



Distribution
Partner

Cisco Security Portfolio

Ionut Davidoiu – Pre-Sales Engineer
Ianuarie 2015



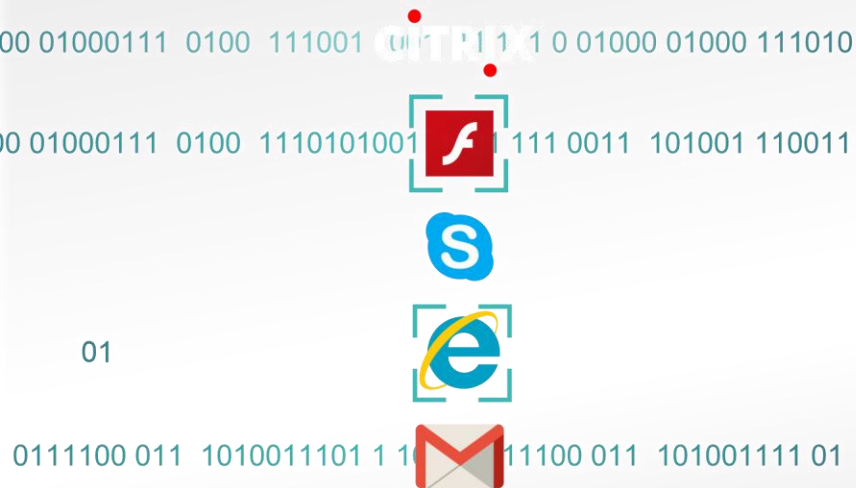
Agenda

- ASA with FirePower
- SourceFire AMP

The Problem with Legacy Next-Generation Firewalls

Focus on the Apps...

...But Miss the Threat



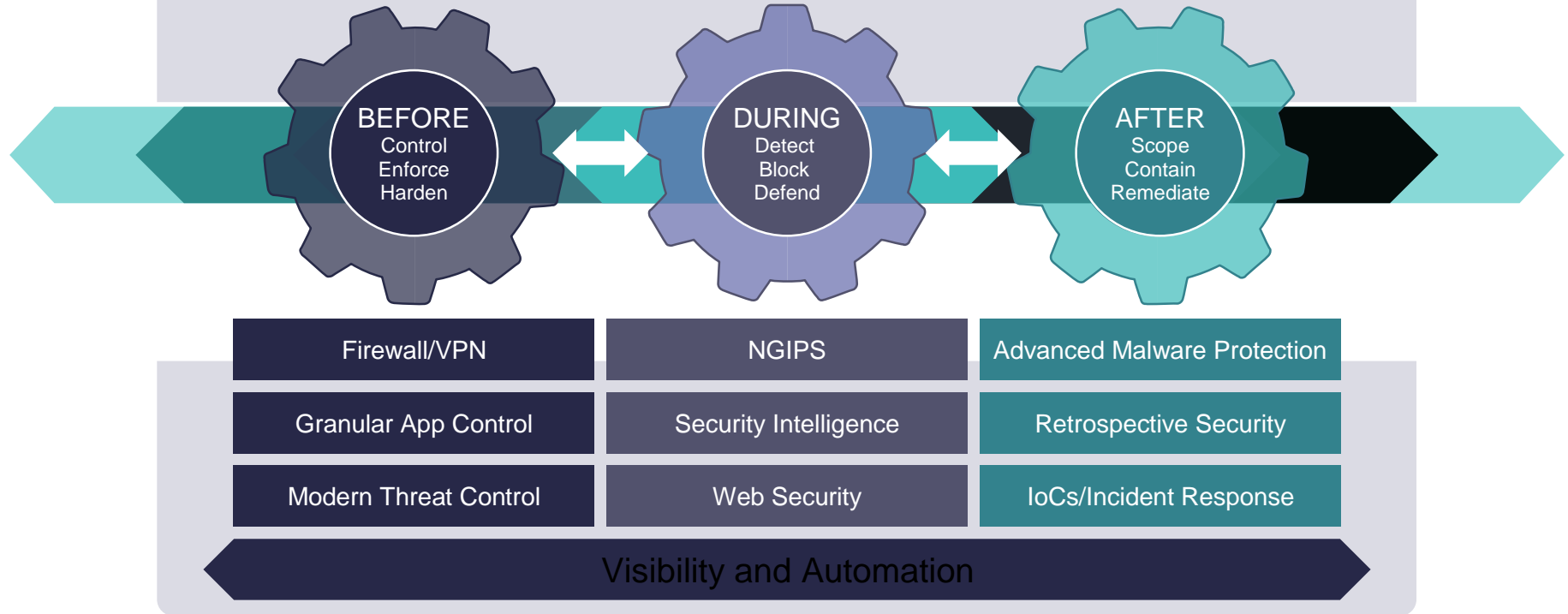
101 010011101 1100001110001110 1001 1101 1110011 01100

1100001 1100 0111010011101 1100001110001110 1001 1101

Legacy NGFWs can reduce attack surface area but advanced malware often evades security controls.

Integrated Threat Defense Across the Attack Continuum

Attack Continuum



Cisco Multi-scale Performance

Security for the Internet Edge

Note: Impact of FirePOWER services on throughput will be covered in the performance section of this course.

1 Gbps Max
100K Connections
10,000 CPS



ASA 5512-X

1.2 Gbps Max
250K Connections
15,000 CPS



ASA 5515-X

Branch Locations

2 Gbps Max
500K Connections
20,000 CPS



ASA 5525-X

3 Gbps Max
750K Connections
30,000 CPS



ASA 5545-X

4 Gbps Max
1M Connections
50,000 CPS



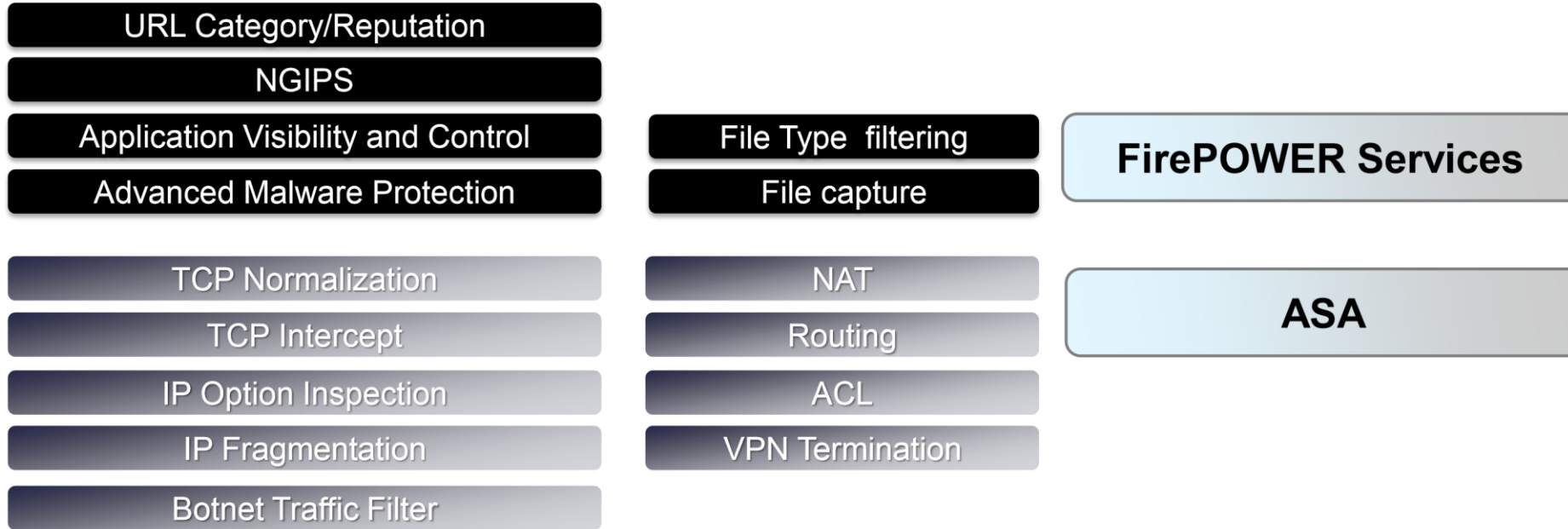
ASA 5555-X

Small / Medium Internet Edge

FireSIGHT Management Center

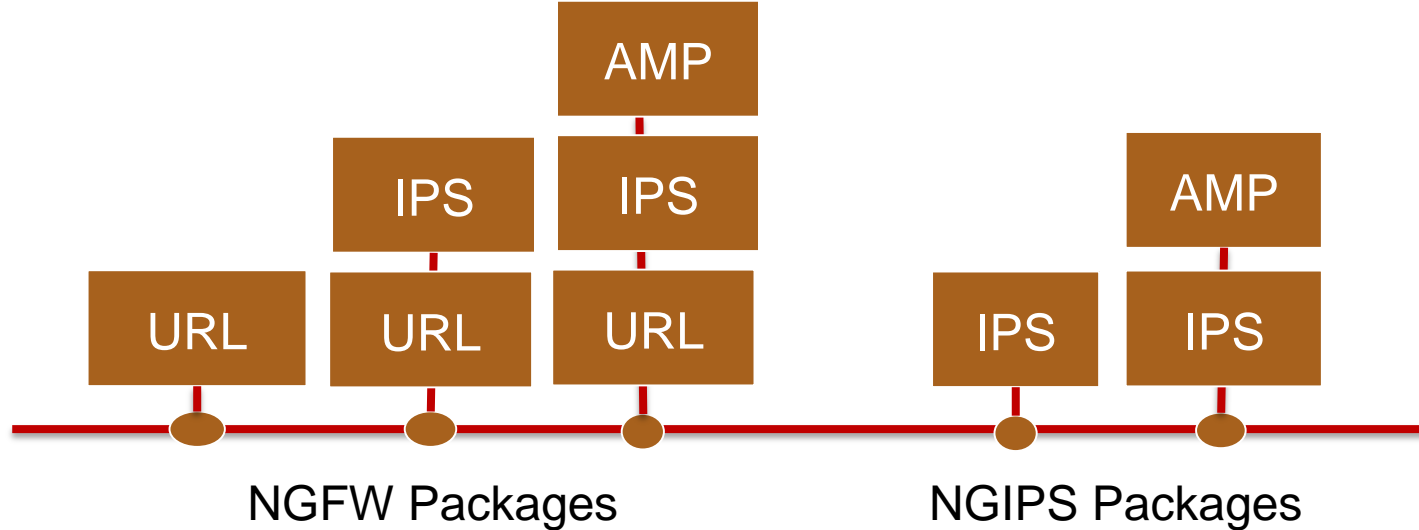
- Required for management of network discovery information, correlated events and the AVC, IPS, URL and AMP functionality.
- The number of sensors to be managed and the event and file storage will determine sizing requirements.

Functional Distribution of Features



Licensing

- Five (5) feature license packages are available
- AVC is part of the default offering
- One (1) and three (3) year terms are available
- SMARTnet is ordered separately with the appliance



Cisco FirePOWER Brings Superior Network Visibility

	Threats	Users	Web Applications	Application Protocols	File Transfers	Malware	Command and Control Servers	Client Applications	Network Servers	Operating Systems	Routers and Switches	Mobile Devices	Printers	VoIP Phones	Virtual Machines
Cisco® FirePOWER Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Typical IPS	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Typical NGFW	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

Impact Assessment

Correlates all intrusion events
to an impact of the attack against the target



Impact Flag

Administrator Action

Why



1

Act immediately;
vulnerable

Event corresponds
to vulnerability
mapped to host



2

Investigate;
potentially vulnerable

Relevant port open
or protocol in use,
but no vulnerability
mapped



3

Good to know;
currently not
vulnerable

Relevant
port not
open or
protocol
not in use



4

Good to know;
unknown target

Monitored network,
but unknown host



0

Good to know;
unknown network

Unmonitored
network

21

AMP Provides Continuous Retrospective Security

Telemetry Stream



File fingerprint and metadata



File and network I/O



Process information



Breadth of Control Points



Email



Endpoints



Web



Network














IPS



Devices

Indications of Compromise (IoCs)

Indications of Compromise (3)						 Edit Rule States		 Mark All Resolved	
Category	Event Type	Description		First Seen	Last Seen				
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit		 2013-09-17 16:46:28	 2013-09-20 06:35:31				
CnC Connected	Security Intelligence Event - CnC	The host may be under remote control		 2013-09-17 16:52:11	 2013-09-20 03:55:45				
CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control		 2013-09-17 20:09:23	 2013-09-19 17:32:49				

Monitor detections

- Exploit kits
- Web app attacks
- CnC connections
- Admin privilege escalations

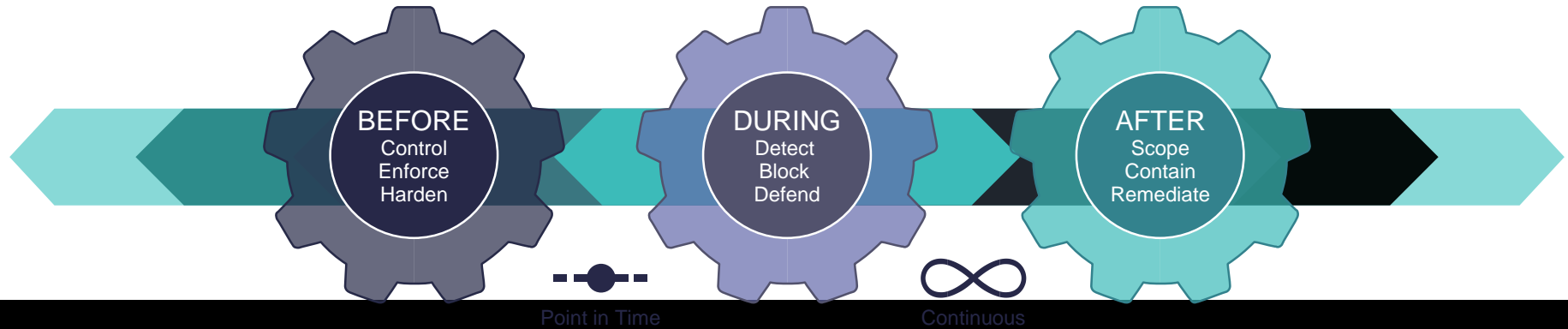
Connections

- to known CnC IPs

Monitor detections

- Office/PDF/Java compromises
- Malware executions
- Dropper infections

Protection Before, During, and After an Attack



With Superior Visibility, Control, and Advanced Threat Remediation Functionality



Retrospection



Retrospective Detection



Behavioral Indications
of Compromise



Trajectory



Threat Hunting

Migration Opportunity

Why migrate to ASA 5500-X NGFW?

\$2.5+ Billion Opportunity!

Protect your install base

**More value/stickiness and
differentiation**

What's in it for partners?



Increase cross sell and up-sell opportunities

Opportunity to sell value added services and support

Why Upgrade?

5 models to meet varied throughput demands



ASA 5555-X



4 Gbps FW Throughput

ASA 5545-X



3 Gbps FW Throughput

ASA 5525-X



2 Gbps FW Throughput

ASA 5515-X



1.2 Gbps FW Throughput

ASA 5512-X
1 Gbps FW Throughput

High Performance

- Up to 4X faster than legacy ASA
- Increased throughput, CPS, sessions

Accelerated, integrated services

- Integrated security acceleration hardware
- No extra hardware required (security services enabled with software licenses)

Next-generation security

- Application control (A

VC)

- Next-Generation IPS
- Security intelligence and URL Filtering
- Advanced Malware Protection

*VPN and IPS acceleration hardware available on select ASA models (ASA 5525-X, 5545-X, 5555-X)

Competitive Overview - NGFW

By Way of Comparison...

can do this...

- Requires 10 unique products and 8 unique management interfaces
- There is minimal correlation of information, of course

can do this...

- Requires four 3rdparty products and 7 unique management interfaces
- ... no correlation...

can do this...

- Like Palo Alto—they need 3rd-party help—at minimum there will be 5 unique management interfaces
- You guessed it — no correlation

and many others...

- Can't do this without using one of solutions to the left! (or Cisco)



How Palo Alto Does It:



1

PanOS or Panorama NGFW Manager

2

WildFire Portal (VERY basic Sandbox)

3

GlobalProtect / Cyvera Client Agent (Windows Only)

3

Bit9 for the rest

4

PickYourFav Vulnerability Mgmt. QualysGuard

5

PickYourFav - SIEM Logging - Splunk

6

PickYourFav Remediation (Soc)

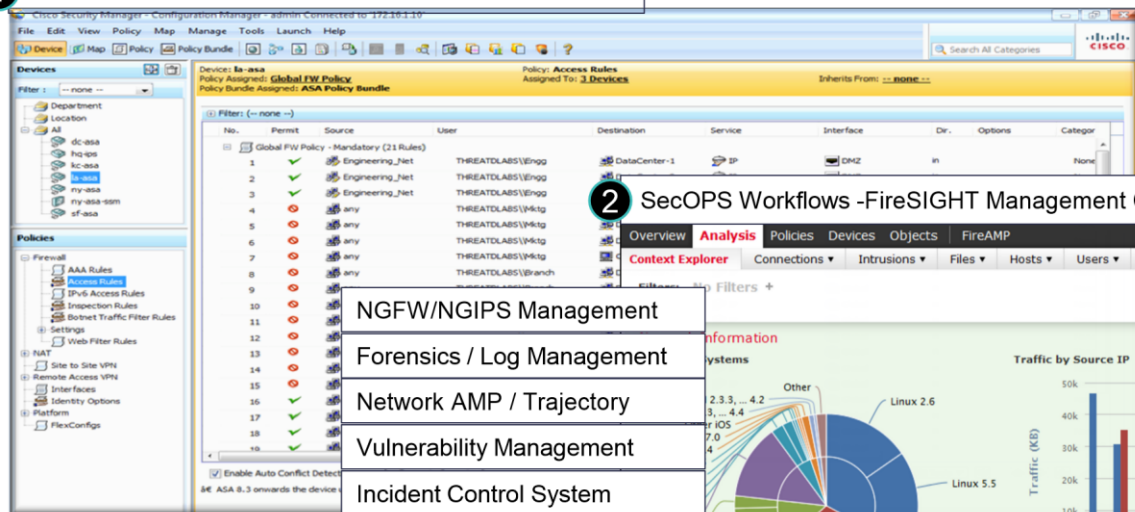
7

PickYourFav Anti-Malware Remediation

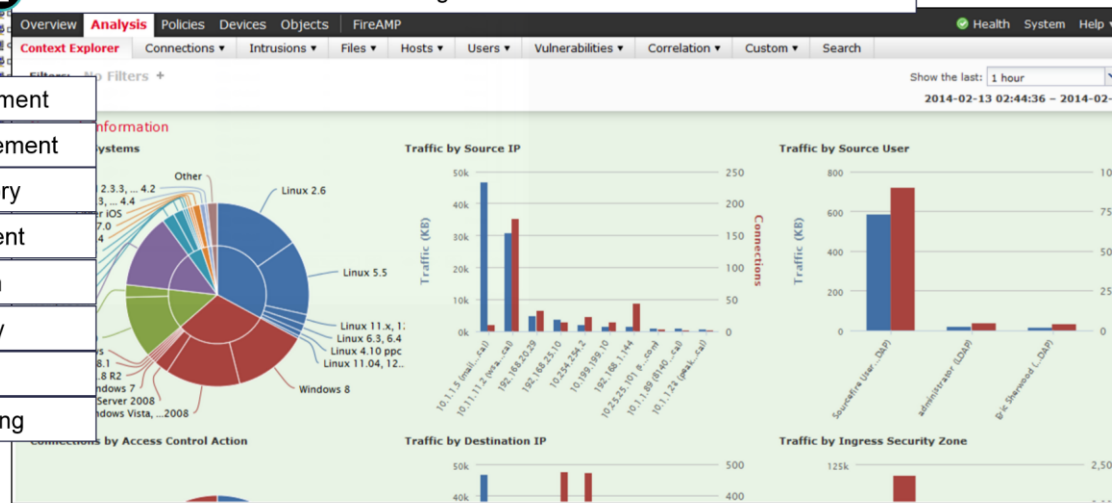
8

Optional But Recommended - Choose a 'Working' Sandbox tool - Like FireEye

1 NetOPS Workflows - CSM 4.6 or ASDM-ASA-On-Box



2 SecOPS Workflows -FireSIGHT Management Center



NGFW/NGIPS Management

Forensics / Log Management

Network AMP / Trajectory

Vulnerability Management

Incident Control System

Adaptive Security Policy

Retrospective Analysis

Correlated SIEM Eventing

How Cisco Does it

Key Differentiators

Key Objection: Fortinet lacks contextual awareness

	Cisco	Fortinet
User Identity Tracking	✓	Limited ⁴
Custom Rules / Signatures	✓	Limited ⁵
Impact Assessment	✓	X
Automated IPS Tuning	<div>✓</div>	X
Network Behavior Analysis	✓	Limited ²
Enterprise Management	✓	Limited
SSL Decryption	✓	Limited ³

1 – Traditional AV inspection only, IPS may detect C&C, no correlation between the two
2 – Separate DDoS appliance, no correlation
3 – Limited
4 – Limited
5 – Limited



Reasons to Choose Cisco over



1. Proven year-over-year protection from threats

- Cisco has achieved leading protection ratings for the past four years [NSS Labs 2009-2012]
- Fortinet scored well in the most recent test, but has a poor track record YoY

2. Better enterprise management

- Cisco management platforms are enterprise proven with an intuitive user interface and analysis workflows
- Management is Fortinet's Achilles heel, complex and non-intuitive

3. Security events with contextual information

- Cisco adds context to events with network, host, application, and user information
- Fortinet events lack context—No OS or device type information

4. Impact Analysis

- Cisco automates event analysis and presents the most critical events first
- Fortinet lacks correlation capabilities, requiring 3rd party tools to perform incident analysis

5. Performance in next-generation configurations

- Cisco outperforms our own perf. ratings in independent tests
- Fortinet underperforms their stated performance [NSS Labs 2012 / IPS 6.2]

Cisco Demo Cloud (dCloud)



- Complete, 'LIVE' environment
- Live traffic, clients and threats
- Easy to use
- Demo script in your dashboard

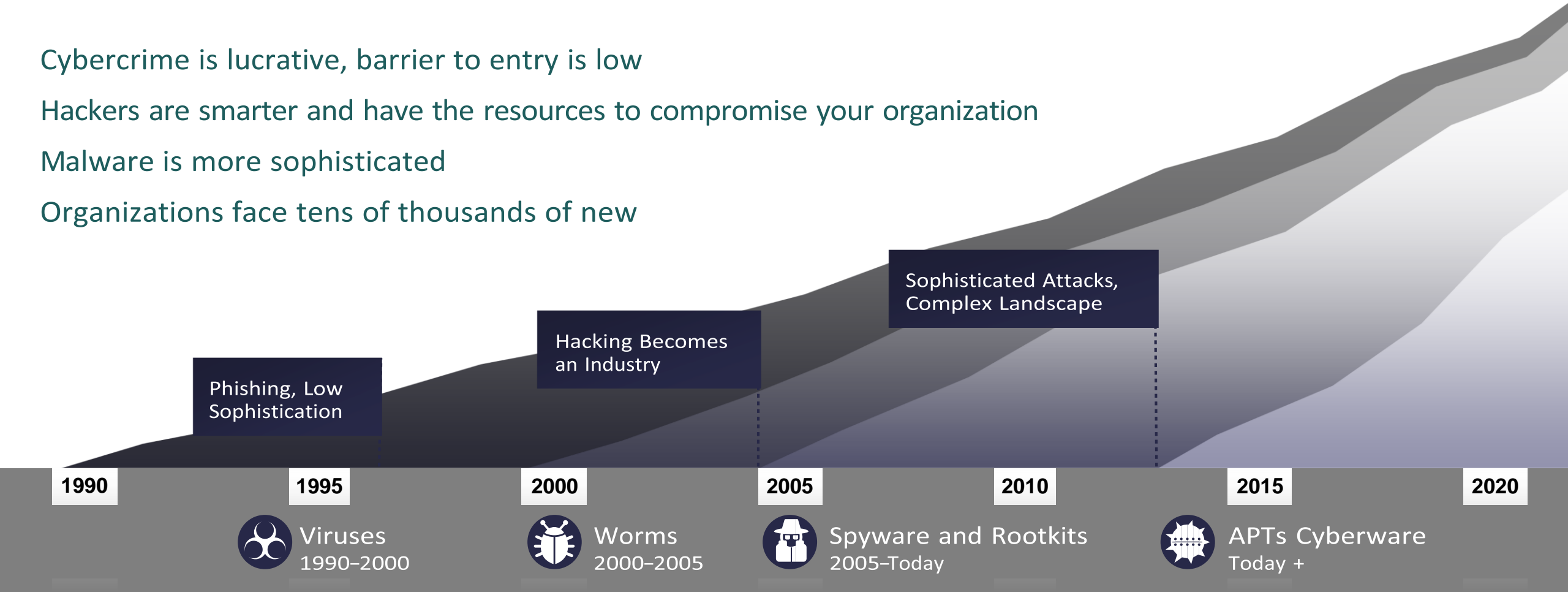


Visit: dcloud.cisco.com

Malware is an ever-growing problem



- Cybercrime is lucrative, barrier to entry is low
- Hackers are smarter and have the resources to compromise your organization
- Malware is more sophisticated
- Organizations face tens of thousands of new



Malware is an ever-growing problem

95%

of large companies
targeted by malicious traffic



100%

of organizations interacted
with websites hosting malware



The Washington Post

March 24, 2014

U.S. notified 3,000 companies in 2013 about cyberattacks

Federal agents notified more than 3,000 U.S. companies last year that their computer systems had been hacked, White House officials have told industry executives, marking the first time the government has revealed how often it tipped off the private sector to cyberintrusions.

The New York Times

April 7, 2014

Hackers Lurking in Vents and Soda Machines

SAN FRANCISCO — They came in through the Chinese takeout menu.

Unable to breach the computer network at a big oil company, hackers infected with malware the online menu of a Chinese restaurant that was popular with employees. When the workers browsed the menu, they inadvertently downloaded code that gave the attackers a foothold in the business's vast computer network.

Security experts summoned to fix the problem were not allowed to disclose the details of the breach, but the lesson from the incident was clear: Companies scrambling to seal up their systems from hackers and government snoops are having to look in the unlikelyst of places for vulnerabilities.

Hackers in the recent Target payment card breach gained access to the retailer's records through its heating and cooling system. In other cases, hackers have used printers, thermostats and videoconferencing equipment.

CIO Journal.

Damage to an organization and its customers happens at light speed, which means senior leaders have to react at light speed to limit the mayhem and protect the organization. Decisions with potentially huge cost and brand implications must be made immediately. Leaders must determine how much liability looms, and how much investment in remediation is needed to account for that.

February 4, 2014

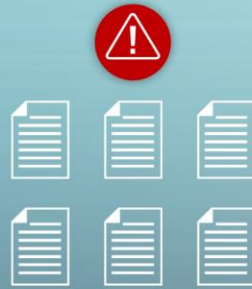
Impact of a Breach

Breach occurs



START

60% data is stolen in hours



HOURS

54% of breaches remain undiscovered for months



MONTHS

Information of up to **750 million** individuals on the black market over last three **years**



YEARS

Source: Verizon Data Breach Report 2014

Selecting your malware protection technology based upon detection rates is really just selecting your method of failure...

Why has detection failed?

- Malware no longer infects as individual files
- The initial virus is often bespoke – custom written for a single attack campaign
- Once the infection has taken place, more unique malware is downloaded and the cycle is repeated.

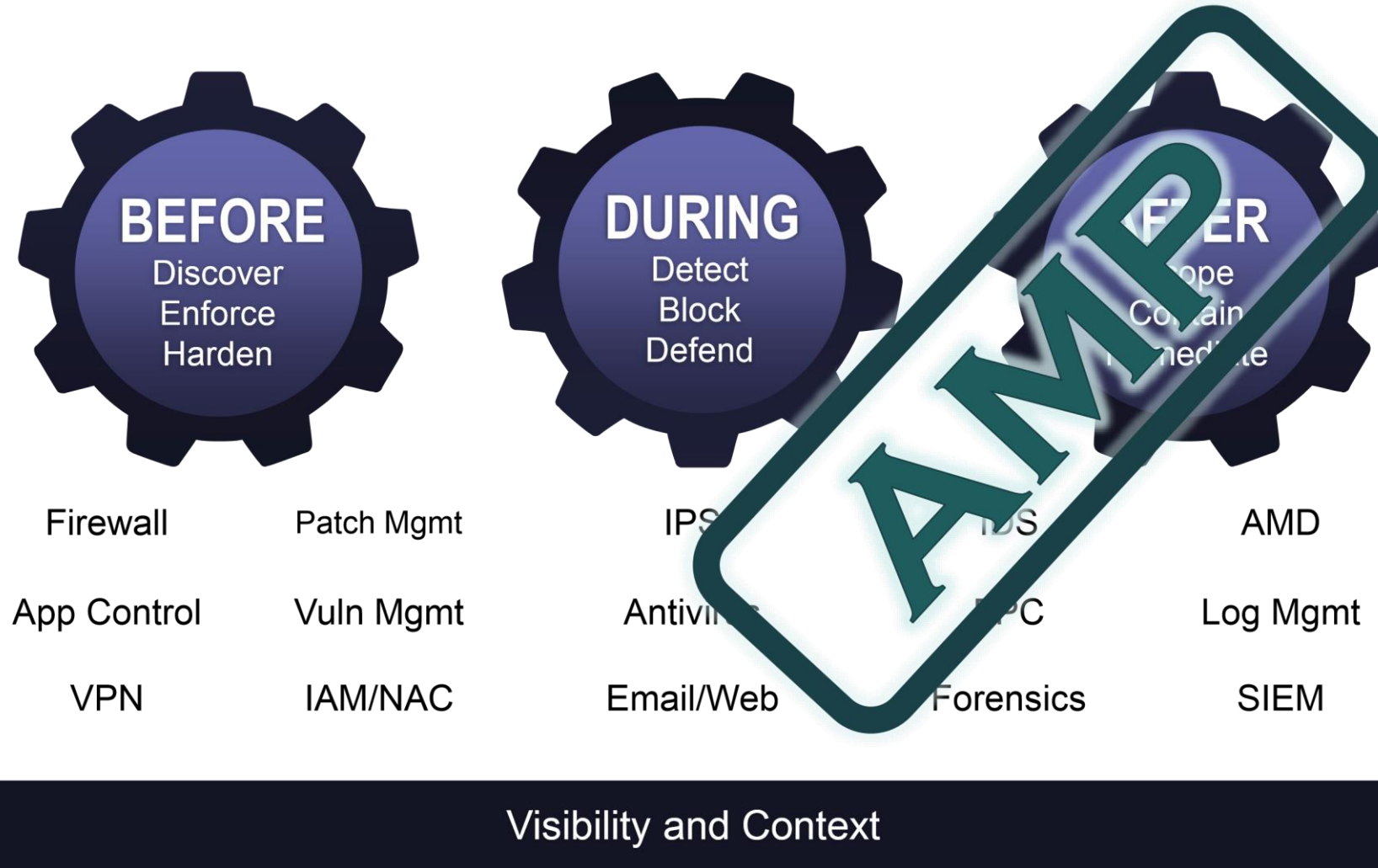
- Local detection lacks the processing power, storage and perspective necessary
- The bad-guys are clever, resourceful and well motivated



If you knew you were going to be compromised, would you do security differently?
It's time for a new approach...

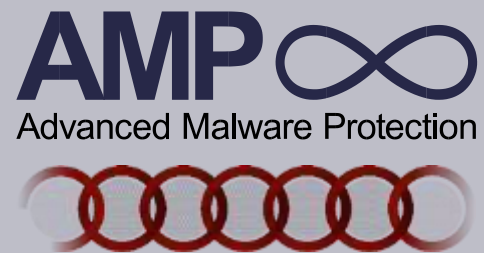
The New Security Model

Attack Continuum



Comprehensive Environment Protection with AMP

Cisco
Advanced
Malware
Protection



AMP
Protection



Content



Network



Endpoint

Threat Vector

Email and Web

Networks

Devices

Method

License with ESA or WSA

Stand Alone Solution
-or-
Enable AMP on FirePOWER
Appliance

Install on endpoints

Ideal for

New or existing Cisco Email or
Web Security customers

IPS/NGFW customers

Windows, Mac, Android, VMs

Cisco Advanced Malware Protection

Built on unmatched collective security intelligence



0011 0110011 101000 0110 00
000 0111000 111010011 101 11
1001 1101 1110011 0110011 101



0011 0110011 101000
000 0111000 111010011 101 11
1001 1101 1110011 0110011 101



www

Email	Endpoints	Web	Networks	IPS	Devices
1.6 million global sensors			35% worldwide email traffic		
100 TB of data received per day			13 billion web requests		
150 million+ deployed endpoints			24x7x365 operations		
600+ engineers, technicians, and researchers			40+ languages		

8 – 10 million samples per month sandboxed

180,000+ File Samples per Day

FireAMP™ Community

Advanced Microsoft and Industry Disclosures

Snort and ClamAV Open Source Communities

Honeypots

Sourcefire AEGIS™ Program

Private and Public Threat Feeds

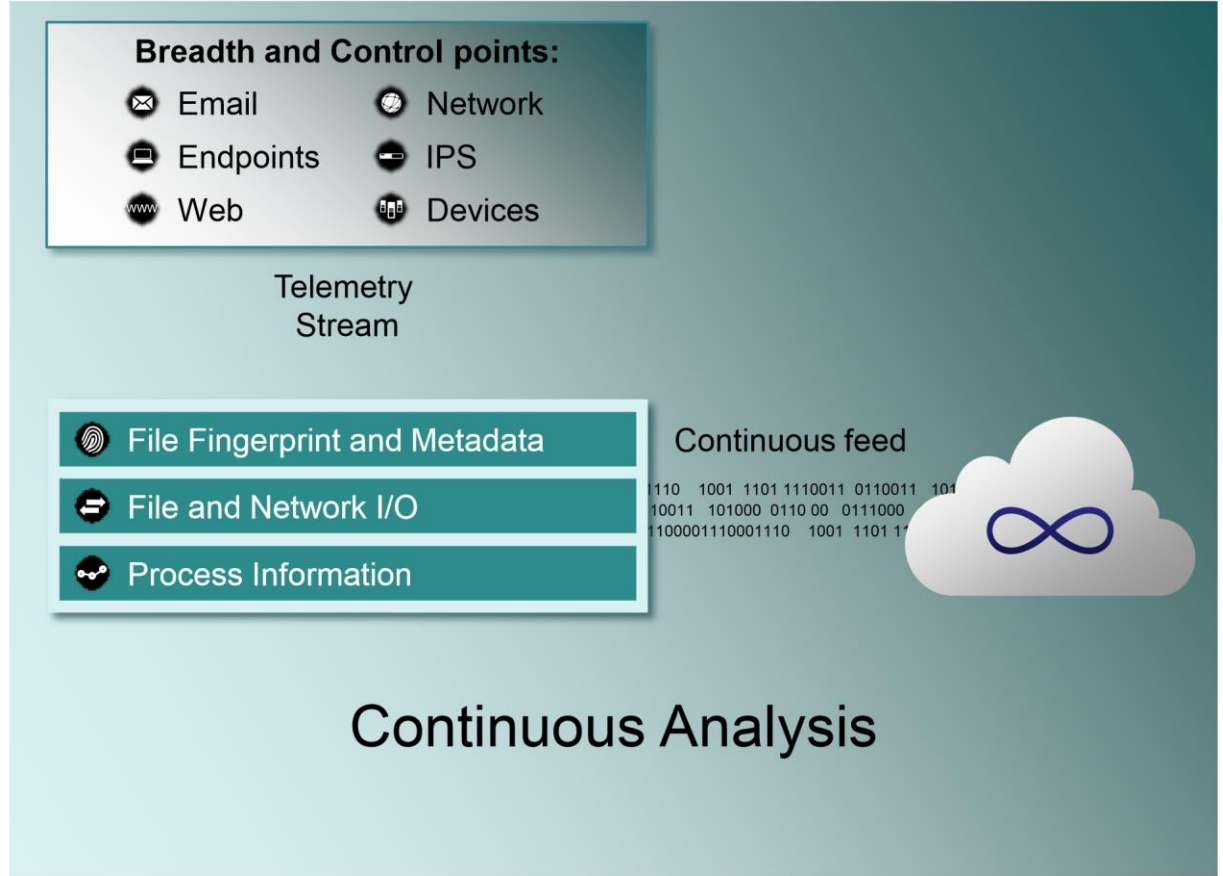
Dynamic Analysis



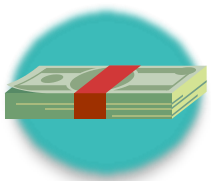
AMP Offers Point-in-Time and Continuous Protection

Point-in-Time Protection

Retrospective Security



Traditional Incident Response is Tough



High Cost of Response – Average cost of responding to a breach is over \$500,000, but costs can skyrocket into the millions of dollars



Too many tools to manage – Proliferation of tools in place, all with their own consoles, making an integrated response difficult



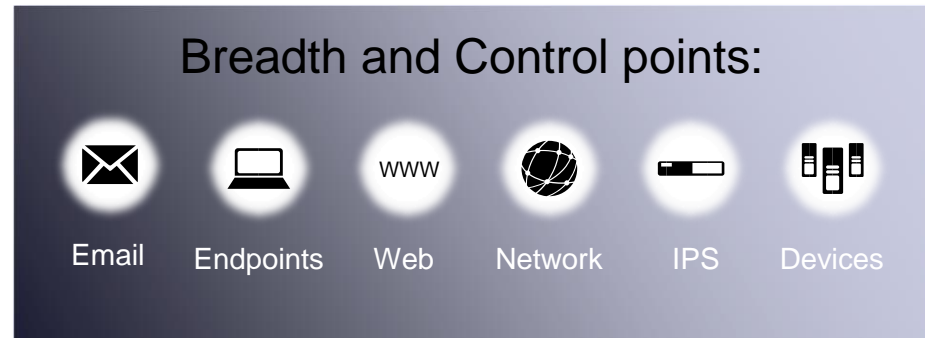
High volume of alerts – It is impossible to effectively manage the countless events generated daily



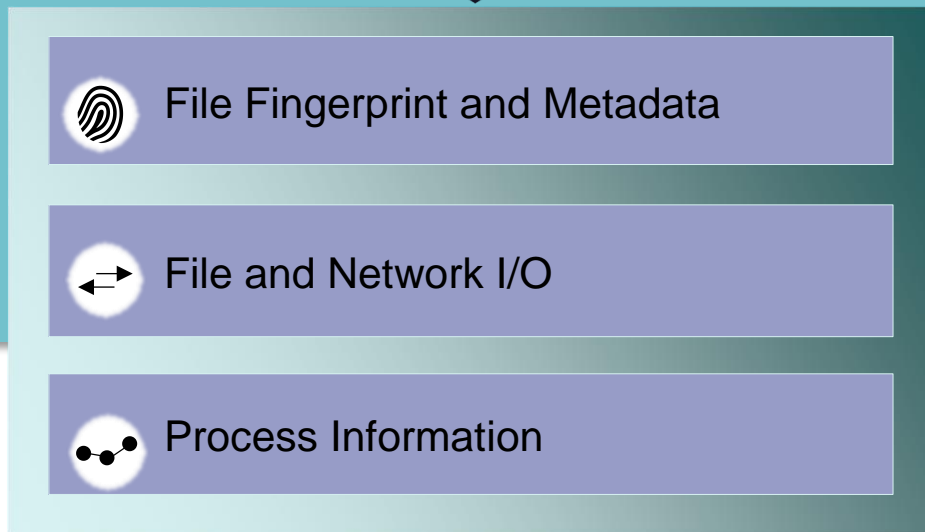
Time – Without the right tools, response takes time and actionable data can decay in minutes or even seconds

Where do I start?

Continuous Analysis



Telemetry Stream



Recording...

Watching...



ALL FILES...

Continuous feed


01110100111011100001110001110 1001 1101 1110011 011
01110 1001 1101 1110011 0110011 101000 0110 00 011
1100001 1100 0111010011101 1100001110001110 1001 11




Continuous analysis

Network File Trajectory for 70a9e87b...2de3d830

File SHA-256

70a9e87b...2de3d830 


First Seen

2014-10-23 09:02:47 on  [10.131.12.76](#)

File Names

[Alureon.exe](#) , [Captiva.exe](#) , [Conhook.exe](#) , [Cridex.exe](#) (+1 more) (+40 more)
(+9 more) (+8 more)

Last Seen

2014-10-23 09:02:47 on  [10.0.108.78](#)

File Type

[MSEXE](#)

Event Count

12

File Category

[Executables](#)

Seen On

13 hosts


Current Disposition

 [Malware](#) 

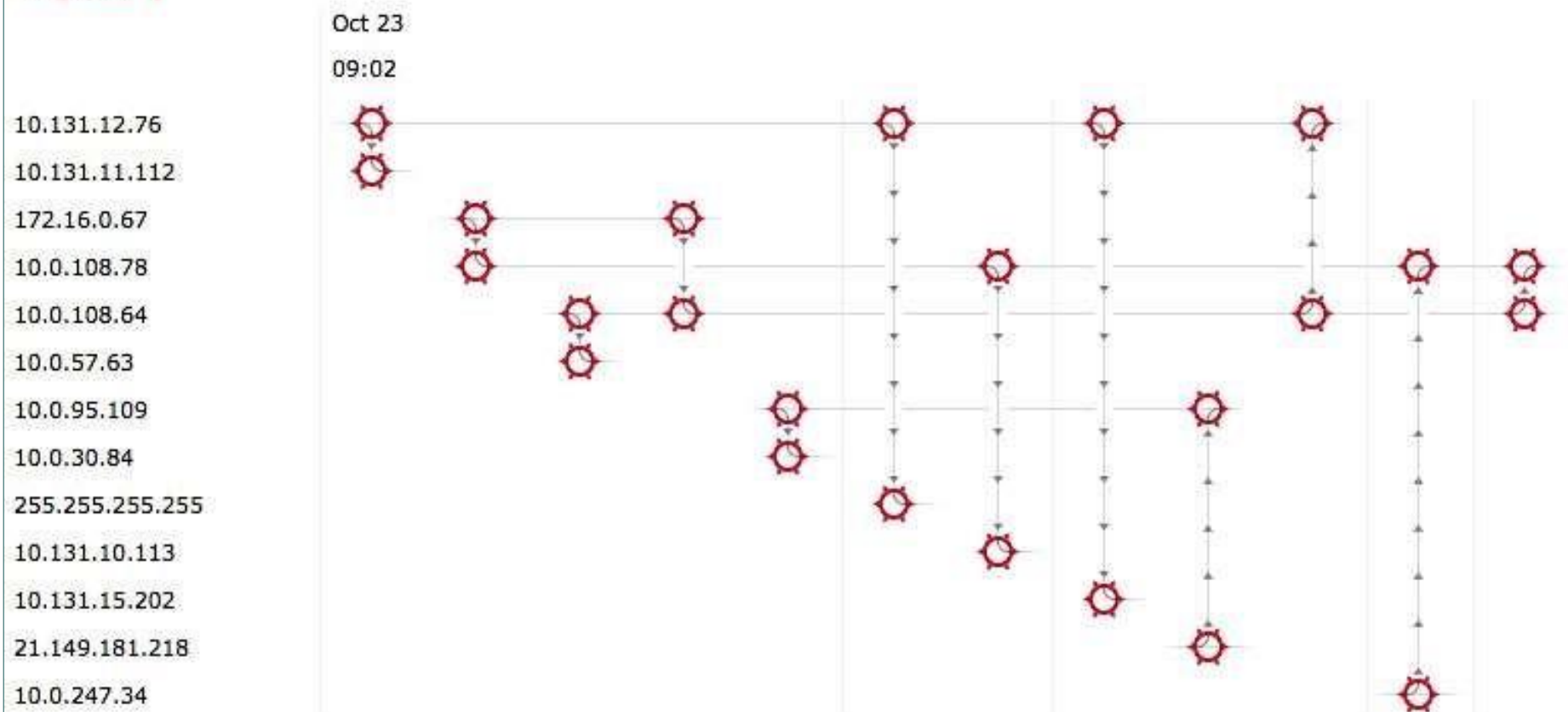
Seen On Breakdown

7 senders → 10 receivers

Threat Score

None 

Trajectory

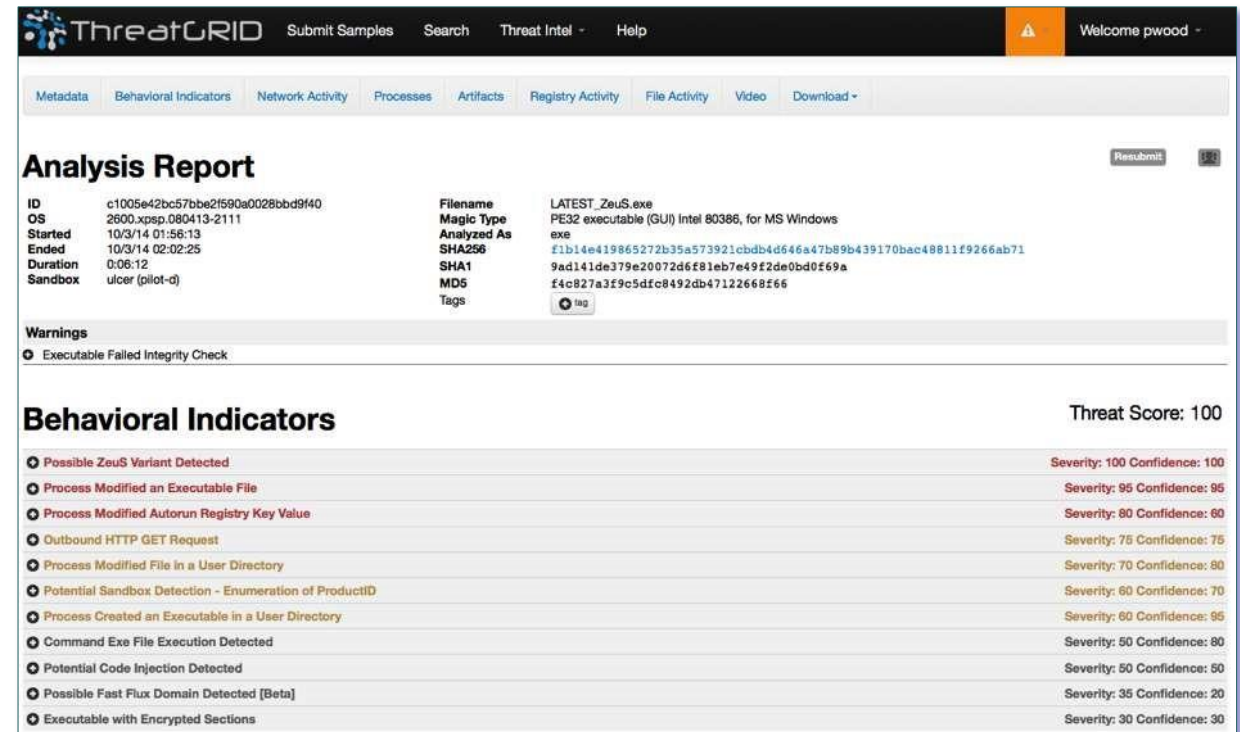


What did the threat do?

- Gives you detailed view of sample behaviour
- No presence in the VM like other sandboxes
- 300+ Behavioural indicators (and growing)
- Malware families, malicious behaviours and more
- Detailed description, actionable
- Prioritize threats with confidence
- Increases speed and accuracy of incident response teams

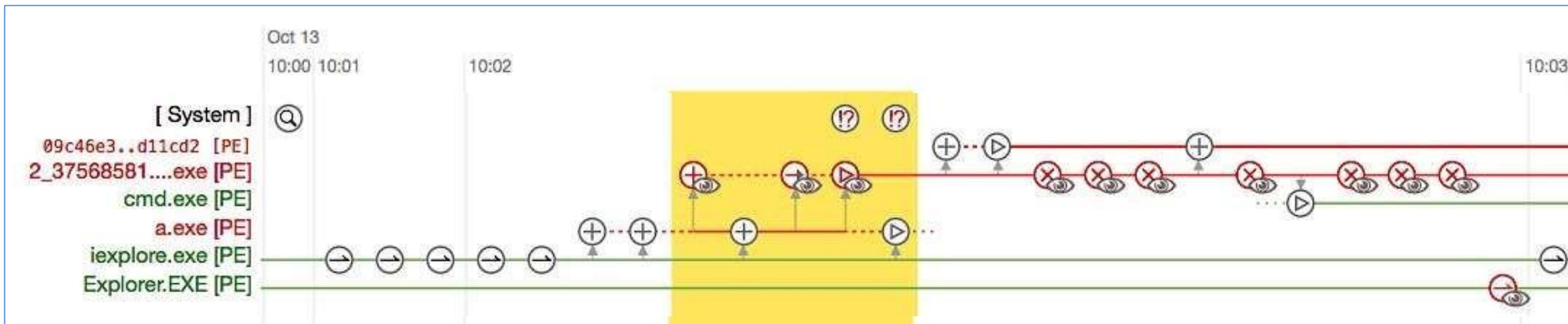
What did the threat do?

- Review a historical record of what a device is doing...



The screenshot shows the ThreatGRID web interface. At the top is a navigation bar with links for Submit Samples, Search, Threat Intel, and Help. Below this is a tabbed interface with options like Metadata, Behavioral Indicators, Network Activity, Processes, Artifacts, Registry Activity, File Activity, Video, and Download. The main content area displays an 'Analysis Report' for a file named 'LATEST_ZeuS.exe'. The report includes metadata such as ID, OS, Started, Ended, Duration, and Sandbox. It also lists file details like Magic Type, Analyzed As, SHA256, SHA1, MD5, and Tags. A 'Warnings' section indicates a failed integrity check. The 'Behavioral Indicators' section lists various actions detected, such as 'Possible ZeuS Variant Detected' and 'Process Modified an Executable File', each with associated severity and confidence scores. A 'Threat Score: 100' is displayed at the top right of the behavioral indicators section.

Analysis Report	
ID	c1005e42bc57bbe2f590a0028bbd9f40
OS	2600.xp.sp.080413-2111
Started	10/3/14 01:56:13
Ended	10/3/14 02:02:25
Duration	0:06:12
Sandbox	ulcer (pilot-d)
Filename	LATEST_ZeuS.exe
Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows
Analyzed As	exe
SHA256	f1b14e419865272b35a573921cbbd4d646a47b89b439170bac48811f9266ab71
SHA1	9ad141de379e20072d6f81eb7e49f2de0bd0f69a
MD5	f4c827a3f9c5dfc8492db47122668f66
Tags	
Warnings	
Executable Failed Integrity Check	
Behavioral Indicators	
Threat Score: 100	
Possible ZeuS Variant Detected	Severity: 100 Confidence: 100
Process Modified an Executable File	Severity: 95 Confidence: 95
Process Modified Autorun Registry Key Value	Severity: 80 Confidence: 60
Outbound HTTP GET Request	Severity: 75 Confidence: 75
Process Modified File in a User Directory	Severity: 70 Confidence: 80
Potential Sandbox Detection - Enumeration of ProductID	Severity: 60 Confidence: 70
Process Created an Executable in a User Directory	Severity: 60 Confidence: 95
Command Exe File Execution Detected	Severity: 50 Confidence: 80
Potential Code Injection Detected	Severity: 50 Confidence: 50
Possible Fast Flux Domain Detected [Beta]	Severity: 35 Confidence: 20
Executable with Encrypted Sections	Severity: 30 Confidence: 30



-

How do we recover?

- Simple Custom Detections
- Quickly and easily write custom signatures
- Advanced Detections

- Create Clam AV signatures

Simple Custom Detections

+ Create

Quick SCD

2 files added

Created by Phil Wood on 2014-09-22 09:47

Used in policies: Audit Policy, Protect Policy, Triage Policy, Server Policy, Domain Controller Policy

Used on groups: Audit, Domain Controller, Protect, Server, Triage

Edit

Remove

Quick SCD

Save

Add SHA-256

Add a file by entering the SHA-256 of that file.

Upload File

Upload File To List

Upload Set of SHA-256's

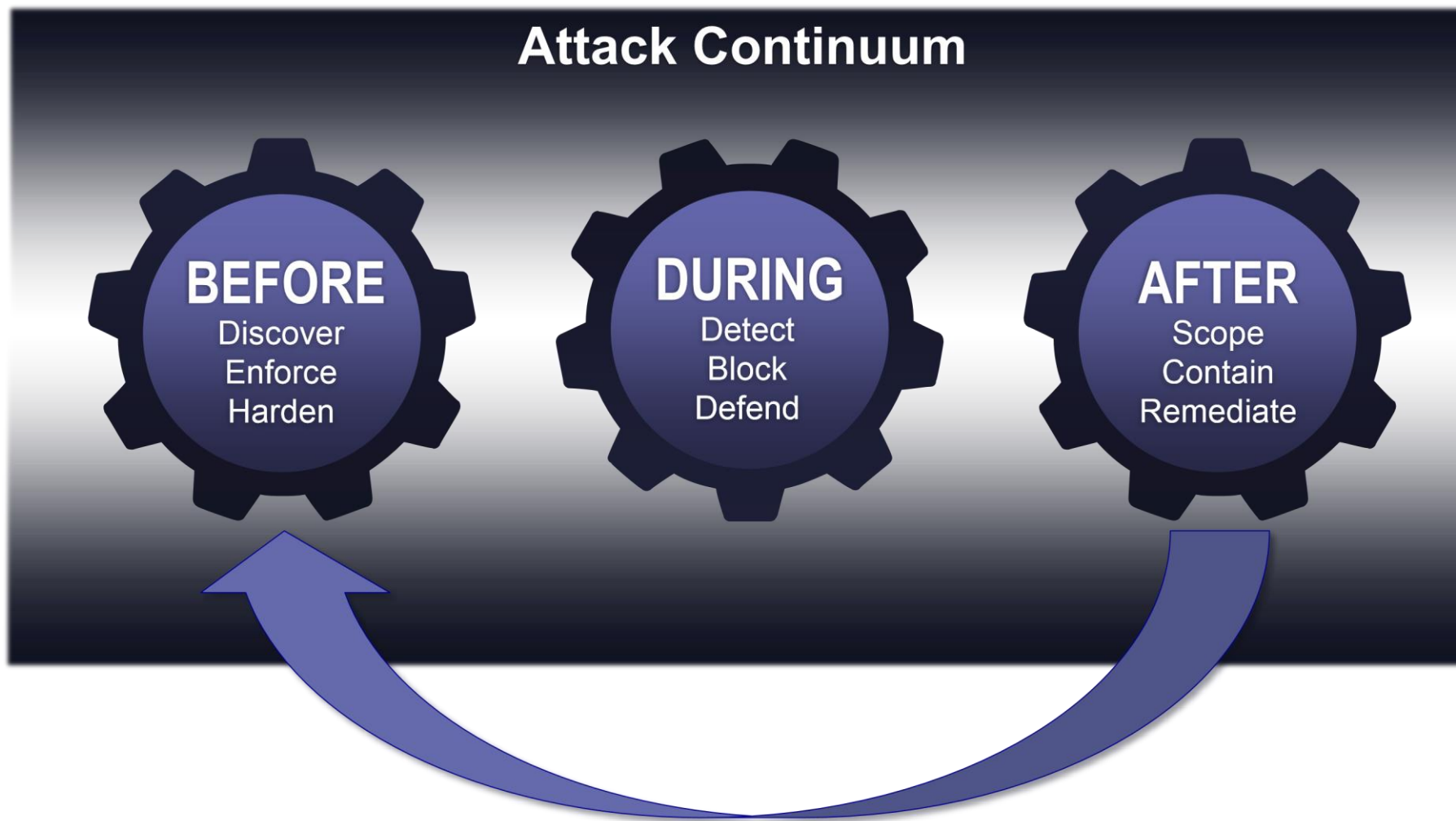
Upload a file containing a set of SHA-256's.

Files included:

09c46e36...82d11cd2

0723932d...1fbfe85f

How do we keep it from happening again?



In conclusion

- You can no longer rely on detection

- What's needed is visibility and control
- In a world where infection is inevitable you need to have the tools in place to find and eliminate the threat
- The goal is to remove the Persistence from Advanced Persistent Threats

Decreasing the Time to Respond...

...Decreases the Cost of the Breach

Questions?

Thank you.

