Email and Web Security are more important than ever

Story Tweedie-Yates

Head of Security Product Marketing, EMEAR

March 2017

Which tree is alive?

Agenda

Web and email in the portfolio context

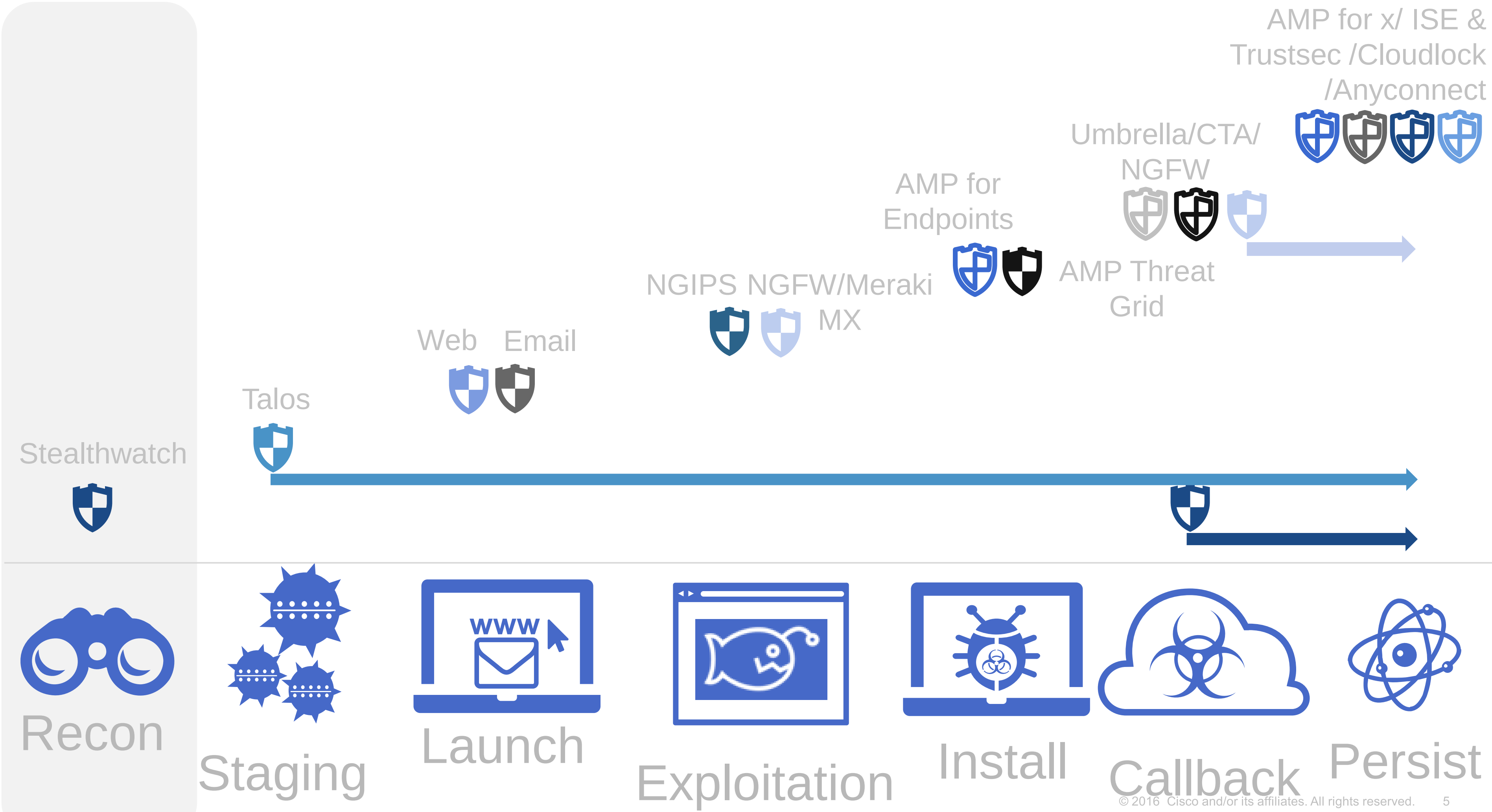
Top two attack vectors

How it works

What’s new

Future vision

Web and email in the portfolio context



Stealthwatch

Talos

Web

Email

NGIPS NGFW/Meraki MX

AMP for Endpoints

AMP Threat Grid

Umbrella/CTA/ NGFW

AMP for x/ ISE & Trustsec /Cloudlock /Anyconnect

Recon

Staging

Launch

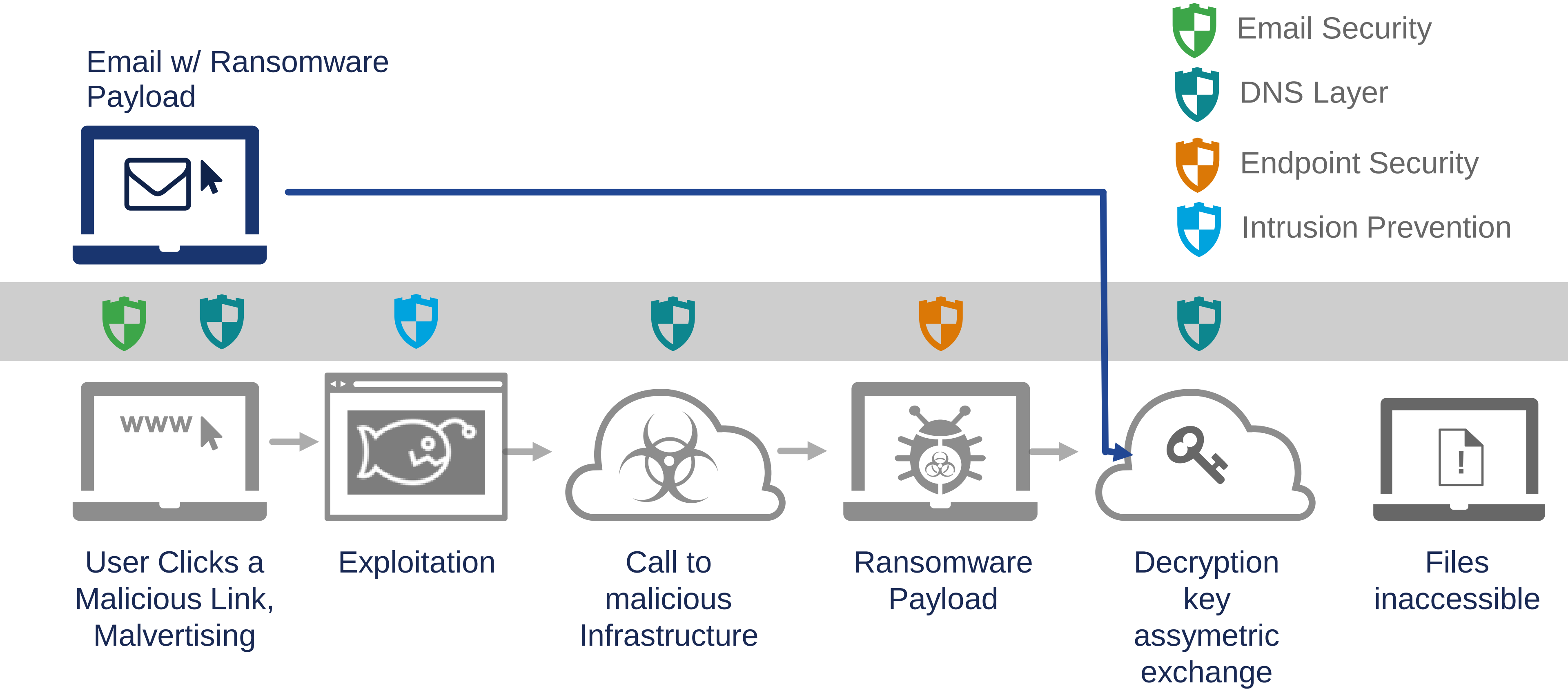
Exploitation

Install

Callback

Persist

Ransomware kill chain and a multi-layer defense



