Changing the Security Equation

Effective Integrated Security

John Maynard
Vice President, Global Security – EMEAR

July 2018

Internet users

415M

2000

→

3.9B

2018

2018

Source: Internet Live Stats

Ransomware

$325M

2015

→

$11.5B

2019

2018 | 2019

Source: Cybersecurity Ventures

IoT Devices

2B
2006

200B
2020

2018 2019 2020

Source: Intel

Cybercrime

$3T

2015

→

$6T

2021

2018 2019 2020 2021

Source: Cybersecurity Ventures

A New Era of Digitization

Brings a new era of security challenges

More IoT devices connect everyday

Expanded attack surface

Users work from anywhere across many devices

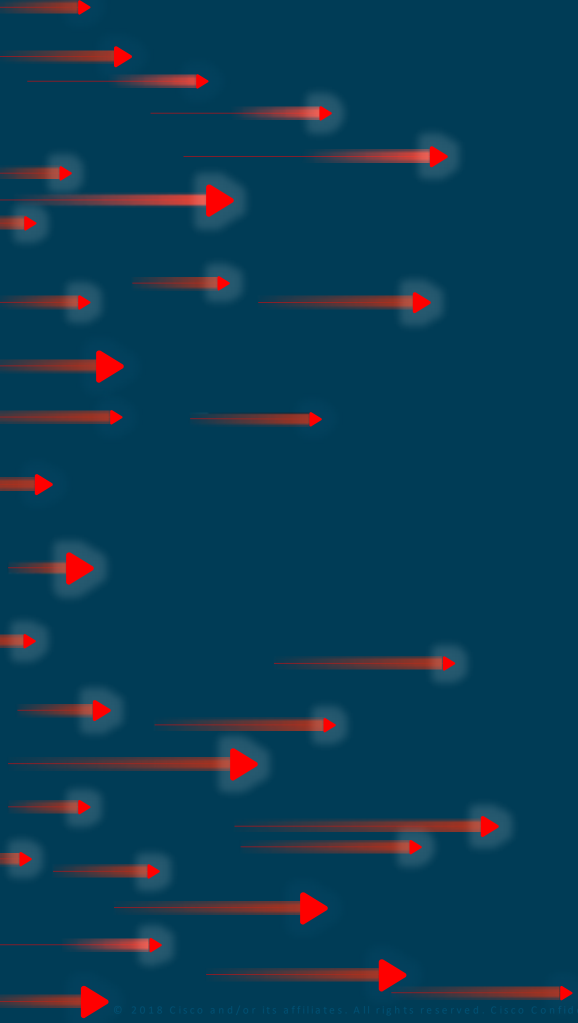
Loss of visibility

Workloads are moving to the cloud

Loss of control

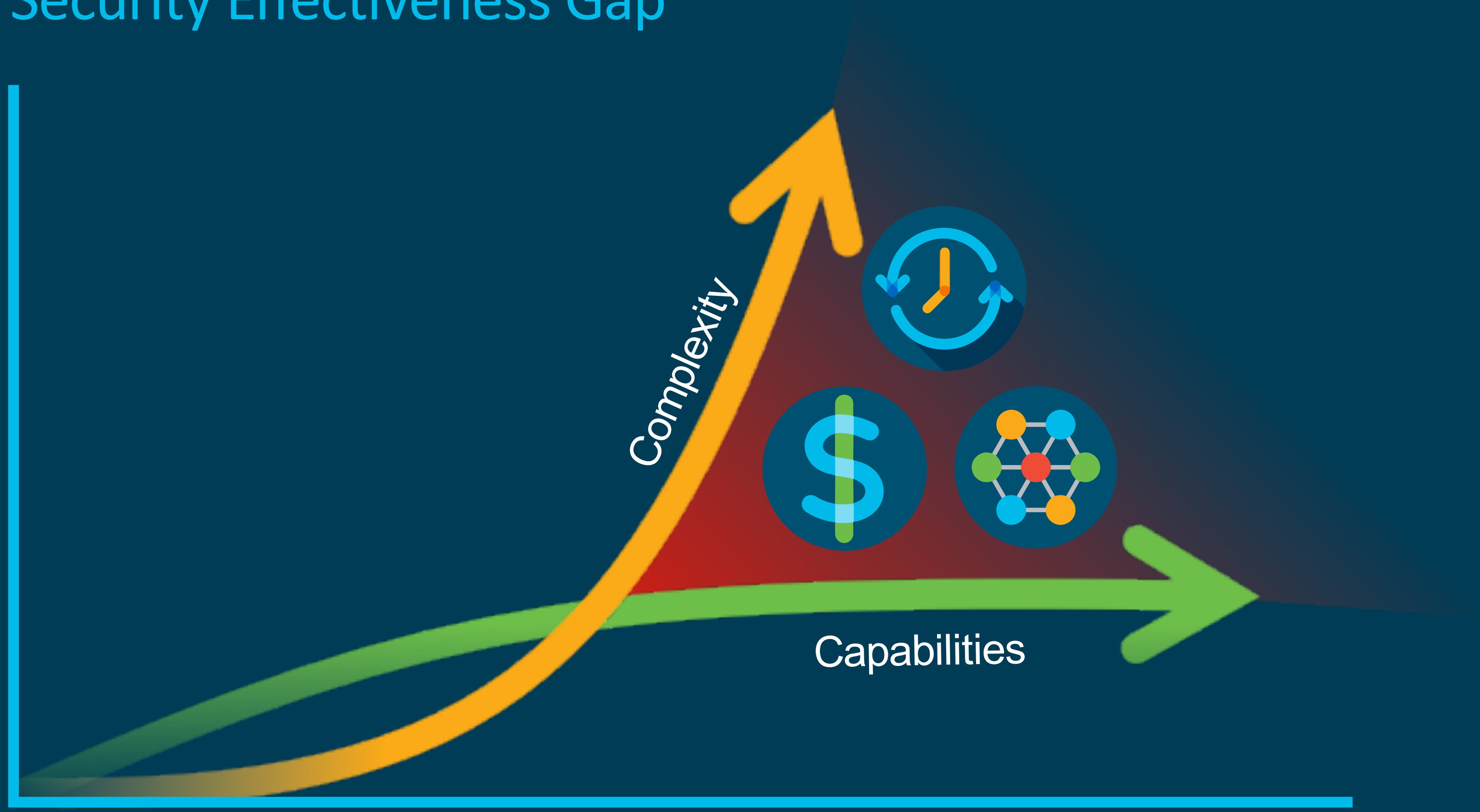
Threats are more numerous and persistent

