

Adaptive IPS Security in a changing world

Dave Venman
Security Engineer, UK & Ireland



KNOW MORE NETWORK RISKS
NO MORE GUESSING



KNOW MORE NETWORK RISKS
NO MORE GUESSING



Who Is Sourcefire?

KNOW MORE NETWORK RISKS
NO MORE GUESSING



Mission: To help customers manage increasing risks and regulations by providing the most effective, efficient security possible—driven by network intelligence.

- ❏ Founded in 2001 by Snort Creator, Martin Roesch
- ❏ Headquarters: Columbia, MD
- ❏ Employees: More than 240
- ❏ More than 1,600 enterprise and government customers
- ❏ Over 30 of the Fortune 100 are customers.
- ❏ Global partner/distributor network
- ❏ NASDAQ: FIRE

Best of Both Worlds

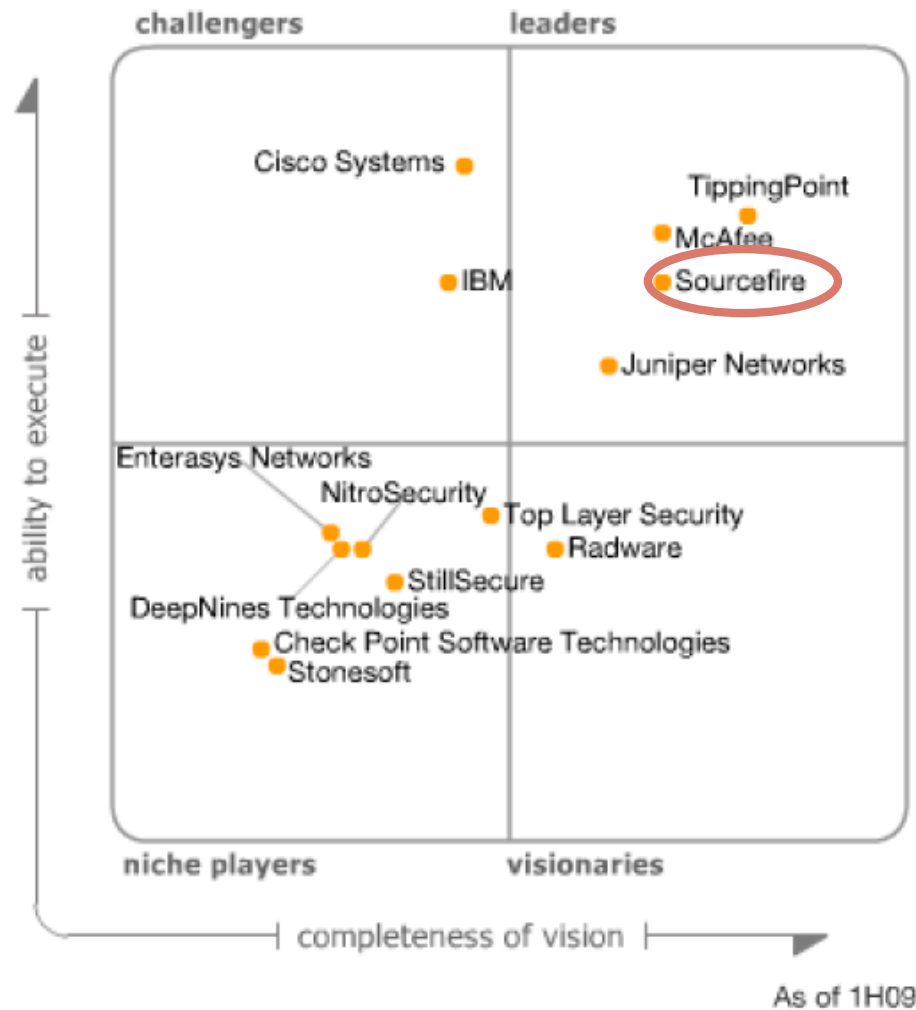
Open Source Community



Corporate
Support & Innovation

Acknowledged Leadership

KNOW MORE NETWORK RISKS
NO MORE GUESSING



FACT:

Sourcefire has been depicted by Gartner as the **most visionary** leader in Gartner's IPS Magic Quadrant since 2006!

Not Knowing can make headlines...

