Getting Ahead of Advanced Threats

Advanced Security Solutions for Trusted IT

Chezki Gil – Territory Manager
Israel & Greece

Threats are Evolving Rapidly

Criminals

Petty criminal

Unsophisticated

Organized crime

Organized, sophisticated supply chains (PII, financial services, retail)

Nation state actors

PII, government, defense industrial base, IP rich organizations

Non-state actors

Terrorist

PII, Government, critical infrastructure

Anti-establishment vigilantes

"Hacktivists"
Targets of opportunity

Business & IT are evolving rapidly too…

Traditional Security is Not Working

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

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			

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

Source: Verizon 2012 Data Breach Investigations Report

Traditional Security is Unreliable

Signature -based

Perimeter oriented

Compliance Driven

Effective

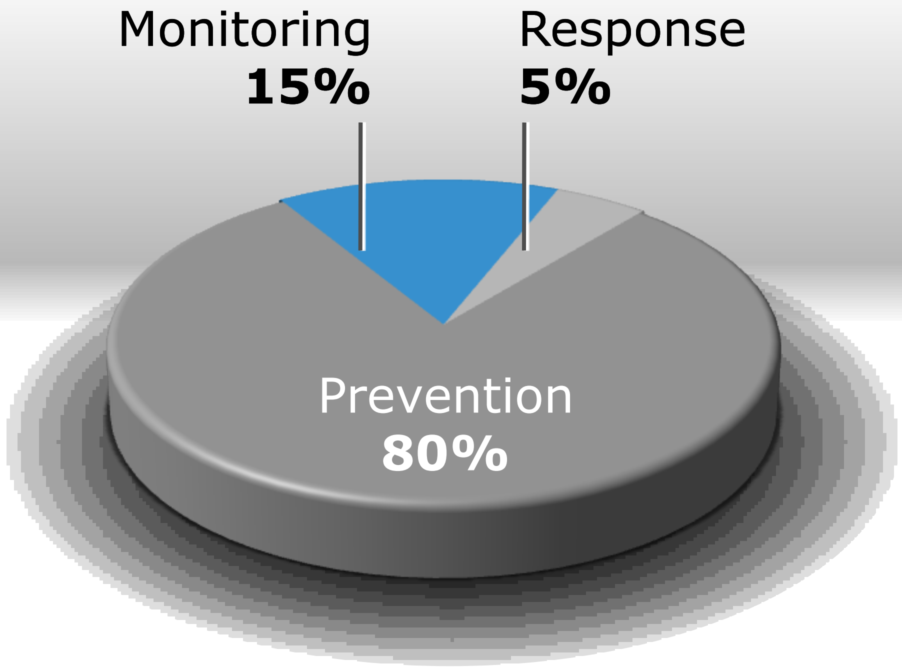
Security Systems need to be:

