RSA® Security Analytics

Gintaras Pelenis
+370 698 75456
Gintaras.pelenis@emc.com

The Problem

Traditional Security Is Not Working

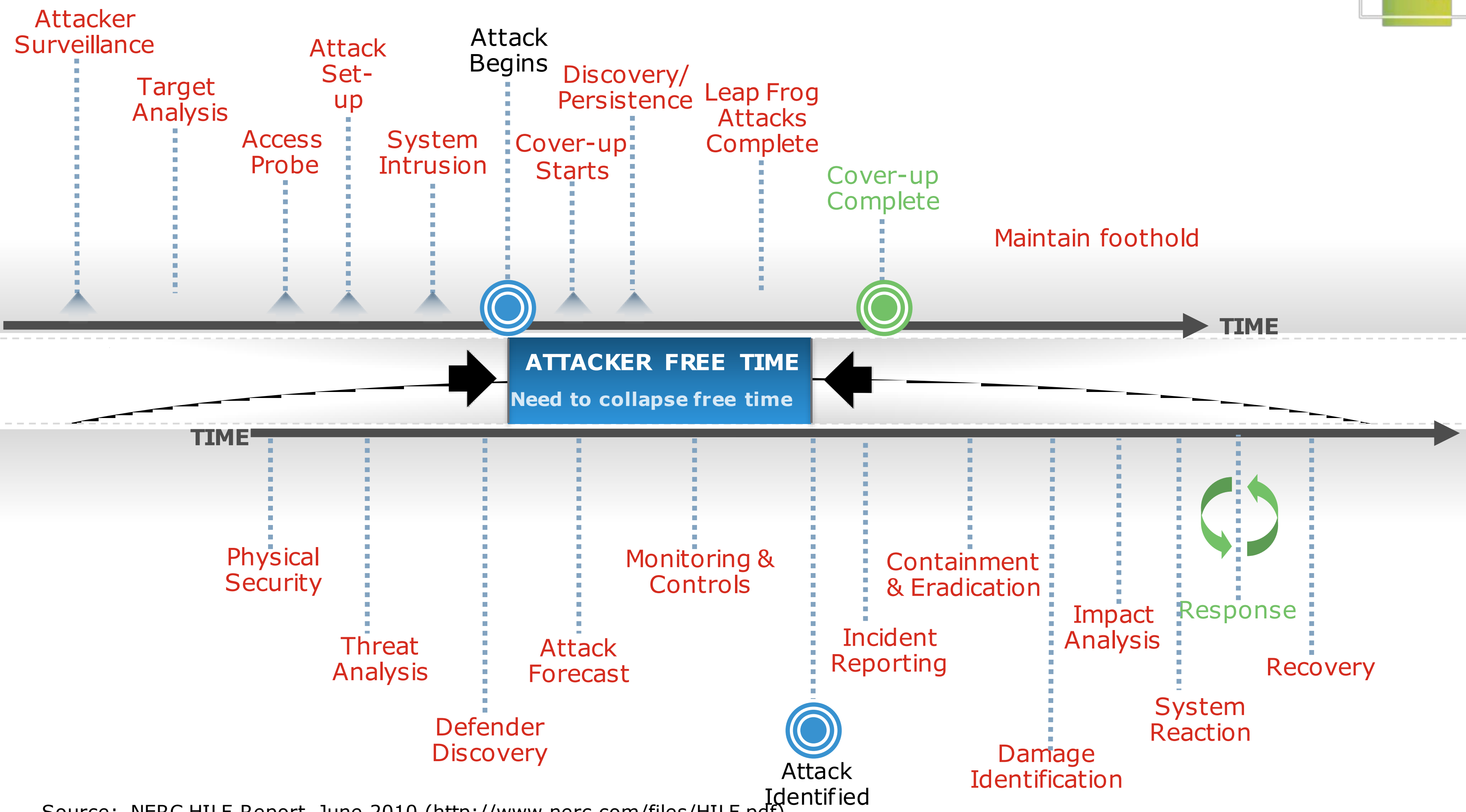
Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

99% of breaches led to compromise within "days" or less with 85% leading to data exfiltration in the same time

85% of breaches took "weeks" or more to discover

Source: Verizon 2012 Data Breach Investigations Report

Reducing Attacker Free Time



Attacker Surveillance

Target Analysis

Access Probe

Attack Set-up

System Intrusion

Attack Begins

Cover-up Starts

Discovery/ Persistence

Leap Frog Attacks Complete

Cover-up Complete

Maintain foothold

TIME

ATTACKER FREE TIME

Need to collapse free time

TIME

Physical Security

Threat Analysis

Defender Discovery

Attack Forecast

Monitoring & Controls

Attack Identified

Incident Reporting

Containment & Eradication

Damage Identification

Impact Analysis

System Reaction

Response

Recovery

Source: NERC HILF Report, June 2010 (http://www.nerc.com/files/HILF.pdf)

What Needs To Be Done?

Today's Security Requirements

Comprehensive Visibility

"Analyze everything happening in my infrastructure"

Agile Analytics

"Enable me to analyze and investigate potential threats in near real time"

Actionable Intelligence

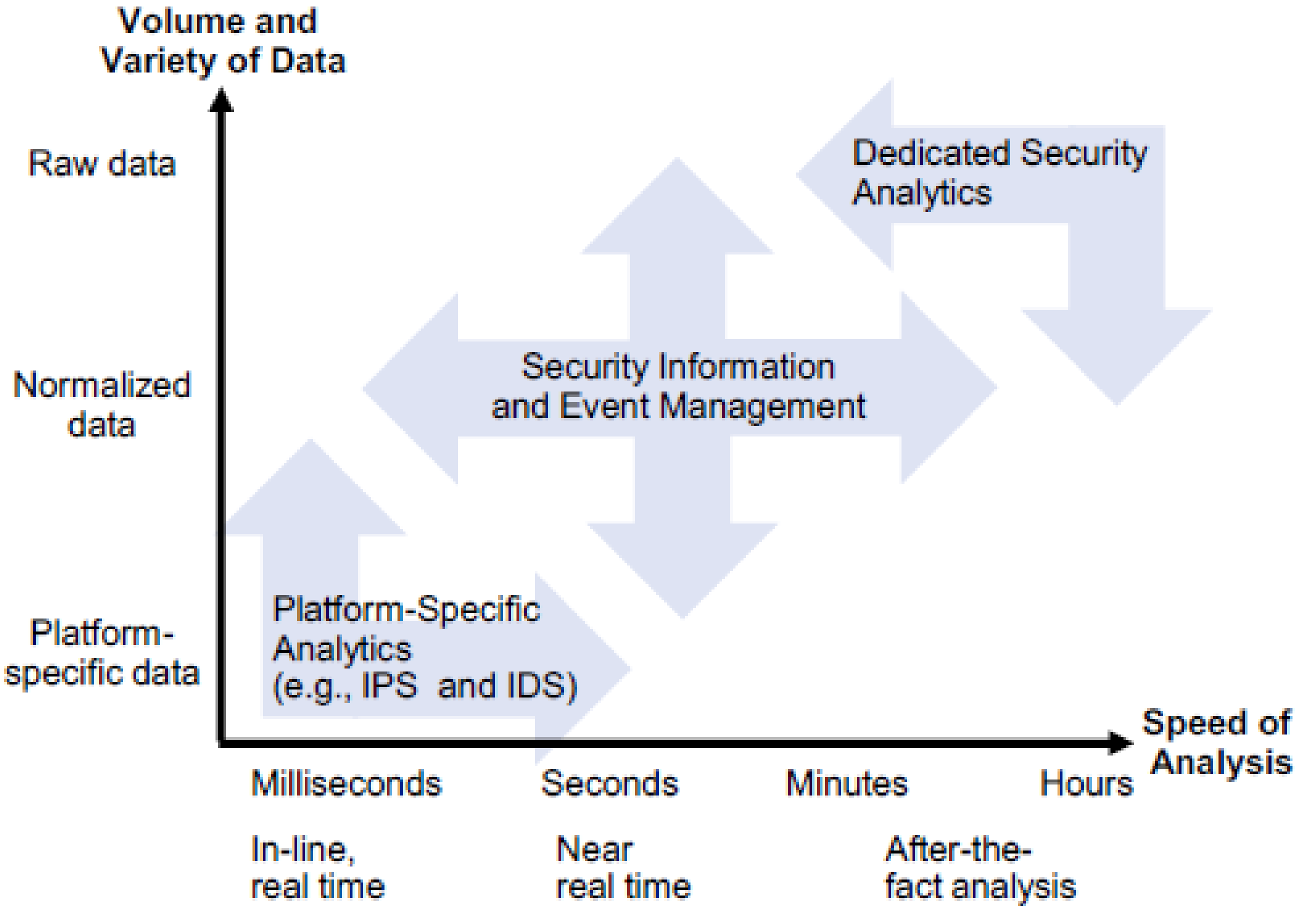
"Help me identify targets, threats & incidents"

Scalable Infrastructure

"Need a flexible infrastructure to conduct short term and long term analysis"

