How to build a multi-layer Security Architecture to detect and remediate threats in real time

Nikos Mourtzinos, CCIE #9763
Cisco Cyber Security Sales Specialist
March 2018

Agenda

Cisco Strategy
Umbrella
AMP for Endpoints
Multi-layer Security Architecture

Cisco Integrated Security Architecture

Vision	???			
Strategy	Hardware	Software		
Execution				
Metrics				

Cisco Integrated Security Architecture

Vision	???			
Strategy	Hardware	Software		
Execution	Threat Prevention			
Metrics				

Cisco Integrated Security Architecture

Vision	???			
Strategy	Hardware	Software		
Execution	Threat Prevention			
Metrics	Perimeter	Endpoint		

Cisco Integrated Security Architecture

Vision	???			
Strategy	Hardware	Software		
Execution	Threat Prevention	Detection		
Metrics	Perimeter	Endpoint		

Cisco Integrated Security Architecture

Vision	???			
Strategy	Hardware	Software		
Execution	Threat Prevention	Detection		
Metrics	Perimeter	Endpoint	Internal Network	Cloud

Cisco Integrated Security Architecture

Vision	Security Everywhere			
Strategy	Hardware	Software	Xware	
Execution	Threat Prevention	Detection	Containment	Response
Metrics	Perimeter	Endpoint	Internal Network	Cloud

Most Security Vendors – Legacy Architecture

Vision	???			
Strategy	Hardware	Software	Xware	
Execution	Threat Prevention	Detection	Containment	Response
Metrics	Perimeter	Endpoint	Internal Network	Cloud

All Cyber Security Startups

Vision				
Strategy	Hardware	Software	Xware	
Execution	Threat Prevention	Detection	Containment	Response
Metrics	Perimeter	Endpoint	Internal Network	Cloud

Cisco Integrated Security Architecture

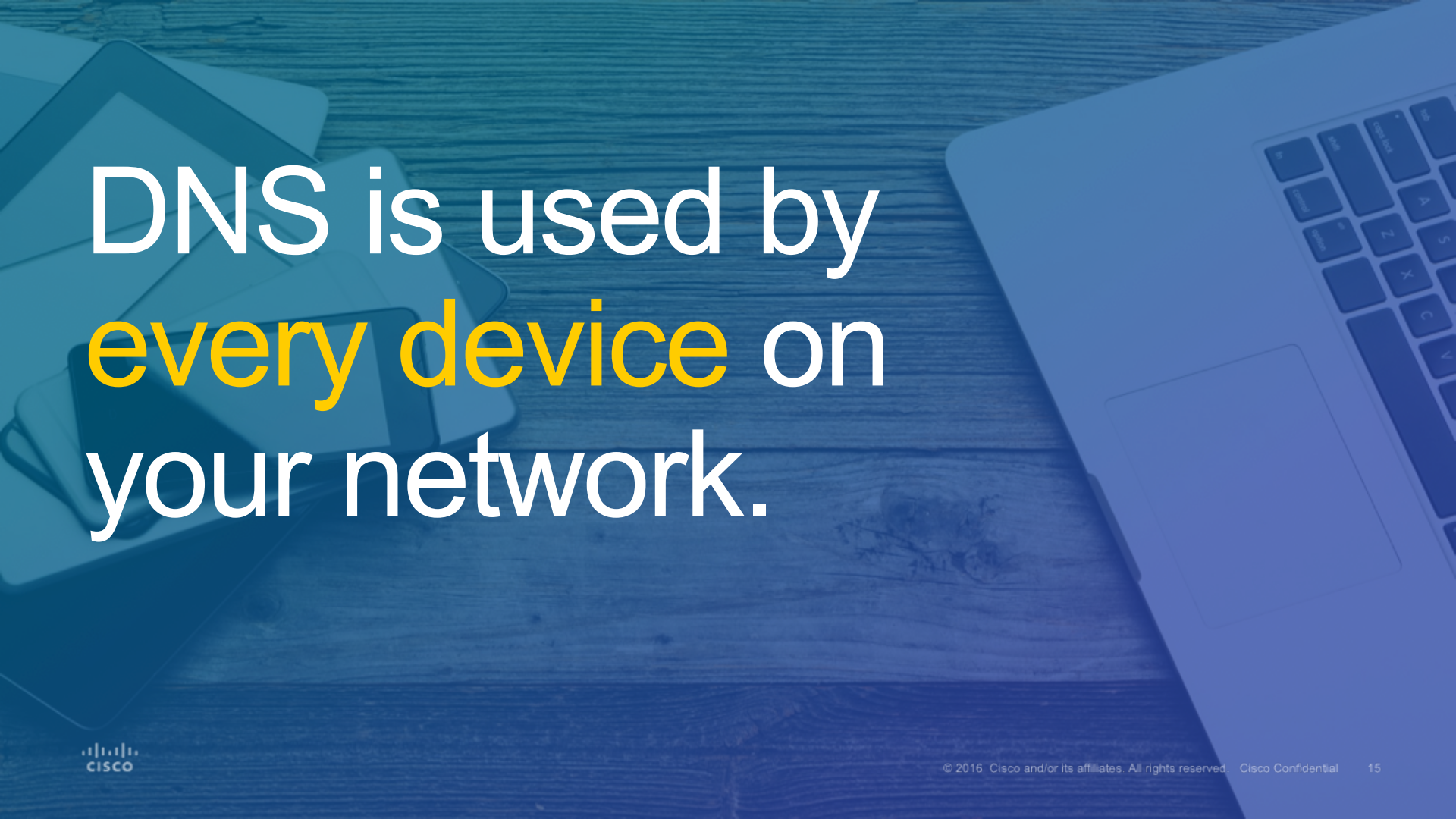
Vision	Security Everywhere			
Strategy	Hardware	Software	Xware	
Execution	Threat Prevention	Detection	Containment	Response
Metrics	Perimeter	Endpoint	Internal Network	Cloud

Cisco Umbrella

Vision	Cisco Umbrella			
Strategy	Hardware	Software	Xware	
Execution	Threat Prevention	Detection	Containment	Response
Metrics	Perimeter	Endpoint	Internal Network	Cloud

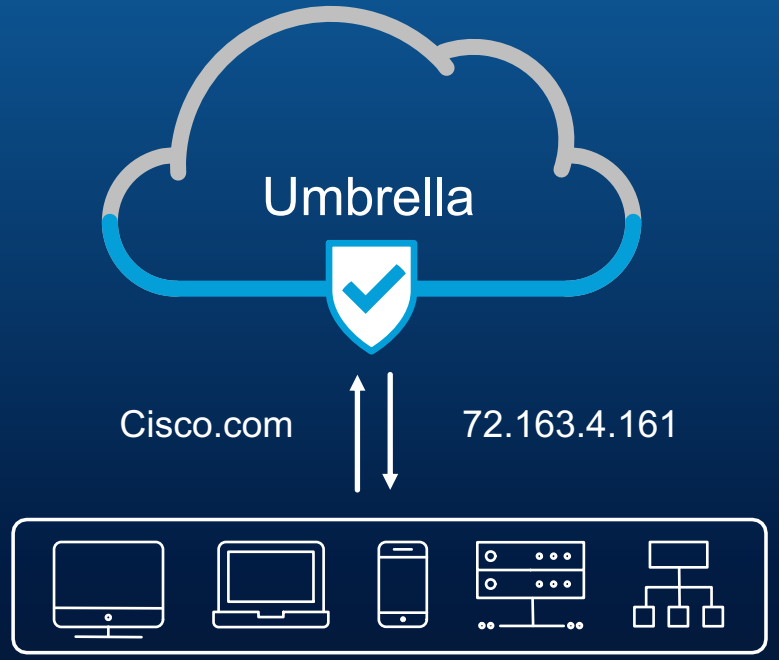
Cisco AMP for Endpoints

Vision	Cisco AMP for Endpoints			
Strategy	Hardware	Software	Xware	
Execution	Threat Prevention	Detection	Containment	Response
Metrics	Perimeter	Endpoint	Internal Network	Cloud