High likelihood of a breach

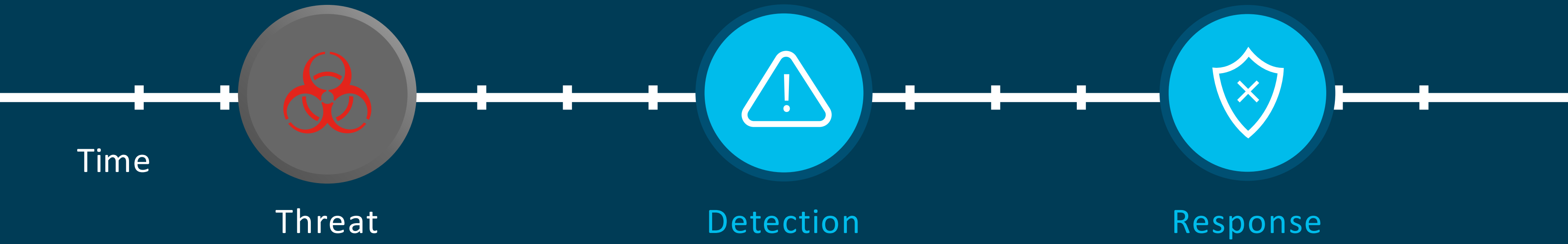


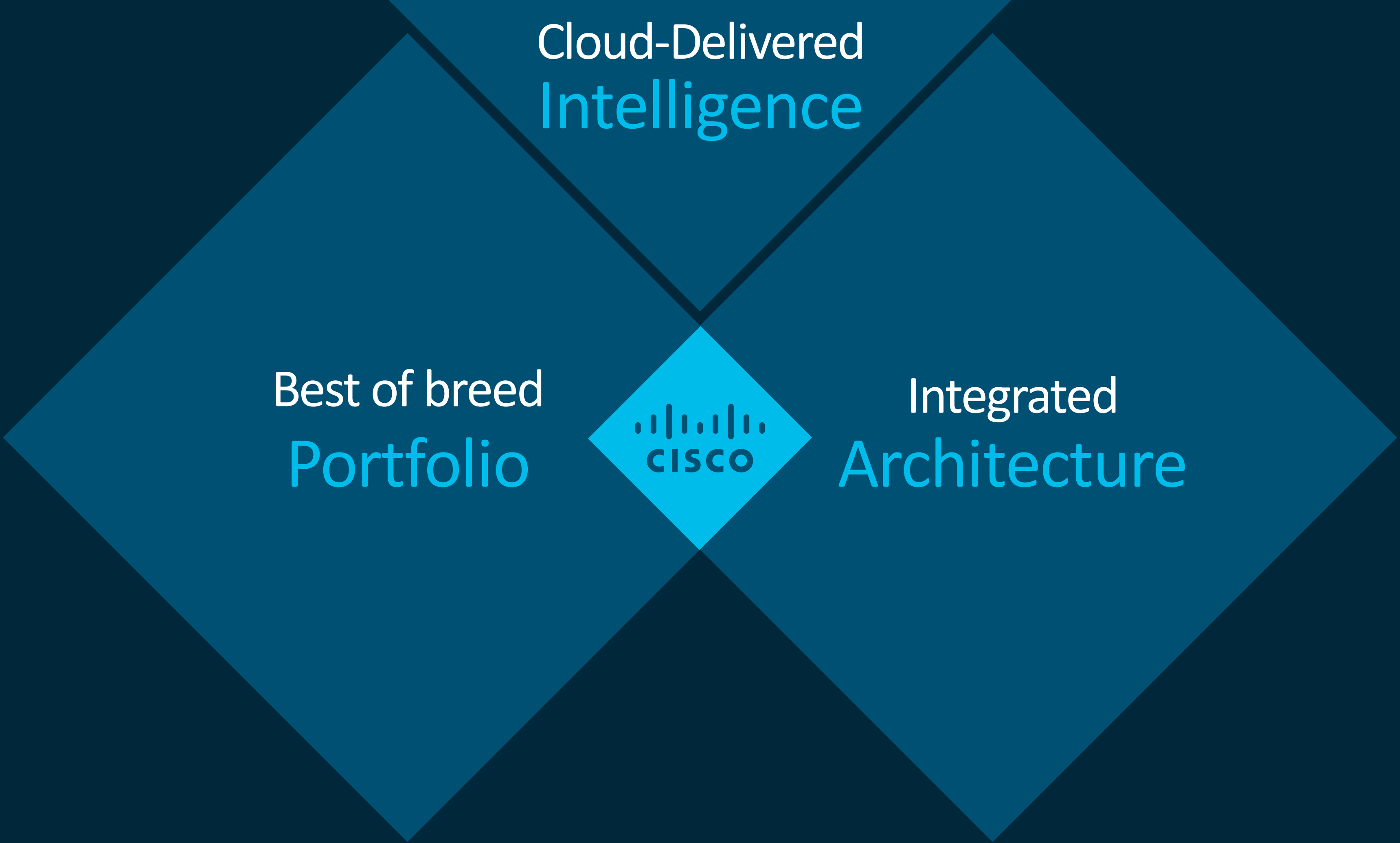
- Multi-vector multi-stage threats
- Flooded with products
- Lack of talent

The Security Effectiveness Gap



Do you have an effective security posture?



