RSA ECAT

Detecting Advanced Threats on Endpoints Faster than Ever Before

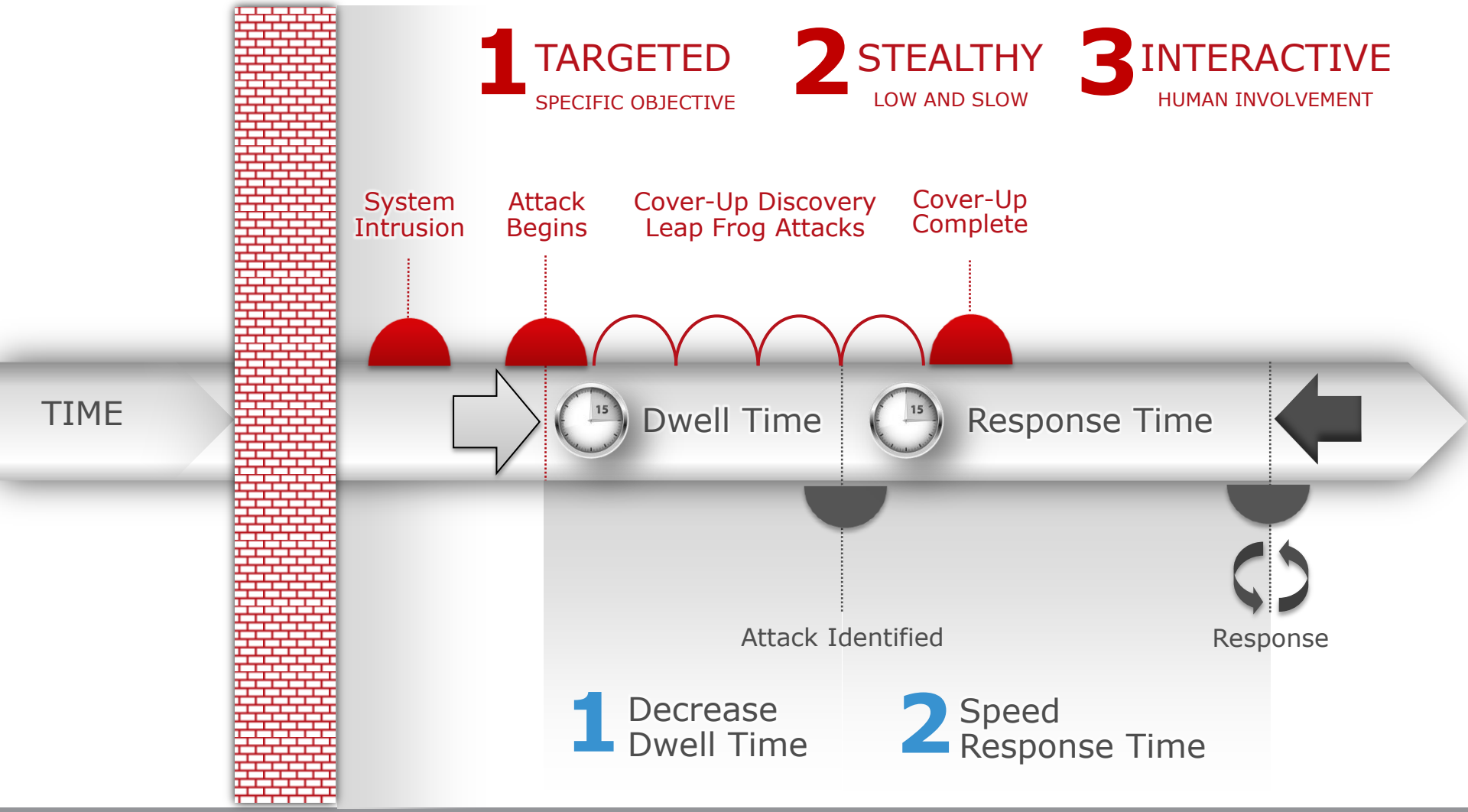
April 25, 2013

Chad Loeven, Sr. Product Manager
Meghan Risica, Sr. Product Marketing Manager
Mike Zeberlein, Principal Practice Consultant

Agenda

- Today's threat landscape
- What is RSA ECAT and how does it detect advanced threats?
- RSA ECAT in action

Advanced Threats Are Different



Enterprise Security Today

Workstations
Antivirus

AV and other signature-based solutions have been rendered ineffective by targeted attacks

Perimeter security
Firewall, Anti-spam, Gateway A/V, IDS, SIEM, Network security monitoring

- Inline devices can't identify what happened on the host in a compromise

- Bluetooth and WiFi can bypass in-line devices

Internet

Recent Targeted Campaign: VOHO

- What is VOHO?
  - APT campaign in 2012
  - Identified by RSA FirstWatch team
  - Attack method = Water Holing

1,000 unique organizations

35,000 unique hosts

12% rate of compromise

How do you better detect advanced threats like this?