It all starts with DNS

- DNS = Domain Name System
- First step in connecting to the internet
- Precedes file execution and IP connection
- Used by all devices
- Port agnostic



Umbrella (OpenDNS)

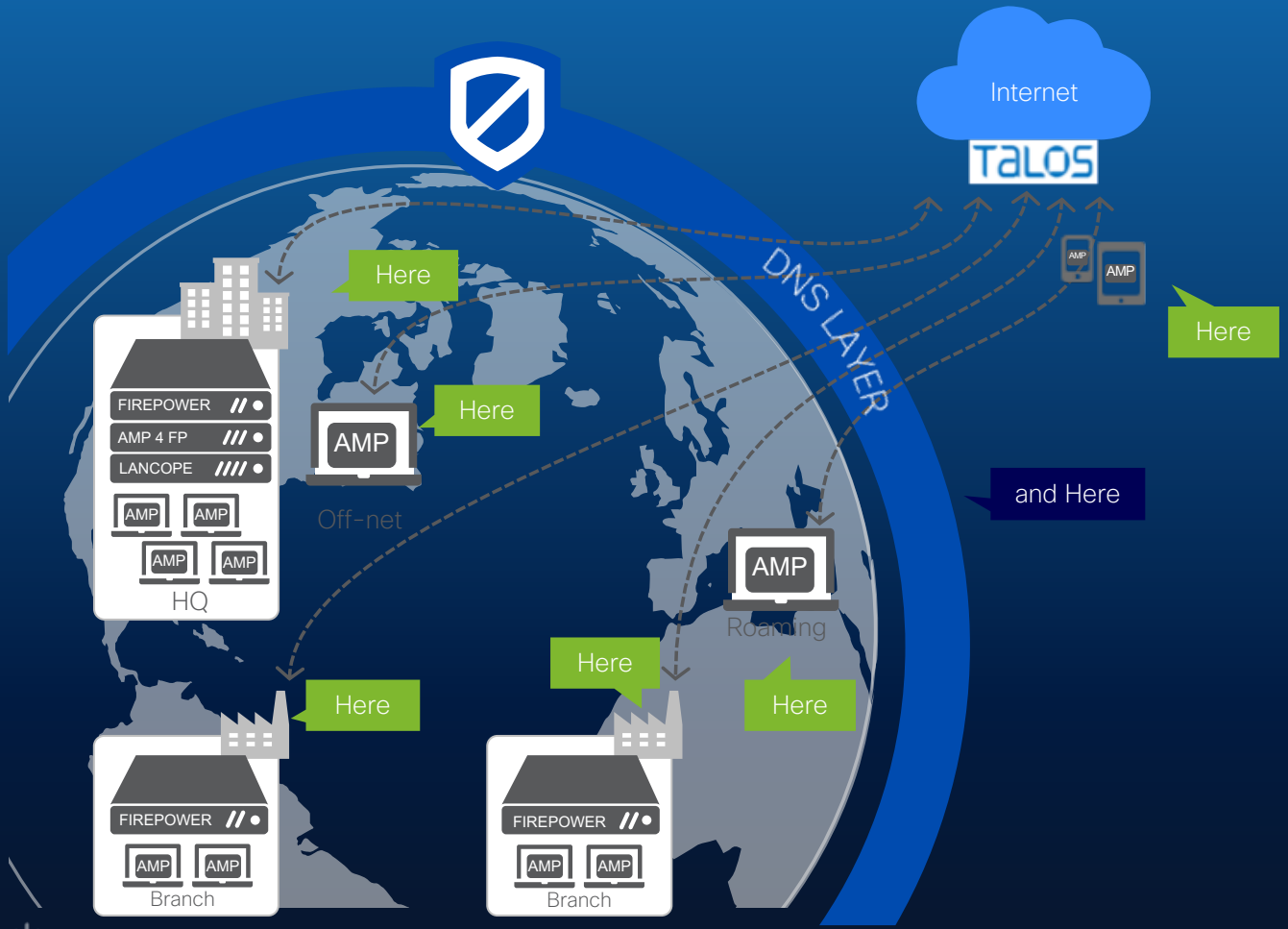
The fastest and easiest way to block threats

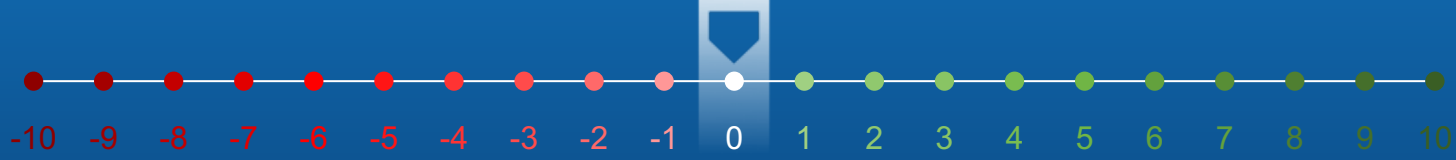
Key points

Visibility and protection everywhere

Deployment in minutes

Integrations to amplify existing investments





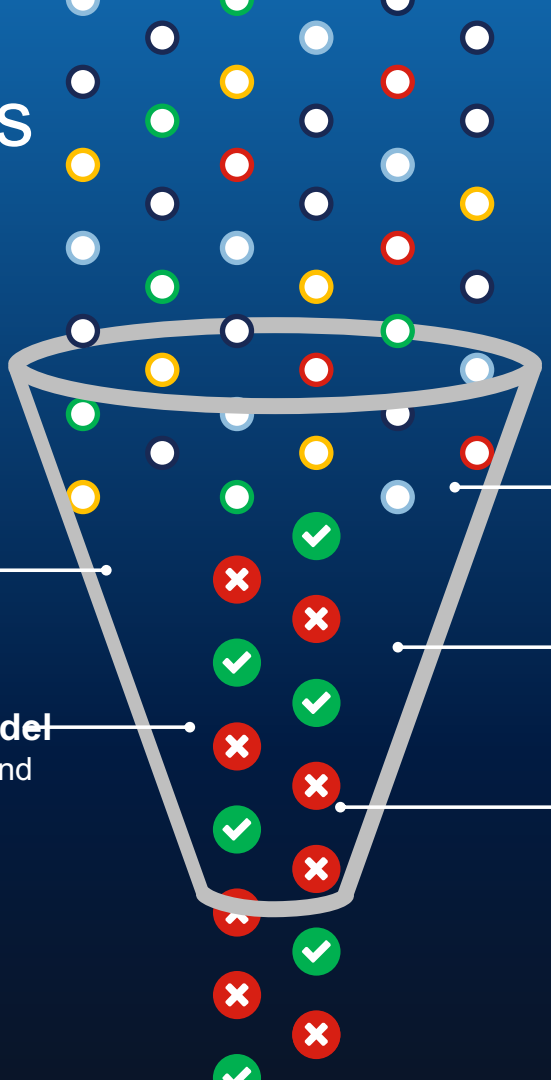
17.0.2.12

Kiev

HTTPS

Web server
< 1 Month

Statistical Models



2M+ live events per second

11B+ historical events

Co-occurrence model
Identifies other domains looked up in rapid succession of a given domain

Natural language processing model
Detect domain names that spoof terms and brands

