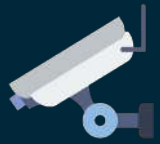
Building CSOC for the Biggest Airport in the World

Protecting Against the Riskiest 1% of Threats

Senad Aruc
Evangelist and Technical Lead. Northern Europe & Turkey.
Advanced Threats Group @ Cisco

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

5000 Servers



40K IOT Devices

15+ Event-Based Integrations

6500 Network Devices

750 IT Rooms

IT & IOT Service Topology

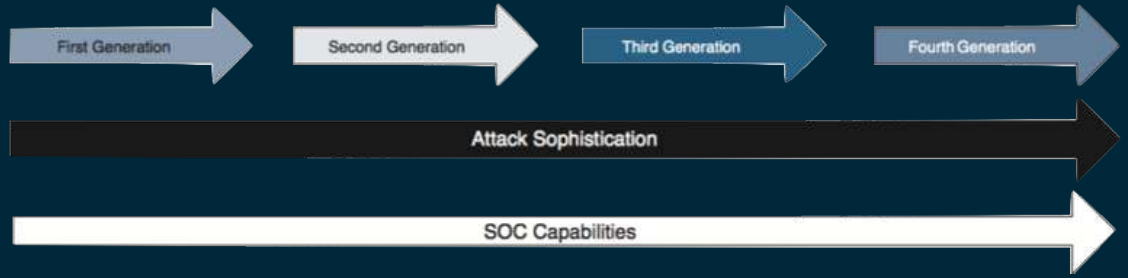
150K Metrics Monitored

100K Events/Hour

TIE III
3 Data Centers

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CSOC Generations



Full custom tailor-made next-gen CSOC design

Engineering

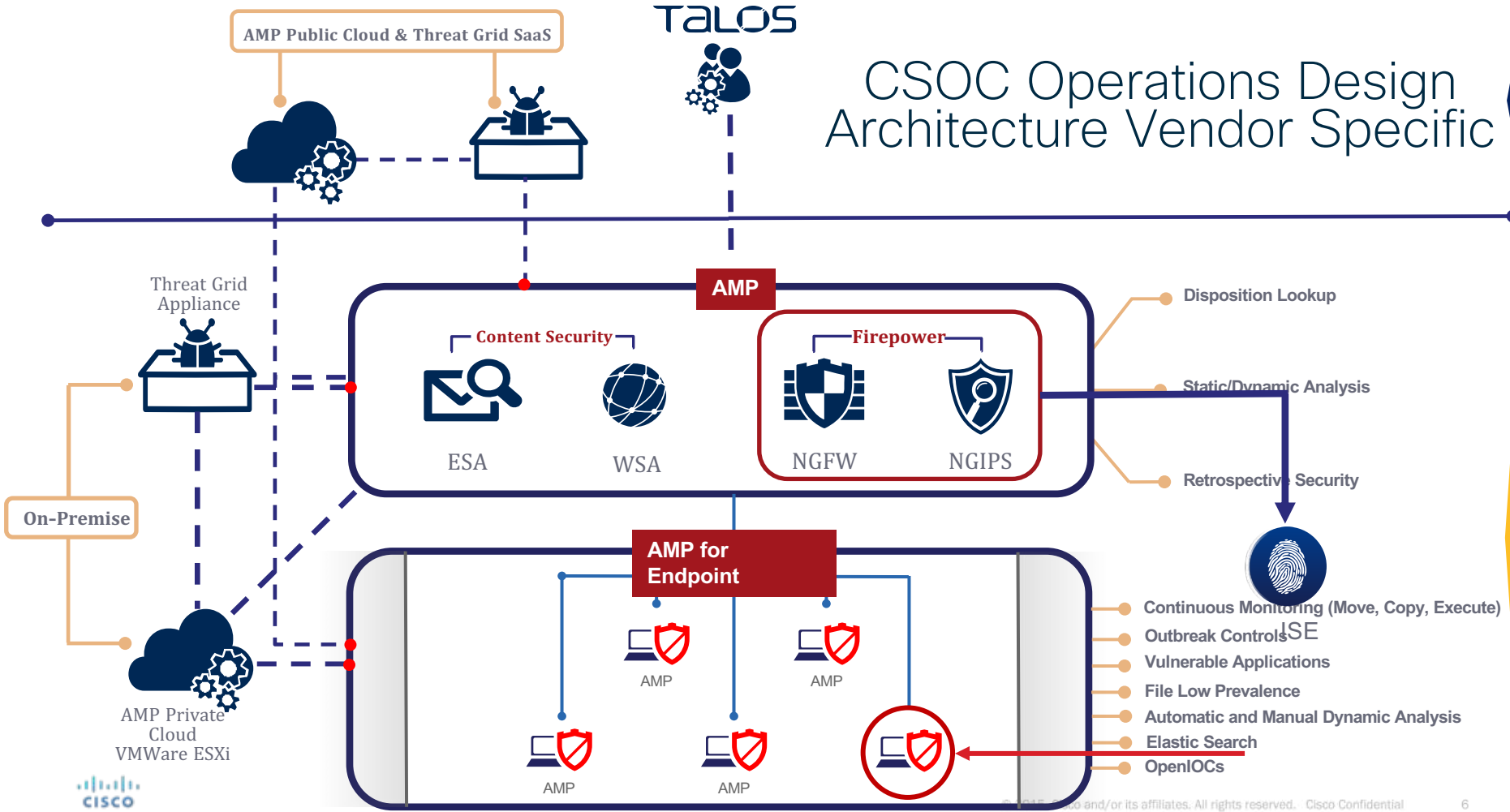
Operations

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

“The first thing you need to do at your CSOC is to separate the Engineering and Operation teams with clear definition of their responsibilities. Threat hunters or incident responder will be not so happy, if she/he is doing vulnerability scanning or patch management”

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CSOC Operations Design Architecture Vendor Specific