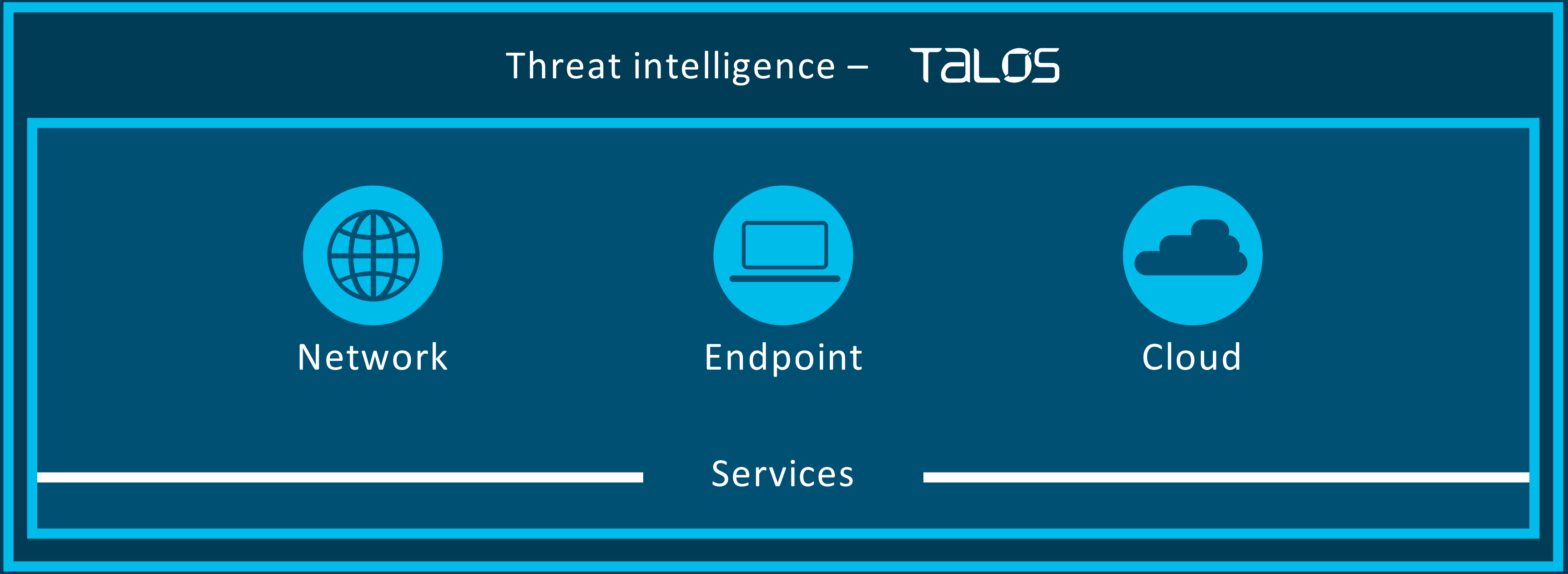


Cloud-Delivered
Intelligence

Best of breed
Portfolio

Integrated
Architecture

Cisco Security Architecture



Threat intelligence – TALOS

Network

Endpoint

Cloud

Services

Unmatched Visibility, Threat Research, and Analytics

7.5 Billion

Total World Population

600 Billion

Email Samples

16 Billion

Web Requests

3.4 Billion

AMP Queries

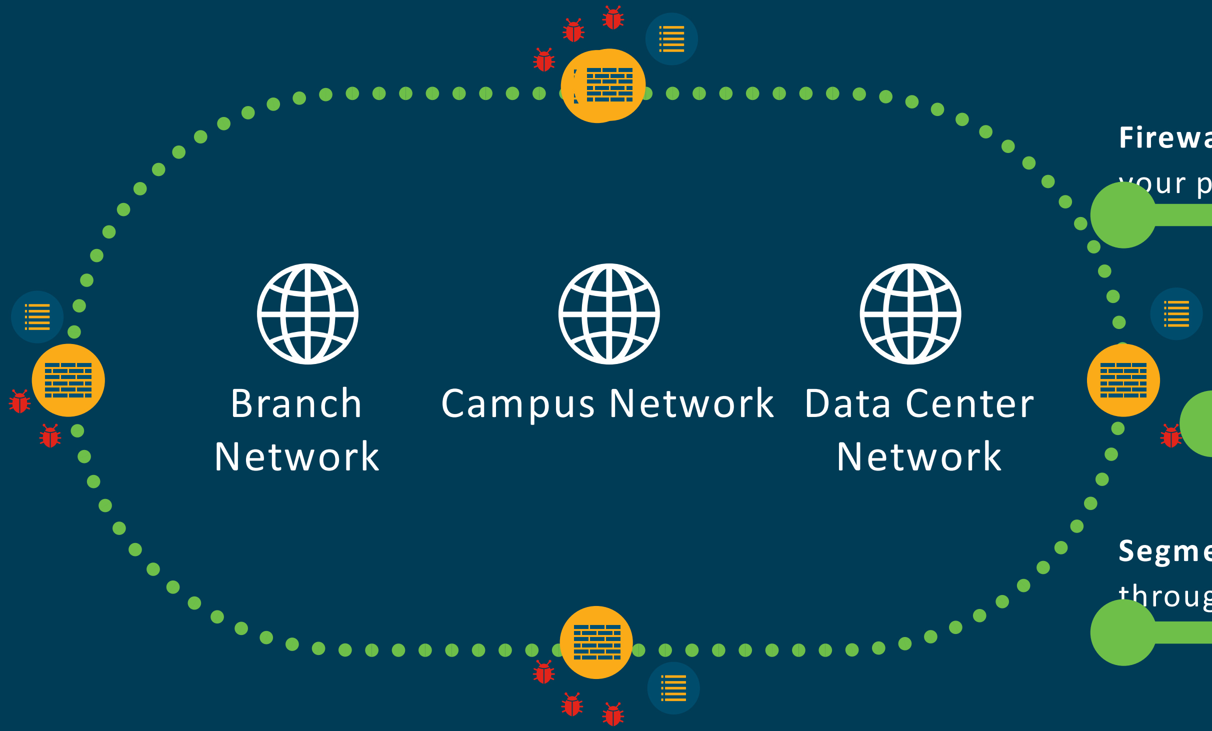
19.7 Billion Threats Blocked DAILY

About 3 threats per person

EVERY DAY

The Network is the Cornerstone of Digital Success (or Failure)