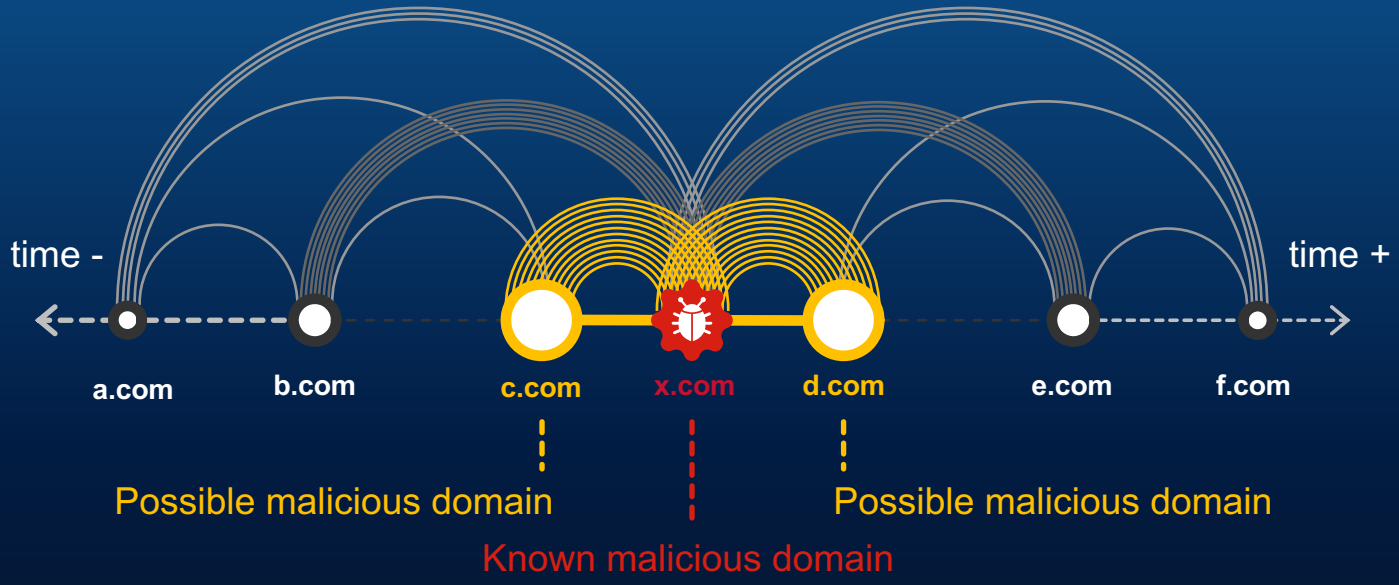
Spike rank model
Detect domains with sudden spikes in traffic

Predictive IP space monitoring
Analyzes how servers are hosted to detect future malicious domains

Dozens more models

Co-occurrence model

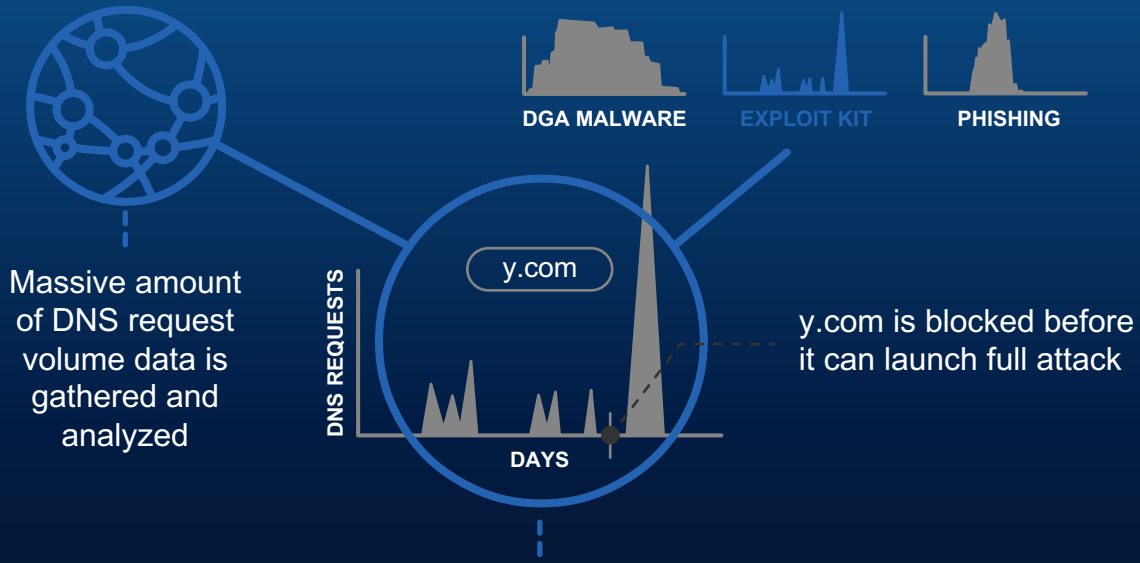
Domains guilty by inference



Co-occurrence of domains means that a statistically significant number of identities have requested both domains consecutively in a short timeframe

Spike rank model

Patterns of guilt



Cisco Umbrella

The fastest and easiest way to block threats

100% uptime

Resolves 80B+ DNS requests daily with no added latency

7M+ unique malicious destinations blocked across 25 data centers

Prevents malware, phishing, C2 callbacks over any port

Identify cloud & IoT usage risks

URL filtering

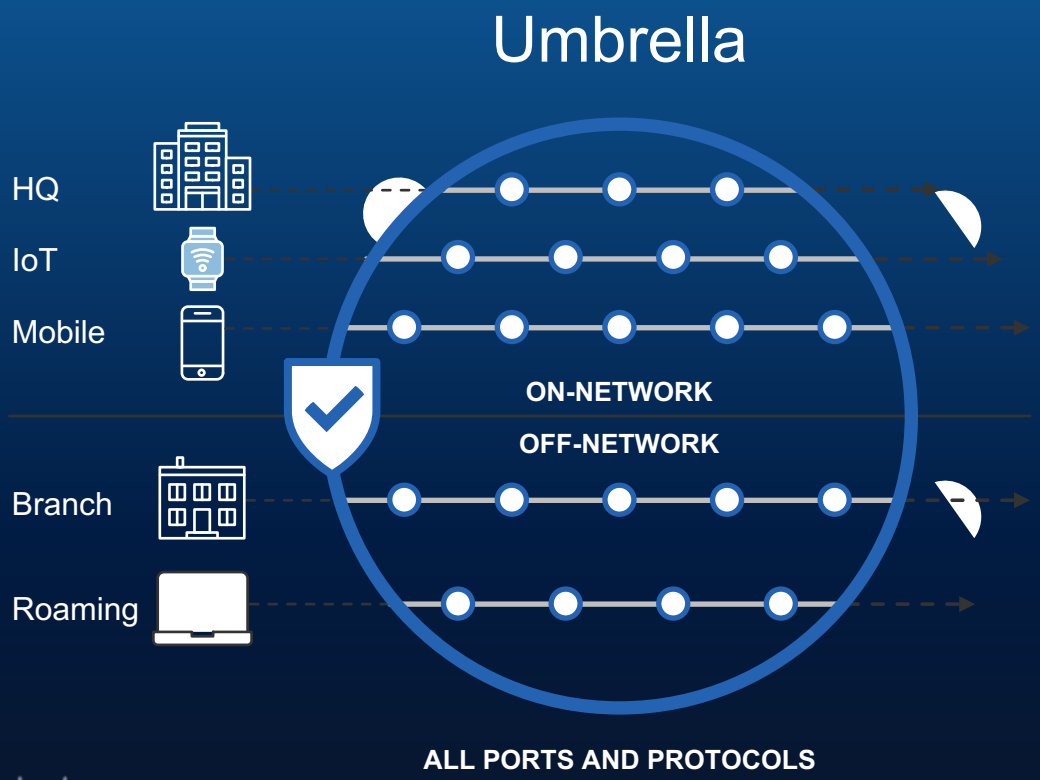
Proxy risky domains / SSL Decryption for file inspection using AV and AMP

Enforcement per internal IP and AD user/group

API

Investigate – Threat intelligence on all domains, IPs, File Hashes

Visibility and protection for all activity, anywhere



All office locations

Any device on your network

Roaming laptops

Every port and protocol

Most Innovative Security Product Of 2017

Security Innovators

Security - Cloud

Winner:

Cisco Umbrella

Cisco Umbrella is a cloud-delivered security platform that serves as the first line of defense to protect employees both on and off the corporate network. The Secure Internet Gateway provides customers with safe access to the internet anywhere that users go, even when they're not on the virtual private network. Cisco Umbrella halts current and emerging threats over all ports and protocols, while blocking access to malicious domains, URLs, IP addresses and files before a connection is established or a file downloaded. Ultimately, Cisco Umbrella protects enterprises as mobility increases and as cloud services are adopted.