KNOW MORE NETWORK RISKS
NO MORE GUESSING



Rogue Trader Costs **Société Générale** \$7 billion



Civil Service Apologises for **HMRC** Data Loss



Hijacked **Bank of India** Website Downloads Malware

Chinese Hackers Breach India's **Ministry of External Affairs**



Indian hacker sell 8 Million private details of **Best Western** customers to Russian Mafia

DoS Attacks on **Estonia** Launched by Students



Korea's **Internet Auction** [eBay] Hacked; Millions Exposed

German Police Attempt to Hack **Skype**



Barts NHS Trust major incident with W/32Mytob virus

...and Be Costly

KNOW MORE NETWORK RISKS
NO MORE GUESSING



❏ Typical Costs Associated With Network Security Breaches:

- Lost revenue
- Lost productivity
- Regulatory fines
- Class-action lawsuits
- Damaged reputation
- Customer erosion



IPS is easy, right?



KNOW MORE NETWORK RISKS
NO MORE GUESSING



Not All Exploits Initially Pass Through an IPS

KNOW MORE NETWORK RISKS
NO MORE GUESSING



Defeating an IPS

KNOW MORE NETWORK RISKS
NO MORE GUESSING



- ❏ The best network security strategy is one with layered defenses
 - Deterministic – IPS, Firewall, Ant-Virus, Anti-Spam
 - Non-Deterministic – NBA



“A \$100,000 IPS can easily be defeated with a laptop and a pair of trainers.”

Martin Roesch
Sourcefire Founder & CTO

IPS History Lesson

KNOW MORE NETWORK RISKS
NO MORE GUESSING



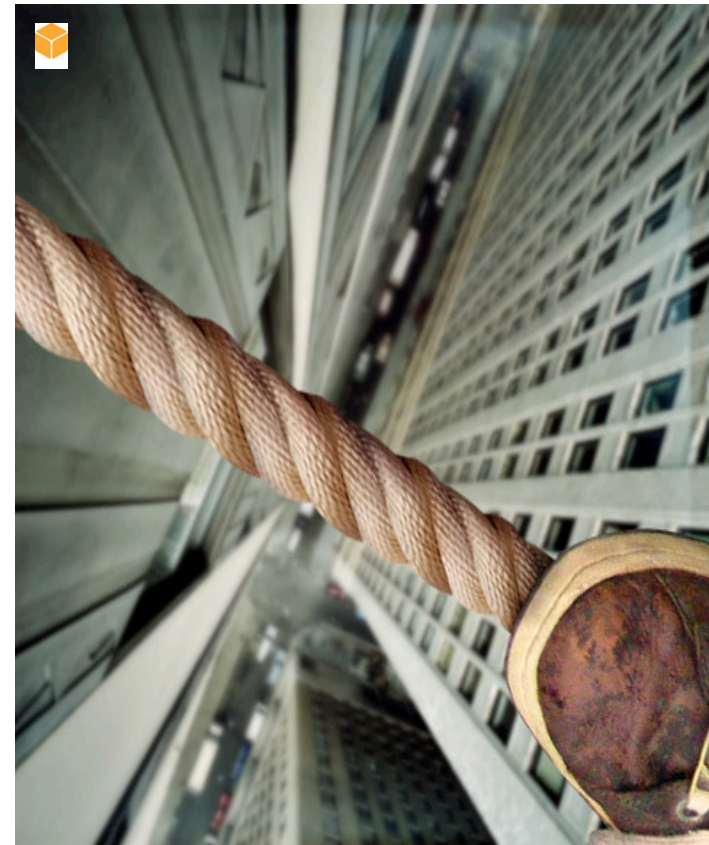
- ❏ Gartner IDS Magic Quadrant 2003 – *“IDS has failed on its promise, 99 out of 100 alerts are meaningless”*
- ❏ IDS vendors respond to Gartner with IPS
 - “We will protect you with our black box, trust us.....”
 - Plug & Play... no tuning?
 - Security or Connectivity?
 - How do I monitor?