RSA EMC²

SIEM Needs To Evolve Into Security Analytics



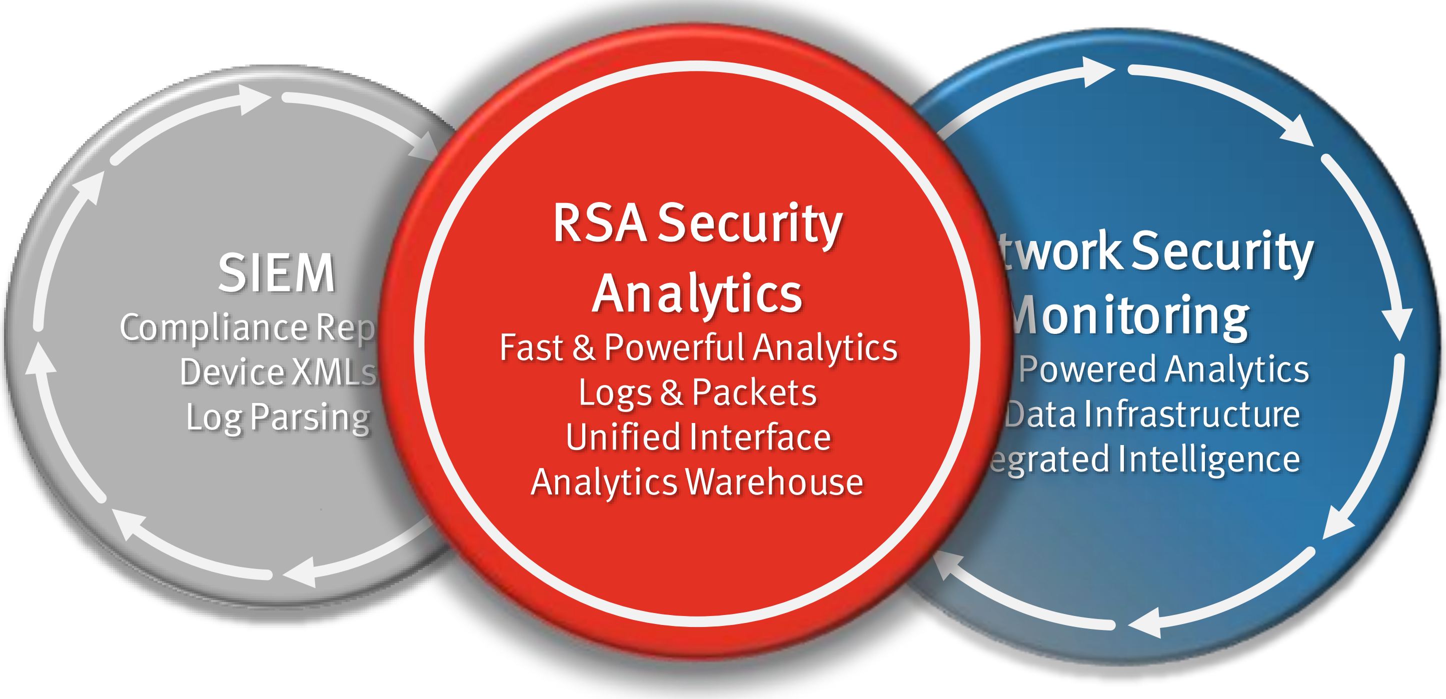
Gartner Source: Gartner (March 2012)

Gartner, Information Security is Becoming a Big Data Analytics Problem, Neil Macdonald, Mar. 23, 2012

Introducing Security Analytics

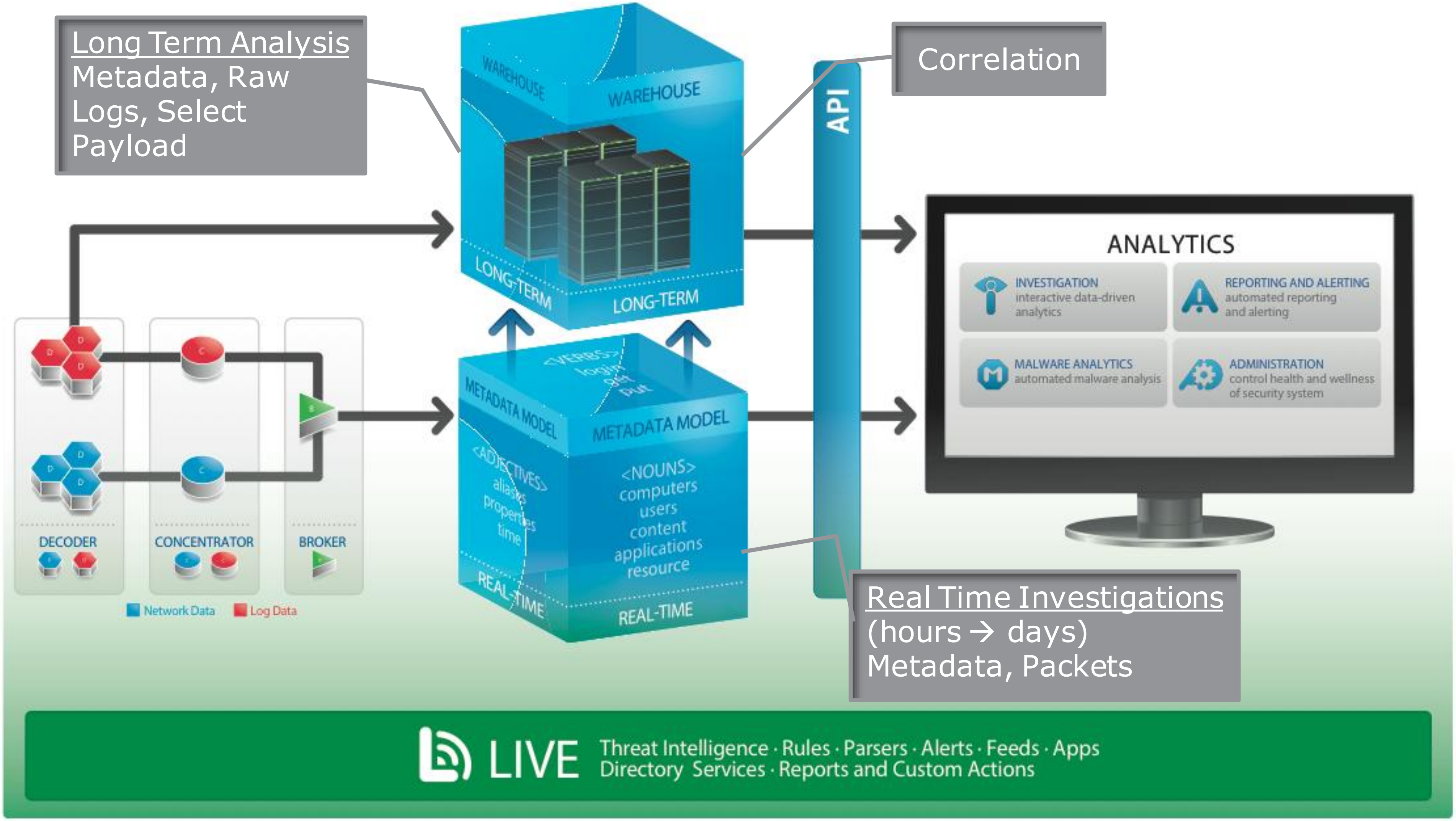
RSA Security Analytics: Changing The Security Management Status Quo

Unified platform for security monitoring, incident investigations and compliance reporting



SEE DATA YOU DIDN'T SEE BEFORE, UNDERSTAND DATA YOU DIDN'T EVEN CONSIDER BEFORE

RSA Security Analytics Architecture



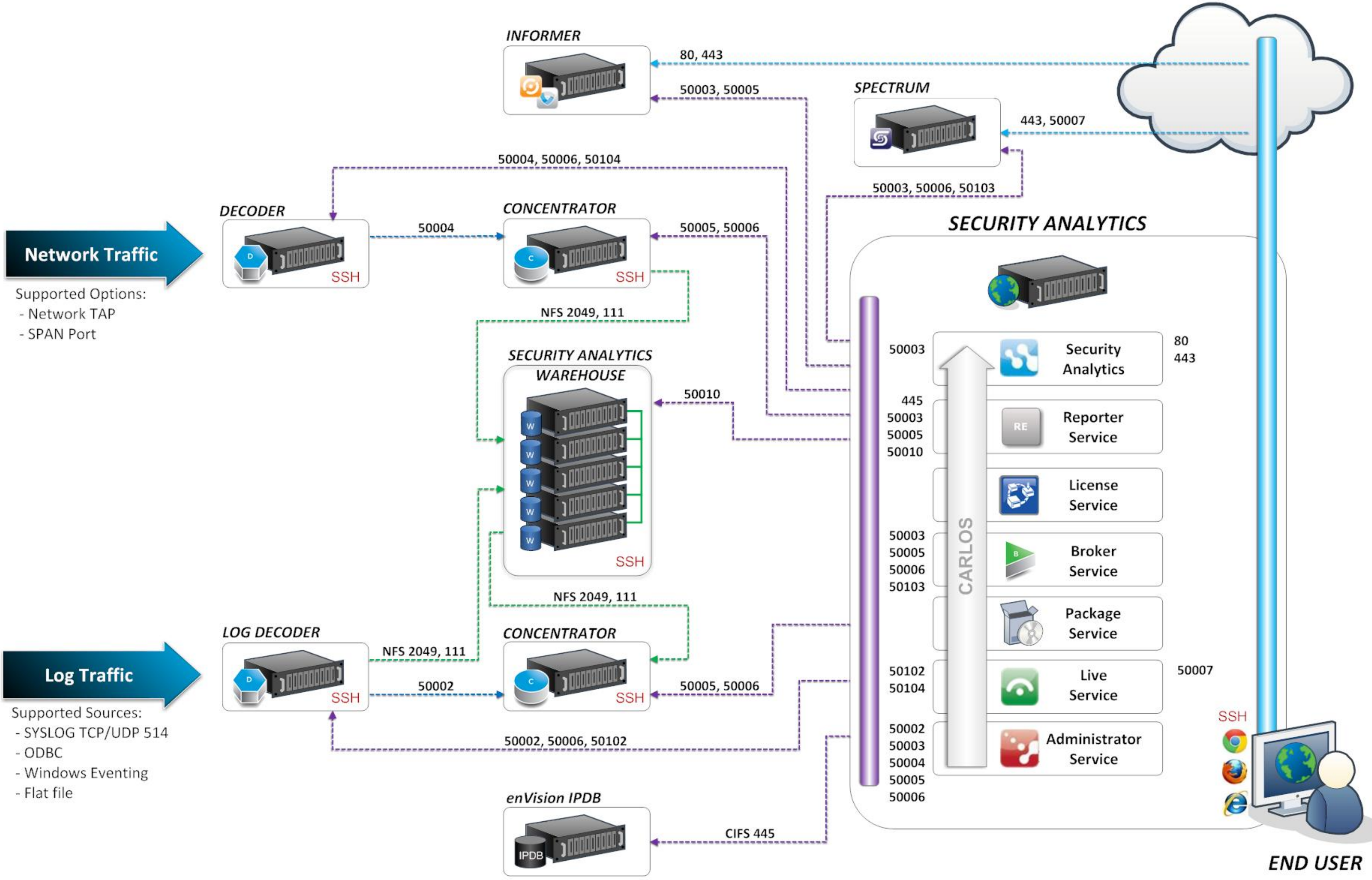
Long Term Analysis
Metadata, Raw Logs, Select Payload