Email Security

DNS Layer

Endpoint Security

Intrusion Prevention

Email w/ Ransomware Payload

User Clicks a Malicious Link, Malvertising

Exploitation

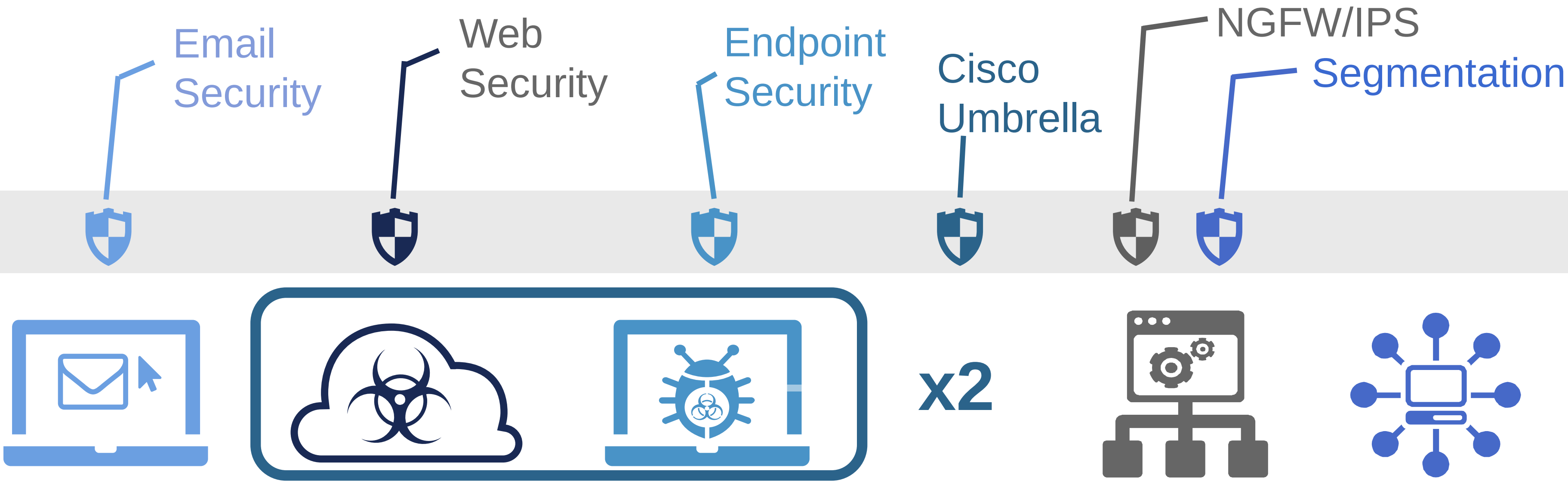
Call to malicious Infrastructure

Ransomware Payload

Decryption key assymetric exchange

Files inaccessible

Email and Web Security are also important for OT environments



Email Security

Web Security

Endpoint Security

Cisco Umbrella

NGFW/IPS

Segmentation

Email w/ weaponized MS Office attachments

C&C through Explorer

Black Energy 3 installed

x2

C&C and plug-in installation

Remote connections using stolen credentials

Attack

