RSA CONFERENCE ASIA PACIFIC 2013

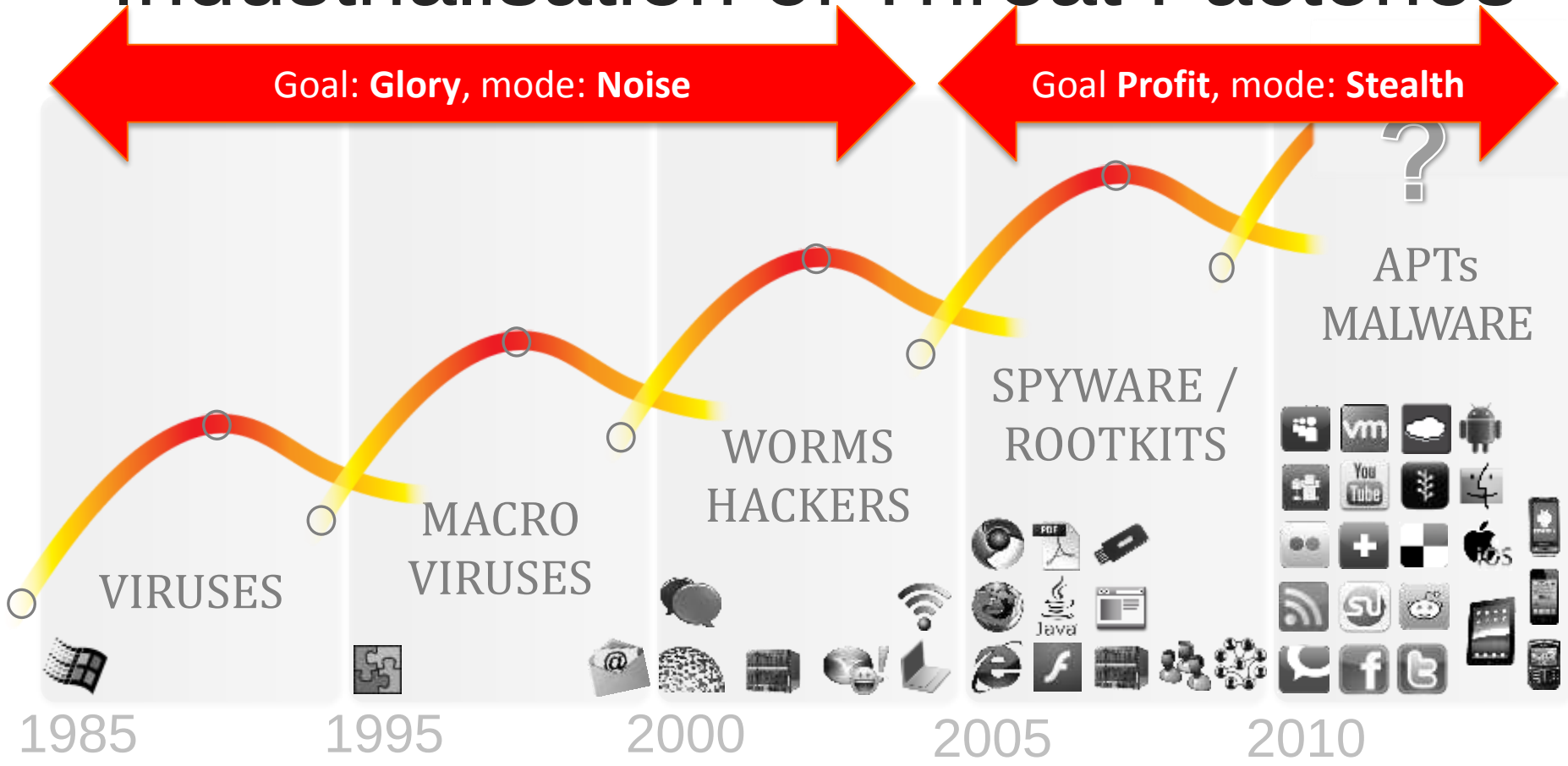
EXTENDING NETWORK SECURITY: TAKING A THREAT CENTRIC APPROACH TO SECURITY

Dean Frye
Sourcefire

Session ID: SEC-W05

Session Classification: Intermediate

Industrialisation of Threat Factories



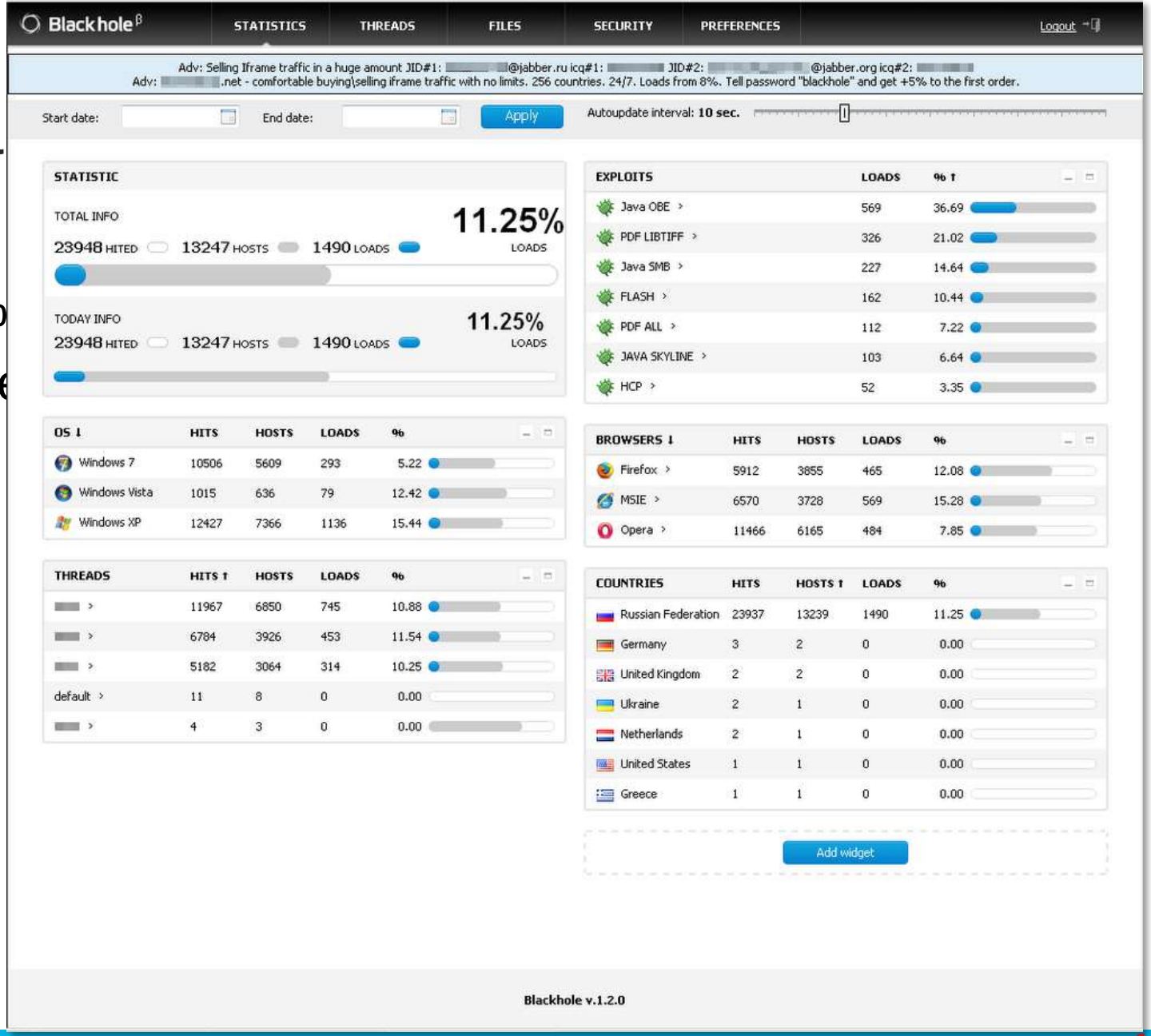
Attackers and defenders drive each other to innovate…
…resulting in distinct threat cycles

"Once a deviant industry is professionalized, crackdowns merely promote innovation."