Correlation

Real Time Investigations
(hours → days)
Metadata, Packets

LIVE Threat Intelligence · Rules · Parsers · Alerts · Feeds · Apps
Directory Services · Reports and Custom Actions

SECURITY ANALYTICS ARCHITECTURE



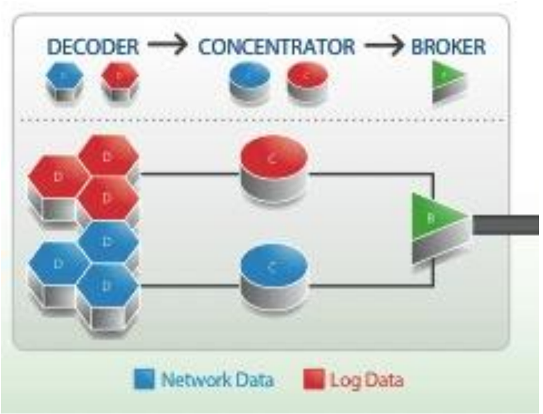
Supported Options:
- Network TAP
- SPAN Port

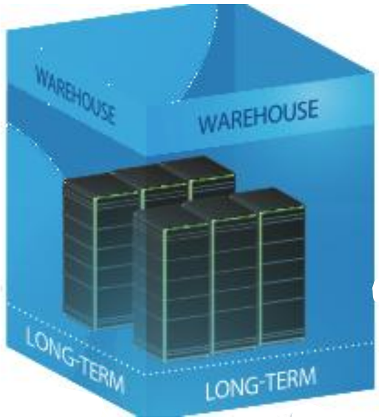
Supported Sources:
- SYSLOG TCP/UDP 514
- ODBC
- Windows Eventing
- Flat file

What Makes Security Analytics Different?

- **Big Data Infrastructure**
  - Fast & Scalable
  - Logs & Packets
  - Security data warehouse plus proven NetWitness infrastructure
- **High Powered Analytics**
  - The speed and smarts to detect, investigate & understand advanced threats
  - Comprehensive visibility to see everything happening in an environment
  - Short term & long term analytics plus compliance
  - Removes the hay vs. digging for needles
- **Integrated Intelligence**
  - Intelligence from the global security community and RSA FirstWatch fused with your organization’s data
  - Understand what to look for and utilize what others have already found

Big Data Infrastructure

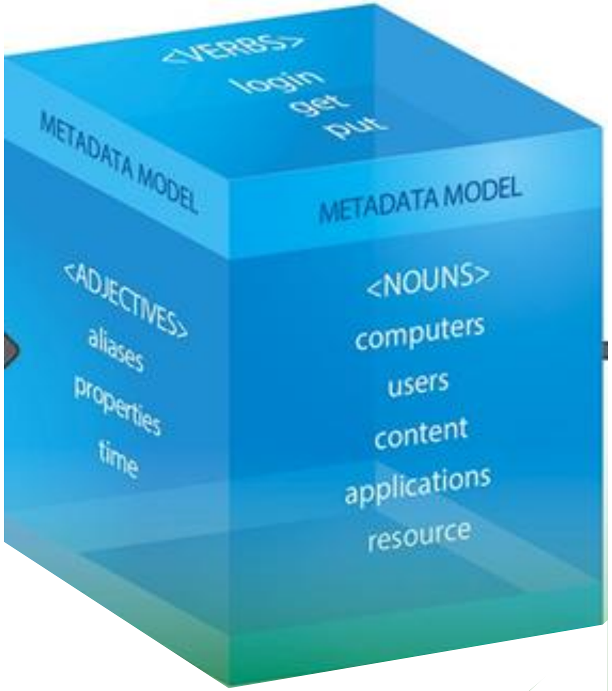




- Single platform for capturing and analyzing large amounts of network and log data
- Distributed, "scale-out" architecture
- Unique architecture to support both "speed" and "smarts" for threat analysis
- Security data warehouse for long term analytics & compliance
- Proven NetWitness infrastructure of short term analytics and investigations

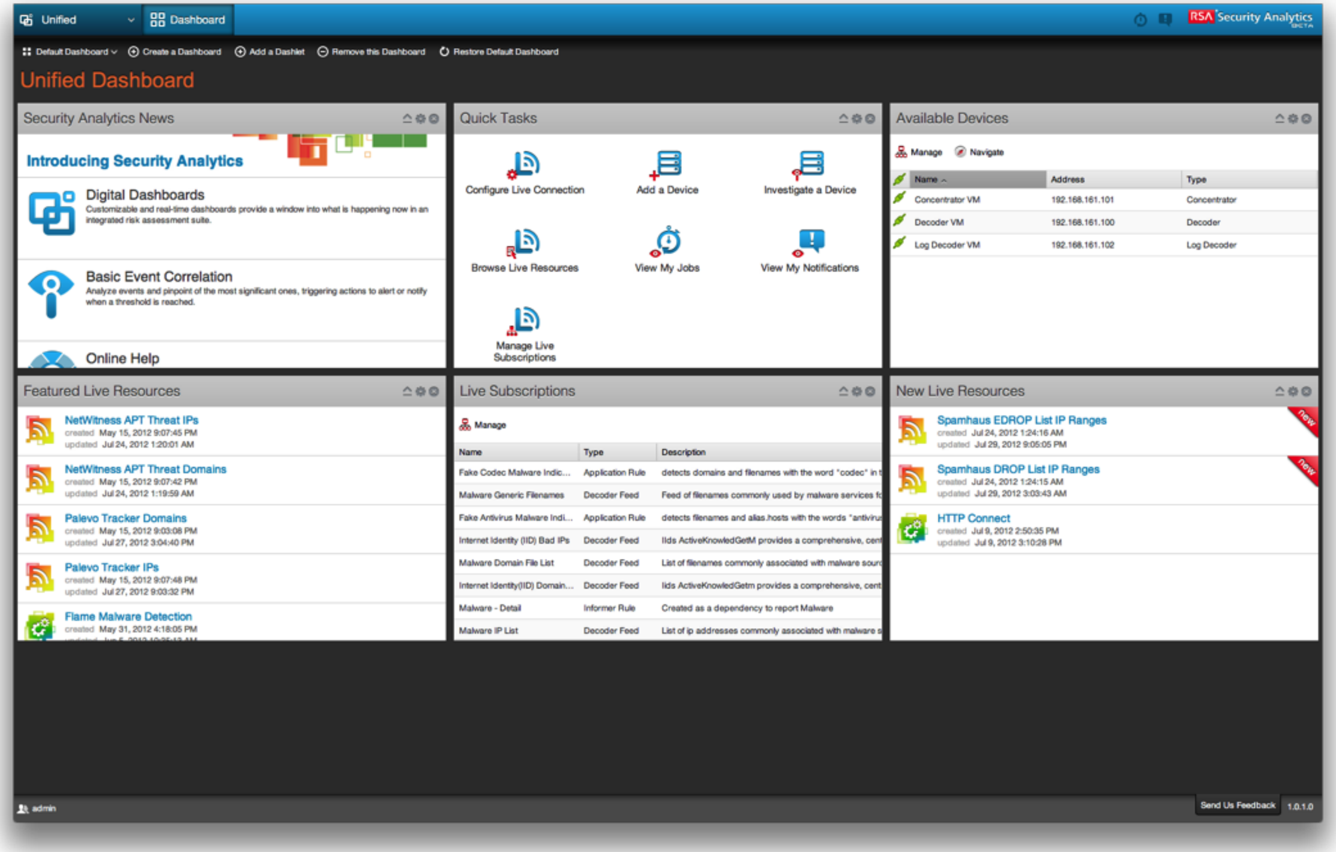
High Powered Analytics

- Eliminates blind spots to achieve comprehensive visibility across the enterprise
- Real-time and “after-the-fact” investigations
- Uses the industry’s most comprehensive and easily understandable analytical workbench
- Proven, patented analytics applies business context to security investigations
- Automates the generation of compliance reports and supports long term forensic analysis



Taking A Closer Look:
Real-Time Investigations

Unified Dashboard



Unified Dashboard

Security Analytics News

Introducing Security Analytics

Digital Dashboards
Customizable and real-time dashboards provide a window into what is happening now in an integrated risk assessment suite.

Basic Event Correlation
Analyze events and pinpoint of the most significant ones, triggering actions to alert or notify when a threshold is reached.