Agile

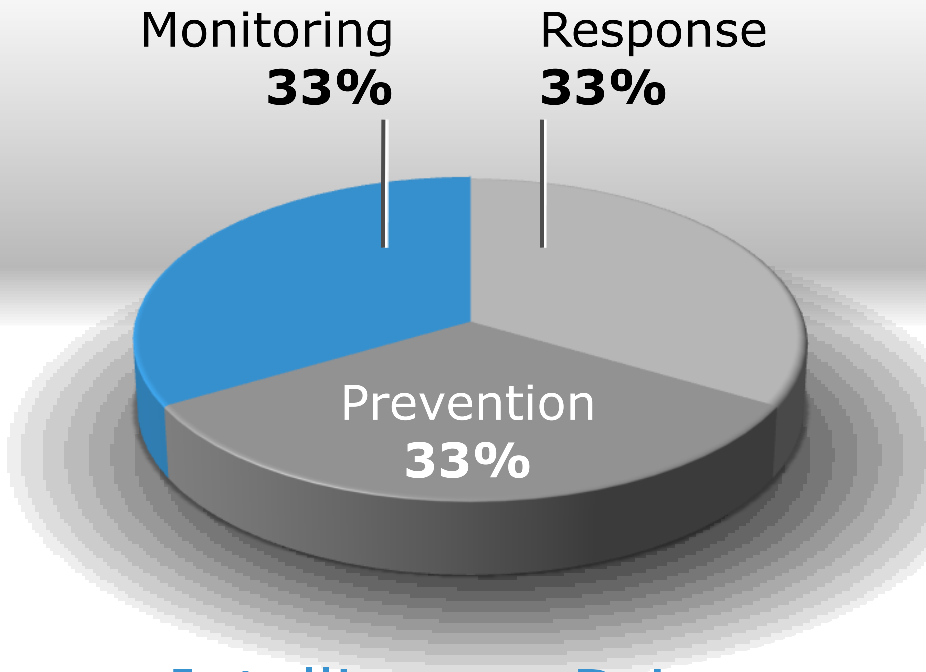
Contextual

Risk-Based

Resource Shift: Budgets and People



Today's Priorities

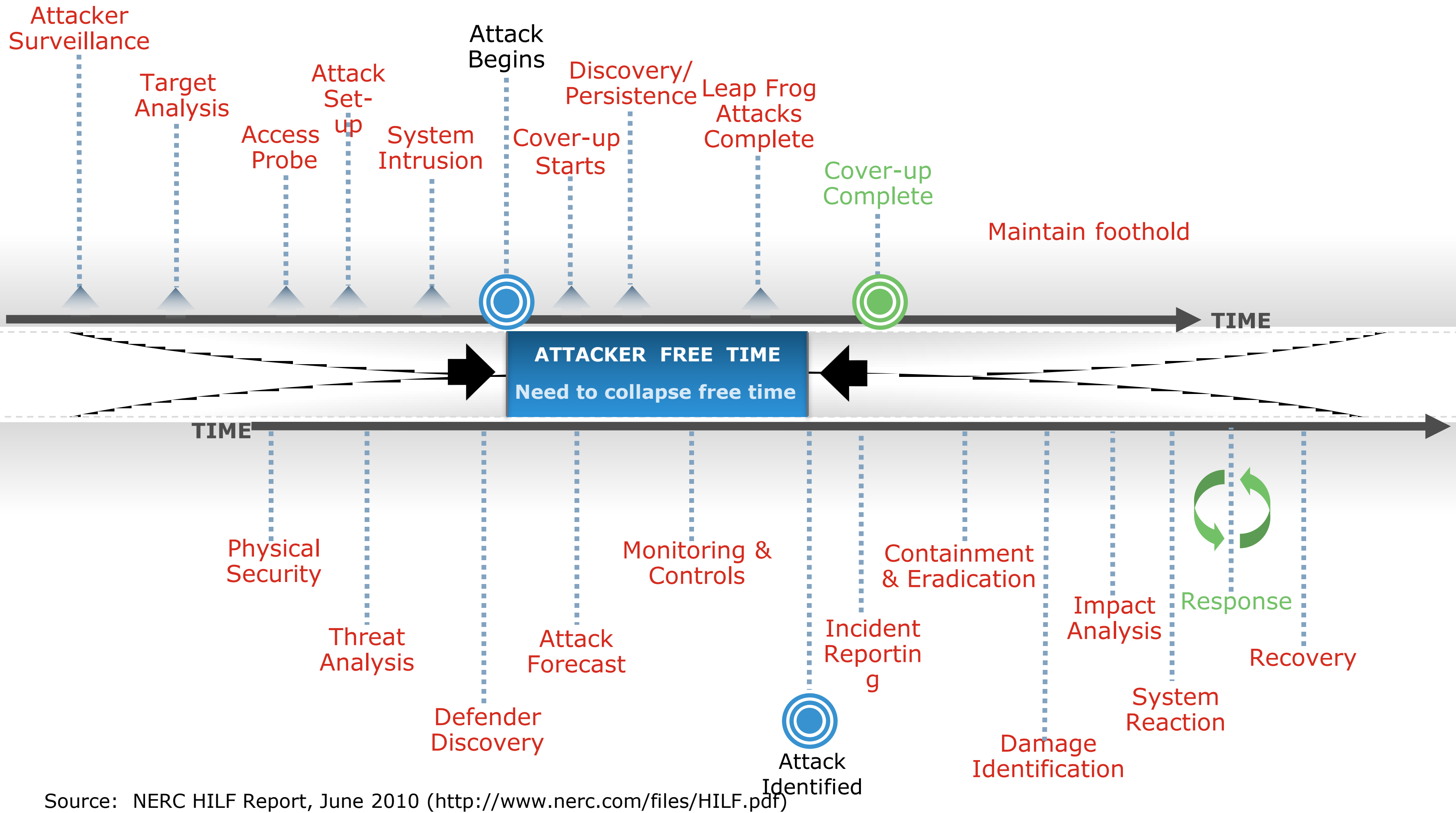


Intelligence-Driven Security

RSA

EMC²

Reducing Attacker Free Time



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

How do Advanced Threats impact the business?