Basic IPS – the Problem

KNOW MORE NETWORK RISKS
NO MORE GUESSING



- ❏ A typical default IPS policy has circa 300 – 1000 blocking rules (Fact)
- ❏ > 33,000 known vulnerabilities (Fact)
 - 6,751 added in 2007
 - 3,901 added in 2008
- ❏ Basic IPS 1- 3% protection
- ❏ 97-99% of other IPS events require human investigation
 - The IPS has no knowledge of the target
 - Therefore blind and virtually useless

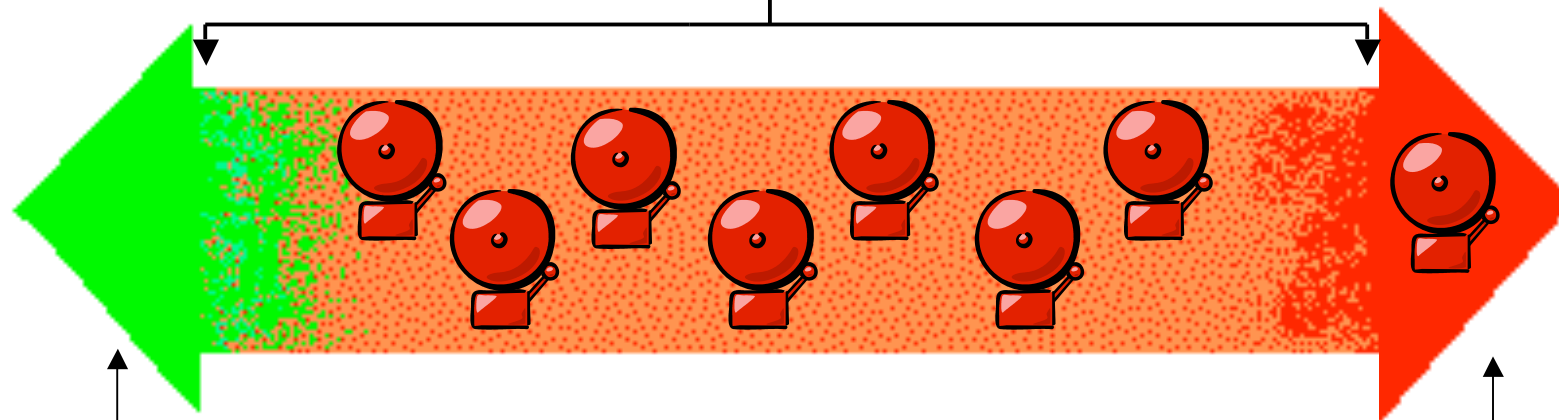


IPS Event Spectrum

KNOW MORE NETWORK RISKS
NO MORE GUESSING



IPS events that require
human investigation



Dismissible Events

Basic IPS
Easy to identify & block
1-3% of vulnerabilities

Security Events Must Have Context

KNOW MORE NETWORK RISKS
NO MORE GUESSING



**Does this traffic
threaten my business?**

SOURCEfire®

Intelligence Driven IPS



KNOW MORE NETWORK RISKS
NO MORE GUESSING



Sourcefire Threat, End Point & Network Intelligence

KNOW MORE NETWORK RISKS
NO MORE GUESSING



- | | |
|-----------------------------|---------------------|
| Sourcefire IPS | Threat |
| Sourcefire RNA™ | End Point / Network |
| Sourcefire RUA™ | End Point / User |
| Sourcefire NetFlow Analysis | Network |



Sourcefire Intelligence Drives...

KNOW MORE NETWORK RISKS
NO MORE GUESSING



- ❏ Network Discovery
- ❏ Impact Assessment
- ❏ Automated IPS Tuning
- ❏ IT Policy Compliance
- ❏ Network Behavior Analysis
- ❏ User Identity Tracking



**A whole lot more than a black box protecting
against the exploit of 1-3% of vulnerabilities**

Threat Intelligence – Sourcefire IPS

KNOW MORE NETWORK RISKS
NO MORE GUESSING



❏ **Snort® – de facto IPS standard**

- Most powerful and flexible rules engine
- Easy for the novice – deploy and listen
- Perfect for the expert – packet-level forensics

❏ **Centralized command and control**

- Reports, alerts and dashboards
- Third-party integration APIs
- Master Defense Center (MDC)

❏ **Backed by the Sourcefire VRT**

- Industry-leading vulnerability research team
- First among all IPS providers in responding to Microsoft Tuesday vulnerabilities