Online Help

Quick Tasks

Available Devices

Name	Address	Type
Concentrator VM	192.168.161.101	Concentrator
Decoder VM	192.168.161.100	Decoder
Log Decoder VM	192.168.161.102	Log Decoder

Featured Live Resources

NetWitness APT Threat IPs
created May 15, 2012 9:07:45 PM
updated Jul 24, 2012 1:20:01 AM

NetWitness APT Threat Domains
created May 15, 2012 9:07:42 PM
updated Jul 24, 2012 1:19:59 AM

Palevo Tracker Domains
created May 15, 2012 9:03:08 PM
updated Jul 27, 2012 3:04:40 PM

Palevo Tracker IPs
created May 15, 2012 9:07:48 PM
updated Jul 27, 2012 9:03:32 PM

Flame Malware Detection
created May 31, 2012 4:18:05 PM

Live Subscriptions

Name	Type	Description
Fake Codec Malware Indic...	Application Rule	detects domains and filenames with the word "codec" in t
Malware Generic Filenames	Decoder Feed	Feed of filenames commonly used by malware services fo
Fake Antivirus Malware Indi...	Application Rule	detects filenames and alias.hosts with the words "antiviru
Internet Identity (IID) Bad IPs	Decoder Feed	Ilds ActiveKnowledGetM provides a comprehensive, cent
Malware Domain File List	Decoder Feed	List of filenames commonly associated with malware sourc
Internet Identity(IID) Domain...	Decoder Feed	Iids ActiveKnowledGetm provides a comprehensive, cent
Malware - Detail	Informer Rule	Created as a dependency to report Malware
Malware IP List	Decoder Feed	List of ip addresses commonly associated with malware s

New Live Resources

Spamhaus EDROP List IP Ranges
created Jul 24, 2012 1:24:16 AM
updated Jul 29, 2012 9:05:05 PM

Spamhaus DROP List IP Ranges
created Jul 24, 2012 1:24:15 AM
updated Jul 29, 2012 3:03:43 AM

HTTP Connect
created Jul 9, 2012 2:50:35 PM
updated Jul 9, 2012 3:10:28 PM

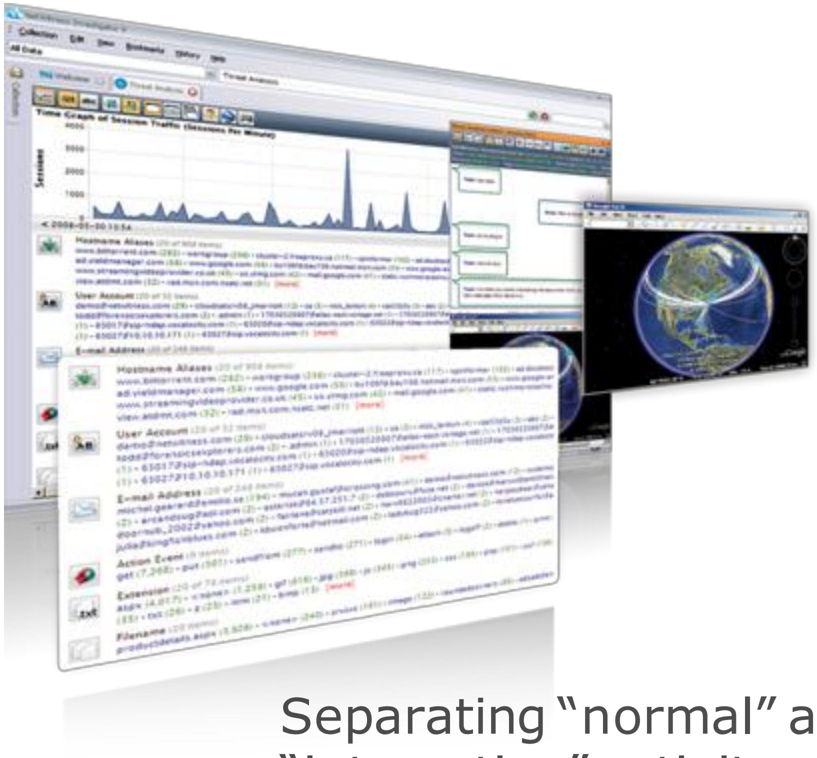
Centralizes analysis with consolidated browser based dashboard

Smashes existing product silos

Increases analyst efficiency and effectiveness

The Approach To Security Analysis

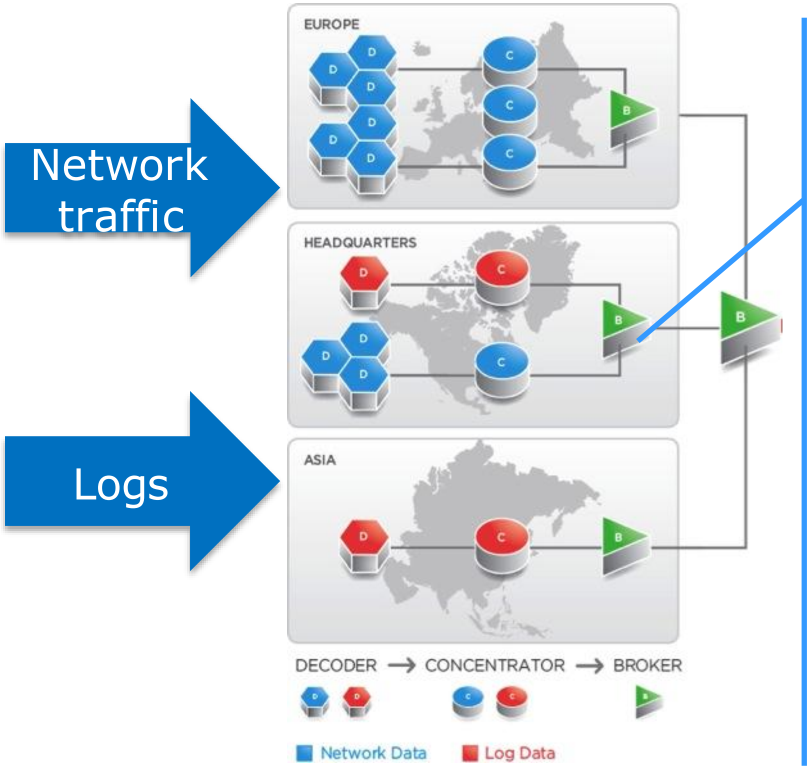
Stop searching for needles in a haystack…



World-class threat analysts remove hay until only needles remain

Separating "normal" activity to discover "interesting" activity - for the *primary* purpose of generating new "intelligence."

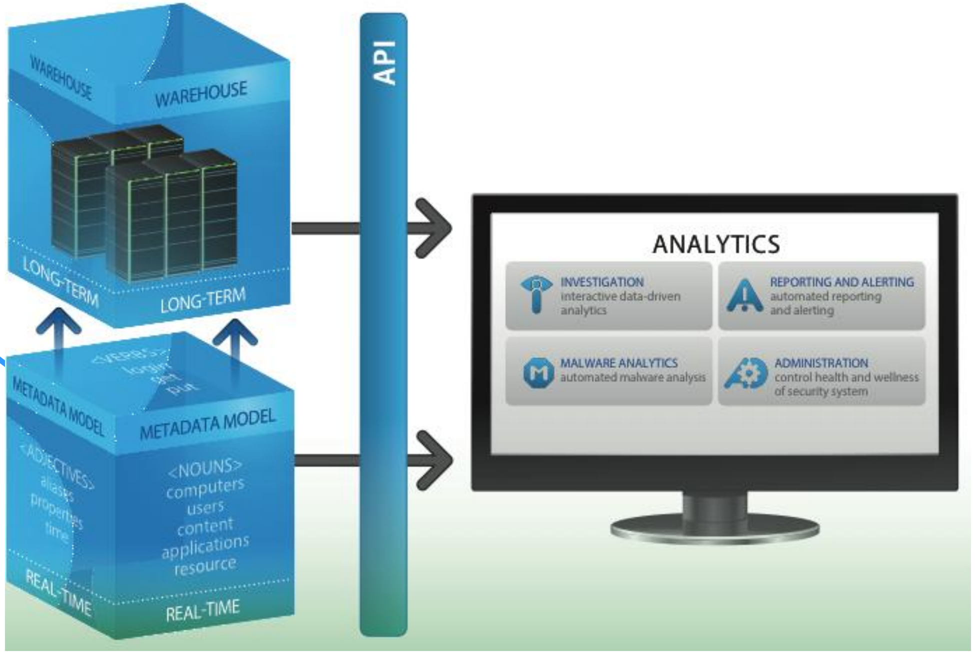
Full Network Visibility



- Gain full visibility into your network including both logs and packets
- Discover advanced threats missed by traditional security approaches
- Completely reconstruct network sessions for real time analysis and investigation
- Capture all data from the network to the application layer
- Perform detailed session analysis – regardless of port or protocol

Patented, Award-Winning Security Analytics

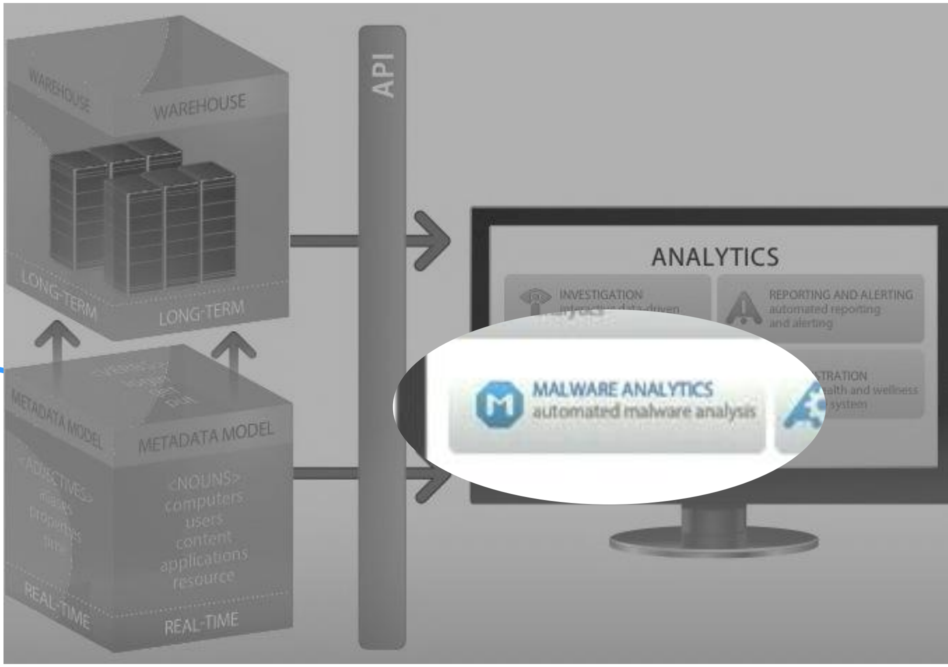
- *Patented* methodology for metadata extraction
- Presents data in understandable format
- *Patented* investigative interface that displays your data in drillable categories
- Speed and flexibility for complete situational awareness



