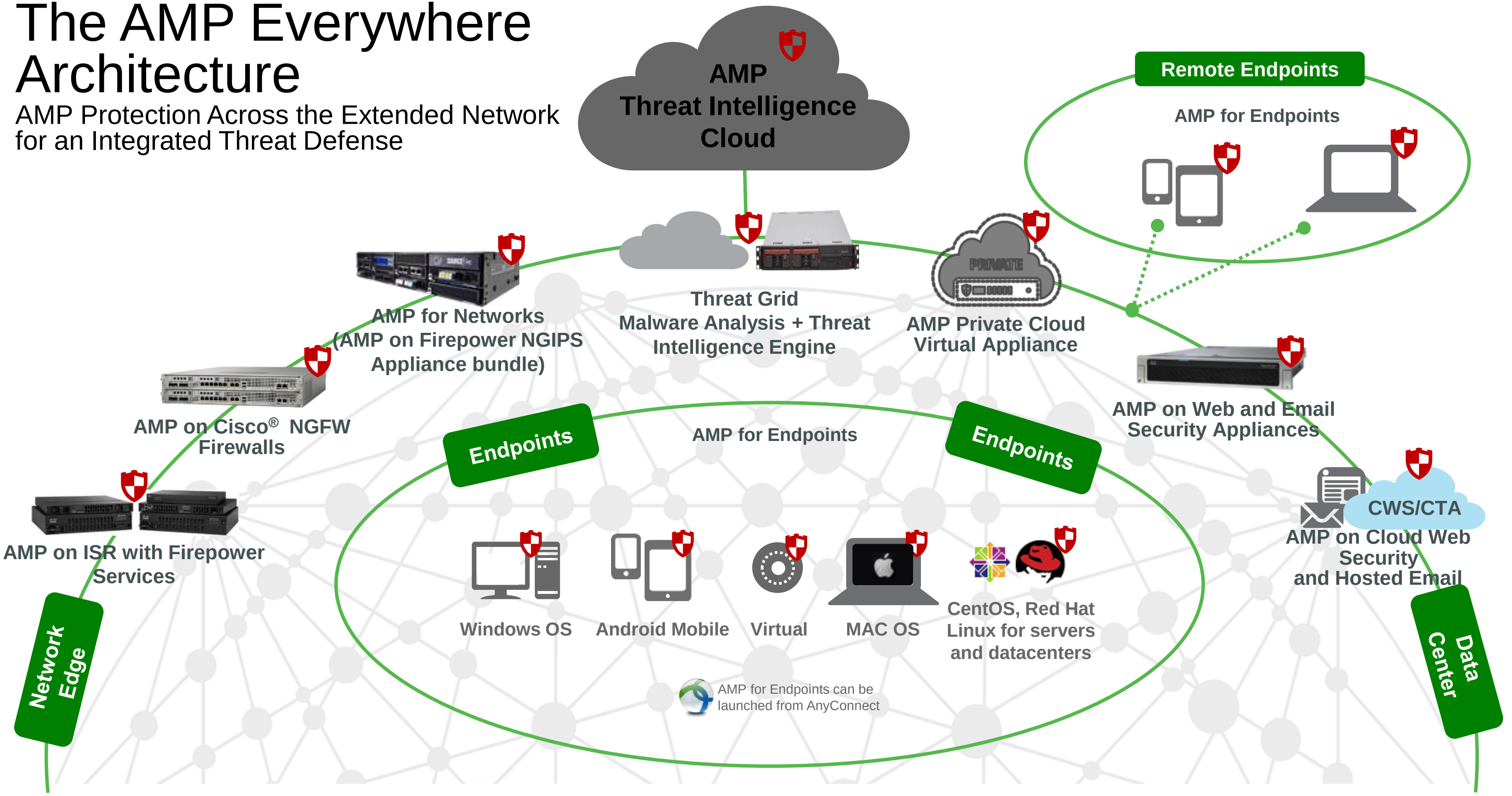
Cisco AMP Solution

Rene Straube
CSE, Cisco Germany
January 2017

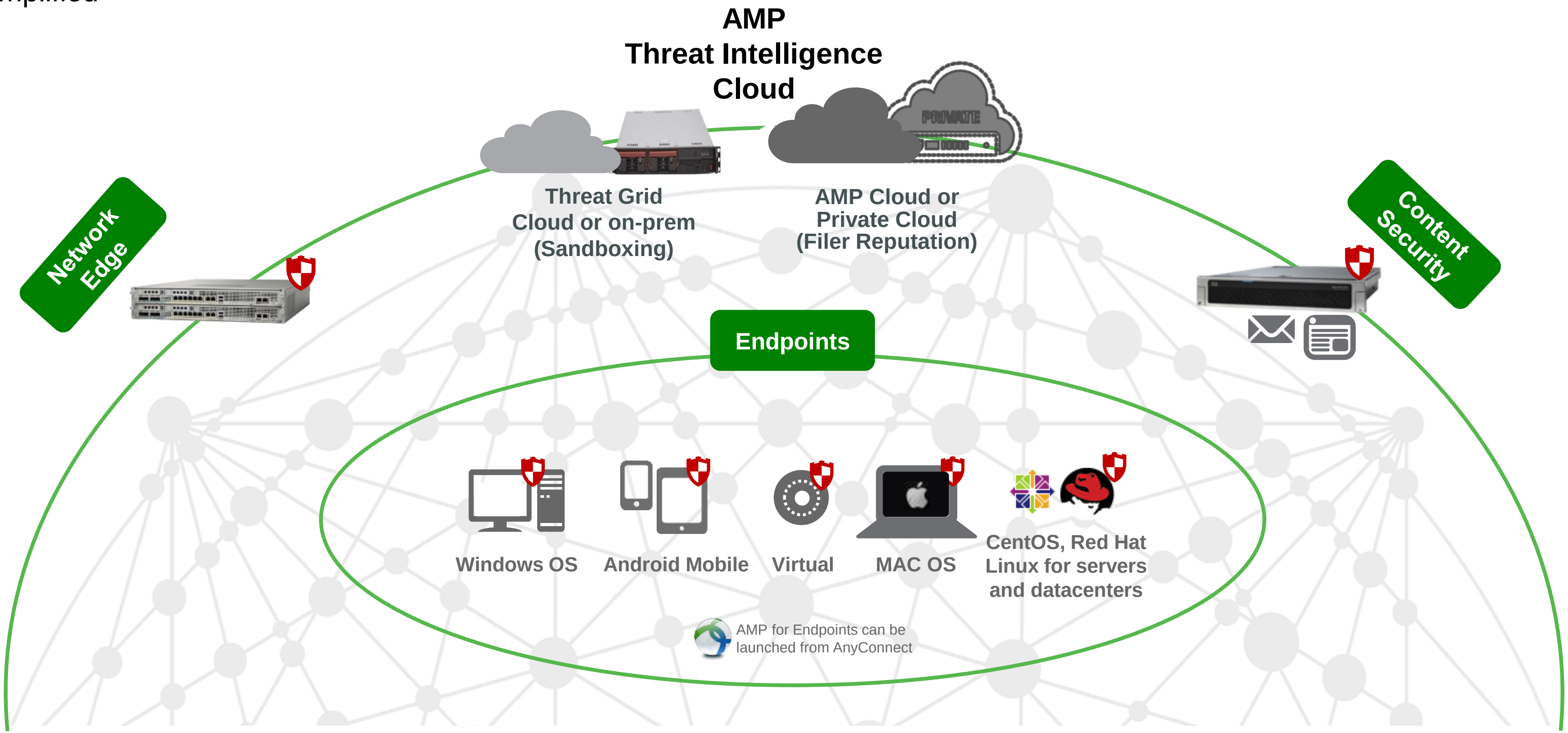
The AMP Everywhere Architecture

AMP Protection Across the Extended Network
for an Integrated Threat Defense



The AMP Everywhere Architecture

Simplified



How does Cisco‘s Adwanced Malware Protection (AMP) work?

Advanced Malware Protection

Summary

File Reputation

Preventative blocking of suspicious files

File Sandboxing

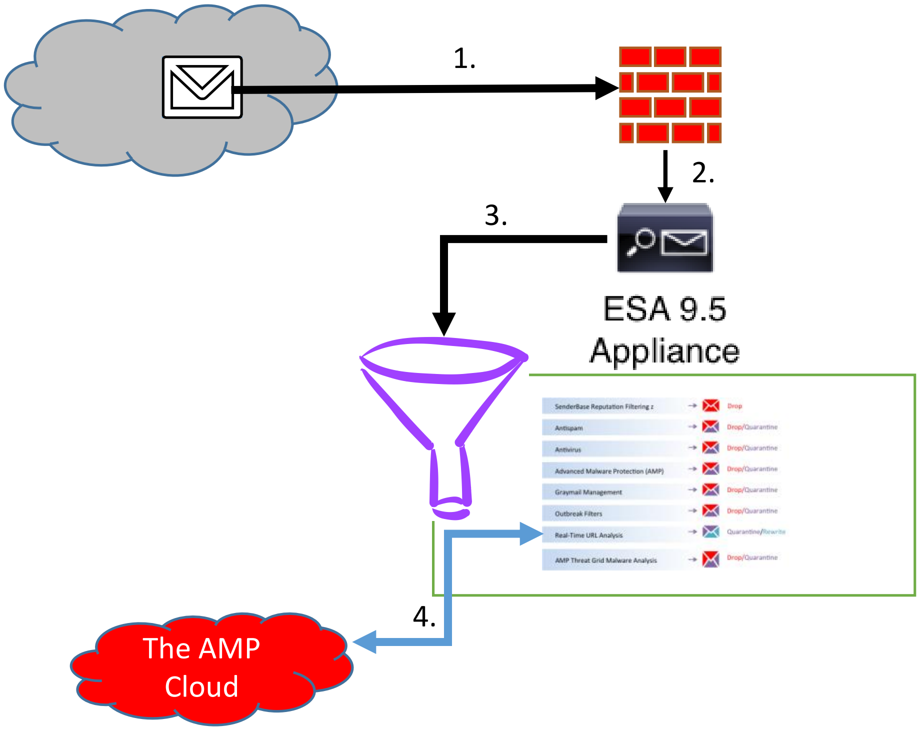
Behavioral analysis of unknown files

File Retrospection

Retrospective alerting after an attack

ESA – AMP Threat Grid Process Flow

Threat Grid in the Cloud



SenderBase Reputation Filtering z	→	Drop
Antispam	→	Drop/Quarantine
Antivirus	→	Drop/Quarantine
Advanced Malware Protection (AMP)	→	Drop/Quarantine
Graymail Management	→	Drop/Quarantine
Outbreak Filters	→	Drop/Quarantine
Real-Time URL Analysis	→	Quarantine/Rewrite
AMP Threat Grid Malware Analysis	→	Drop/Quarantine

1. Email sent from Internet
2. Accepted by ESA Appliance
3. Email passed through security stack on ESA
4. Threat intelligence from AMP Cloud used to determine if email or attachments match malicious indicators (SHA Lookup)

Advanced Malware Protection

Summary

File Reputation

Preventative blocking of suspicious files

File Sandboxing

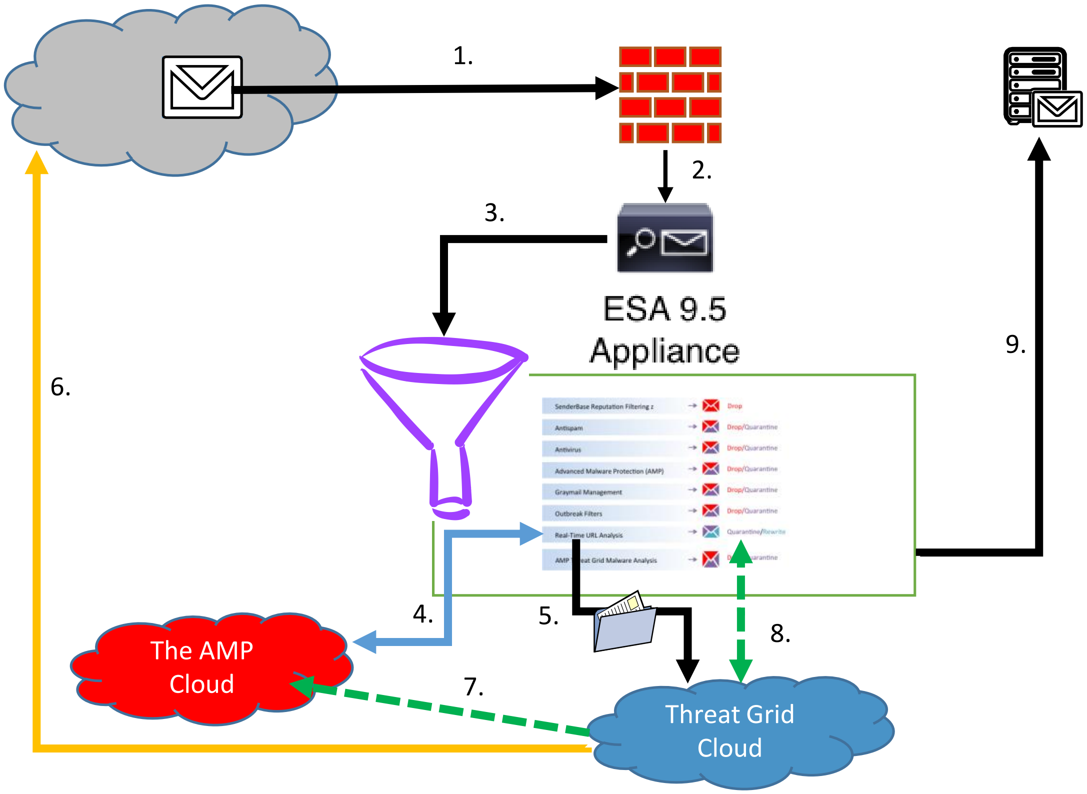
Behavioral analysis of unknown files

File Retrospection

Retrospective alerting after an attack

ESA – AMP Threat Grid Process Flow

Threat Grid in the Cloud



1. Email sent from Internet
2. Accepted by ESA Appliance
3. Email passed through security stack on ESA
4. Threat intelligence from AMP Cloud used to determine if email or attachments match malicious indicators (SHA Lookup)
5. If the file is still suspicious and qualifies for sandboxing, it is sent to cloud instance of AMP Threat Grid for analysis
6. Threat Grid cloud allows malware to access Internet and retrieve additional files
7. If AMP Threat Grid malware analysis determines that it has serious malicious behaviors and indicators, the AMP Cloud is updated (poked) to mark file as bad
8. ESA polls and is updated to mark file as bad
9. ESA processes file accordingly and send email, email notification or quarantines email