Top two attack vectors

Adware and Malvertising Shift Into High Gear

Malvertising

Using brokers (gates) to increase speed and agility

Switching quickly between servers without changing redirection

ShadowGate: a cost-effective campaign

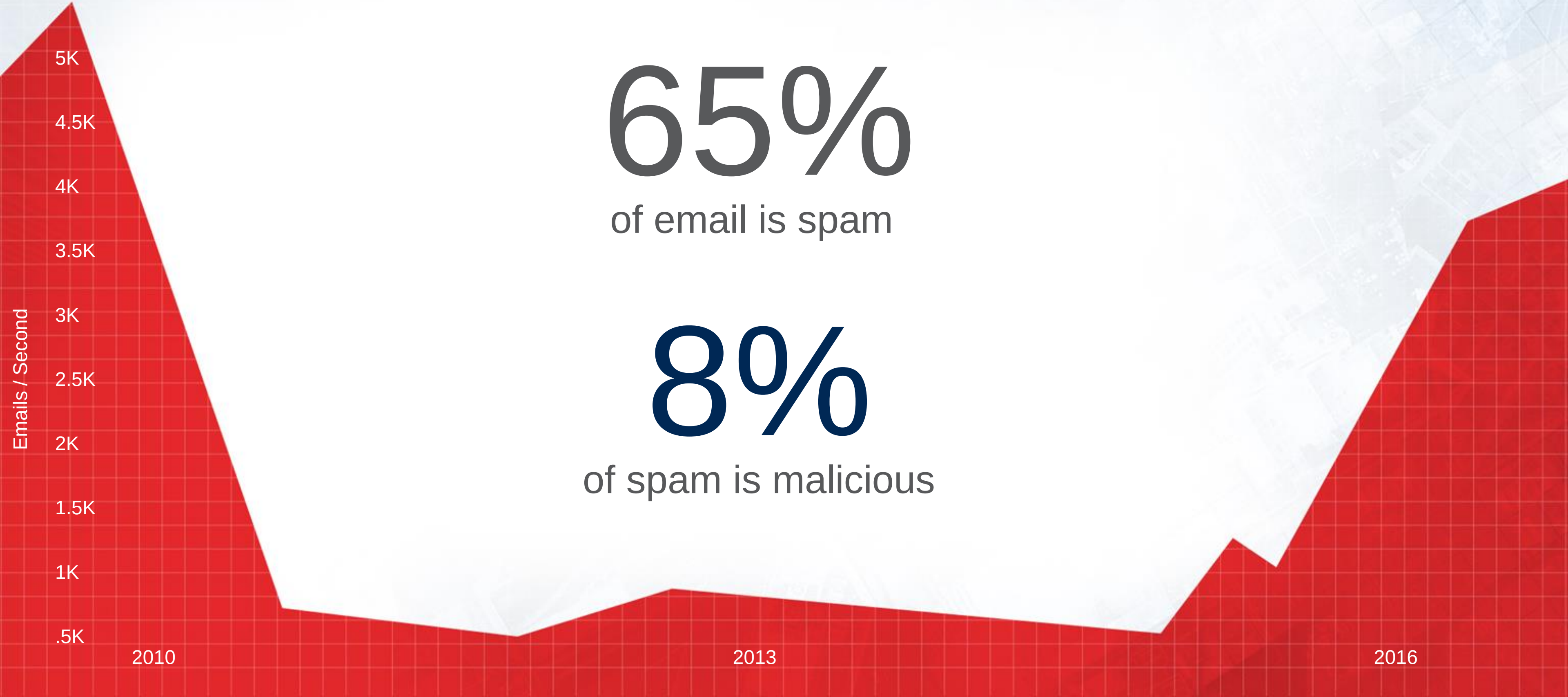
Adware

75%

of organizations investigated had adware infections

Spam Comes Roaring Back

Email is Back in Vogue



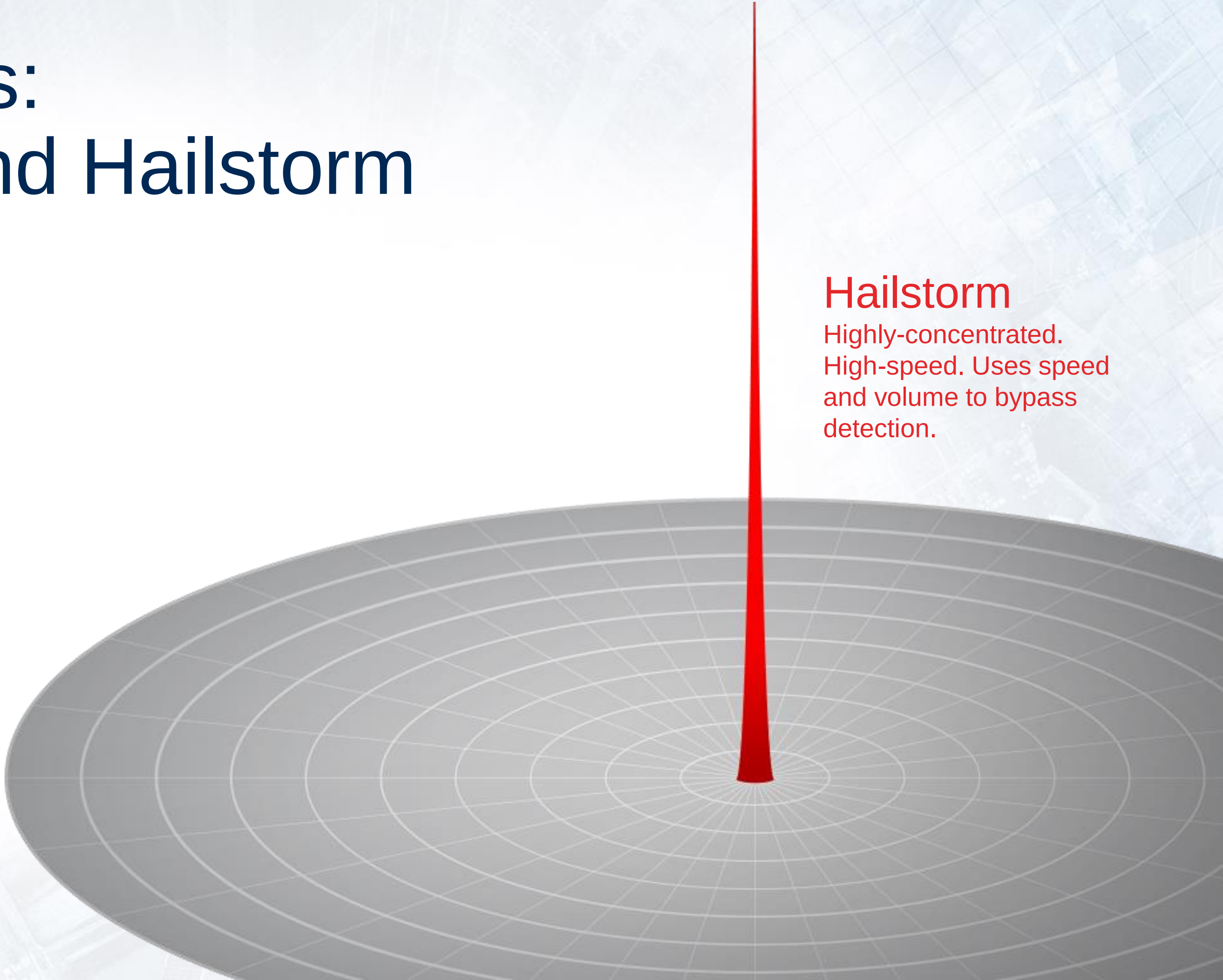
65%

of email is spam

8%

of spam is malicious

Spam Attacks: Snowshoe and Hailstorm



Hailstorm

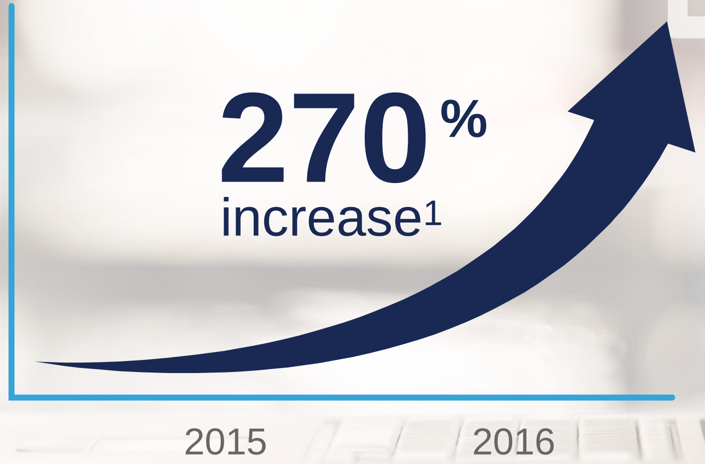
Highly-concentrated. High-speed. Uses speed and volume to bypass detection.