What is RSA ECAT?

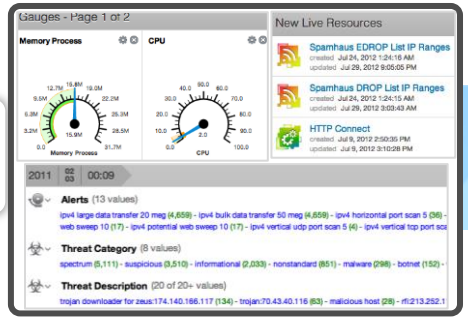
RSA ECAT

- ECAT= **E**nterprise **C**ompromise **A**ssessment **T**ool
- Detect, Analyze & Respond to advanced malware on endpoints

- Signature-less malware detection
- In-depth endpoint visibility
- Gain actionable intelligence for rapid breach detection
- Increase SOC Efficiency

ECAT for Incident Response

RSA Security Analytics



1

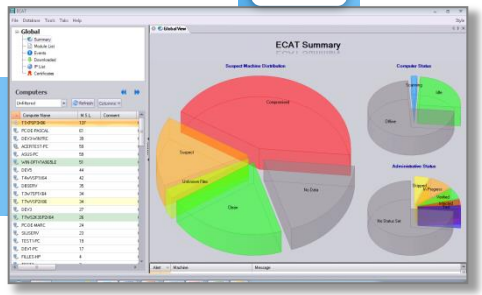
Deploy and Scan
RSA ECAT agent deployed to machine to conduct in-depth scan

2

Alert about suspicious network traffic
- Beaconing, connection to known bad IP address, etc.

Assess & Investigate
Analyst assesses results in ECAT console to determine if the machine is infected