Advanced Malware Protection

Summary

File Reputation

Preventative blocking of suspicious files

File Sandboxing

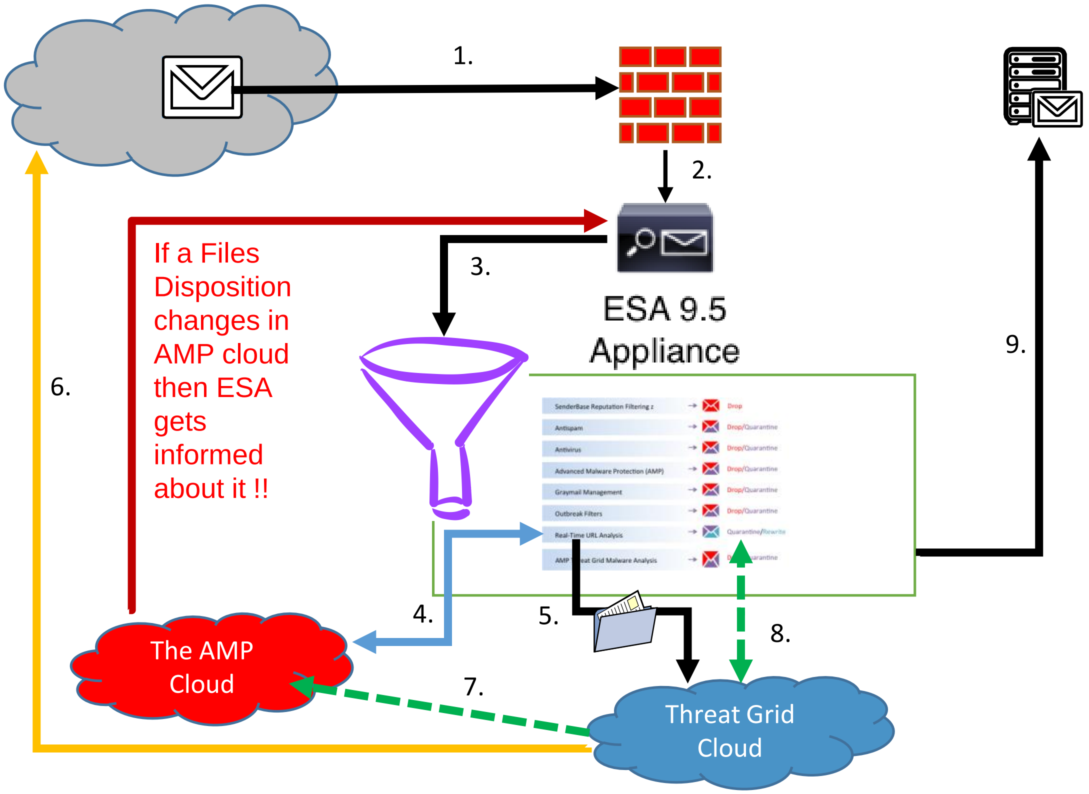
Behavioral analysis of unknown files

File Retrospection

Retrospective alerting after an attack

ESA – AMP Threat Grid Process Flow

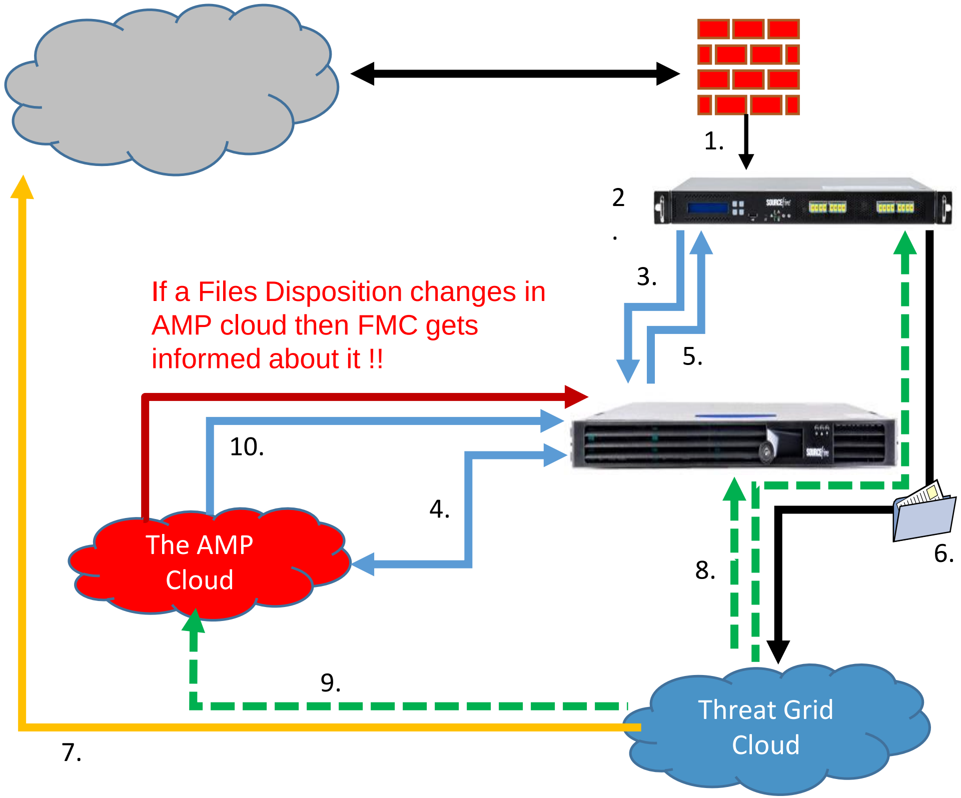
Threat Grid in the Cloud


1.
2.
3.
ESA 9.5 Appliance
If a Files Disposition changes in AMP cloud then ESA gets informed about it !!
SenderBase Reputation Filtering z → Drop
Antispam → Drop/Quarantine
Antivirus → Drop/Quarantine
Advanced Malware Protection (AMP) → Drop/Quarantine
Graymail Management → Drop/Quarantine
Outbreak Filters → Drop/Quarantine
Real-Time URL Analysis → Quarantine/Rewrite
AMP T eat Grid Malware Analysis → D uarantine
4.
5.
6.
7.
8.
9.
The AMP Cloud
Threat Grid Cloud

1. Email sent from Internet
2. Accepted by ESA Appliance
3. Email passed through security stack on ESA
4. Threat intelligence from AMP Cloud used to determine if email or attachments match malicious indicators (SHA Lookup)
5. If the file is still suspicious and qualifies for sandboxing, it is sent to cloud instance of AMP Threat Grid for analysis
6. Threat Grid cloud allows malware to access Internet and retrieve additional files
7. If AMP Threat Grid malware analysis determines that it has serious malicious behaviors and indicators, the AMP Cloud is updated (poked) to mark file as bad
8. ESA polls and is updated to mark file as bad
9. ESA processes file accordingly and send email, email notification or quarantines email

Firepower – AMP ThreatGrid Process Flow

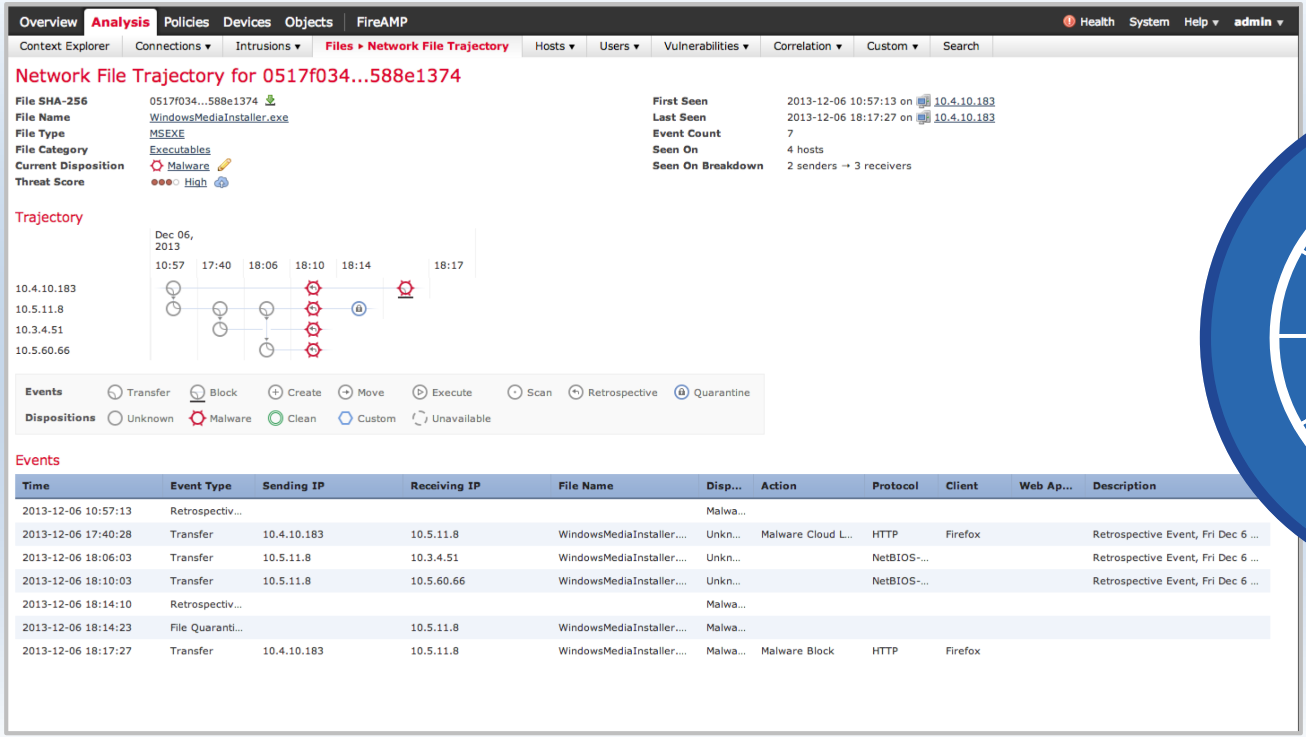
ThreatGrid in the Cloud


1.
2
.
3.
5.
If a Files Disposition changes in AMP cloud then FMC gets informed about it !!
10.
4.
The AMP Cloud
8.
6.
9.
Threat Grid Cloud
7.

1. Appliance integrated via SPAN or in-line
2. AMP appliance extracts files from flows
3. AMP appliance connects to FMC to perform a File Reputation Check
4. FMC collects File Reputation from AMP Cloud to determine if the file is known malicious, known good or unknown
5. FMC forwards File Reputation information and the AMP appliance acts accordingly (block/allow)
6. If the file is still suspicious (unknown) and qualifies for sandboxing (file type), it is sent to AMP Threat Grid cloud for dynamic analysis and file transfer will be allowed at this time
7. AMP Threat Grid allows malware to connect to Internet and download additional files
8. FMC and AMP appliance poll to mark file as good or bad in file trajectory
9. If TG analysis determines a threat score >95, then AMP Cloud is updated (poked) to mark file as bad
10. AMP cloud issues a retrospective event in FMC, generating potential IoC's and future file blocks

Example: How Cisco AMP Works

Network File Trajectory Use Case



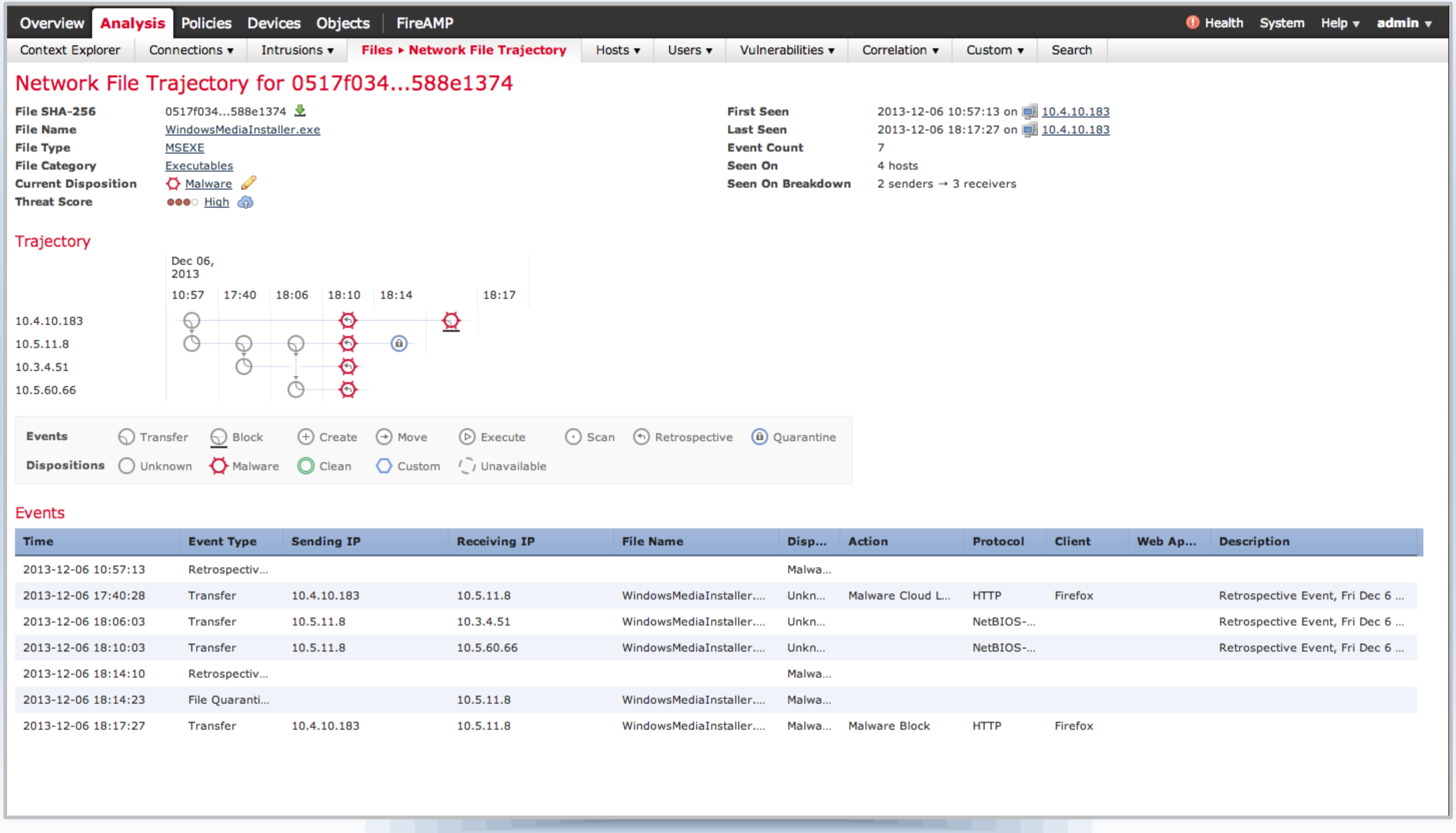
Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374	**First Seen**	2013-12-06 10:57:13 on 10.4.10.183
File Name	WindowsMediaInstaller.exe	**Last Seen**	2013-12-06 18:17:27 on 10.4.10.183
File Type	MSEXE	**Event Count**	7
File Category	Executables	**Seen On**	4 hosts
Current Disposition	Malware	**Seen On Breakdown**	2 senders → 3 receivers
Threat Score	●●●○ High		

