
- Sourcefire solutions run on a wide range of hardware, offering the *right solution* to fit your size of business

SECURITY for the REAL WORLD.



Questions & Answers

SOURCEfire