Trusted by enterprises worldwide

Fortune 500 companies in retail, healthcare, energy, and entertainment

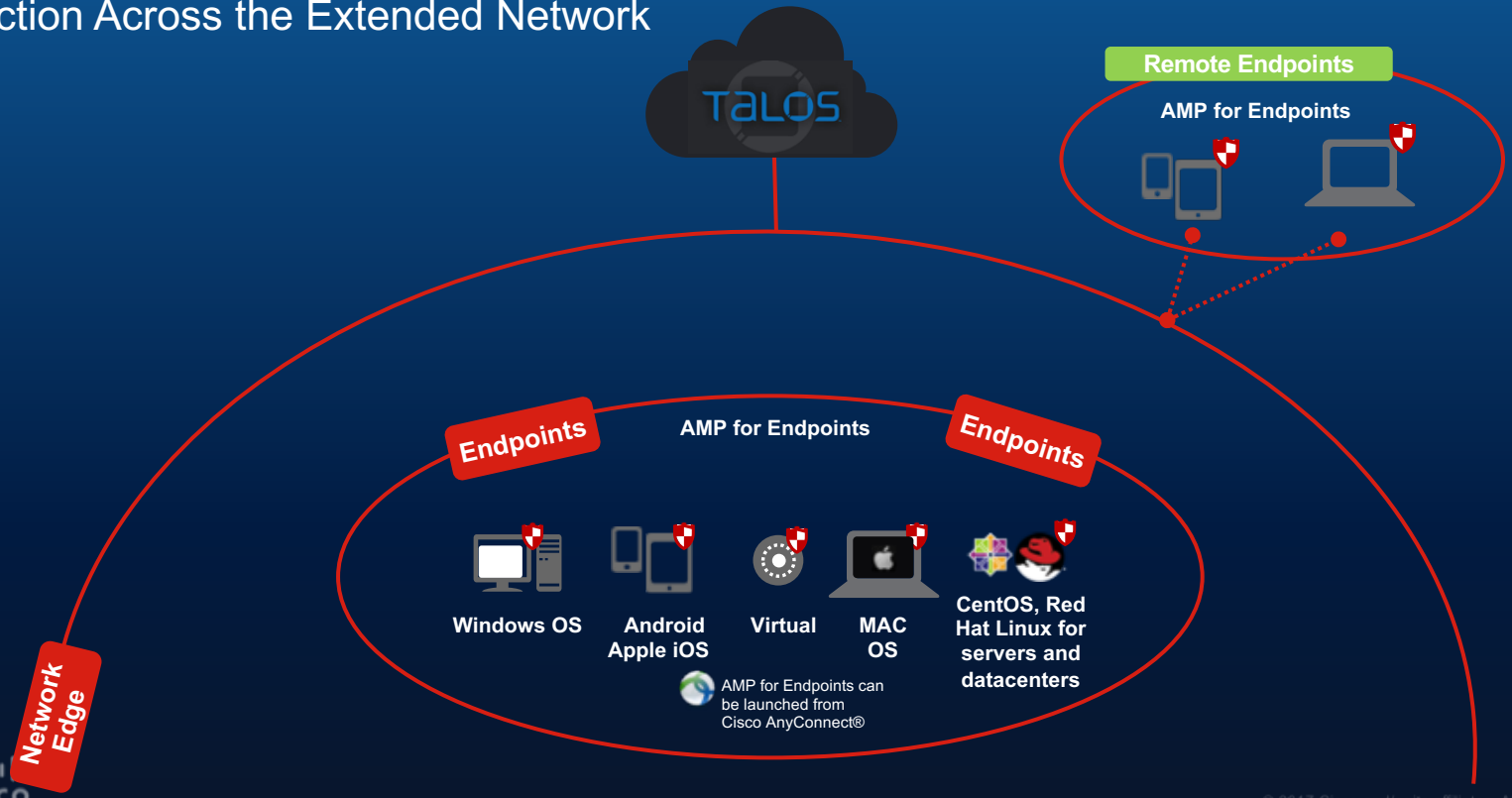
Over 600 leading professional services including law and consulting firms

Over 500 leading finance, banking, and insurance companies

Over 500 leading manufacturing and technology companies

AMP : Next Gen Endpoint Protection

Advanced Malware Protection
Protection Across the Extended Network



What's different between Next-Gen Endpoint Security, vs Traditional AV?

How has the threat landscape changed, and why are these next-gen technologies important in protecting against the latest threats?

- The volume of malware, and its ability to mutate and disguise itself in new ways, has become extraordinary.

- The attackers have become more sophisticated. Businesses are no longer just protecting against a computer getting infected. Now they're protecting against their business being breached.

Nyetya, Petyam, WannaCry and other sophisticated ransomware

- The WannaCry attack took advantage of a recently-patched Windows vulnerability to spread via the network, and then dropped previously-unseen malware that encrypted users' files.
- This shows that a comprehensive security program, that covers everything from your users' behavior to what enters your organization via email or web to how your endpoints are protected, is critical.

Machine Learning

- Machine learning does not rely on signatures, it can stop malware that has never been seen before by determining how similar it is to the universe of known threats.
- Machine learning is best when trained on very large data sets that have been analyzed and accurately categorized by experts.
- Machine learning has the ability to detect both known and unknown malware before the file executes

User and entity behavior analytics (UEBA)

- User and entity behavior analytics (UEBA) is great at detecting anomalies,

- The key to UEBA is that it is attempting to see what is normal and what is abnormal for a specific user, versus a universal population

AMP for Endpoints - Exploit Prevention to Stop File-Less Attacks

Cisco AMP for Endpoints now introduces "exploit prevention" capabilities that will defend your endpoints from file-less attacks that use memory injection on unpatched software vulnerabilities.

These types of attacks include:

- web-borne attacks, such as Java exploits that use shellcode to run payload
- malicious Adobe and Office document files
- malicious sites containing Flash, Silverlight and Javascript attacks
- vulnerabilities exploited by file-less and non-persistent malware
- zero-day attacks on software vulnerabilities yet to be patched
- ransomware, Trojans, or macros using in-memory techniques

AMP for Endpoints - Exploit Prevention to Stop File-Less Attacks

Some of the more common processes that Cisco AMP for Endpoints protects include:

- Microsoft Excel Application
- Microsoft Word Application
- Microsoft PowerPoint Application
- Microsoft Outlook Application
- Internet Explorer Browser
- Mozilla Firefox Browser
- Google Chrome Browser
- Microsoft Skype Application
- TeamViewer Application
- VLC Media player Application
- Microsoft Windows Script Host
- Microsoft Powershell Application
- Adobe Acrobat Reader Application
- Microsoft Register Server
- Microsoft Task Scheduler Engine

Malicious Activity Protection (or MAP) defends your endpoints from ransomware attacks

- observes the behavior of running processes
- identifies malicious actions of processes when they execute

and

- stops them from encrypting your data.

The need for next-gen endpoint security

- Next-gen endpoint protection is a valuable part of this multi-layered strategy.
- Machine learning detects and stops previously unseen malware.
- Behavior-based protection catches ransomware “in the act” and prevents files from being encrypted.
- Exploit Prevention to stop file-less attacks.
- Malicious Activity Protection

What do you get with AMP for Endpoints ?