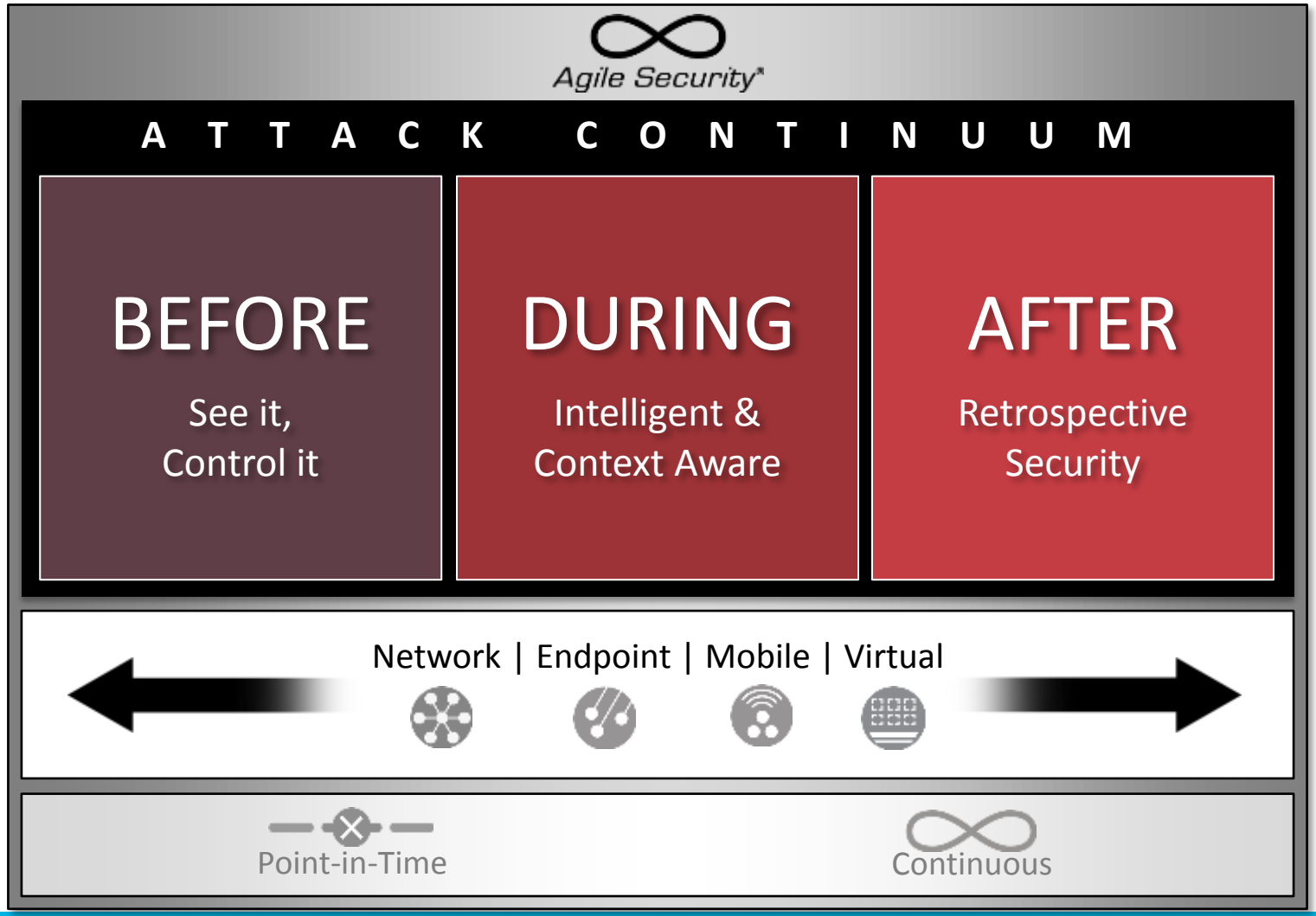
Nils Gilman, 4th European Futurists Conference

Bla

- 28%
- Rece


Blackhole β
STATISTICS
THREADS
FILES
SECURITY
PREFERENCES
Logout
Adv: Selling Iframe traffic in a huge amount JID#1: [redacted]@jabber.ru icq#1: [redacted] JID#2: [redacted]@jabber.org icq#2: [redacted]
Adv: [redacted].net - comfortable buying\selling iframe traffic with no limits. 256 countries. 24/7. Loads from 8%. Tell password "blackhole" and get +5% to the first order.
Start date:
End date:
Apply
Autoupdate interval: 10 sec.
STATISTIC
TOTAL INFO
11.25%
LOADS
23948 HITED
13247 HOSTS
1490 LOADS
TODAY INFO
11.25%
LOADS
23948 HITED
13247 HOSTS
1490 LOADS
EXPLOITS
LOADS
% ↑
Java OBE 569 36.69
PDF LIBTIFF 326 21.02
Java SMB 227 14.64
FLASH 162 10.44
PDF ALL 112 7.22
JAVA SKYLINE 103 6.64
HCP 52 3.35
OS ↓
HITS
HOSTS
LOADS
%
Windows 7 10506 5609 293 5.22
Windows Vista 1015 636 79 12.42
Windows XP 12427 7366 1136 15.44
BROWSERS ↓
HITS
HOSTS
LOADS
%
Firefox 5912 3855 465 12.08
MSIE 6570 3728 569 15.28
Opera 11466 6165 484 7.85
THREADS
HITS ↑
HOSTS
LOADS
%
[redacted] 11967 6850 745 10.88
[redacted] 6784 3926 453 11.54
[redacted] 5182 3064 314 10.25
default 11 8 0 0.00
[redacted] 4 3 0 0.00
COUNTRIES
HITS
HOSTS ↑
LOADS
%
Russian Federation 23937 13239 1490 11.25
Germany 3 2 0 0.00
United Kingdom 2 2 0 0.00
Ukraine 2 1 0 0.00
Netherlands 2 1 0 0.00
United States 1 1 0 0.00
Greece 1 1 0 0.00
Add widget
Blackhole v.1.2.0

New Model of Security



There is no Silver Bullet

- You need to address the full Attack Continuum

Before	**During**	**After**
Policy & Control	***Identification & Block***	***Analysis & Remediation***
Discover environment	Detect	Determine scope of damage
Implement policy and control	Prevent	Contain the spread of attacks
Harden assets		Remediate

What is needed is a new Technique to protect your organization

Before the Threat:

- Discover Your Environment

Before
Policy & Control


Threats

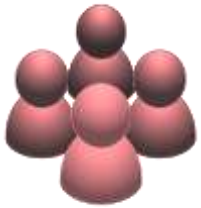

Devices

Applications


Flow


Vulnerabilities

OS


Users


Files

Before the Threat:

- Implement Policy & Control

Before
Policy & Control

Policy Enforcement:

Application Control:

Automated Tuning:

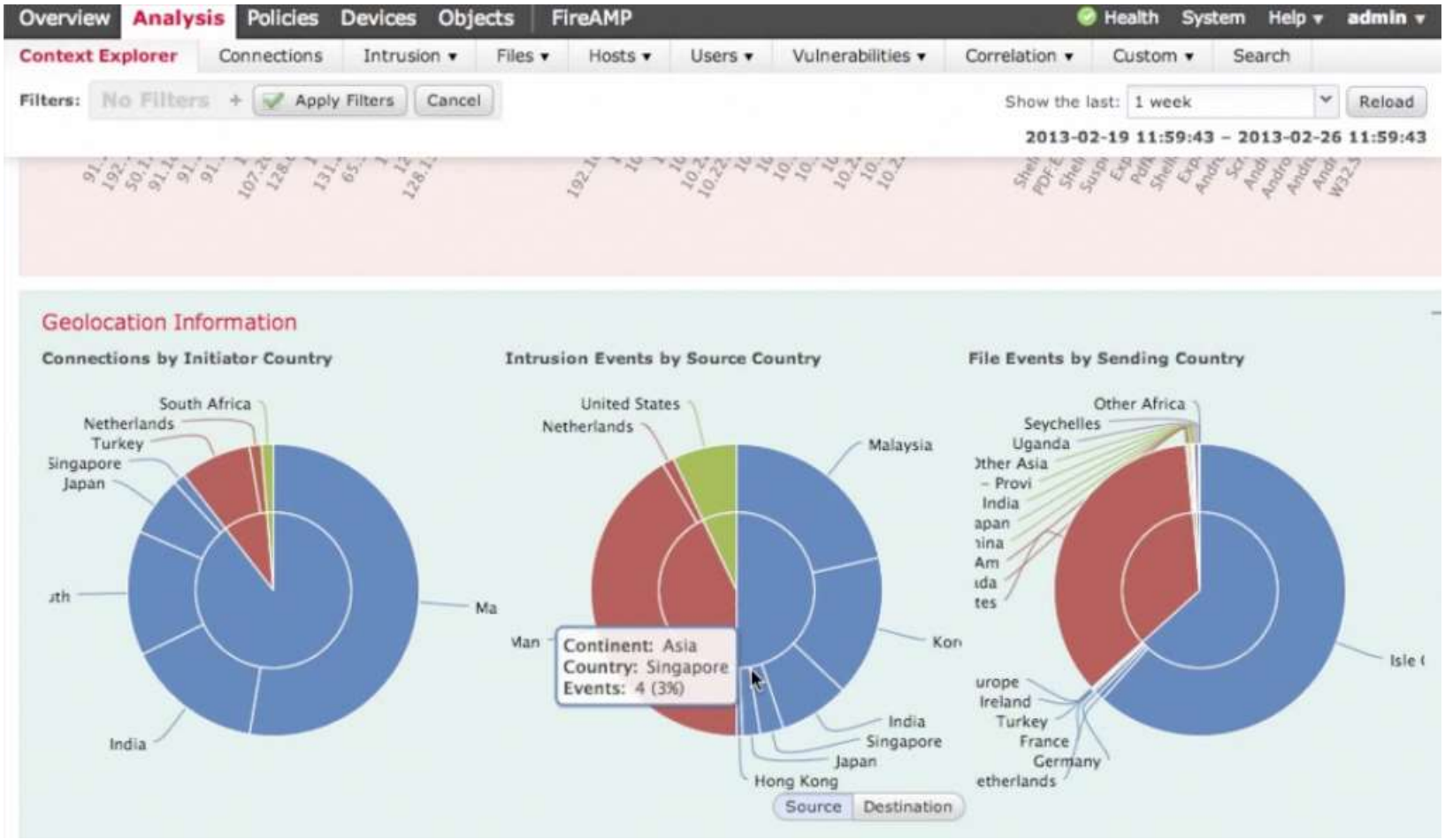
URL Filtering:

During the Threat:

- Security Intelligence – Contextual Decisions

During

Identification & Block



During

Identification & Block

- World Class Research
- Global Data Collection
- Openly Published

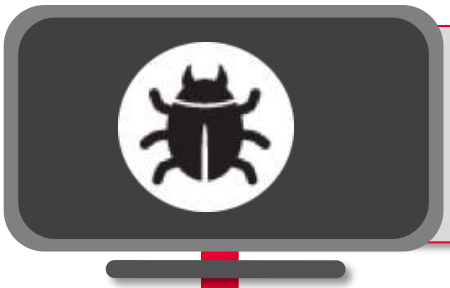
Content

- A focused list of the vulnerabilities you're most likely to be affected by *this week*
- Top in field malware detections last week
- Notable new attack methods, and how attacks work

http://vrt-blog.snort.org

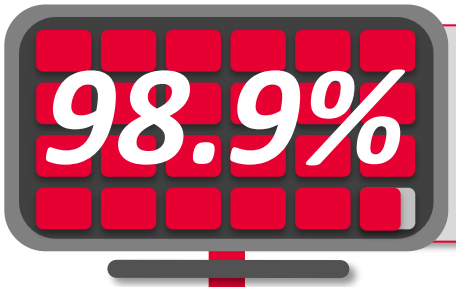
Intelligence by the numbers

During
Identification & Block

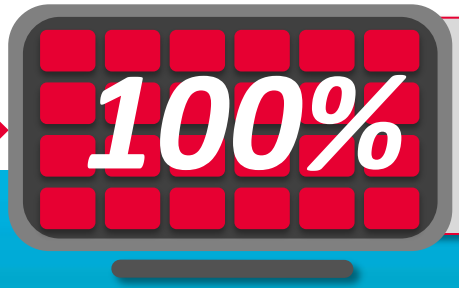


14,443,920 *pieces of malware submitted for analysis*

>2,250,000 *end points feeding real-time threat intelligence to FireCLOUD*



Industry's ***best*** *vulnerability coverage achieved in NSS Labs IPS group test*



Same-day *protection for Microsoft vulnerabilities for all customers*

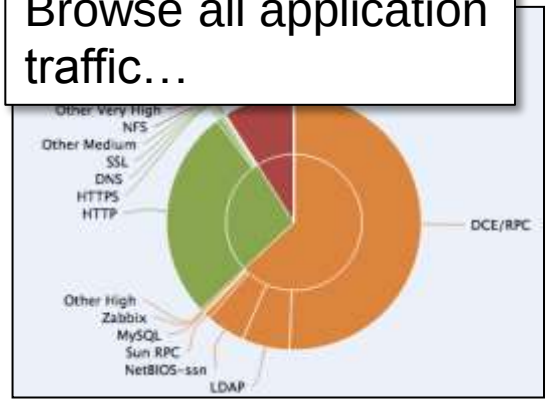
After the Threat:

- Leverage Context

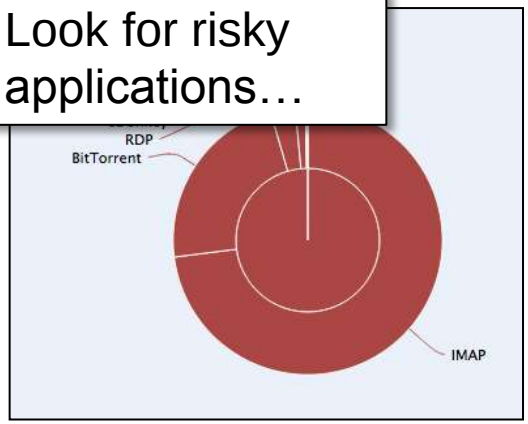
After

Analysis & Remediation

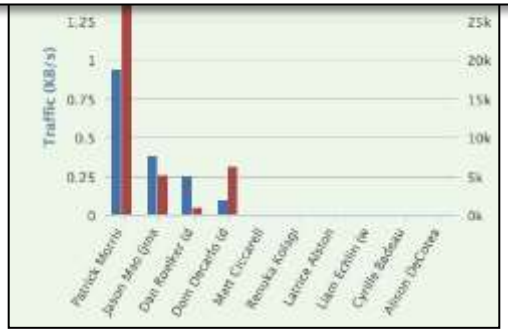
Browse all application traffic…



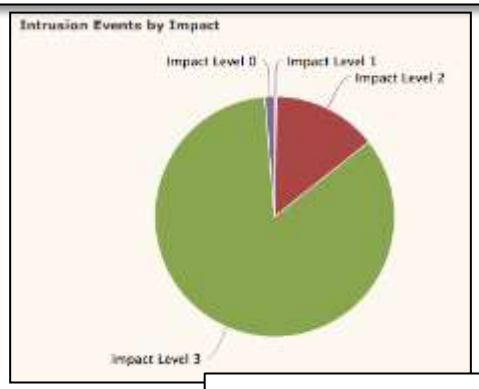
Look for risky applications…



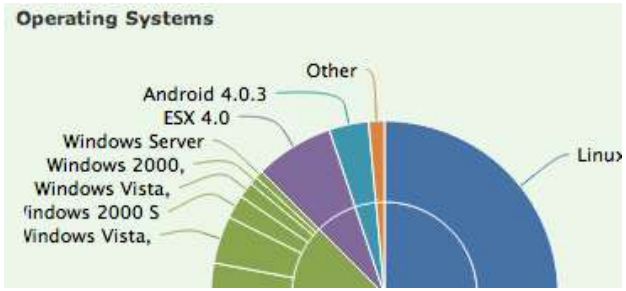
Who is using them?