Snowshoe

Uses various IP address. Hides from detection with low volume.

Spoofing rates are on the rise

- Phishing
- **Spoofing**
- Ransomware



270% increase[1]

$2.3B

In losses from spoofing 2013 - 2015[1]

[1]FBI Warns of Dramatic Increase in Business email scams, 2016

Forged addresses fool recipients

Threat actors extensively research targets

Money and sensitive information are targeted

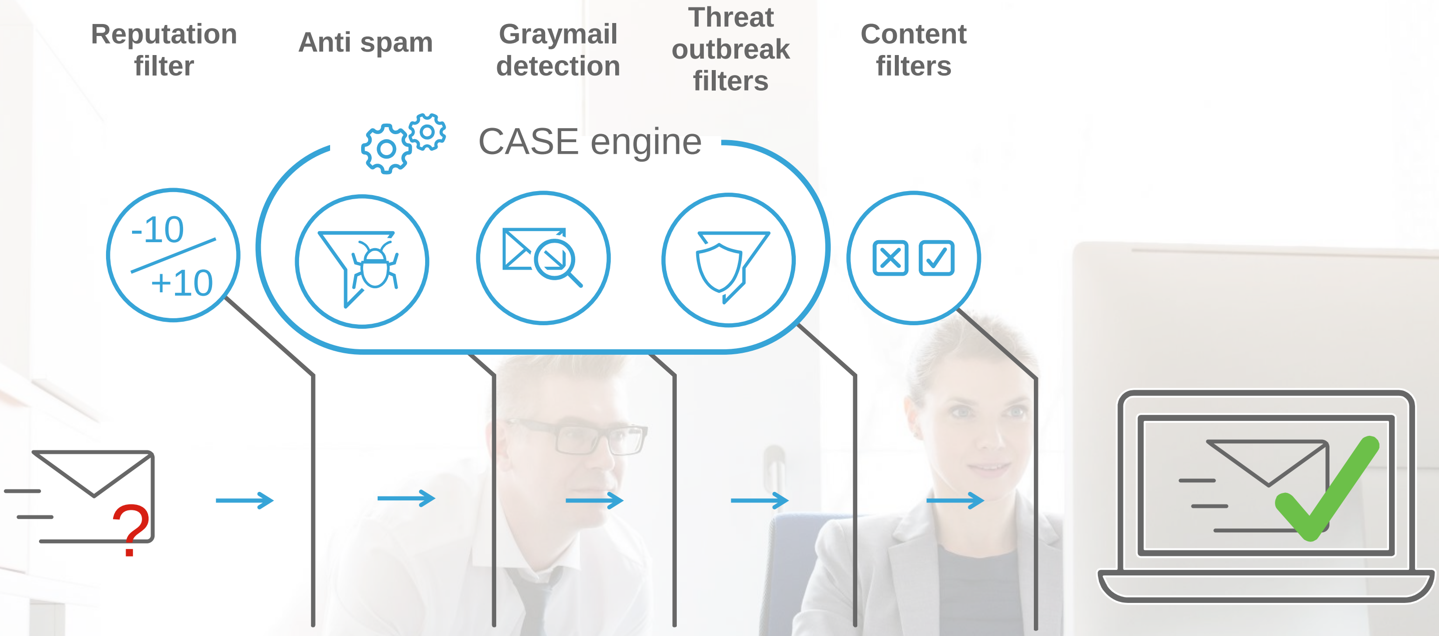
How it works

Detect threats embedded in email content

Optimize detection with machine and human intelligence

Stop more than 99% of Spam

Keep good emails flowing with a < 1 in 1M false-positive rate

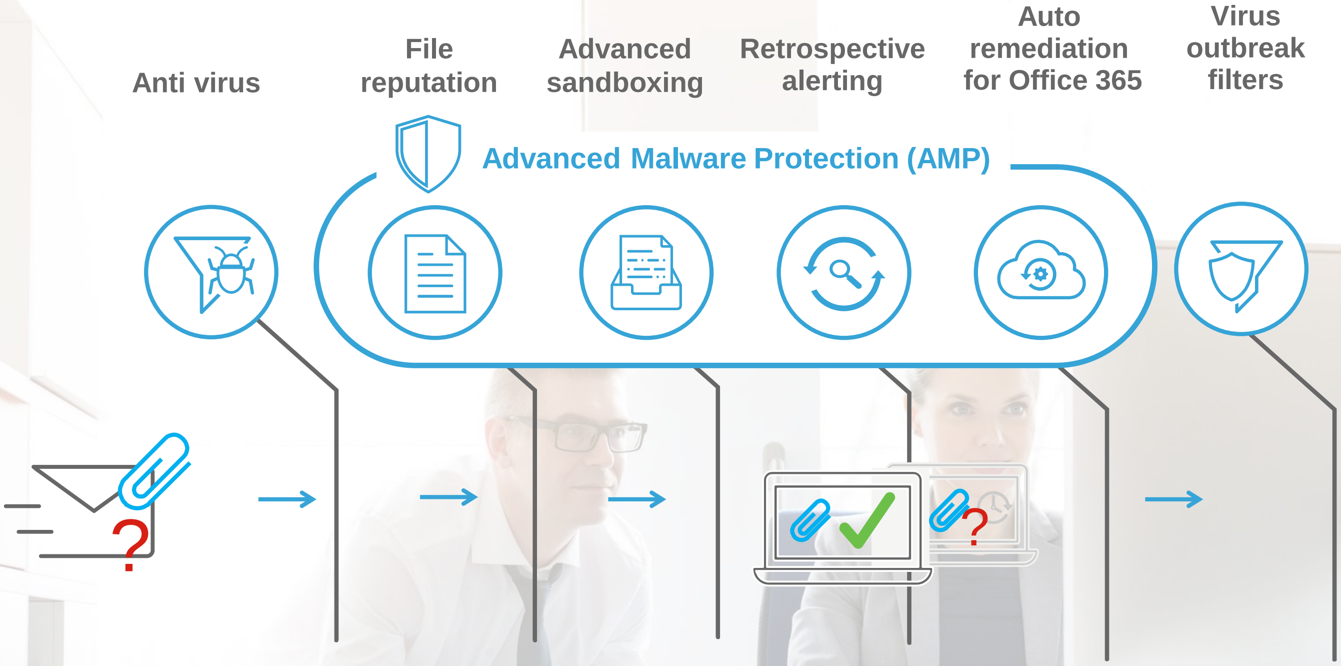


Guard against malicious attachments

Track email behavior with over 560 indicators

Quickly neutralize threats with Zero Hour Malware Protection

Continuously track files with retrospective security



Anti virus

File reputation

Advanced sandboxing

Retrospective alerting

Auto remediation for Office 365