Includes Antivirus and 0day threat detection

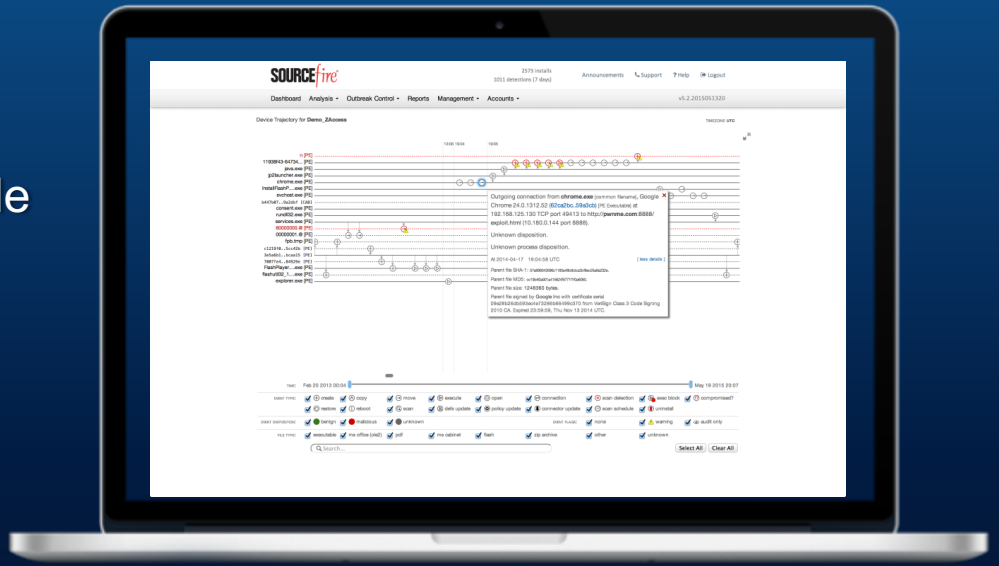
Identifies Known and unknown threats

Continuous Visibility into File Activity, File Operations, processes Vulnerabilities

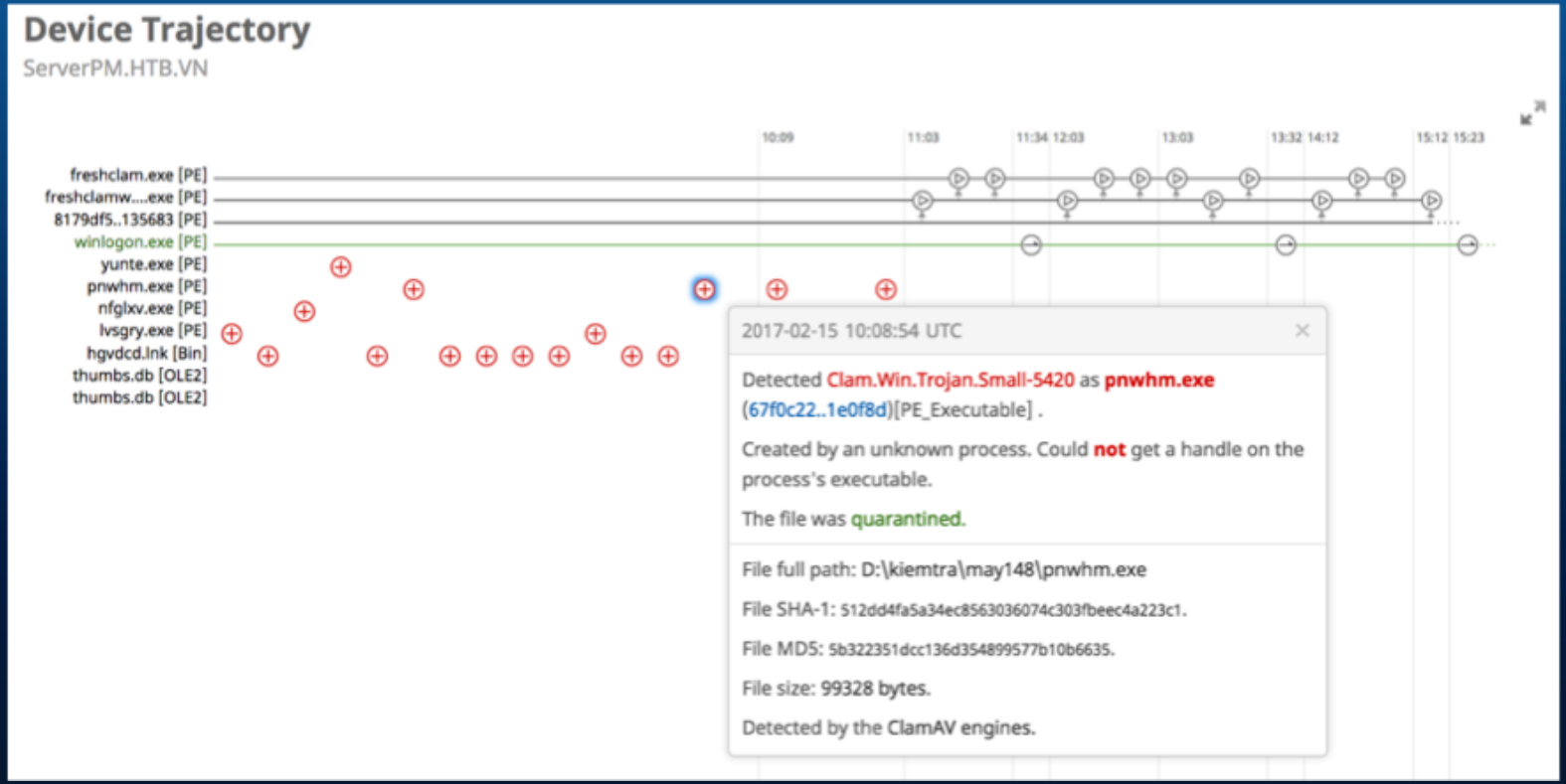
Visibility both On and Off the Network

Quarantine Threats on the Endpoint

Prevention, Monitoring + Detection, Response



Track active processes and see history



What do you get with AMP for Endpoints ?

What do you get with AMP for Endpoints ?

AV Engine

Command Line Visibility

File Reputation

Exploit Prevention

Machine Learning

Indications of Compromise

Malicious Activity Protection

Sandboxing

Continuous Analysis

Compare Endpoint Security Solutions

Close all	Cisco AMP for Endpoints	Carbon Black Endpoint Security	CrowdStrike Falcon	CylancePROTECT
Detection				
Number of integrated detection techniques	13	4	4	3
Continuous analysis and retrospective detection	✓	Limited	✓	✓
Device trajectory	Continuous	✓	✗	Limited
Detection measures	Multiple	Multiple	Multiple	Multiple
Dynamic file analysis	Threat Grid	✗	✗	✗
File analysis deployment model	Both	✗	✗	✗
API support	✓	✓	✓	✓
File trajectory	✓	Limited	Limited	Limited

https://www.cisco.com/c/m/en_us/products/security/advanced-malware-protection/competitive-comparison.html