The Aftermath of an Advanced Attack

- Hard costs hurt
  - Emergency cleanup costs
  - Regulatory penalties
  - Customer restitution
  - Business process re-engineering
- Soft costs really hurt
  - Missed opportunity due to cleanup focus
  - Loss of customer confidence
  - Decline in employee morale & goodwill

What is the approach for the future?

Today’s Security Requirements

Big Data Infrastructure

“Need a fast and scalable infrastructure to conduct short term and long term analysis”

Comprehensive Visibility

“See everything happening in my environment and normalize it”

High Powered Analytics

“Give me the speed and smarts to discover and investigate potential threats in near real time”

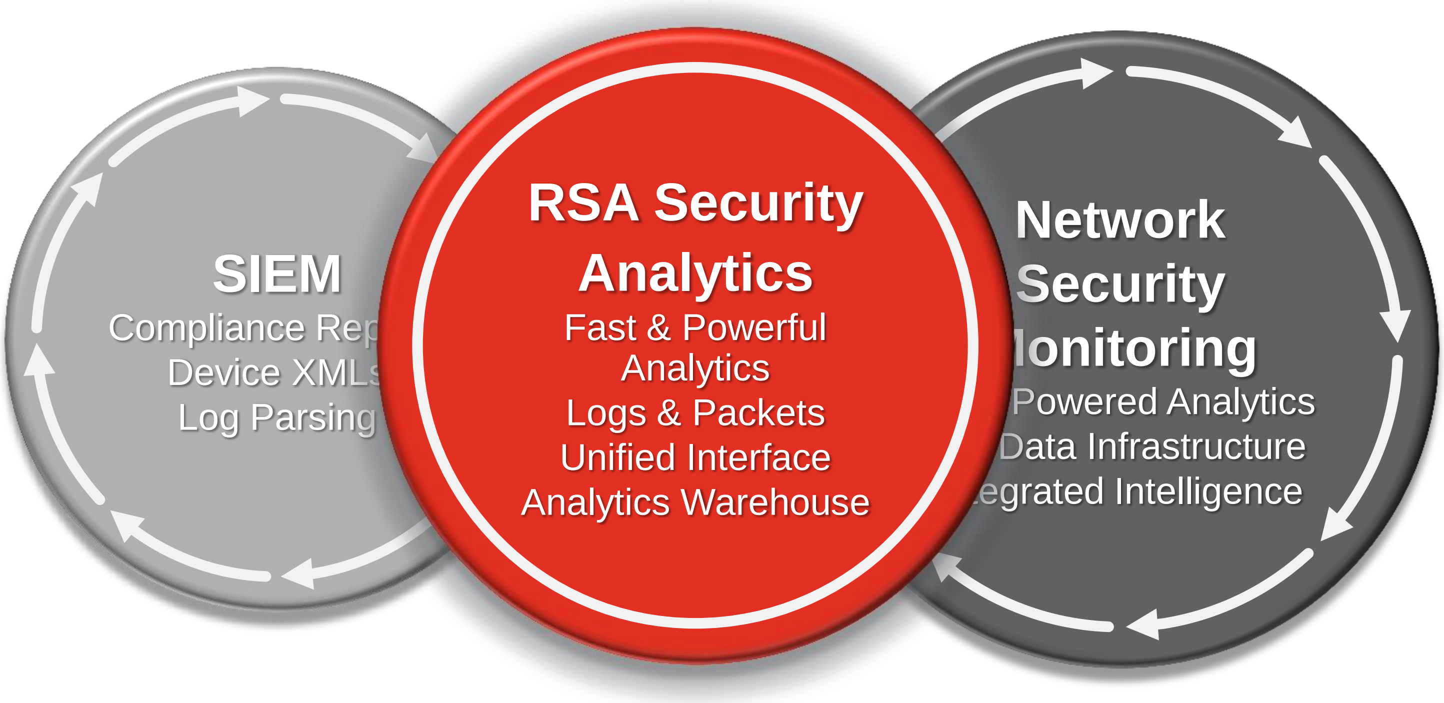
Integrated Intelligence

“Help me understand what to look for and what others have discovered”