Trajectory

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		



Network File Trajectory for 0517f034...588e1374

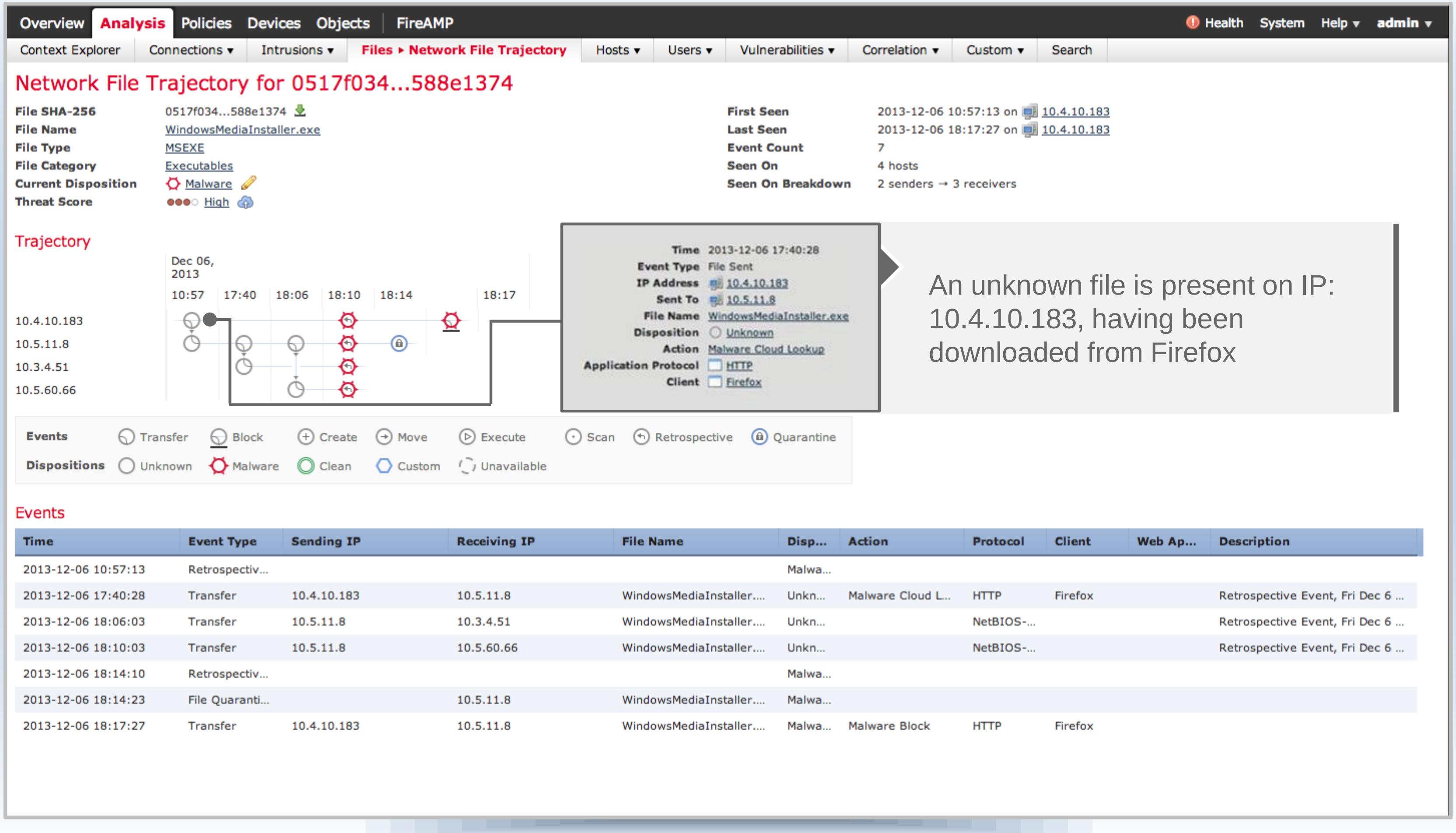
File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	●●●○ High

First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

Trajectory

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		



Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374	**First Seen**	2013-12-06 10:57:13 on 10.4.10.183
File Name	WindowsMediaInstaller.exe	**Last Seen**	2013-12-06 18:17:27 on 10.4.10.183
File Type	MSEXE	**Event Count**	7
File Category	Executables	**Seen On**	4 hosts
Current Disposition	Malware	**Seen On Breakdown**	2 senders → 3 receivers
Threat Score	●●●○ High		

Trajectory

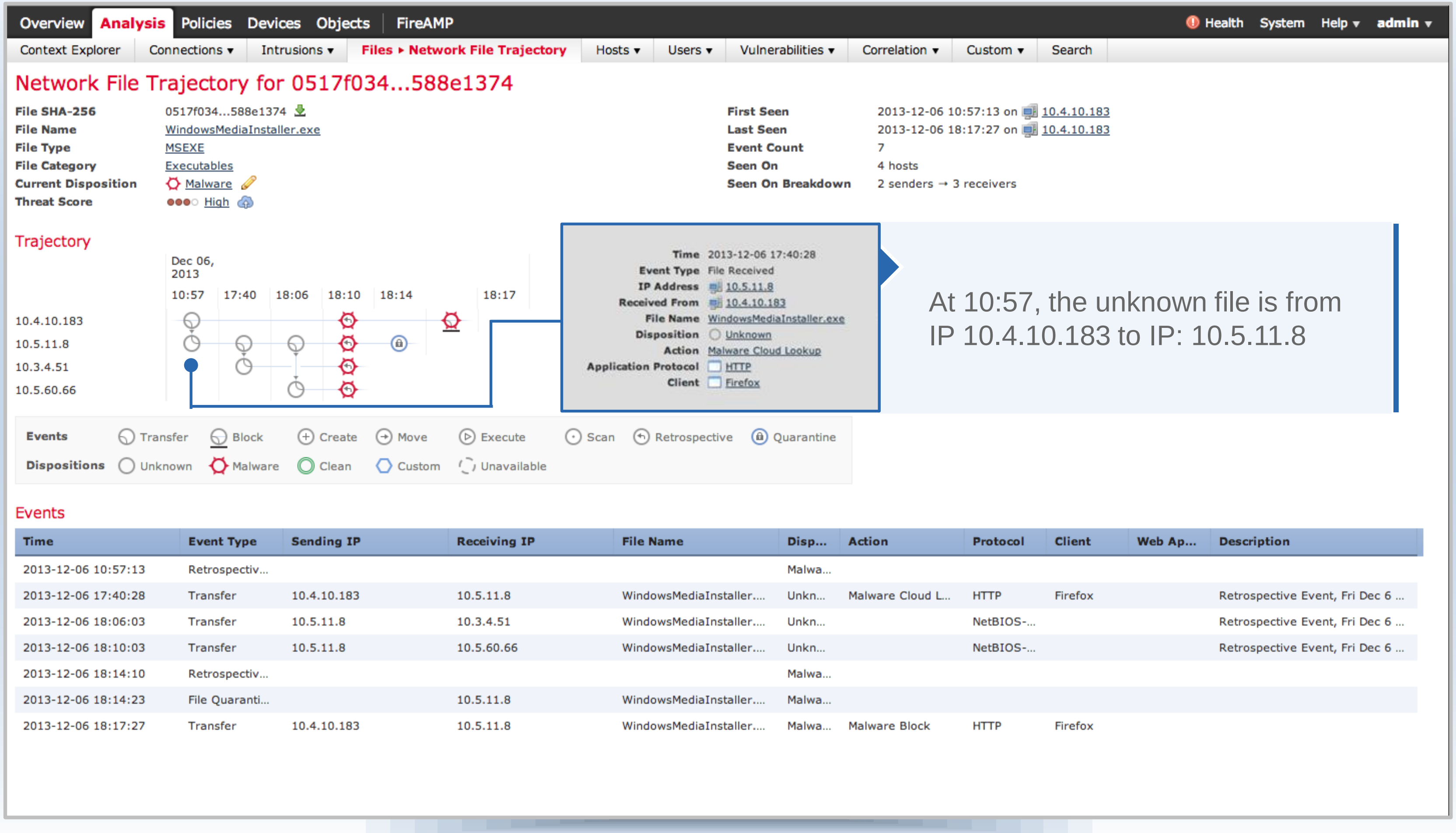
Time	2013-12-06 17:40:28
Event Type	File Sent
IP Address	10.4.10.183
Sent To	10.5.11.8
File Name	WindowsMediaInstaller.exe
Disposition	Unknown
Action	Malware Cloud Lookup
Application Protocol	HTTP
Client	Firefox

Events	Transfer	Block	Create	Move	Execute	Scan	Retrospective	Quarantine
Dispositions	Unknown	Malware	Clean	Custom	Unavailable			

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

An unknown file is present on IP: 10.4.10.183, having been downloaded from Firefox



Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	●●●○ High

First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

Trajectory

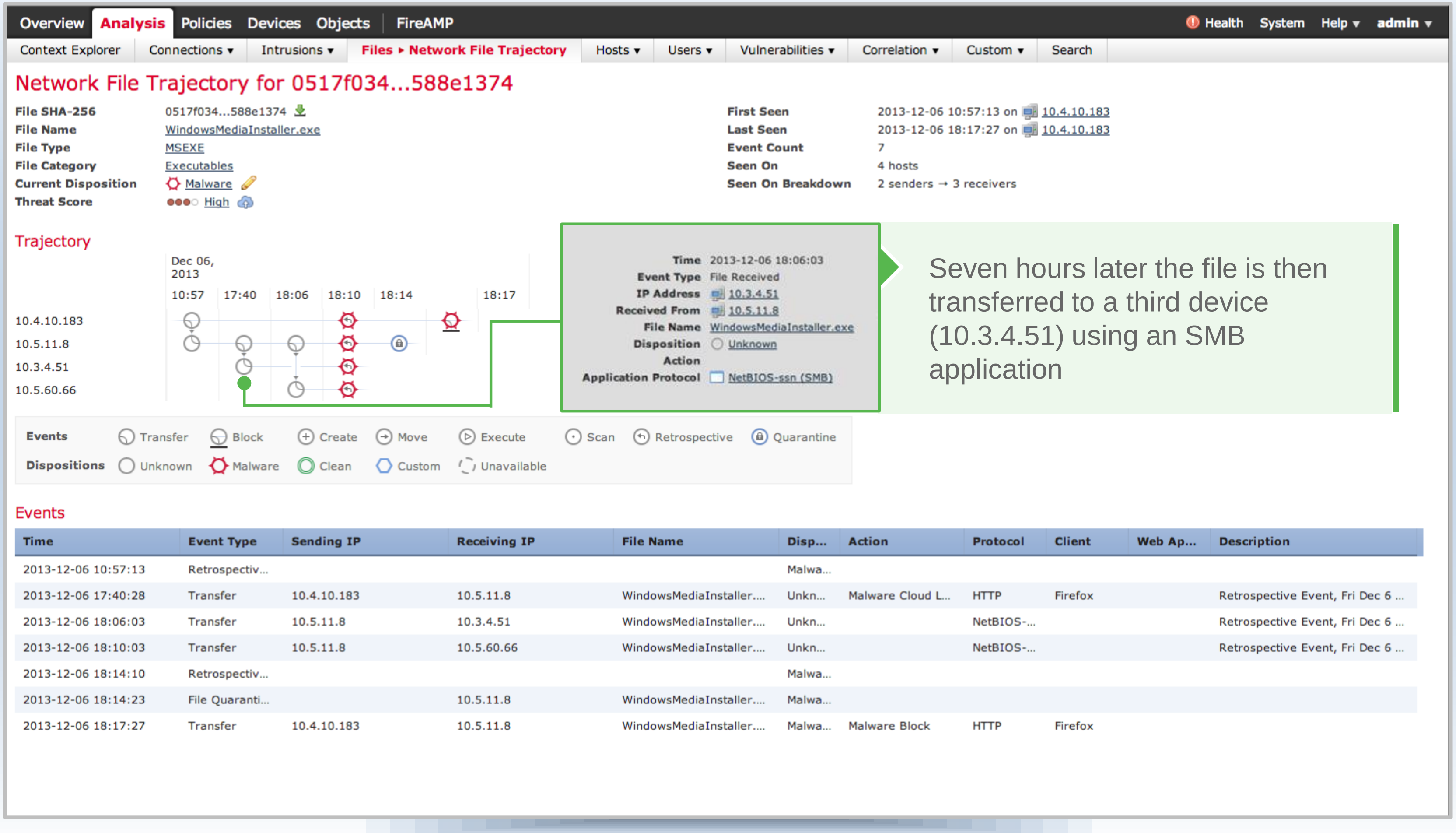
Time	2013-12-06 17:40:28
Event Type	File Received
IP Address	10.5.11.8
Received From	10.4.10.183
File Name	WindowsMediaInstaller.exe
Disposition	Unknown
Action	Malware Cloud Lookup
Application Protocol	HTTP
Client	Firefox

At 10:57, the unknown file is from IP 10.4.10.183 to IP: 10.5.11.8

Events	Transfer	Block	Create	Move	Execute	Scan	Retrospective	Quarantine
Dispositions	Unknown	Malware	Clean	Custom	Unavailable			

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		



Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	●●●○ High

First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

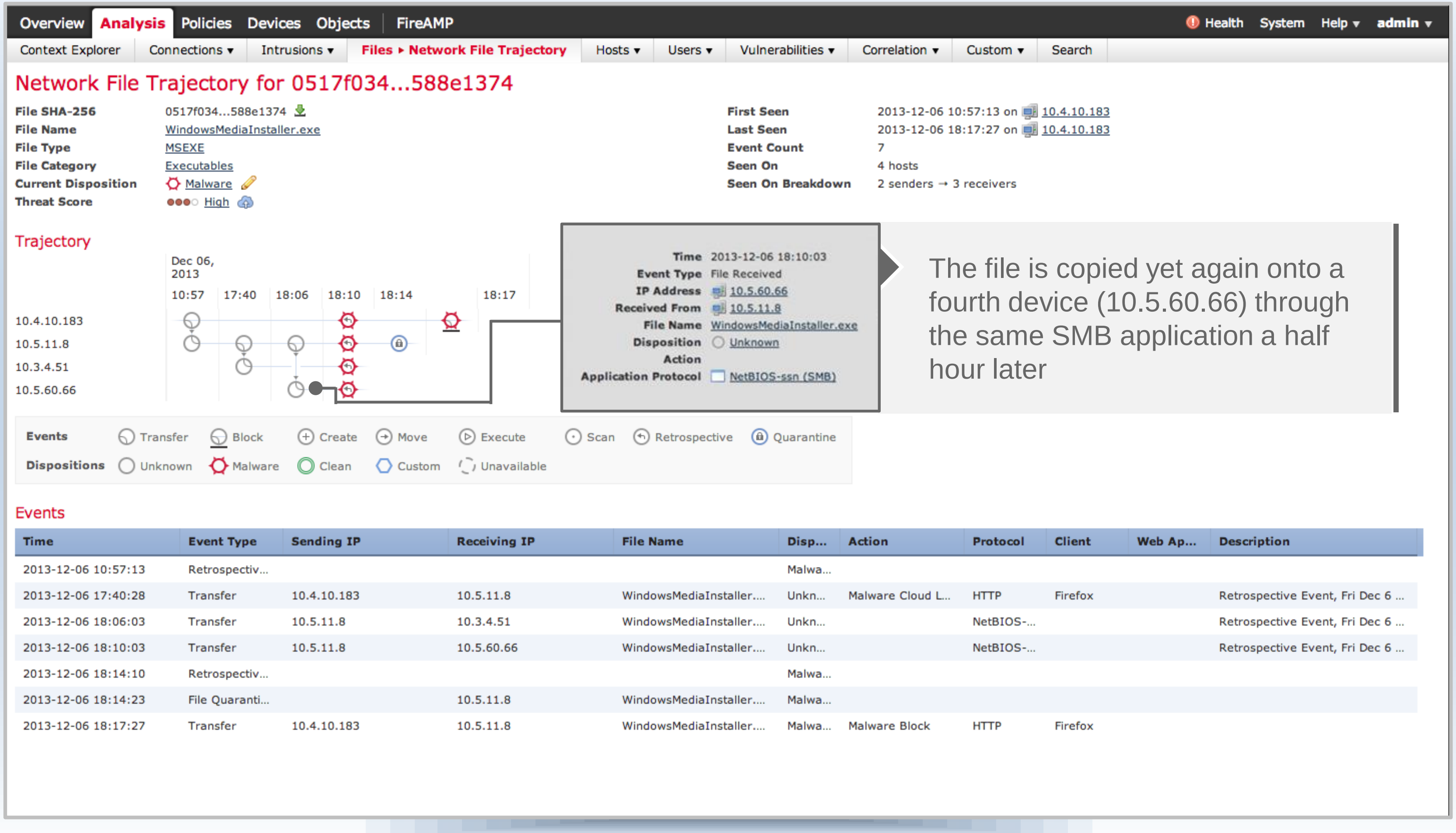
Trajectory

Time	2013-12-06 18:06:03
Event Type	File Received
IP Address	10.3.4.51
Received From	10.5.11.8
File Name	WindowsMediaInstaller.exe
Disposition	○ Unknown
Action	
Application Protocol	NetBIOS-ssn (SMB)