Network security was focused on the perimeter



Firewalls secured your perimeter

Visibility into what's leaving and coming in

Segmentation managed through IP access lists

Cisco has embedded security into the network

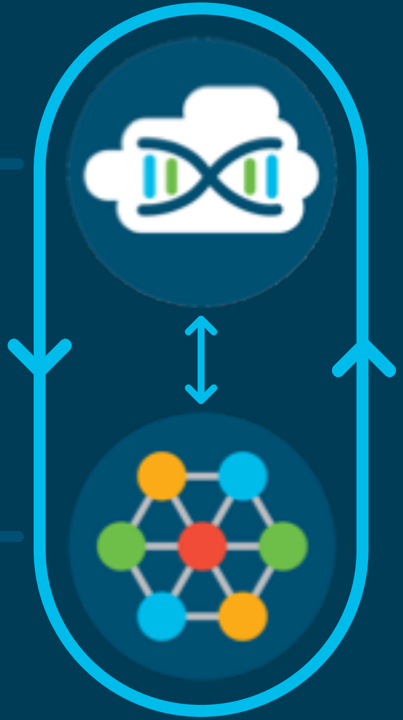
Network Security

Visibility

Segmentation

Threat Protection

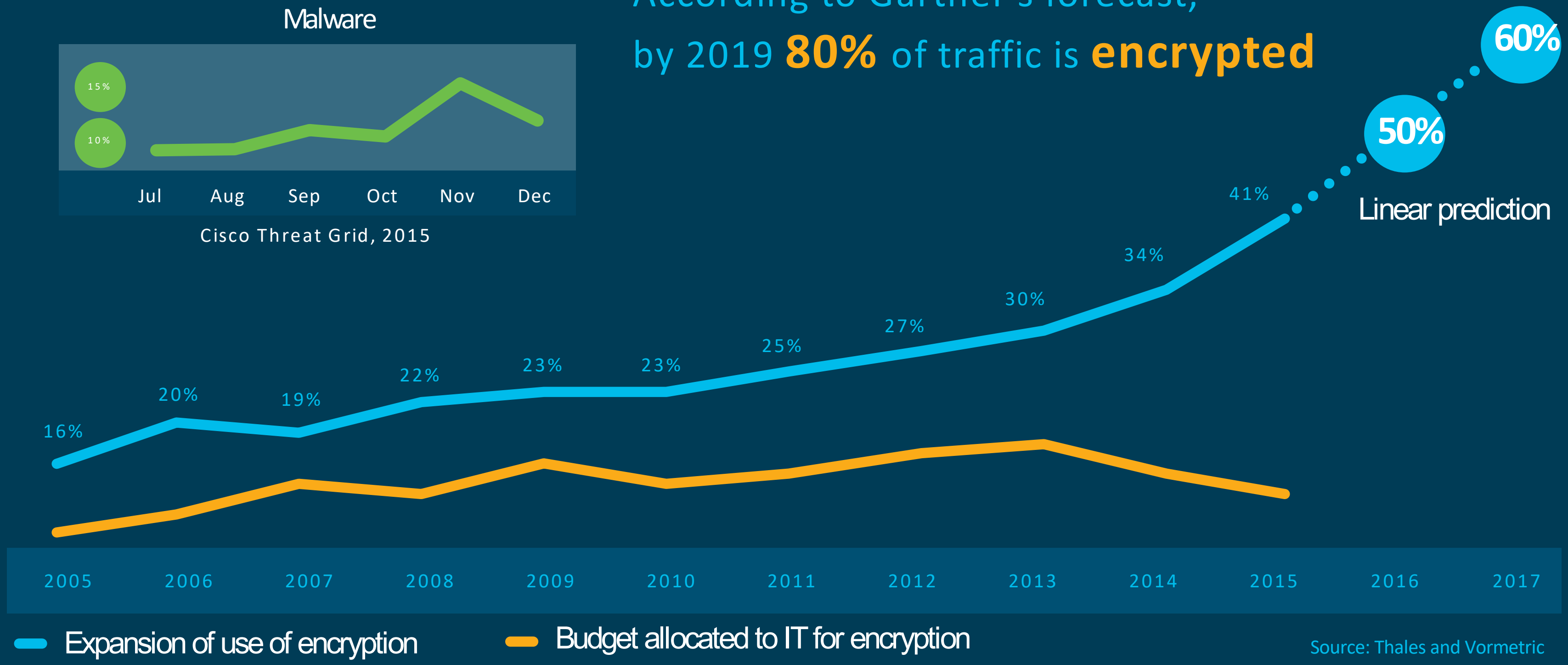
Intent-based Network Infrastructure



SECURITY

Threats changing by encryption

According to Gartner's forecast,
by 2019 **80%** of traffic is **encrypted**



Source: Thales and Vormetric

Protect the Business: Encrypted Traffic Analytics

Visibility and Malware Detection without Decryption

Malware in Encrypted Traffic

ETA algorithms analyze multiple network data sources

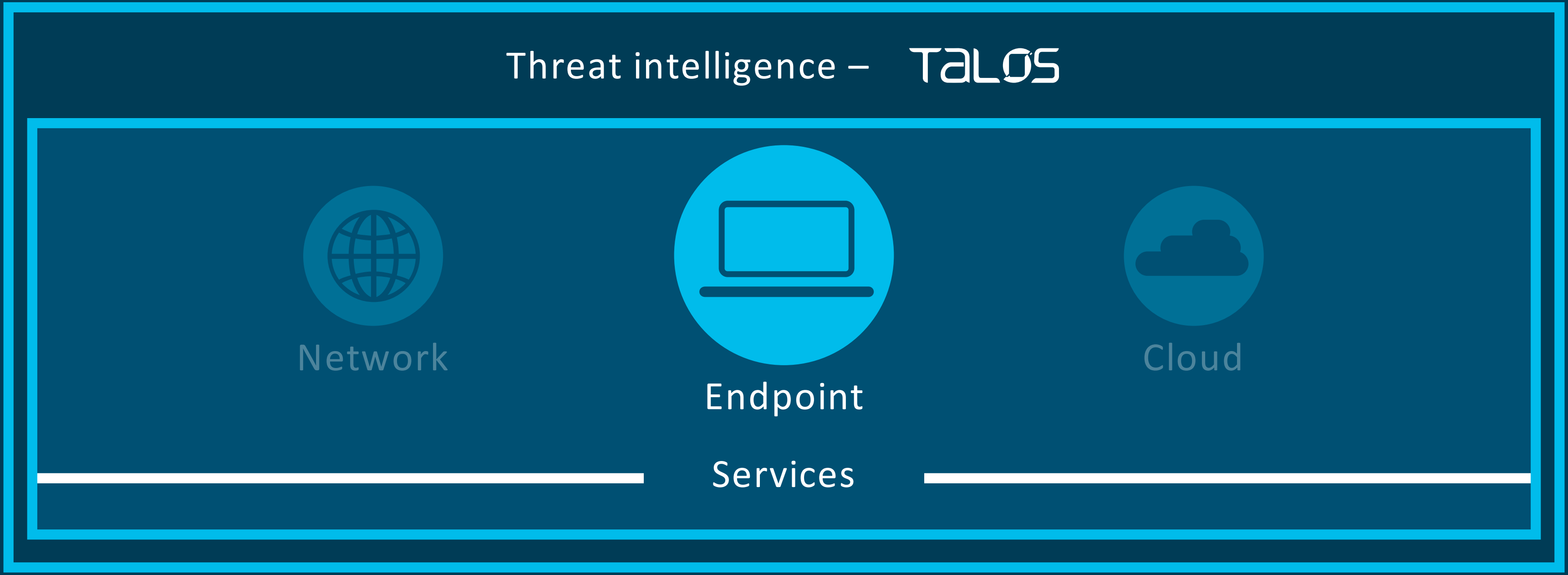
Security AND Privacy

No information is decrypted

Detection Accuracy

99.99% Accuracy

Cisco Security Architecture



Threat intelligence – TALOS

Network

Endpoint

Cloud

Services

Uncover the 1% with Cisco AMP for Endpoints

Stop malware

Using multiple detection and protection mechanisms

Eliminate blind spots

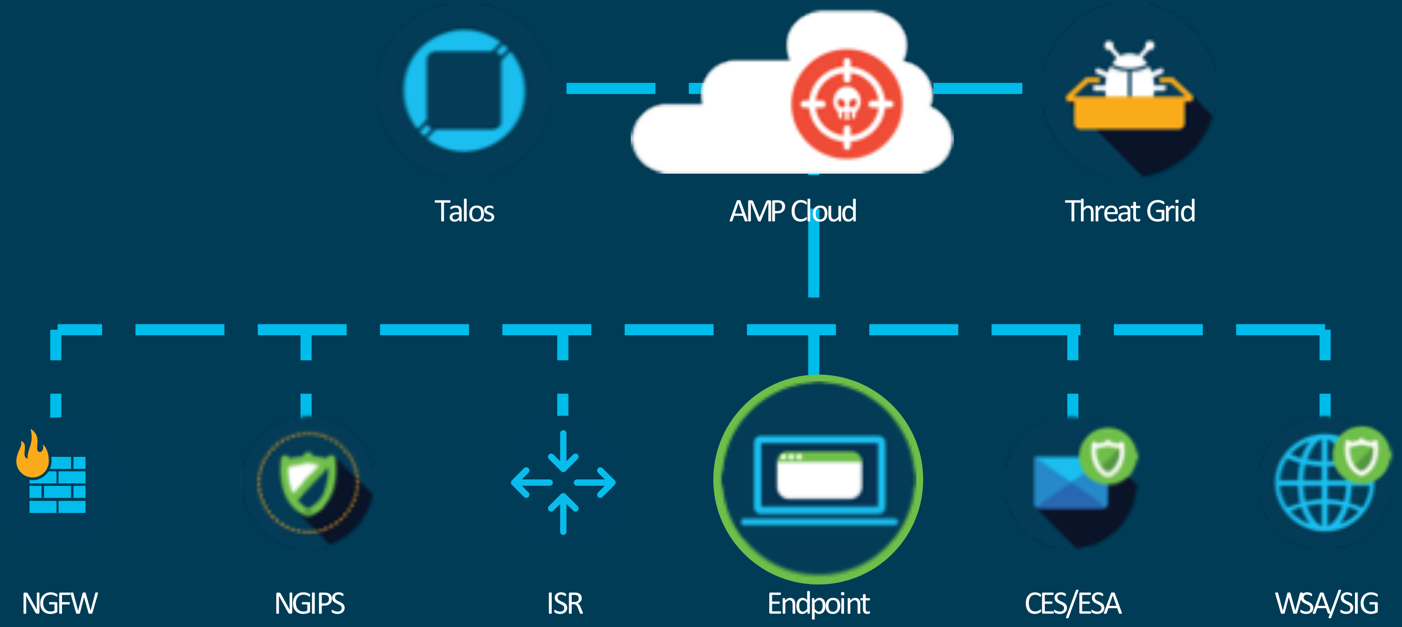
The network and endpoint, working together across all operating systems

Discover unknown threats

With proactive threat hunting

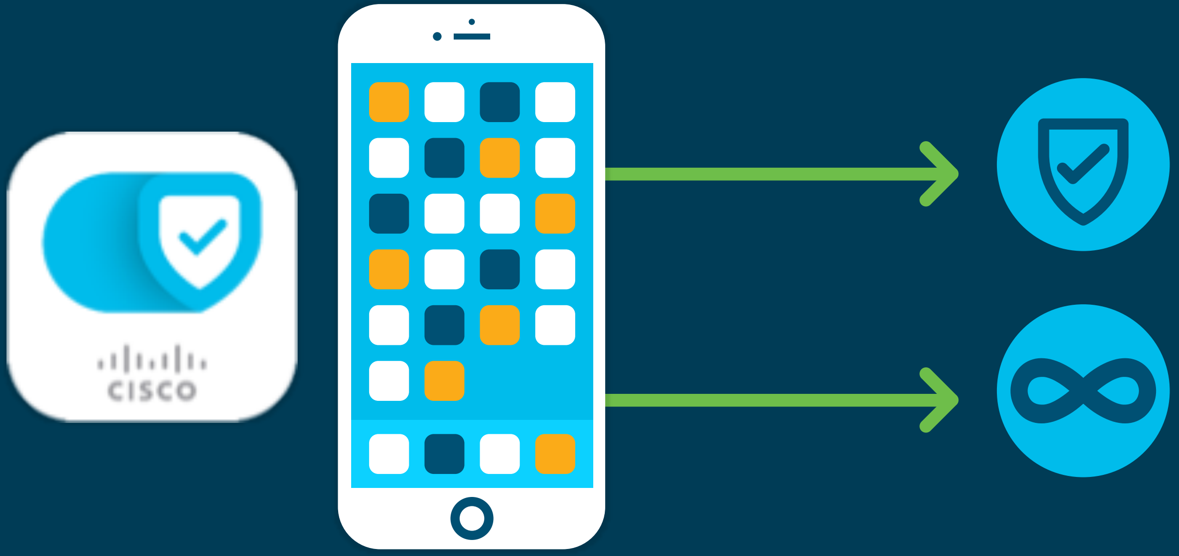
See once, block everywhere

Share intelligence across network, web, email, and endpoints to see once, block everywhere



