TOMORROW
starts here.

Embrace Cloud Web Security With Your Cisco Network

BRKSEC-2902

Hideyuki Kobayashi

Consulting System Engineer

#clmel

Cisco live!

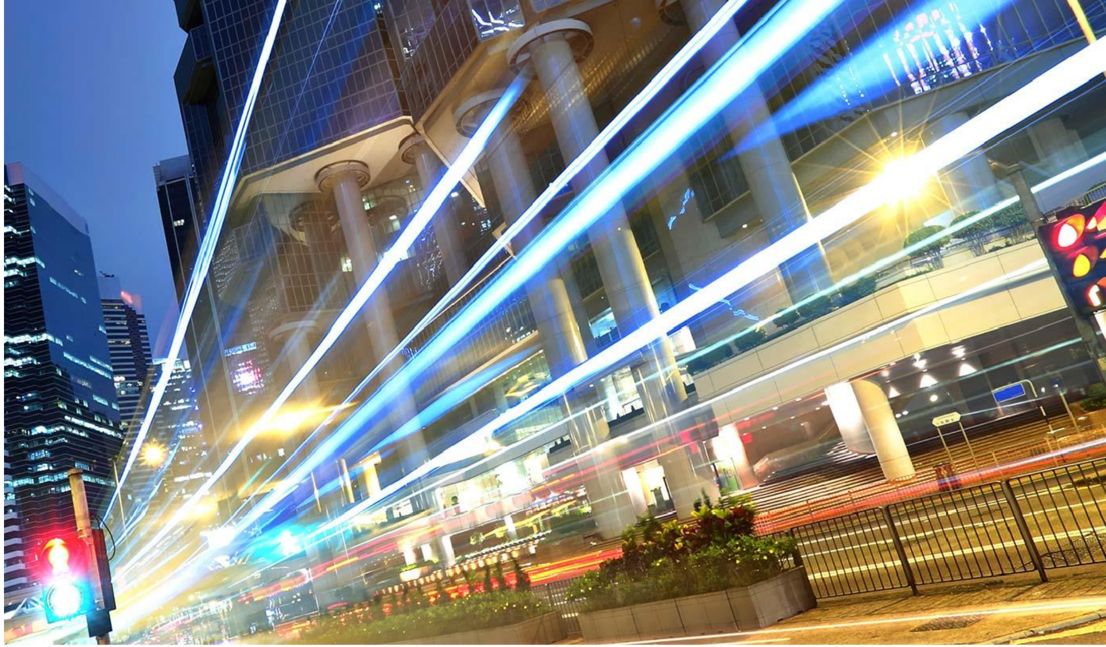
For Your Reference…

- Additional information for your reference can be found on slides with this icon
- Presentation with footnotes available on

For Your Reference

Agenda

- Introduction
- What is Cloud Web Security?
- Protecting Against Advanced Threats
- Live Demo(AMP/CTA)
- Summary



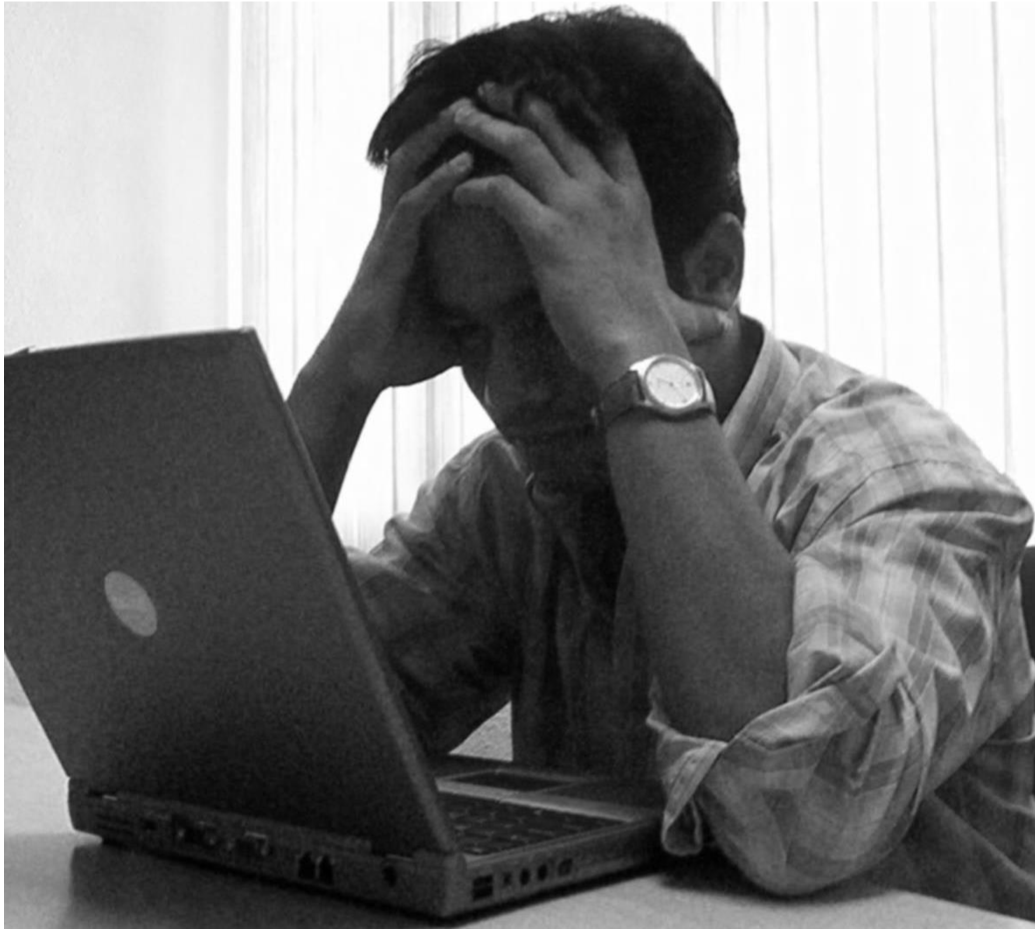
Web Security Challenges

Admin Challenges?

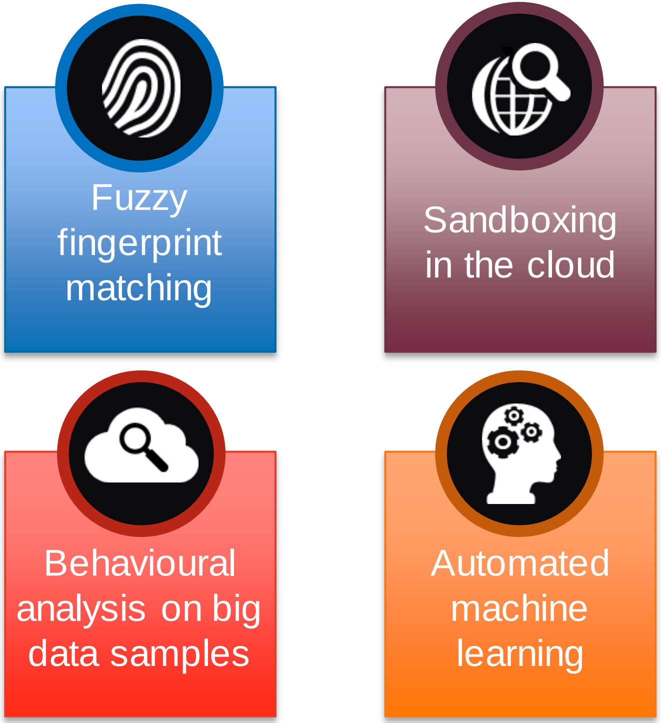
Admin Nightmares!

No Silver Bullet Against Malware

- Web-based attacks more sophisticated
- Breaking down of physical networks
- BYOD and managed devices
- Acceptable usage of web-based apps



Multiple Layers, Multiple Methods



Fuzzy fingerprint matching

Sandboxing in the cloud

Behavioural analysis on big data samples

Automated machine learning

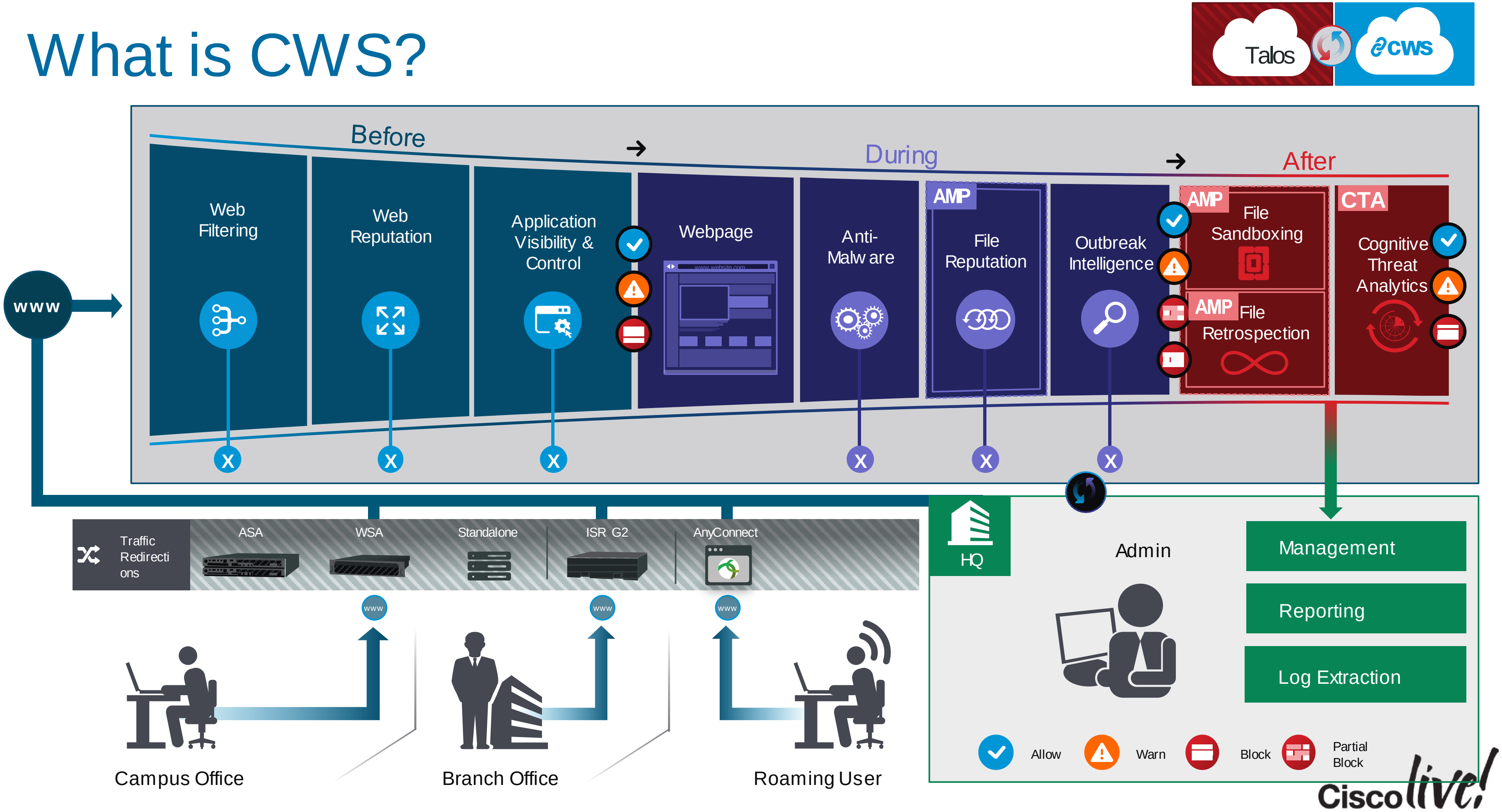
CWS protects your organisation against advanced and sophisticated malware using a variety of unconventional methods

Agenda

- Introduction
- What is Cloud Web Security?
- Protecting Against Advanced Threats
- Live Demo(AMP/CTA)
- Summary

- Cloud Proxy Architecture
- Data Flow and Statistics
- Deployment Options
- Authentication

What is CWS?



Talos
CWS
Before
During
After
www
Web Filtering
Web Reputation
Application Visibility & Control
Webpage
Anti-Malw are
AMP
File Reputation
Outbreak Intelligence
AMP
File Sandboxing
AMP
File Retrospection
CTA
Cognitive Threat Analytics
X
Traffic Redirecti ons
ASA
WSA
Standalone
ISR G2
AnyConnect
www
HQ
Admin
Management
Reporting
Log Extraction
Allow
Warn
Block
Partial Block
Campus Office
Branch Office
Roaming User

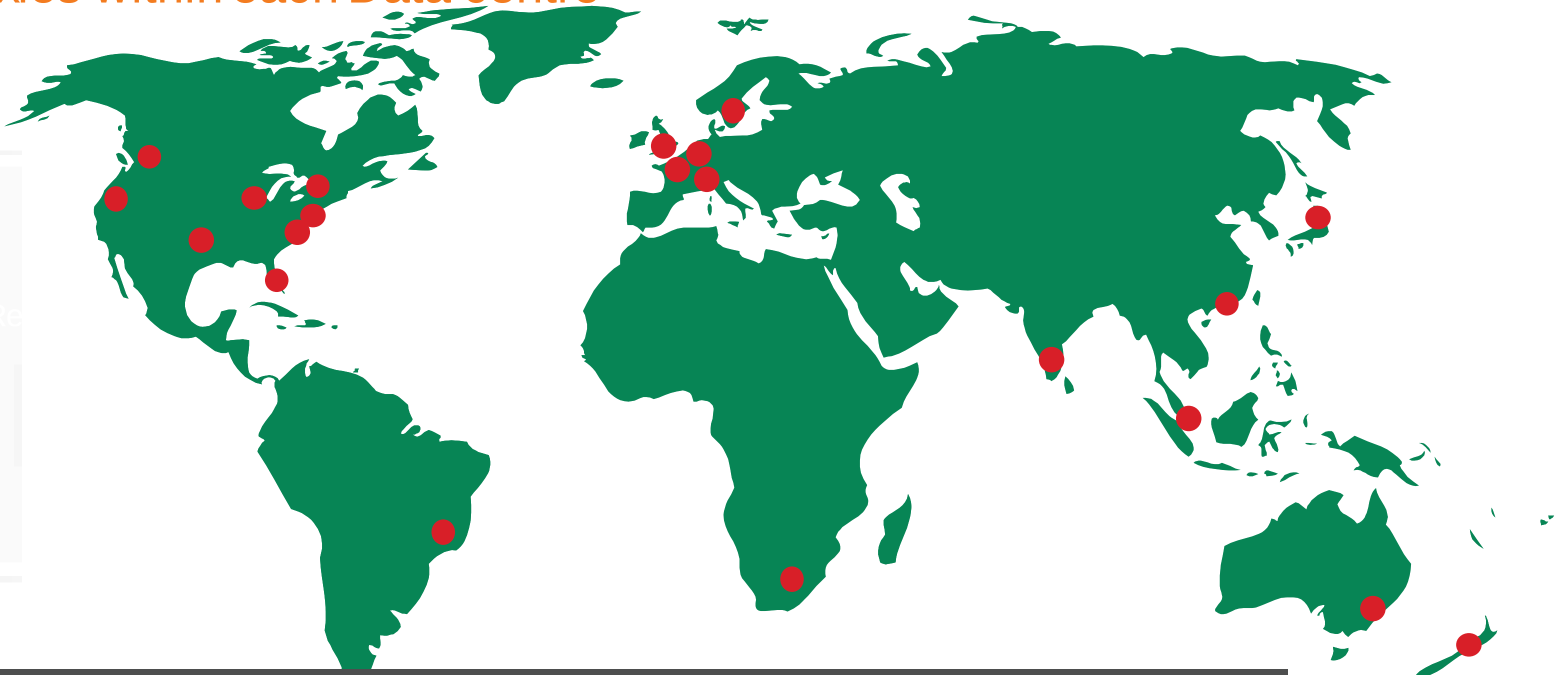
Cloud Proxy Architecture

Global Data Centre Footprint

Multiple proxies within each Data centre

Admin

HQ



- Auckland
- Chennai
- Chicago
- Copenhagen
- Dallas
- Frankfurt
- Hong Kong
- Johannesburg
- London (x2)
- Miami
- New Jersey (x2)
- Paris
- San Jose
- Sao Paulo
- Singapore
- Sydney
- Tokyo
- Toronto
- Vancouver
- Washington DC
- Zurich

So What is a Cloud Proxy?

Next Gen Cloud Infrastructure

Built from the ground up to deliver the next gen Cloud delivered Security Services

Convergence

Intelligence

Automation

Higher throughput over existing infrastructure

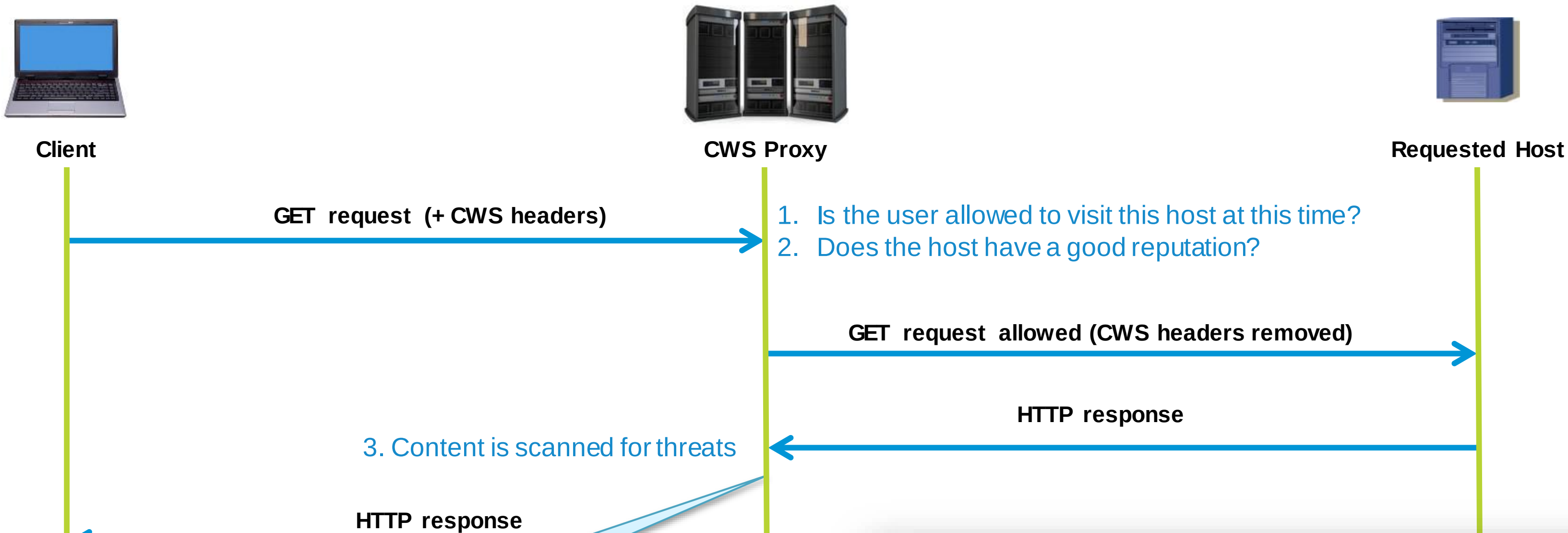
Auto-Configuration detects best tower
Independently assigned egress IPs

Ability to deploy new services without disruptions

VM infrastructure on scalable Cisco UCS hardware
Multi-Service Capable + Capacity for product evolution

Data Flow and Statistics

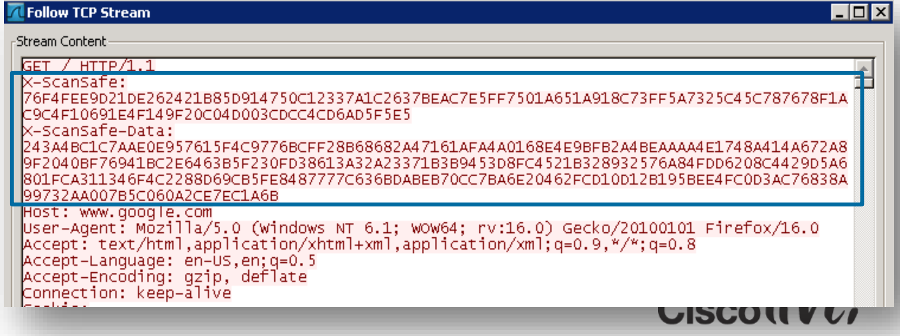
CWS Data Flow


Client
CWS Proxy
Requested Host
GET request (+ CWS headers)
GET request allowed (CWS headers removed)
HTTP response
HTTP response

