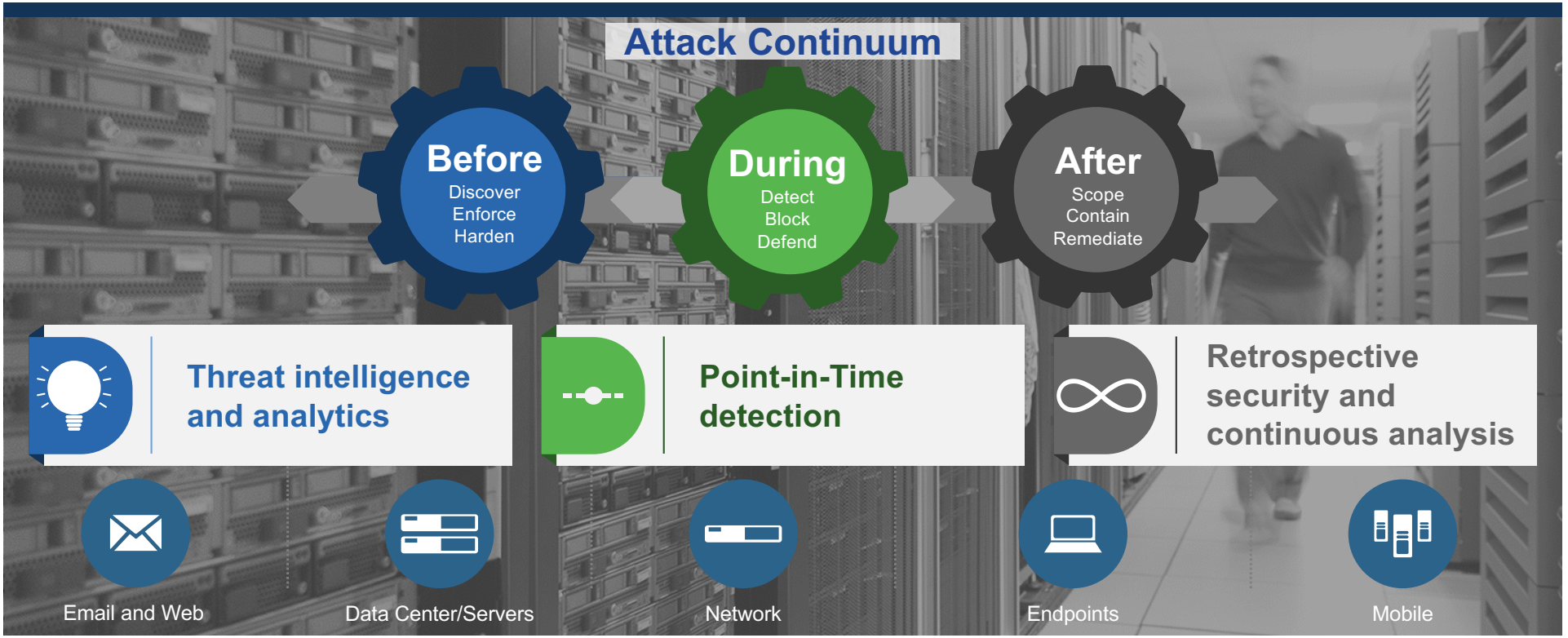
Cisco Security

Advanced Malware Protection

Guillermo González
Security Systems Engineer
Octubre 2017

The New Security Model



Gain security backed by the most advanced threat intelligence

Cisco Advanced Malware Protection
Built on Unmatched Collective Security Intelligence

Cisco® Collective Security Intelligence

1001 1101 1110011 0110011 101000 0110 00 1001 1101 1110011 0110011
101000 0110 00 0111000 111010011 101 1100001 110 101000 0110 00
00001110001110 1001 1101 1110011 0110011 101000 0110 00 1100001110001110

AMP Threat Intelligence Cloud

Automatic Updates in real time

Email
- 1.6 million global sensors
- 100 TB of data received per day
- 150 million+ deployed endpoints
- Team of engineers, technicians, and researchers
- 35% worldwide email traffic

Endpoints

Web
- 13 billion web requests
- 24x7x365 operations
- 4.3 billion web blocks per day
- 40+ languages
- 1.1 million incoming malware samples per day
- AMP Community
- Private/Public Threat Feeds