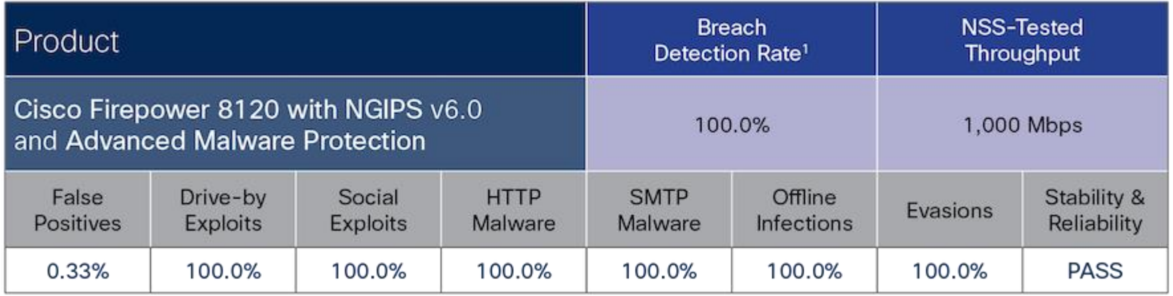
Virus outbreak filters

Advanced Malware Protection (AMP)

A Leader in Security Effectiveness

Only Cisco with its architectural approach to security can provide an integrated solution that can see a threat once and block it everywhere.

Figure 1. NSS Breach Detection Test Results for Cisco



Product				Breach Detection Rate[1]		NSS-Tested Throughput	
Cisco Firepower 8120 with NGIPS v6.0 and Advanced Malware Protection				100.0%		1,000 Mbps	
False Positives	Drive-by Exploits	Social Exploits	HTTP Malware	SMTP Malware	Offline Infections	Evasions	Stability & Reliability
0.33%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	PASS

- **A leader for 3rd year in a row in BDS test – detecting 100% of malware, exploits & evasions.**
- **Faster time to detection than any other vendor**
- Cisco delivers breach detection across **more platforms and attack vectors** than any other solution - blocking more threats, faster**.**