RSA EMC²

RSA Security Analytics: Changing The Security Management Status Quo

Unified platform for security monitoring, incident investigations and compliance reporting



SIEM

Compliance Rep
Device XMLs
Log Parsing

RSA Security Analytics

Fast & Powerful Analytics
Logs & Packets
Unified Interface
Analytics Warehouse

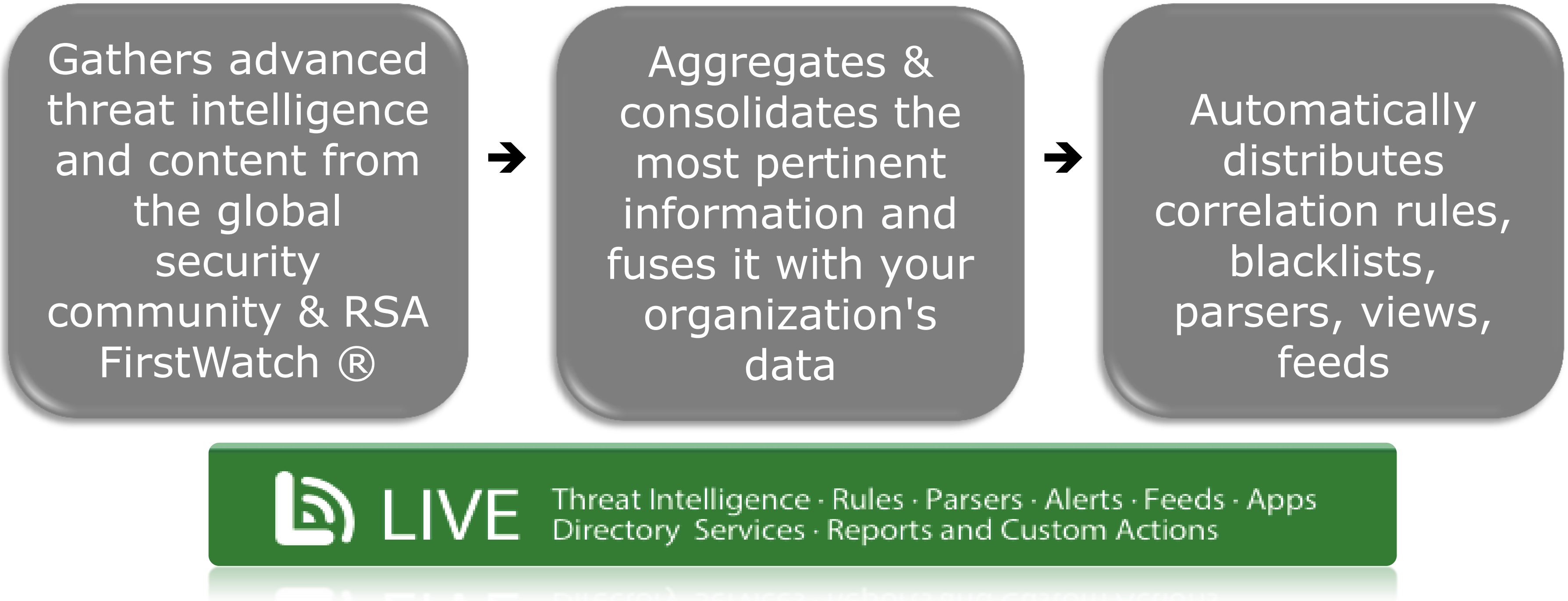
Network Security lonitoring

Powered Analytics
Data Infrastructure
egrated Intelligence

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

RSA Live Integrated Intelligence

How Do I Know What To Look For?