What else have these users been up to?



On what operating systems?



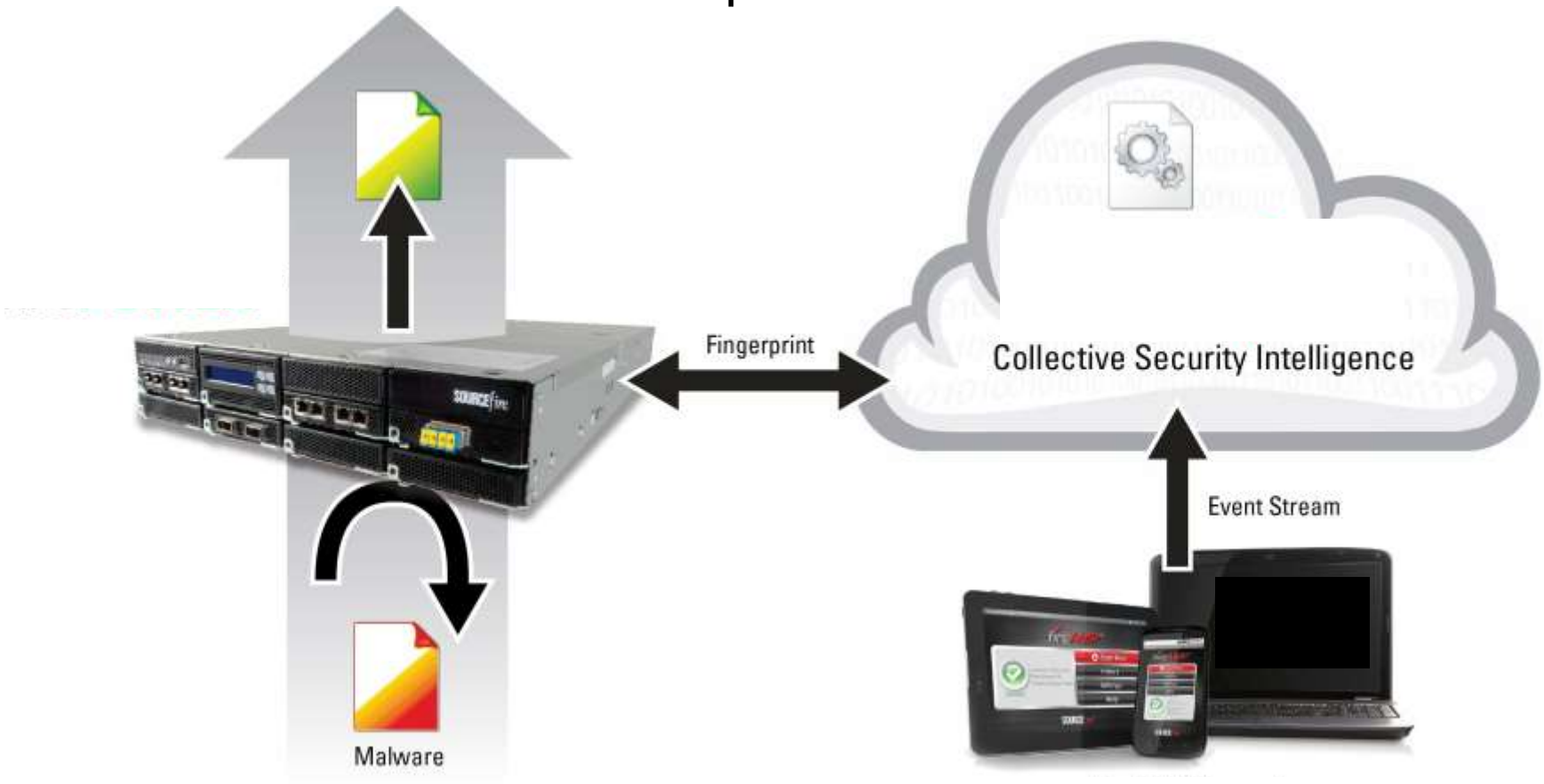
What does their traffic look like over time?

After the Threat:

- Continuous Analysis & Remediation
- Network Detection – Endpoint Remediation

After

Analysis & Remediation



After the Threat:

- Device Trajectory

Outgoing connection from Google Chrome 24.0.1312.52 (62ca2bc..59a3cb), most common filename chrome.exe, at TCP port 1156 to http://**10.180.0.144**:8888/exploit.html (10.180.0.144 port 8888).

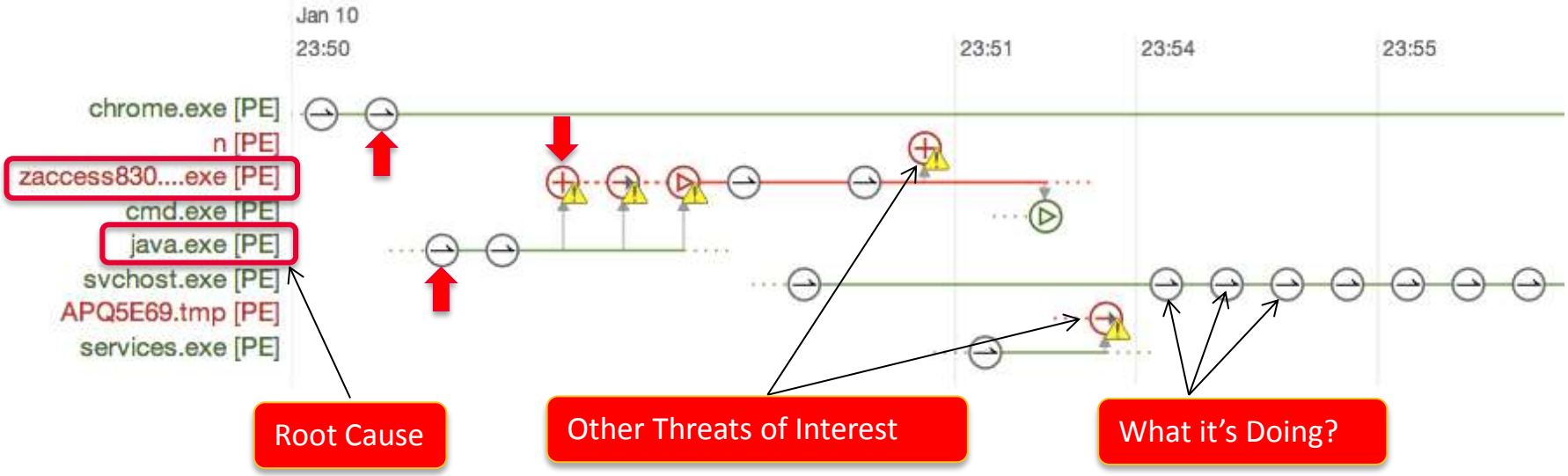
Neutral disposition.

