



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

1 TARGETED
SPECIFIC OBJECTIVE

2 STEALTHY
LOW AND SLOW

3 INTERACTIVE
HUMAN INVOLVEMENT

System
Intrusion

Attack
Begins

Cover-Up Discovery
Leap Frog Attacks

Cover-Up
Complete

TIME



Dwell Time



Response Time



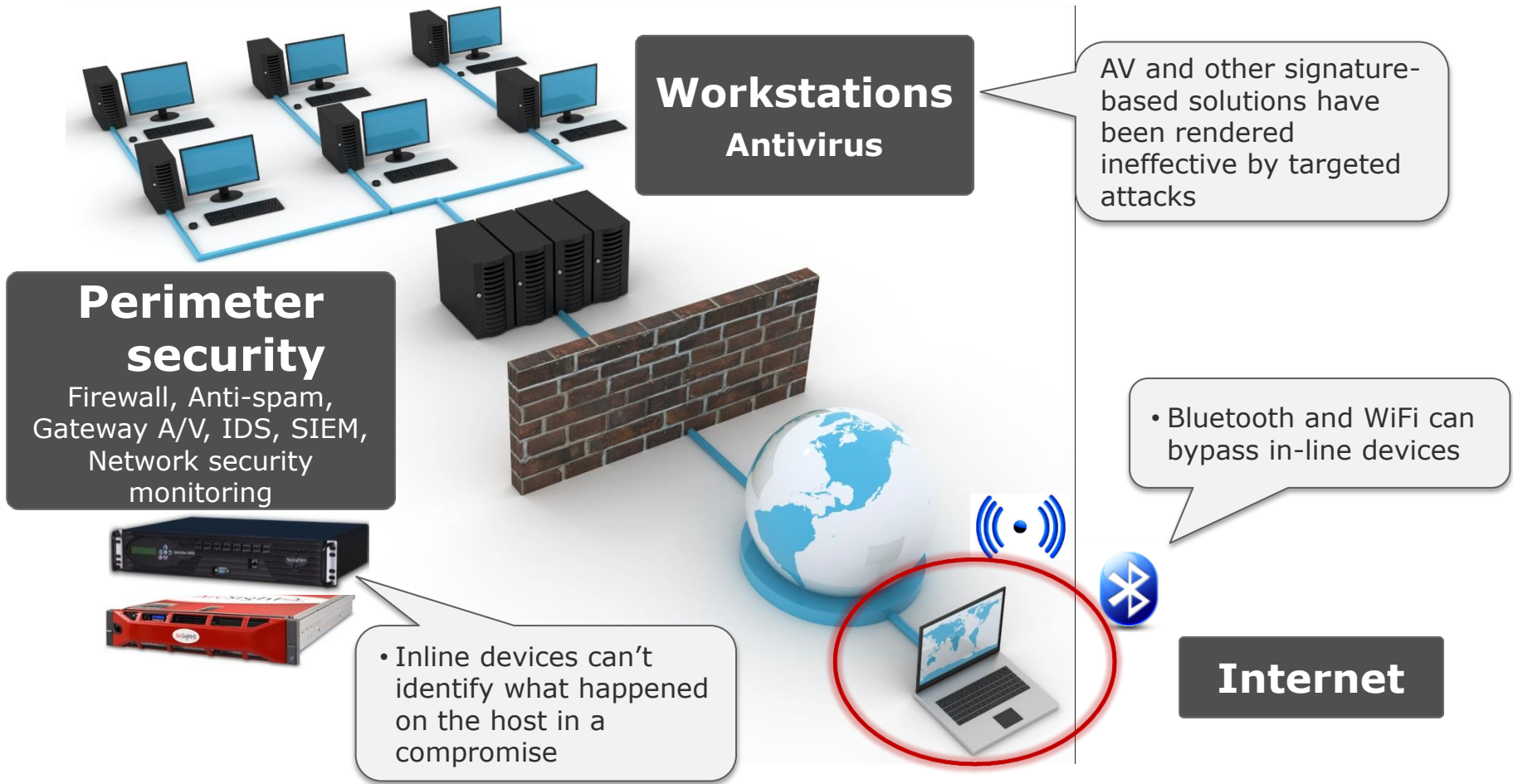
Attack Identified



1 Decrease
Dwell Time

2 Speed
Response Time

Enterprise Security Today



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?