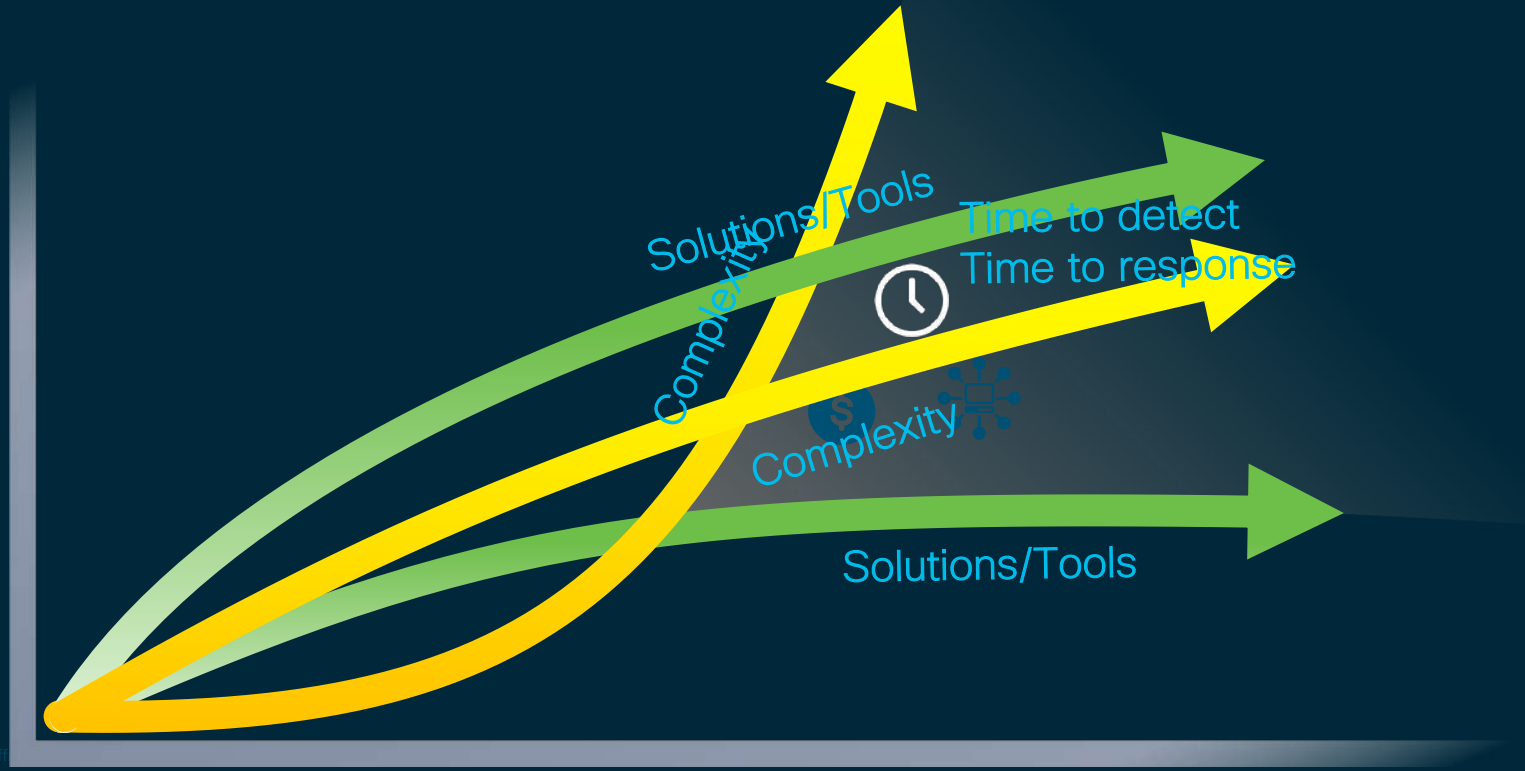


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CISCO TALOS

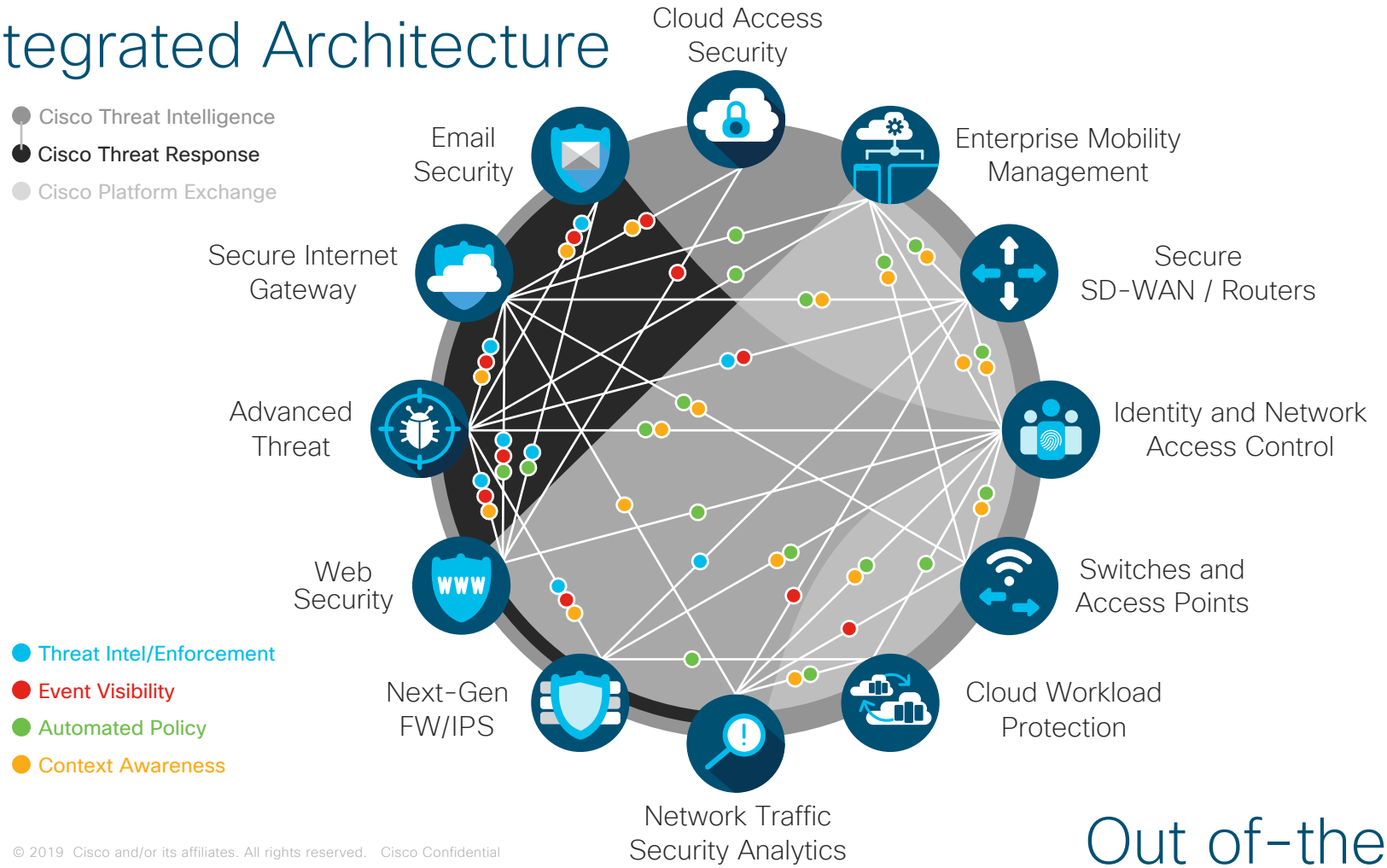
CUSTOMER SITE

The Security Effectiveness Gap



© 2019 Cisco and/or its aff

Integrated Architecture

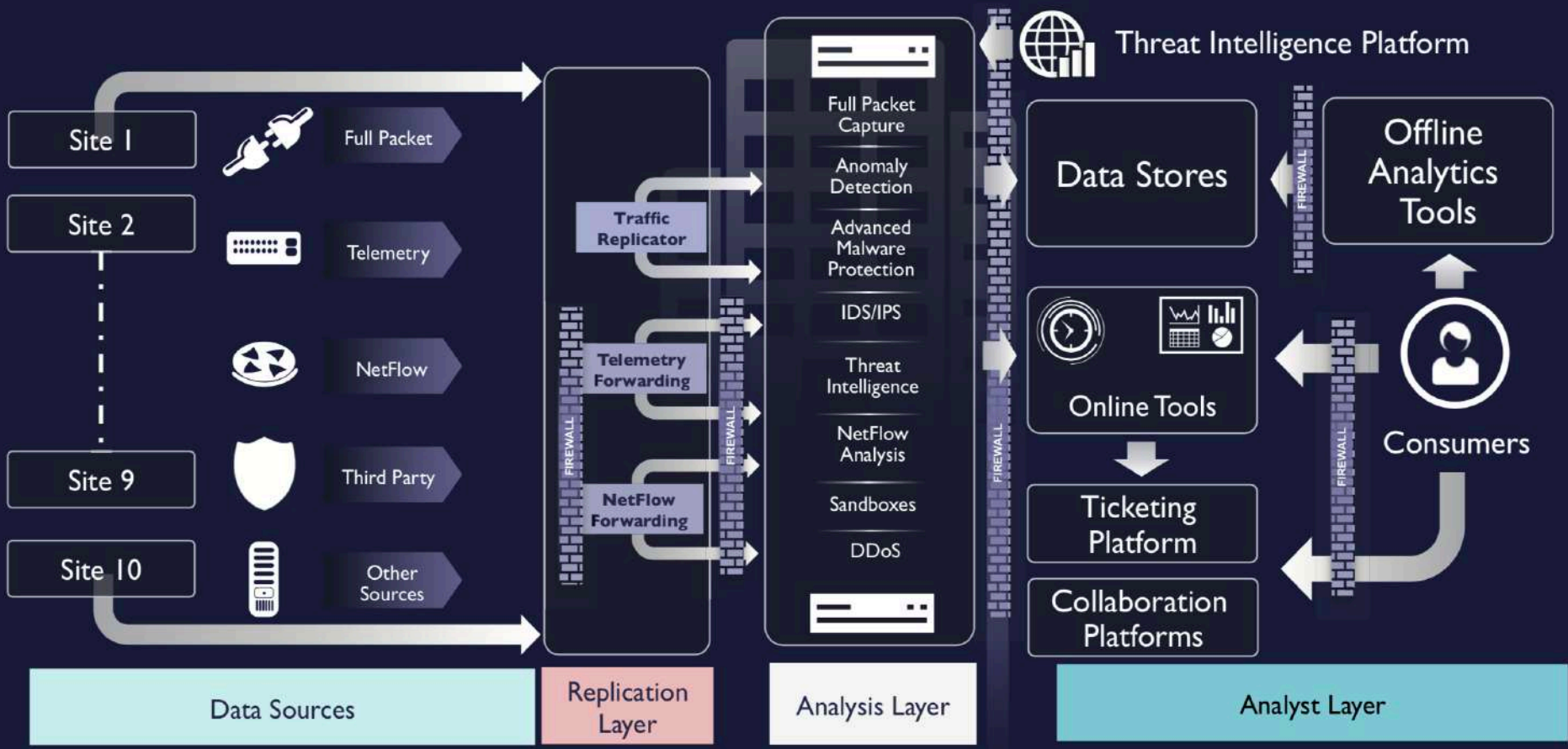


© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Out of-the box

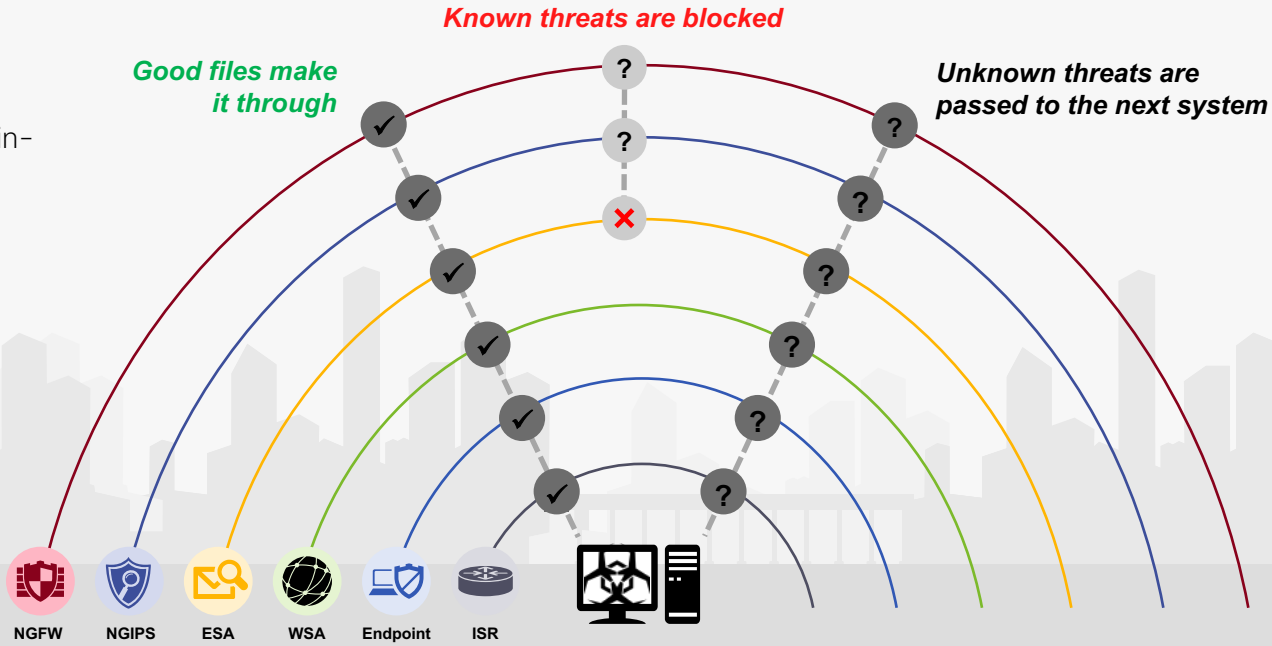
Example: Security Analytics for National Critical Infrastructure

CSOC Design Architecture



Why defense in-depth is BROKEN!

Current defense in-depth approach is built on binary detection



Single points of inspection have their limitations