Cisco Security Connector

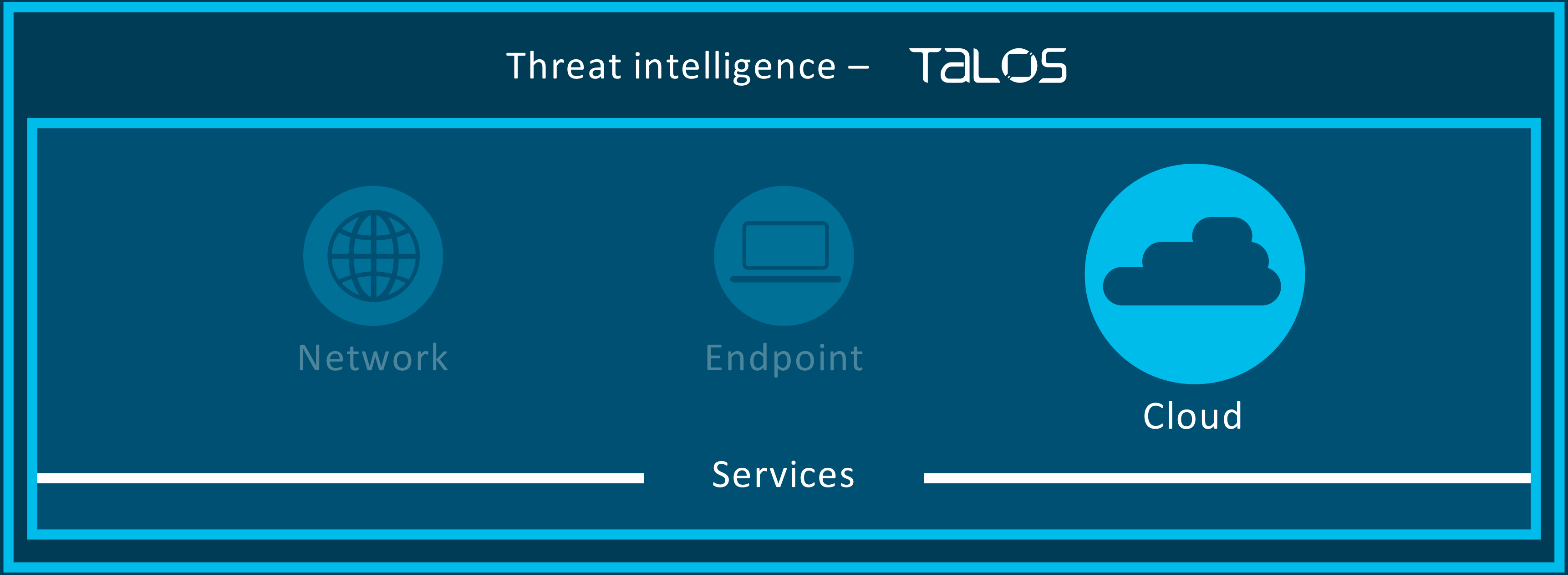
The first ever security application for iOS



Cisco Umbrella

Advanced Malware Protection (AMP)

Cisco Security Architecture



Most Everyone using the Cloud

Organizations increase reliance on the cloud

84%

will use multiple clouds

53%

manage over half
of their infrastructure
in the cloud

$3.6B

Cloud security market by 2020

Multicloud Security – What’s needed

Security to get
to the Cloud

**Secure Internet Gateway
(SIG)**

Security for
SaaS Apps

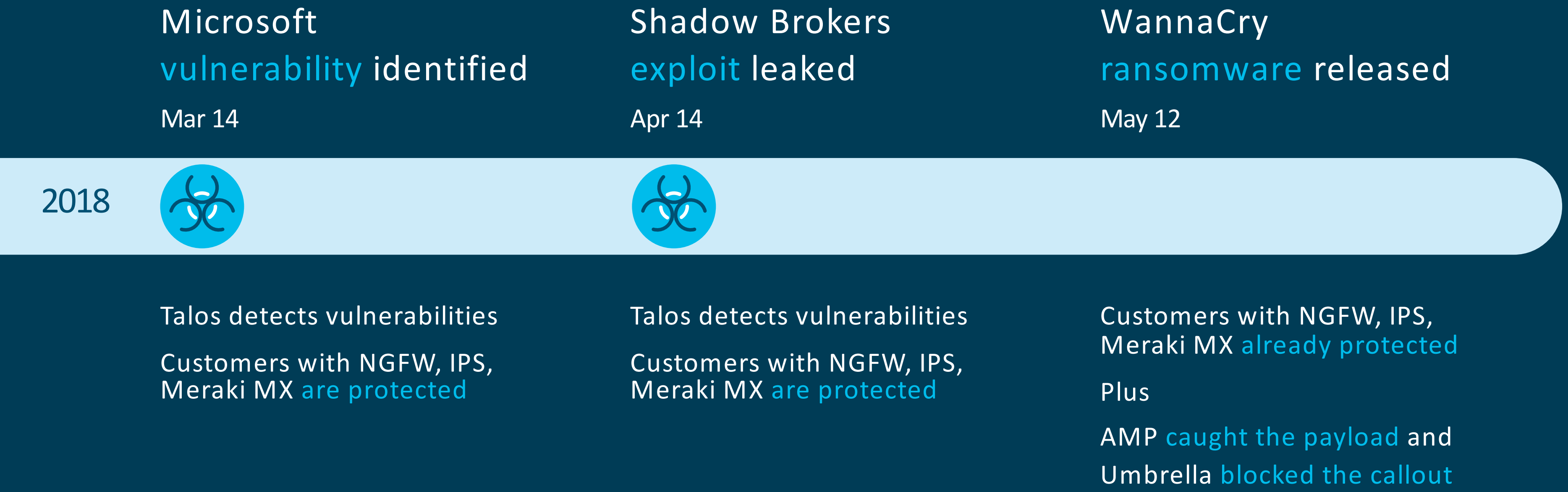
User, Data & App Security

Security for
Public Cloud

Visibility & Protection

WANNACRY

Talos brings the intelligence – Smarter every day



Microsoft vulnerability identified

Mar 14

Shadow Brokers exploit leaked

Apr 14

WannaCry ransomware released

May 12

2018

Talos detects vulnerabilities

Customers with NGFW, IPS, Meraki MX are protected

Talos detects vulnerabilities

Customers with NGFW, IPS, Meraki MX are protected

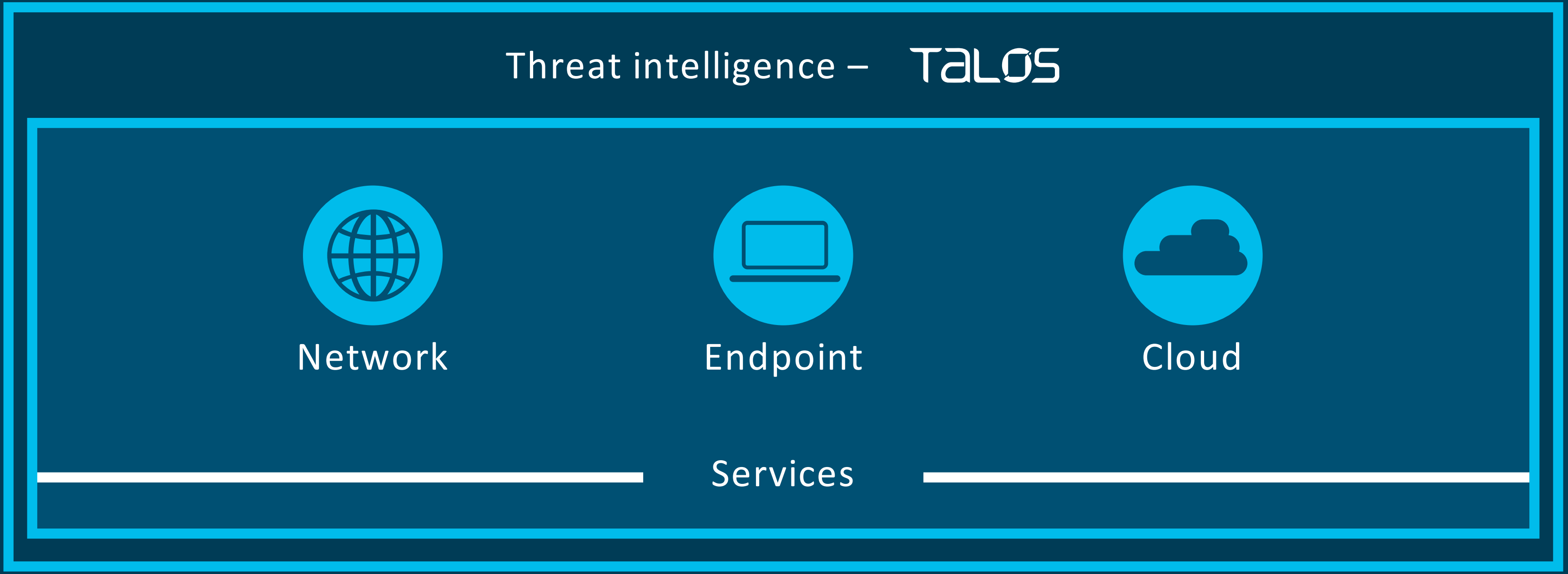
Customers with NGFW, IPS, Meraki MX already protected