Defense Against:

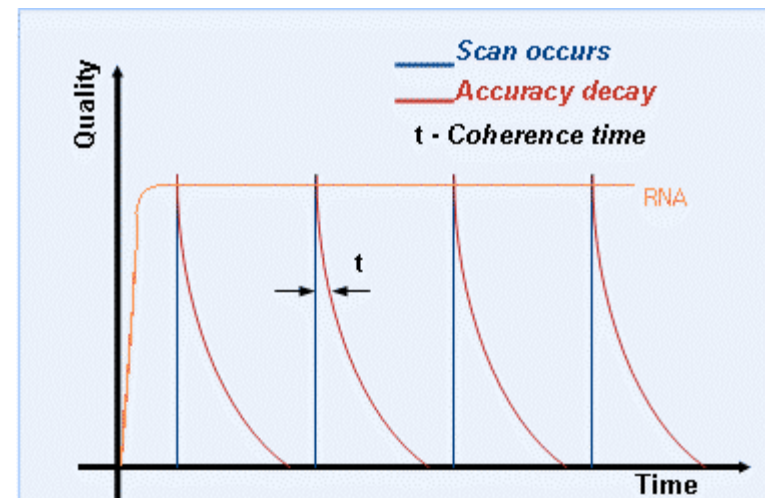
Worms
Trojans
Buffer overflows
DoS attacks
Backdoor attacks
Spyware
Port scans
VoIP attacks
IPv6 attacks
Statistical anomalies
Protocol anomalies
P2P attacks
Blended threats
Zero-day attacks
And more!

Network & End Point Intelligence

KNOW MORE NETWORK RISKS
NO MORE GUESSING



- Sourcefire RNA™ is watching “all the time, in real time”
 - 24x7 passive discovery
 - Surgical Active scans when required
- You 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 it's potential vulnerabilities are