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

“If we are still blaming the CSOC Operation teams (incident responders, threat hunters and malware/digital forensic) people for breaches. Then we are doing a big mistake, remember human cannot protect against the threats! Technology/machines can do this to some level. So go and blame your technology!”

“Protection = Machines where Detection Response = Humans”

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Preventing Malware Attacks is **Ideal**

But What Happens if One is **Missed**?

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Most Security Solutions Block **99%** of Threats

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

But what about the **1%** of threats you are missing?

© 2019 Cisco and/or its affiliates. All rights reserved · Cisco Confidential

The **Most Dangerous 1%** of Threats **Try to Hide**

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Using Advanced Evasion Techniques

- Fileless malware
- Environmentally-aware malware
- Polymorphism
- Exploit legitimate processes

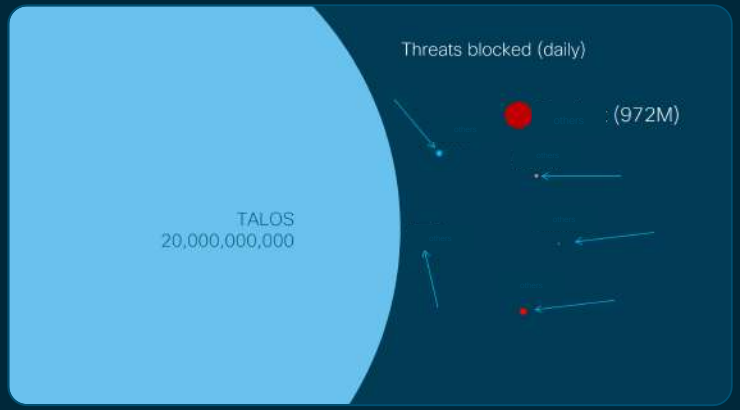
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Finding Them Is **Not Easy**

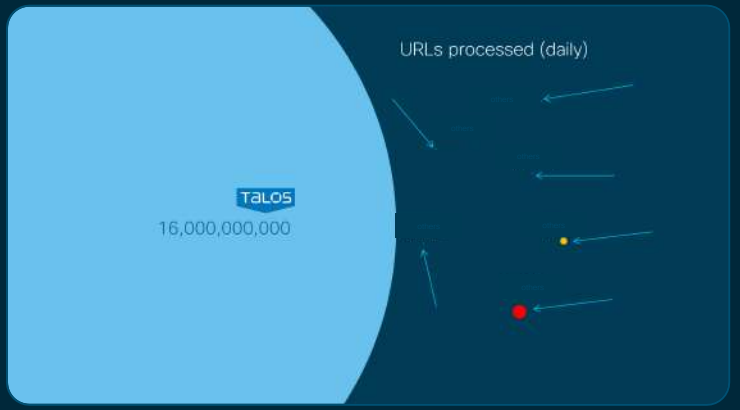
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

But how much is the 1% of threats you are missing?