Plus

AMP caught the payload and

Umbrella blocked the callout

Cisco Security Architecture



Threat intelligence – Talos

Network

Endpoint

Cloud

Services

Cisco Security Portfolio

Best of breed products integrated to protect all key vectors

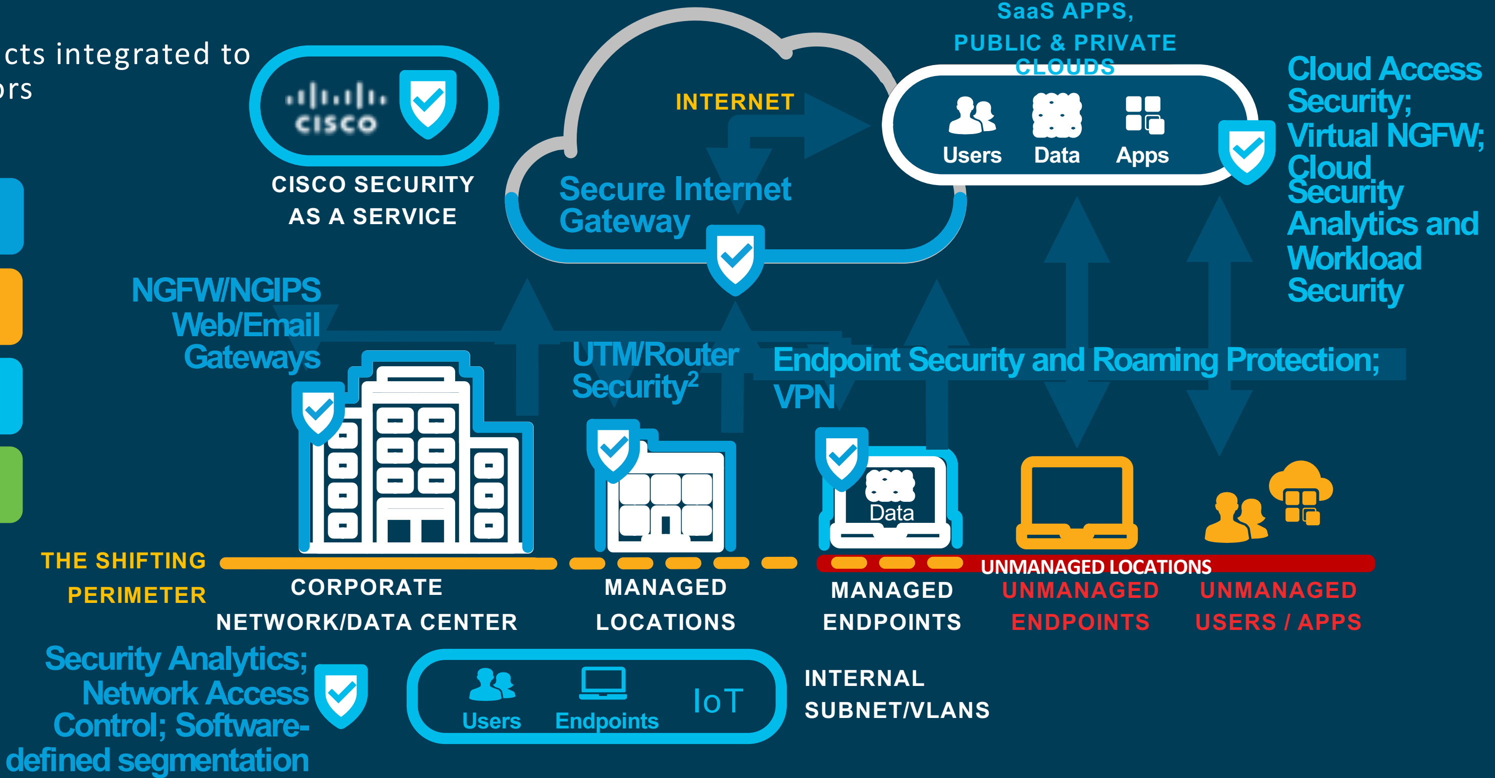
Network Security

Endpoint Security

Cloud Security

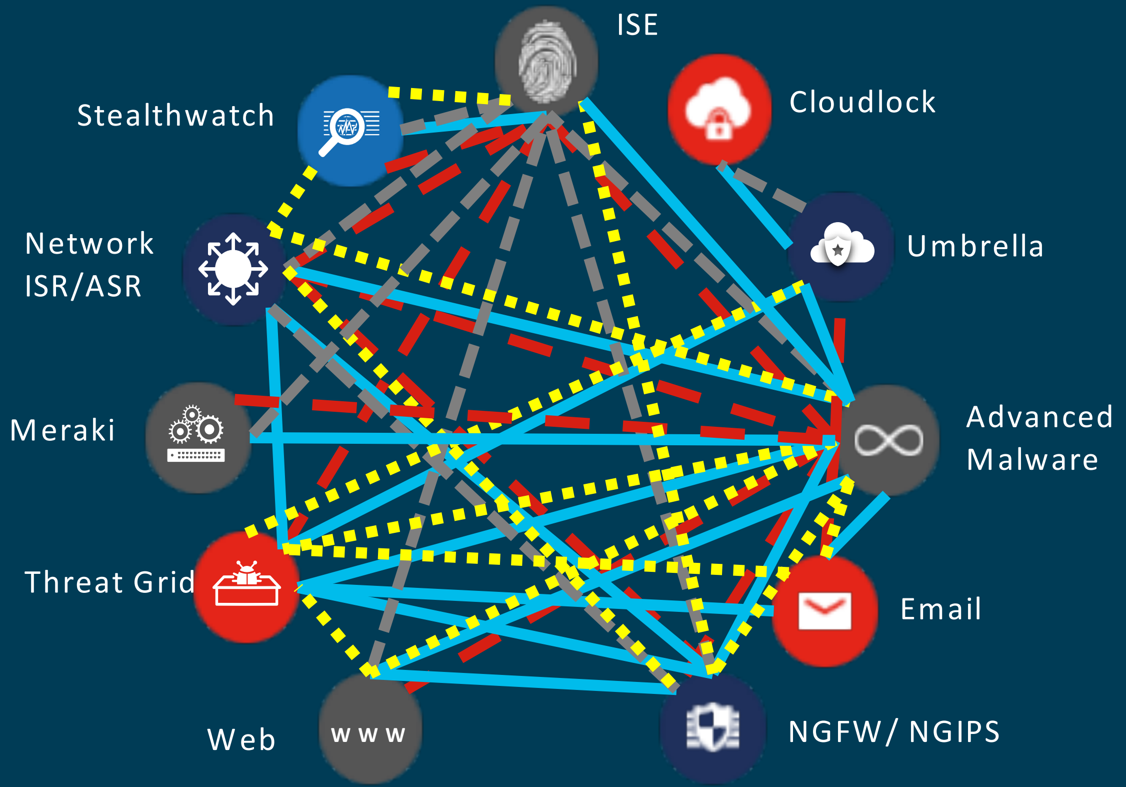
Security via the cloud

Cloud-managed network security, cloud–managed UTM, Cloud Threat Analytics and Sandboxing, Cloud Email Security