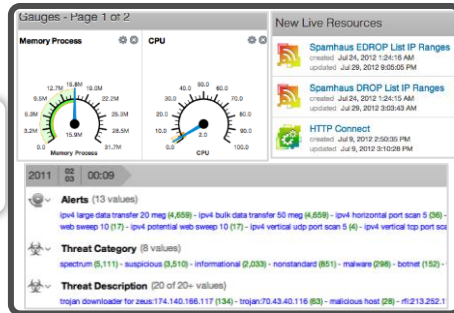
What is RSA ECAT?

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

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

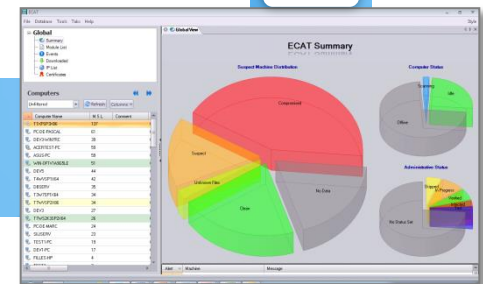
Deploy and Scan
RSA ECAT agent deployed to machine to conduct in-depth scan



2

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

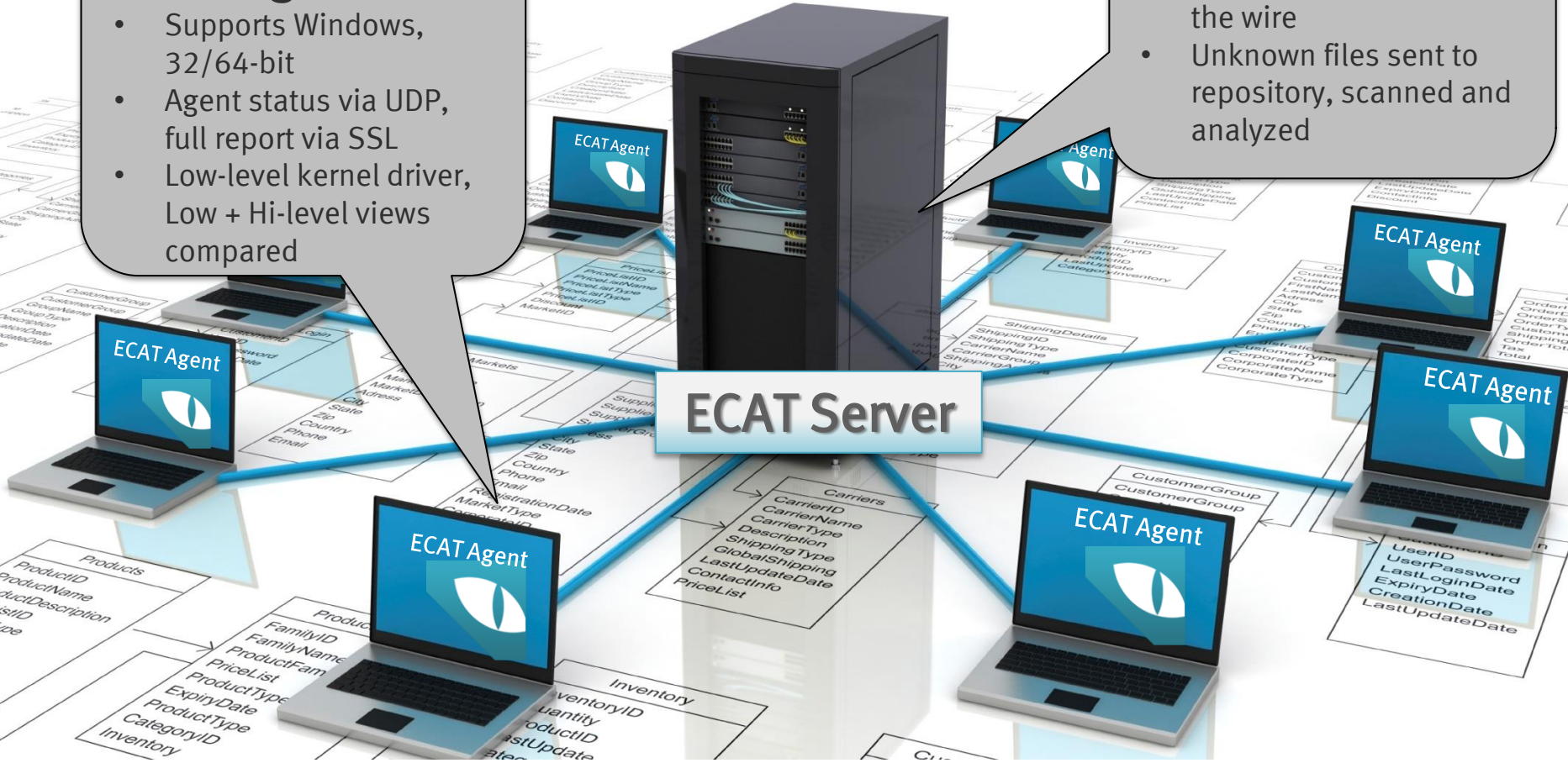
Agent

- Supports Windows, 32/64-bit
- Agent status via UDP, full report via SSL
- Low-level kernel driver, Low + Hi-level views compared

Server

- Scan report 0.5MB on the wire
- Unknown files sent to repository, scanned and analyzed

ECAT Server



RSA ECAT Scan Techniques

1) Live Memory Analysis

- Full system inventory of everything in running memory