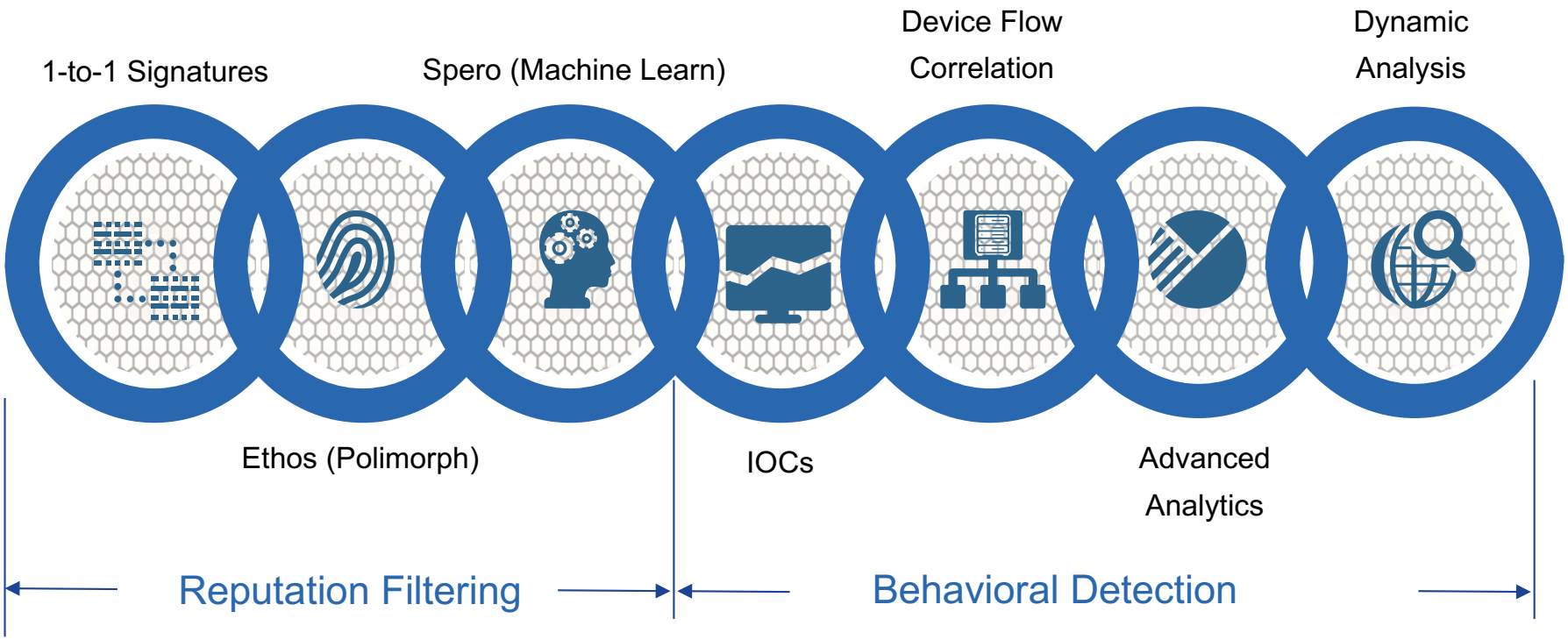
Networks

IPS
- Talos Security Intelligence
- AMP Threat Grid Intelligence
- AMP Threat Grid Dynamic Analysis 10 million files/month
- Advanced Microsoft and Industry Disclosures
- Snort and ClamAV Open Source Communities
- AEGIS Program