CISCO
CISCO SECURITY AS A SERVICE
INTERNET
Secure Internet Gateway
SaaS APPS, PUBLIC & PRIVATE CLOUDS
Users
Data
Apps
Cloud Access Security; Virtual NGFW; Cloud Security Analytics and Workload Security
NGFW/NGIPS Web/Email Gateways
UTM/Router Security²
Endpoint Security and Roaming Protection; VPN
Data
THE SHIFTING PERIMETER
UNMANAGED LOCATIONS
CORPORATE NETWORK/DATA CENTER
MANAGED LOCATIONS
MANAGED ENDPOINTS
UNMANAGED ENDPOINTS
UNMANAGED USERS / APPS
Security Analytics; Network Access Control; Software-defined segmentation
Users
Endpoints
IoT
INTERNAL SUBNET/VLANS

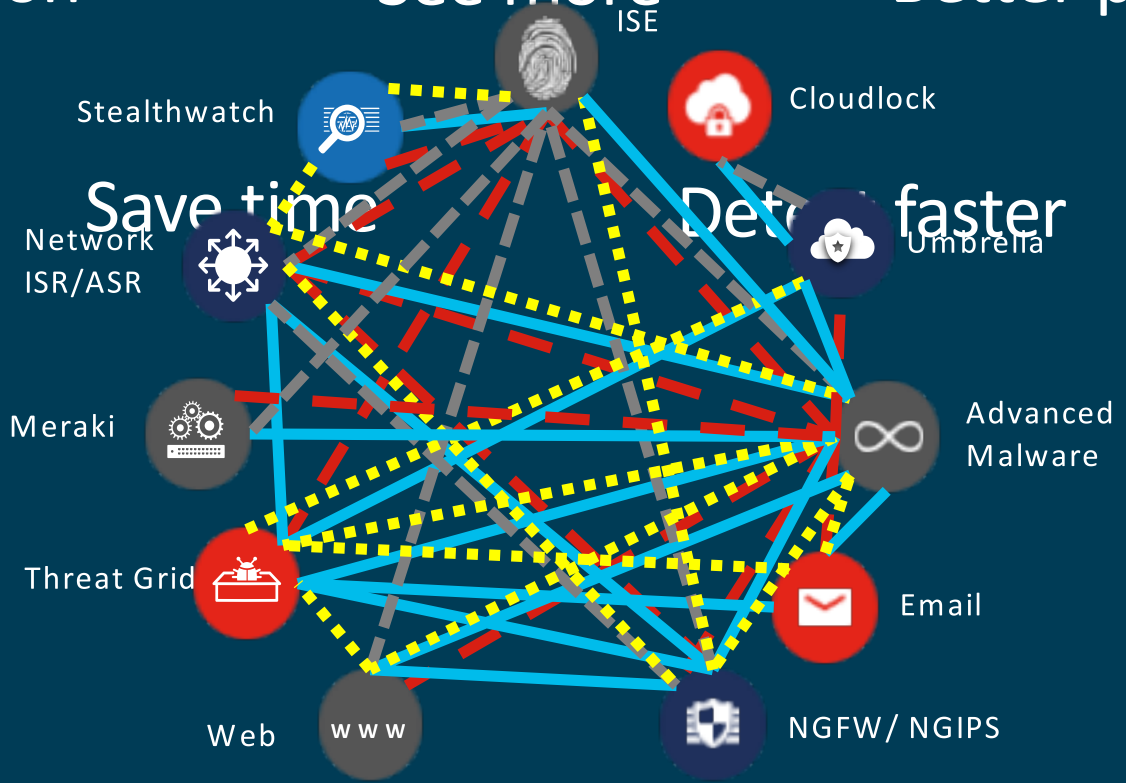
1. Not the same as cloud security
2. ISR Firepower services


ISE
Stealthwatch
Cloudlock
Network ISR/ASR
Umbrella
Meraki
Advanced Malware
Threat Grid
Email
Web
w w w
NGFW/ NGIPS