- Executables, DLL's, Drivers, etc.

2) Direct Physical Disk Inspection

- Finds all files on disk
- Validates Windows kernel internal structures

Critical Technique used by ECAT:

Compares the file on disk with what is running in memory to make sure no modification or tampering

3) Host-Based Network Traffic Analysis

- Continuously monitor network traffic
- Visibility even off corporate network

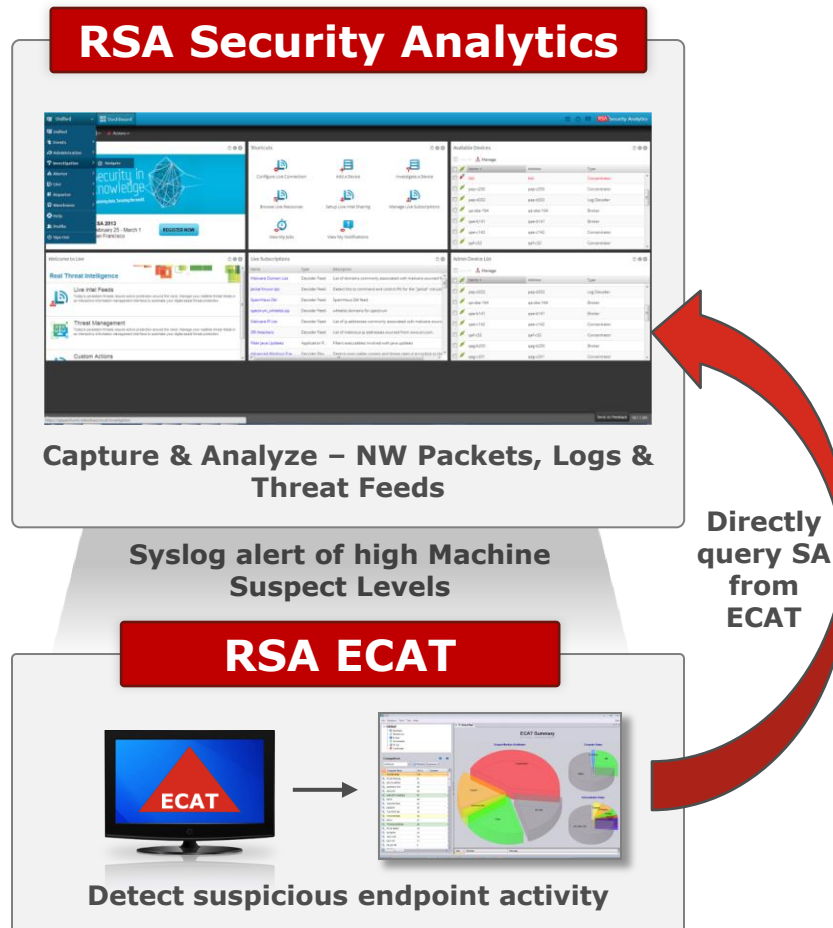
RSA ECAT: Key Functionality

Certificate Validation
Multi-engine AV scan
Application Whitelisting
Network Traffic analysis
Full System Inventory
Direct physical disk inspection
Live Memory Analysis

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[®]