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Seven hours later the file is then transferred to a third device (10.3.4.51) using an SMB application



Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	●●●○ High

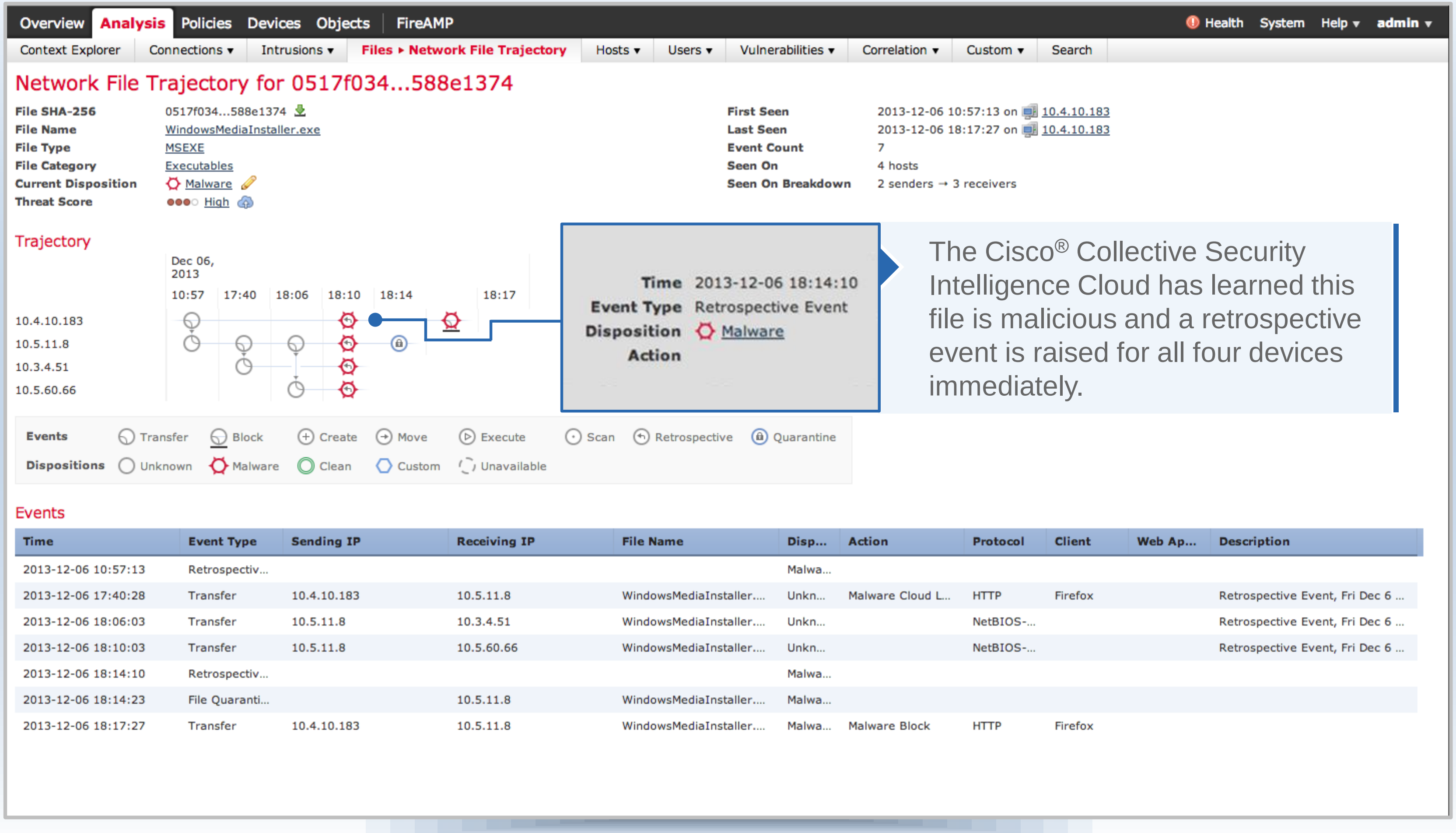
First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

Time	2013-12-06 18:10:03
Event Type	File Received
IP Address	10.5.60.66
Received From	10.5.11.8
File Name	WindowsMediaInstaller.exe
Disposition	Unknown
Action	
Application Protocol	NetBIOS-ssn (SMB)

The file is copied yet again onto a fourth device (10.5.60.66) through the same SMB application a half hour later

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		



Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	●●●○ High

First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

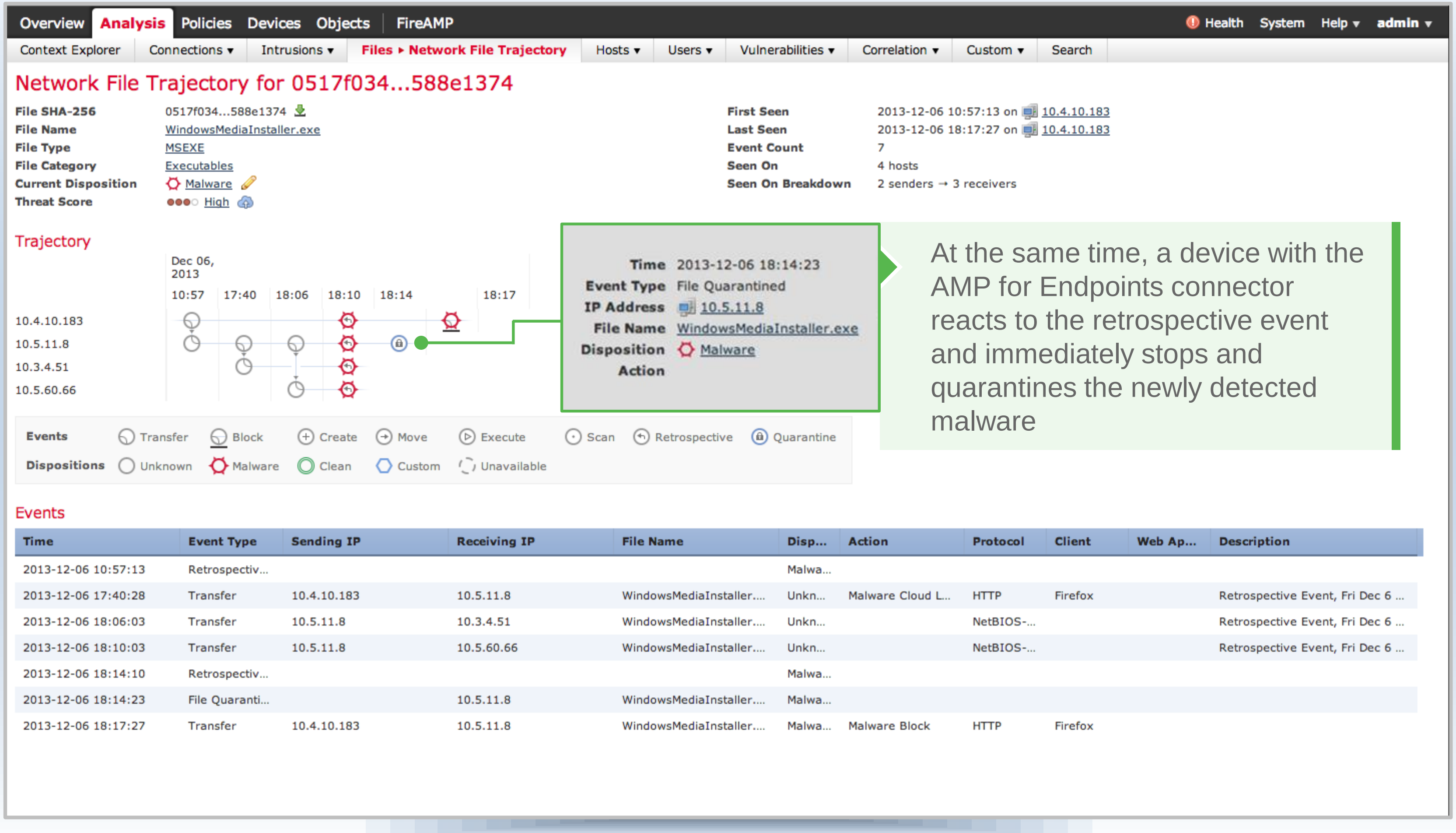
Trajectory

Time	2013-12-06 18:14:10
Event Type	Retrospective Event
Disposition	Malware
Action	

The Cisco® Collective Security Intelligence Cloud has learned this file is malicious and a retrospective event is raised for all four devices immediately.

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		



Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374	**First Seen**	2013-12-06 10:57:13 on 10.4.10.183
File Name	WindowsMediaInstaller.exe	**Last Seen**	2013-12-06 18:17:27 on 10.4.10.183
File Type	MSEXE	**Event Count**	7
File Category	Executables	**Seen On**	4 hosts
Current Disposition	Malware	**Seen On Breakdown**	2 senders → 3 receivers
Threat Score	●●●○ High		

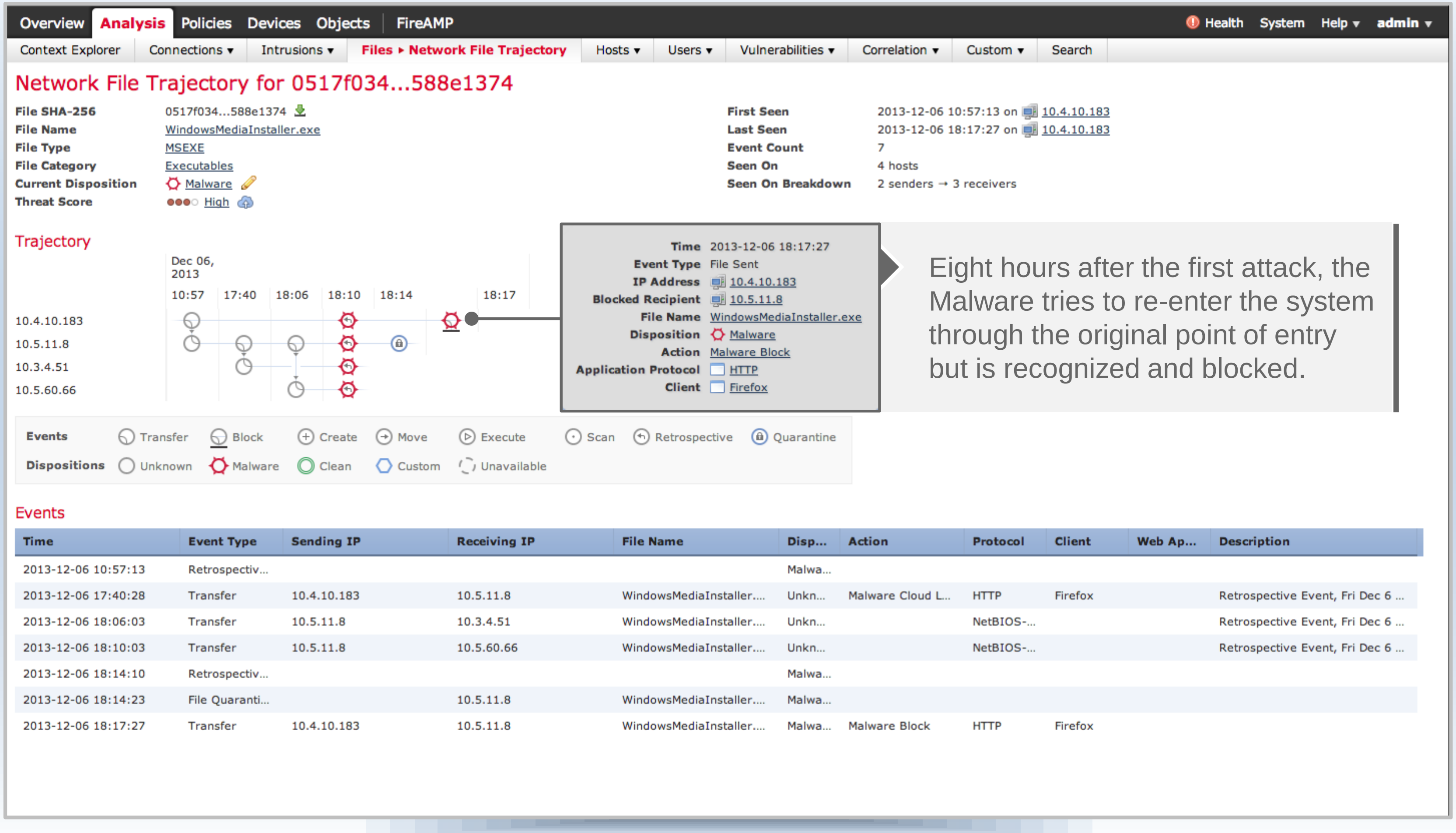
Trajectory

Time	2013-12-06 18:14:23
Event Type	File Quarantined
IP Address	10.5.11.8
File Name	WindowsMediaInstaller.exe
Disposition	Malware
Action	

At the same time, a device with the AMP for Endpoints connector reacts to the retrospective event and immediately stops and quarantines the newly detected malware

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		



Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374	**First Seen**	2013-12-06 10:57:13 on 10.4.10.183
File Name	WindowsMediaInstaller.exe	**Last Seen**	2013-12-06 18:17:27 on 10.4.10.183
File Type	MSEXE	**Event Count**	7
File Category	Executables	**Seen On**	4 hosts
Current Disposition	Malware	**Seen On Breakdown**	2 senders → 3 receivers
Threat Score	●●●○ High		

Trajectory

Time	2013-12-06 18:17:27
Event Type	File Sent
IP Address	10.4.10.183
Blocked Recipient	10.5.11.8
File Name	WindowsMediaInstaller.exe
Disposition	Malware
Action	Malware Block
Application Protocol	HTTP
Client	Firefox

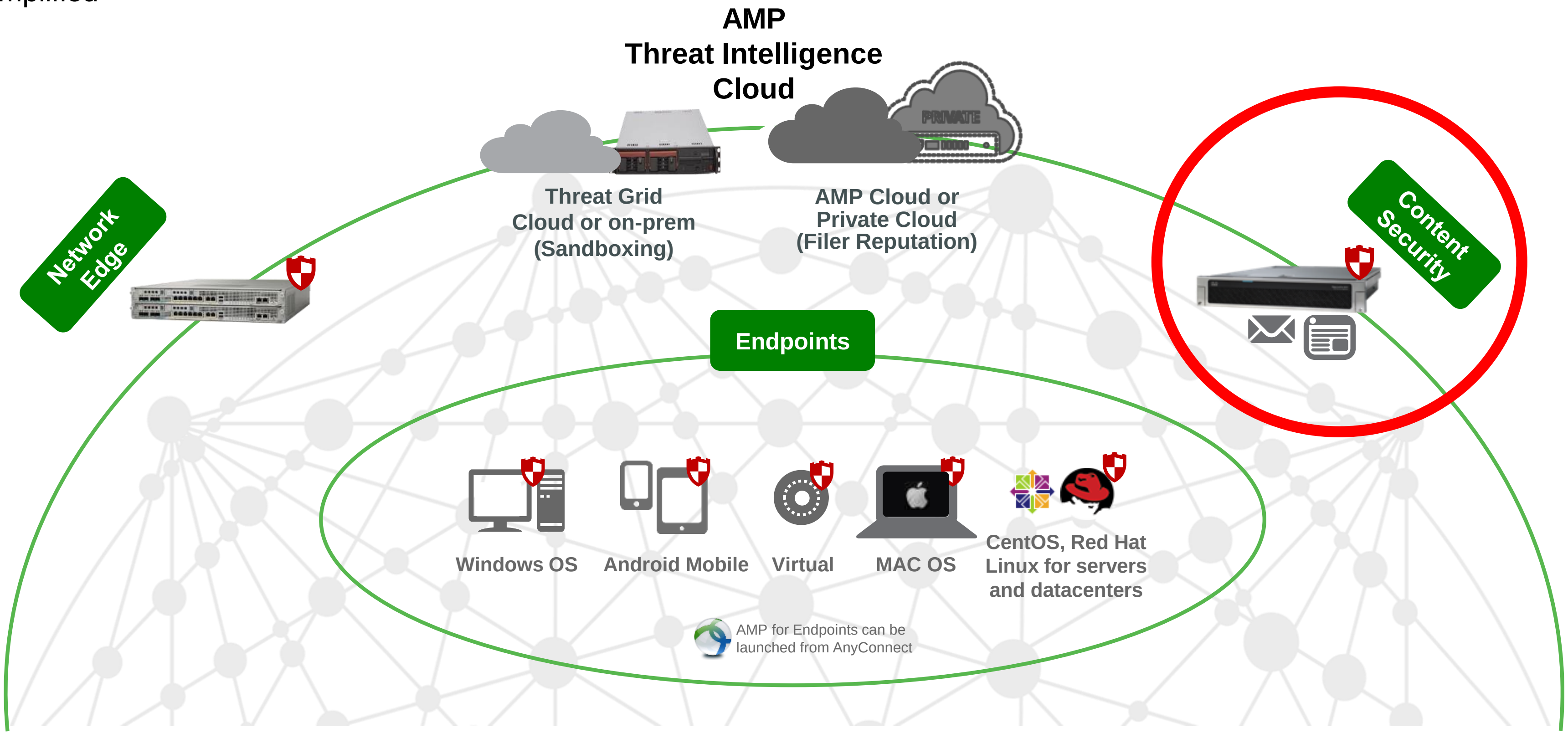
Eight hours after the first attack, the Malware tries to re-enter the system through the original point of entry but is recognized and blocked.