At 23:50:44, Thu Jan 10 2013 UTC

After

Analysis & Remediation

Device Trajectory for **Java-0-Day**

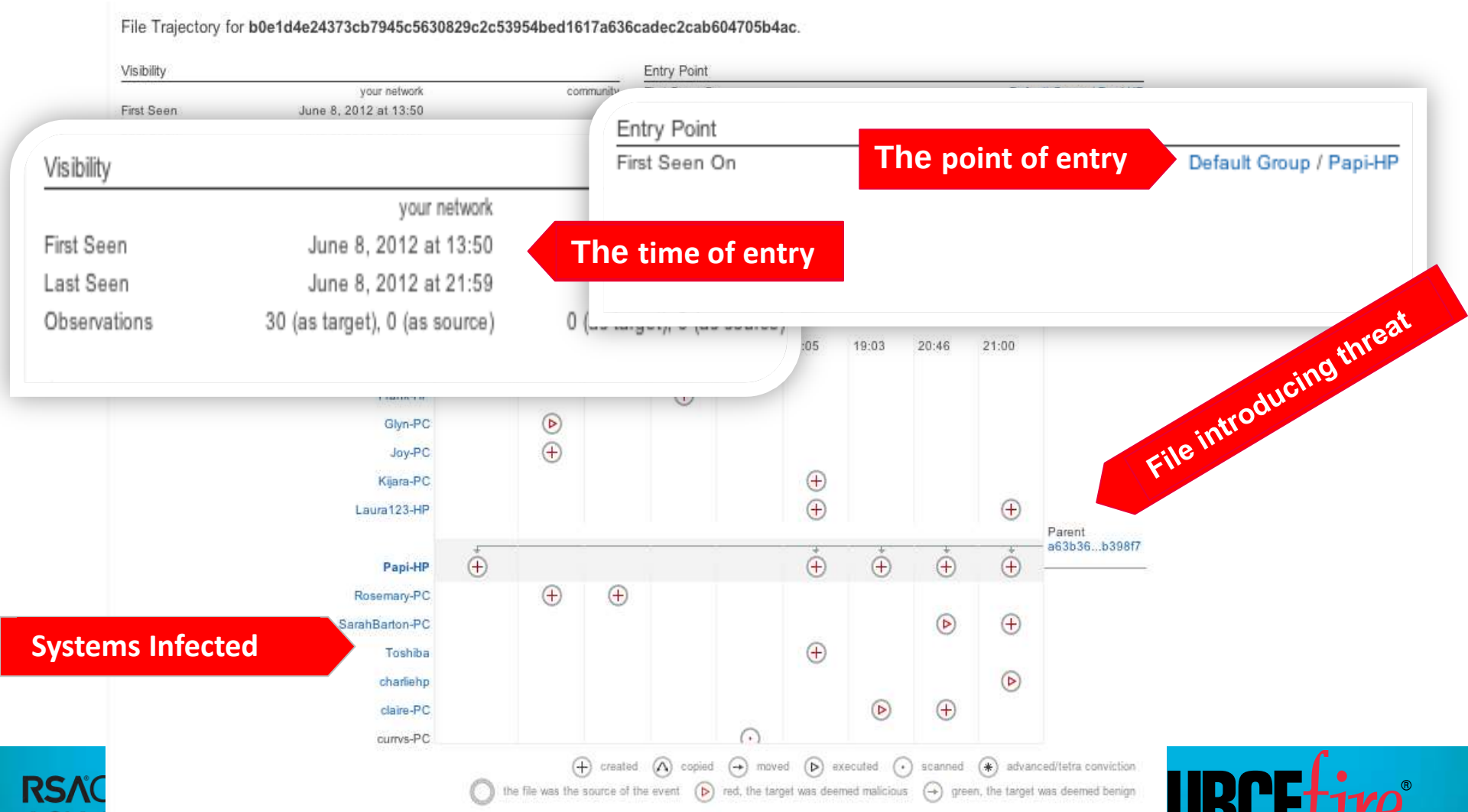


After the Threat:

- File Trajectory

After

Analysis & Remediation

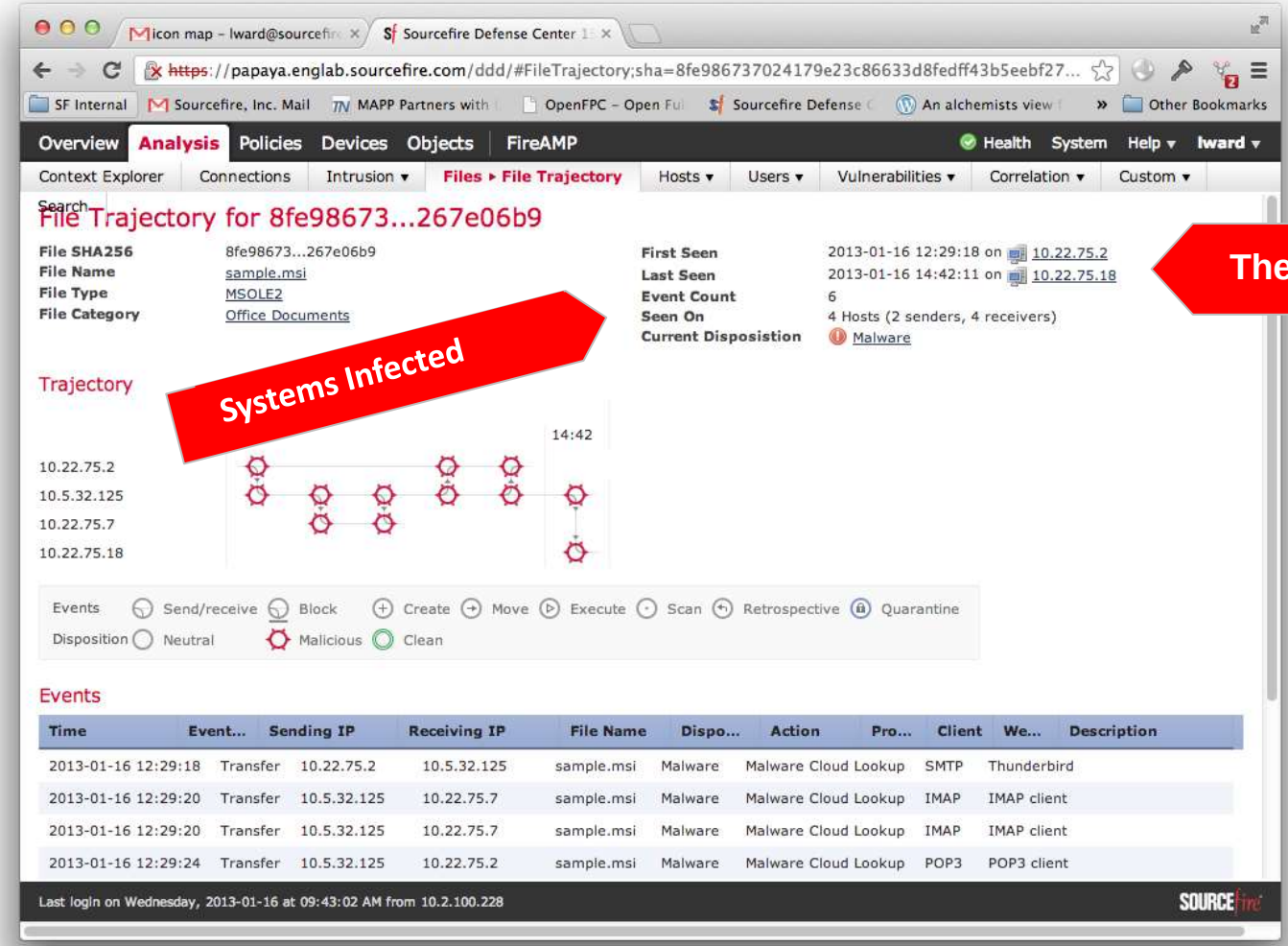


After the Threat:

- Network File Trajectory

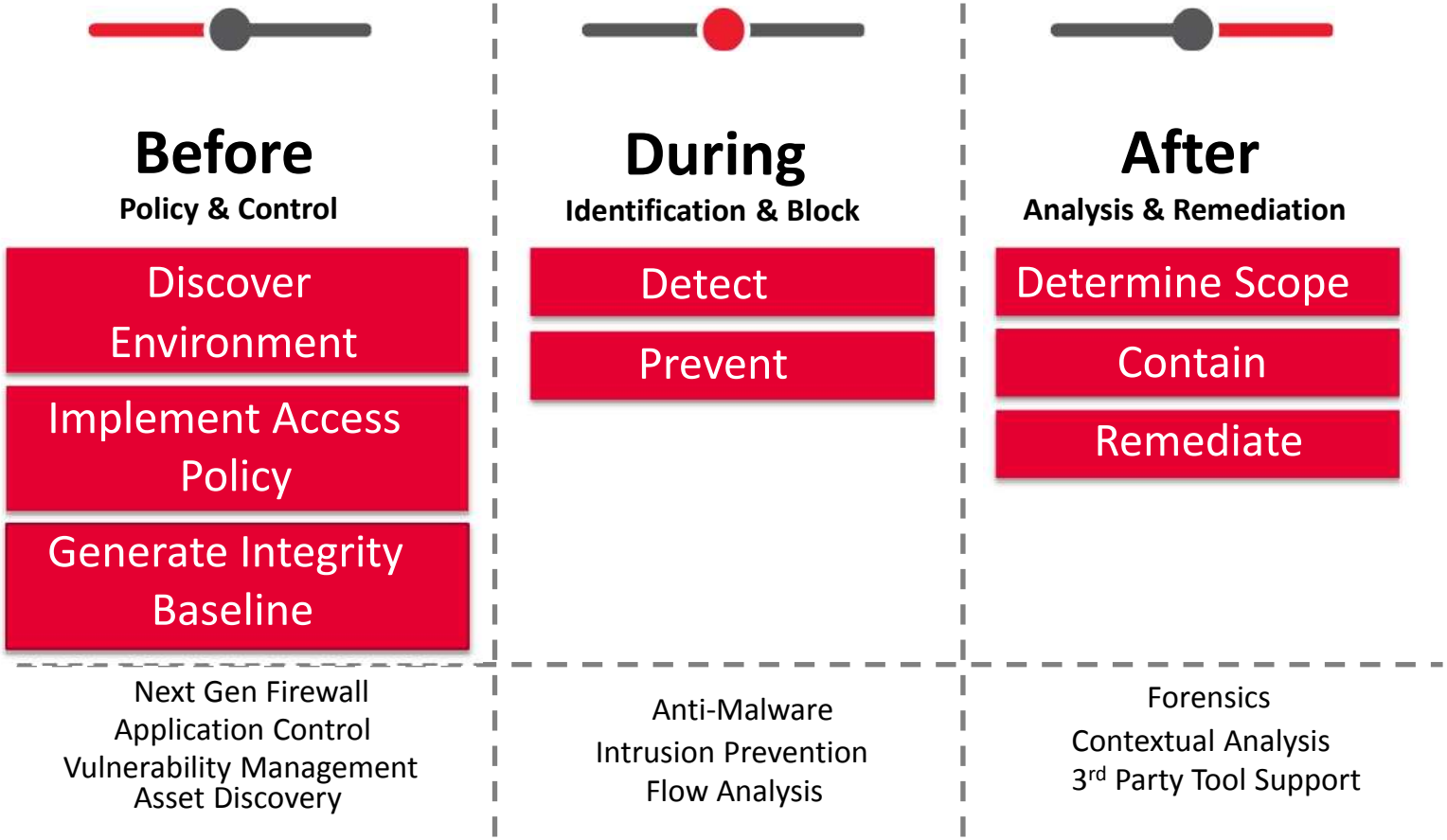
After

Analysis & Remediation



The time of entry

Address the Entire Attack Continuum



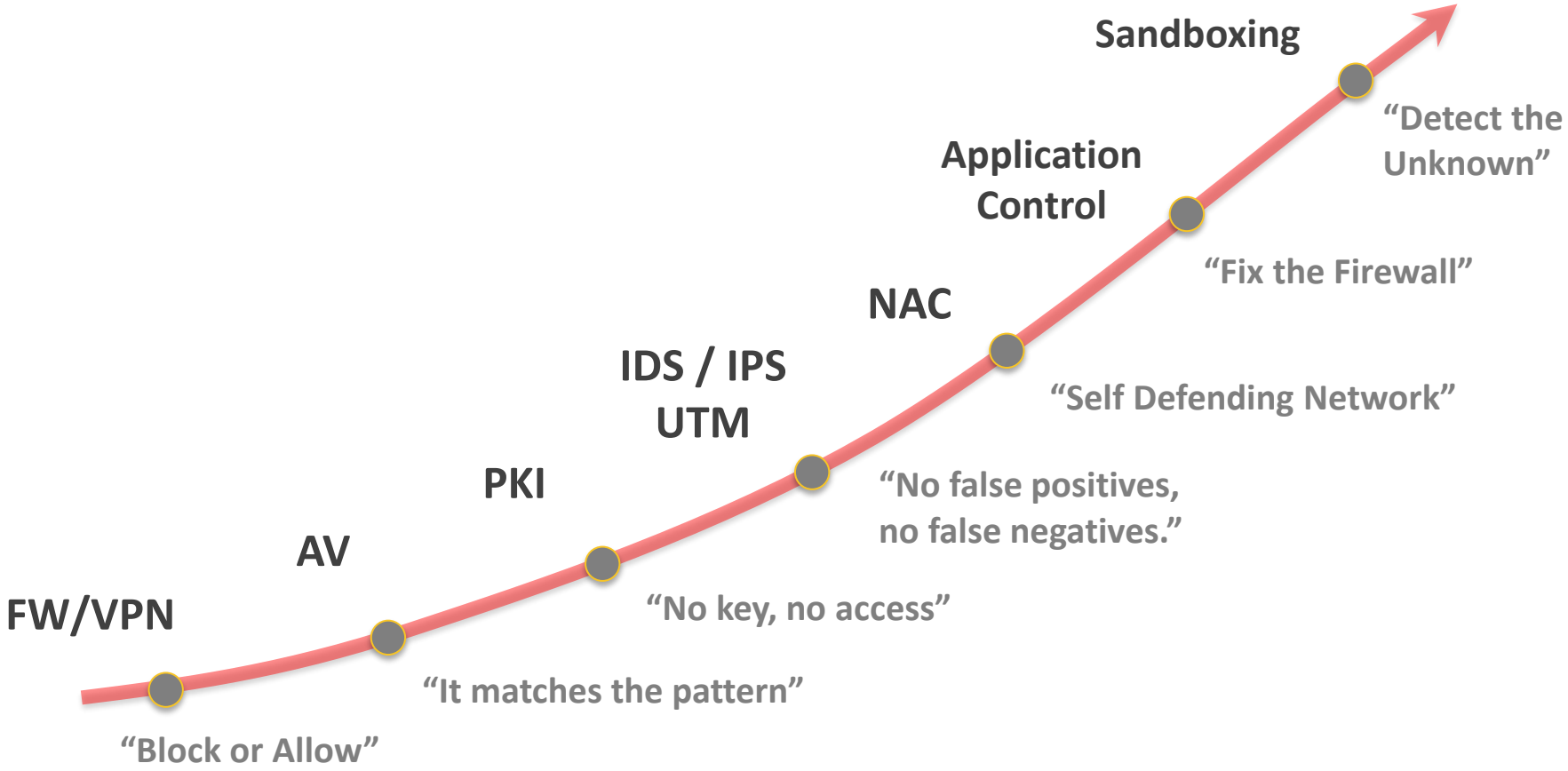
Addressing Threat Evolution

- Vendors intrusions, malware …s … what are all th eats
- Threat C e ?
- Obsessi n Bigger, Single B
- Assump e Unrealis