Malware Analysis

Identifies the widest spectrum of malware-based attacks

- Sandboxing, community intelligence, file content and network behavior analysis
- Automatically answer thousands of questions

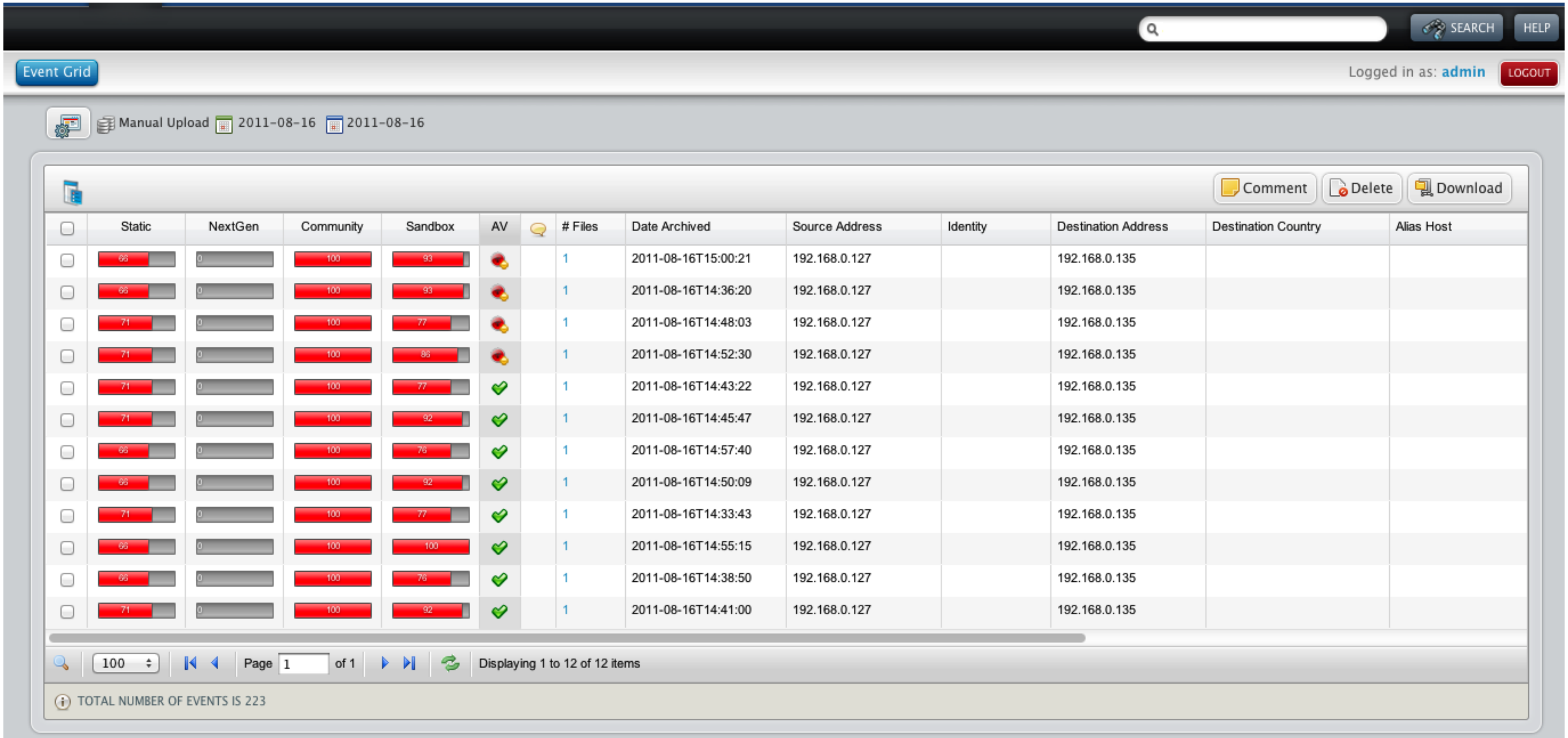


Malware Analysis

- **Identify the widest spectrum of malware-based attacks, including zero-day attacks**
  - Gain insight into attacks missed by both traditional and modern approaches to malware protection
  - Consider all the network data and behavior to provide the full context of an attack
- **Analyze attacks by utilizing a wide spectrum of investigation techniques**
  - Combine sandboxing, community intelligence, file content and network behavior analysis
  - Automatically answer thousands of questions to help determine an attacker’s intent, their potential targets and the level of threat they pose
- **Increase the speed and accuracy of investigations**
  - Replicate and automate the workflow of an advanced malware analyst
  - Save hours of work and ensure analysts focus on the most critical malware-related events

RSA Security Analytics Malware Analysis

An analytical workbench that utilizes multiple analytical methods to identification and analysis of malware-based attacks, including attacks not seen before.



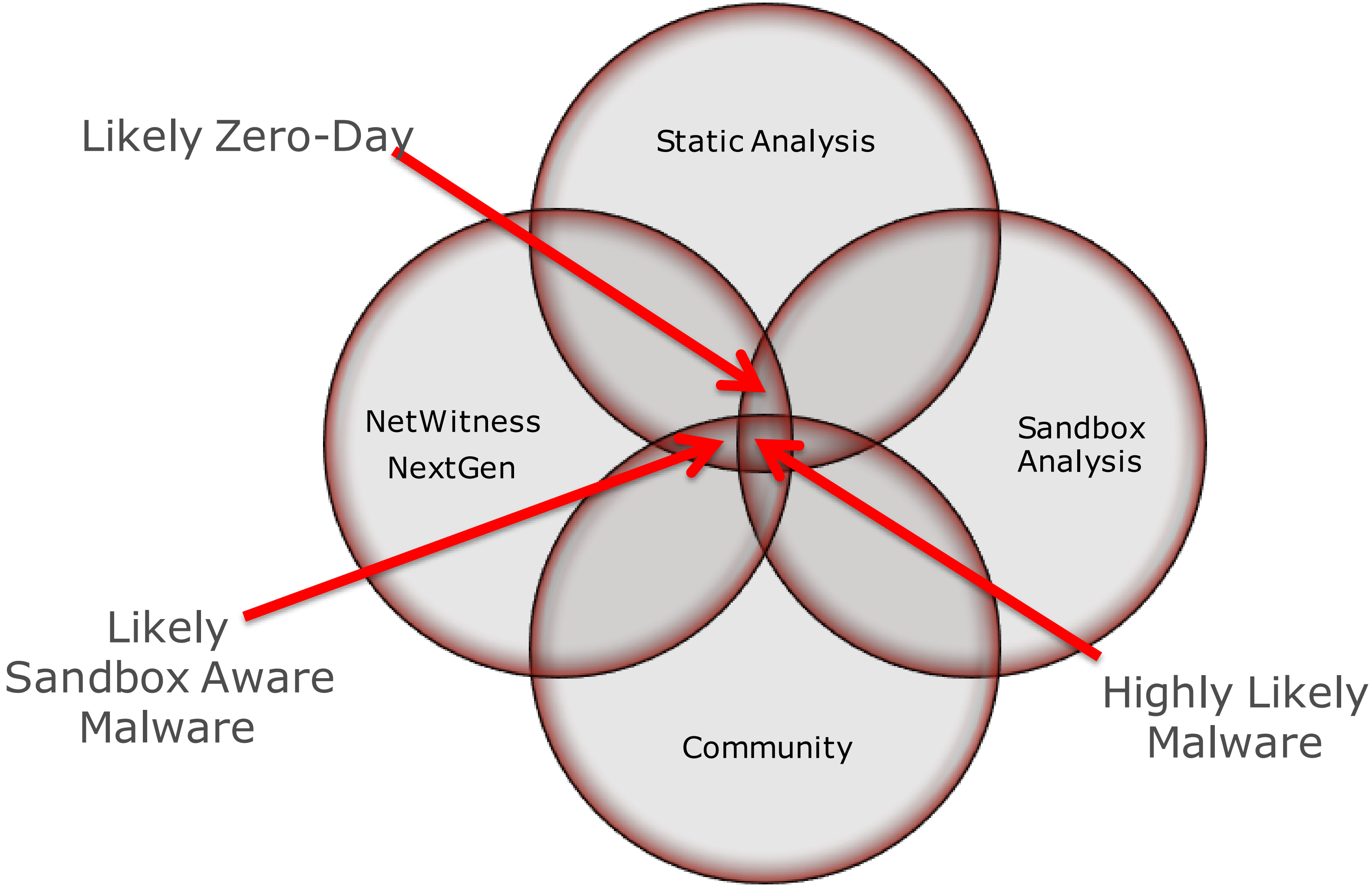
□	Static	NextGen	Community	Sandbox	AV	💬	# Files	Date Archived	Source Address	Identity	Destination Address	Destination Country	Alias Host
□	66	0	100	93	●		1	2011-08-16T15:00:21	192.168.0.127		192.168.0.135		
□	66	0	100	93	●		1	2011-08-16T14:36:20	192.168.0.127		192.168.0.135		
□	71	0	100	77	●		1	2011-08-16T14:48:03	192.168.0.127		192.168.0.135		
□	71	0	100	86	●		1	2011-08-16T14:52:30	192.168.0.127		192.168.0.135		
□	71	0	100	77	✓		1	2011-08-16T14:43:22	192.168.0.127		192.168.0.135		
□	71	0	100	92	✓		1	2011-08-16T14:45:47	192.168.0.127		192.168.0.135		
□	66	0	100	76	✓		1	2011-08-16T14:57:40	192.168.0.127		192.168.0.135		
□	66	0	100	92	✓		1	2011-08-16T14:50:09	192.168.0.127		192.168.0.135		
□	71	0	100	77	✓		1	2011-08-16T14:33:43	192.168.0.127		192.168.0.135		
□	66	0	100	100	✓		1	2011-08-16T14:55:15	192.168.0.127		192.168.0.135		
□	66	0	100	76	✓		1	2011-08-16T14:38:50	192.168.0.127		192.168.0.135		
□	71	0	100	92	✓		1	2011-08-16T14:41:00	192.168.0.127		192.168.0.135		