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

The AMP Everywhere Architecture

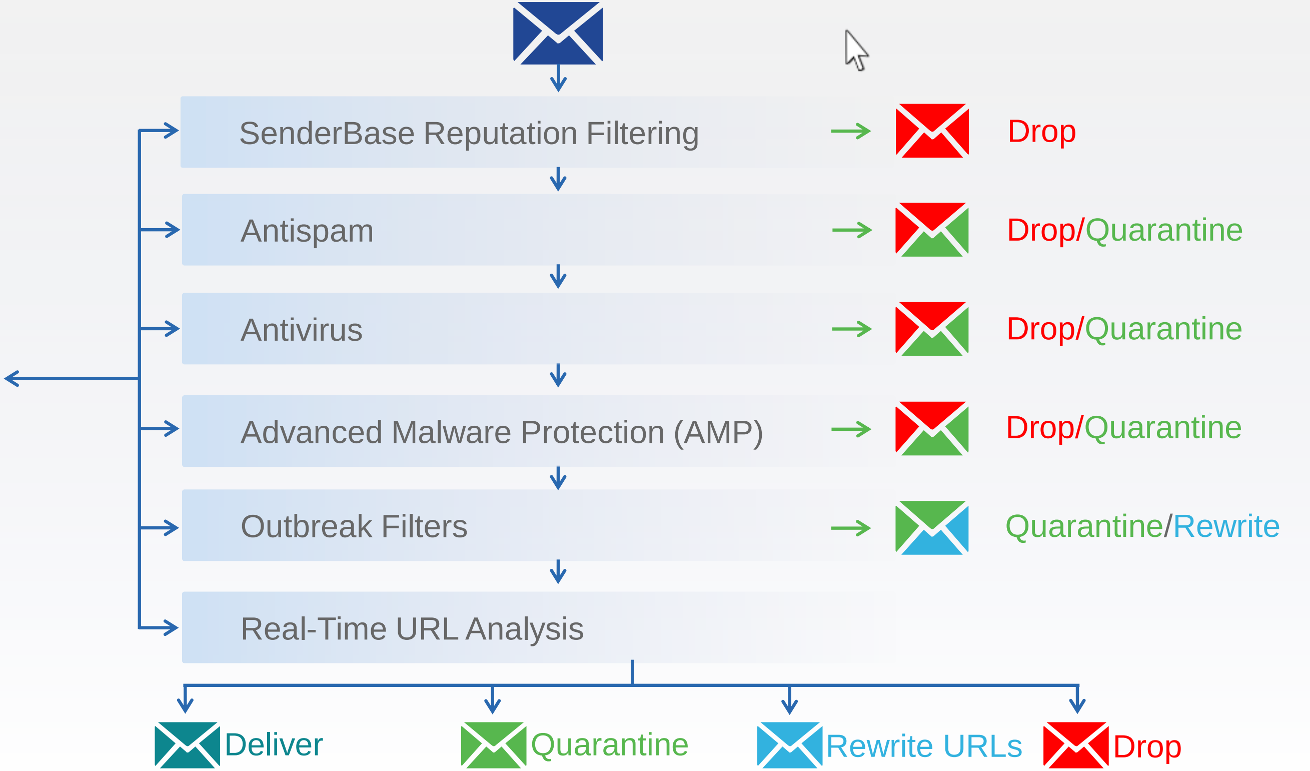
Simplified



Cisco Email Security Threat Defense

Complete Inbound Protection

Cisco® Talos



SenderBase Reputation Filtering → Drop

Antispam → Drop/Quarantine

Antivirus → Drop/Quarantine

Advanced Malware Protection (AMP) → Drop/Quarantine

Outbreak Filters → Quarantine/Rewrite

Real-Time URL Analysis

Deliver

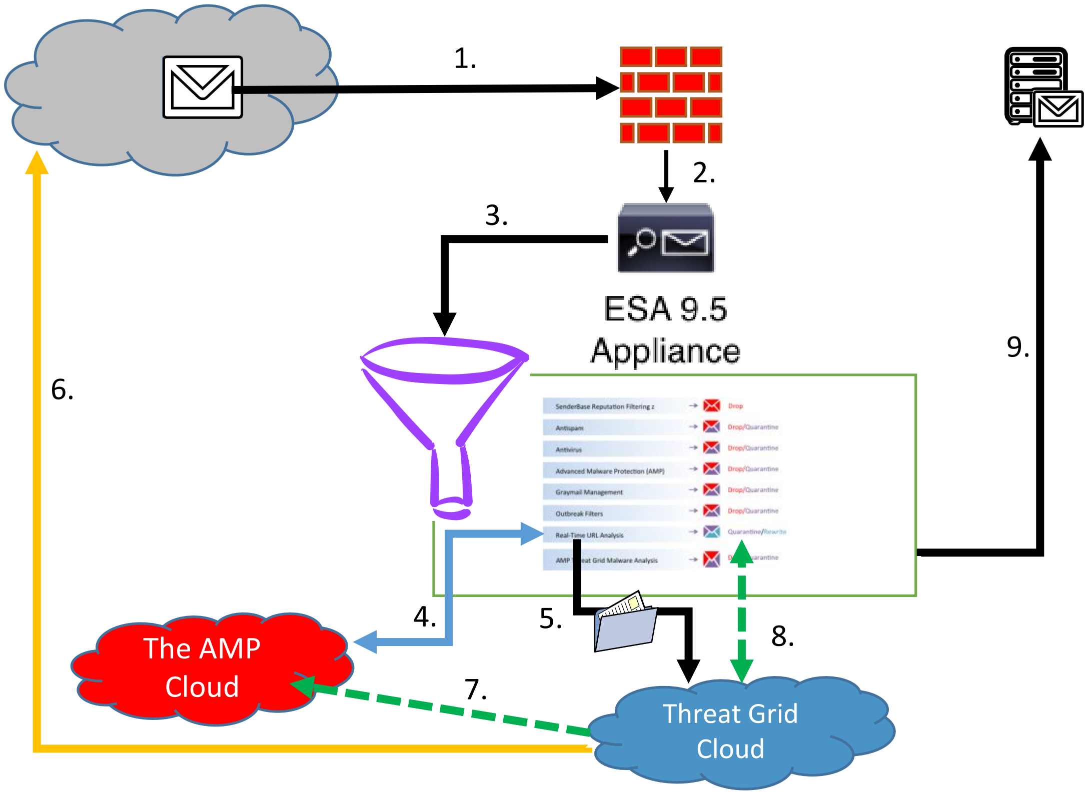
Quarantine

Rewrite URLs

Drop

ESA – AMP Threat Grid Process Flow

Threat Grid in the Cloud

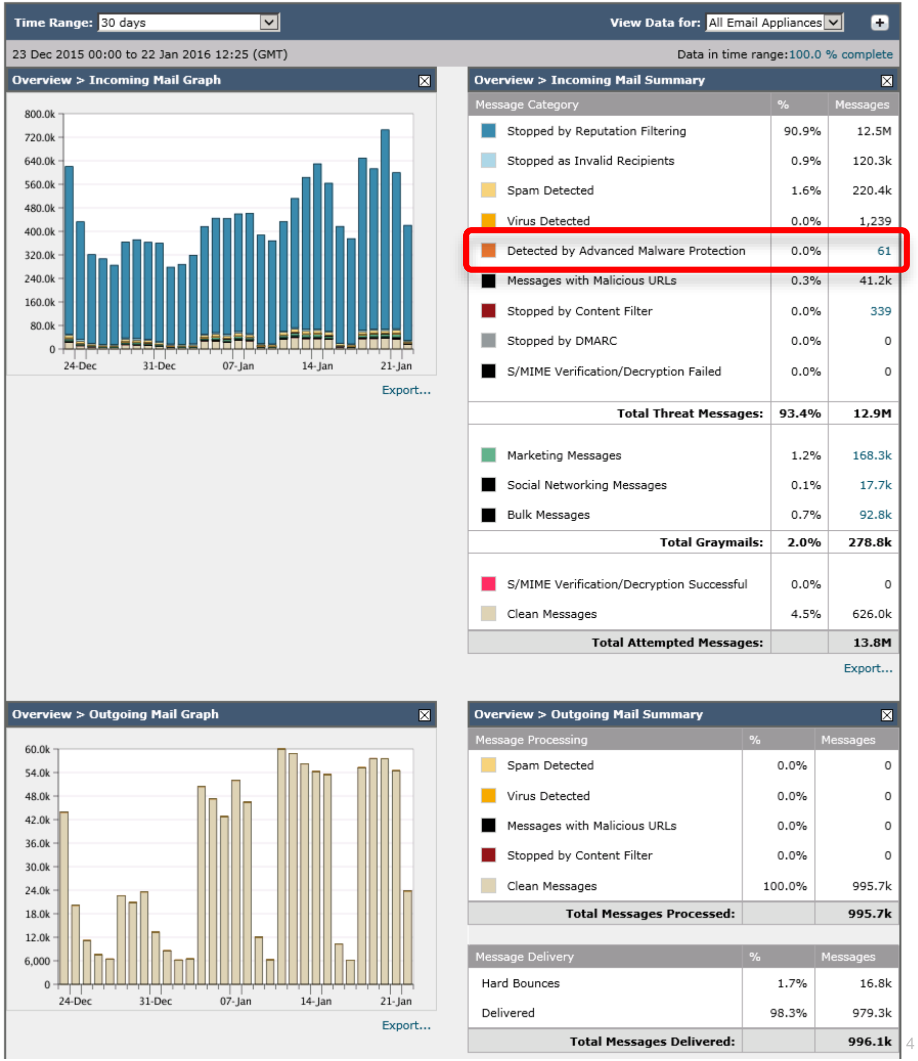

1.
2.
3.
ESA 9.5 Appliance
SenderBase Reputation Filtering z → Drop
Antispam → Drop/Quarantine
Antivirus → Drop/Quarantine
Advanced Malware Protection (AMP) → Drop/Quarantine
Graymail Management → Drop/Quarantine
Outbreak Filters → Drop/Quarantine
Real-Time URL Analysis → Quarantine/Rewrite
AMP Threat Grid Malware Analysis → Drop/Quarantine
4.
5.
6.
7.
8.
9.
The AMP Cloud
Threat Grid Cloud

1. Email sent from Internet
2. Accepted by ESA Appliance
3. Email passed through security stack on ESA
4. Threat intelligence from AMP Cloud used to determine if email or attachments match malicious indicators (SHA Lookup)
5. If low prevalence executable is still suspicious, it is sent to cloud instance of AMP Threat Grid for analysis
6. Threat Grid cloud allows malware to access Internet and retrieve additional files
7. If AMP Threat Grid malware analysis determines that it has serious malicious behaviors and indicators, the AMP Cloud is updated (poked) to mark file as bad
8. ESA polls and is updated to mark file as bad
9. ESA processes file accordingly and send email, email notification or quarantines email

AMP on ESA in action

30 days of Evaluation Results

- Real Life example:
  - 9500 users organization
  - ESA for Email Security
  - AMP license activated for eval
  - AMP Threat Grid appliance for sandboxing
- On ESA AMP works after Reputation Filtering, AS and AV
- However AMP catched 61 threats within 30 days
- That‘s ADVANCED Malware Protection



Time Range: 30 days

View Data for: All Email Appliances

23 Dec 2015 00:00 to 22 Jan 2016 12:25 (GMT)

Data in time range:100.0 % complete

Overview > Incoming Mail Graph

Export...

Overview > Incoming Mail Summary

Message Category	%	Messages
Stopped by Reputation Filtering	90.9%	12.5M
Stopped as Invalid Recipients	0.9%	120.3k
Spam Detected	1.6%	220.4k
Virus Detected	0.0%	1,239
Detected by Advanced Malware Protection	0.0%	61
Messages with Malicious URLs	0.3%	41.2k
Stopped by Content Filter	0.0%	339
Stopped by DMARC	0.0%	0
S/MIME Verification/Decryption Failed	0.0%	0
Total Threat Messages:	**93.4%**	**12.9M**
Marketing Messages	1.2%	168.3k
Social Networking Messages	0.1%	17.7k
Bulk Messages	0.7%	92.8k
Total Graymails:	**2.0%**	**278.8k**
S/MIME Verification/Decryption Successful	0.0%	0
Clean Messages	4.5%	626.0k
Total Attempted Messages:		**13.8M**

Export...

Overview > Outgoing Mail Graph

Export...

Overview > Outgoing Mail Summary

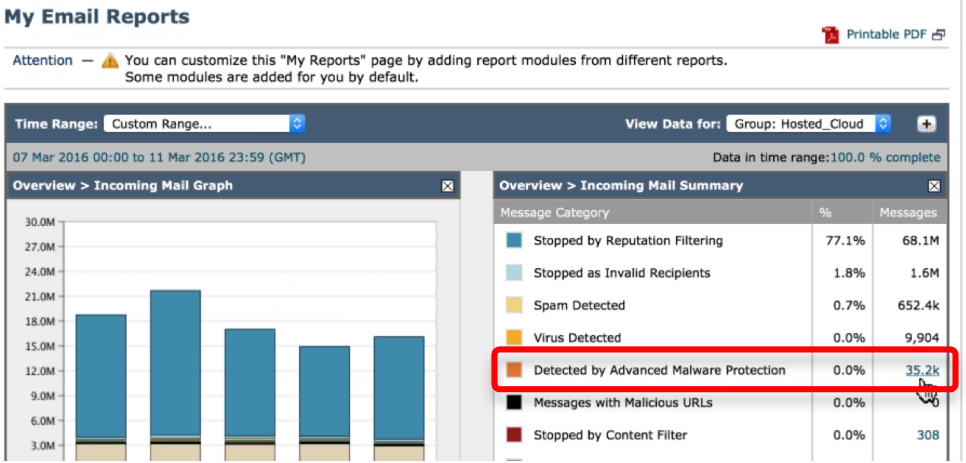
Message Processing	%	Messages
Spam Detected	0.0%	0
Virus Detected	0.0%	0
Messages with Malicious URLs	0.0%	0
Stopped by Content Filter	0.0%	0
Clean Messages	100.0%	995.7k
Total Messages Processed:		**995.7k**

Message Delivery	%	Messages
Hard Bounces	1.7%	16.8k
Delivered	98.3%	979.3k
Total Messages Delivered:		**996.1k**

AMP on ESA in action

1 week of Evaluation Results

- Real Life example:
  - 220.000 users organization
  - CES for Email Security
  - AMP license activated for eval
- Here we‘ve seen the opposite:
  - almost 10.000 AV hits
  - more than 35.000 hits by AMP
- BUT this was not a regular week
- Looking at a week with usual mail traffic, AMP still provides huge value



My Email Reports

Printable PDF

Attention — ⚠ You can customize this "My Reports" page by adding report modules from different reports. Some modules are added for you by default.

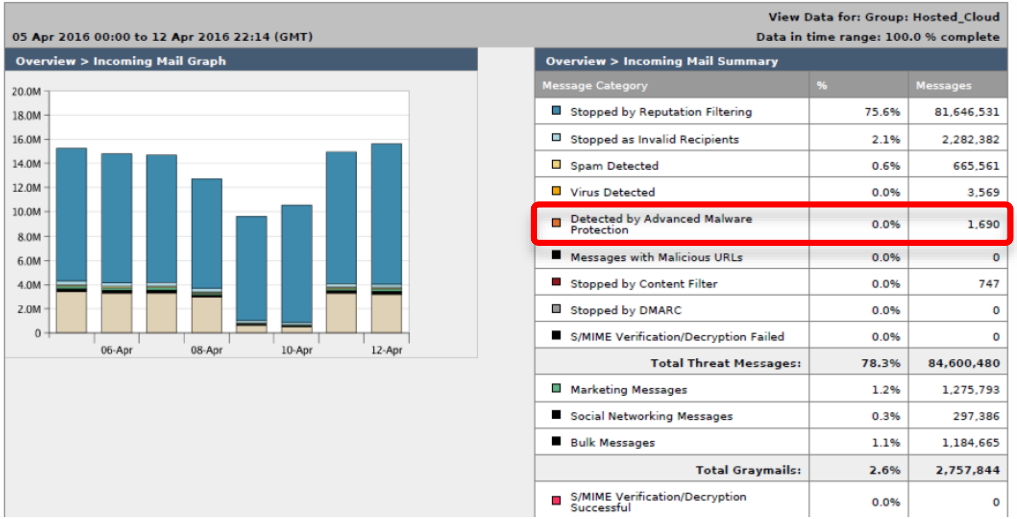
Time Range: Custom Range... View Data for: Group: Hosted_Cloud

07 Mar 2016 00:00 to 11 Mar 2016 23:59 (GMT) Data in time range: 100.0 % complete

Overview > Incoming Mail Graph

Overview > Incoming Mail Summary

Message Category	%	Messages
■ Stopped by Reputation Filtering	77.1%	68.1M
■ Stopped as Invalid Recipients	1.8%	1.6M
■ Spam Detected	0.7%	652.4k
■ Virus Detected	0.0%	9,904
■ Detected by Advanced Malware Protection	0.0%	35.2k
■ Messages with Malicious URLs	0.0%	0
■ Stopped by Content Filter	0.0%	308



05 Apr 2016 00:00 to 12 Apr 2016 22:14 (GMT)

View Data for: Group: Hosted_Cloud
Data in time range: 100.0 % complete

Overview > Incoming Mail Graph

Overview > Incoming Mail Summary

Message Category	%	Messages
■ Stopped by Reputation Filtering	75.6%	81,646,531
■ Stopped as Invalid Recipients	2.1%	2,282,382
■ Spam Detected	0.6%	665,561
■ Virus Detected	0.0%	3,569
■ Detected by Advanced Malware Protection	0.0%	1,690
■ Messages with Malicious URLs	0.0%	0
■ Stopped by Content Filter	0.0%	747
■ Stopped by DMARC	0.0%	0
■ S/MIME Verification/Decryption Failed	0.0%	0
Total Threat Messages:	78.3%	84,600,480
■ Marketing Messages	1.2%	1,275,793
■ Social Networking Messages	0.3%	297,386
■ Bulk Messages	1.1%	1,184,665
Total Graymails:	2.6%	2,757,844
■ S/MIME Verification/Decryption Successful	0.0%	0

AMP on ESA in action

Two weeks, 25.000 mail users, more detailed analysis

```
======================================= AMP file reputation results ====================
Number of files extracted from mails:                                          195472
Number of AMP reputation responses from cloud:                                 101476
Number of AMP reputation responses from cache:                                  93996
Number of files with AMP disposition MALWARE - DROPPED:                          1259
Number of files with AMP disposition CLEAN - PASSED:                             4188
Number of files with AMP disposition UNKNOWN:                                  190251
======================================= AMP upload_action ==============================
Number of unknown files not to be uploaded (0):                                   147
Number of unknown files not to be uploaded (2):                                 49420
Number of unknown files to be uploaded (1):                                    140684
======================================= Threat Grid results ============================
Number of files already uploaded or known to the Threat Grid server:              332
Number of all file submissions to the Threat Grid server:                        3830
Number of files successfully analyzed in the Threat Grid server:                 3830
Number of analyzed files with threat score = 0 - NOT DROPPED after sandboxing:   3230
Number of analyzed files with threat score <95 - NOT DROPPED after sandboxing:    582
Number of analyzed files with threat score >95 - DROPPED after sandboxing:         18
======================================== Retrospective events =========================
Number of files with retrospective disposition changes to MALICIOUS:              159
========================================================================================
```

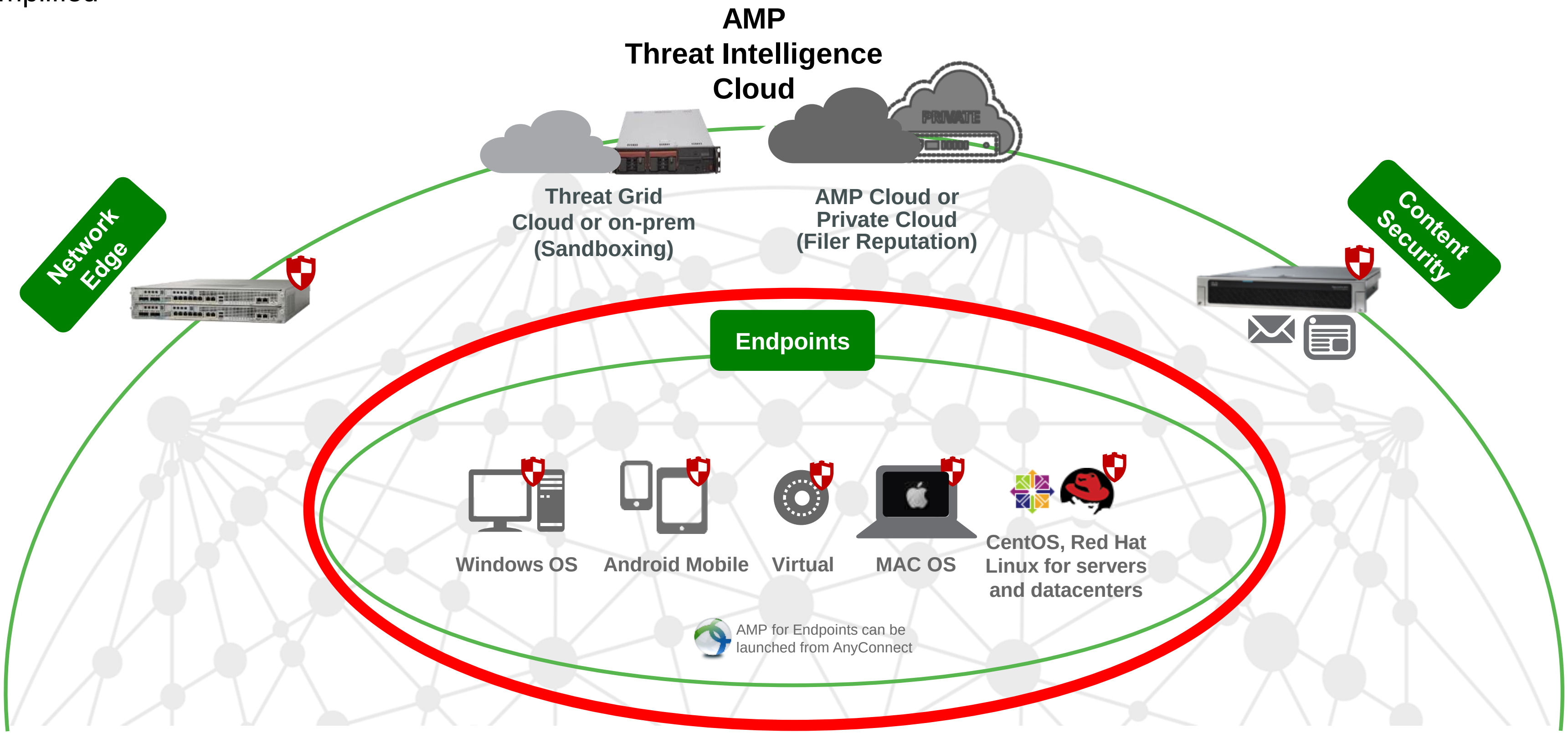
File Reputation

File Analysis

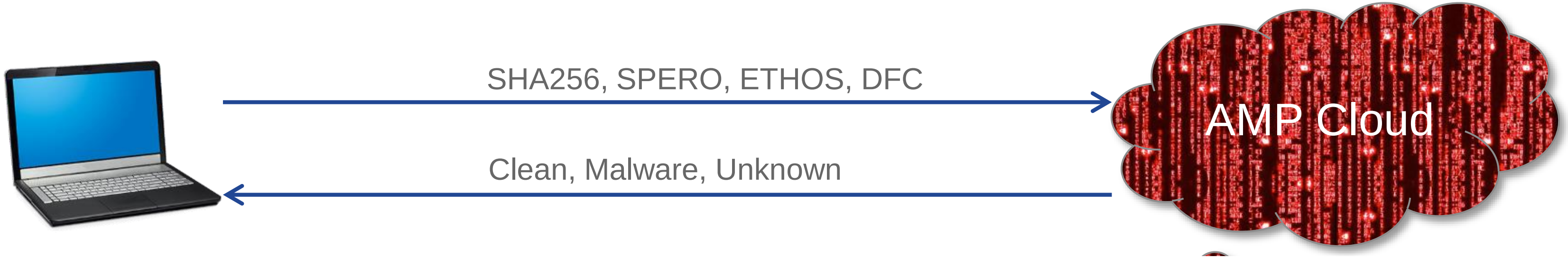
Retrospection

The AMP Everywhere Architecture

Simplified



AMP for Endpoint
Connector Details



- Local Connector
  - No local definitions (sort of)
  - Minimal resource usage
- Approx 30 MB RAM
  - 150 MB HDD
  - 1GB if using TETRA Engine

- Propagation Delay
  - N. America ~ 200mS
  - We do NOT Block File I/O during Cloud Lookups
  - Passive Mode Kernel Blocking
- Traffic
  - File Cloud Query = ~ 390 bytes
  - Average Client is 39 Queries per Day
  - 5000 Client = 76MB/Day

- Detection Engines
  - 1-1
  - SPERO
  - ETHOS
  - Advanced Analytics
  - Dynamic Analysis
- Trajectory Data

AMP for Endpoints

Supported Operating Systems

- **Windows**
  - XP SP3 +
  - Vista SP2 +
  - Windows 7
  - Windows 8 & 8.1
  - Windows Server 2003
  - Windows Server 2008
  - Windows Server 2012
  - Windows 10

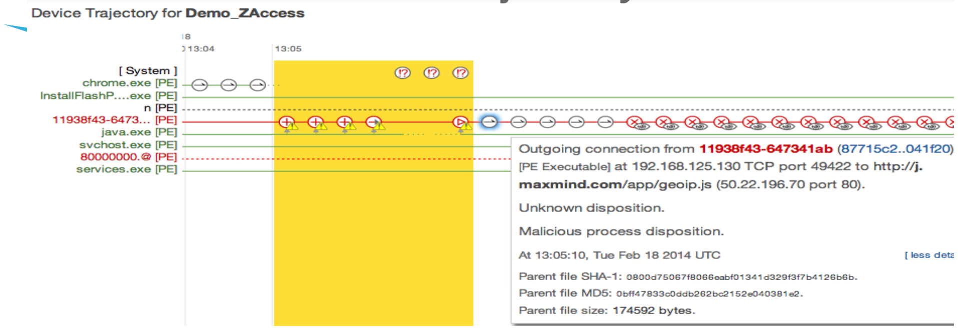
- **Linux**
  - Centos 6.4
  - Centos 6.5
  - Centos 6.6
  - RHEL 6.5
  - RHEL 6.6

- **Mac**
  - OSX 10.7 – Lion
  - OSX 10.8 – Mountain Lion
  - OSX 10.9 – Mavericks
  - OSX 10.10 – Yosemite
  - OSX 10.11 – El Captain

- **Android**
  - Android 2.1 - Éclair
  - Android 2.2 - Froyo
  - Android 2.3 - Gingerbread
  - Android 3.0 - Honeycomb
  - Android 4.0 - Ice Cream Sandwich
  - Android 4.1 - 4.3 - Jelly Bean
  - Android 4.4 - KitKat
  - Android 5.0 - 5.1 - Lollipop

When Malware Strikes, Have Answers

Device Trajectory



Outgoing connection from **11938f43-647341ab** (87715c2..041f20) [PE Executable] at 192.168.125.130 TCP port 49422 to http://**j.maxmind.com**/app/geoip.js (50.22.196.70 port 80).

Unknown disposition.

Malicious process disposition.

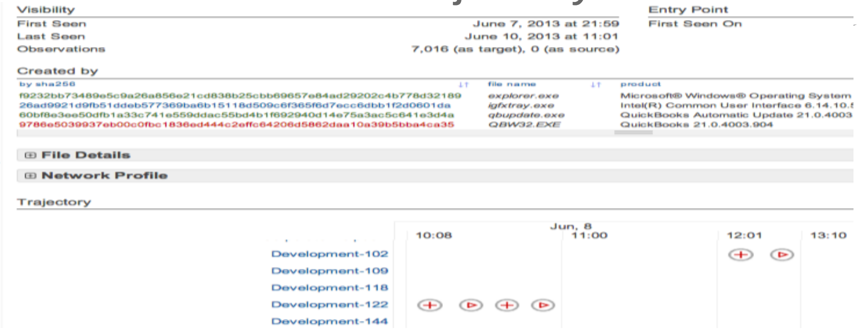
At 13:05:10, Tue Feb 18 2014 UTC [less deta

Parent file SHA-1: 0800d75067f8066eabf01341d329f3f7b4126b6b.

Parent file MD5: 0bff47833c0ddb262bc2152e040381e2.

Parent file size: 174592 bytes.

File Trajectory



Visibility	
First Seen	June 7, 2013 at 21:59
Last Seen	June 10, 2013 at 11:01
Observations	7,016 (as target), 0 (as source)

Entry Point	
First Seen On	

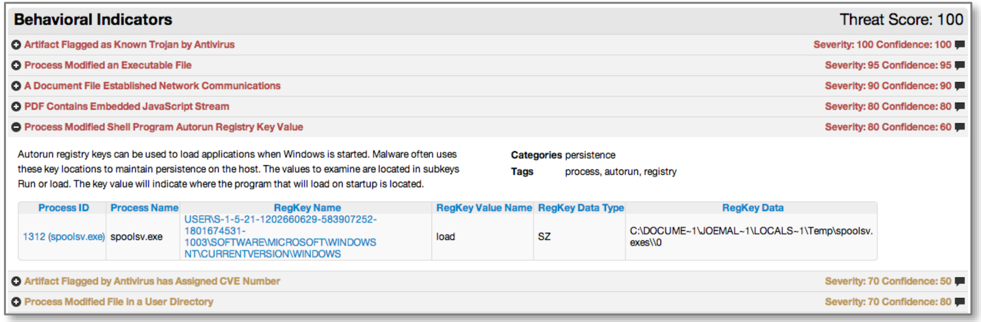
Created by

by sha256	file name	product
f9232bb73489e5c9a26a856e21cd838b25cbb69657e84ad29202c4b778d32189	*explorer.exe*	Microsoft® Windows® Operating System
26ad9921d9fb51ddeb577369ba6b15118d509c6f365f6d7ecc6dbb1f2d0601da	*igfxtray.exe*	Intel(R) Common User Interface 6.14.10.5
60bf8e3ee50dfb1a33c741e559ddac55bd4b1f692940d14e75a3ac5c641e3d4a	*qbupdate.exe*	QuickBooks Automatic Update 21.0.4003
9786e5039937eb00c0fbc1836ed444c2effc64206d5862daa10a39b5bba4ca35	*QBW32.EXE*	QuickBooks 21.0.4003.904

⊞ **File Details**

⊞ **Network Profile**

Trajectory



Behavioral Indicators Threat Score: 100

⊕ Artifact Flagged as Known Trojan by Antivirus	Severity: 100 Confidence: 100
⊕ Process Modified an Executable File	Severity: 95 Confidence: 95
⊕ A Document File Established Network Communications	Severity: 90 Confidence: 90
⊕ PDF Contains Embedded JavaScript Stream	Severity: 80 Confidence: 80
⊖ Process Modified Shell Program Autorun Registry Key Value	Severity: 80 Confidence: 60

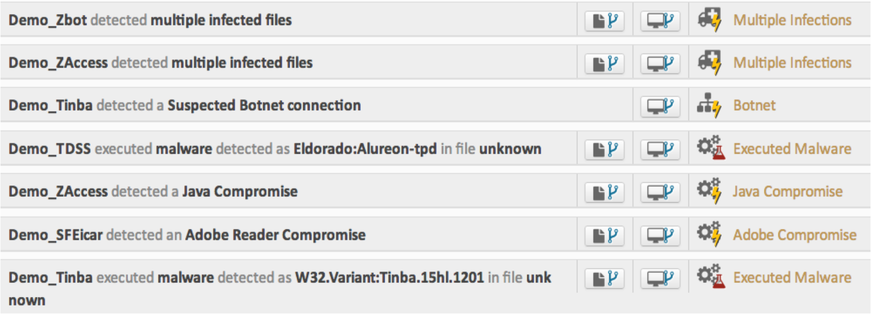
Autorun registry keys can be used to load applications when Windows is started. Malware often uses these key locations to maintain persistence on the host. The values to examine are located in subkeys Run or load. The key value will indicate where the program that will load on startup is located.

Categories persistence

Tags process, autorun, registry

Process ID	Process Name	RegKey Name	RegKey Value Name	RegKey Data Type	RegKey Data
1312 (spoolsv.exe)	spoolsv.exe	USER\S-1-5-21-1202660629-583907252-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINDOWS	load	SZ	C:\DOCUME~1\JOEMAL~1\LOCALS~1\Temp\spoolsv.exes\\0

⊕ Artifact Flagged by Antivirus has Assigned CVE Number	Severity: 70 Confidence: 50
⊕ Process Modified File in a User Directory	Severity: 70 Confidence: 80

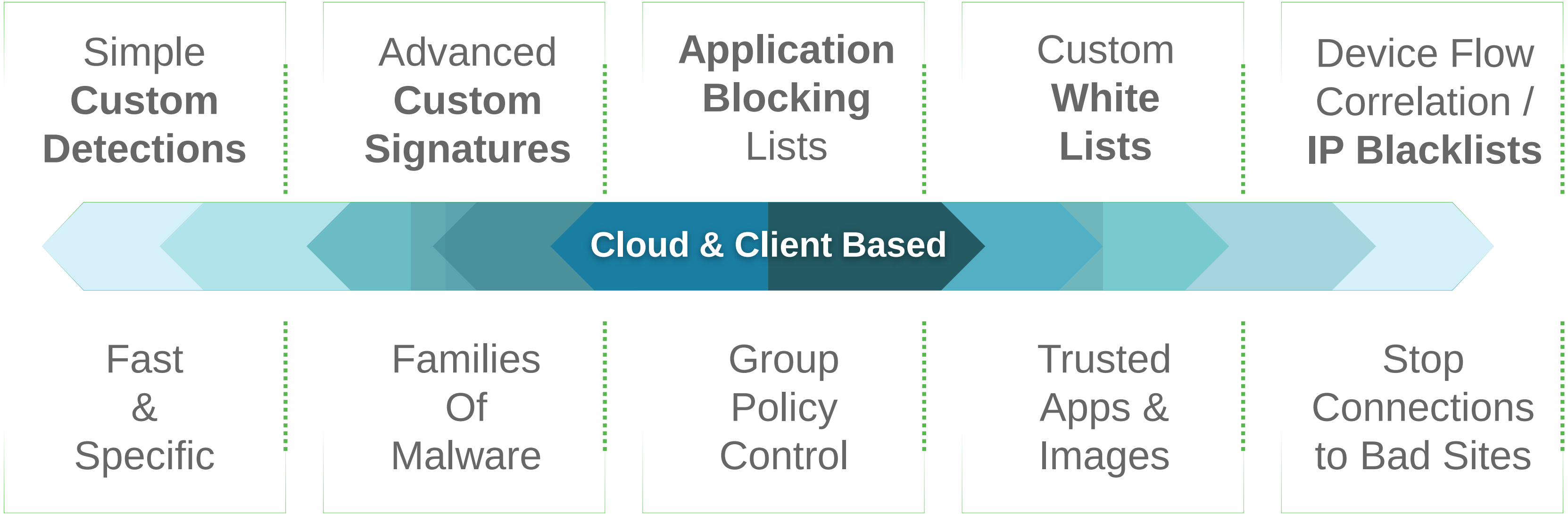


Demo_Zbot detected **multiple infected files**	Multiple Infections
Demo_ZAccess detected **multiple infected files**	Multiple Infections
Demo_Tinba detected a **Suspected Botnet connection**	Botnet
Demo_TDSS executed **malware** detected as **Eldorado:Alureon-tpd** in file **unknown**	Executed Malware
Demo_ZAccess detected a **Java Compromise**	Java Compromise
Demo_SFEicar detected an **Adobe Reader Compromise**	Adobe Compromise
Demo_Tinba executed **malware** detected as **W32.Variant:Tinba.15hl.1201** in file **unknown**	Executed Malware

And Solutions : Outbreak Control

Multiple ways to stop threats and eliminate root causes

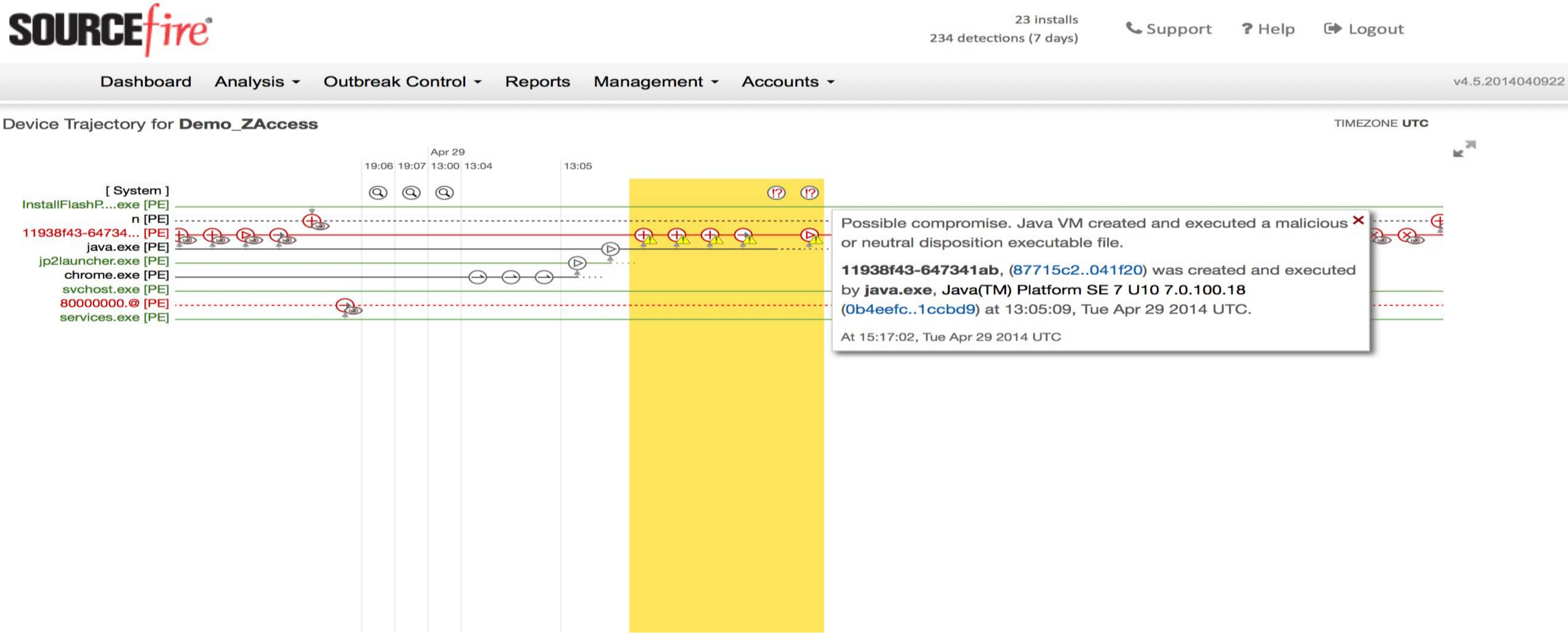
Simple and specific controls **OR** Context rich signatures for broader control



Simple **Custom Detections**	Advanced **Custom Signatures**	**Application Blocking** Lists	Custom **White Lists**	Device Flow Correlation / **IP Blacklists**
Fast & Specific	Families Of Malware	Group Policy Control	Trusted Apps & Images	Stop Connections to Bad Sites

Cloud & Client Based

AMP for Endpoint – Detection is “Table Stakes”



Possible compromise. Java VM created and executed a malicious or neutral disposition executable file.

11938f43-647341ab, (87715c2..041f20) was created and executed by **java.exe**, Java(TM) Platform SE 7 U10 7.0.100.18 (0b4eefc..1ccbd9) at 13:05:09, Tue Apr 29 2014 UTC.

At 15:17:02, Tue Apr 29 2014 UTC

Cisco Advanced Malware Protection Summary

AMP Provides Contextual Awareness and Visibility

Who

Focus on these users first

What

These applications are affected

Where

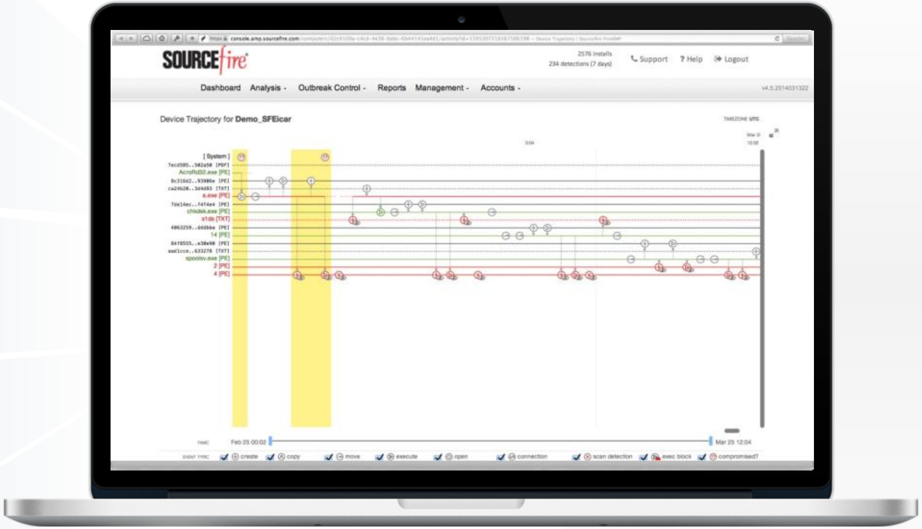
The breach affected these areas

When

This is the scope of exposure over time

How

Here is the origin and progression
of the threat



cisco

Meraki MX
AMP & Threat Grid Integration

Rene Straube, CSE, Germany
Advanced Threat Group

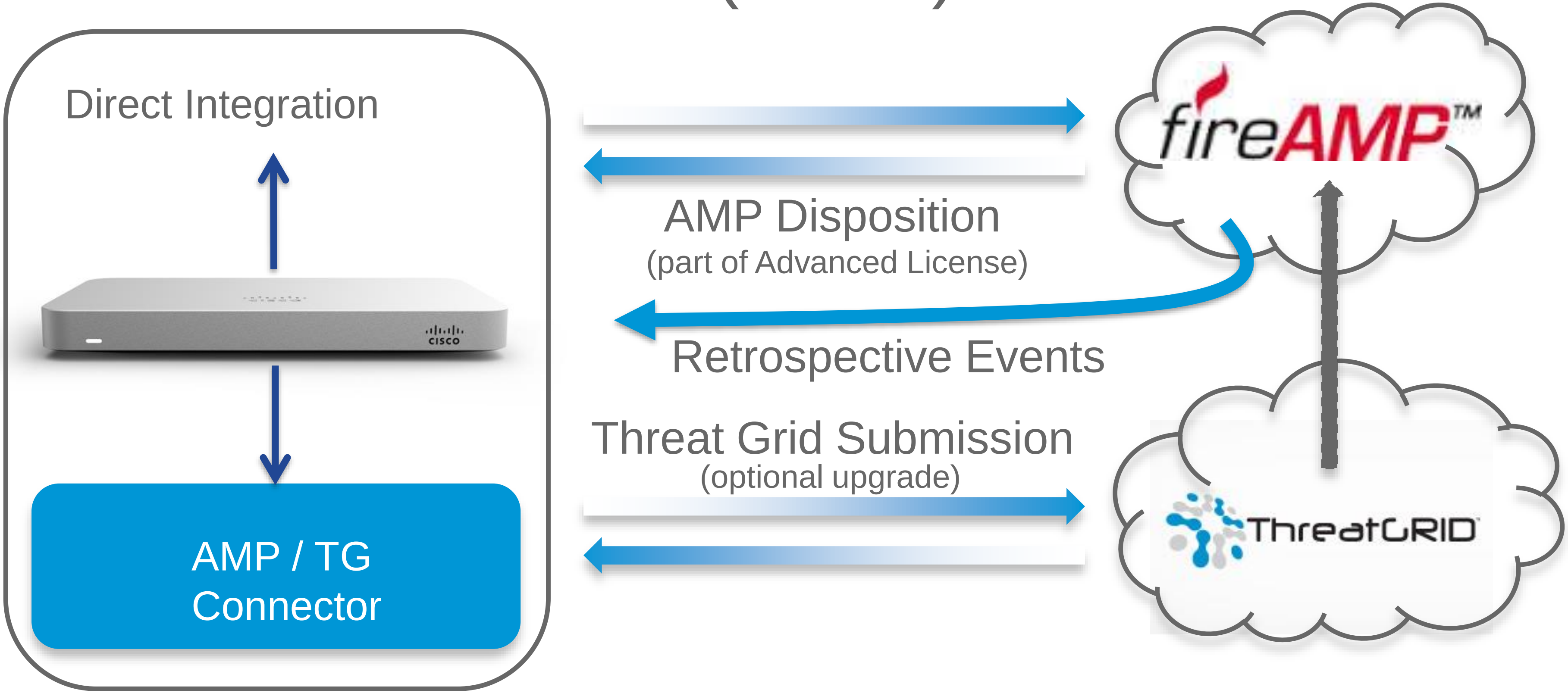
Meraki MX is UTM

Security
NG Firewall, Client VPN, Site to Site VPN, IDS/IPS, Anti-Malware, Geo-Firewall

Networking
NAT/DHCP, 3G/4G Cellular, Intelligent WAN (IWAN)

Application Control
Web Caching, Traffic Shaping, Content Filtering

AMP and TG on MX (Cloud)



Direct Integration

AMP / TG Connector

AMP Disposition

(part of Advanced License)

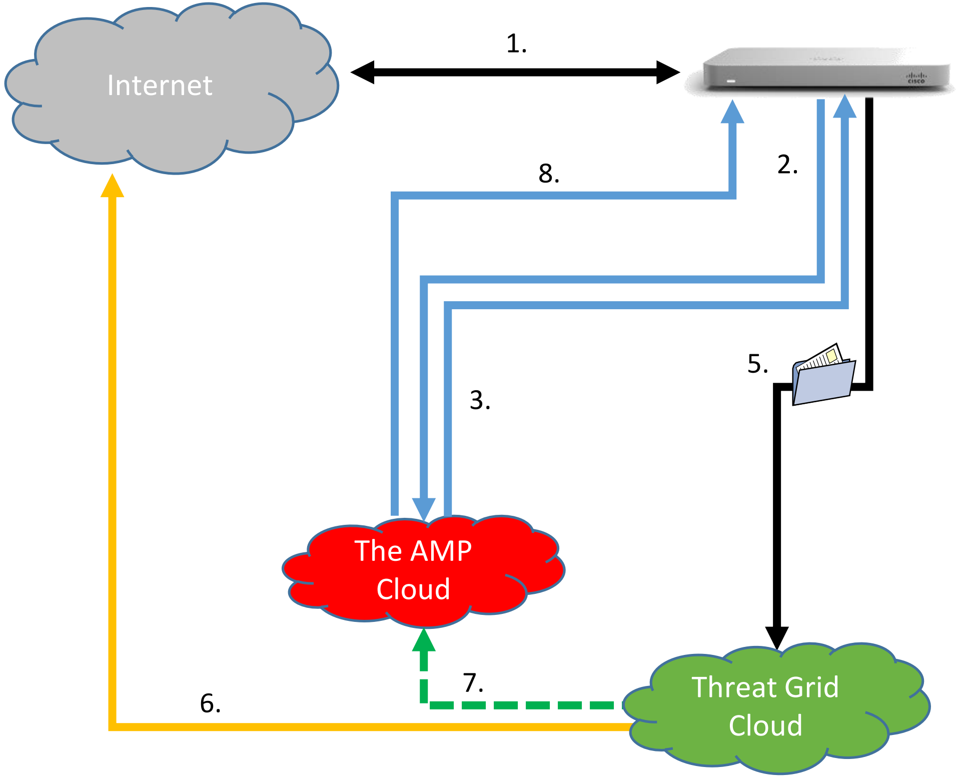
Retrospective Events

Threat Grid Submission

(optional upgrade)

Meraki MX – AMP ThreatGrid Process Flow

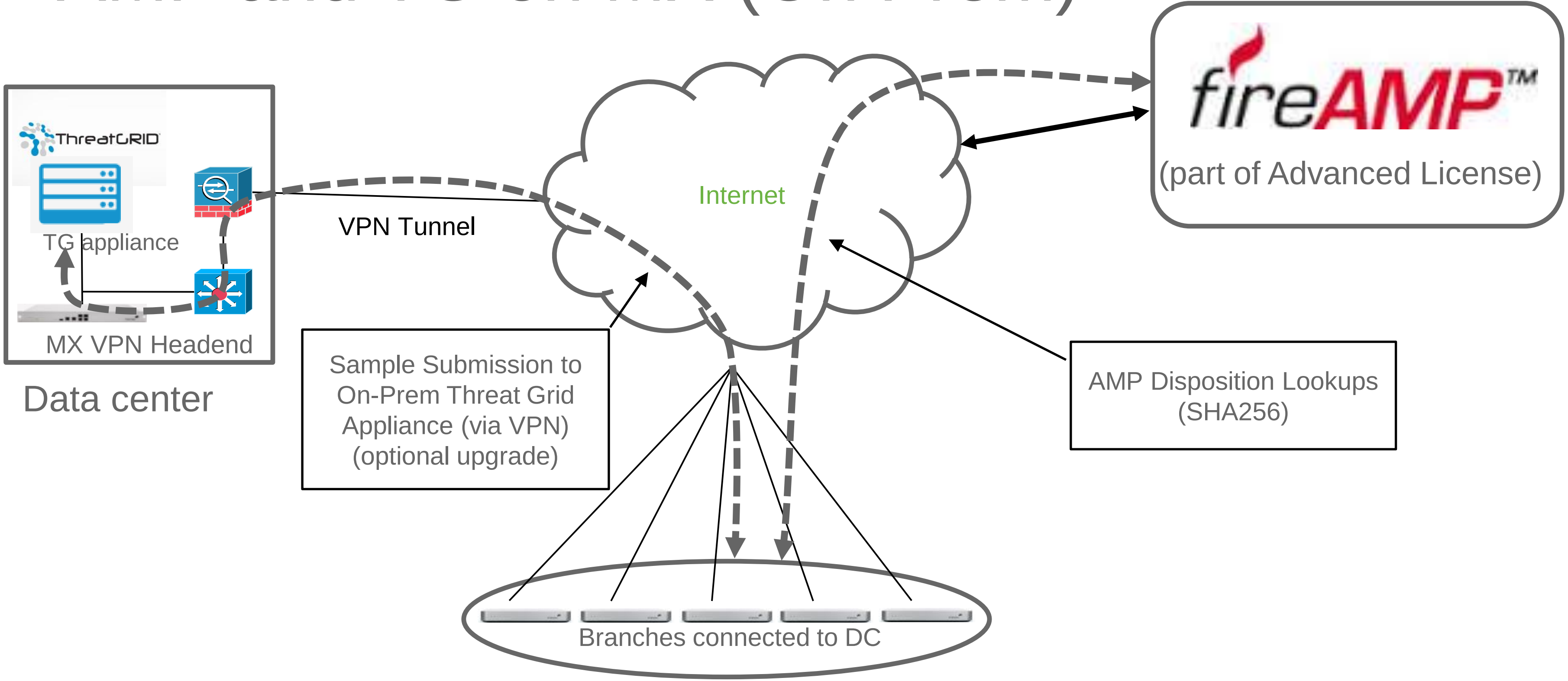
ThreatGrid in the Cloud



1. MX inspects file transfers in-line and extracts files from flows
2. MX calculates SHA-256 from file and sends the file reputation lookup to AMP cloud
3. AMP Cloud determines if the file is known malicious, known good or unknown

5. If executable or document is still suspicious (unknown, analyzable, contains risky content), it is sent to AMP Threat Grid cloud for dynamic analysis, file transfer will be allowed at this time
6. AMP Threat Grid runs or opens the file in a controlled, monitored VM and allows malware to connect to Internet and download additional files
7. If TG analysis determines a threat score >95, then AMP Cloud is updated (poked) to mark file as malicious
8. AMP Cloud sends a Retrospective event to MX (respectively the Dashboard) to highlight the occurrence of a malicious file that was not blocked

AMP and TG on MX (On Prem)



(part of Advanced License)

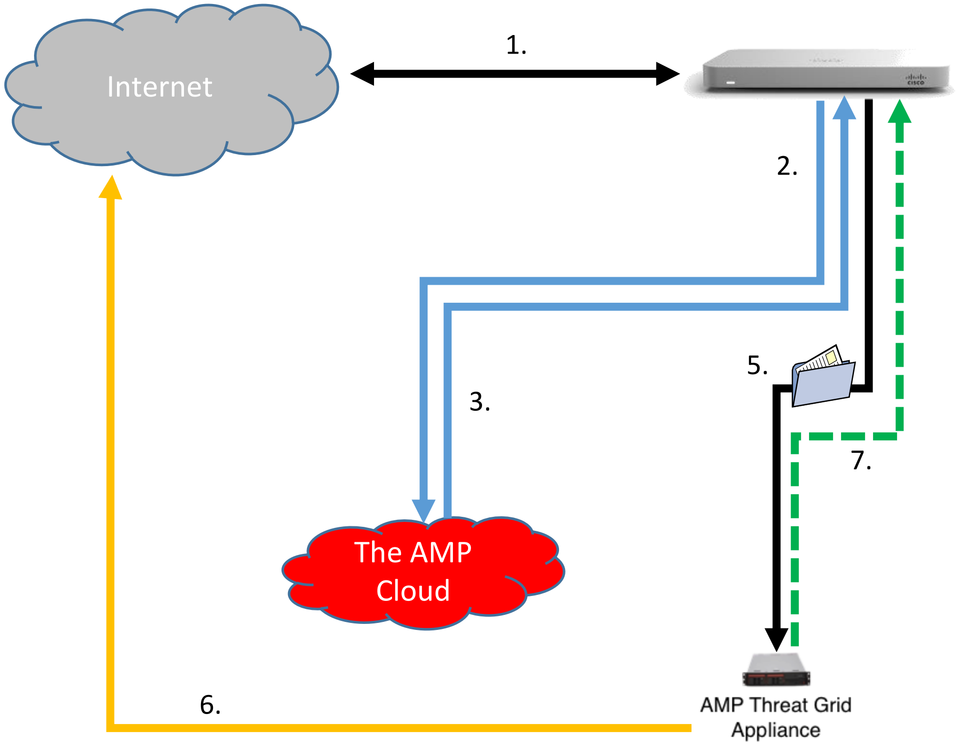
Data center

Sample Submission to On-Prem Threat Grid Appliance (via VPN) (optional upgrade)

AMP Disposition Lookups (SHA256)

Meraki MX – AMP ThreatGrid Process Flow

ThreatGrid on-prem appliance



1. MX inspects file transfers in-line and extracts files from flows

2. MX calculates SHA-256 from file and sends the file reputation lookup to AMP cloud

3. AMP Cloud determines if the file is known malicious, known good or unknown

5. If executable or document is still suspicious (unknown, analyzable, contains risky content), it is sent to AMP Threat Grid appliance for dynamic analysis, file transfer will be allowed at this time

6. AMP Threat Grid appliance runs or opens the file in a controlled, monitored VM and allows malware to connect to Internet and download additional files

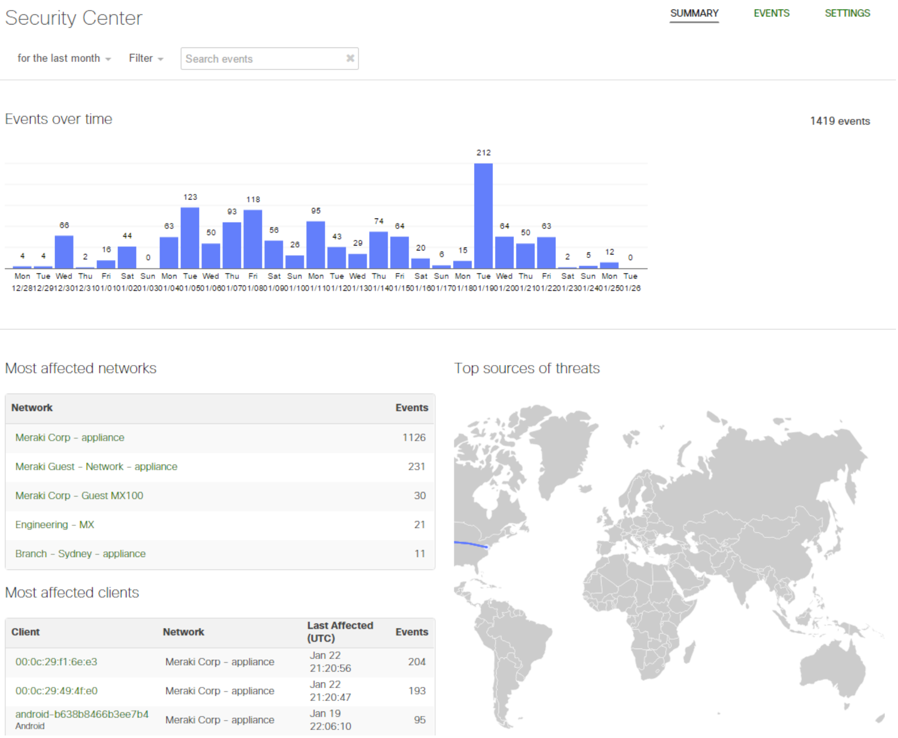
7. MX polls TG appliance periodically to fetch the result, if TG analysis determines a threat score >95, then MX receives a malicious disposition

Details

- No file storage => upsell to ThreatGrid
- All AMP / TG filetypes are supported
  - AMP: SWF, ZIP, MSOLE2, MSCAB, PDF, EXE, ELF, MACHO, MACHO UNIBIN, JAVA
  - TG: PE executables, DLLs, PDF, MS office documents (RTF, DOC, PPT(X)), ZIP
- Only dynamic file submission (no manual submission)
- No perceived delay to the end user
- Retrospection is supported (current max is 2 weeks)

New Security Center (replaces Security Reports)

- All security-related events in one place
- Pivot on the client, network, threat or remote source
- Quickly identify clients and networks that are potentially infected
- Identify threats that appear across multiple networks



Most affected networks

Network	Events
Meraki Corp – appliance	1126
Meraki Guest – Network – appliance	231
Meraki Corp – Guest MX100	30
Engineering – MX	21
Branch – Sydney – appliance	11

Most affected clients

Client	Network	Last Affected (UTC)	Events
00:0c:29:f1:6e:e3	Meraki Corp – appliance	Jan 22 21:20:56	204
00:0c:29:49:4f:e0	Meraki Corp – appliance	Jan 22 21:20:47	193
android-b638b8466b3ee7b4 Android	Meraki Corp – appliance	Jan 19 22:06:10	95

MX Security Appliances: Licenses

Enterprise License

- Stateful firewall
- Site to site VPN
- Branch routing
- Internet load-balancing (over dual WAN)
- Application control
- Web caching
- Intelligent WAN (IWAN)
- Client VPN

Advanced Security License

All enterprise features, plus

- Content filtering (with Google SafeSearch)
- Kaspersky Anti-Virus and Anti-Phishing
- SourceFire IPS / IDS
- Geo-based firewall rules

Meraki MX License options comparison

Cloud TG Basic

- Meraki advanced security
- AMP TG per box license

- Submission through MX dashboard
- Access to TG report
- Basic search through submitted files

Cloud TG Full

- Meraki advanced security

- TG cloud subscription license

- Access to TG portal for submission and data base search
- Threat Intelligence context and correlation
- Cloud API access for submission and search
- AMP TG feeds
- Glovebox, video, process map, JSON reports, sample runtime adjustment

On-premise TG Full

- Meraki advanced security

- TG appliance
- TG appliance subscription

- Can be headless or with appliance subscription
- Appliance UI and API access
- Threat Feeds
- Cloud API for database search
- Glovebox, video, process map, JSON reports, sample runtime adjustment

HA
Internet
LAN
Reset
USB
Management
Internet
meraki
meraki