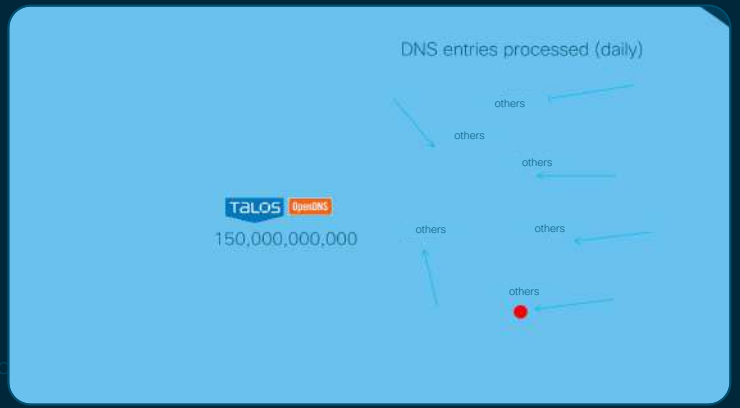
THREATS BLOCKED



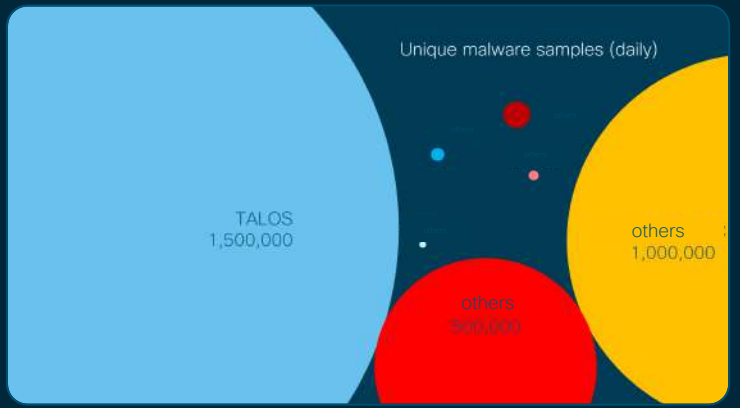
URLS PROCESSED



DNS ENTRIES PROCESSED



UNIQUE MALWARE SAMPLES



© 2019 C

It Takes a **Whole Lot of Time**

Security Analyst

- Large scale alerts
- Flood of false positives
- Lots of tools & tedious tasks

Incident Responder

- Sifting through disparate data
- Lack of contextual info
- Gather/present evidence

IT Security Director

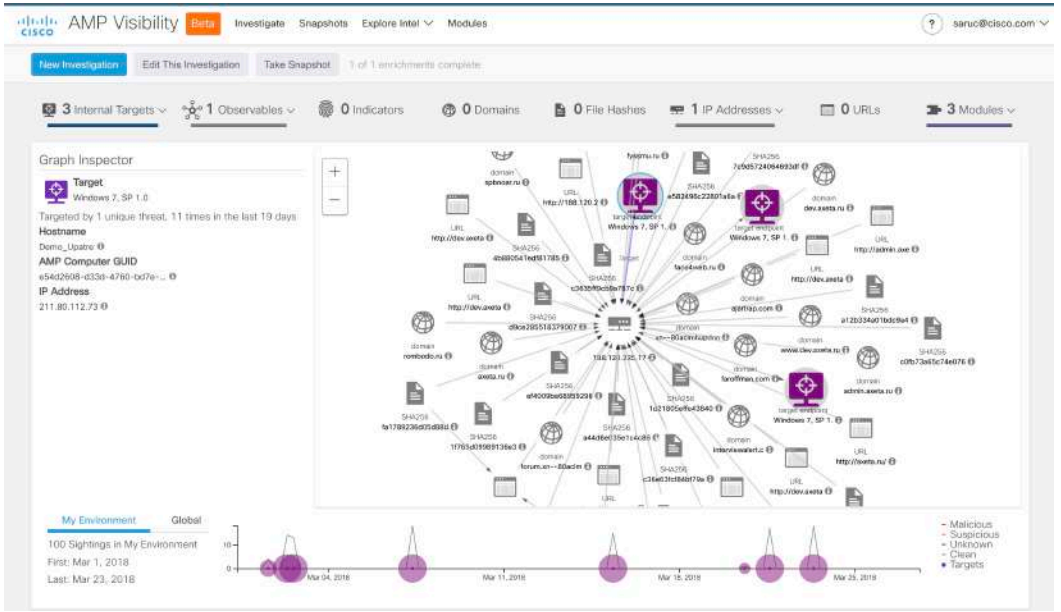
- Budget & staffing constraints
- IP/asset protection
- Technology integration

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Automation & Orchestration

Key Issues at modern CSOC's: Excessive Alerts, Outdated Metrics, and Limited Integration Lead to Over-taxed SOCs

Figure 4: Most SOC analysts can only handle between 7-8 investigations in a day



Take Back Control of **Time**

Respond to incidents in
Hours not days or months

Proactively Hunt for the
riskiest 1% of threats

Find and fix the most vulnerable
endpoints before compromise

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Giving You **Time**

Focus on the Riskiest 1% of Threats

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

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Stop Malware

Using multiple detection and protection mechanisms

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What to have..

Prevent

- Antivirus
- Fileless malware detection
- Cloud lookups (1:1, 1:many)
- Client Indicators of Compromise

Detect

- Static analysis
- Sandboxing
- Malicious Activity Protection
- Machine learning
- Device flow correlation
- Cloud Indicators of Compromise

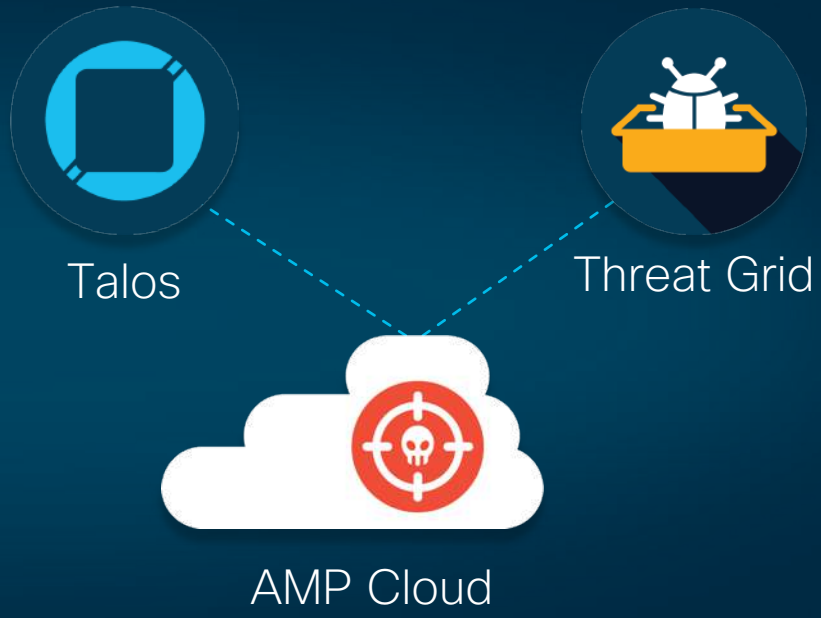
Reduce Risk

- Vulnerable software
- Low prevalence
- Proxy log analysis

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cloud-based Analysis and Threat Intelligence

AMP cloud constantly updated with the latest threat intelligence and research to protect against advanced threats.