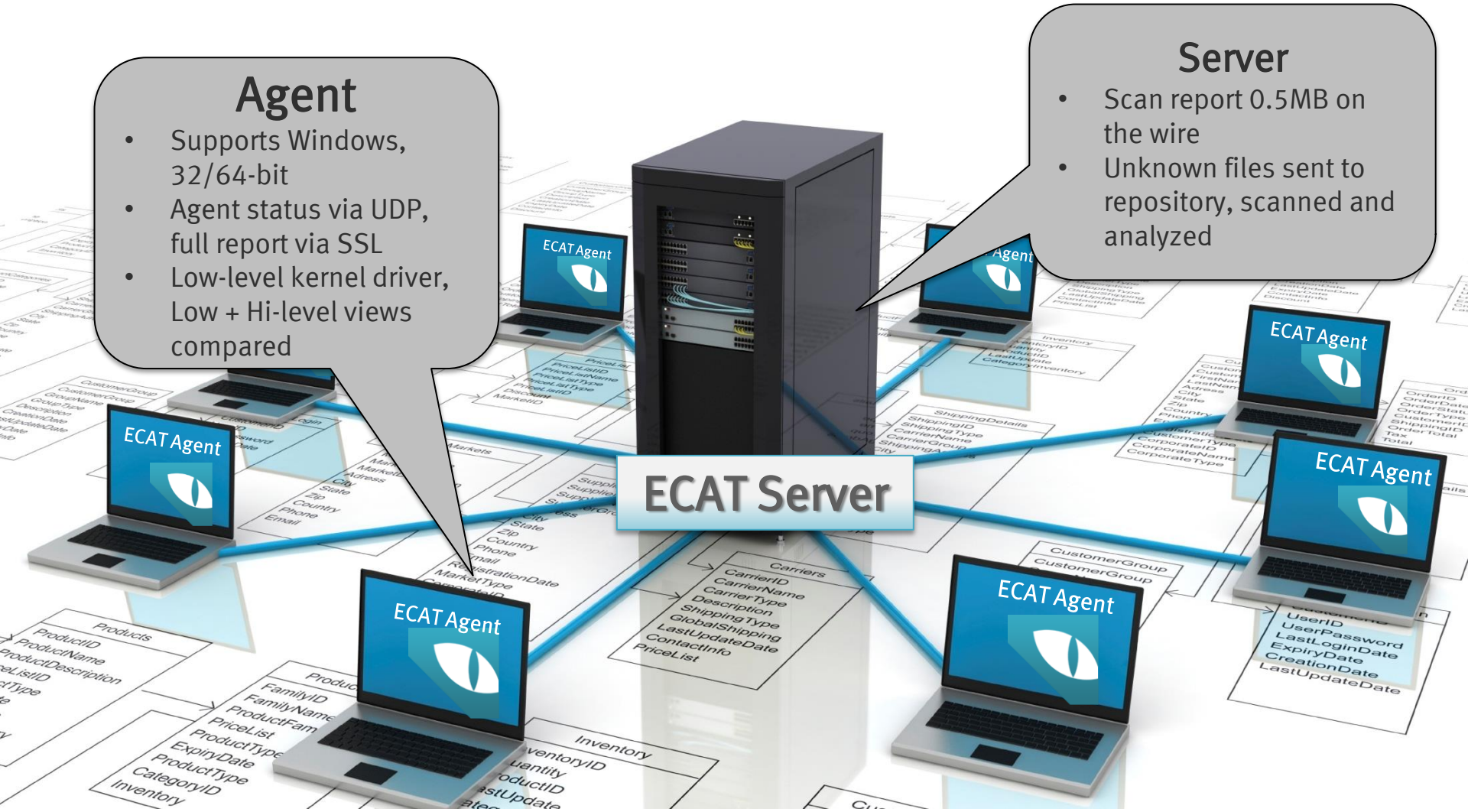
3



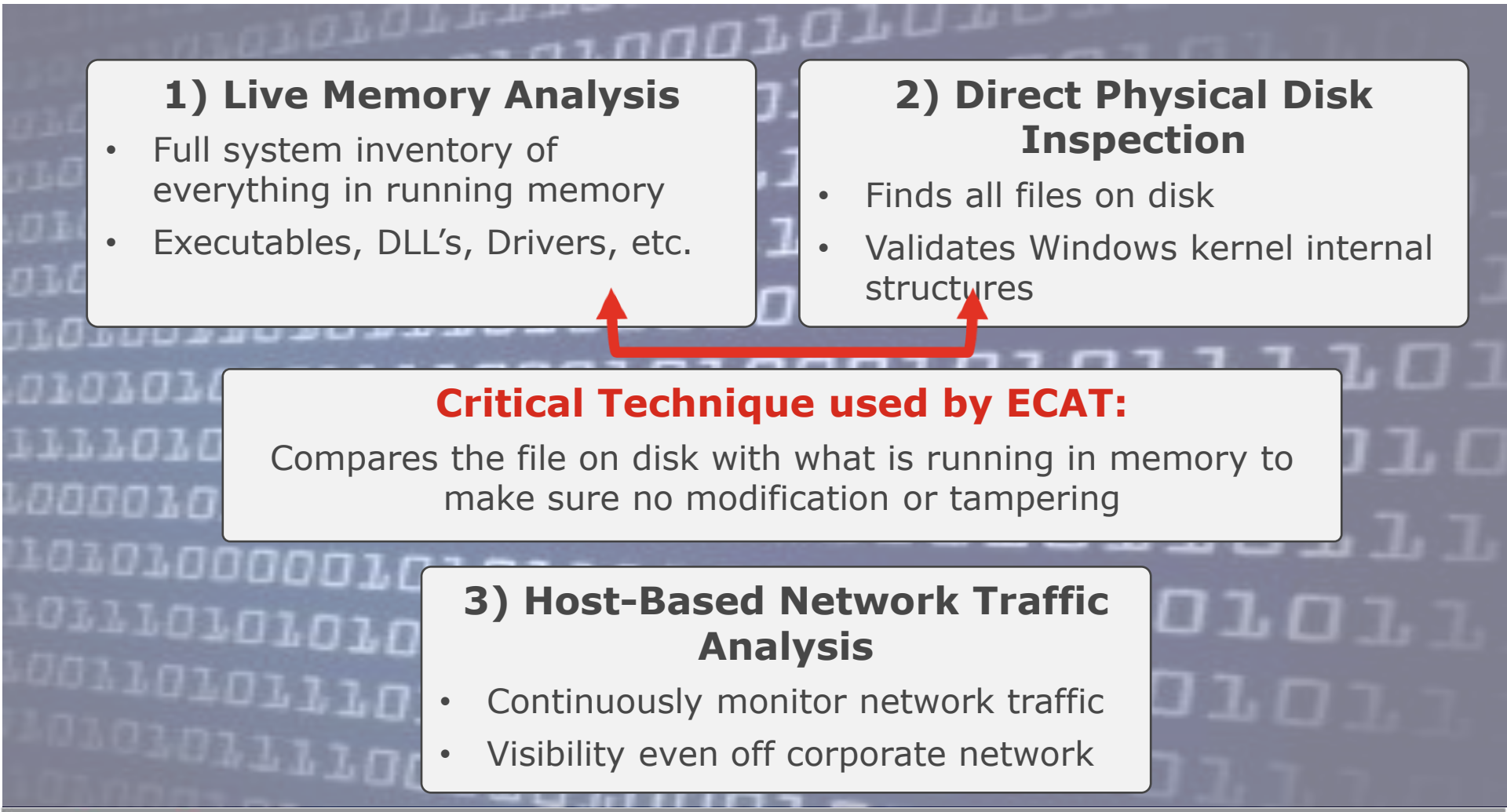
4

Remediation
Reimage machine or use Hitman Pro agent (3rd party) to clean

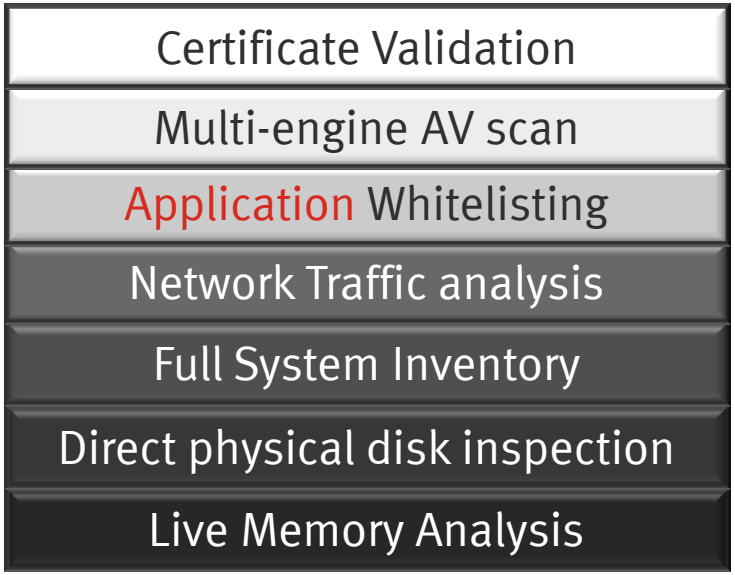
How RSA ECAT Works



RSA ECAT Scan Techniques



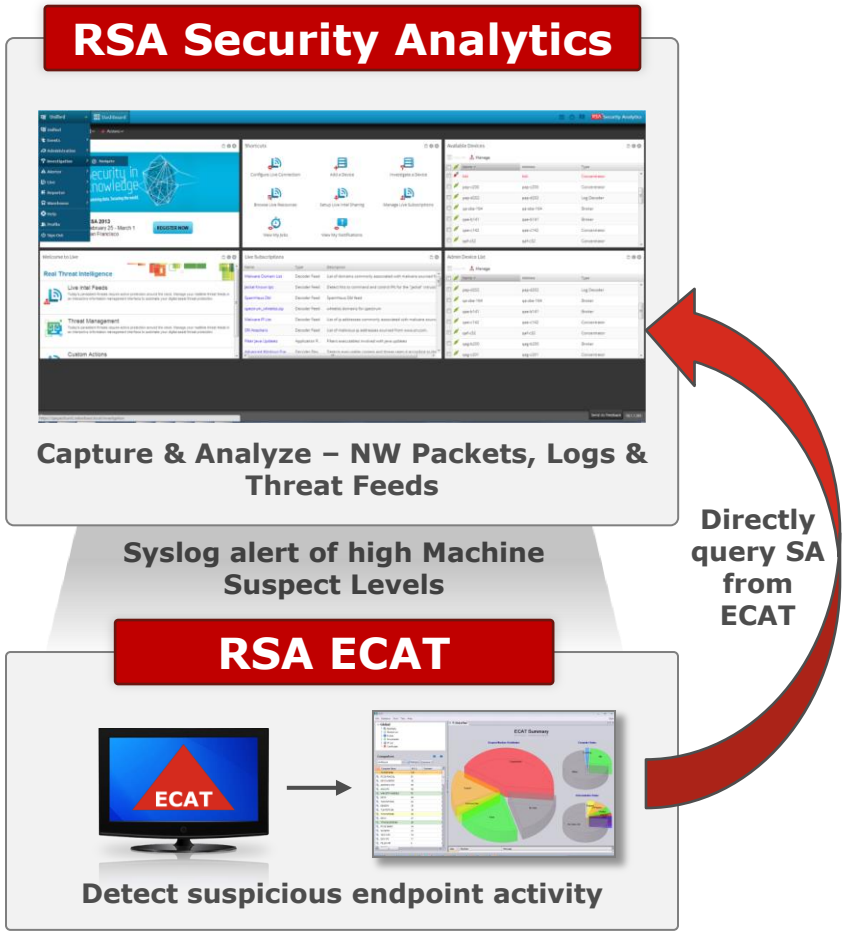
RSA ECAT: Key Functionality



Benefits

- X-ray view of what's happening on hosts
- Identify behavior related to malware
- Highlight likely infections with Machine Suspect Level (MSL)
- Quickly filter through results to gain actionable intelligence
- Triage & find other infected machines
- Remediation & Forensics capabilities

RSA ECAT & RSA Security Analytics



- Detect and Respond to Advanced Threats
- Complete network and host visibility
- Faster investigations to shorten attacker dwell time

RSA ECAT in Action


RSA


EMC²