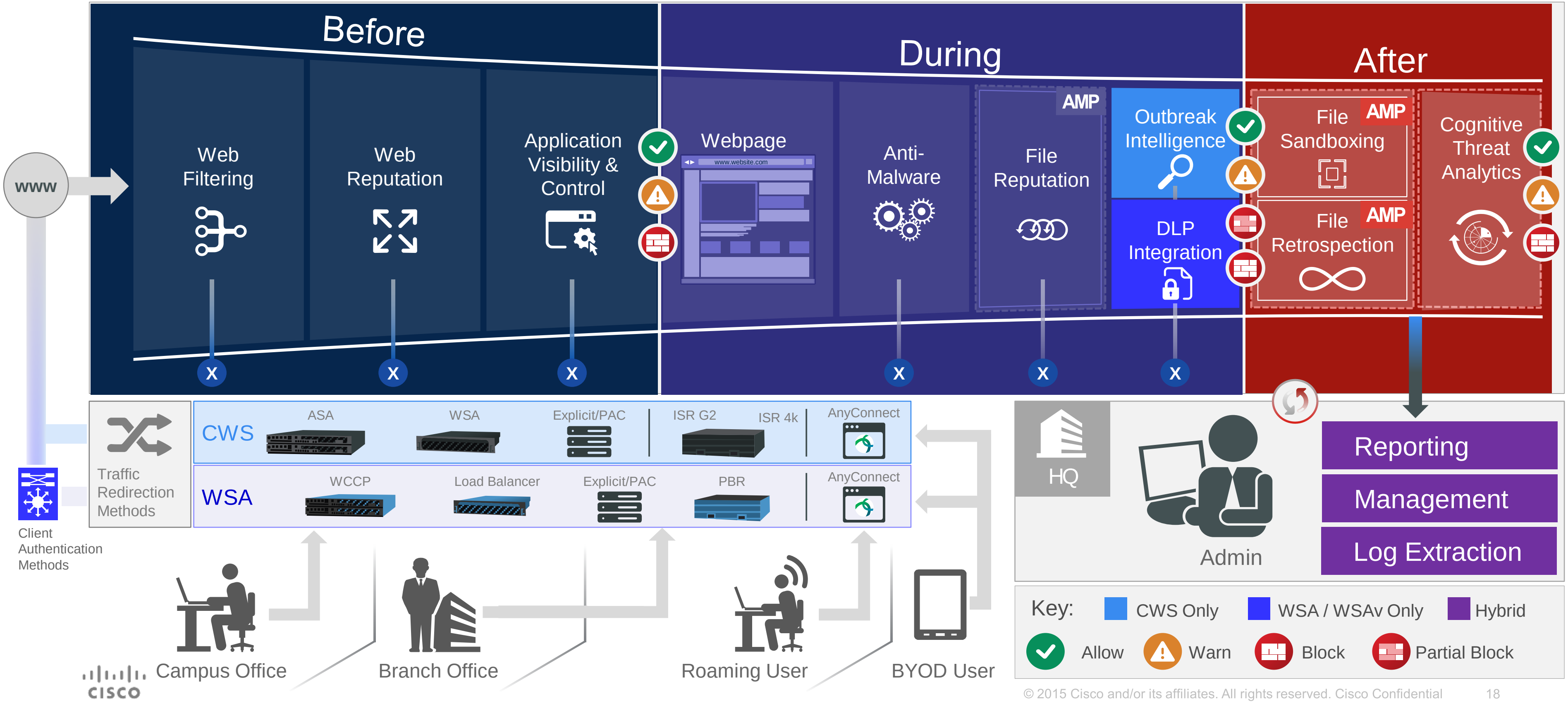
Talos

WSA

WSAv

Cisco Web Security

CWS



Before

Web Filtering

Web Reputation

Application Visibility & Control

During

Webpage

Anti-Malware

AMP

File Reputation

Outbreak Intelligence

DLP Integration

After

AMP

File Sandboxing

AMP

File Retrospection

Cognitive Threat Analytics

Traffic Redirection Methods

Client Authentication Methods

CWS	ASA	WSA	Explicit/PAC	ISR G2	ISR 4k	AnyConnect
WSA	WCCP	Load Balancer	Explicit/PAC	PBR		AnyConnect

Campus Office

Branch Office

Roaming User

BYOD User

HQ

Admin

Reporting

Management

Log Extraction

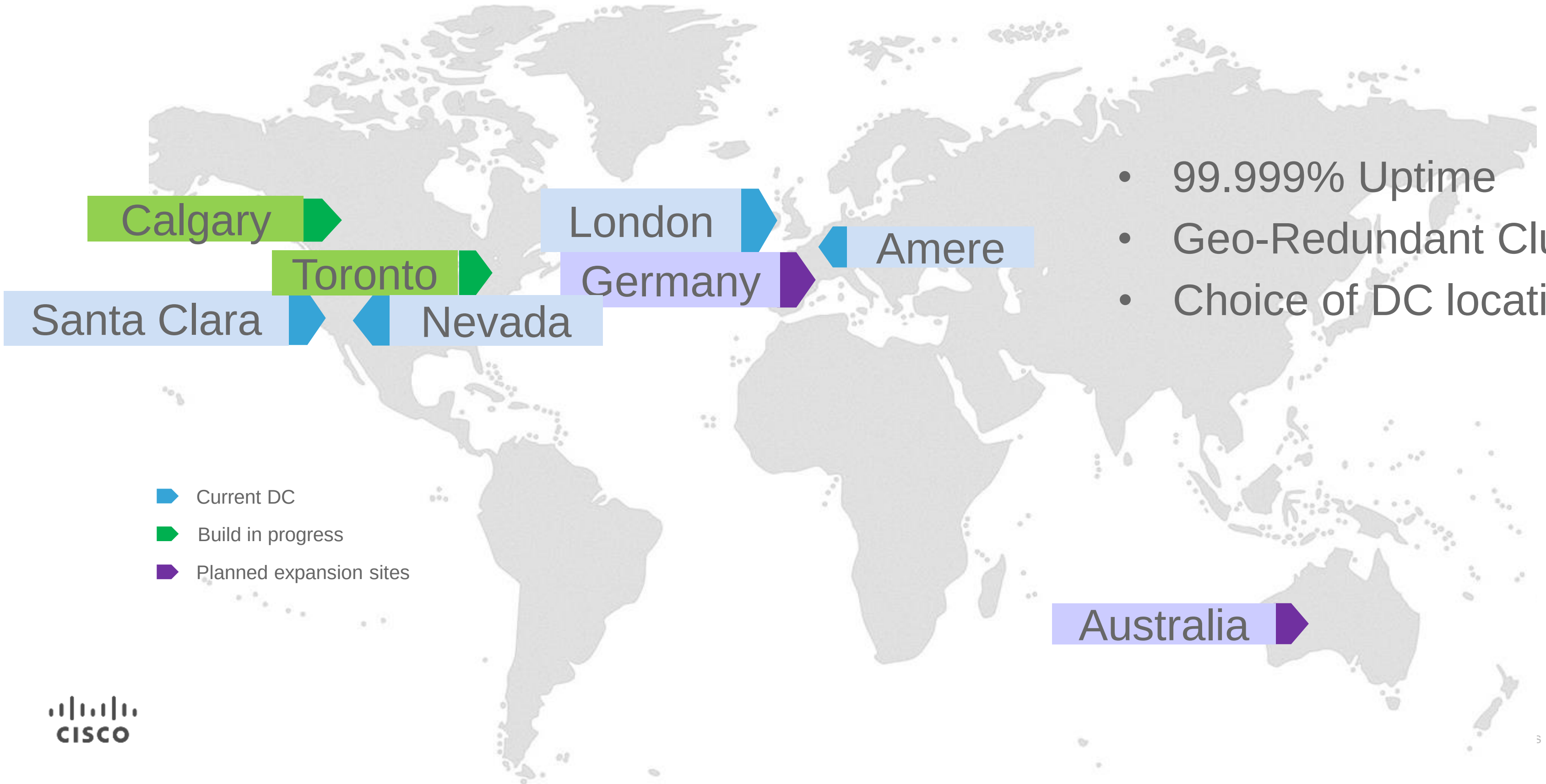
Key: 🟦 CWS Only 🟦 WSA / WSAv Only 🟪 Hybrid