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Prevent Fileless Malware

Malware Has Evolved. We Need to Protect Against More than Just Files.

Monitor process activity and guard against attempts to hijack legitimate applications.

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Protect Against Ransomware

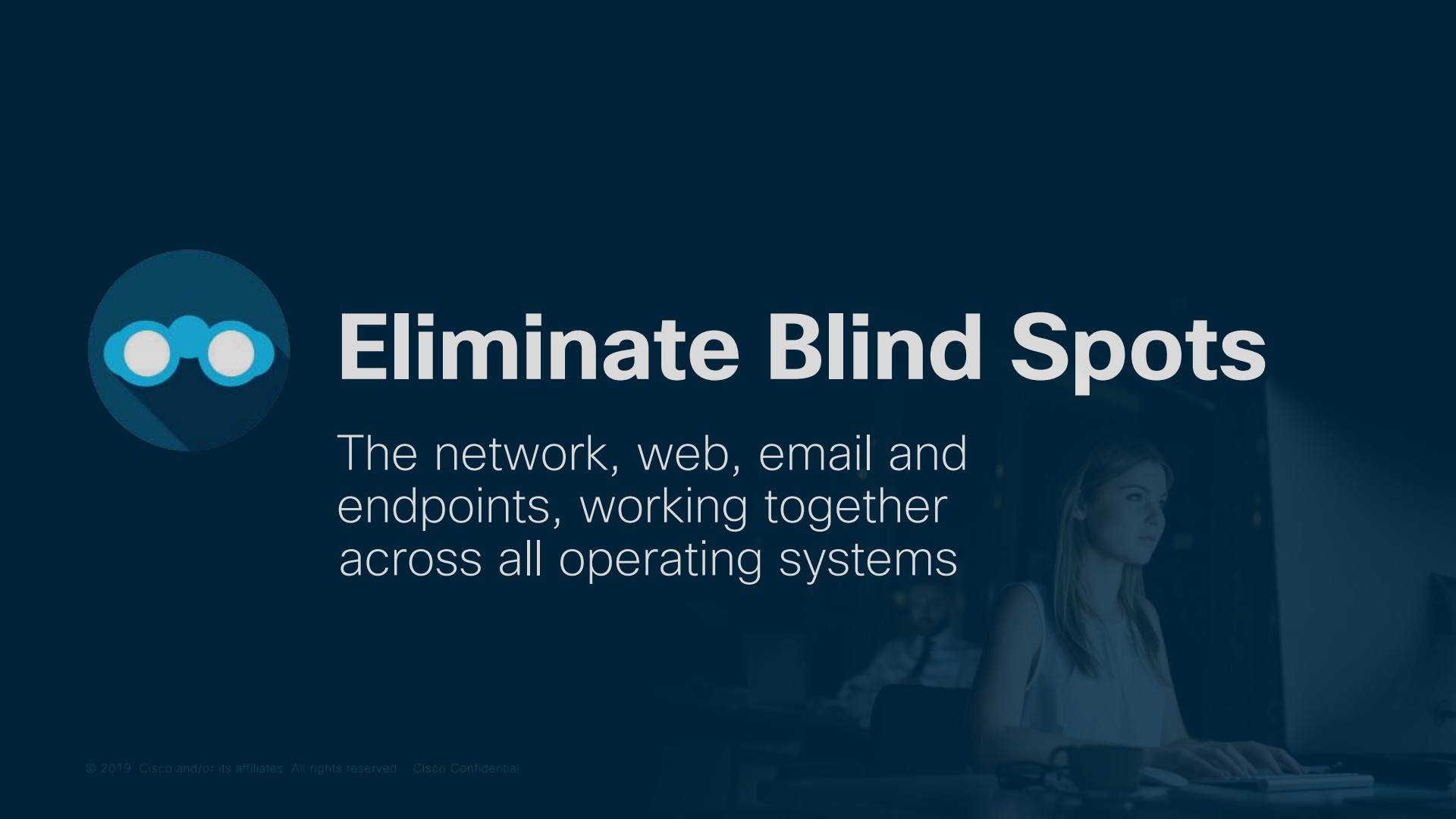
Malicious Activity Protection

- Monitor Process behavior at execution
- Tuned to detect tell-tale ransomware signs
- Quarantine and terminate associated files and processes
- Log and alert encryption attempt

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Eliminate Blind Spots

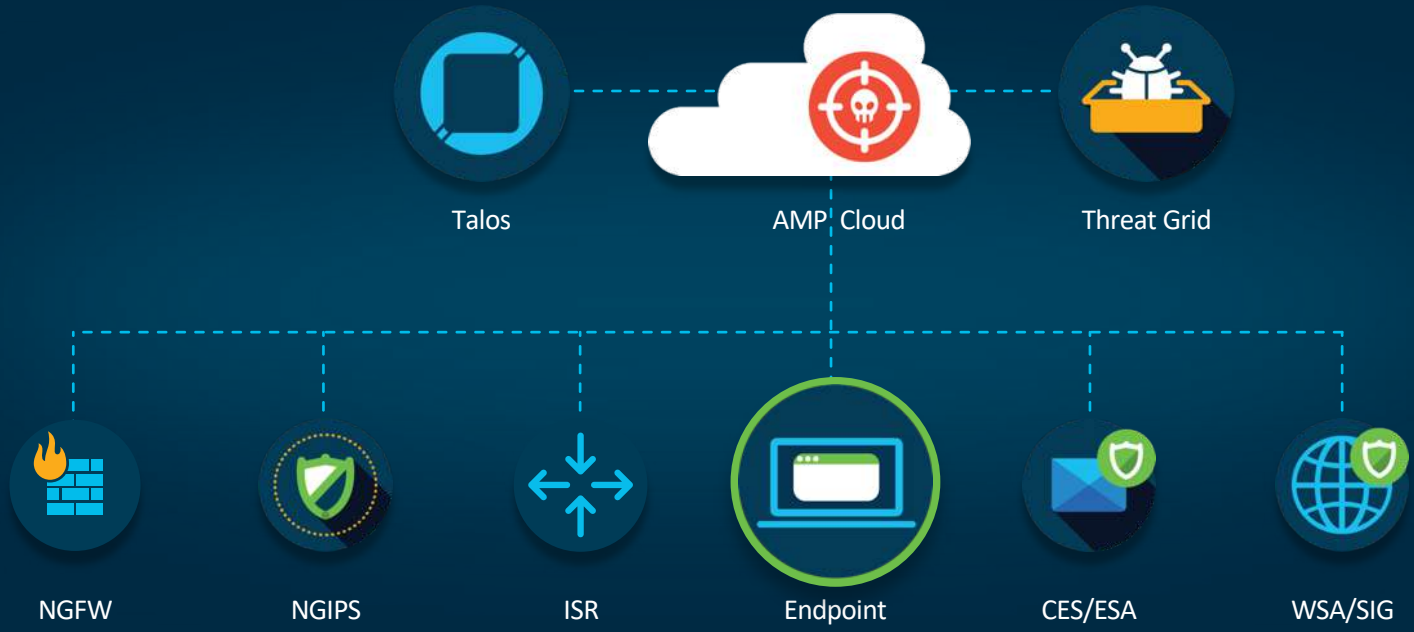
The network, web, email and endpoints, working together across all operating systems