100 Page 1 of 1 Displaying 1 to 12 of 12 items

TOTAL NUMBER OF EVENTS IS 223

Malware Analysis

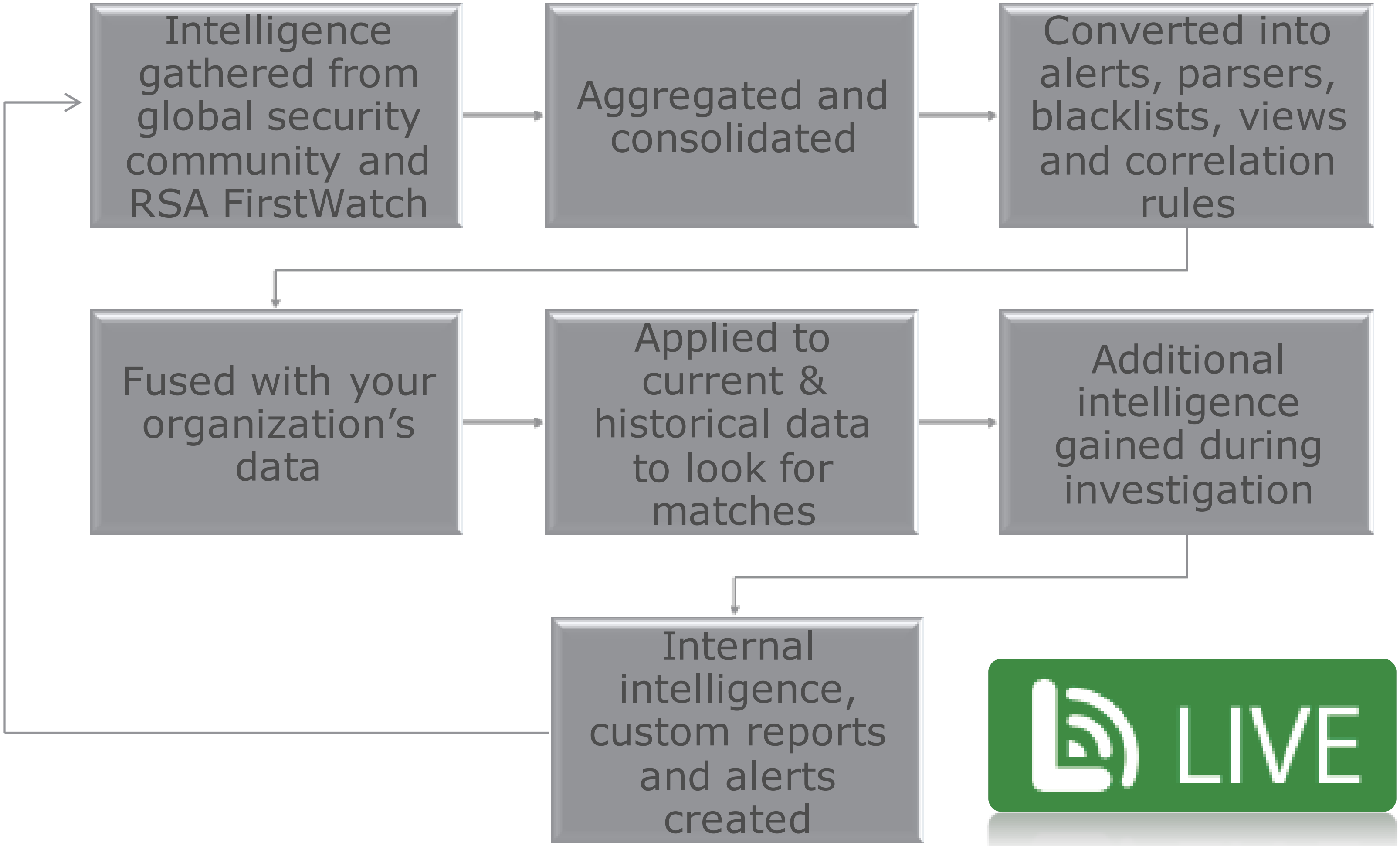
Multiple analytical methods in one tool



Enriching data

Integrated Intelligence

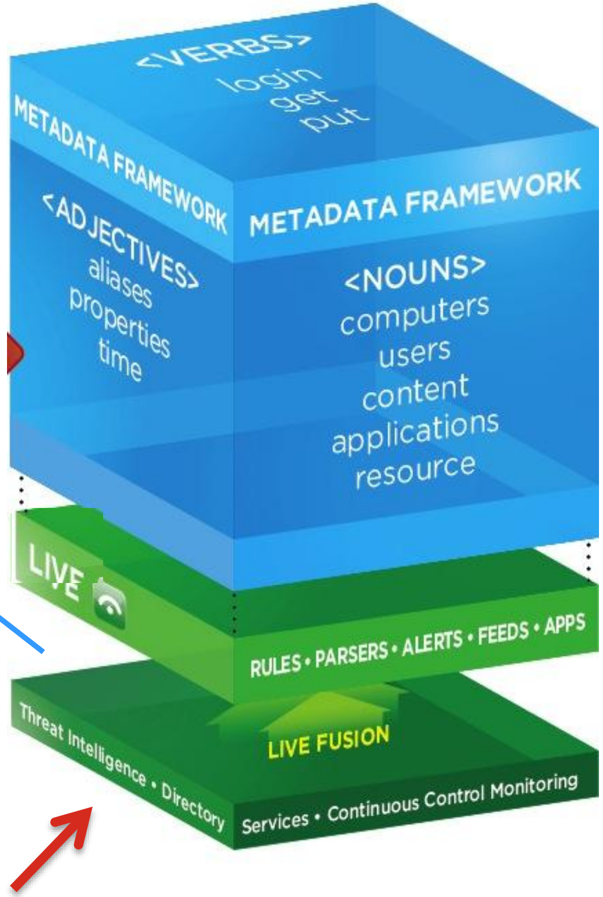
How Do I Know What To Look For?


Intelligence gathered from global security community and RSA FirstWatch
Aggregated and consolidated
Converted into alerts, parsers, blacklists, views and correlation rules
Fused with your organization's data
Applied to current & historical data to look for matches
Additional intelligence gained during investigation
Internal intelligence, custom reports and alerts created

LIVE

Fusion of Threat Intelligence With Your Data

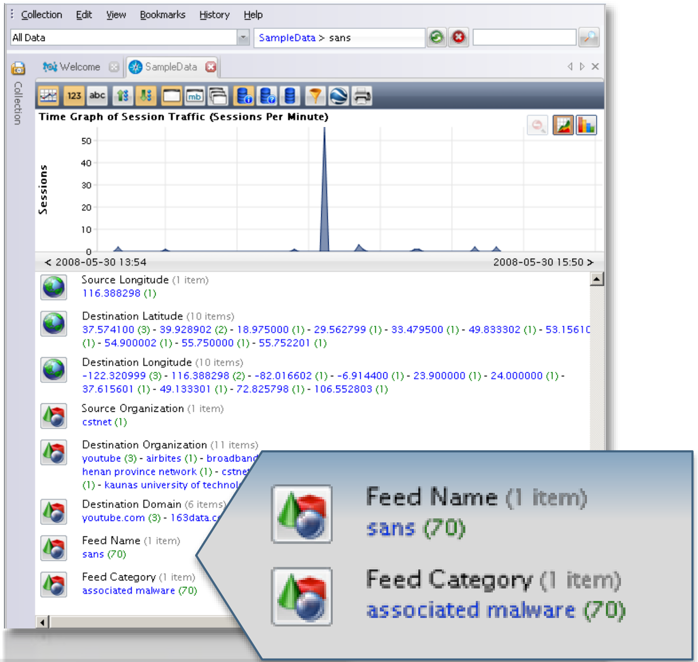
- Automatically enrich data with intelligence to help level playing field
- Integrate custom feeds
- Centralize intelligence
- Take advantage of the best 3rd party and RSA First Watch Intelligence



Fusion of Threat Intelligence

RSA Live In Action

- Definitively classify computers associated with illegal third party exploits, open proxies, worms/viruses, spam engines, Botnets and other current and zero-day exploits
- Prioritize intersection of threat indicators
- Provides real-time, full content navigation of enterprise security intelligence
- Synchronize with RSA FirstWatch and global content derived from best of breed sources



Source Longitude (1 item)
116.388298 (1)