1. Is the user allowed to visit this host at this time?
2. Does the host have a good reputation?

3. Content is scanned for threats

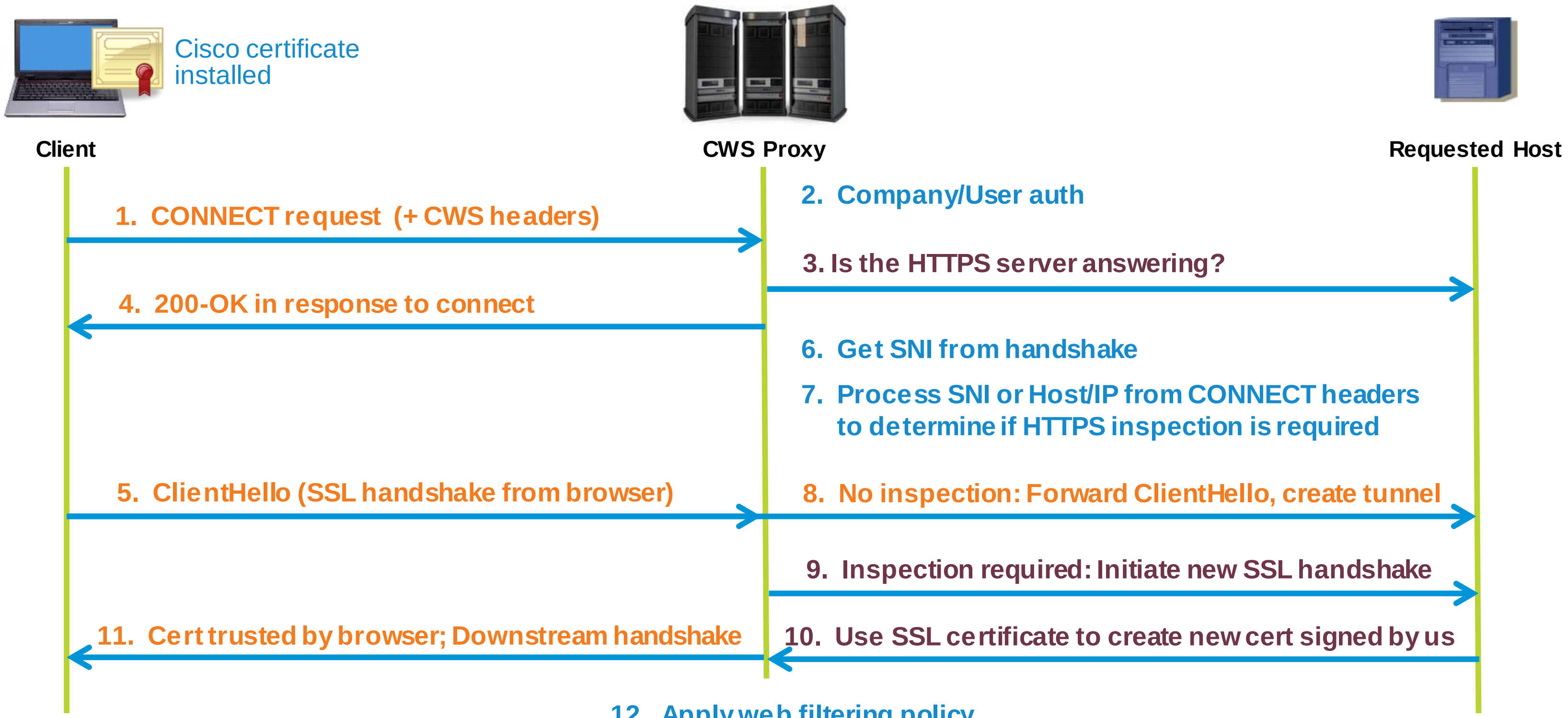
Logging of all request and response events



```
GET / HTTP/1.1
X-ScanSafe:
76F4FEE9D21DE262421B85D914750C12337A1C2637BEAC7E5FF7501A651A918C73FF5A7325C45C787678F1A
C9C4F10691E4F149F20C04D003CDCC4CD6AD5F5E5
X-ScanSafe-Data:
243A4BC1C7AAE0E957615F4C9776BCFF28B68682A47161AFA4A0168E4E9BFB2A4BEAAAA4E1748A414A672A8
9F2040BF76941BC2E6463B5F230FD38613A32A23371B3B9453D8FC4521B328932576A84FDD6208C4429D5A6
801FCA311346F4C2288D69CB5FE8487777C636BDABEB70CC7BA6E20462FCD10D12B195BEE4FC0D3AC76838A
99732AA007B5C060A2CE7EC1A6B
Host: www.google.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

Unencrypted data in CWS headers:
ScanSafeAgentVersion=AP-ISR-15.1(2)T;time=2010-04-29T17:09:59Z;
X-Scansafe-License=12345678912345678912345678912345;cxn=1027;X-Client-IP=20.1.1.2;X-Authenticated-User=c2l2YQ==;X-Authenticated-Groups=SVQ=;

CWS Data Flow - HTTPS



Cisco certificate installed

Client

CWS Proxy

Requested Host

1. CONNECT request (+ CWS headers)

2. Company/User auth

3. Is the HTTPS server answering?

4. 200-OK in response to connect

6. Get SNI from handshake

7. Process SNI or Host/IP from CONNECT headers to determine if HTTPS inspection is required

5. ClientHello (SSL handshake from browser)

8. No inspection: Forward ClientHello, create tunnel

9. Inspection required: Initiate new SSL handshake

11. Cert trusted by browser; Downstream handshake

10. Use SSL certificate to create new cert signed by us

12. Apply web filtering policy

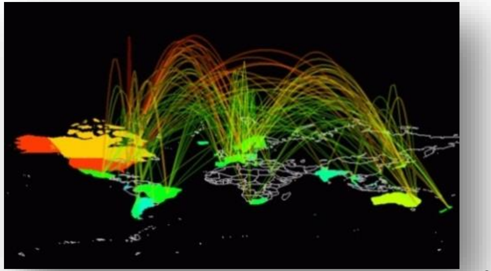
13. Scan content for threats

Big Data in Numbers

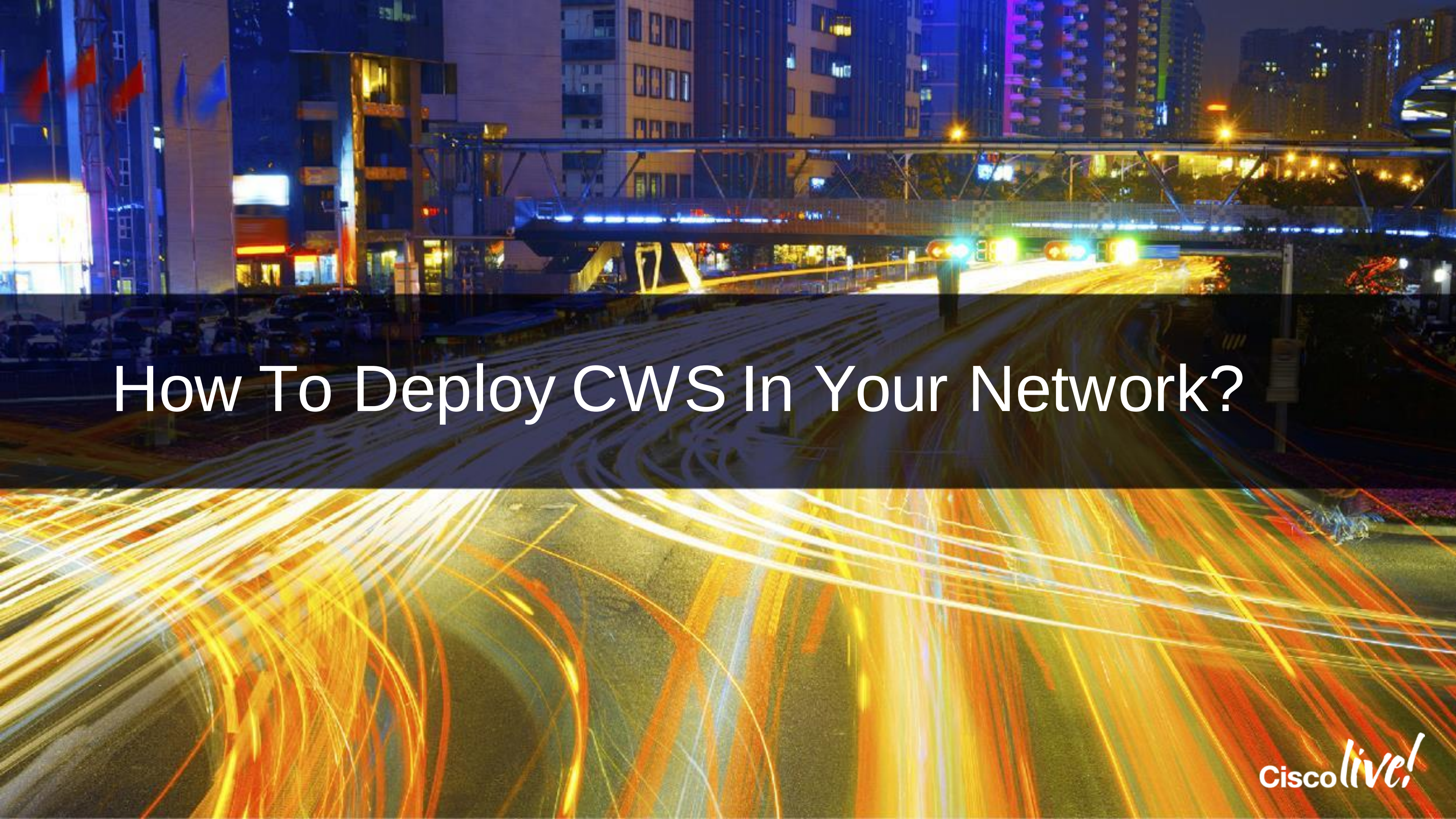
- 6,711,497,122 (6.7B) Requests in a typical business day *
- 124,888,190 (~125M) Blocks in a typical business day (25.6M malware blocks) *
- As a comparison: Google receives over 3B requests/day **
- 7.6M rows of data processed per minute for reporting data

* 15 December 2014

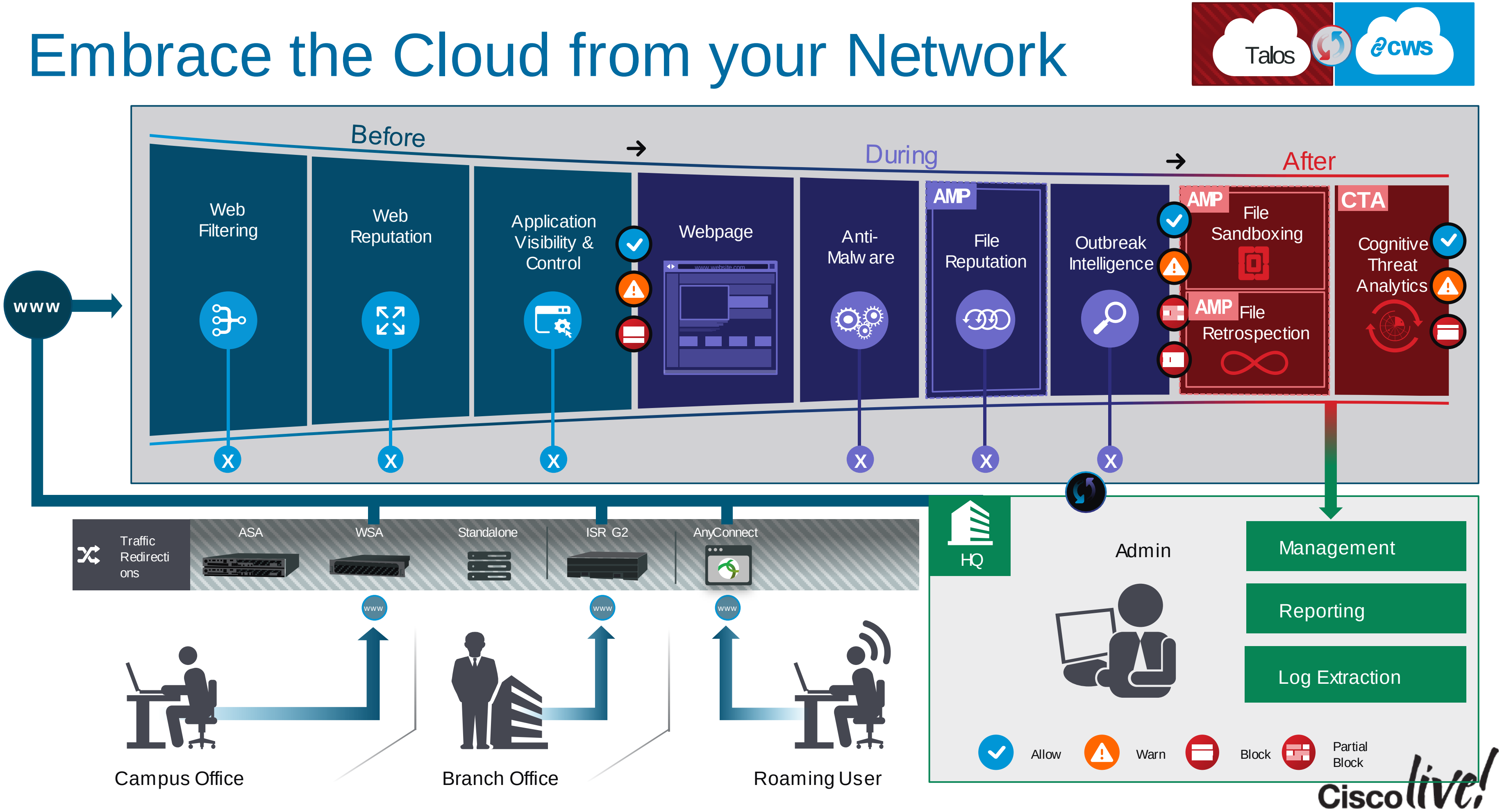
** Published on Wikipedia



How To Deploy CWS In Your Network?

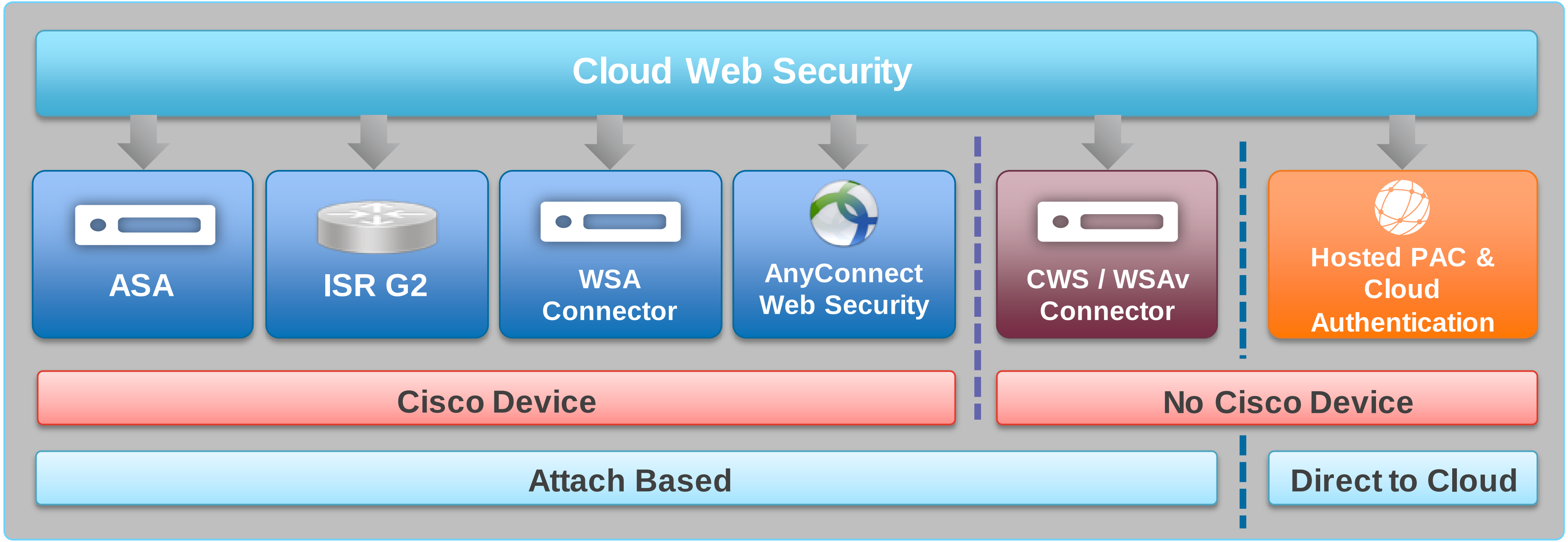


Embrace the Cloud from your Network



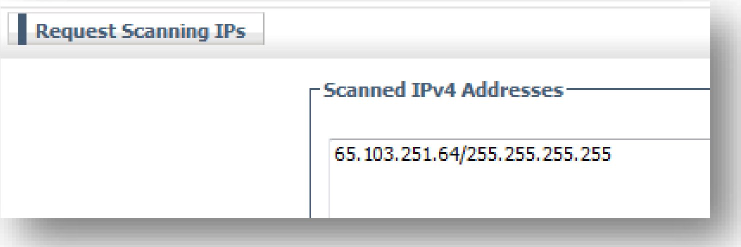
Cisco Cloud Attach Model

Use your existing Cisco asset to leverage CWS



Connector Functionality

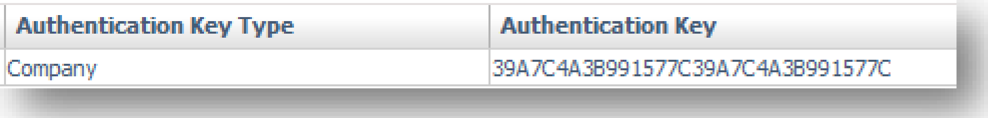
- Traffic redirection to CWS proxy
- Failover between primary and backup proxies
- User authentication using device’s built-in mechanism
- Whitelisting of traffic (requests will go direct to destination website)
- Adding of CWS encrypted headers to requests
  - Important also for identifying and authenticating company (company/group key)
  - When no connector, companies are identified by their registered egress IP address



Request Scanning IPs

Scanned IPv4 Addresses

65.103.251.64/255.255.255.255



Authentication Key Type	Authentication Key
Company	39A7C4A3B991577C39A7C4A3B991577C

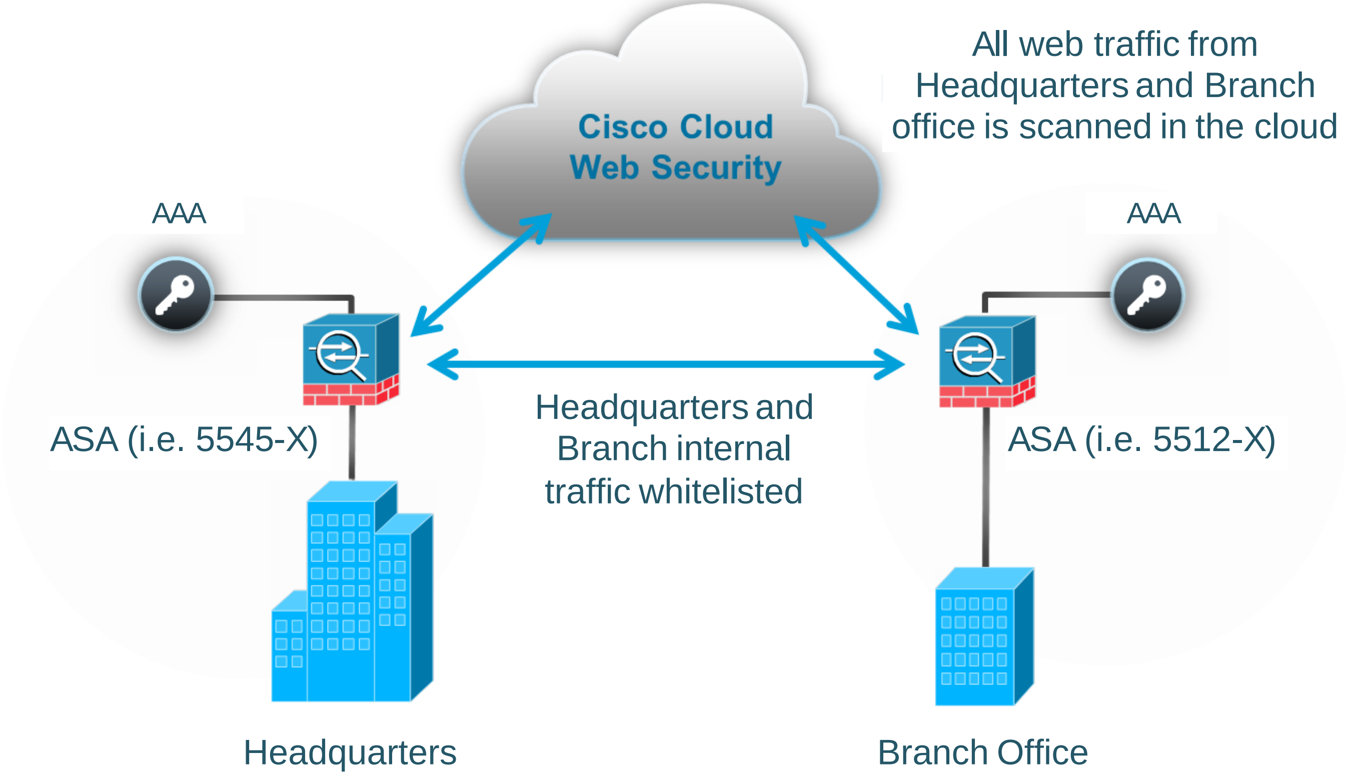
ASA Connector

ASA Connector - Main Features

- The ASA Connector is available from v9.0, and runs on all ASA models
- Can be used for transparent deployment in HQ and branch offices
- Single and Multiple Context Modes are supported for HTTP and HTTPS traffic
- No need for special license on ASA (K8 → K9 free upgrade)
- User authorisation provided from AD via IDFW
- Automated fail-over to secondary data centre
- No need to install software on dedicated hardware, or make any browser changes/install a client on end users' machines
- CWS licensing on a per-user basis, so not tied to number of devices

CWS Connector on ASA

Transparent redirection to the cloud with Identity



All web traffic from Headquarters and Branch office is scanned in the cloud

Headquarters and Branch internal traffic whitelisted

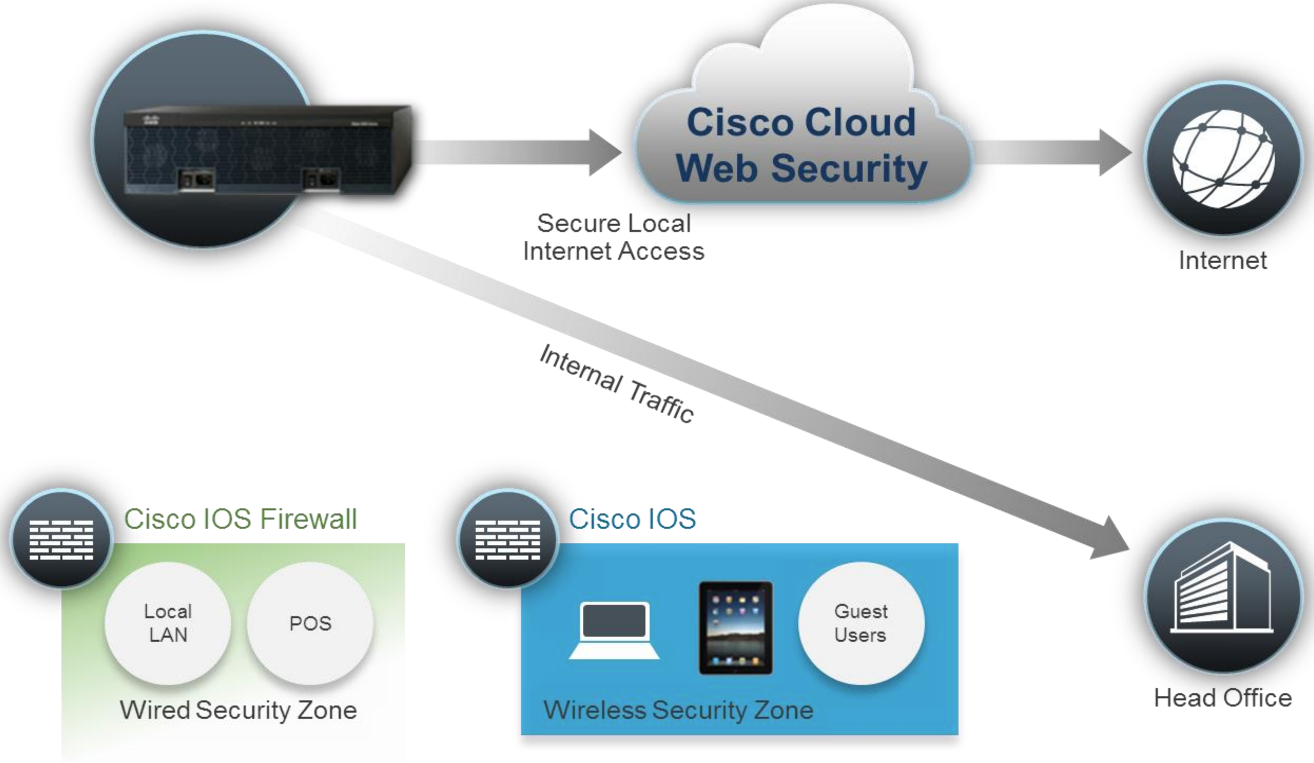
ISR G2 Connector

ISR G2 Connector - Main Features

- The Connector is available in IOS (universal) images with the K9 security feature set (SEC) licenses
- Supported on 880, 890, 19xx, 29xx & 39xx/E ISR G2 platforms
- Supports re-direction of HTTP/HTTPS internet traffic directly to the cloud securely without having to backhaul to the corporate network
- User authorisation through AAA service on ISR
- Automated fail-over to secondary data centre
- No need to install software on dedicated hardware, or make any browser changes/install AnyConnect on end users' machines
- CWS licensing on a per-user basis, so not tied to number of devices

Break out Directly to the Internet from Branches

Cloud Redirection for Web Integrated into the ISRG2 Routers



WSA Connector

WSA Connector - Main Features

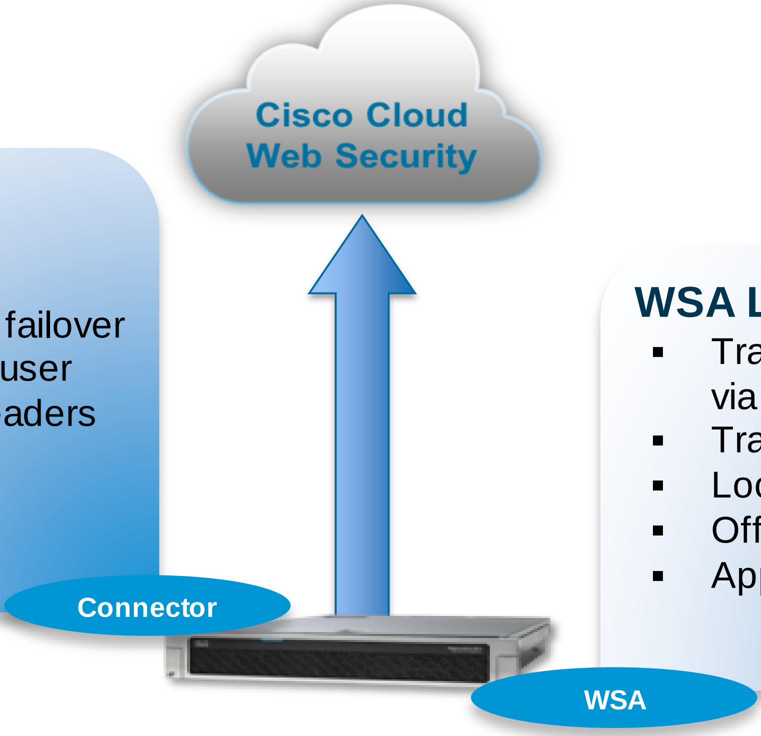
- The Connector is available in AsyncOS ver. 8
- Dedicated Connector configuration via Configuration Wizard
- Supported on S-Series x70 and x80, and WSAv platforms
- Automated fail-over to secondary cloud proxy
- User authorisation through existing WSA mechanism
- CWS licensing on a per-user basis, not per WSA devices
- Common use cases:
  - Connector can be run in a virtual environment when no Cisco appliances available
  - Useful for customers looking for a mix of cloud security with appliance-based features
  - Existing WSA in place, and want to move to CWS to also support roaming users in single policy

WSA Connector

Combine centralised cloud advantages with local features

WSA Connector

- Redirection to CWS
- Primary/Backup proxy failover
- Company, group, and user details in encrypted headers
- Fail-open/fail-closed mechanism



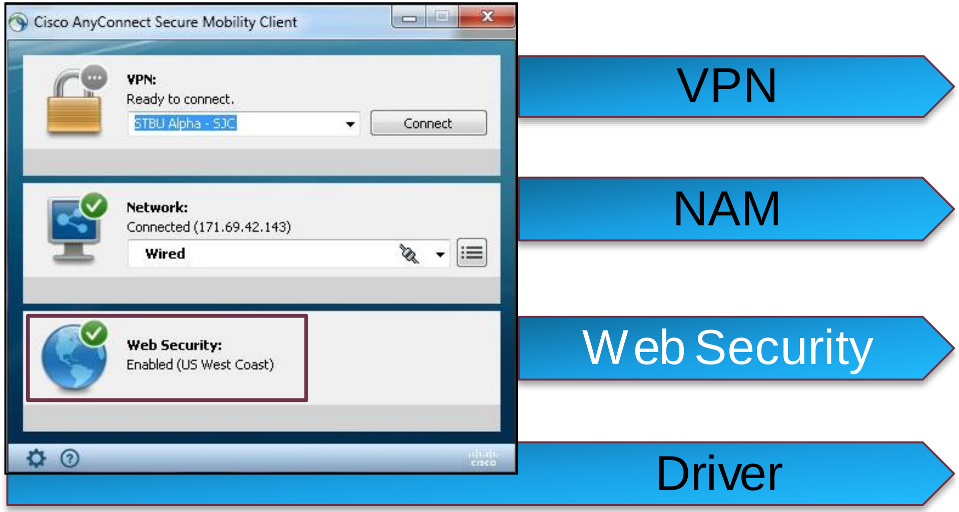
WSA Local Features

- Transparent authentication via on-box NTLM v2
- Transparent or explicit proxy
- Local caching support
- Off-box DLP integration
- Appliance based

AnyConnect Web Security

What is AnyConnect Web Security?

- Web Security is one of the components of Cisco’s AnyConnect VPN client
- Web Security is an additional layer within Any Connect, that works with the driver, alongside the other existing features

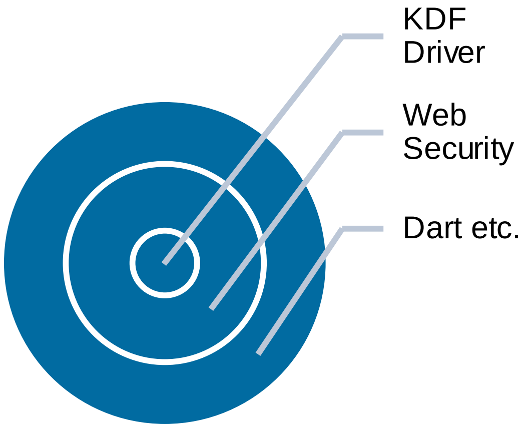


Cisco AnyConnect Secure Mobility Client

VPN:
Ready to connect.
STBU Alpha - SJC
Connect

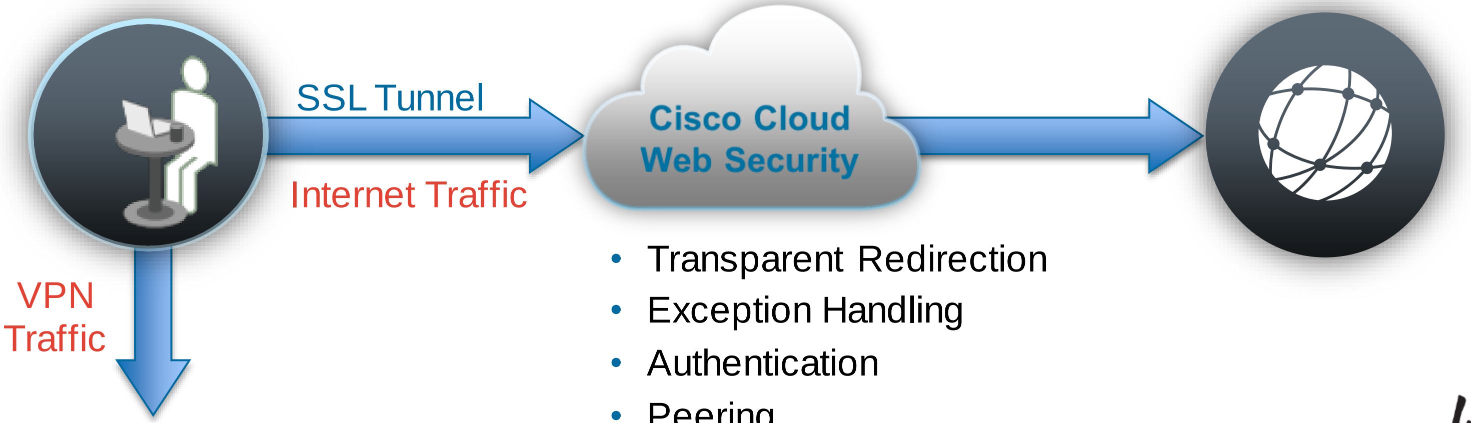
Network:
Connected (171.69.42.143)
Wired

Web Security:
Enabled (US West Coast)



AnyConnect Web Security for Roaming Users

- Intercepts and redirects the user's external web traffic to the cloud proxies
- Automatic peering to the closest data centre for best performance
- Traffic is SSL encrypted for improved security over public networks
- Works with Full or Split Tunnel VPN clients



- Transparent Redirection
- Exception Handling
- Authentication
- Peering

No Cisco Device? No Problem!

Redirection Options

- When no Cisco device is available, web traffic can still be redirected to the cloud through one of these methods:
  - WSA Connector on a virtual environment (full connector features + auth)
  - CWS Connector (originally ScanSafe Connector) running on customer’s Windows Server or Linux platform as an explicit proxy that redirects to CWS. NTLM auth via internal LDAP integration, or ICAP/ISA integration
  - Browser proxy settings/hosted proxy auto configuration (PAC) for browser redirection

WSAv Connector

CWS Connector

Hosted PAC

Deployment Summary

Find your Deployment Guide

ASA/ASAv

Next Generation Firewall

Cisco Cloud Web Security
ASA 5500/ASAv Deployment Guide
September 2014 – Internal Use Only

WSA/WSAv

Cisco Web Security Appliance

Cisco Cloud Web Security
WSA/WSAv Deployment Guide
September 2014 – Internal Use Only

ISR G2

Integrated Services Router

Cisco Cloud Web Security
ISR G2 Deployment Guide
September 2014 – Internal Use Only

AnyConnect

AnyConnect Secure Mobility

Cisco Cloud Web Security
AnyConnect Web Security Deployment Guide
September 2014 – Internal Use Only

Standalone

Use existing settings and PAC/WPAD

Cisco Cloud Web Security
Standalone Deployment Guide
September 2014 – Internal Use Only

http://www.cisco.com/c/en/us/support/security/cloud-web-security/products-installation-and-configuration-guides-list.html

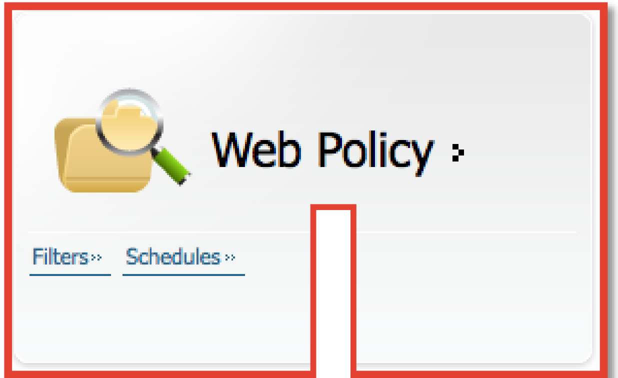
Agenda

- Introduction
- What is Cloud Web Security?
- Protecting Against Advanced Threats
- Live Demo(AMP/CTA)
- Summary

- Managing Policy
- Delegated Administration
- Reporting
- Log Extractaction

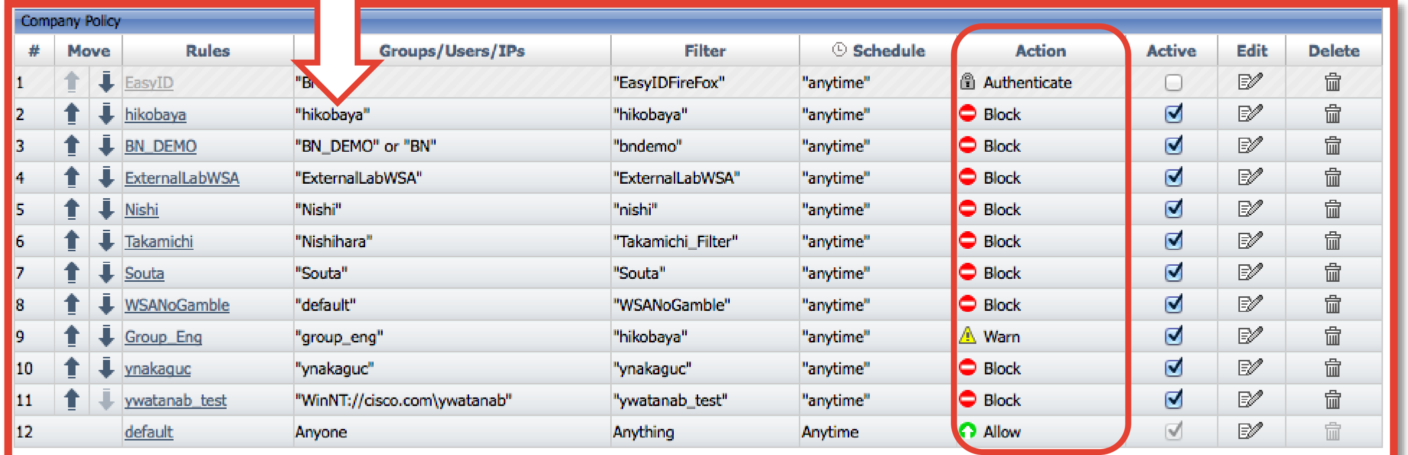
Managing Policy

Policy Enables You to Set the Rules for Applying Filters



Each rule has one of the following actions associated with it:

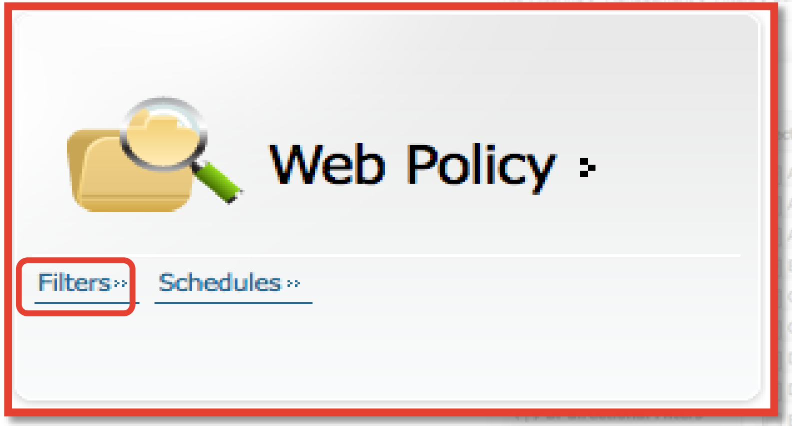
- Allow— Access is allowed, and data is stored for reporting purposes.
- Anonymise— User, group, internal, and external IP details are replaced with “ undisclosed” in reporting data.
- Authenticate— The user must authenticate. Typically this is used with clientless authentication.
- Block— Access is denied.
- Warn— Access is allowed only if the user clicks through the warning page.



Company Policy

#	Move	Rules	Groups/Users/IPs	Filter	Schedule	Action	Active	Edit	Delete
1	⬆ ⬇	EasyID	"Bi	"EasyIDFireFox"	"anytime"	Authenticate	□	✎	🗑
2	⬆ ⬇	hikobaya	"hikobaya"	"hikobaya"	"anytime"	Block	☑	✎	🗑
3	⬆ ⬇	BN_DEMO	"BN_DEMO" or "BN"	"bndemo"	"anytime"	Block	☑	✎	🗑
4	⬆ ⬇	ExternalLabWSA	"ExternalLabWSA"	"ExternalLabWSA"	"anytime"	Block	☑	✎	🗑
5	⬆ ⬇	Nishi	"Nishi"	"nishi"	"anytime"	Block	☑	✎	🗑
6	⬆ ⬇	Takamichi	"Nishihara"	"Takamichi_Filter"	"anytime"	Block	☑	✎	🗑
7	⬆ ⬇	Souta	"Souta"	"Souta"	"anytime"	Block	☑	✎	🗑
8	⬆ ⬇	WSANoGamble	"default"	"WSANoGamble"	"anytime"	Block	☑	✎	🗑
9	⬆ ⬇	Group_Eng	"group_eng"	"hikobaya"	"anytime"	Warn	☑	✎	🗑
10	⬆ ⬇	ynakaguc	"ynakaguc"	"ynakaguc"	"anytime"	Block	☑	✎	🗑
11	⬆ ⬇	ywatanab_test	"WinNT://cisco.com\ywatanab"	"ywatanab_test"	"anytime"	Block	☑	✎	🗑
12		default	Anyone	Anything	Anytime	Allow	☑	✎	🗑

Filters are Used to Control Content that Passes into, and out of, Your Network



With Outbound Content Control enabled, the following filters are also available:

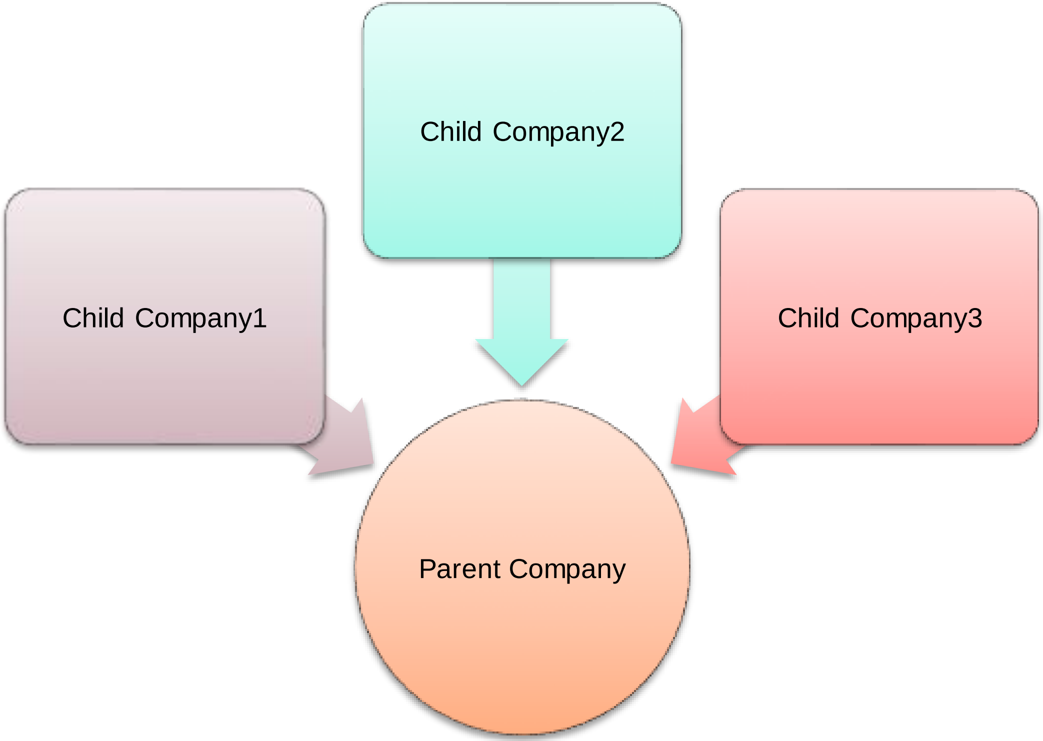
- ✓ Keywords
- ✓ Outbound File Types
- ✓ Pre-configured IDs
- ✓ Regular Expressions

The following filter types are available:

- ✓ Categories (HTTP)
- ✓ Categories (HTTPS)
- ✓ Domains and URLs
- ✓ Content Types
- ✓ File Types
- ✓ Applications
- ✓ Exceptions
- ✓ Protocols
- ✓ User Agents

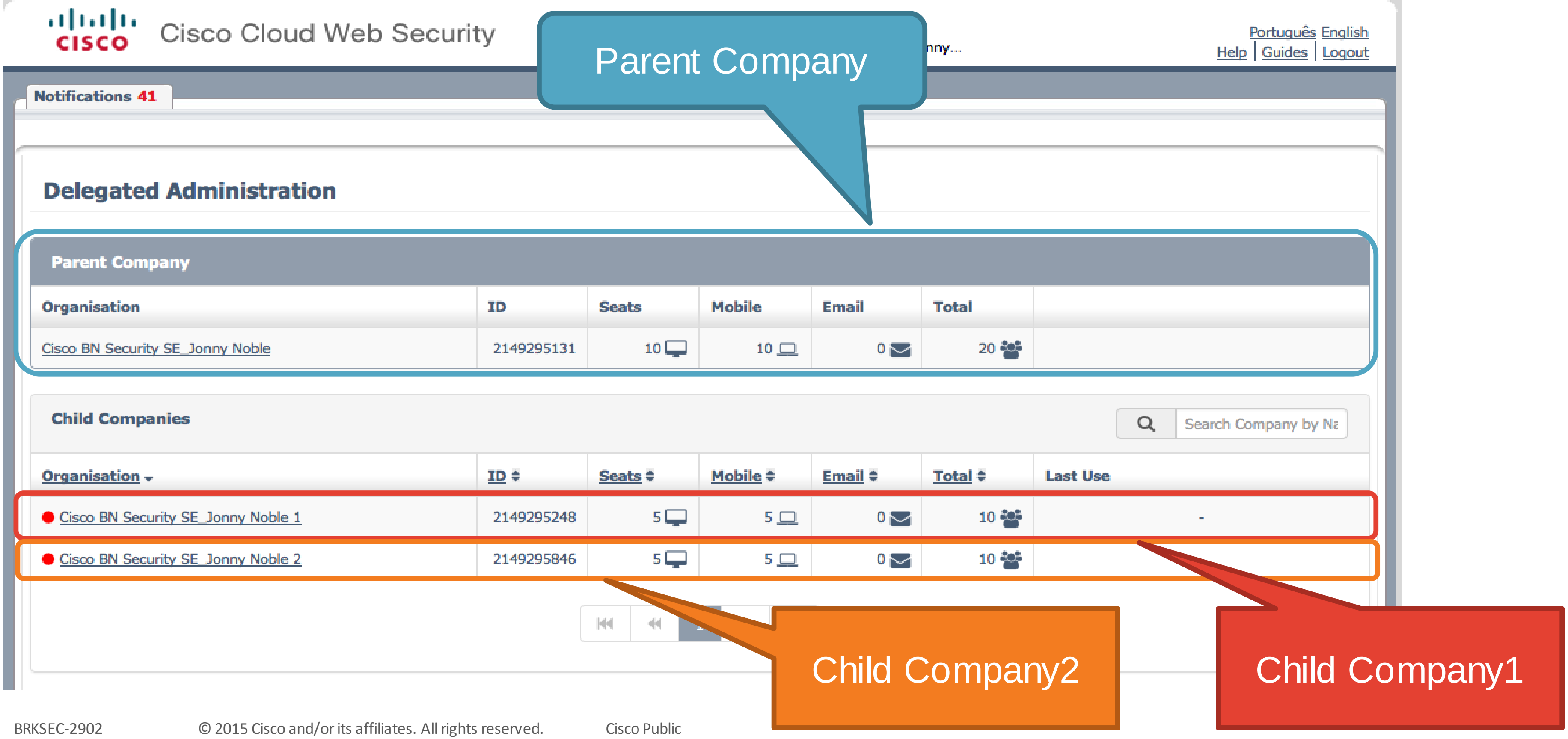
Delegated Administration

Delegated Administration Between Parent and Subsidiary



Parent Company

Delegated Administration



Cisco Cloud Web Security

nny…

Português English
Help | Guides | Logout

Notifications 41

Delegated Administration

Parent Company

Organisation	ID	Seats	Mobile	Email	Total
Cisco BN Security SE_Jonny Noble	2149295131	10 🖥	10 💻	0 ✉	20 👥

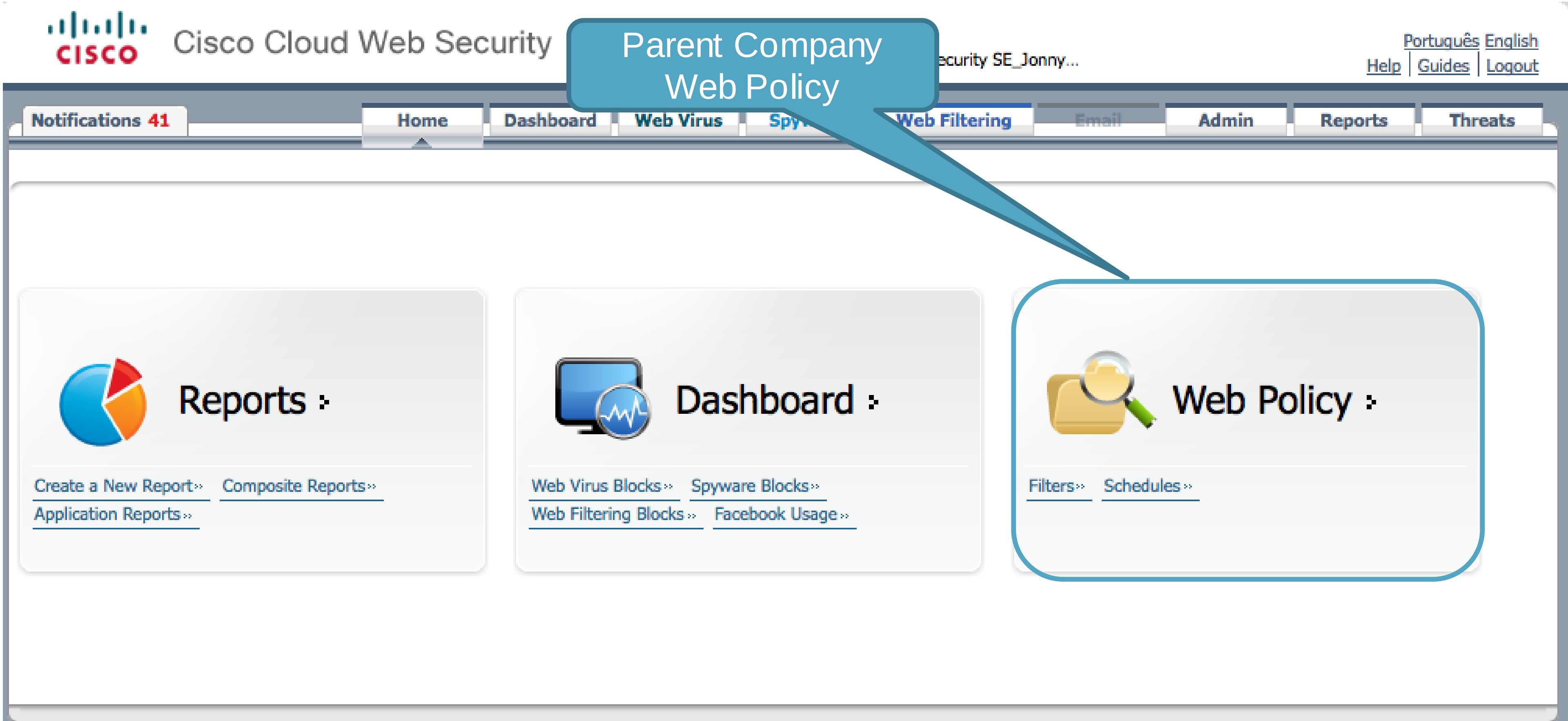
Child Companies

Search Company by Na

Organisation ▾	ID ⬍	Seats ⬍	Mobile ⬍	Email ⬍	Total ⬍	Last Use
● Cisco BN Security SE_Jonny Noble 1	2149295248	5 🖥	5 💻	0 ✉	10 👥	-
● Cisco BN Security SE_Jonny Noble 2	2149295846	5 🖥	5 💻	0 ✉	10 👥	

Parent Company

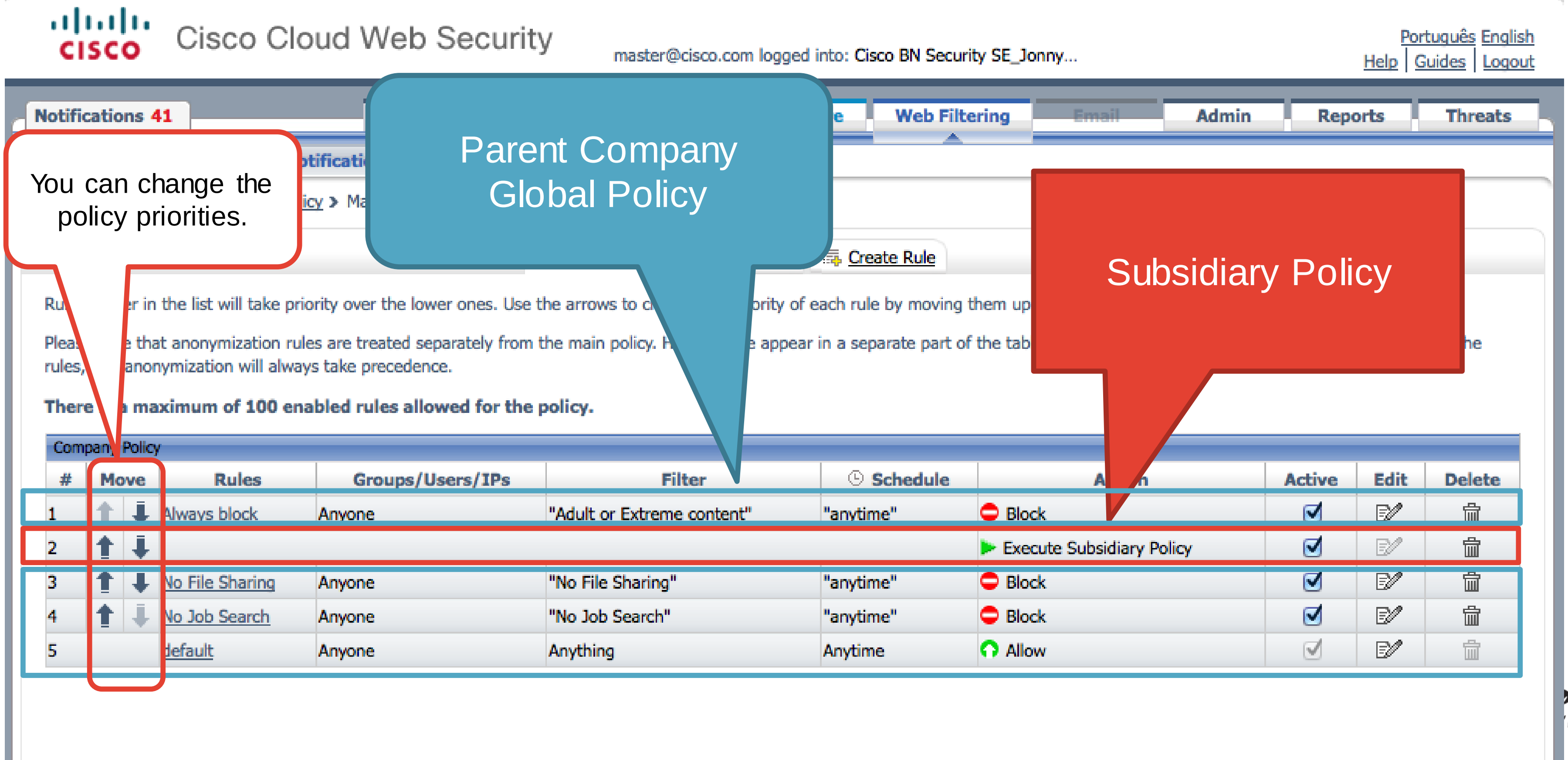
Delegated Administration



Parent Company
Web Policy

Parent Company

Delegated Administration



master@cisco.com logged into: Cisco BN Security SE_Jonny...

Ru r in the list will take priority over the lower ones. Use the arrows to c ority of each rule by moving them up

Plea e that anonymization rules are treated separately from the main policy. H e appear in a separate part of the tab he rules, anonymization will always take precedence.

There a maximum of 100 enabled rules allowed for the policy.

Compan Policy

#	Move	Rules	Groups/Users/IPs	Filter	Schedule	Action	Active	Edit	Delete
1	⬆ ⬇	Always block	Anyone	"Adult or Extreme content"	"anytime"	⛔ Block	☑	✎	🗑
2	⬆ ⬇					▶ Execute Subsidiary Policy	☑	✎	🗑
3	⬆ ⬇	No File Sharing	Anyone	"No File Sharing"	"anytime"	⛔ Block	☑	✎	🗑
4	⬆ ⬇	No Job Search	Anyone	"No Job Search"	"anytime"	⛔ Block	☑	✎	🗑
5		default	Anyone	Anything	Anytime	Allow	☑	✎	🗑

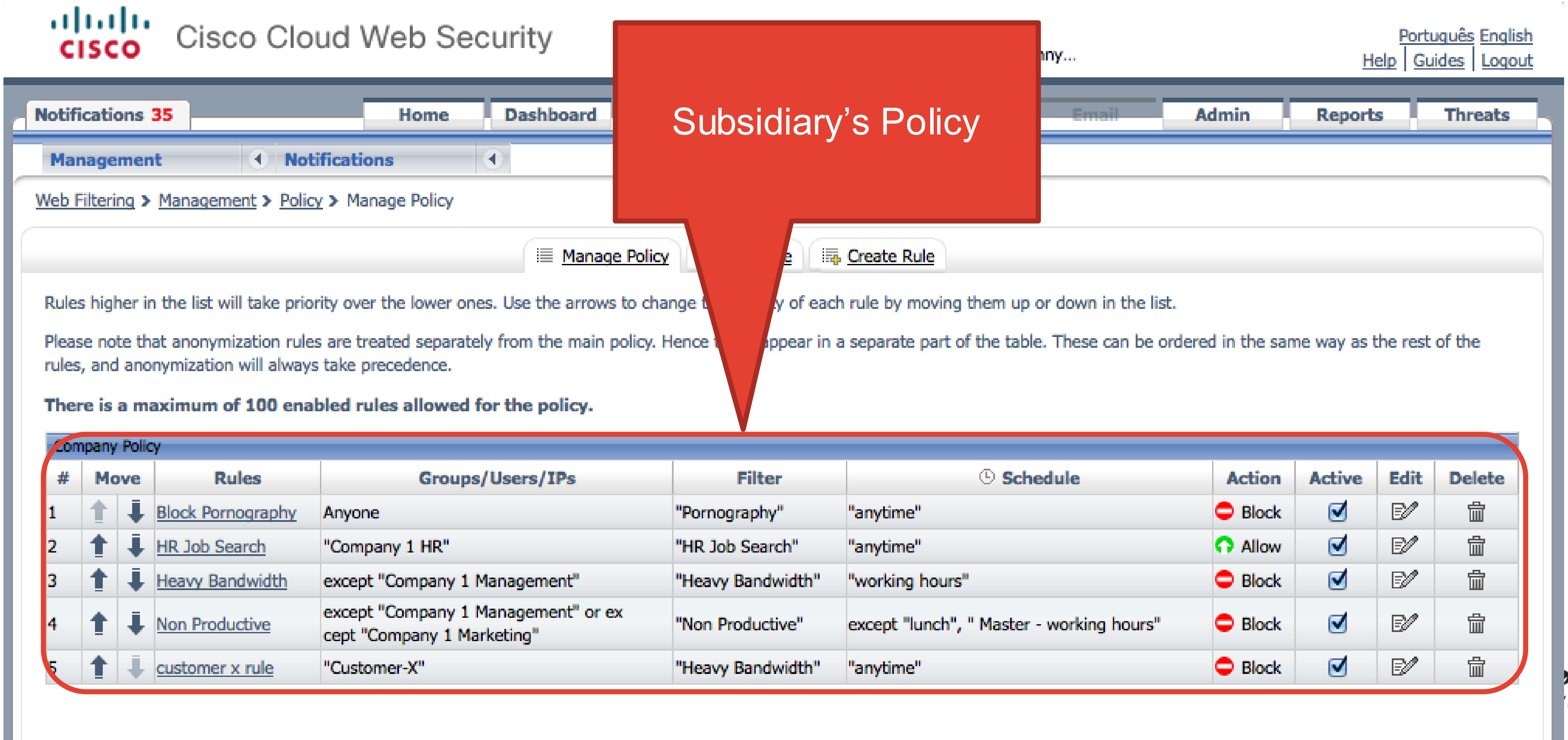
You can change the policy priorities.

Parent Company Global Policy

Subsidiary Policy

Subsidiary

Delegated Administration



Cisco Cloud Web Security

Web Filtering > Management > Policy > Manage Policy

Rules higher in the list will take priority over the lower ones. Use the arrows to change t y of each rule by moving them up or down in the list.

Please note that anonymization rules are treated separately from the main policy. Hence t ppear in a separate part of the table. These can be ordered in the same way as the rest of the rules, and anonymization will always take precedence.

There is a maximum of 100 enabled rules allowed for the policy.

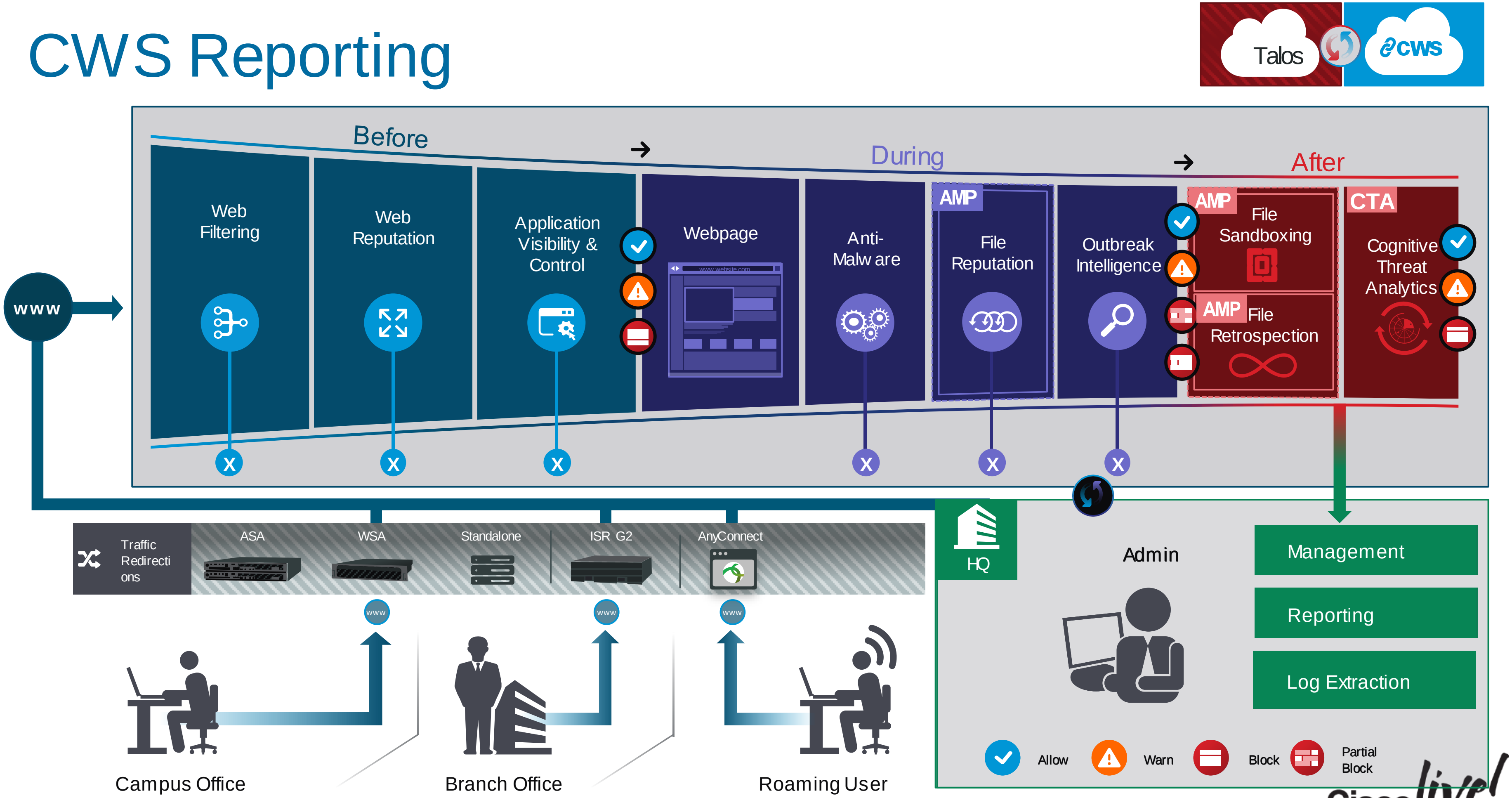
Company Policy

#	Move	Rules	Groups/Users/IPs	Filter	Schedule	Action	Active	Edit	Delete
1	↑ ↓	Block Pornography	Anyone	"Pornography"	"anytime"	Block	☑	✎	🗑
2	↑ ↓	HR Job Search	"Company 1 HR"	"HR Job Search"	"anytime"	Allow	☑	✎	🗑
3	↑ ↓	Heavy Bandwidth	except "Company 1 Management"	"Heavy Bandwidth"	"working hours"	Block	☑	✎	🗑
4	↑ ↓	Non Productive	except "Company 1 Management" or except "Company 1 Marketing"	"Non Productive"	except "lunch", " Master - working hours"	Block	☑	✎	🗑
5	↑ ↓	customer x rule	"Customer-X"	"Heavy Bandwidth"	"anytime"	Block	☑	✎	🗑

Subsidiary's Policy

Reporting

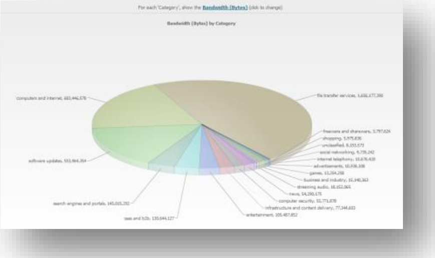
CWS Reporting

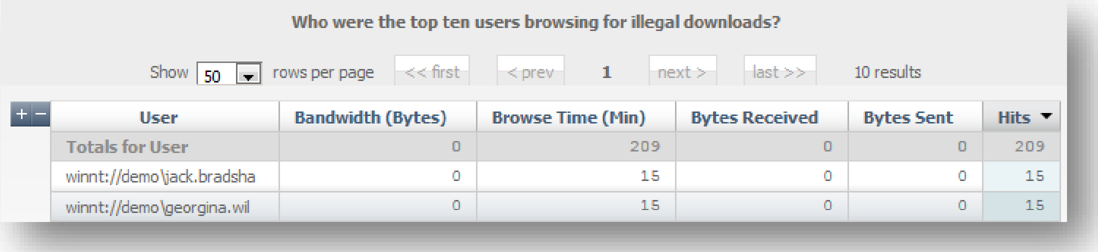


Cisco live!

Web Intelligence Reporting

- Ultimate flexibility in reporting criteria: ~100 attributes for each web request
- Multiple output options: Detailed reports, time trends, user audits, scheduling
- Complete visibility into web and applications usage, bandwidth, browse time, and activities
- Enhanced risk & resource management through an understanding of potential exposure to threats and inappropriate content
- Visibility into how valuable resources are being utilised





Who were the top ten users browsing for illegal downloads?

User	Bandwidth (Bytes)	Browse Time (Min)	Bytes Received	Bytes Sent	Hits
Totals for User	0	209	0	0	209
winnt://demo\jack.bradsha	0	15	0	0	15
winnt://demo\georgina.wil	0	15	0	0	15

Reporting High Level Architecture

CWS Data × Search condition × Sort = Online result

Reports

CWS Data

Search condition

Time Period

Filter

- Attributes
- Metrics
- Filter set

Selecting Attributes
(Detailed search only)

Sort

Sorted Metric

- Ascending
- Descending

Online result

Chart

- Grid
- Column
- Bar
- Pine
- Line

Reports

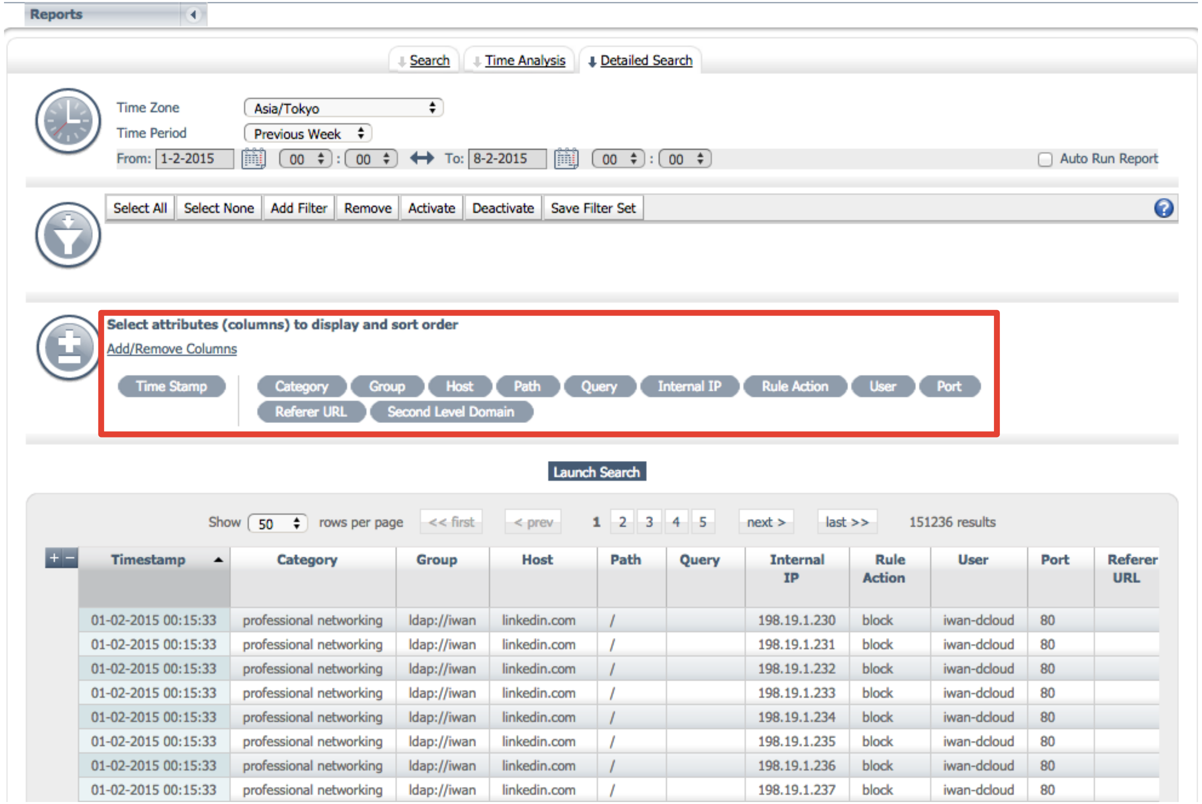
Manual reports

- Custom search
- Pre-defined search

Scheduled reports

- Custom search
- Pre-defined search

Detailed Search:



Time Zone: Asia/Tokyo

Time Period: Previous Week

From: 1-2-2015 00 : 00 ↔ To: 8-2-2015 00 : 00

□ Auto Run Report

Select attributes (columns) to display and sort order

Add/Remove Columns

Time Stamp | Category | Group | Host | Path | Query | Internal IP | Rule Action | User | Port | Referer URL | Second Level Domain

Show 50 rows per page

151236 results

Timestamp	Category	Group	Host	Path	Query	Internal IP	Rule Action	User	Port	Referer URL
01-02-2015 00:15:33	professional networking	ldap://iwan	linkedin.com	/		198.19.1.230	block	iwan-dcloud	80	
01-02-2015 00:15:33	professional networking	ldap://iwan	linkedin.com	/		198.19.1.231	block	iwan-dcloud	80	
01-02-2015 00:15:33	professional networking	ldap://iwan	linkedin.com	/		198.19.1.232	block	iwan-dcloud	80	
01-02-2015 00:15:33	professional networking	ldap://iwan	linkedin.com	/		198.19.1.233	block	iwan-dcloud	80	
01-02-2015 00:15:33	professional networking	ldap://iwan	linkedin.com	/		198.19.1.234	block	iwan-dcloud	80	
01-02-2015 00:15:33	professional networking	ldap://iwan	linkedin.com	/		198.19.1.235	block	iwan-dcloud	80	
01-02-2015 00:15:33	professional networking	ldap://iwan	linkedin.com	/		198.19.1.236	block	iwan-dcloud	80	
01-02-2015 00:15:33	professional networking	ldap://iwan	linkedin.com	/		198.19.1.237	block	iwan-dcloud	80	

- Combined Attributes

  Good reference to create your reports

- All data mining is done in CWS cloud like big data analysis

Cloud Log Extraction

Cloud Log Extraction

1 Browsing data is captured by CWS

2 Data securely stored in Core data centre

3 Logs available within 2 hours and stored for 5 days

4 S3 Compatible HTTPS API for automatic data transfer

5 Correlates with existing data for analysis

Available Attributes

24 reporting attributes are available

#	Attribute Name	#	Attribute Name	#	Attribute Name
1	Datetime	9	cs-uri-path	17	s-ip
2	c-ip	10	cs-uri-query	18	x-ss-category
3	cs(X-Forwarded-For)	11	cs(User-Agent)	19	x-ss-last-rule-name
4	cs-username	12	cs(Content-Type)	20	x-ss-last-rule-action
5	cs-method	13	cs-bytes	21	x-ss-block-type
6	cs-uri-scheme	14	sc-bytes	22	x-ss-block-value
7	cs-host	15	sc-status	23	x-ss-referer-host
8	cs-uri-port	16	sc(Content-Type)	24	x-ss-external-ip

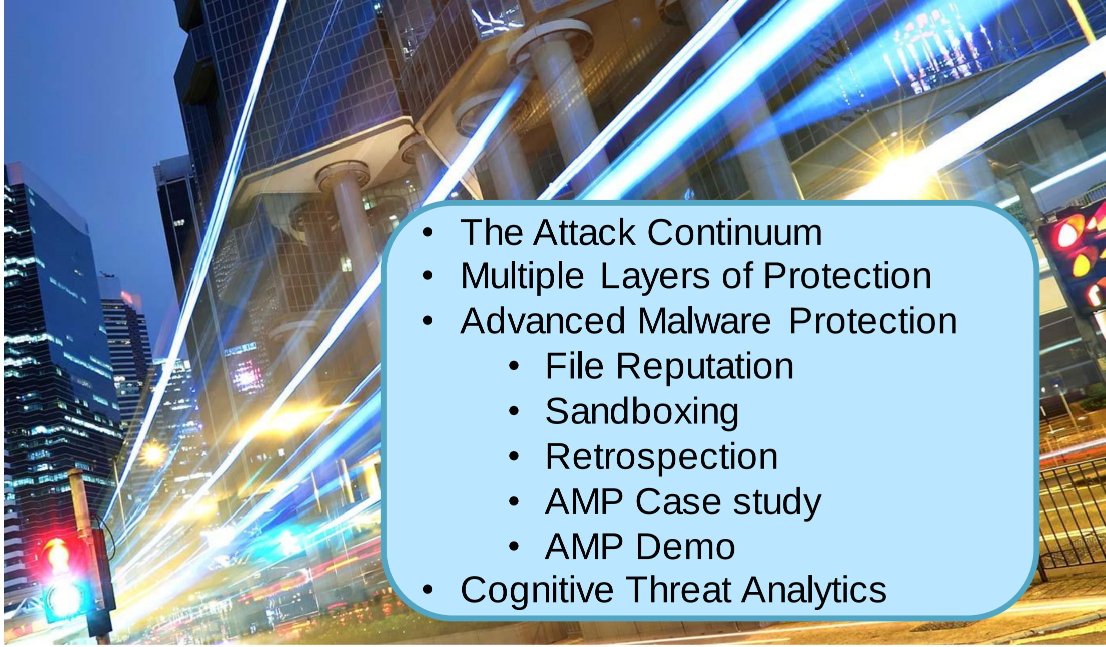
c: client
s: server

cs: client-server
sc: server-client

x-ss: CWS custom field

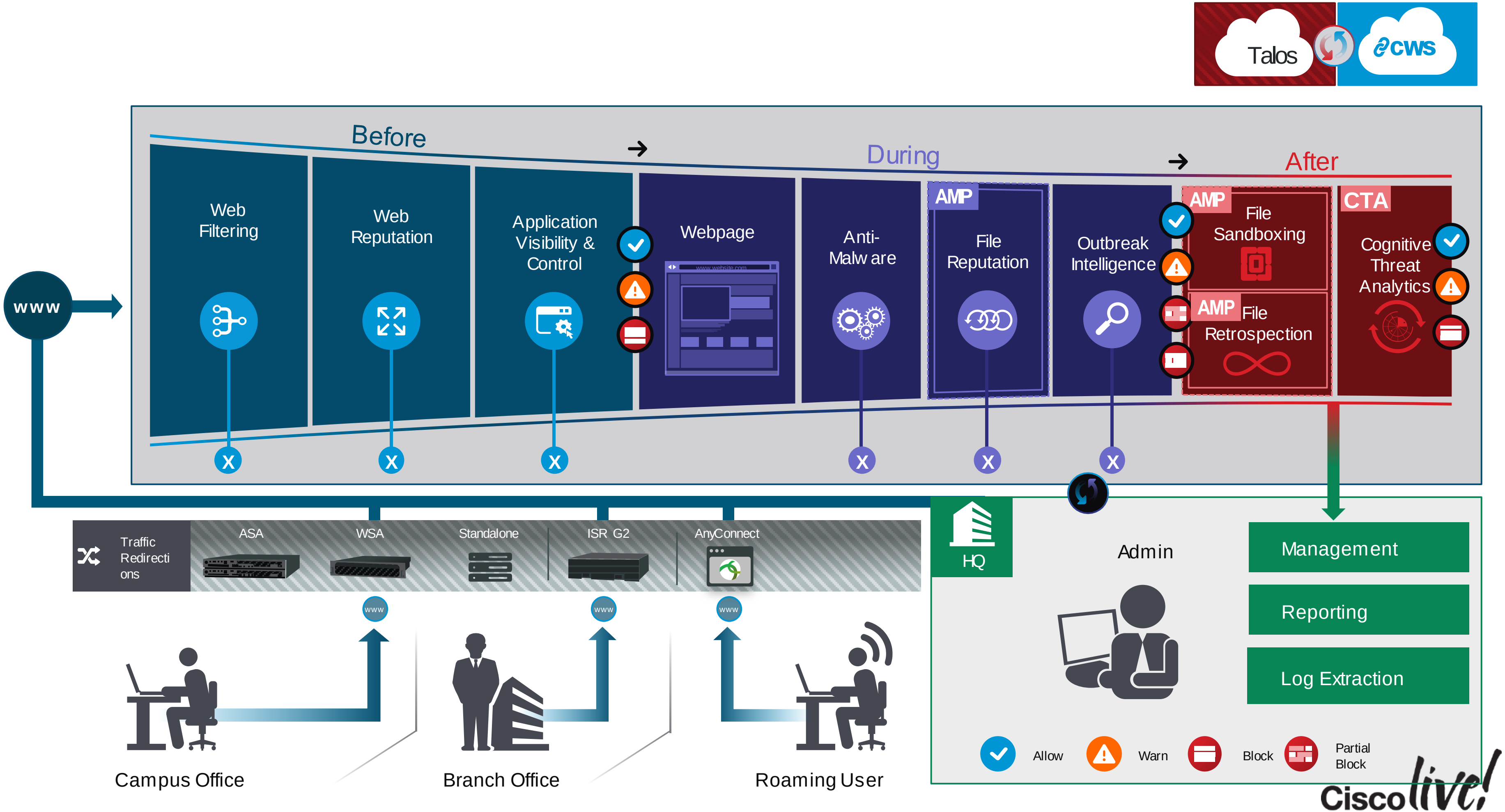
Agenda

- Introduction
- What is Cloud Web Security?
- Protecting Against Advanced Threats
- Live Demo(AMP/CTA)
- Summary



- The Attack Continuum
- Multiple Layers of Protection
- Advanced Malware Protection
  - File Reputation
  - Sandboxing
  - Retrospection
  - AMP Case study
  - AMP Demo
- Cognitive Threat Analytics

Protecting Across the Attack Continuum



Talos

CWS

Before → During → After

Web Filtering

Web Reputation

Application Visibility & Control

Webpage

Anti-Malw are

AMP File Reputation

Outbreak Intelligence

AMP File Sandboxing

AMP File Retrospection

CTA Cognitive Threat Analytics

www

Traffic Redirecti ons

ASA

WSA

Standalone

ISR G2

AnyConnect

Campus Office

Branch Office

Roaming User

HQ

Admin

Management

Reporting

Log Extraction

✓ Allow

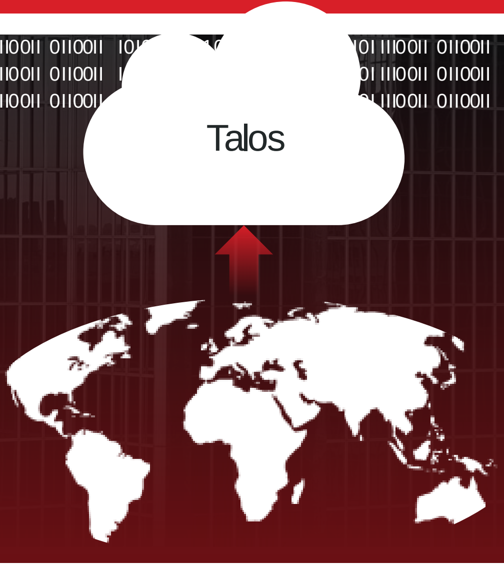
⚠ Warn

Block

Partial Block

Talos - Cisco’s Security Intelligence & Research Group

Threat Focused Global Visibility



Threat Intelligence

Email · Endpoints · Web · Networks · IPS · Devices

- 100 TB Intelligence
- 1.6M sensors
- 150 million+ endpoints
- 35% email worldwide
- FireAMP™, 3+ million
- 13B web requests

- AEGIS™ & SPARK
- Open Source Communities
- 180,000+ Files per Day
- 1B SBRS Queries per Day
- 3.6PB Monthly though CWS

Research Response

600+ Researchers

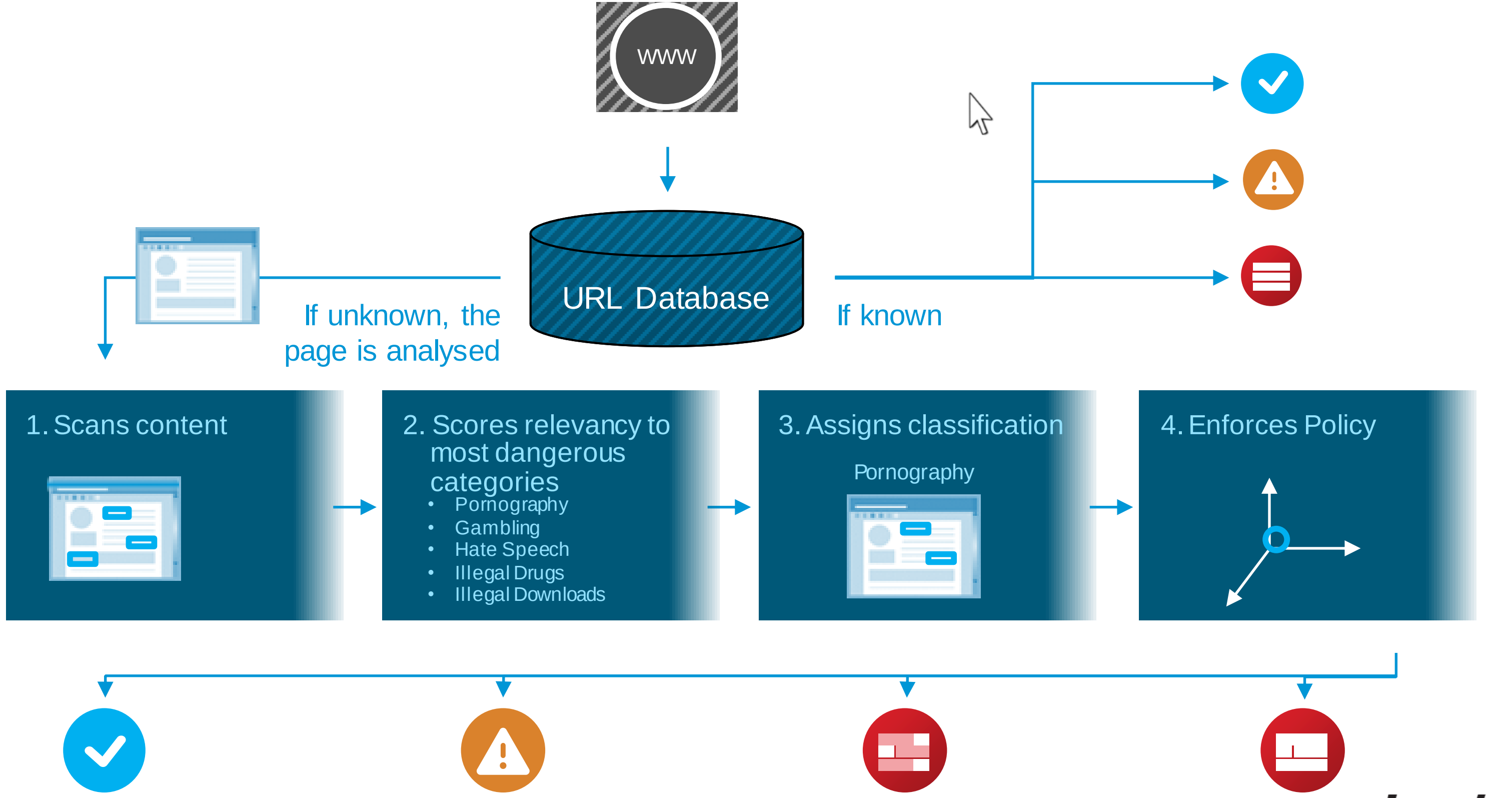
24 • 7 • 365 operations

- Advanced Industry Disclosures
- Outreach Activities
- Dynamic Analysis
- Threat Centric Detection Content
- SEU/SRU
- Sandbox
- VDB
- Security Intelligence
- Email & Web Reputation

Best of Breed Multiple Levels of Protection

Web Filtering

Web Filtering



URL Database

If unknown, the page is analysed

If known

1. Scans content

2. Scores relevancy to most dangerous categories
   - Pornography
   - Gambling
   - Hate Speech
   - Illegal Drugs
   - Illegal Downloads

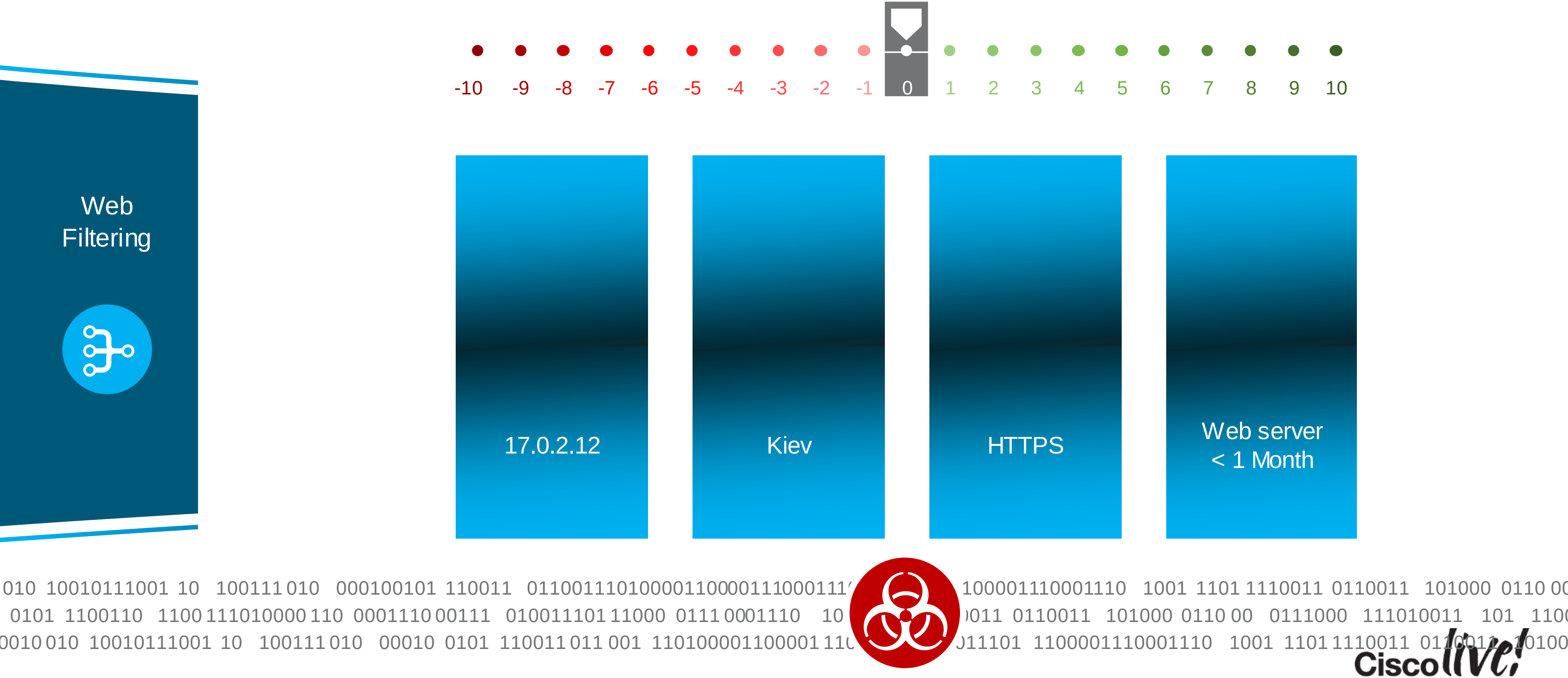
3. Assigns classification

Pornography

4. Enforces Policy

Web Reputation

BEFORE
Discover
Enforce
Harden



Application Visibility and Control (AVC)

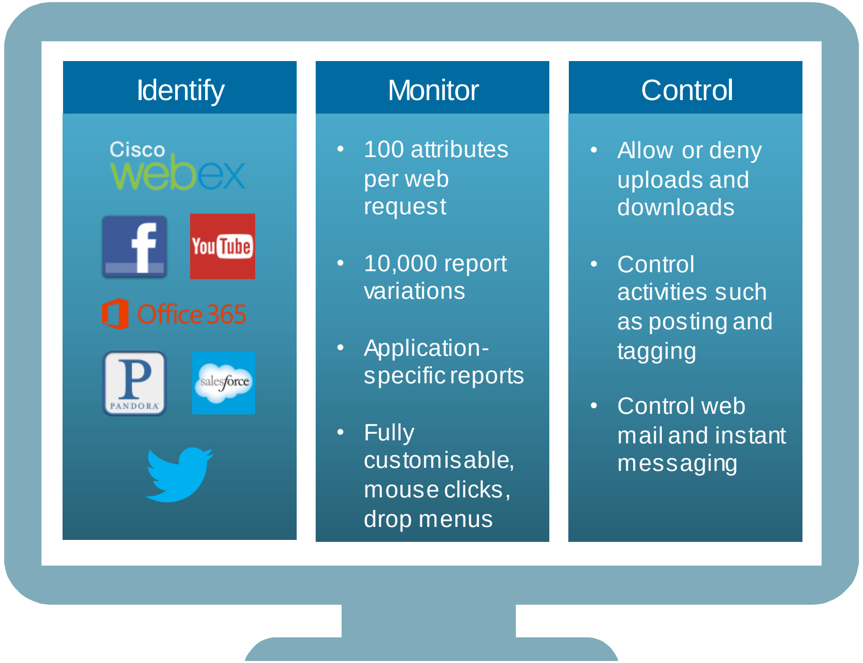
BEFORE DURING AFTER

Web Reputation

Identify application use

Monitor top users

Control application abuse



Identify

Monitor

- 100 attributes per web request
- 10,000 report variations
- Application-specific reports
- Fully customisable, mouse clicks, drop menus

Control

- Allow or deny uploads and downloads
- Control activities such as posting and tagging
- Control web mail and instant messaging

Simple to set

Easy to enforce

Effortless to scale

Cisco live!

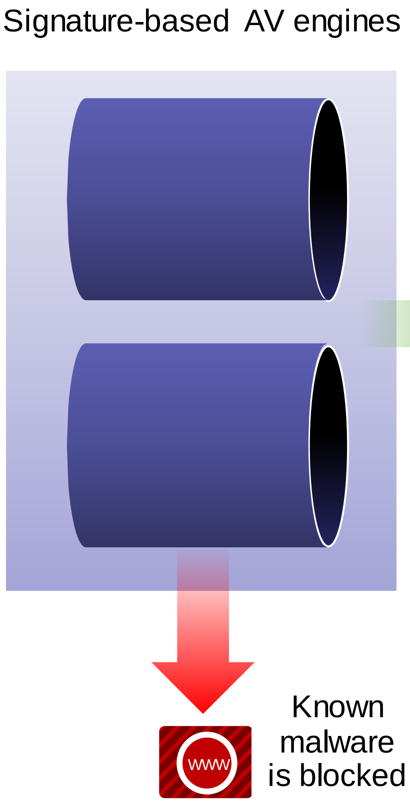
Multiple Anti-Malware Scanning Engines

Anti-Malware

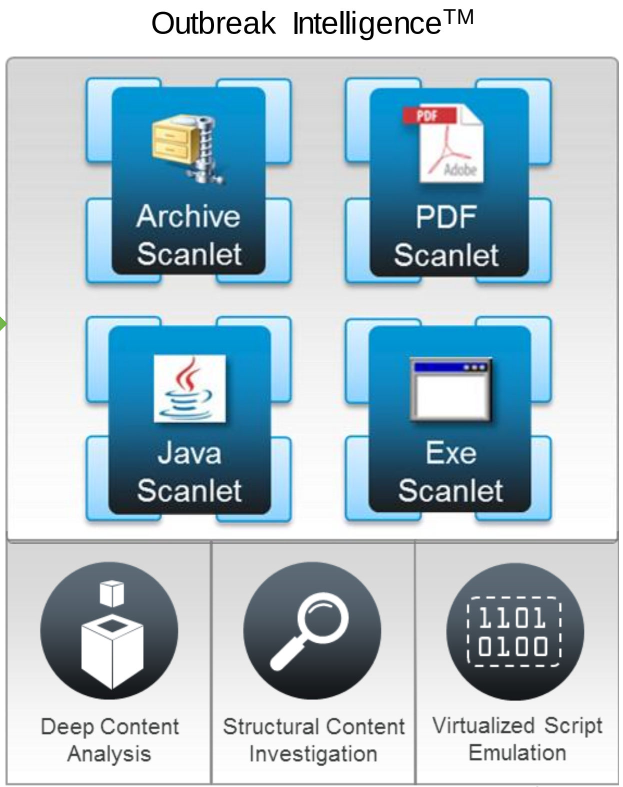
Outbreak Intelligence

Optimises efficiency and catch rate with signature-based scanning engines

Real-time Heuristic engine effectively detects unknown threats and zero hour outbreaks


Signature-based AV engines

Known malware is blocked


Outbreak Intelligence™

Deep Content Analysis

Structural Content Investigation

Virtualized Script Emulation

Is This Really Enough?

- All these best in breed engines are very efficient in detecting and blocking attacks and other malware with proven track records

- However, they are competing against…

Sophistication

Targeted, scope of data

Longer running

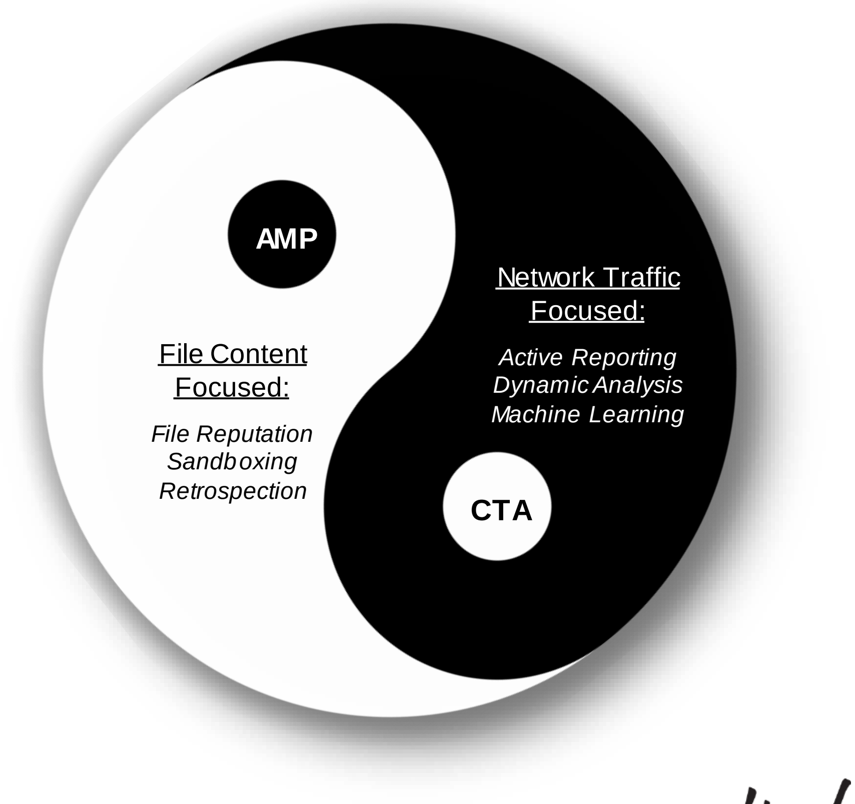
CWS Gives You More

- Cisco CWS provides additional differentiators in the form of AMP and CTA technologies under the CWS Premium licensing
- Full Integration on CWS, covering the During and After phases
- No configuration or fine-tuning required
- AMP provides additional "Point-in-time" protection with inline blocking based on File Reputation
- Retrospective security and continuous analysis
  - AMP Sandboxing engine
  - AMP Retrospection engine
  - Cognitive Threat Analytics

AMP and CTA

Complimenting Each Other

- AMP - Advanced Malware protection
  - Based on files
  - Works from inside-out
  - Focuses on the initial breach
- CTA - Cognitive Threat Analytics
  - Analyses network behaviour
  - Works from outside-in
  - Sees the bigger picture and detects sophisticated attacks such as established Command & Control channels



Advanced Malware Protection (AMP)

AMP on CWS

Advanced Threat Protection

Advanced Malware Protection (AMP)

File Reputation

Increase the accuracy of threat detection by examining every aspect of a file

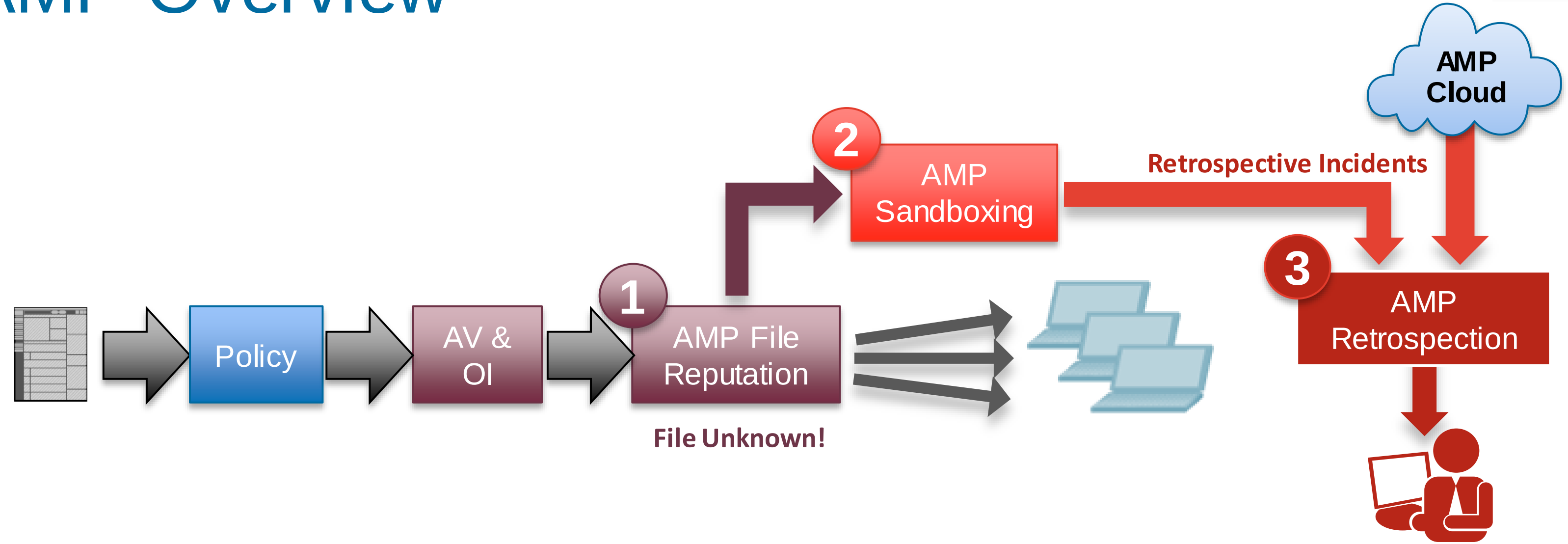
File Sandboxing

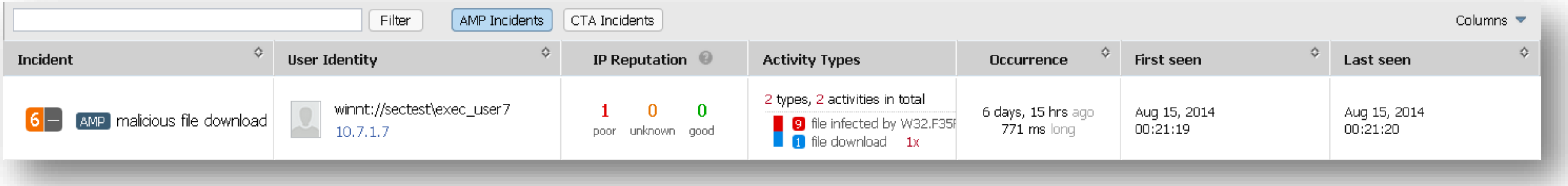
Determine the malicious intent of a file before it enters the network

File Retrospection

Identify a breach faster by tracking a file's disposition over time

AMP Overview



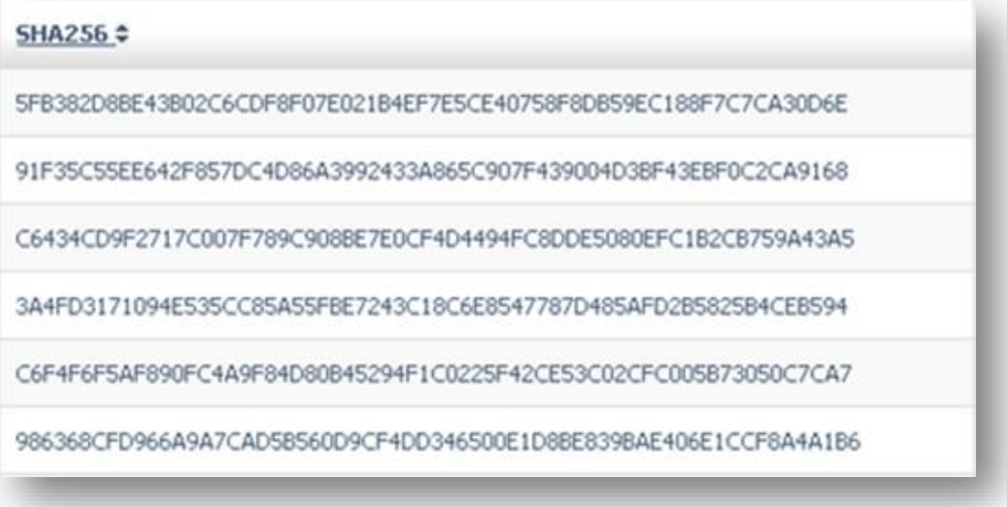


Incident	User Identity	IP Reputation	Activity Types	Occurrence	First seen	Last seen
6 – AMP malicious file download	winnt://sectest\exec_user7 10.7.1.7	1 poor 0 unknown 0 good	2 types, 2 activities in total 9 file infected by W32.F35F 1 file download 1x	6 days, 15 hrs ago 771 ms long	Aug 15, 2014 00:21:19	Aug 15, 2014 00:21:20

Incidents Overview on Threats Tab

AMP - What is SHA256?

- SHA256 is a unique signature assigned to files
- Calculated for all files traversing CWS proxy towers
- Used by AMP to find matching files and detection results



SHA256 ⬍
5FB382D8BE43B02C6CDF8F07E021B4EF7E5CE40758F8DB59EC188F7C7CA30D6E
91F35C55EE642F857DC4D86A3992433A865C907F439004D3BF43EBF0C2CA9168
C6434CD9F2717C007F789C908BE7E0CF4D4494FC8DDE5080EFC1B2CB759A43A5
3A4FD3171094E535CC85A55FBE7243C18C6E8547787D485AFD2B5825B4CEB594
C6F4F6F5AF890FC4A9F84D80B45294F1C0225F42CE53C02CFC005B73050C7CA7
986368CFD966A9A7CAD5B560D9CF4DD346500E1D8BE839BAE406E1CCF8A4A1B6

AMP File Reputation

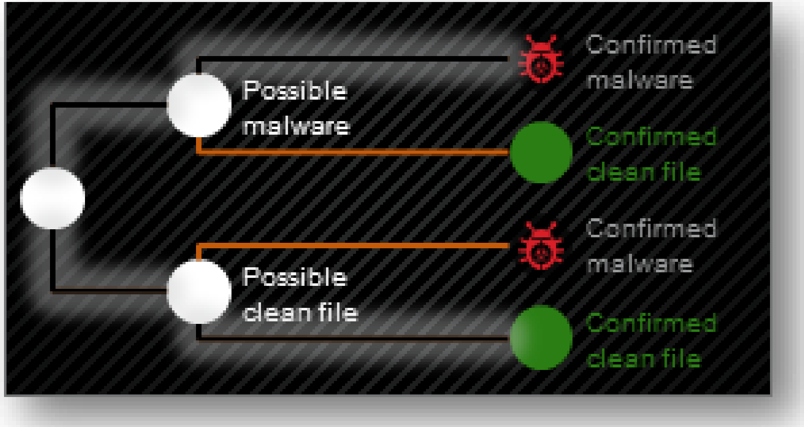
AMP - File Reputation

- Looks at databases of files in real time
- Checks whether they are known to be malware, considered to be clean, or have been considered in the state of unknown for a period of time
- Performs inline blocking based on one-to-one signature matching (static)
- Also incorporates machine learning for additional accuracy (behavioural)

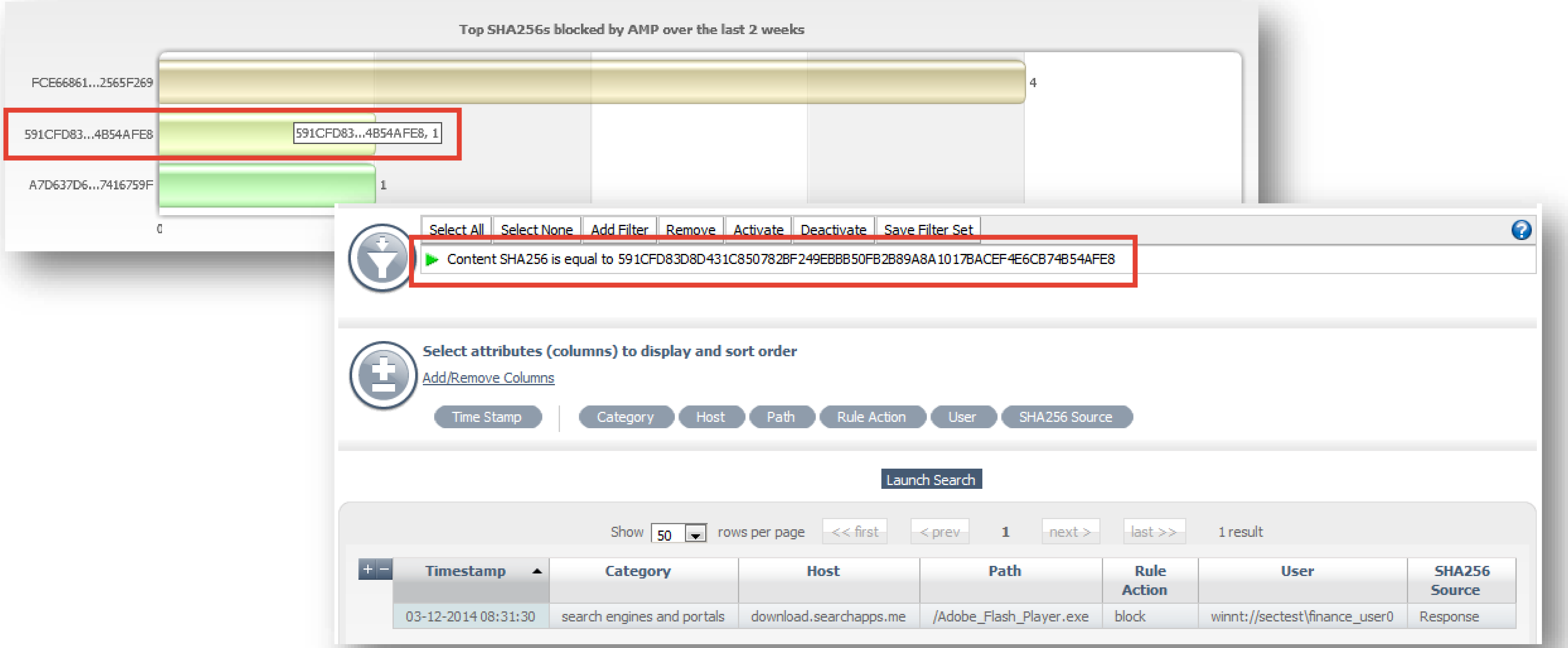
Increase the accuracy of threat detection with Big Data analytics

Machine Learning Decision Tree

- If new files match these classifiers then they are flagged appropriately
- Machine Intelligence can unearth classifiers that humans are unable to find, largely due to the volumes of data analysed



Result: AMP Inline Blocking



Content SHA256 is equal to 591CFD83D8D431C850782BF249EBBB50FB2B89A8A1017BACEF4E6CB74B54AFE8

Select attributes (columns) to display and sort order

Add/Remove Columns

Show 50 rows per page &lt;&lt; first &lt; prev 1 next &gt; last &gt;&gt; 1 result

Timestamp	Category	Host	Path	Rule Action	User	SHA256 Source
03-12-2014 08:31:30	search engines and portals	download.searchapps.me	/Adobe_Flash_Player.exe	block	winnt://sectest\finance_user0	Response

AMP Sandboxing

AMP - Sandboxing

- Files that remain unidentified by AMP are analysed in a sandbox environment in the AMP cloud
- Passed through a decision tree
- Sandboxing verdict updated across AMP cloud
- If found to be malicious, an AMP incident will be created on the Threats page
- Incorporates various engines
  - Advanced Analytics
  - Dynamic Analysis

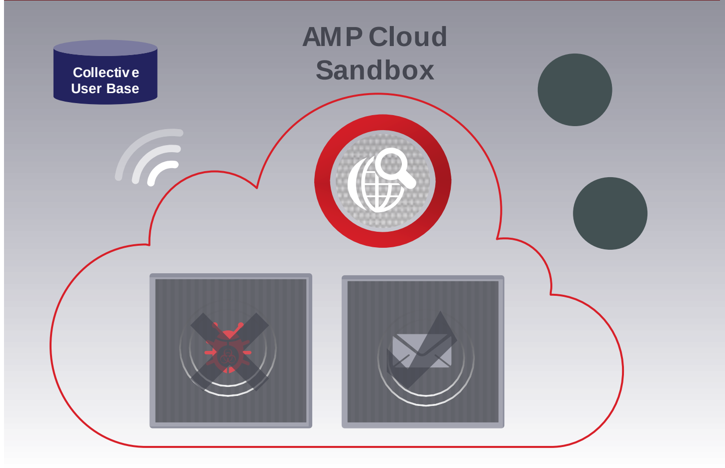
Sandboxes unknown files in the AMP cloud

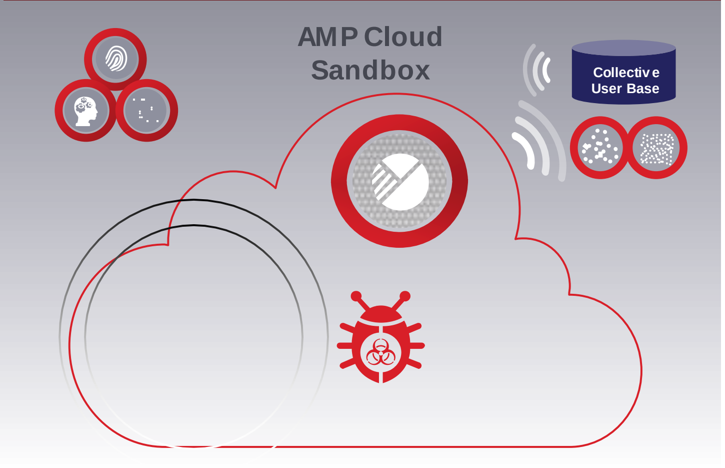
Sandboxing Methods

File Sandboxing - Determines the malicious intent of a file

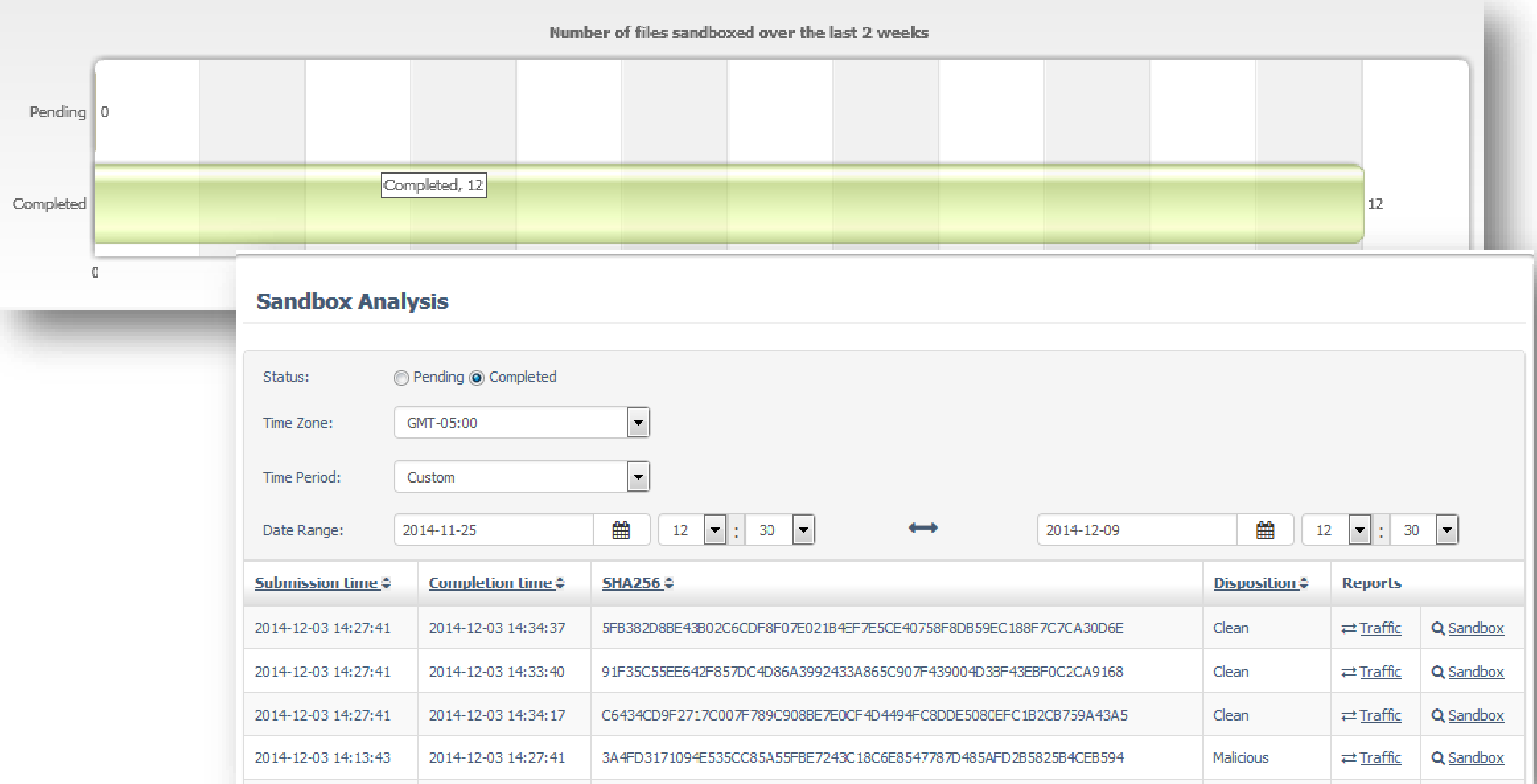
Dynamic Analysis - Analyses unknown malware and assigns a threat score within minutes

Advanced Analytics - Works in tandem with One-to-One, Fuzzy Fingerprinting and Machine learning to identify malware that remains undetected





Sandboxing Result



Sandbox Analysis

Status: ○ Pending ● Completed

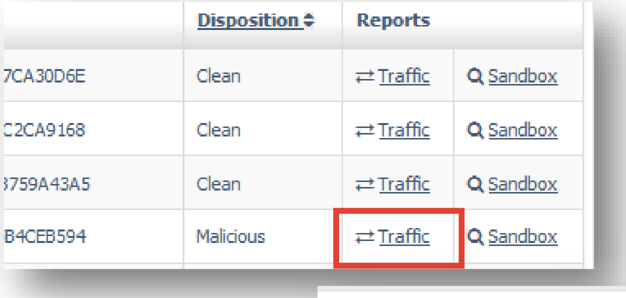
Time Zone: GMT-05:00

Time Period: Custom

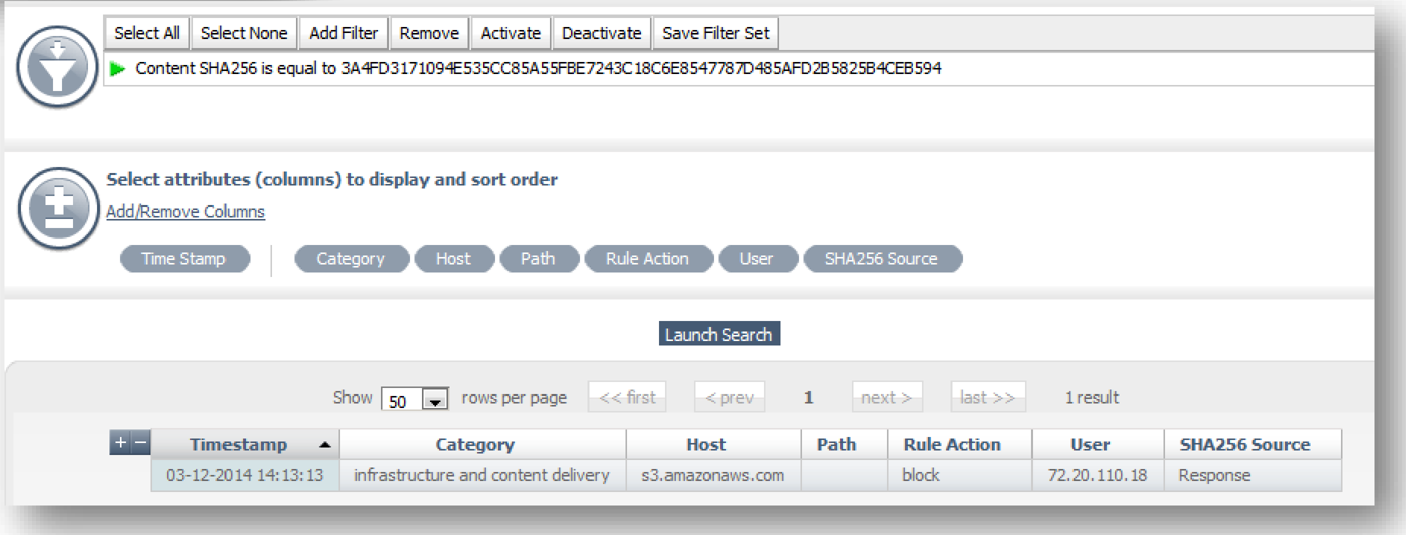
Date Range: 2014-11-25 12 : 30 ⟷ 2014-12-09 12 : 30

Submission time	Completion time	SHA256	Disposition	Reports	
2014-12-03 14:27:41	2014-12-03 14:34:37	5FB382D8BE43B02C6CDF8F07E021B4EF7E5CE40758F8DB59EC188F7C7CA30D6E	Clean	⇄ Traffic	Sandbox
2014-12-03 14:27:41	2014-12-03 14:33:40	91F35C55EE642F857DC4D86A3992433A865C907F439004D3BF43EBF0C2CA9168	Clean	⇄ Traffic	Sandbox
2014-12-03 14:27:41	2014-12-03 14:34:17	C6434CD9F2717C007F789C908BE7E0CF4D4494FC8DDE5080EFC1B2CB759A43A5	Clean	⇄ Traffic	Sandbox
2014-12-03 14:13:43	2014-12-03 14:27:41	3A4FD3171094E535CC85A55FBE7243C18C6E8547787D485AFD2B5825B4CEB594	Malicious	⇄ Traffic	Sandbox

Traffic Report



	Disposition ⬍	Reports	
7CA30D6E	Clean	⇄ Traffic	🔍 Sandbox
C2CA9168	Clean	⇄ Traffic	🔍 Sandbox
3759A43A5	Clean	⇄ Traffic	🔍 Sandbox
B4CEB594	Malicious	⇄ Traffic	🔍 Sandbox



▶ Content SHA256 is equal to 3A4FD3171094E535CC85A55FBE7243C18C6E8547787D485AFD2B5825B4CEB594

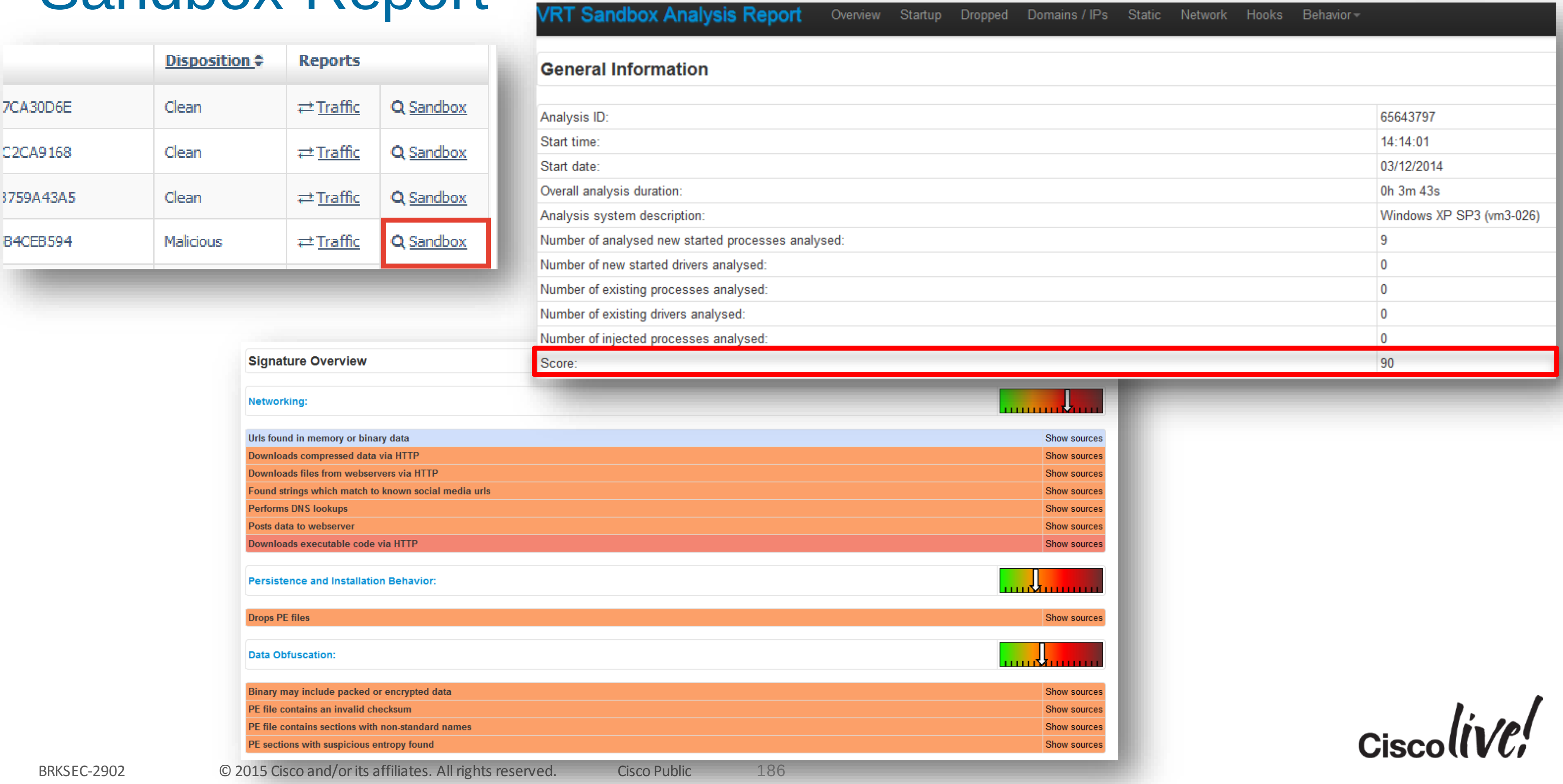
Select attributes (columns) to display and sort order

Add/Remove Columns

Show 50 rows per page << first < prev 1 next > last >> 1 result

Timestamp ▲	Category	Host	Path	Rule Action	User	SHA256 Source
03-12-2014 14:13:13	infrastructure and content delivery	s3.amazonaws.com		block	72.20.110.18	Response

Sandbox Report



	Disposition ⇕	Reports	
7CA30D6E	Clean	⇄ Traffic	🔍 Sandbox
C2CA9168	Clean	⇄ Traffic	🔍 Sandbox
3759A43A5	Clean	⇄ Traffic	🔍 Sandbox
B4CEB594	Malicious	⇄ Traffic	🔍 Sandbox

General Information

Analysis ID:	65643797
Start time:	14:14:01
Start date:	03/12/2014
Overall analysis duration:	0h 3m 43s
Analysis system description:	Windows XP SP3 (vm3-026)
Number of analysed new started processes analysed:	9
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Score:	90

Signature Overview

Networking:

Urls found in memory or binary data	Show sources
Downloads compressed data via HTTP	Show sources
Downloads files from webservers via HTTP	Show sources
Found strings which match to known social media urls	Show sources
Performs DNS lookups	Show sources
Posts data to webserver	Show sources
Downloads executable code via HTTP	Show sources

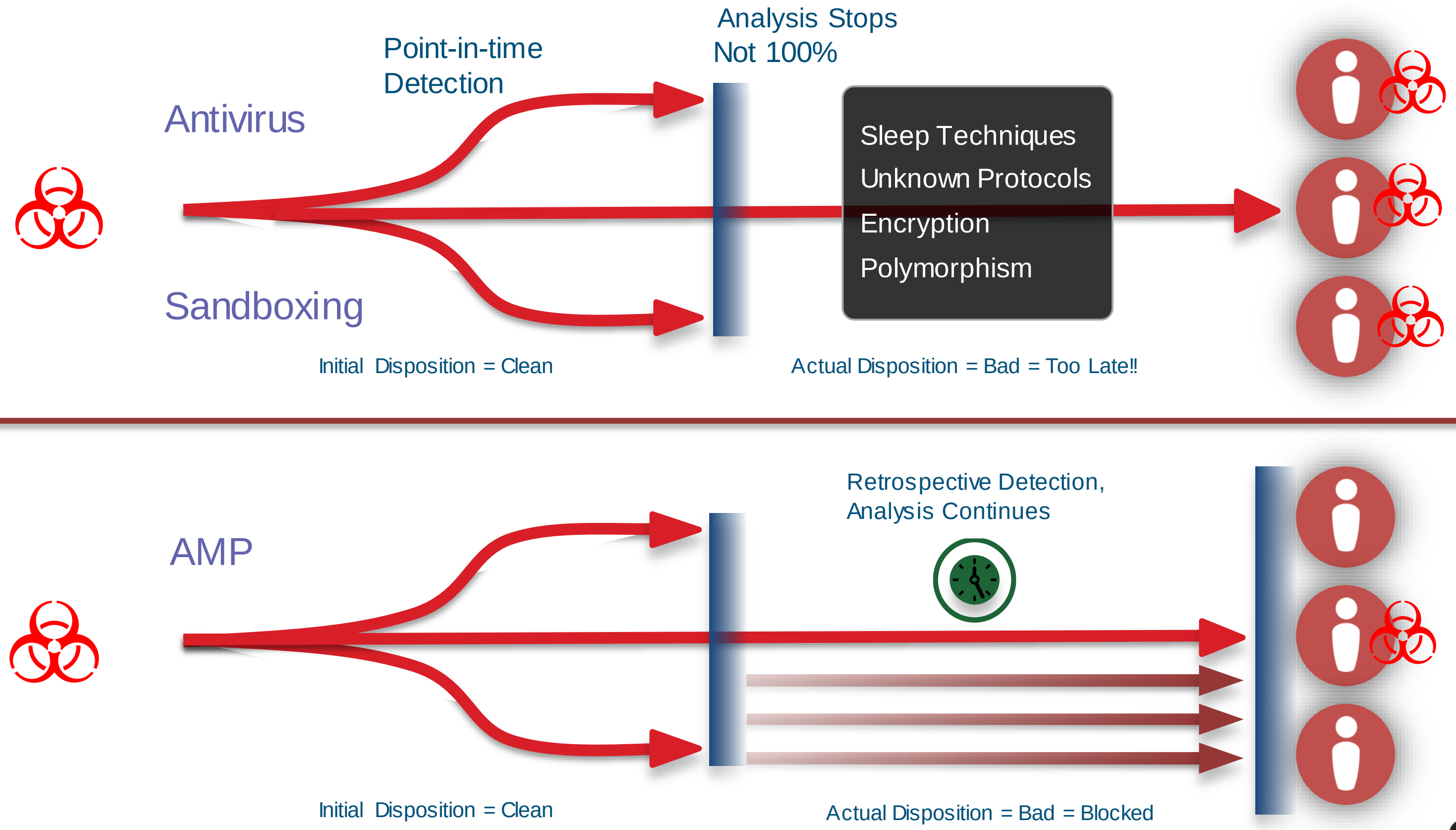
Persistence and Installation Behavior:

Drops PE files	Show sources

Data Obfuscation:

Binary may include packed or encrypted data	Show sources
PE file contains an invalid checksum	Show sources
PE file contains sections with non-standard names	Show sources
PE sections with suspicious entropy found	Show sources

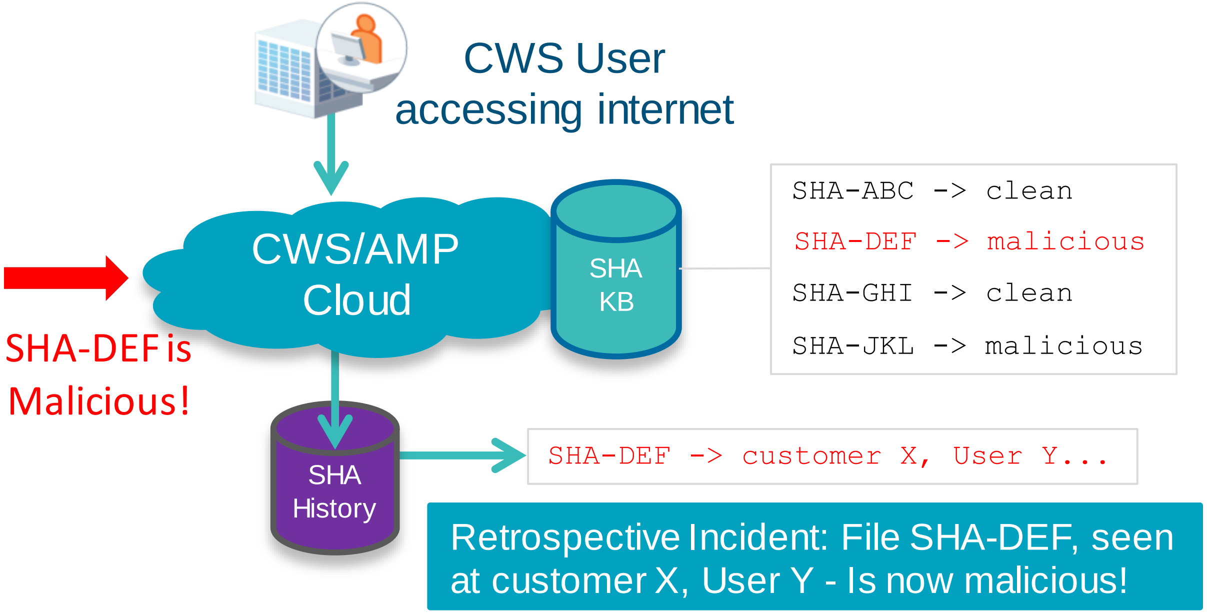
Is THIS Really Enough?



AMP Retrospection

AMP Cloud - SHA Knowledge-Base

- AMP maintains a large cloud-based knowledge-base of hundreds of millions of files, constantly evolving and expanding from several sources:
  - AMP Sandbox
  - Behaviour detection
  - AMP for Endpoints
  - AMP for Networks
  - Feed updates

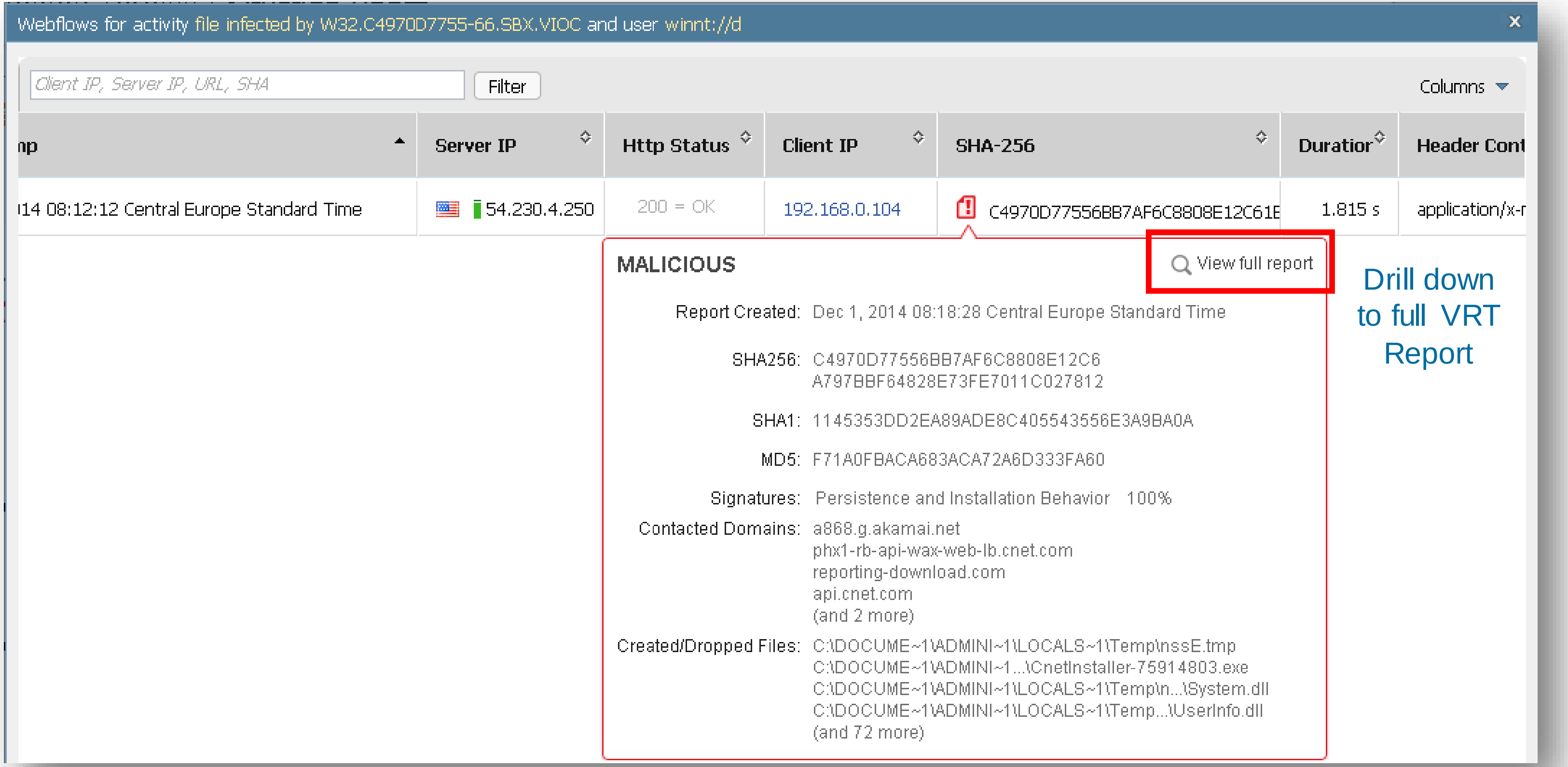


```
SHA-ABC -> clean
SHA-DEF -> malicious
SHA-GHI -> clean
SHA-JKL -> malicious
```

```
SHA-DEF -> customer X, User Y...
```

Retrospective Incident: File SHA-DEF, seen at customer X, User Y - Is now malicious!

AMP - Retrospective Incident



Webflows for activity file infected by W32.C4970D7755-66.SBX.VIOC and user winnt://d

np	Server IP	Http Status	Client IP	SHA-256	Duratior	Header Cont
14 08:12:12 Central Europe Standard Time	54.230.4.250	200 = OK	192.168.0.104	C4970D77556BB7AF6C8808E12C61E	1.815 s	application/x-r

MALICIOUS

Report Created: Dec 1, 2014 08:18:28 Central Europe Standard Time

SHA256: C4970D77556BB7AF6C8808E12C6
A797BBF64828E73FE7011C027812

SHA1: 1145353DD2EA89ADE8C405543556E3A9BA0A

MD5: F71A0FBACA683ACA72A6D333FA60

Signatures: Persistence and Installation Behavior 100%

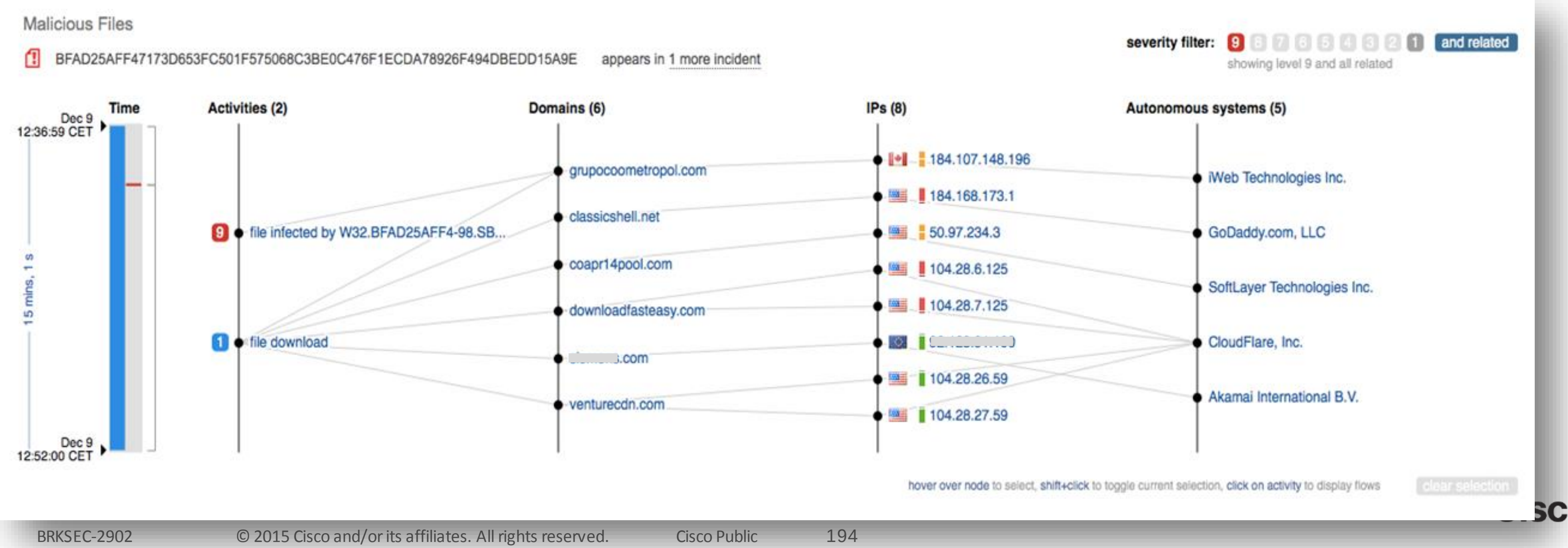
Contacted Domains: a868.g.akamai.net
phx1-rb-api-wax-web-lb.cnet.com
reporting-download.com
api.cnet.com
(and 2 more)

Created/Dropped Files: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nssE.tmp
C:\DOCUME~1\ADMINI~1...\CnetInstaller-75914803.exe
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\n...\System.dll
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp...\UserInfo.dll
(and 72 more)

Drill down to full VRT Report

AMP - Case Study

- Unknown file is downloaded by CWS user (zero detects on external verification)
- File is submitted to the sandbox in AMP cloud
- Sandbox classifies as malicious, provides retrospective alert to Admin



Malicious Files

BFAD25AFF47173D653FC501F575068C3BE0C476F1ECDA78926F494DBEDD15A9E appears in 1 more incident

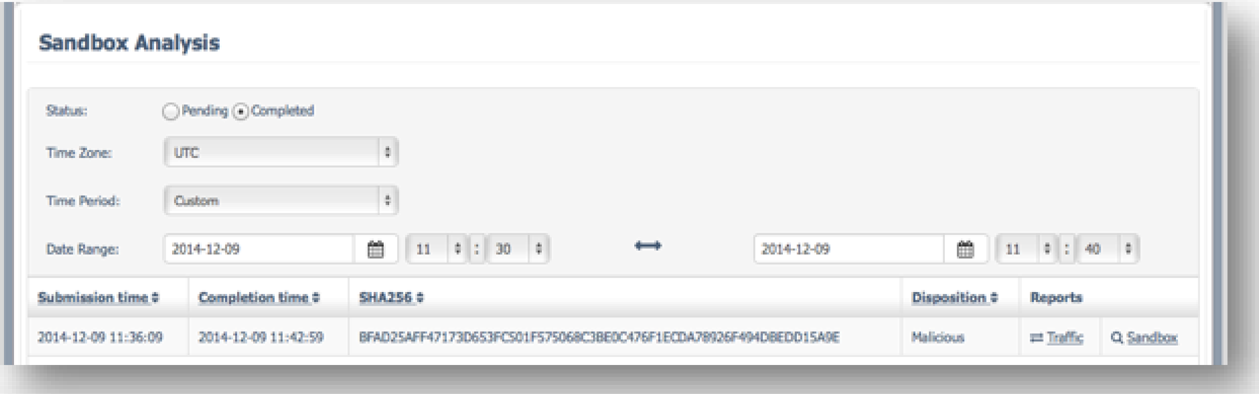
severity filter: 9 8 7 6 5 4 3 2 1 and related

showing level 9 and all related

hover over node to select, shift+click to toggle current selection, click on activity to display flows

AMP - Case Study

- Over the next 12 hours the file was detected and blocked for users of 9 other CWS enterprise customers
- Same file was also detected by FireAMP, ESA, WSA & FireSight deployments



Sandbox Analysis

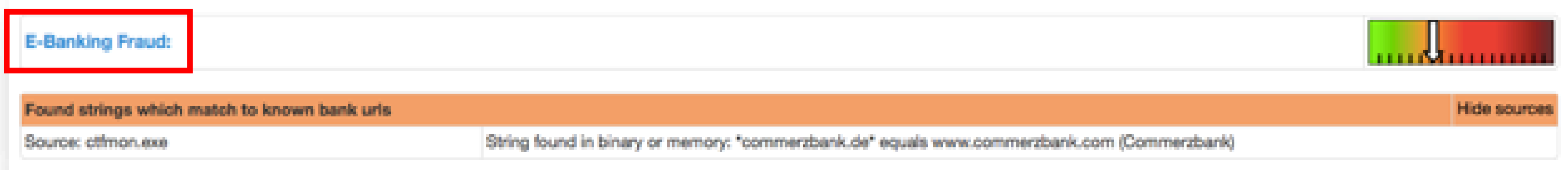
Status: ○ Pending ● Completed

Time Zone: UTC

Time Period: Custom

Date Range: 2014-12-09 11 : 30 ⟷ 2014-12-09 11 : 40

Submission time	Completion time	SHA256	Disposition	Reports	
2014-12-09 11:36:09	2014-12-09 11:42:59	BFAD25AFF47173D653FC501F575068C3BE0C476F1ECDA78926F494D8EDD15A9E	Malicious	Traffic	Sandbox



E-Banking Fraud:

Found strings which match to known bank urls	Hide sources
Source: ctfmon.exe	String found in binary or memory: "commerzbank.de" equals www.commerzbank.com (Commerzbank)

AMP Demo

Agenda

- Introduction
- What is Cloud Web Security?
- Protecting Against Advanced Threats
- Live Demo(AMP/CTA)
- Summary

- The Attack Continuum
- Multiple Layers of Protection
- Advanced Malware Protection
- Cognitive Threat Analytics
    - Architecture and Capabilities
    - CTA Case Studies
    - CTA Demo

Cognitive Threat Analytics (CTA)

CTA - Network Traffic Behaviour Analysis

Behaviour Analysis

Machine Learning

Anomaly Detection

Reduced time to discovery

Active, continuous monitoring to stop the spread of an attack

Normal… or not?

Spots symptoms of infection using behavioural anomaly detection algorithms and trust modelling

Security that learn

Uses machine learning and Big Data Analytics to learn from what it sees and adapts over time

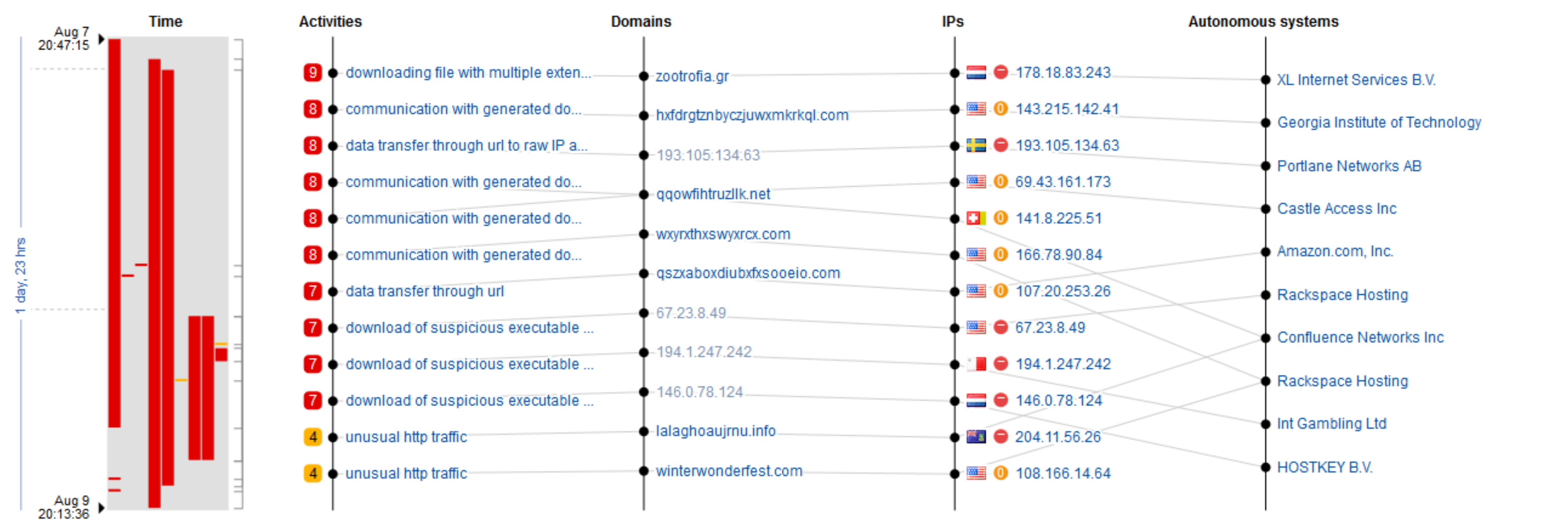
No more rule sets

Discovers threats on its own… just turn it on

CTA Architecture and Capabilities

CTA Incident Drilldown

- Presented visually on the Parallel Coordinates within Incident detailed view
- While many of the individual activities alone are supposedly innocent, CTA ties them together, constructing a complete incident, often spread over multiple days



Activities

- 9 downloading file with multiple exten...
- 8 communication with generated do...
- 8 data transfer through url to raw IP a...
- 8 communication with generated do...
- 8 communication with generated do...
- 8 communication with generated do...
- 7 data transfer through url
- 7 download of suspicious executable ...
- 7 download of suspicious executable ...
- 7 download of suspicious executable ...
- 4 unusual http traffic
- 4 unusual http traffic

Domains

- zootrofia.gr
- hxfdrgtznbyczjuwxmkrkql.com
- 193.105.134.63
- qqowfihtruzllk.net
- wxyrxthxswyxrcx.com
- qszxaboxdiubxfxsooeio.com
- 67.23.8.49
- 194.1.247.242
- 146.0.78.124
- lalaghoaujrnu.info
- winterwonderfest.com

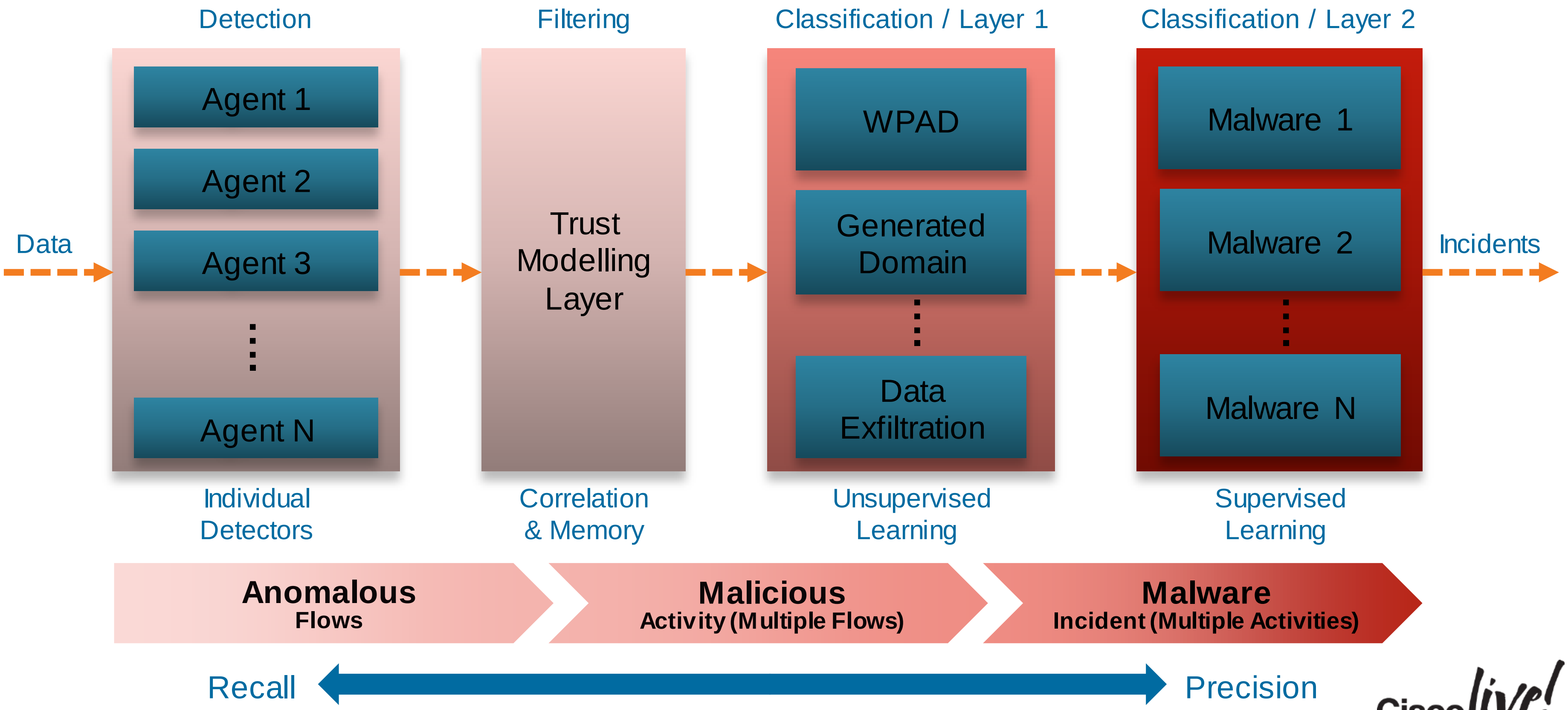
IPs

- 178.18.83.243
- 143.215.142.41
- 193.105.134.63
- 69.43.161.173
- 141.8.225.51
- 166.78.90.84
- 107.20.253.26
- 67.23.8.49
- 194.1.247.242
- 146.0.78.124
- 204.11.56.26
- 108.166.14.64

Autonomous systems

- XL Internet Services B.V.
- Georgia Institute of Technology
- Portlane Networks AB
- Castle Access Inc
- Amazon.com, Inc.
- Rackspace Hosting
- Confluence Networks Inc
- Rackspace Hosting
- Int Gambling Ltd
- HOSTKEY B.V.

CTA - Layered Detection Engine



Detection

Filtering

Classification / Layer 1

Classification / Layer 2

Data

Agent 1

Agent 2

Agent 3

Agent N

Trust Modelling Layer

WPAD

Generated Domain

Data Exfiltration

Malware 1

Malware 2

Malware N

Incidents

Individual Detectors

Correlation & Memory

Unsupervised Learning

Supervised Learning

Anomalous
Flows

Malicious
Activity (Multiple Flows)

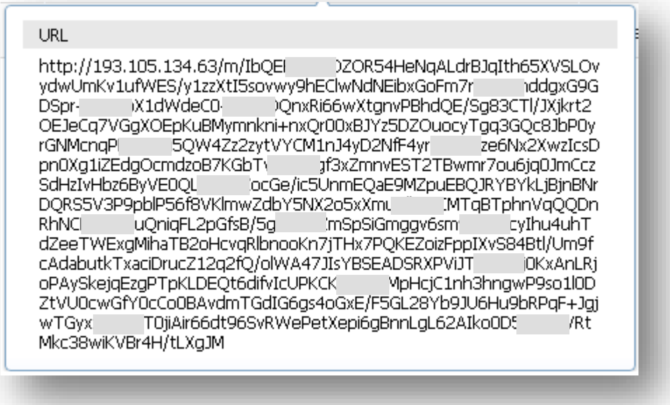
Malware
Incident (Multiple Activities)

Recall

Precision

Attack Techniques Detected

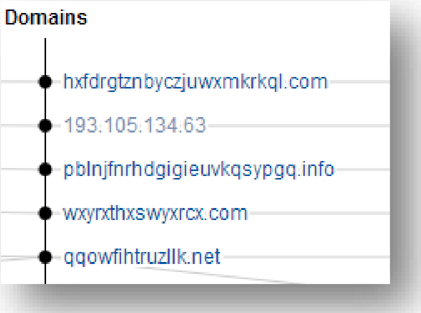
- Data tunnelling via URL
  - Command and control channel using URL
  - Data is encoded and often encrypted



URL

```
http://193.105.134.63/m/IbQE[redacted]ZOR54HeNqALdrBJqIth65XVSLOv
ydwUmKv1ufWES/y1zzXtI5sovwy9hEClwNdNEibxGoFm7r[redacted]ddgxG9G
DSpr-[redacted]X1dWdeC0-[redacted]QnxRi66wXtgnvPBhdQE/Sg83CTl/JXjkrt2
OEJeCq7VGgXOEpKuBMymnkni+nxQr00xBJYz5DZOuocyTgq3GQc8JbP0y
rGNMcnqP[redacted]5QW4Zz2zytVYCM1nJ4yD2NfF4yr[redacted]ze6Nx2XwzIcsD
pn0Xg1iZEdgOcmdzoB7KGbT[redacted]gf3xZmnvEST2TBwmr7ou6jq0JmCcz
SdHzIvHbz6ByVE0QL[redacted]ocGe/ic5UnmEQaE9MZpuEBQJRYBYkLjBjnBNr
DQRS5V3P9pblP56f8VKlmwZdbY5NX2o5xXmu[redacted]MTqBTphnVqQQDn
RhNC[redacted]uQniqFL2pGfsB/5g[redacted]mSpSiGmggv6sm[redacted]cyIhu4uhT
dZeeTWExgMihaTB2oHcvqRlbnooKn7jTHx7PQKEZoizFppIXvS84Btl/Um9f
cAdabutkTxaciDrucZ12q2fQ/olWA47JIsYBSEADSRXPViJT[redacted]0KxAnLRj
oPAySkejqEzgPTpKLDEQt6difvIcUPKCK[redacted]MpHcjC1nh3hngwP9so1l0D
ZtVU0cwGfY0cCo0BAvdmTGdIG6gs4oGxE/F5GL28Yb9JU6Hu9bRPqF+Jgj
wTGyx[redacted]T0jiAir66dt96SvRWePetXepi6gBnnLgL62AIko0D5[redacted]/Rt
Mkc38wiKVBr4H/tLXgJM
```

- Communication with generated domain
  - Domains created very recently
  - Often comprised of random-looking characters or words
  - Used as rendezvous points for botnet infections
  - Sophisticated malware infrastructure

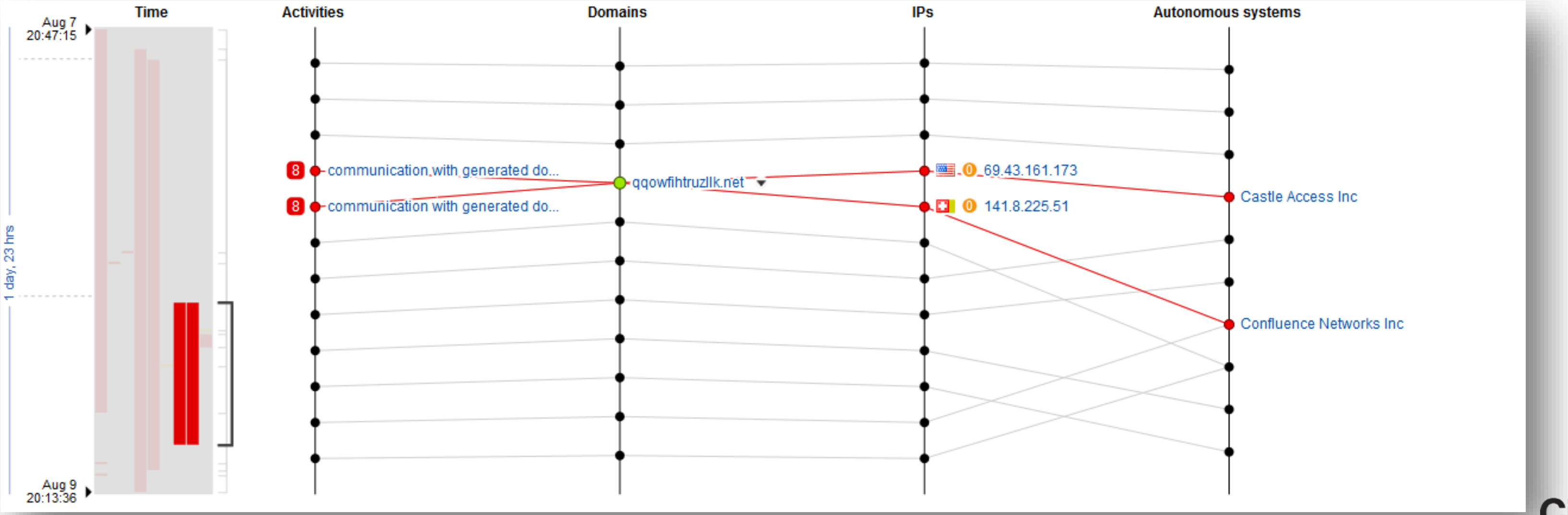


Domains

- hxfdrgtznbyczjuwxmkrkql.com
- 193.105.134.63
- pblnjfnrhdgigieuvkqsypgq.info
- wxyrxthxswyxrcx.com
- qqowfihtruzllk.net

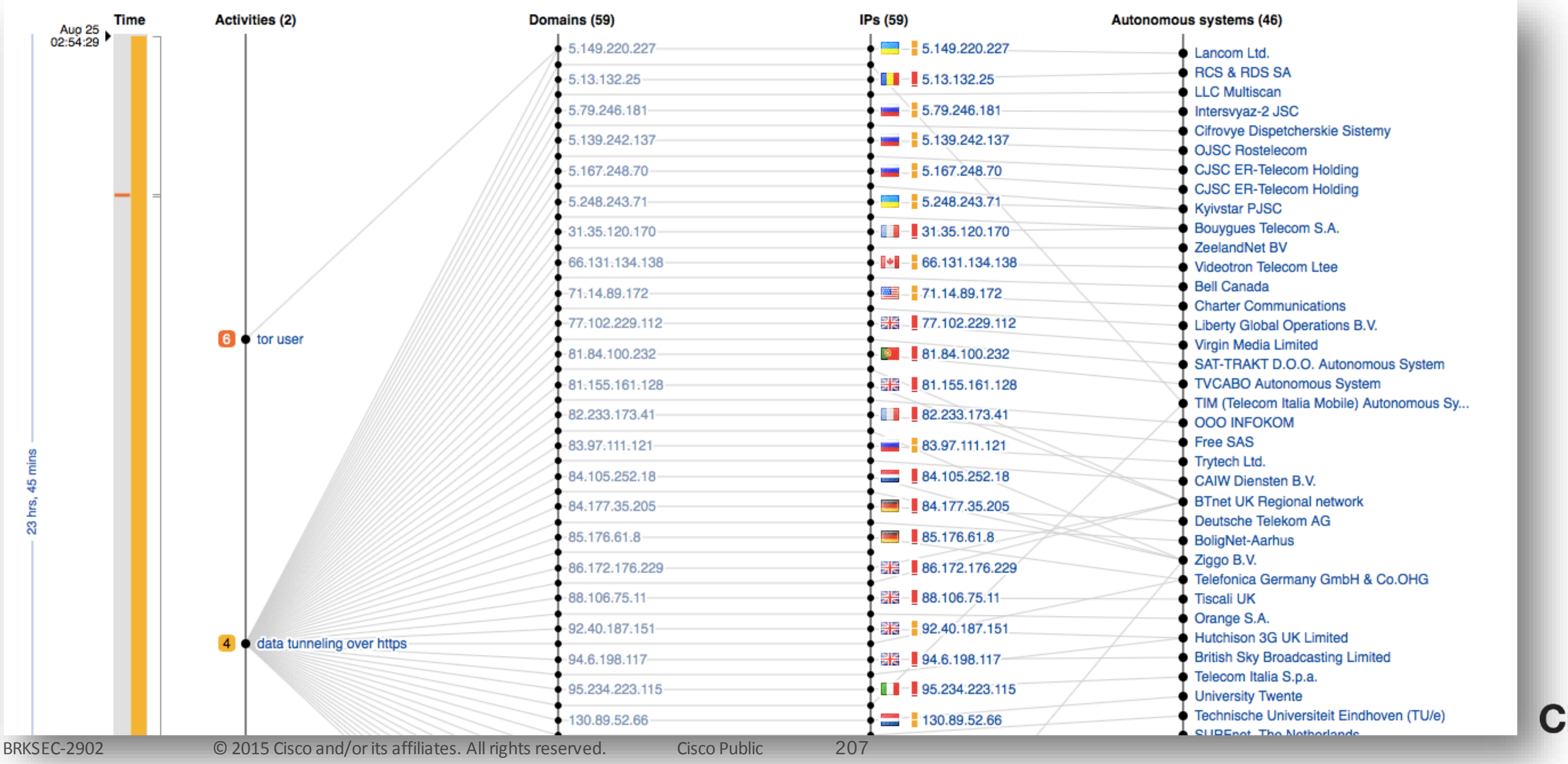
Example - Generated Domain

- The domain identified is clearly a generated domain
- Parallel Coordinates powerfully demonstrates relationship between activity, risk, domain and IP, global reputation, and autonomous system in the time context

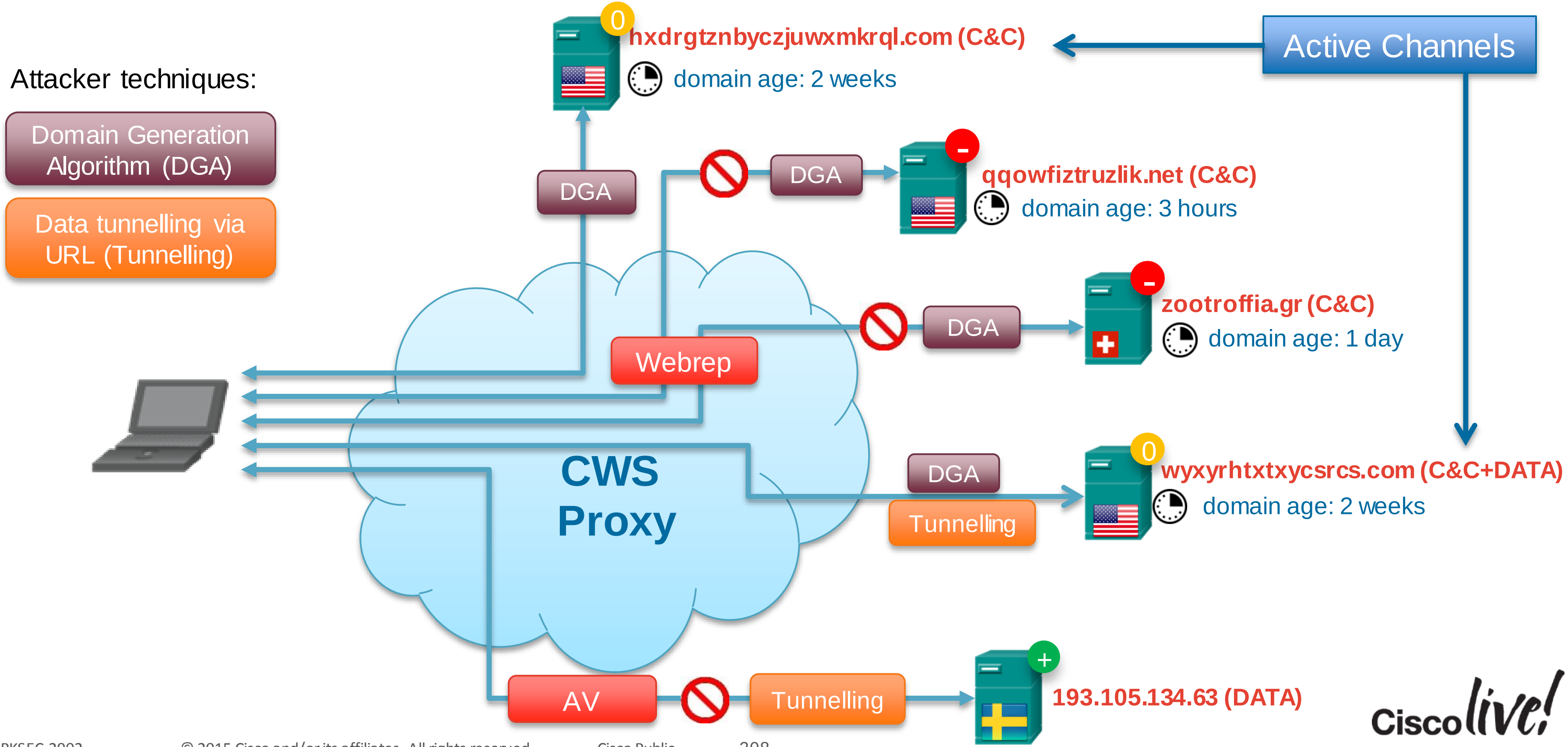


Example - TOR

- Distinguishes TOR by time, sequences, and recognition of hidden IP’s

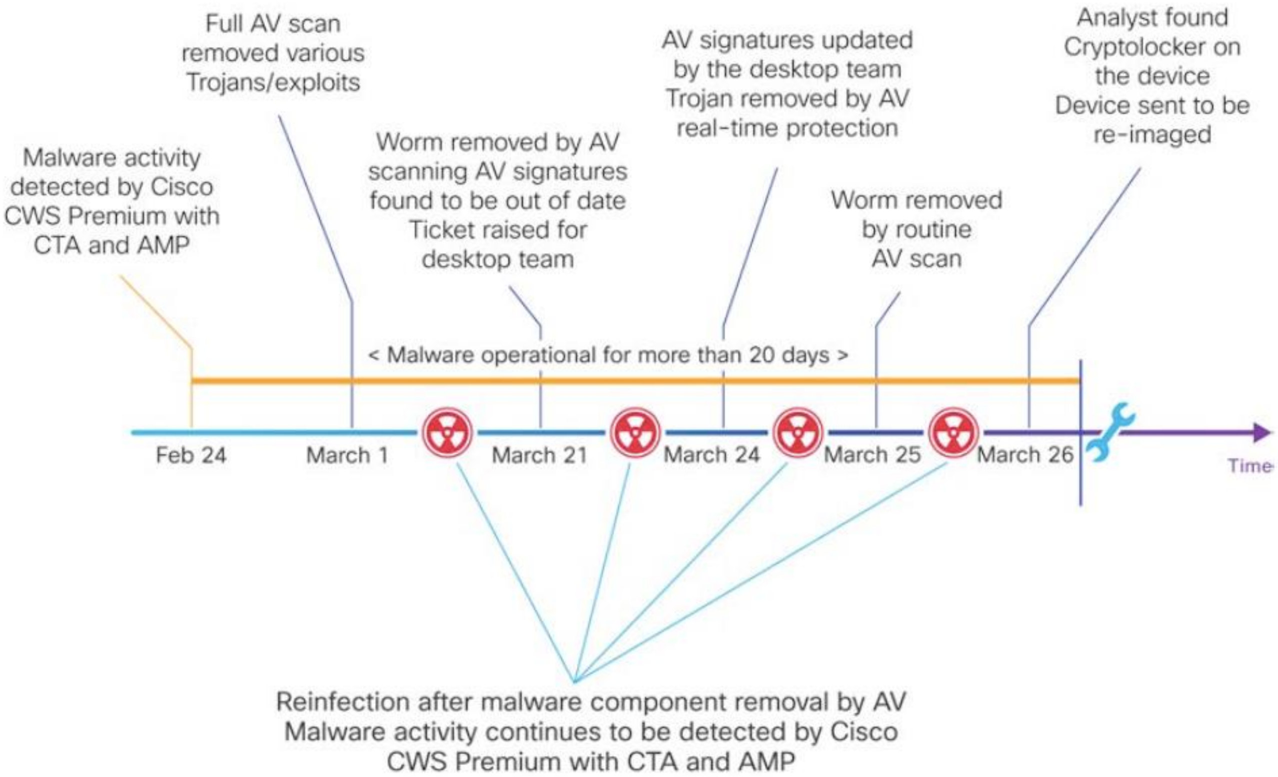


CTA Full Flow Example



CTA Case Studies

Case Study 1 - Repeated Infections



Malware activity detected by Cisco CWS Premium with CTA and AMP
Full AV scan removed various Trojans/exploits
Worm removed by AV scanning AV signatures found to be out of date Ticket raised for desktop team
AV signatures updated by the desktop team Trojan removed by AV real-time protection
Worm removed by routine AV scan
Analyst found Cryptolocker on the device Device sent to be re-imaged
< Malware operational for more than 20 days >
Feb 24
March 1
March 21
March 24
March 25
March 26
Time

Reinfection after malware component removal by AV
Malware activity continues to be detected by Cisco
CWS Premium with CTA and AMP

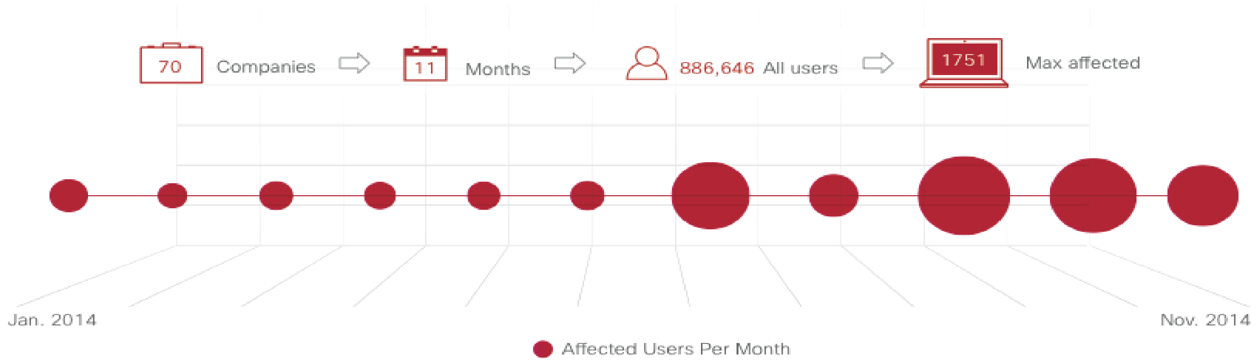
Example of HTTP request (anonymised and truncated)

http://109.XXX.XX.XXX/m/IbQXXXVjjpc
E6+54HXXXdmmGcNZxtMZdvqyB5EkJ
AUmL/1sOXXXvq5zzXtIu9SzgnJhj
WlxdE7FiqDEYFm5A+TPlXXXQpGhxG
u0r3WLZoX1KHnCShKJDAufwiISy69w
Apgn4e79NFw/108XXX.g+fq4XXX
OTYke6uhGHDOEeqje76v7z7i+wgqXX
XFBuMz5k08yocxOH63bwQ9JMfwy8u
NRM...

CTA Case Study 2 - Malvertising Botnet

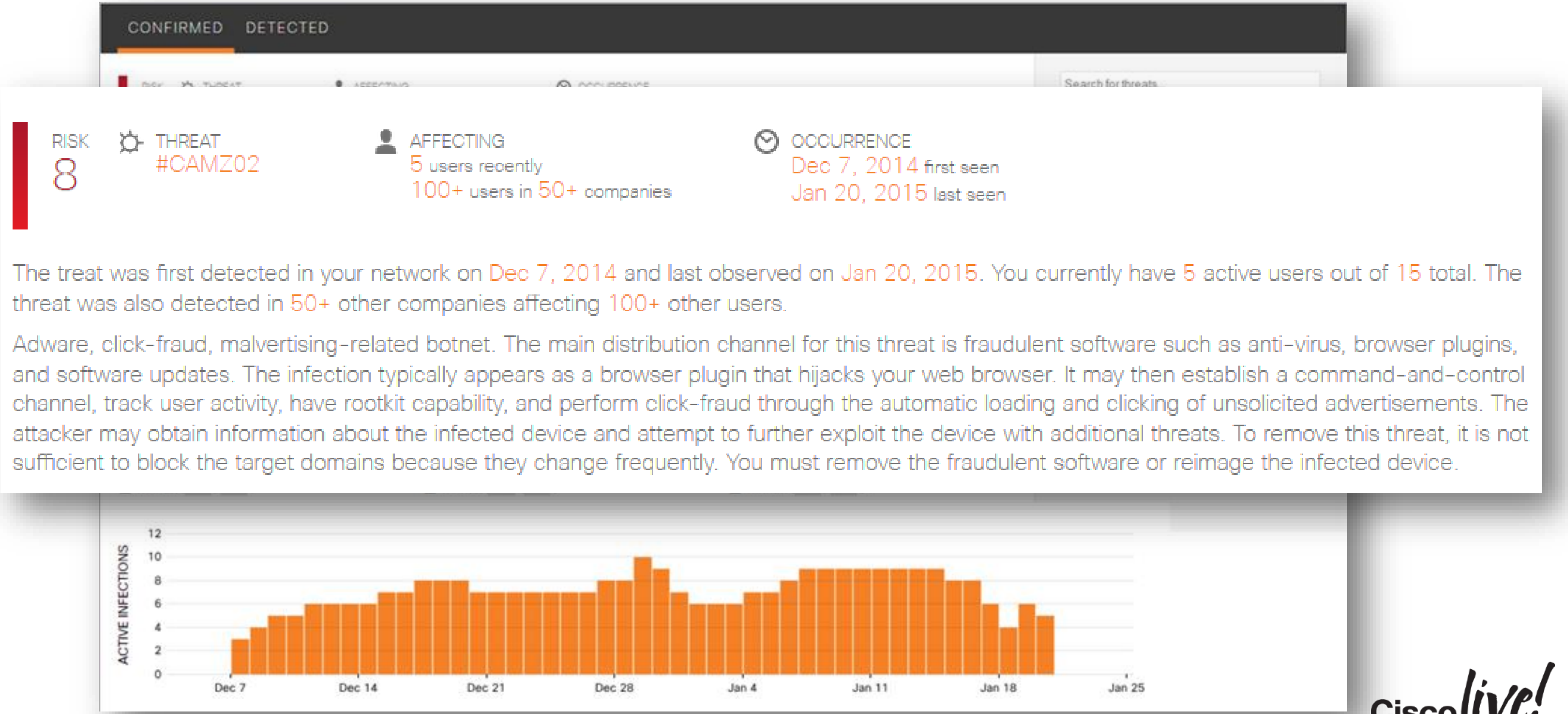
- Malvertising from Browser add-ons inflicts slight damage on each user to collect huge rewards. Close to 2000 users were affected by this Botnet
- Sophisticated code paired with refined business model
- Cisco security finds 4000+ add-on names

Figure 18. Number of Affected Users Per Month, Jan. through Nov. 2014



Source: Cisco Security Research

CTA Case Study 2 - Malvertising Botnet



RISK 8

THREAT #CAMZ02

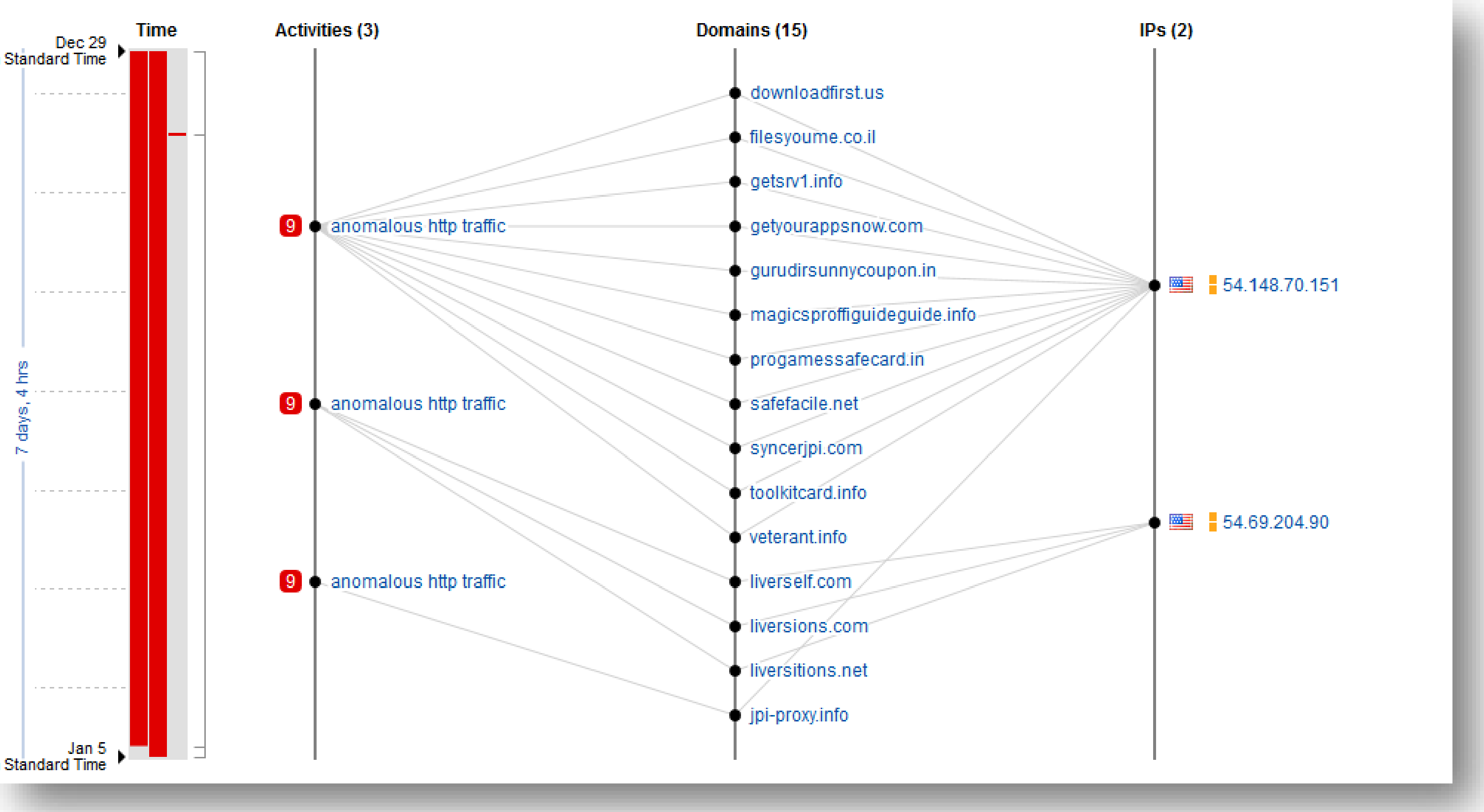
AFFECTING
5 users recently
100+ users in 50+ companies

OCCURRENCE
Dec 7, 2014 first seen
Jan 20, 2015 last seen

The treat was first detected in your network on Dec 7, 2014 and last observed on Jan 20, 2015. You currently have 5 active users out of 15 total. The threat was also detected in 50+ other companies affecting 100+ other users.

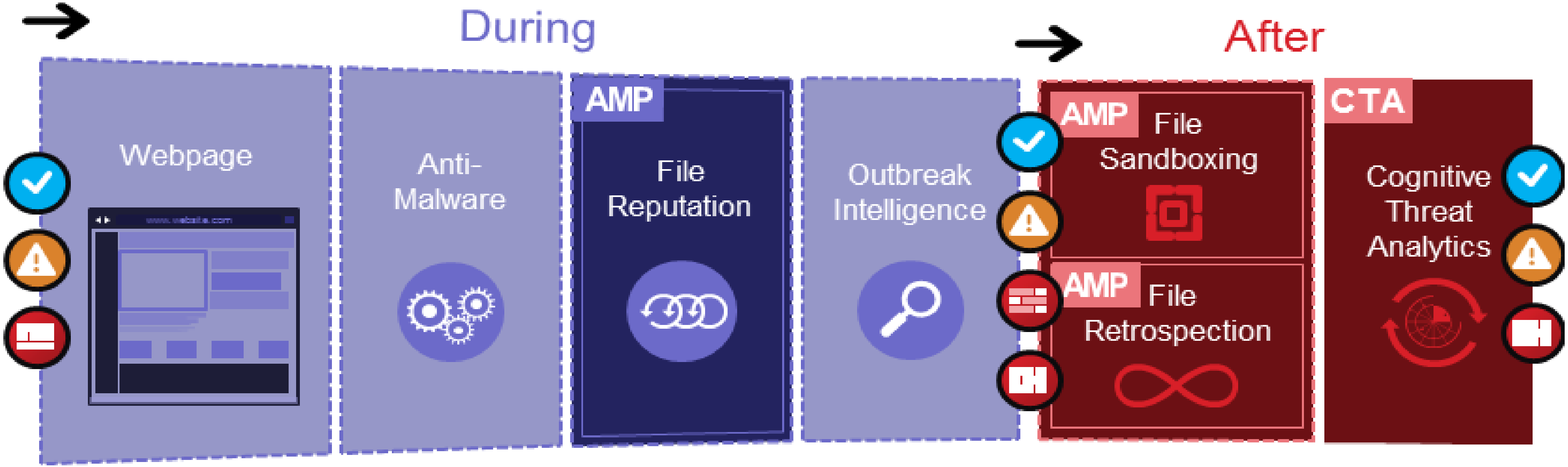
Adware, click-fraud, malvertising-related botnet. The main distribution channel for this threat is fraudulent software such as anti-virus, browser plugins, and software updates. The infection typically appears as a browser plugin that hijacks your web browser. It may then establish a command-and-control channel, track user activity, have rootkit capability, and perform click-fraud through the automatic loading and clicking of unsolicited advertisements. The attacker may obtain information about the infected device and attempt to further exploit the device with additional threats. To remove this threat, it is not sufficient to block the target domains because they change frequently. You must remove the fraudulent software or reimage the infected device.

CTA Case Study 2 - Malvertising Botnet



CTA Demo

CWS Premium Summary



AMP improves CWS resistance to direct attacks from the web
CTA detects malicious activities in the after phase, including infections by mail, USB stick, IM, unique threats

Summary

Fitting Your Business Needs:

- Global Infrastructure
- Flexible Deployment in Your Network
- Security Without Compromise
- Demos

- Robust, scalable, resilient ✓
- Visibility into Global trends
- On the backbone of the Internet
- Granular policies and reports

- Simple deployment ✓
- Multiple options, roaming users
- Leverage of existing infrastructure
- Fewer parts, one vendor

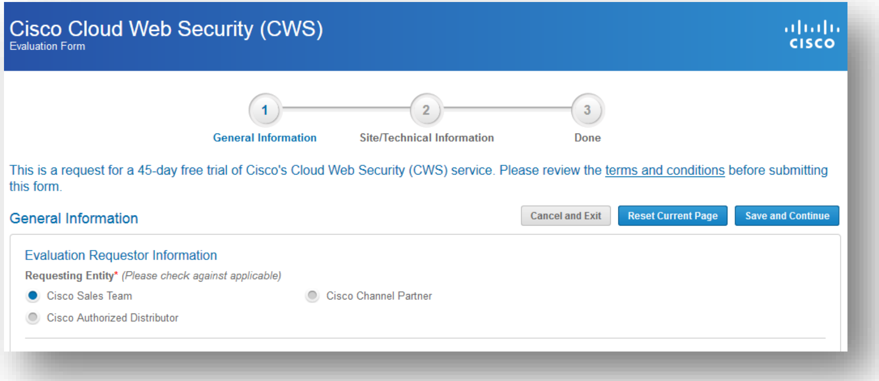
- Multiple layers of protection ✓
- Effective Zero-hour detection
- Covered by Cisco's Talos
- Complete Attack Continuum

✓

- Try for yourself…

Try it for Yourself…

- Free evaluations available
  - 45 days
  - Up to 250 users
- Advanced features can be included in evaluations
  - Log Extraction
  - AMP



Cisco Cloud Web Security (CWS)

Evaluation Form

This is a request for a 45-day free trial of Cisco's Cloud Web Security (CWS) service. Please review the terms and conditions before submitting this form.

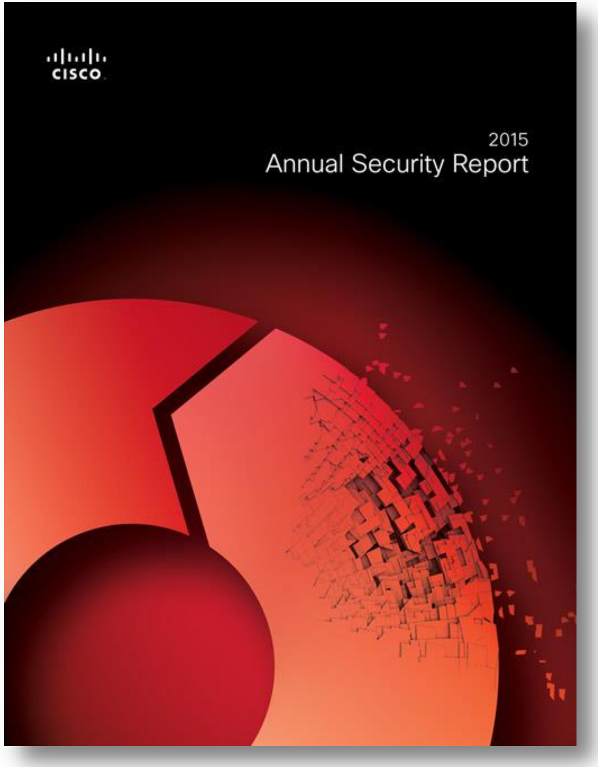
General Information

Evaluation Requestor Information

Requesting Entity* *(Please check against applicable)*

● Cisco Sales Team ○ Cisco Channel Partner

○ Cisco Authorized Distributor



2015
Annual Security Report

Cisco 2015 Annual Security Report

Now available:

cisco.com/go/asr2015

Final Thought…

Web filtering, reputation, application control

AV and heuristic scanning engines

File reputation, sandboxing, points in time

Behavioural analysis and retrospective events

No vendor can prevent 100% of targeted and sophisticated attacks, but CWS brings you as close as you'll get, AND continues to work for you over time

Try an easy 45 day free evaluation

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Liv
2015 T-Shirt!

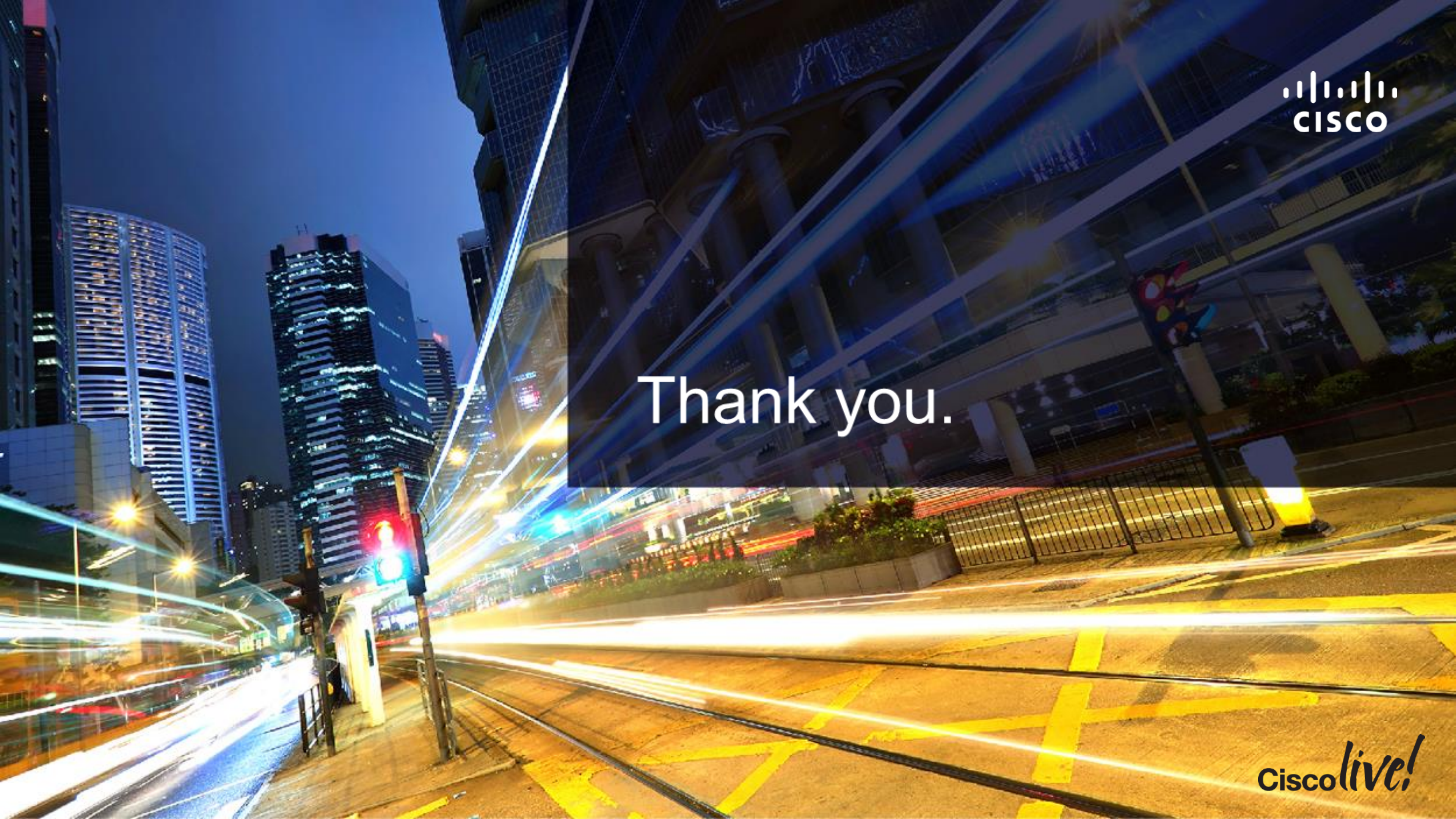
Complete your Overall Event Survey and 5 Session Evaluation

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site http://showcase.genie connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughou the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com

Cisco live!



Thank you.

CISCO