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

See Once, Block Everywhere

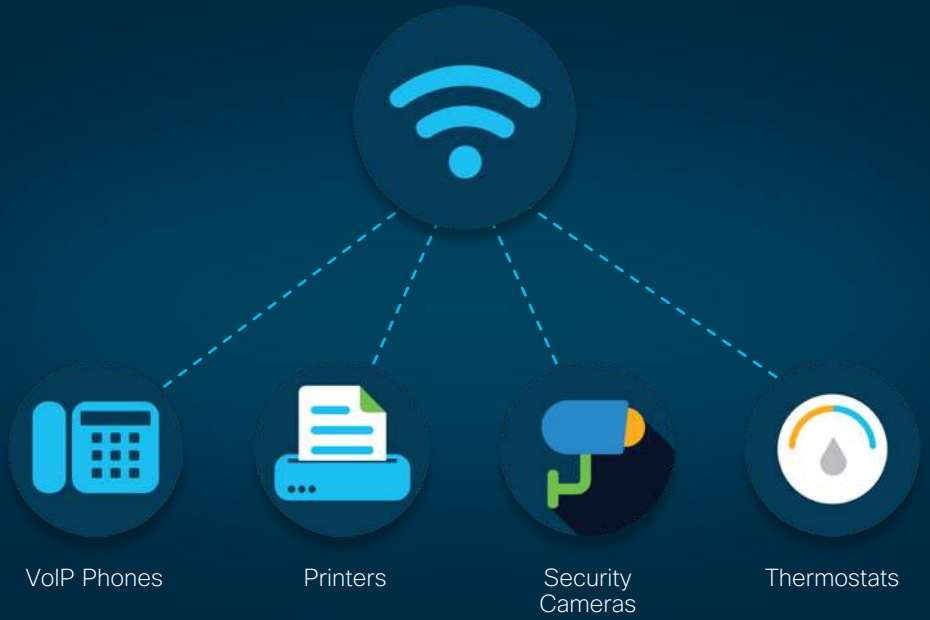
Share intelligence across network, web, email, and endpoints to see once, block everywhere.



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Agentless Detection with Proxy Analysis

Identify Anomalous Traffic Occurring Within Your Network



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

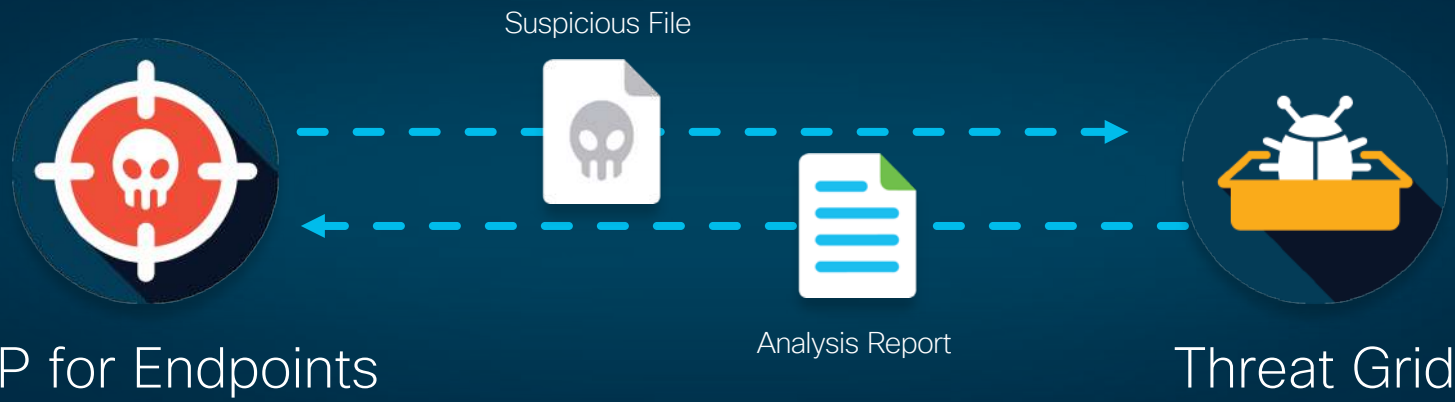
Discover Unknown Threats

With proactive threat hunting

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Dynamic and Behavioral Analysis with Sandboxing

Execute, analyze, and test malware behavior in order to discover previously unknown zero-day threats