Devices

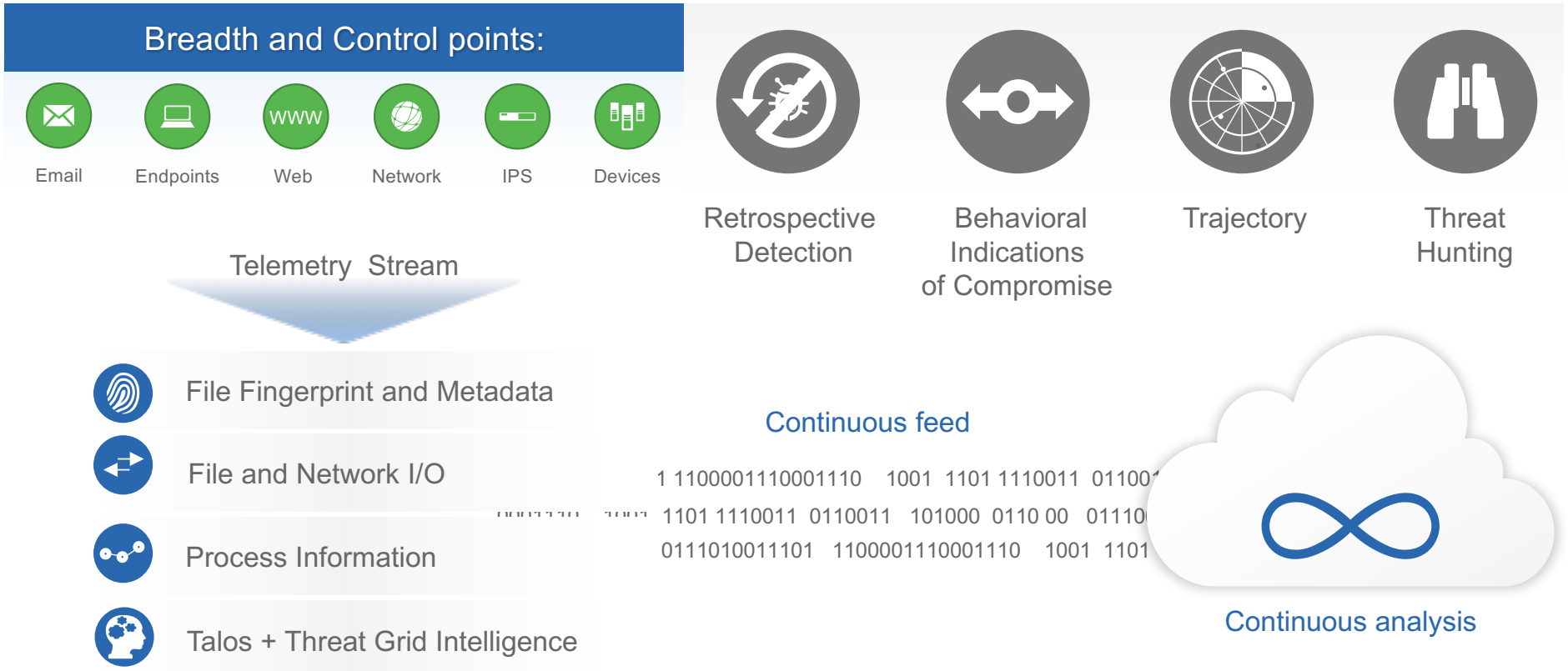
AMP
Advanced Malware Protection

AMP Plan A: The Prevention
AMP Plan B: Retrospective Security



All Methods < 100% Detection

Continuous Analysis and Retrospective Security



Cisco AMP

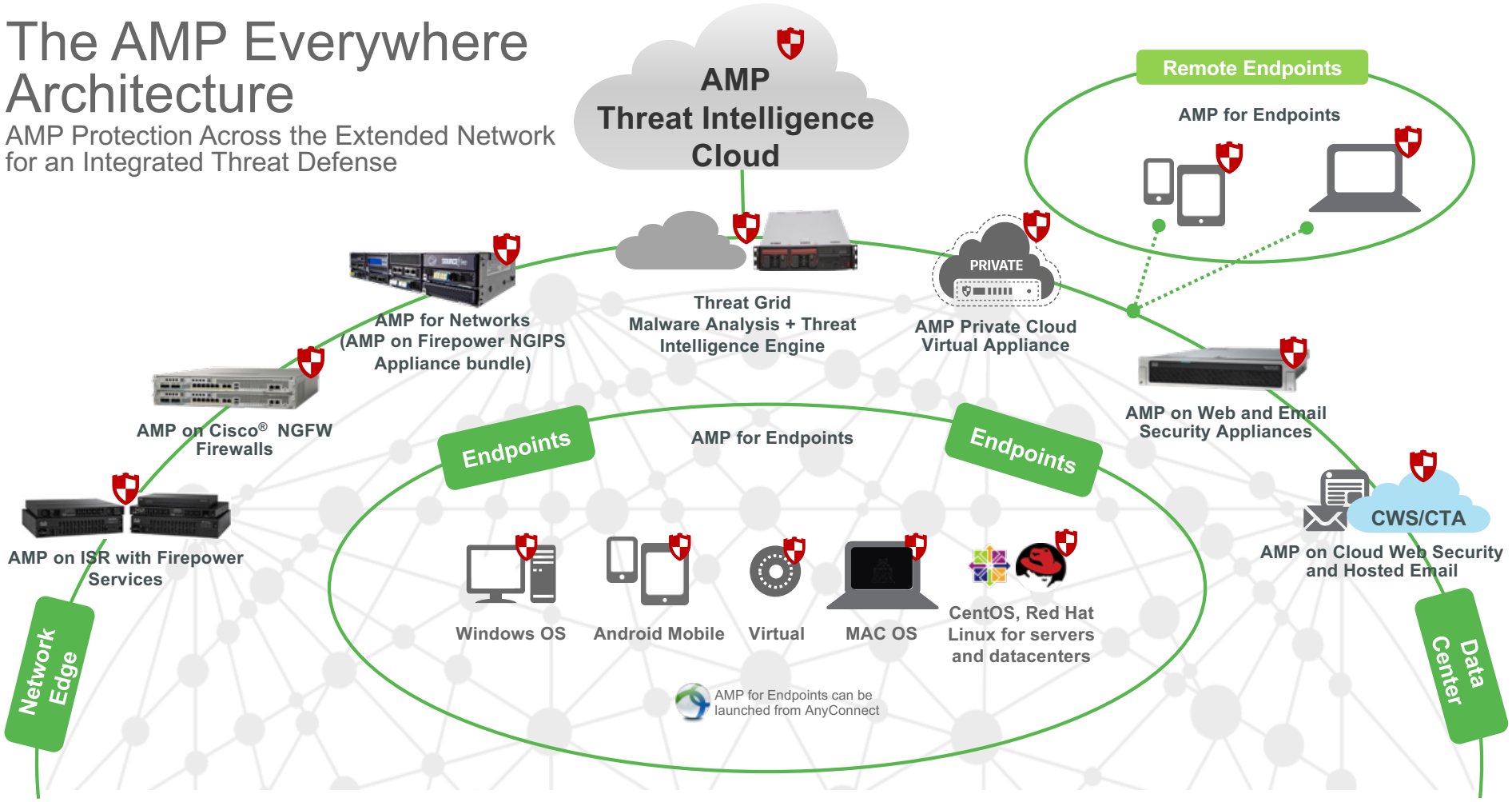
Cisco AMP gives you the answers for the most common questions after a Breach