✓ Allow ⚠ Warn 🟥 Block 🟥 Partial Block

What’s new

Cloud Email Security

New Data Centers



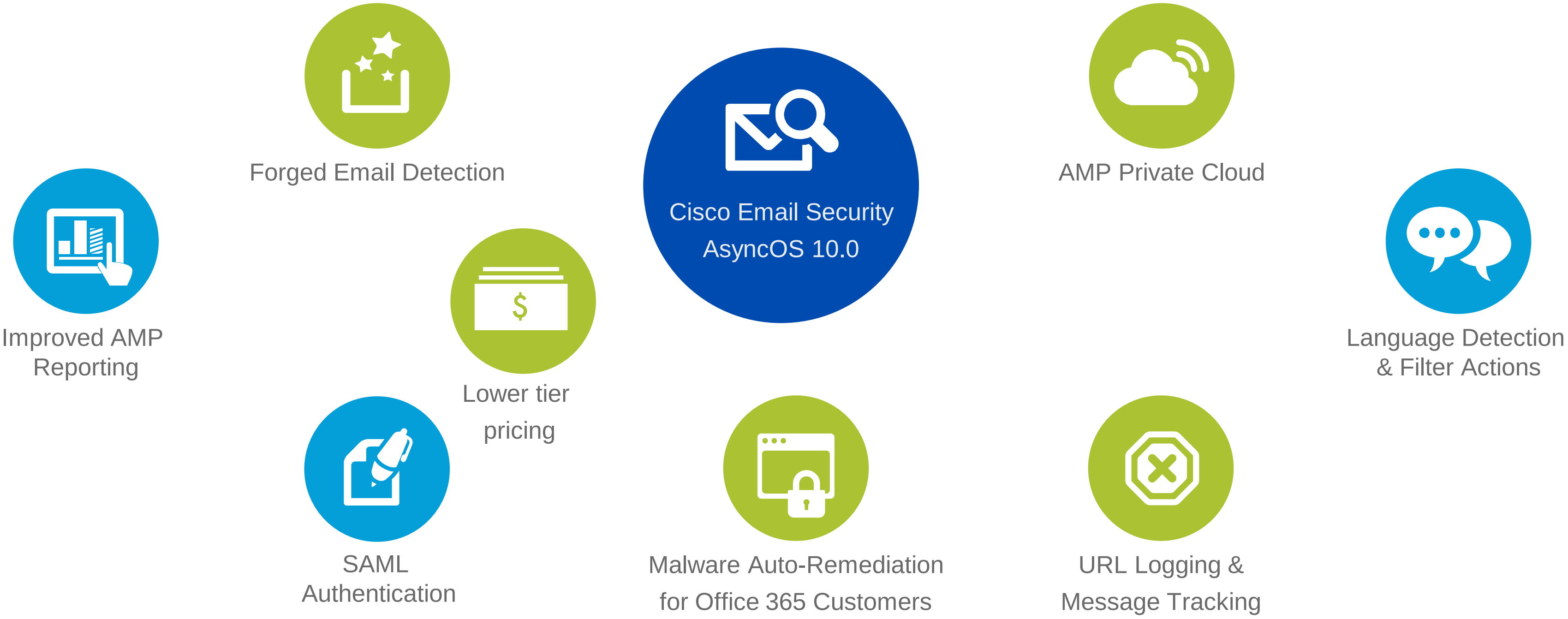
- 99.999% Uptime
- Geo-Redundant Clusters
- Choice of DC location

🟦 Current DC

🟩 Build in progress

🟪 Planned expansion sites

ESA - AsyncOS 10.0



Cisco Email Security AsyncOS 10.0

Forged Email Detection

AMP Private Cloud

Improved AMP Reporting

Lower tier pricing

Language Detection & Filter Actions

SAML Authentication

Malware Auto-Remediation for Office 365 Customers

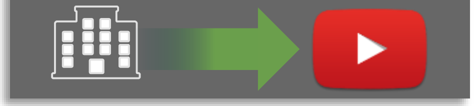
URL Logging & Message Tracking

Reduce exposure **Support growth** **Achieve agility**

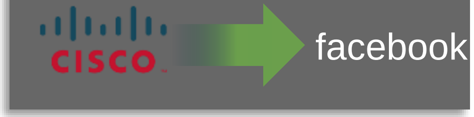
WSA - Async 10.0

- Easier management of exceptions
- On-premises options for privacy concerns
- Better user experience for https browsing

YouTube is blocked as a corporate policy but when browsed using corporate website is allowed.



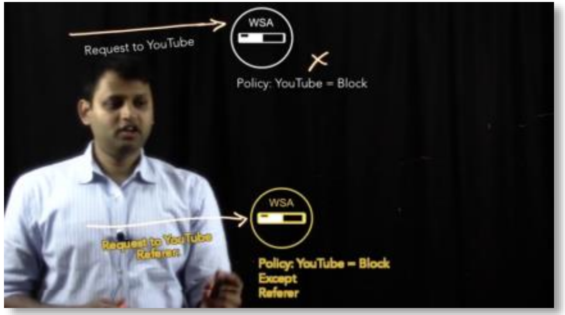
Facebook is blocked, but certain pages on facebook.com allowed when referred from Cisco.com



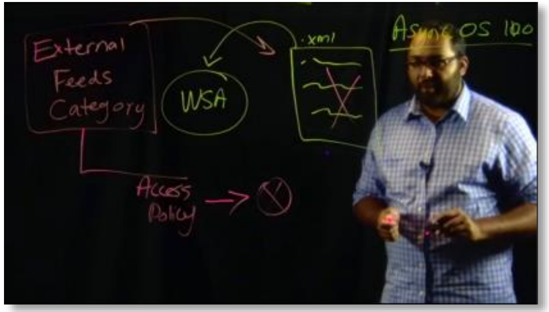
Security Chalk Talks

https://www.youtube.com/playlist?list=PLFT-9JpKjRTANXKBmLbQ611TPYLXbUL_0

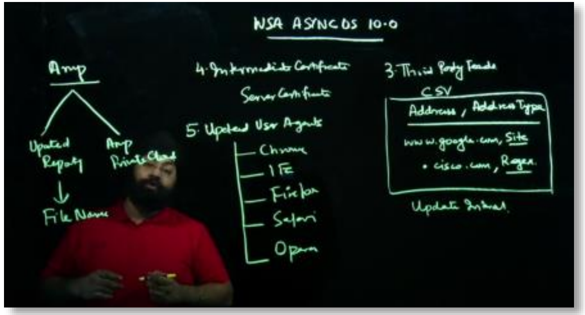
Referrer Header Bypass


Request to YouTube
WSA
Policy: YouTube = Block
Request to YouTube Referer
WSA
Policy: YouTube = Block Except Referer