Automation

See more

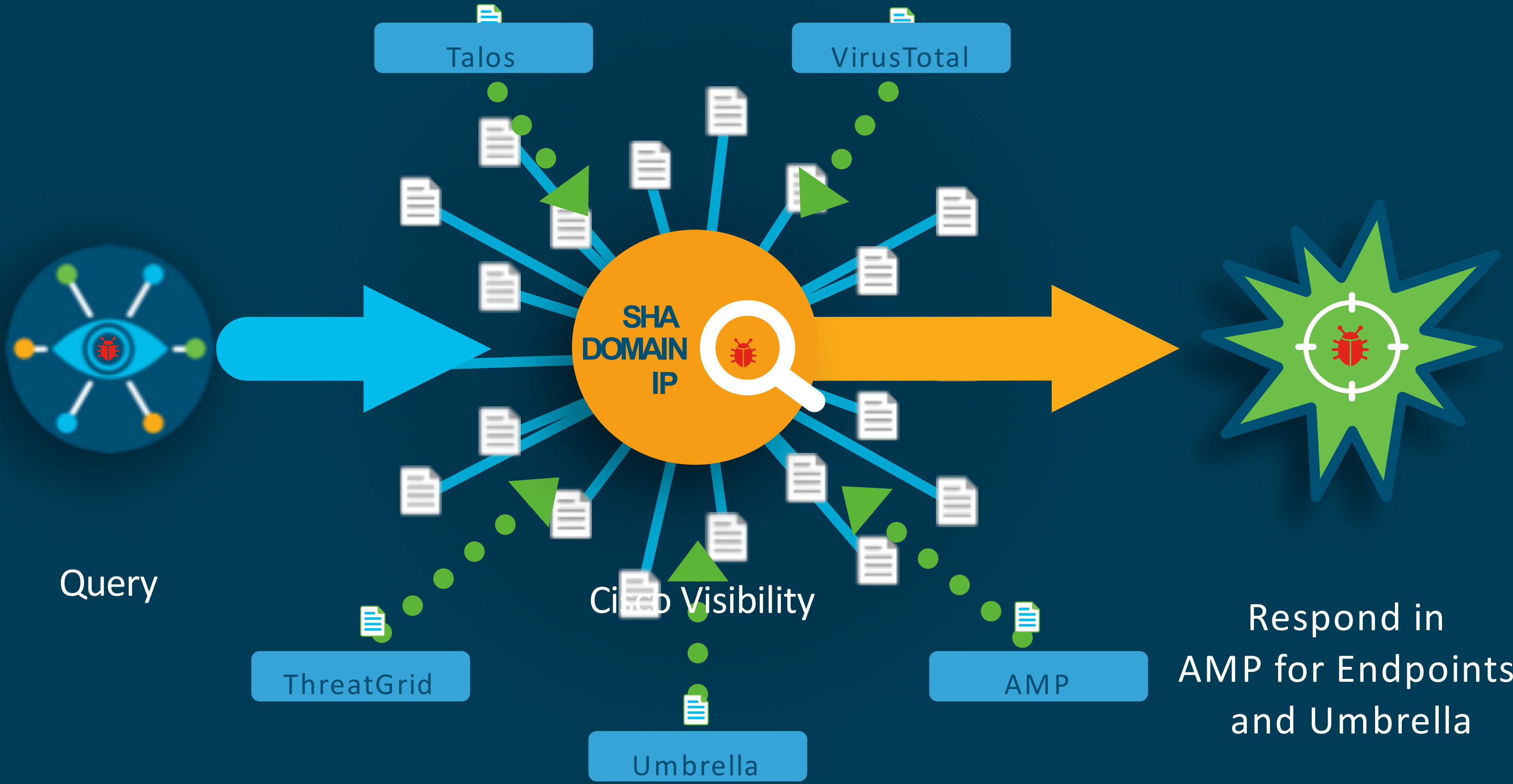
Better protection



Save time

Detect faster

Integrated Portfolio Security/Response



Talos

VirusTotal

SHA
DOMAIN
IP

Query

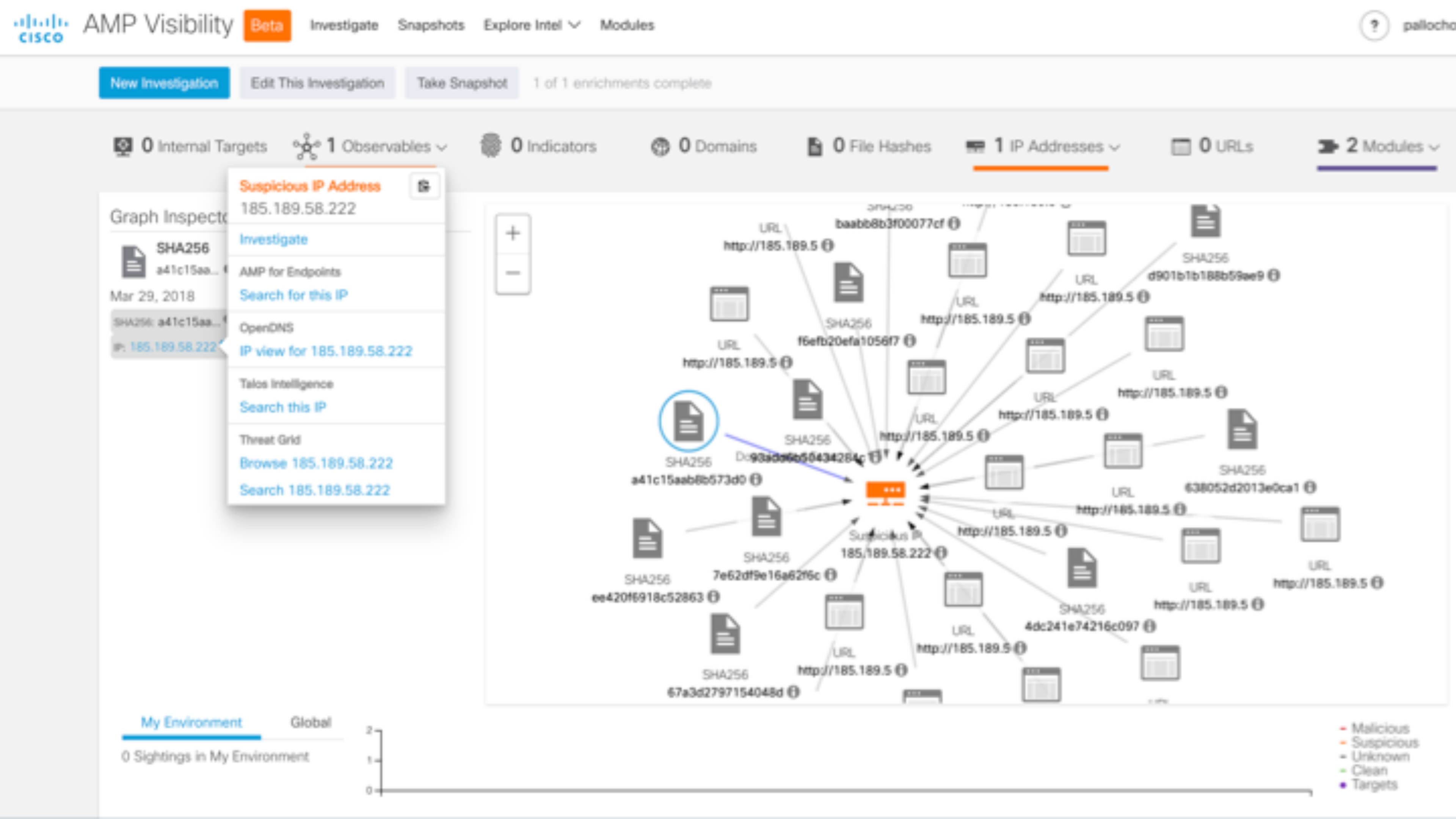
Cisco Visibility

ThreatGrid

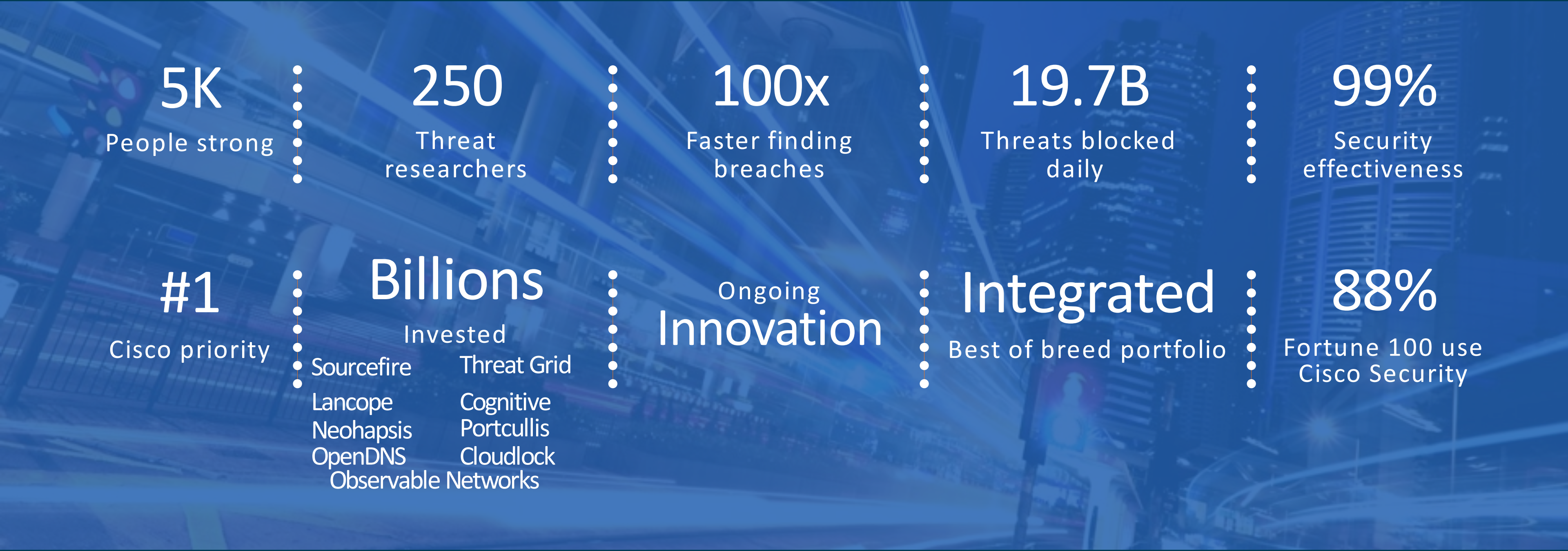
Umbrella

AMP

Respond in
AMP for Endpoints
and Umbrella


AMP Visibility
Beta
Investigate
Snapshots
Explore Intel
Modules
New Investigation
Edit This Investigation
Take Snapshot
1 of 1 enrichments complete
0 Internal Targets
1 Observables
0 Indicators
0 Domains
0 File Hashes
1 IP Addresses
0 URLs
2 Modules
Suspicious IP Address
185.189.58.222
Investigate
AMP for Endpoints
Search for this IP
OpenDNS
IP view for 185.189.58.222
Talos Intelligence
Search this IP
Threat Grid
Browse 185.189.58.222
Search 185.189.58.222
Graph Inspecto
SHA256
a41c15aa...
Mar 29, 2018
SHA256: a41c15aa...
IP: 185.189.58.222
SHA256
a41c15aab8b573d0
Suspicious IP
185.189.58.222
URL
http://185.189.5
SHA256
baabb8b3f00077cf
SHA256
f6efb20efa1056f7
SHA256
d901b1b188b59ae9
SHA256
638052d2013e0ca1
SHA256
7e62df9e16a62f6c
SHA256
ee420f6918c52863
SHA256
67a3d2797154048d
SHA256
4dc241e74216c097
My Environment
Global
0 Sightings in My Environment
2
1
0
Malicious
Suspicious
Unknown
Clean
Targets

Cisco Security commitment



5K
People strong

250
Threat researchers

100x
Faster finding breaches

19.7B
Threats blocked daily

99%
Security effectiveness

#1
Cisco priority

Billions
Invested

Sourcefire
Lancope
Neohapsis
OpenDNS

Threat Grid
Cognitive
Portcullis
Cloudlock

Observable Networks

Ongoing
Innovation

Integrated
Best of breed portfolio

88%
Fortune 100 use Cisco Security