Looks ACROSS the organization and answers:

- When did it happen?
- Where is patient 0?
- What systems were infected?
- What was the entry point?
- What else did it bring in?

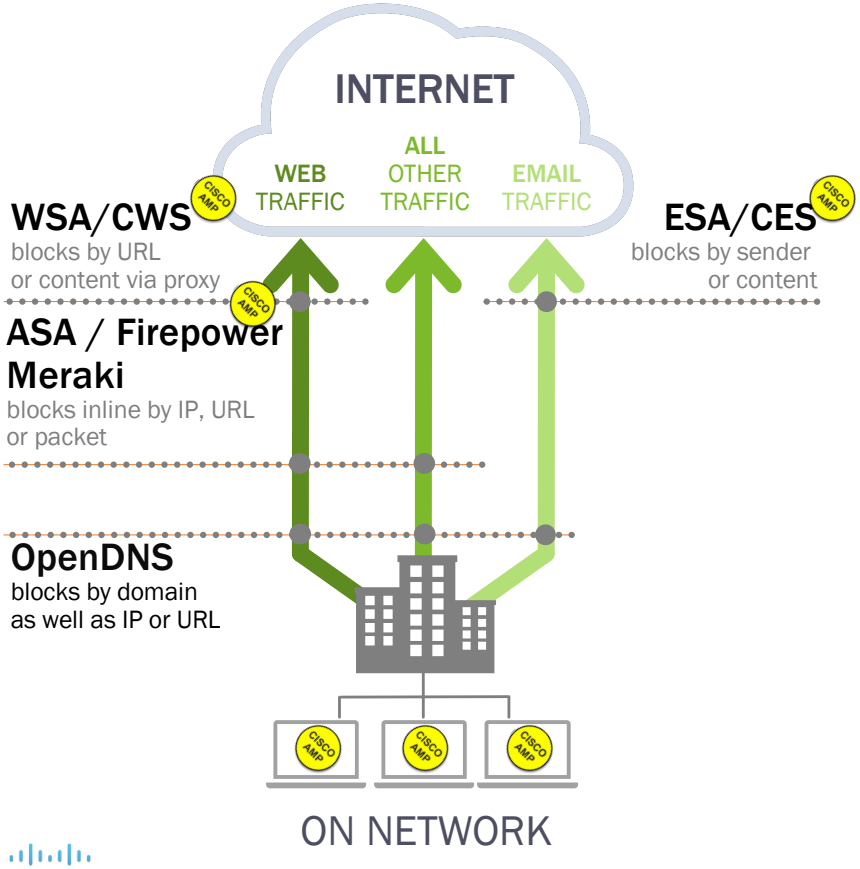
The AMP Everywhere Architecture

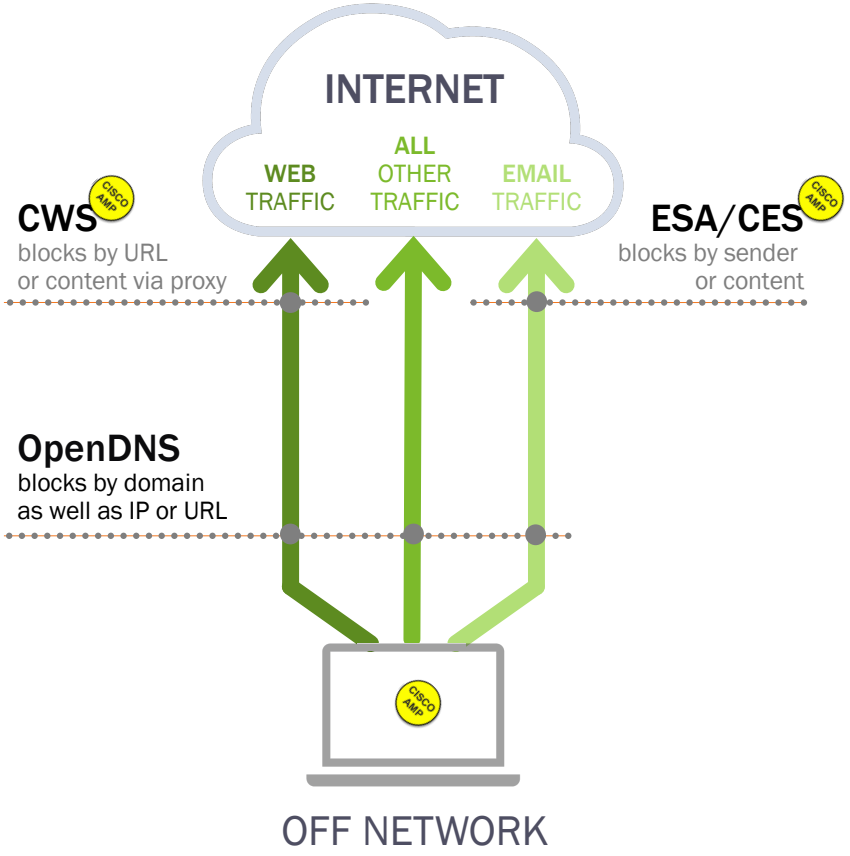
AMP Protection Across the Extended Network for an Integrated Threat Defense