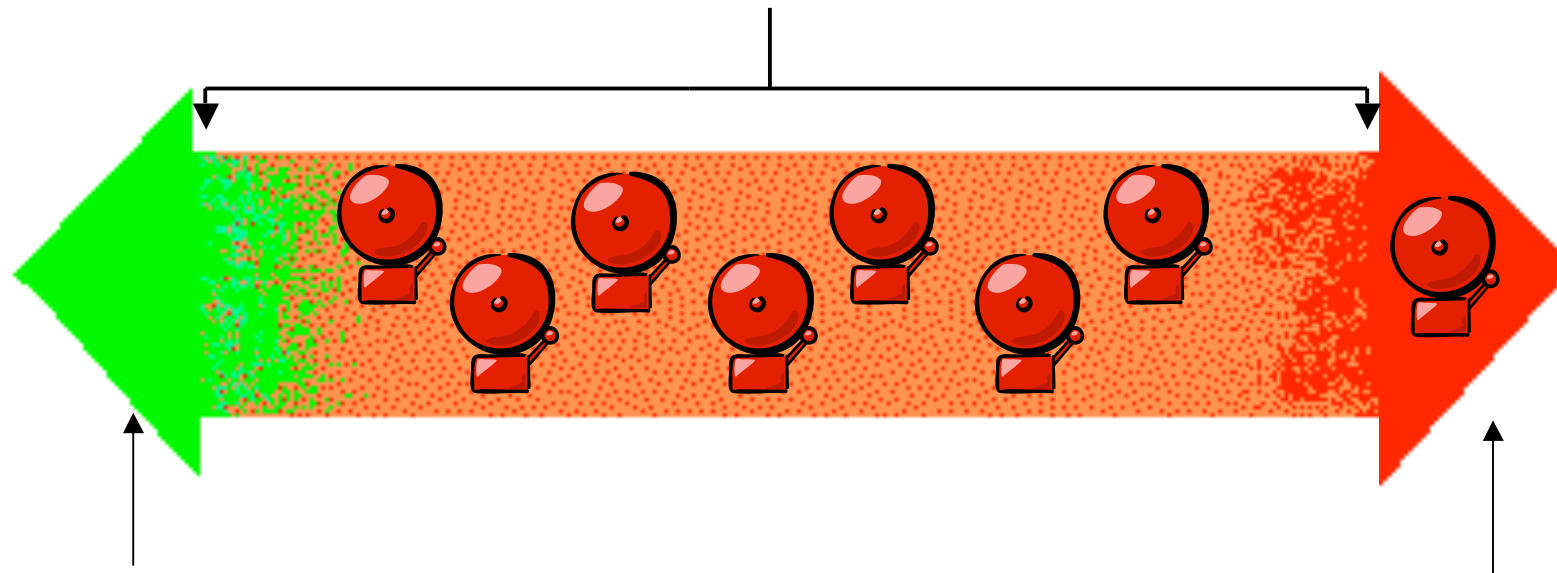


Sourcefire IPS event spectrum

KNOW MORE NETWORK RISKS
NO MORE GUESSING



Sourcefire automates this process, so your security staff can focus on the events that matter.



Sourcefire automatically eliminates false positives

Sourcefire default IPS policies balance security & connectivity.
Blocking

Typical Customer Feedback


KNOW MORE NETWORK RISKS
NO MORE GUESSING



**99.9% Event
Reduction!**


**“We were generating
20,000,000 IPS events
per month.”**

**“Events...have been
reduced...to approximately
2,000 per month.”**

 **THE INSTITUTE**
FOR APPLIED NETWORK SECURITY

Business/Technology Problem You are Facing

- In July of 2001 we found the Code Red worm. 2 months later, and many other worms, we had no choice to implement the commercial version of Sourcefire to help rid ourselves of these first two worm infections.
- After implementing the commercial Sourcefire solution, it became apparent to us. Who is looking at the massive events these things generate? We were generating 20,000,000 events per month.
- As time went on our Security Operations center (SOC) staff became overwhelmed by the events in the IDS. Even with a 24x7 staff monitoring the data we could not find all of the proverbial "needles in the hay stacks". We needed a way to prioritize the events coming in to the system, and it needed to be automated. This is where Marty Roesch's promise of RNA came into our decision to purchase the solution.

 **THE INSTITUTE**
FOR APPLIED NETWORK SECURITY

Results

- 6 months of testing, and 1 year to completely roll out to production.
- Since the RNA solution has been in place....
 - We have been able to reduce the time and number of staff who are dedicated to analyzing IDS data, re-utilizing these SOC resources for other activities.
 - We now can provide context to the systems involved in IDS events (OS, Services, Applications, etc).
 - Ability to identify exploits in real time now. We know the service/application involved matches up to the exploit in use.
- Manual reviews have been reduced from over 20,000,000 per month down to approximately 2,000 per month.

New England Information Security Forum

Automated IPS Tuning

KNOW MORE NETWORK RISKS
NO MORE GUESSING





- ❏ How often does your network change?
- ❏ How often do you tune your IPS?
- ❏ Key “Adaptive IPS” capabilities include:
 - RNA Recommended Rules
 - Adaptive Traffic Profiles
 - Non-Standard Port Handling



Adaptive IPS Capabilities Comparison

KNOW MORE NETWORK RISKS
NO MORE GUESSING



Capability						
Impact Analysis			Limited			
Automated IPS Tuning						
Adaptive Traffic Profiling						
Non-Standard Port Handling				Limited		

User Identity Tracking

KNOW MORE NETWORK RISKS
NO MORE GUESSING



- ❏ Pairs an Active Directory or LDAP username with a host IP address
- ❏ Correlates usernames with security events so incidents can be resolved more quickly
- ❏ Click on username to reveal full name, telephone, email, and department
- ❏ Integrated into all Sourcefire 3D Sensors



"Mapping a username to an IP address was taking us away from a backlog of other important tasks. What used to take up to an hour now takes just a second or two."



Tamara Fisher,
AutoTrader.com

Benefits of Sourcefire Intelligence Driven IPS

KNOW MORE NETWORK RISKS
NO MORE GUESSING



❏ Reduces Risk

- You know what you're protecting
- You know when your network changes
- You can detect exploits originating from inside and outside your network
- Your network is a safer place by monitoring and enforcing IT compliance policies

❏ Saves Time & Money

- Your IPS is always “tuned”—even when your network changes
- You no longer have to sift through thousands of events to uncover what really matters
- You know who to call when a host is compromised

Sourcefire 3D System Components

KNOW MORE NETWORK RISKS
NO MORE GUESSING



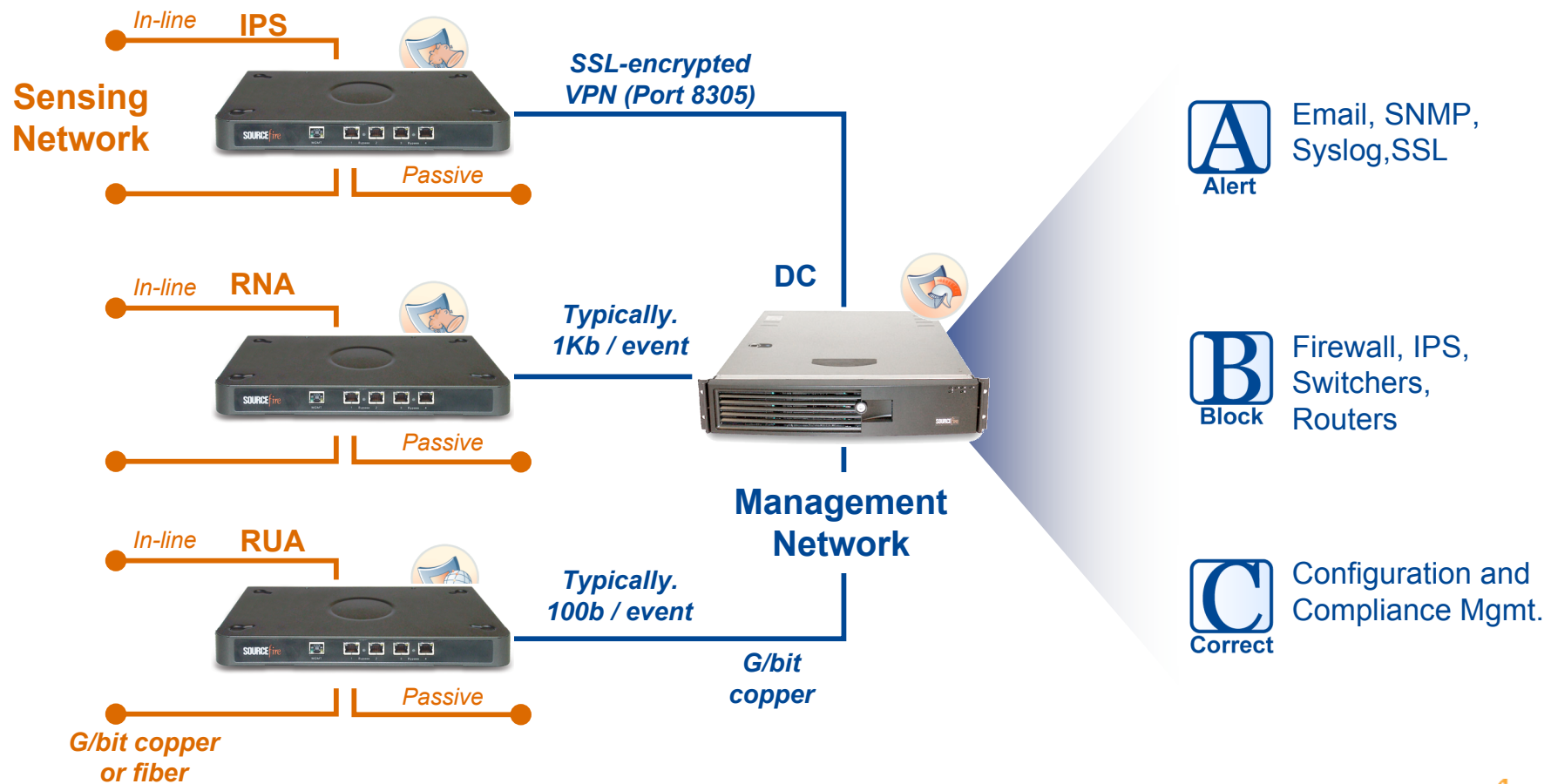
Discover



Determine



Defend



And Best Of All,
It Keeps You Out of the Headlines!

KNOW MORE NETWORK RISKS
NO MORE GUESSING



Questions?