Detection Race

- Defining a Failed Technology Frames New Technology as Advancement
- Vendor Should Focus on What is Not Working Not On Infosec Arms Race
  - Amazing How Quickly Countermeasures Are Redundant
- Failed Detections Are Expensive!
  - Skills and Costs Massively Higher
- The Detection Race Hurts the Technology Buyer

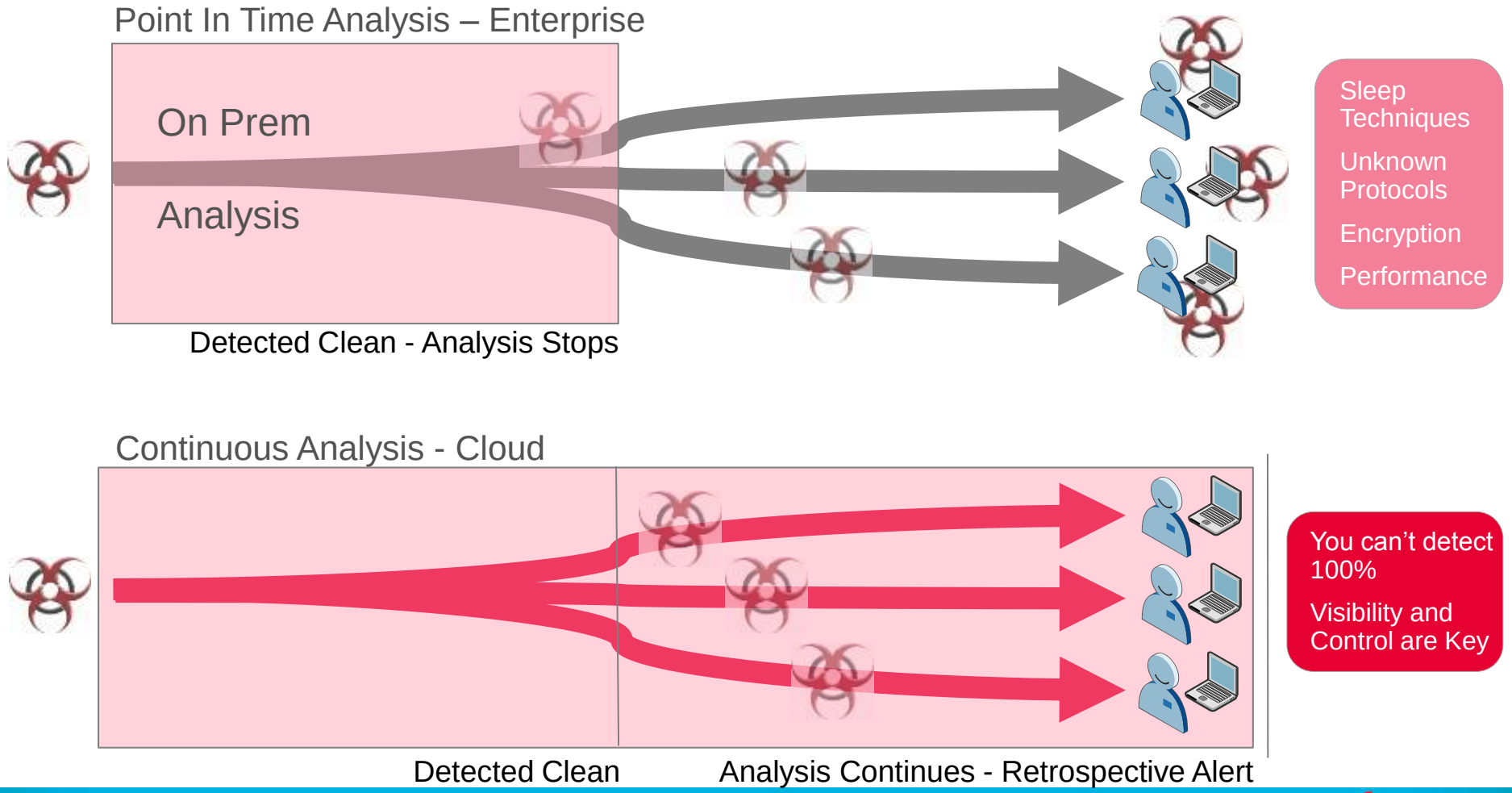
Guns Need Bullets



Technique Vs Technology

- Technology Lifecycles are Short
- Modular Frameworks With Multiple Technologies
  - Give Longer Technology Cycles
  - Allow Technologies to Co-Exist
- Let's Look At 2 Emergent Technologies

Technology Example: Sandboxing



Technology Example: IOCs

- Generic Indicators of Compromise – Attack Pathology
- May be Behavioural, Intrinsic Characteristic, Almost Anything
  - Process Name, Communication Metadata, Registry Key, Encoding
- Can Be Shared
- Weak Signal In Isolation - Can Be Weighted
- Particularly Promising As An Analysis and Recognition Technology Post Compromise

Cloud Enables Technique

- Both These Technologies Are Promising
- Centralised Support and Huge Processing Capability Co-Ordinates Many New Technologies
- … and Reinvigorates the Old

Detection Lattice

- Co-Ordinated Detection Technologies

One-to-One

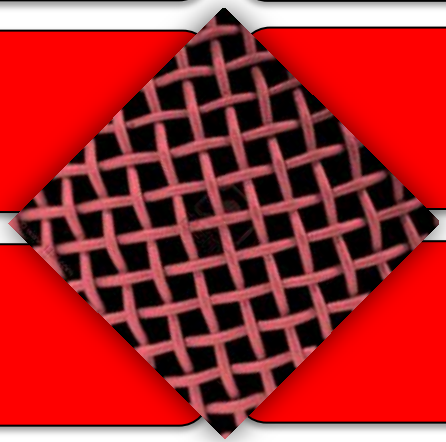
Signature-based, 1st line of defense, Coarse ACL