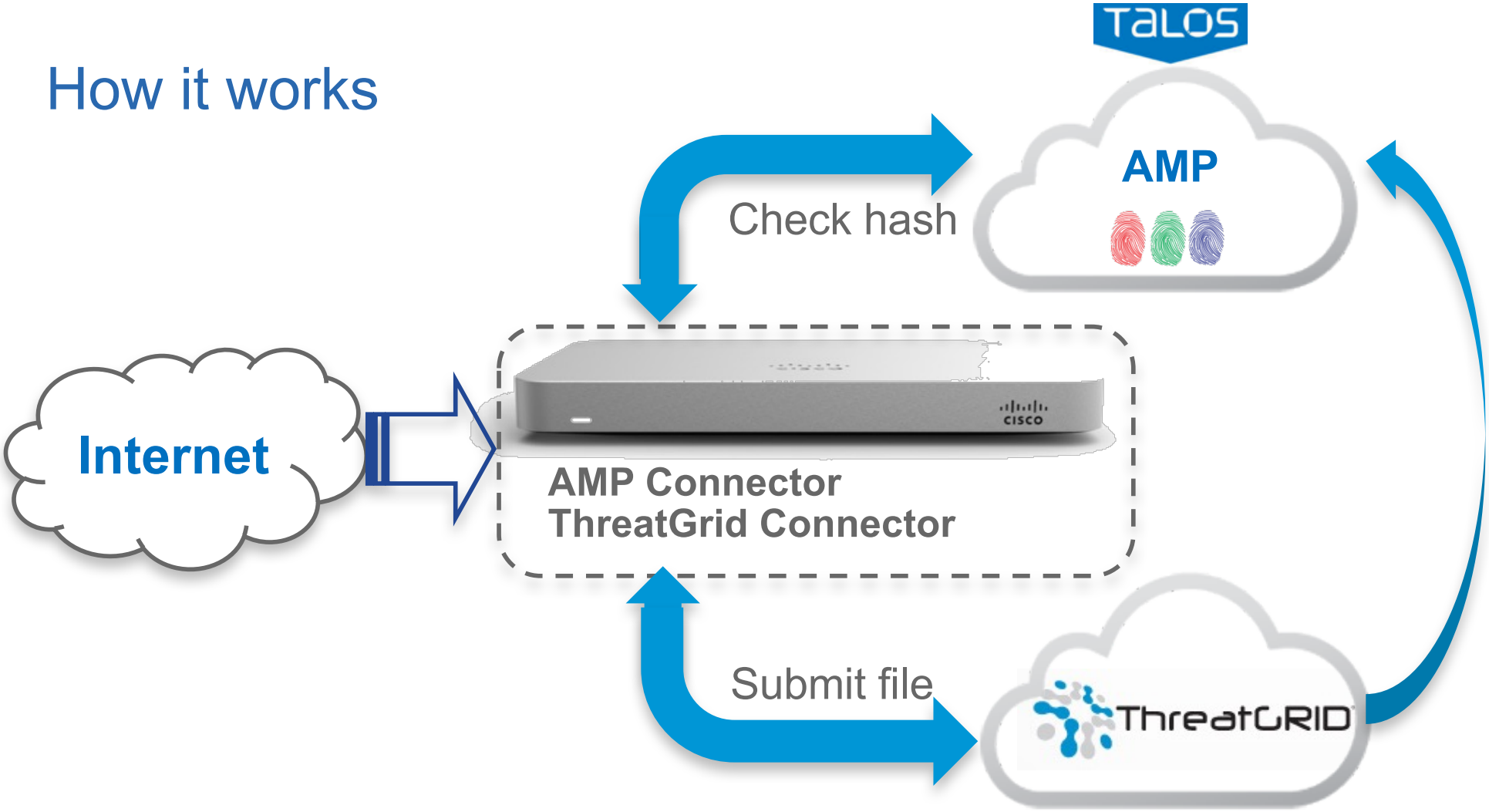
Cisco AMP

AMP Everywhere





How it works



Behavioral Indicators

Threat Score: 100

- **Locky Ransomware Detected** — Severity: 100 Confidence: 100
- **Ransomware Backup Deletion Detected** — Severity: 100 Confidence: 100
- **Shadow Copy Deletion Detected** — Severity: 100 Confidence: 100