Destination Latitude (10 items)
37.574100 (3) - 39.928902 (2) - 18.975000 (1) - 29.562799 (1) - 33.479500 (1) - 49.833302 (1) - 53.1561C
(1) - 54.900002 (1) - 55.750000 (1) - 55.752201 (1)

Destination Longitude (10 items)
-122.320999 (3) - 116.388298 (2) - -82.016602 (1) - -6.914400 (1) - 23.900000 (1) - 24.000000 (1) -
37.615601 (1) - 49.133301 (1) - 72.825798 (1) - 106.552803 (1)

Source Organization (1 item)
cstnet (1)

Destination Organization (11 items)
youtube (3) - airbites (1) - broadband
henan province network (1) - cstnet
(1) - kaunas university of technol

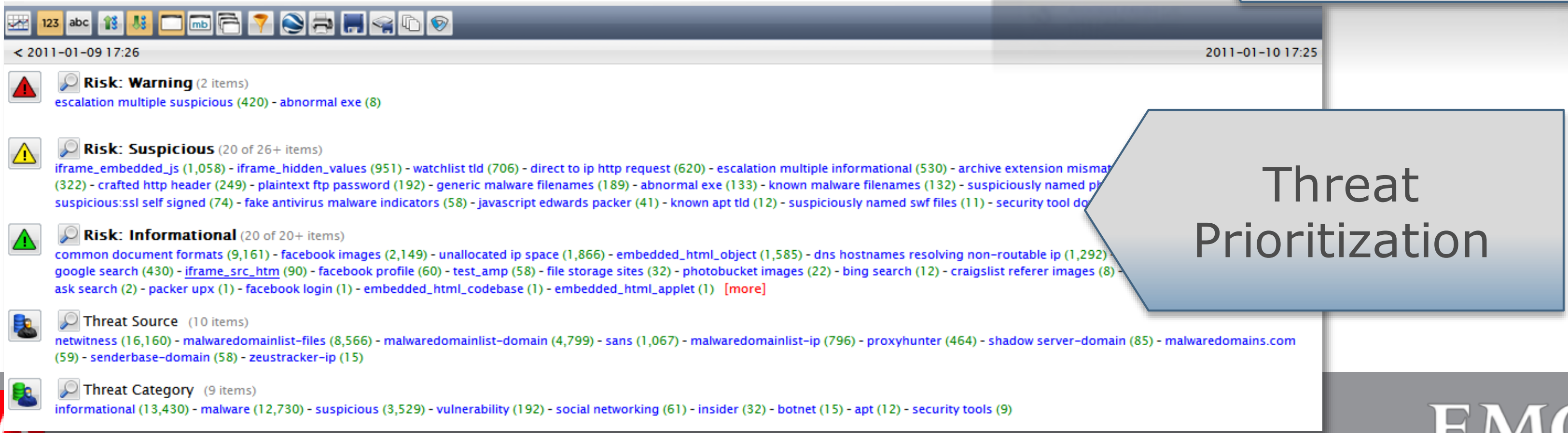
Destination Domain (6 items)
youtube.com (3) - 163data.c

Feed Name (1 item)
sans (70)

Feed Category (1 item)
associated malware (70)

Feed Name (1 item)
sans (70)

Feed Category (1 item)
associated malware (70)



Risk: Warning (2 items)
escalation multiple suspicious (420) - abnormal exe (8)

Risk: Suspicious (20 of 26+ items)
iframe_embedded_js (1,058) - iframe_hidden_values (951) - watchlist tld (706) - direct to ip http request (620) - escalation multiple informational (530) - archive extension mismat
(322) - crafted http header (249) - plaintext ftp password (192) - generic malware filenames (189) - abnormal exe (133) - known malware filenames (132) - suspiciously named ph
suspicious:ssl self signed (74) - fake antivirus malware indicators (58) - javascript edwards packer (41) - known apt tld (12) - suspiciously named swf files (11) - security tool do

Risk: Informational (20 of 20+ items)
common document formats (9,161) - facebook images (2,149) - unallocated ip space (1,866) - embedded_html_object (1,585) - dns hostnames resolving non-routable ip (1,292) -
google search (430) - iframe_src_htm (90) - facebook profile (60) - test_amp (58) - file storage sites (32) - photobucket images (22) - bing search (12) - craigslist referer images (8) -
ask search (2) - packer upx (1) - facebook login (1) - embedded_html_codebase (1) - embedded_html_applet (1) [more]

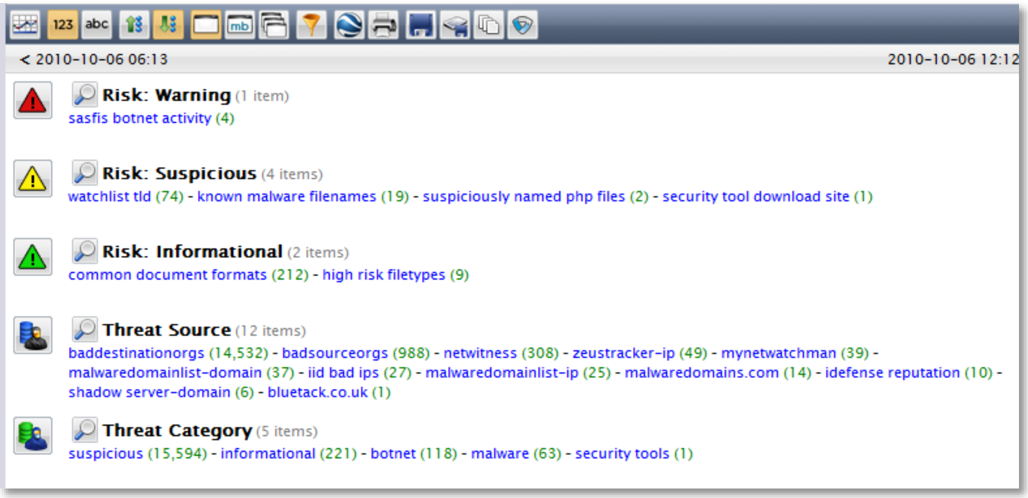
Threat Source (10 items)
netwitness (16,160) - malwaredomainlist-files (8,566) - malwaredomainlist-domain (4,799) - sans (1,067) - malwaredomainlist-ip (796) - proxyhunter (464) - shadow server-domain (85) - malwaredomains.com
(59) - senderbase-domain (58) - zeustracker-ip (15)

Threat Category (9 items)
informational (13,430) - malware (12,730) - suspicious (3,529) - vulnerability (192) - social networking (61) - insider (32) - botnet (15) - apt (12) - security tools (9)

Threat Prioritization

RSA Live In Action – Threat Prioritization

- Risk: Warning –high likelihood of malicious activity (botnet, malicious obfuscation, and other malware activity).
- Risk: Suspicious – not overtly malicious, but suspicious when combined with other behaviors (known malware filenames, non-standard exe structure, pdfs with javascript, etc).
- Risk: Informational – notable when combined with other behaviors. (hits to file sharing sites, bittorrent activity, social networking use)



< 2010-10-06 06:13 2010-10-06 12:12

Risk: Warning (1 item)
sasfis botnet activity (4)

Risk: Suspicious (4 items)
watchlist tld (74) - known malware filenames (19) - suspiciously named php files (2) - security tool download site (1)

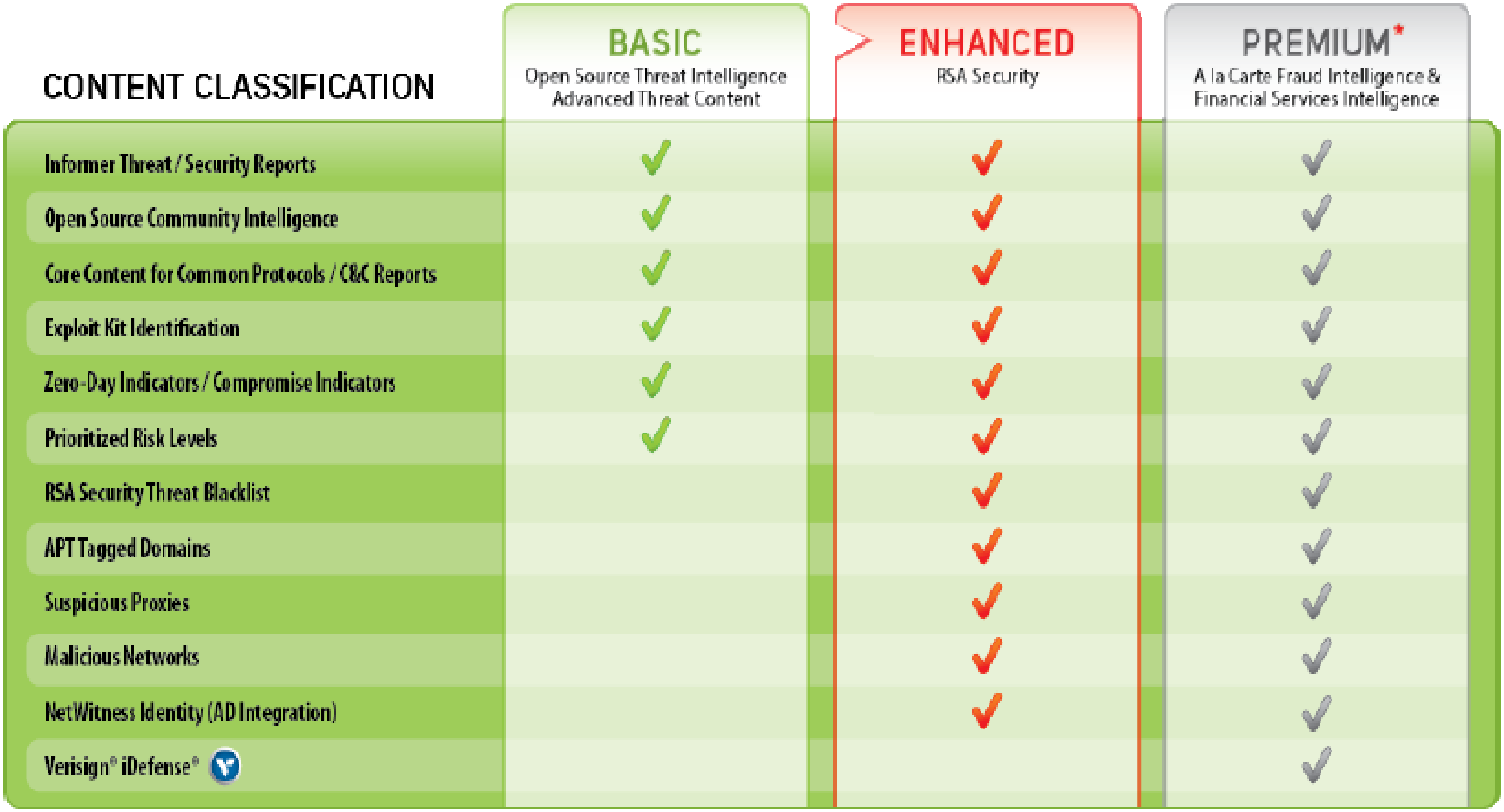
Risk: Informational (2 items)
common document formats (212) - high risk filetypes (9)