AMP : Third Party Validation

Gartner

NSS LABS
RECOMMENDED

cisco

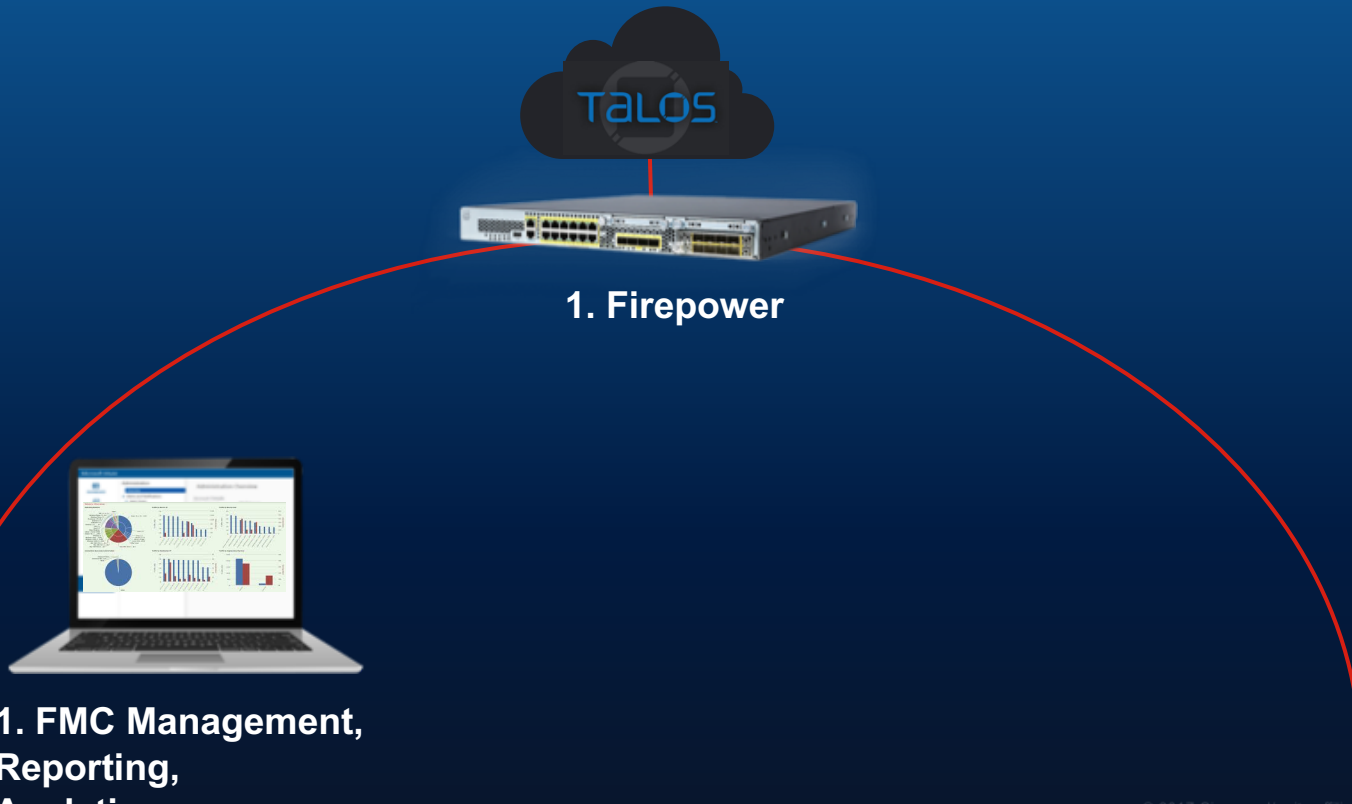
IDC Names Cisco AMP for Endpoints a Leader in 2017 Endpoint Security Marketscape

IDC Names Cisco AMP for Endpoints a Leader in 2017 Endpoint Security Marketscape

https://blogs.cisco.com/security/idc-names-cisco-amp-for-endpoints-a-leader-in-2017-endpoint-security-marketscape