Volume Shadow Copies are snapshots of portions of a file system used for backups
to remov
make rec
especiall
copies m

Categories weakening

Report Error

Advanced Malware Protection Verdict Updates

Printable PDF

Time Range: Week

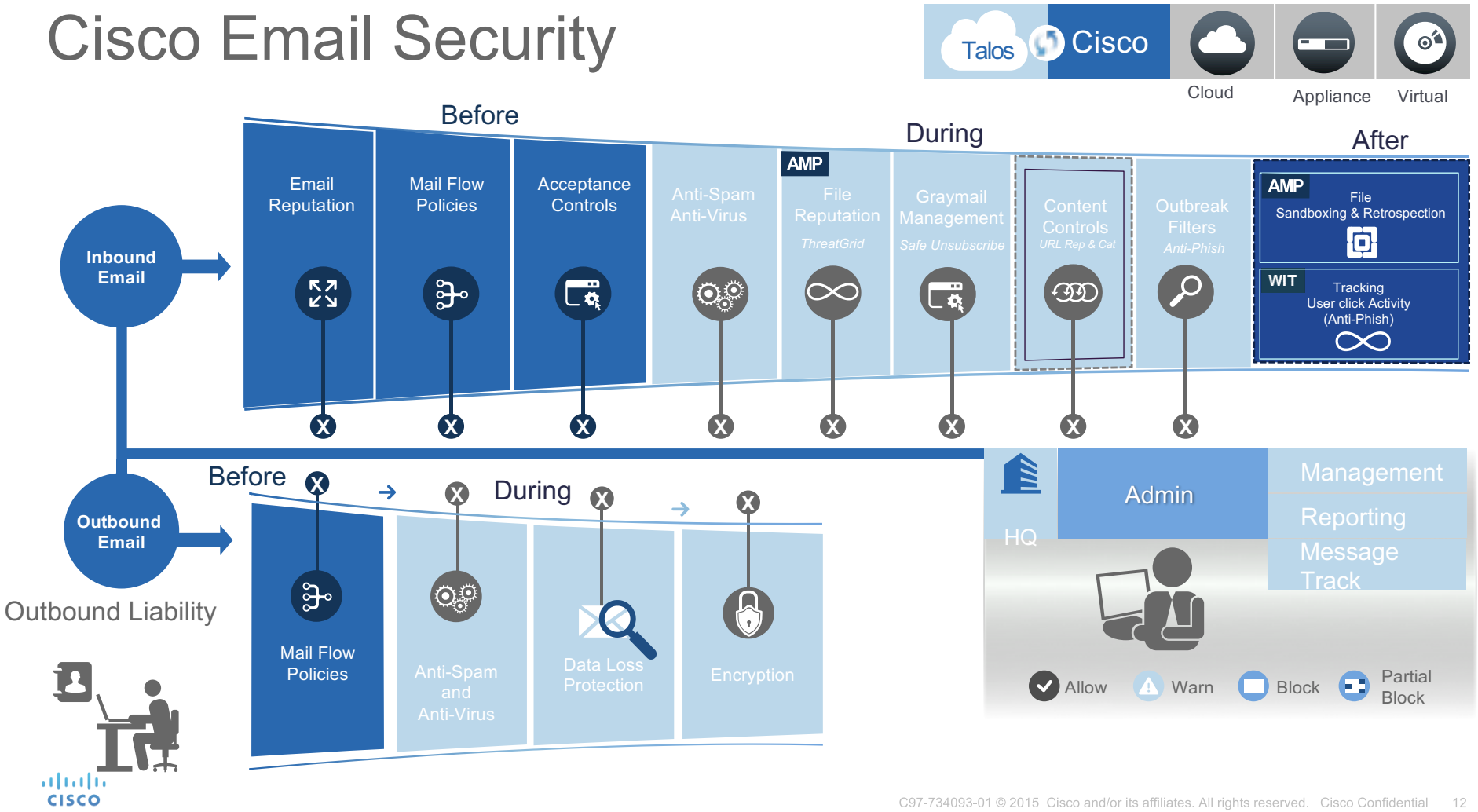
14 Aug 2015 00:00 to 21 Aug 2015 22:44 (GMT +02:00) — Data in time range: 15.84 % complete