Fuzzy Fingerprinting

Algorithms identify polymorphic malware

Sandbox

Code Behavioural Analysis



IOC

Indicators of Compromise – Weighted Decisions

Machine Learning

Analyzes 400+ attributes for unknown malware

Advanced Analytics

Combines data from lattice with global trends

IP And File Reputation

Massive Repository of File and IP Disposition

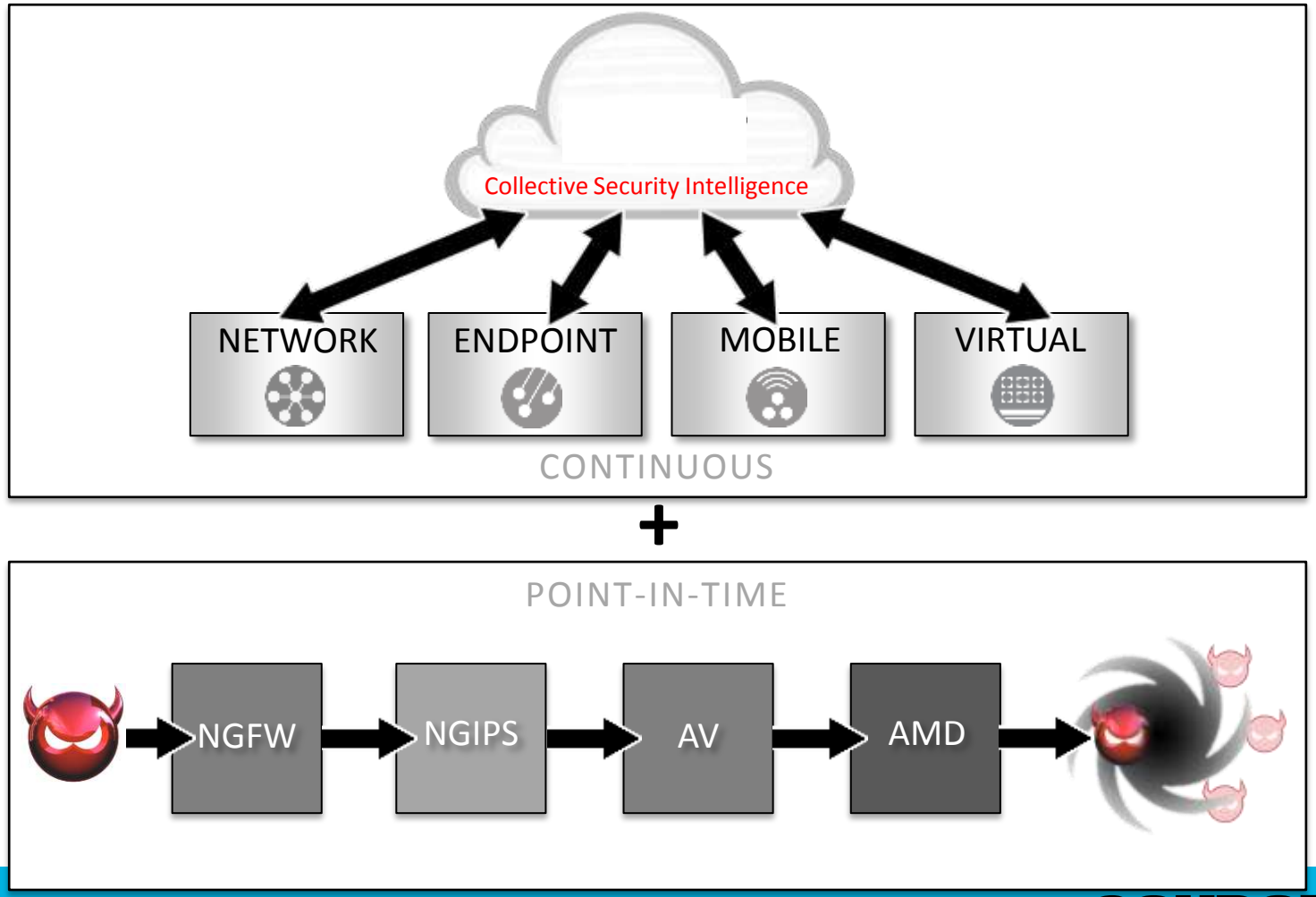
Cloud Recall Engine

Retrospective Analysis

Cloud-based delivery, results in better protection plus lower storage & compute burden within the Enterprise

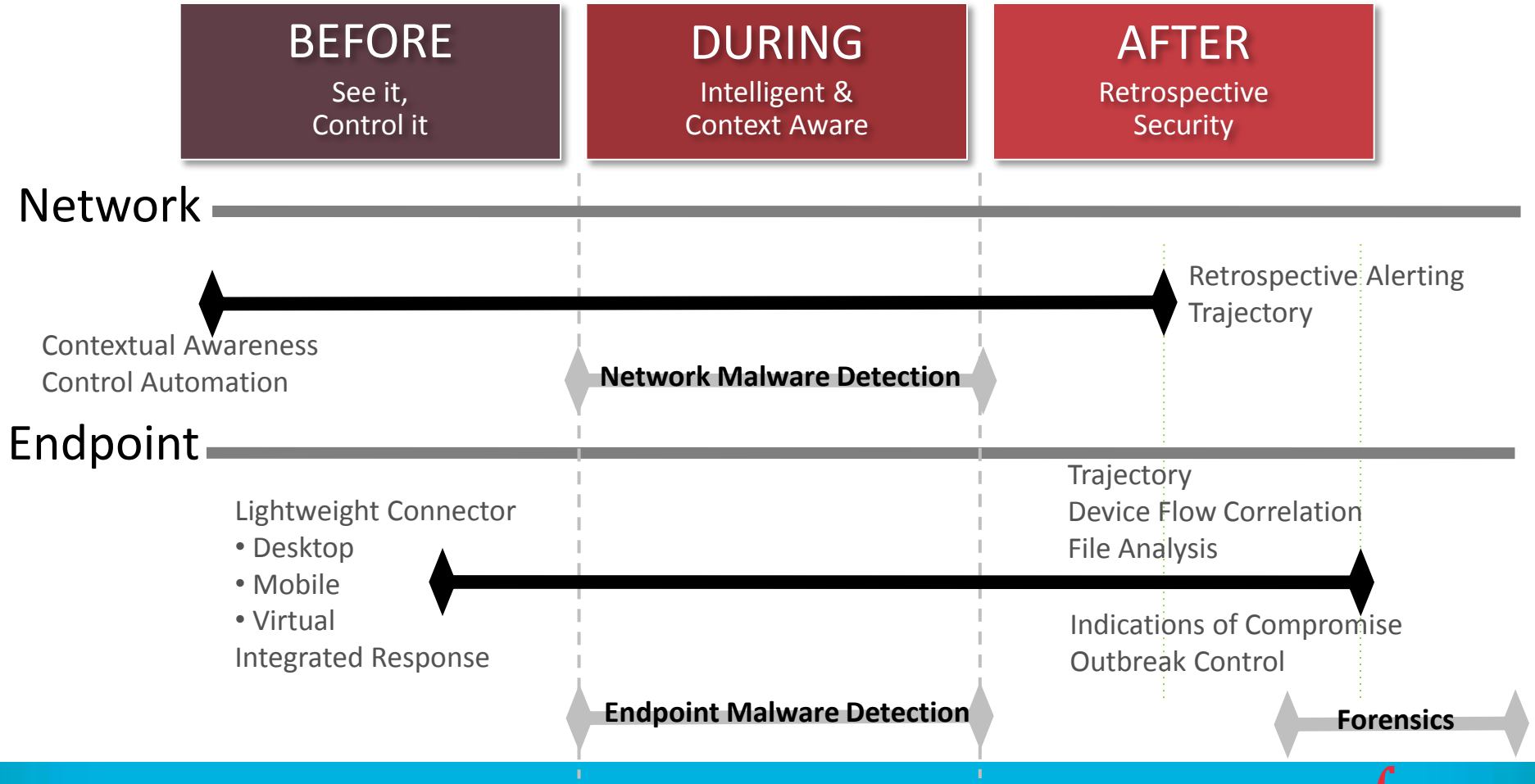
Continuous Capability

- Coherent & Co-Ordinated



Breadth & Depth

- Address the Entire Attack Continuum



Open Platform

- Open Detections, Open Data Model

BEFORE	DURING	AFTER
See it, Control it	Intelligent & Context Aware	Retrospective Security

Vulnerability Management

tenable network security · RAPID7 · QUALYS · Critical Watch · Greenbone

Custom Detection

onapsis · WhiteHat SECURITY · NTO

Full Packet Capture

nPULSE · NETSCOUT · SOLERA

NAC

BRADFORD NETWORKS · PacketFence · extreme networks · CITRIX

Incident Response

Guidance SOFTWARE

Network Access/Data Capture

XIXIA · NetOptics · Network Critical · VSS monitoring · Gigamon · GARLAND

Visualization

realstatus

SIEM

BlackStratus · Tier-3 · Trustwave · ArcSight · loglogic · splunk> · Labs · LogRhythm

Sourcefire STP Program – API Framework

More

- @VRT_Sourcefire
- http://vrt-blog.snort.org
- www.sourcefire.com
- go.sourcefire.com/sourcefirechalktalks
- VRT Service Blog

RSA CONFERENCE ASIA PACIFIC 2013

THANK YOU

Dean Frye
Sourcefire

Session ID:

Session Classification: