Next-Generation IPS: Automated Security Through Awareness

Brian Tan
Technical Consultant – ASEAN & North Asia
btan@sourcefire.com

About Sourcefire

Mission: To be the leading provider of intelligent cybersecurity solutions for the enterprise.

- Founded in 2001 by Snort Creator, Martin Roesch, CTO
- Headquarters: Columbia, MD
- Leader in Gartner IPS Magic Quadrant
- Winner of 2011 SC Magazine Award for Best IDS/IPS
- NASDAQ: FIRE

Today's Threat Landscape

Defending the Dynamic Network

- Dynamic threats
  - Many threats are "unknown"
  - Well-financed attackers
  - New threats emerge daily

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

- Dynamic networks
  - New and changing devices, operating systems, services, protocols, and ports
  - New vulnerabilities
  - New and changing users
- Static defenses simply aren't good enough
  - To be truly effective, the IPS must "adapt" to dynamically changing threats and networks

So how can I keep my business secure?

Don't just throw products at the problem…


9 months

+


9 months

≠


4.5 months


Security Product

+


Security Product

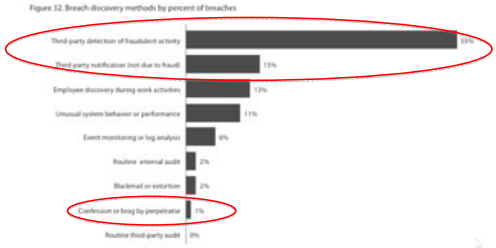
≠ **Twice As Secure**

… because your people won't cope

- Information Overload
- People are vigilant
- People are responsive

We can all be caught asleep at the wheel

Verizon Business 2009 Data Breach Study



Understand what you are trying to protect…

"My concern right now isn't what I'm being attacked with, its finding what I need to defend"

Sourcefire customer

In security, context is everything

Network and user context

Event:	Attempted Privilege Gain
Severity:	Medium
Target:	96.16.242.135 (vulnerable)
Host OS:	Windows
Applications:	Mail, Browser, Twitter
Location:	Corp. HQ
User ID:	jsmith
Full Name:	John Smith
Department:	Executive Team

Network context

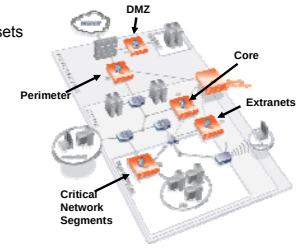
Event:	Attempted Privilege Gain
Severity:	Medium
Target:	96.16.242.135 (vulnerable)
Host OS:	Windows
Applications:	Mail, Browser, Twitter
Location:	Corp. HQ

No context

Event:	Attempted Privilege Gain
Severity:	Medium
Target:	96.16.242.135

Protect your network

- **Awareness**
  - Monitor for intruders
  - Identify your network assets
  - Monitor your network behaviour
- **Enforcement**
  - Block where possible
  - Enforce network configuration
- **Automate everything**
  - Minimise your TCO
  - Only possible with good data



Next-Generation IPS Approach

They said it …

"Begin the transformation to context-aware and adaptive security infrastructure now as you replace legacy static security infrastructure."

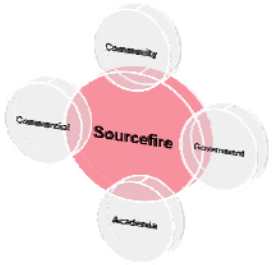
Gartner

Neil MacDonald
VP & Gartner Fellow

Source: Gartner, Inc., "The Future of Information Security is Context Aware and Adaptive," May 14, 2010

Introducing Next-Generation IPS (NGIPS)

Next-Gen IPS – Open Architecture



- Powerful Engine & Rules
  - Adaptable
  - Custom fit to network
  - Comprehensive coverage
- Open Community
  - Information sharing
  - Shared protection

Awareness is the foundation behind ...

- Intrusion event prioritization
- Automated IPS tuning
- IT policy compliance
- Network behaviour analysis (NBA)
- User Intelligence
- .. in other words Adaptive IPS

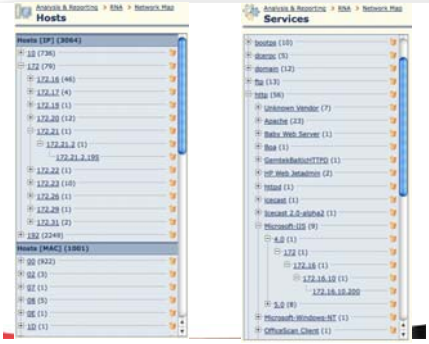
Network
Know what's there, what's vulnerable, and what's under attack

Application
Identify change and enforce policy on hundreds of applications

Identity
Know who is doing what, with what, and where

Behavior
Detect anomalies in configuration, connections and data flow

Host & Services Map



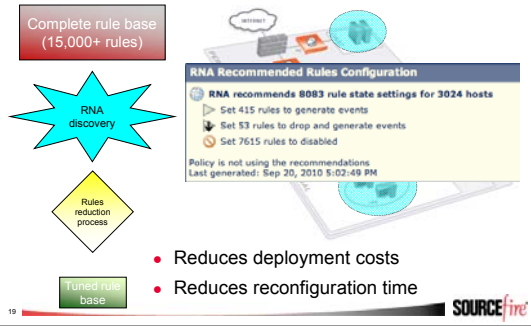
Host Profile

... Intrusion event prioritisation

Typically, 95% reduction of events seen

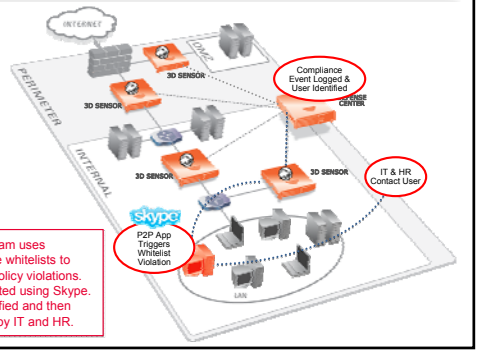
- Intrusion event
- **Vulnerable** (exploit targets known vulnerability)
- **Possibly vulnerable** (exploit targets OS and/or service)
- **Not vulnerable** (no service present)
- **Not present** (no host present)

... Automated IPS tuning



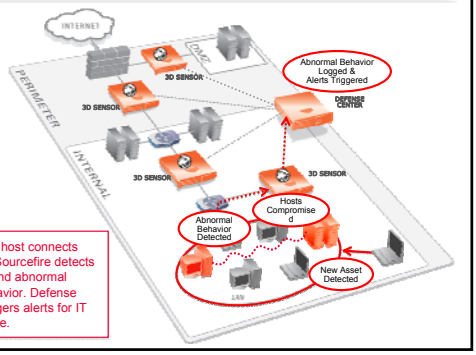
- Reduces deployment costs
- Reduces reconfiguration time

... IT policy compliance



Security team uses compliance whitelists to detect IT policy violations. Host detected using Skype. User identified and then contacted by IT and HR.

… Network behaviour analysis

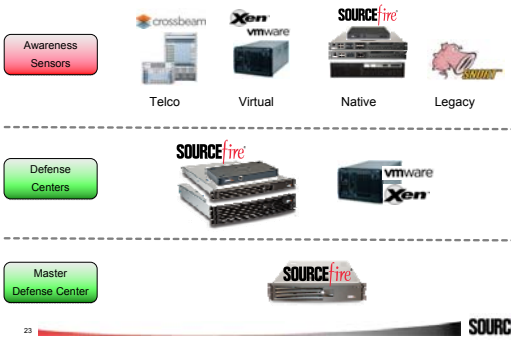


New rogue host connects internally. Sourcefire detects new host and abnormal server behavior. Defense Center triggers alerts for IT to remediate.

… User Intelligence

"People are the perpetrators (or victims) of computer crime, not computers"

Sourcefire Next-Gen IPS Platforms



Next-Gen IPS Benefits

- Increased accuracy
- Reduced tuning overhead
- Tracks network change
- Better forensic capability
- Enforce compliance

- ***Lowest cost of ownership***

Thank You