Files with Retrospective Verdict Changes

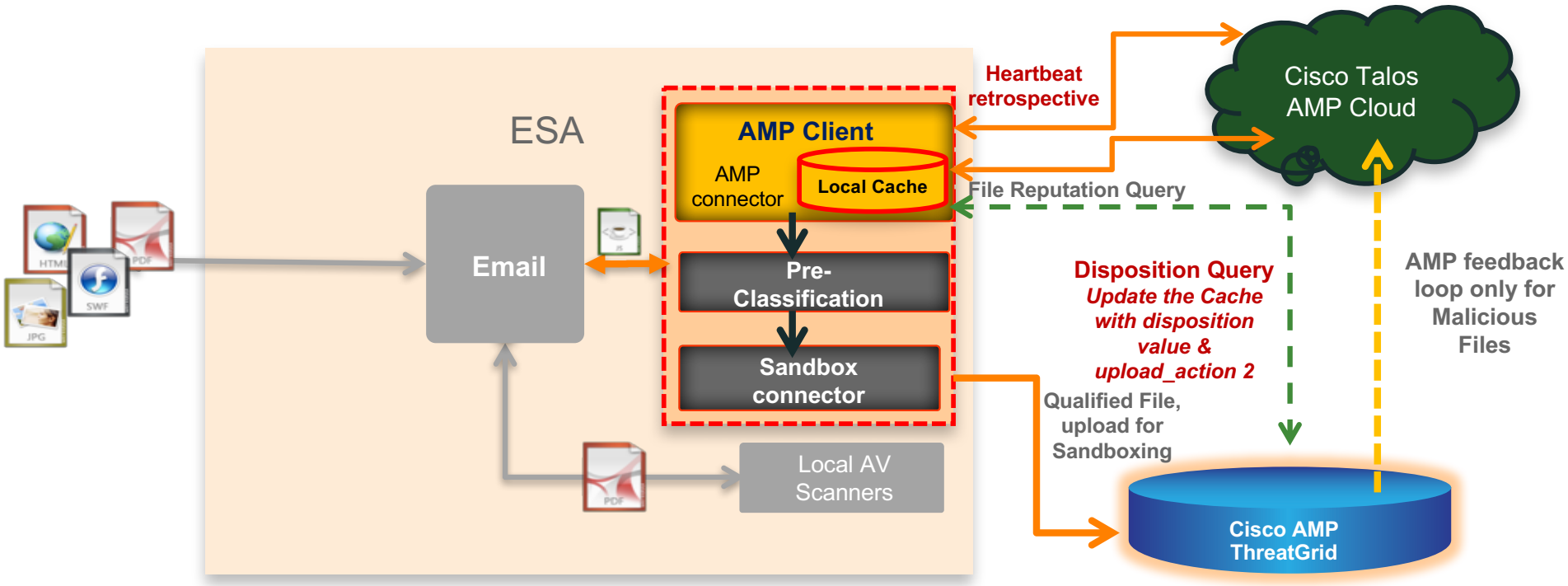
File SHA256	Time of Retrospective Verdict Change	Current Disposition
07e787ff...253caf5f	21 Aug 2015 21:39:39	malicious
ea84f794...41387831	21 Aug 2015 00:38:59	malicious
cf0d08e0...59d05a4b	21 Aug 2015 00:38:59	malicious
0189760b...93d971d3	21 Aug 2015 00:38:59	malicious
2bd015ae...f1ab9c30	20 Aug 2015 22:53:59	malicious