External Feeds Category

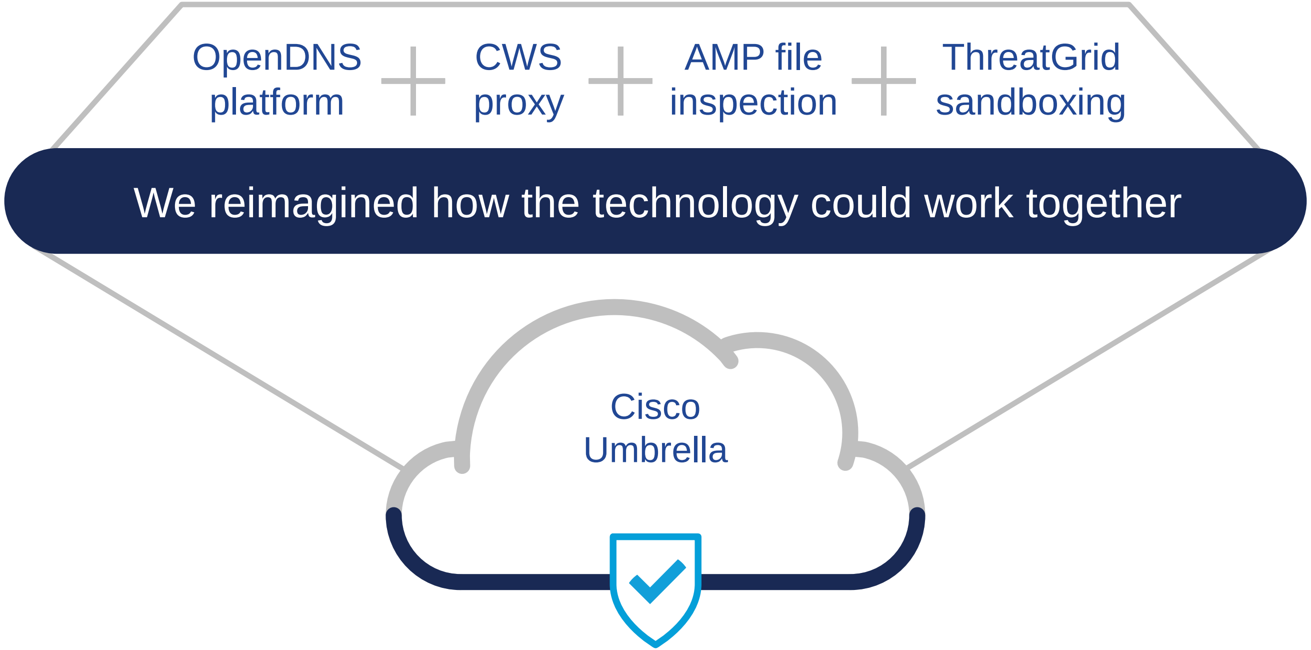


AsyncOS 10.0 Overview



Roadmap and vision

Cisco Umbrella: the making of Cisco’s Secure Internet Gateway

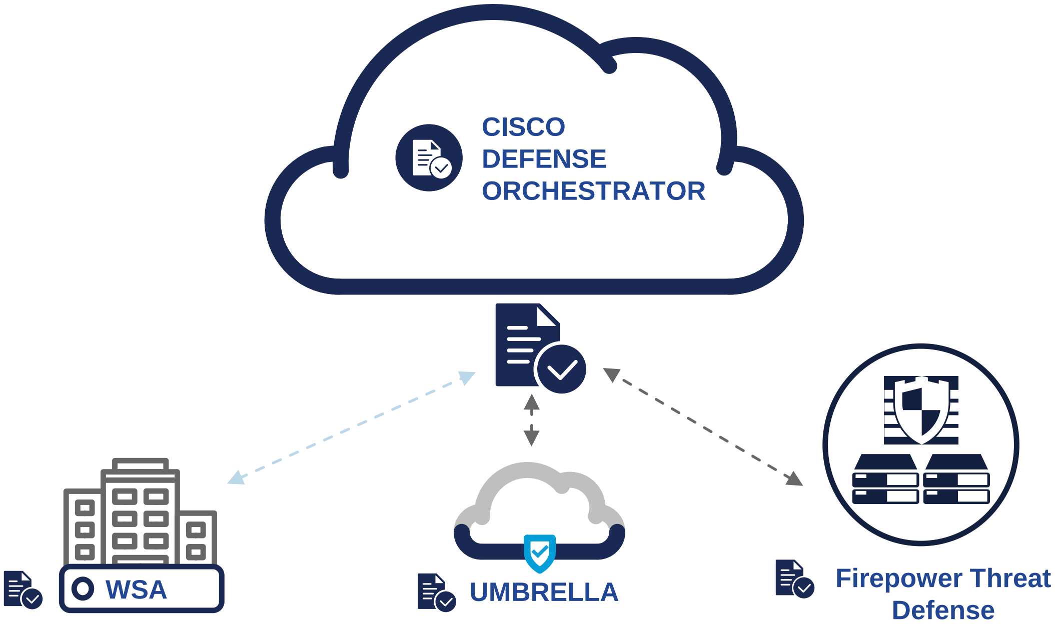


OpenDNS platform + CWS proxy + AMP file inspection + ThreatGrid sandboxing

We reimagined how the technology could work together

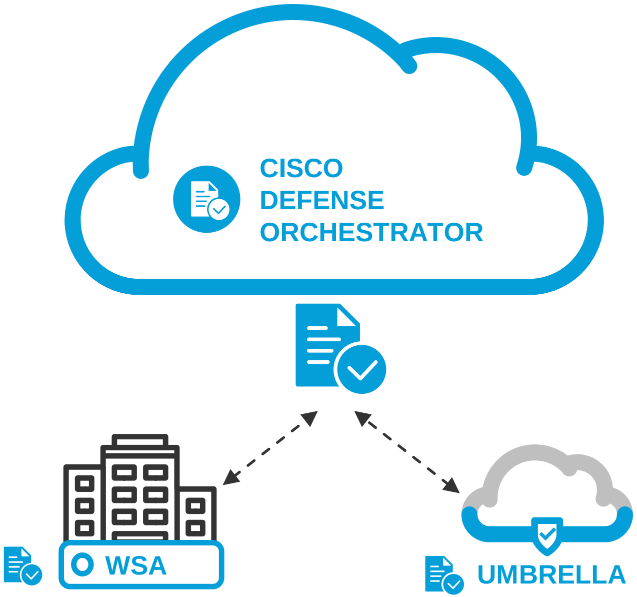
Cisco Umbrella

Cloud Defense Orchestrator – now available in Europe



How Umbrella fits with Cisco Web Security Appliance (WSA)

Flexibility to fit different use cases



Umbrella provides safe internet access anywhere users go, even off the VPN

WSA solves on-prem requirements for usage/bandwidth controls and compliance

Cisco Defense Orchestrator (CDO) for ongoing policy management

- Single place to add domains/URLs to block across cloud (Umbrella) and on-prem (WSA, NGFW)

What kind of a boat would you need?

Country of records: most active volcano, largest waterfall, cleanest capital, longest life expectancy, first female president, northern most botanical garden and golf course

Iceland plants most trees per head

Country with youngest land-mass

English word ‘geyser’ comes from Great Geysir in Haukadalur