Gathers advanced threat intelligence and content from the global security community & RSA FirstWatch ® →

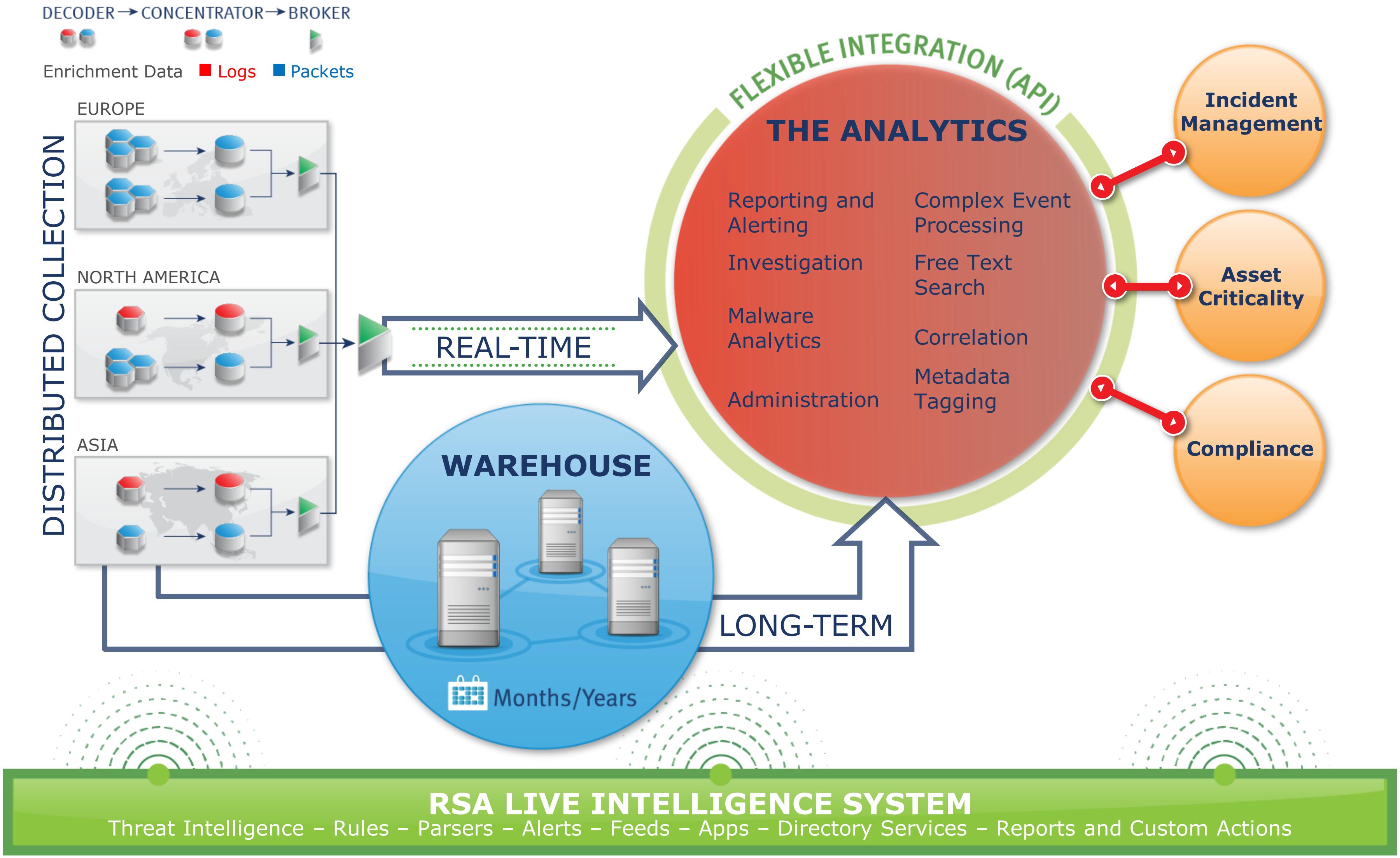
Aggregates & consolidates the most pertinent information and fuses it with your organization's data →

Automatically distributes correlation rules, blacklists, parsers, views, feeds

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

Operationalize Intelligence: Take advantage of what others have already found and apply against your current and historical data

Security Analytics Architecture



RSA®

EMC^2®