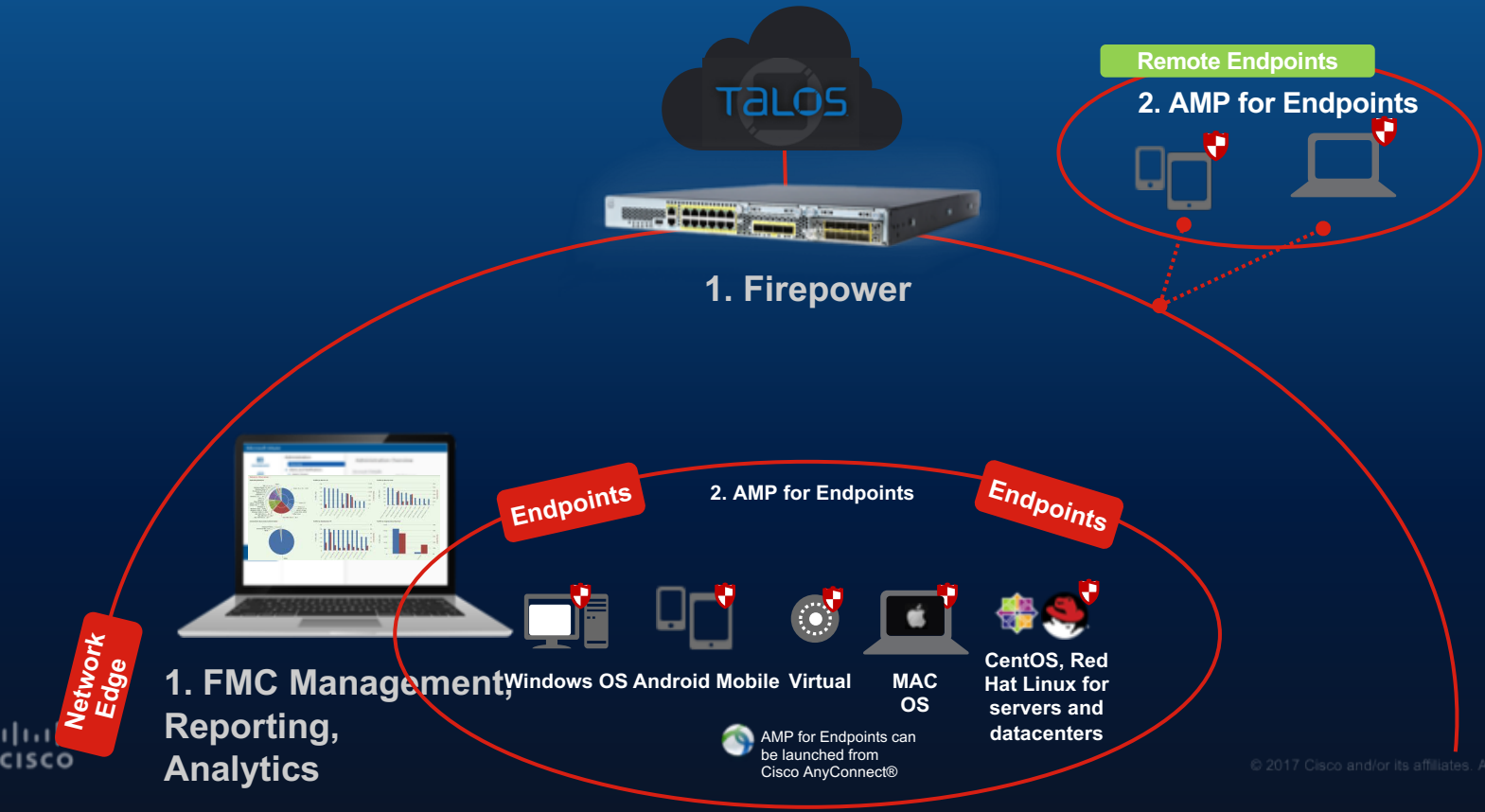
https://engage2demand.cisco.com/LP=3933

Security Architecture



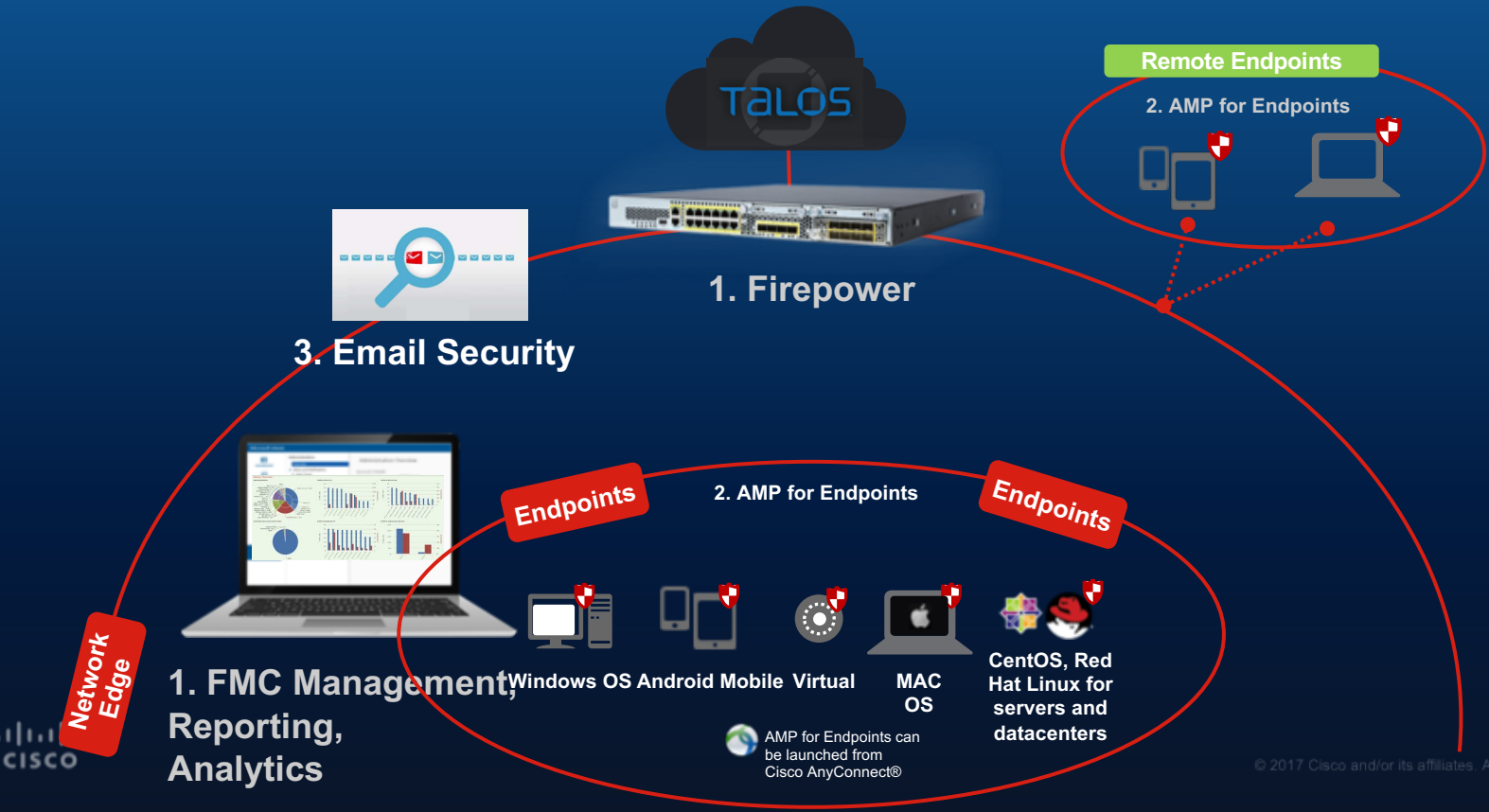
Security Architecture

1. Firepower
2. AMP for endpoint



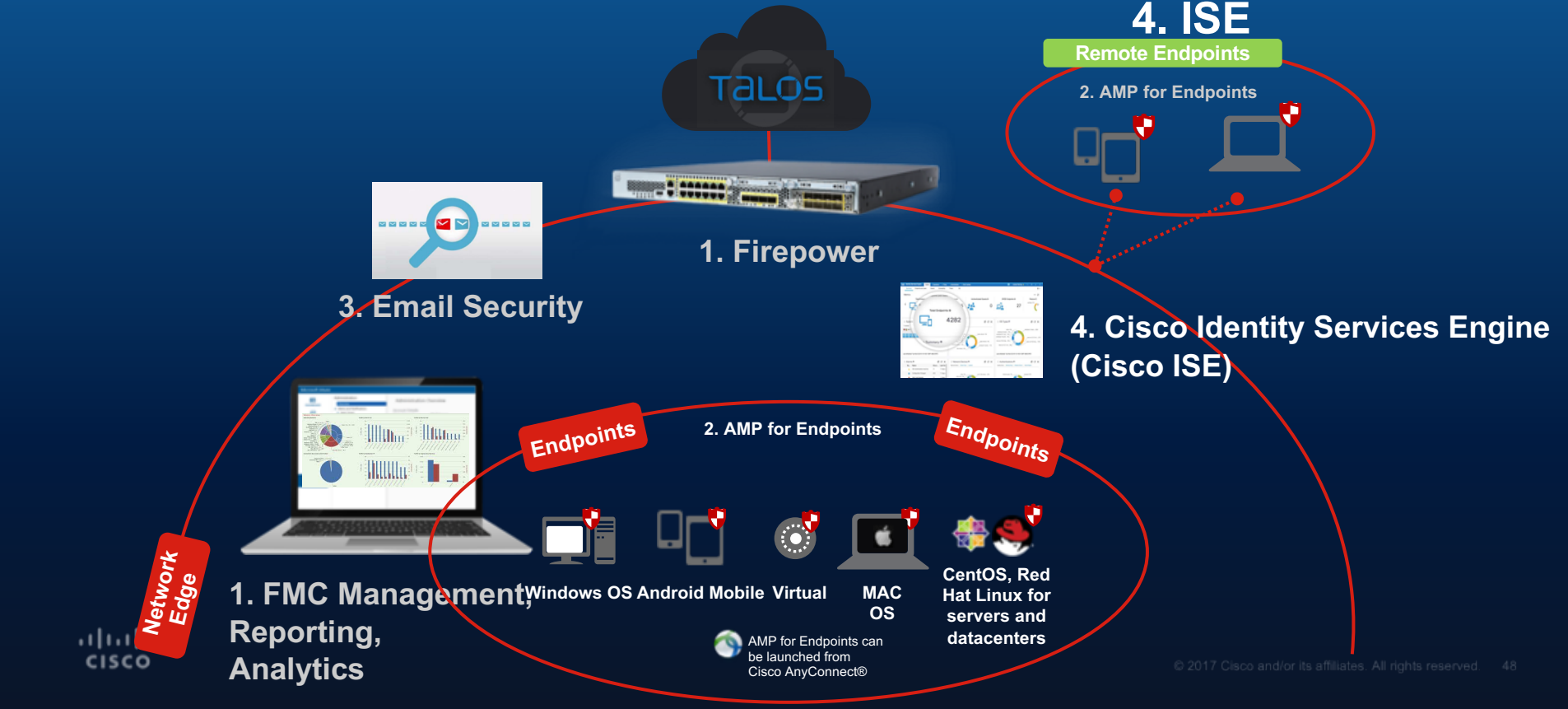
Security Architecture

1. Firepower
2. AMP for endpoint
3. Email Security



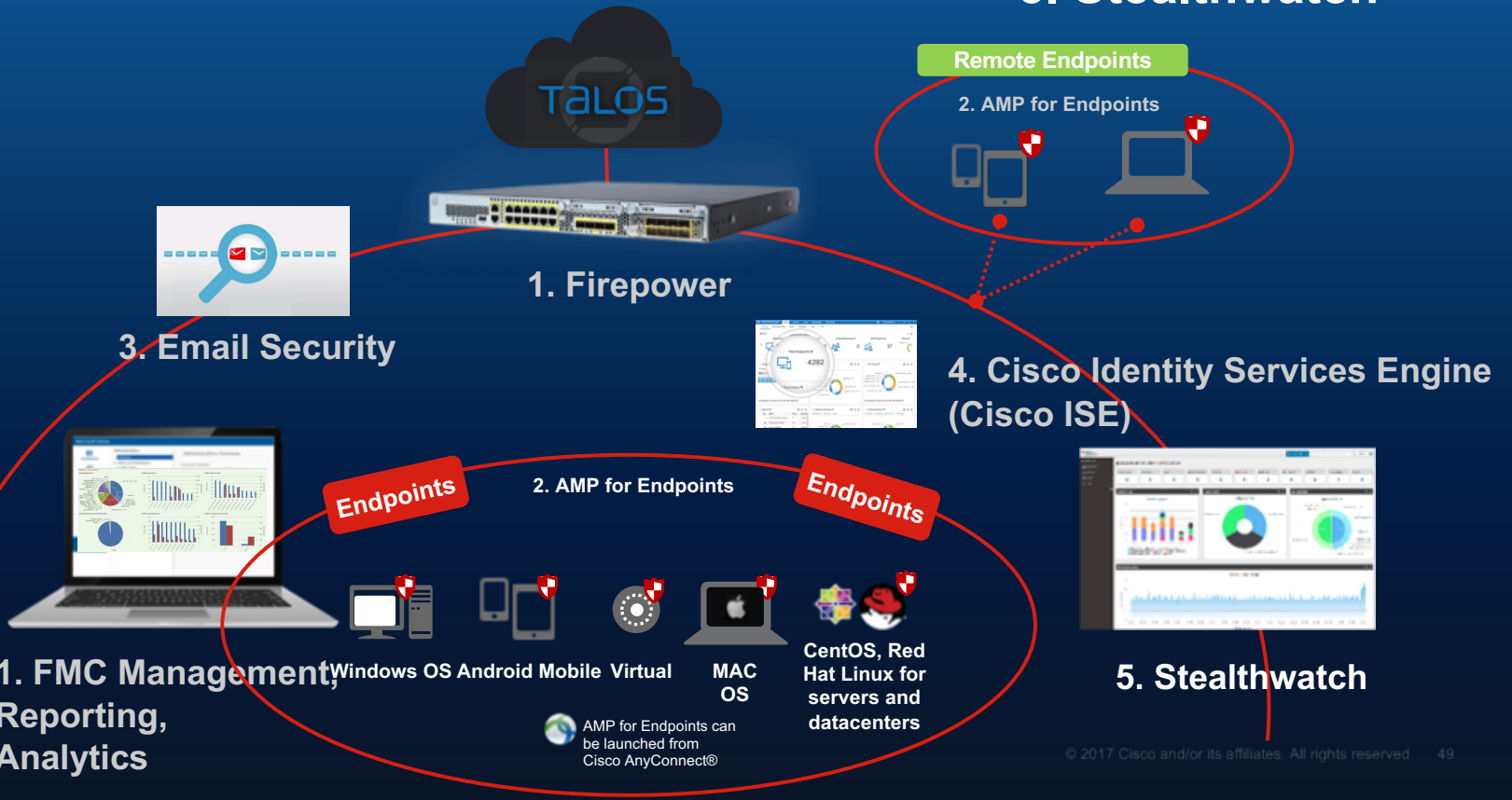
Security Architecture

1. Firepower
2. AMP for endpoint
3. Email Security
4. ISE



Security Architecture

1. Firepower
2. AMP for endpoint
3. Email Security
4. ISE
5. Stealthwatch



Security Architecture

1. Firepower
2. AMP for endpoint
3. Email Security
4. ISE
5. Stealthwatch