Threat Source (12 items)
baddestinationorgs (14,532) - badsourceorgs (988) - netwitness (308) - zeustracker-ip (49) - mynetwatchman (39) - malwaredomainlist-domain (37) - iid bad ips (27) - malwaredomainlist-ip (25) - malwaredomains.com (14) - idefense reputation (10) - shadow server-domain (6) - bluetack.co.uk (1)

Threat Category (5 items)
suspicious (15,594) - informational (221) - botnet (118) - malware (63) - security tools (1)

- ○ *Prioritized alerts to guide analysis based on intersection / threshold of indicators*

RSA Live Subscription Offering



CONTENT CLASSIFICATION	BASIC Open Source Threat Intelligence Advanced Threat Content	ENHANCED RSA Security	PREMIUM* A la Carte Fraud Intelligence & Financial Services Intelligence
Informer Threat / Security Reports	✓	✓	✓
Open Source Community Intelligence	✓	✓	✓
Core Content for Common Protocols / C&C Reports	✓	✓	✓
Exploit Kit Identification	✓	✓	✓
Zero-Day Indicators / Compromise Indicators	✓	✓	✓
Prioritized Risk Levels	✓	✓	✓
RSA Security Threat Blacklist		✓	✓
APT Tagged Domains		✓	✓
Suspicious Proxies		✓	✓
Malicious Networks		✓	✓
NetWitness Identity (AD Integration)		✓	✓
Verisign® iDefense®			✓

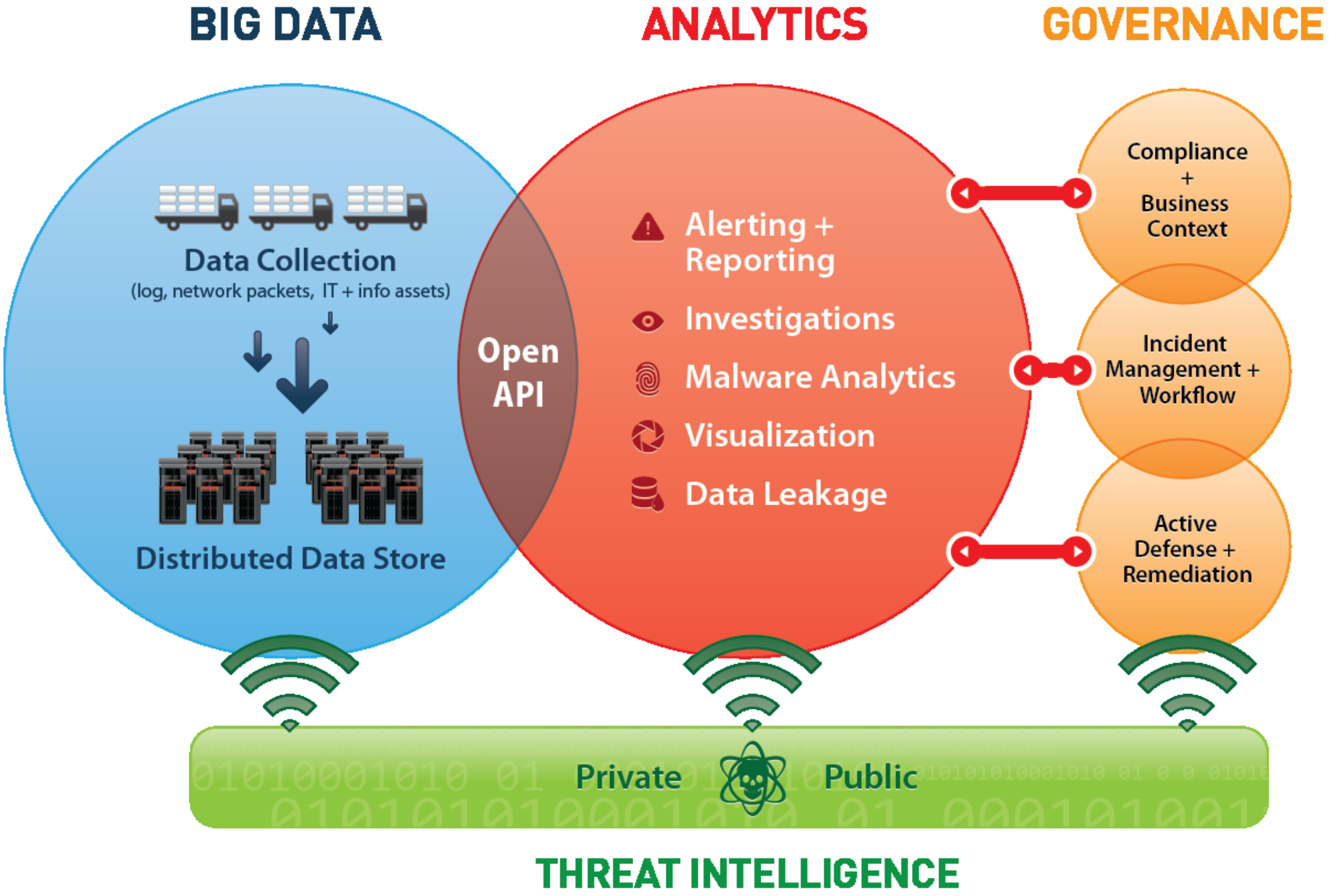
RSA Live – System Metrics

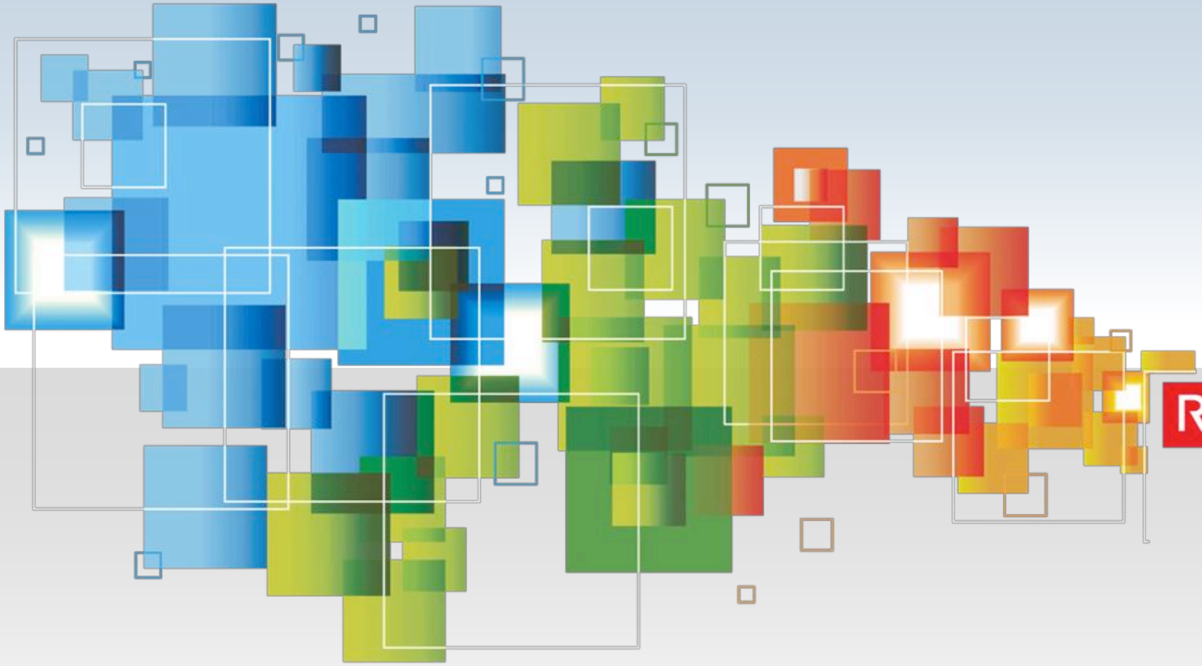
- 1000+ pieces of content
- 100+ Distinct feed sources
  - Over 5 million IP's and Domains tracked
  - 20% grown in unique feed sources over past 6 months
- Content library grew by aggregate 30% over past 6 months

- Average of 1.4 million new data points imported and processed week over week
- Live Content Library updated dynamically ever hour
  - 8760 updates over past year
- Support for 2 new platforms added over past year
  - RSA for Logs
  - Spectrum

RSA Security Management Compliance Vision

Delivering Visibility, Intelligence and Governance





RSA® Security Analytics

RSA® EMC²