- **Windows Picture And Fax Viewer Used To Display Decoy Image** — Severity: 70 Confidence: 100
- **An HTTP Request Was Made to a Numeric IP Address** — Severity: 75 Confidence: 80
- **Process Modified File in a User Directory** — Severity: 70 Confidence: 80
- **Process Disabled Internet Explorer Proxy** — Severity: 70 Confidence: 70
- **Very Large Registry Data** — Severity: 50 Confidence: 80
- **Command Exe File Execution Detected** — Severity: 50 Confidence: 80
- **File Downloaded to Disk** — Severity: 30 Confidence: 90
- **Pending File Deletions** — Severity: 40 Confidence: 50
- **Hook Procedure Detected in Executable** — Severity: 35 Confidence: 40

Cisco Email Security

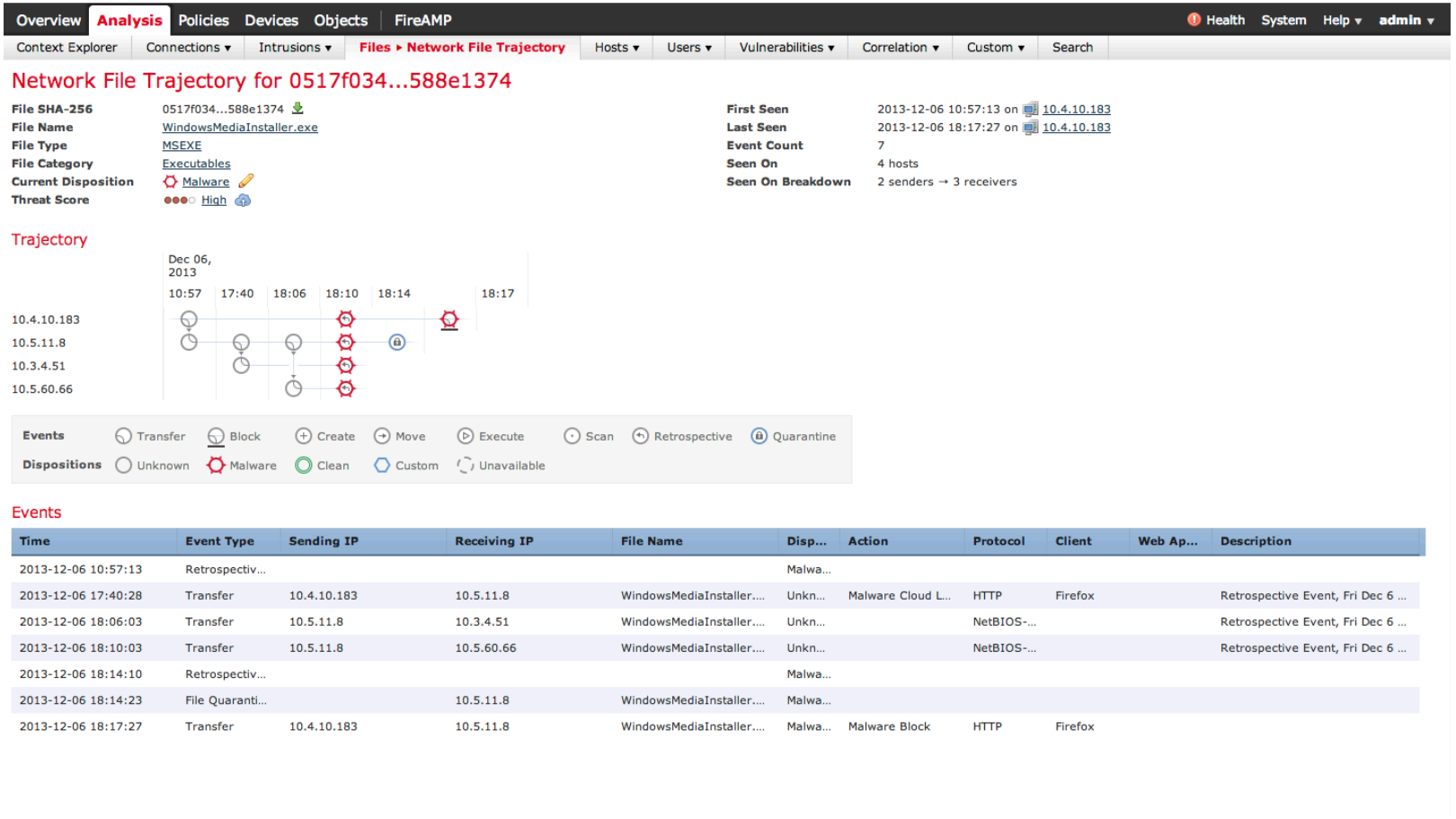


AMP with ThreatGrid



Starting with the 9.5 version of code, public cloud and local sandboxing is supported

Plan B: Security Retrospective
AMP for Networks



AMP Provides Contextual Awareness and Visibility

That Allows You to Take Control of an Attack Before It Causes Damage