6. Cloud Security

6. Cloud Security

Umbrella

CloudLock

TALOS

Remote Endpoints

2. AMP for Endpoints

1. Firepower

3. Email Security

4. Cisco Identity Services Engine (Cisco ISE)

Endpoints

2. AMP for Endpoints

Endpoints

Windows OS

Android Mobile

Virtual

MAC OS

CentOS, Red Hat Linux for servers and datacenters

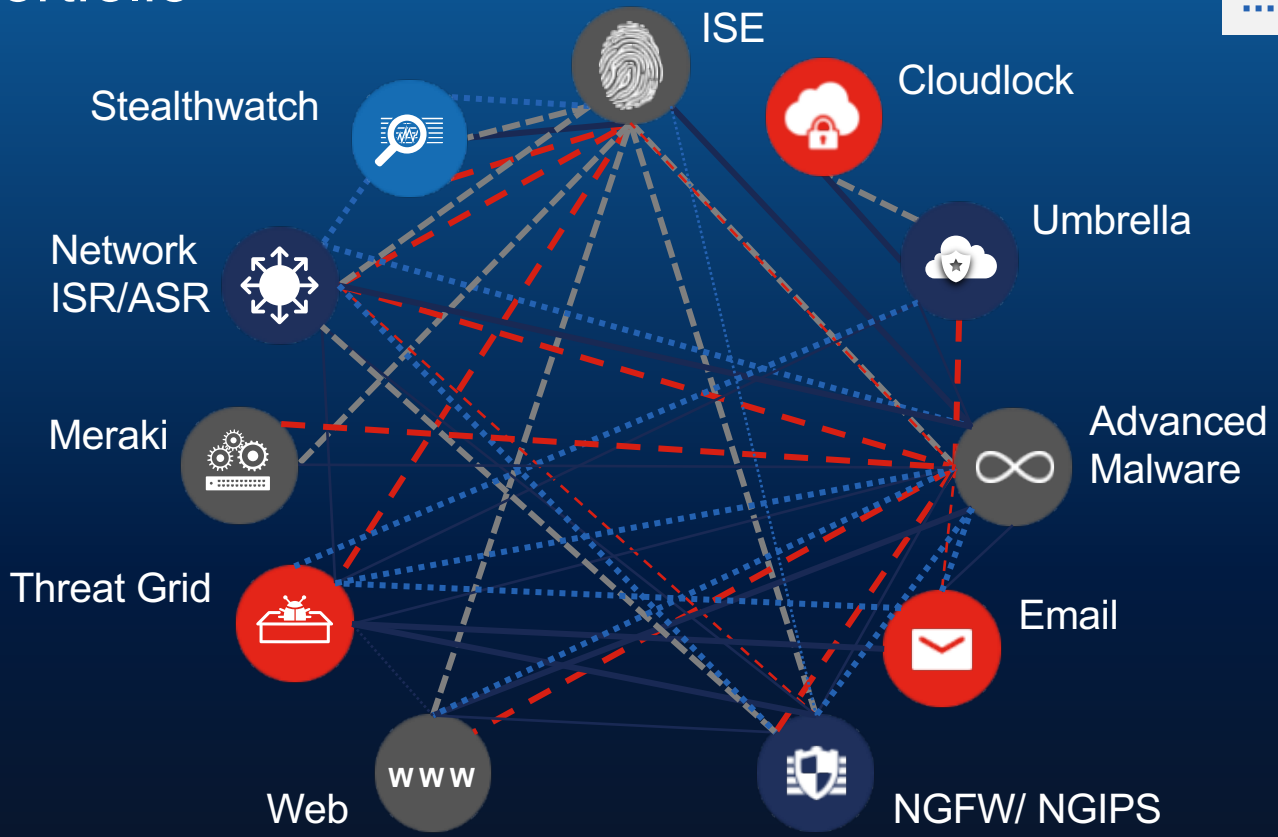
AMP for Endpoints can be launched from Cisco AnyConnect®

Network Edge

1. FMC Management, Reporting, Analytics

5. Stealthwatch

Solution Integration:
Cisco Portfolio



Nikos Mourtzinos,
Cyber Security Sales Specialist
nmourtzi@cisco.com
Linkedin nmourtzi
Twitter: @nmourtzinos