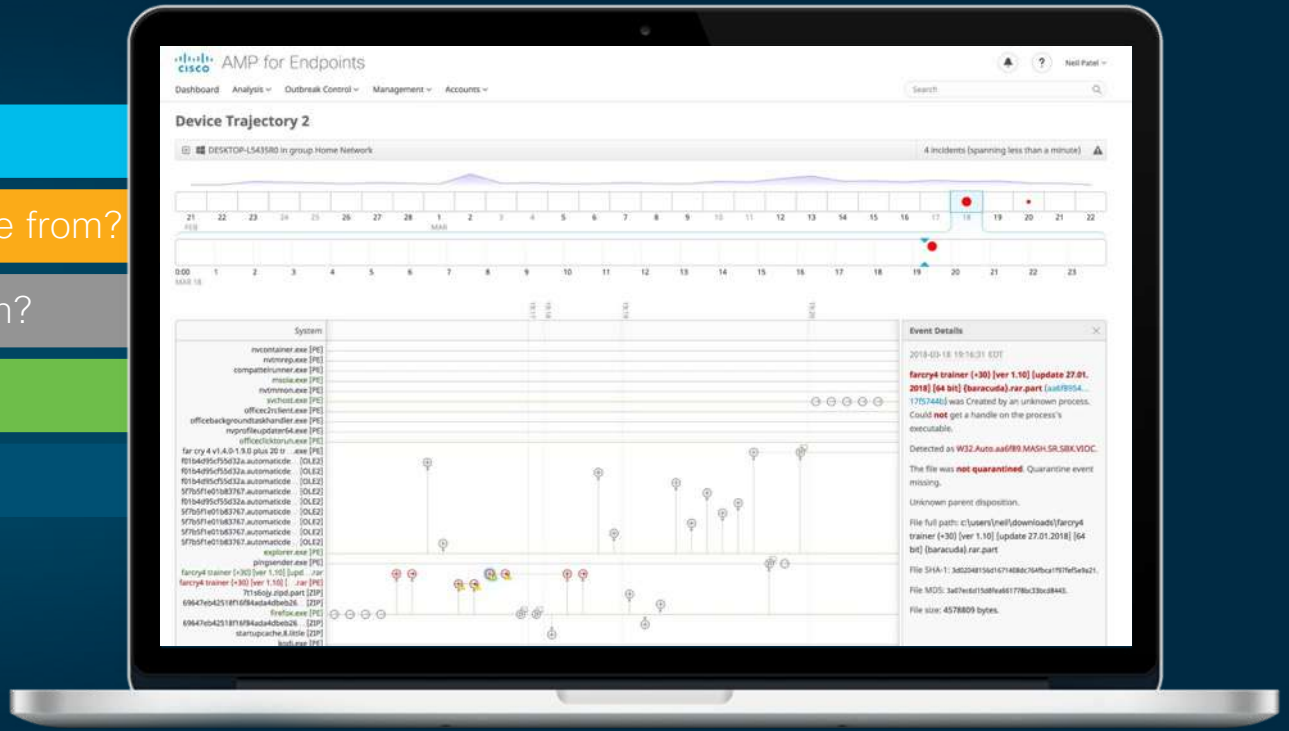
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

“How your expensive security solutions with expensive Threat Intelligence service can protect you from a "document.doc" with "macros enabled" that I just created? Threat intelligence will not protect you against zero-day malware and targeted attacks”

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Capability to Continuous Monitoring

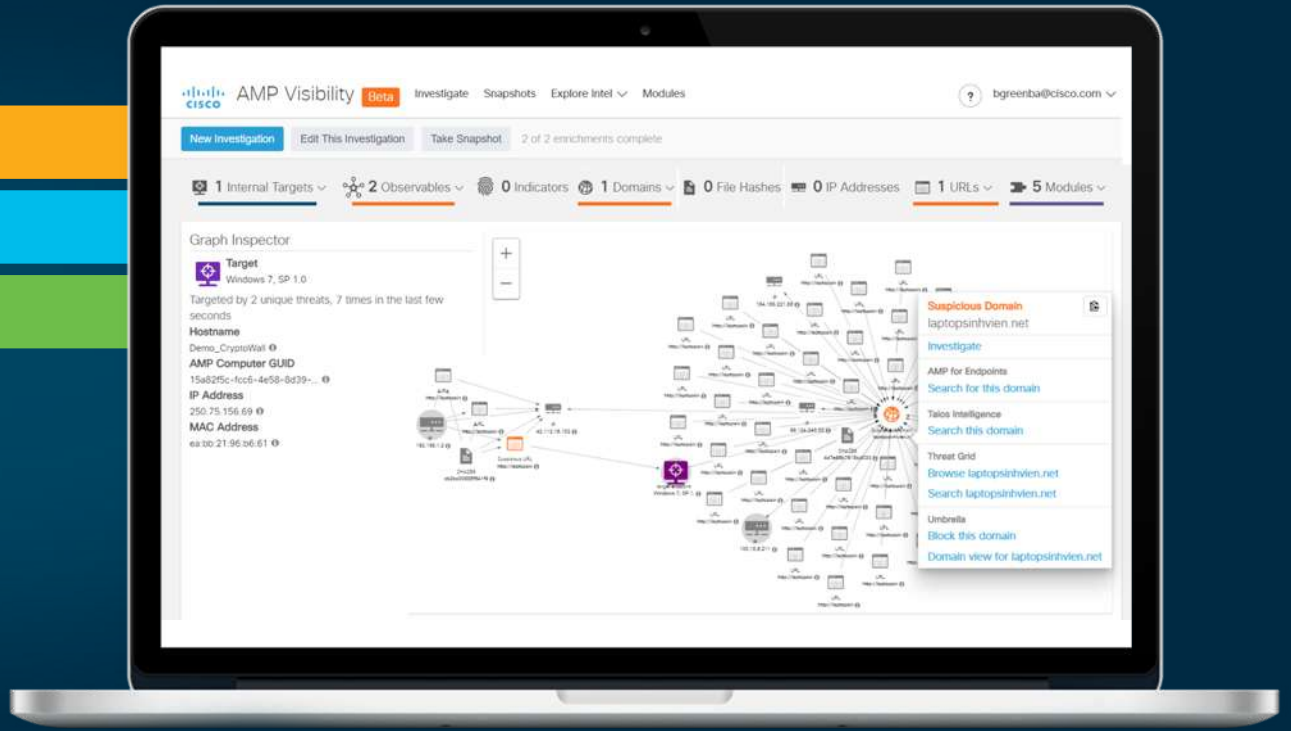
- What happened?
- Where did the malware come from?
- Where has the malware been?
- What is it doing?
- How do we stop it?



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Capability to Perform In-depth Investigations

- Threat Hunting
- One Click Remediation
- Intelligence Correlation



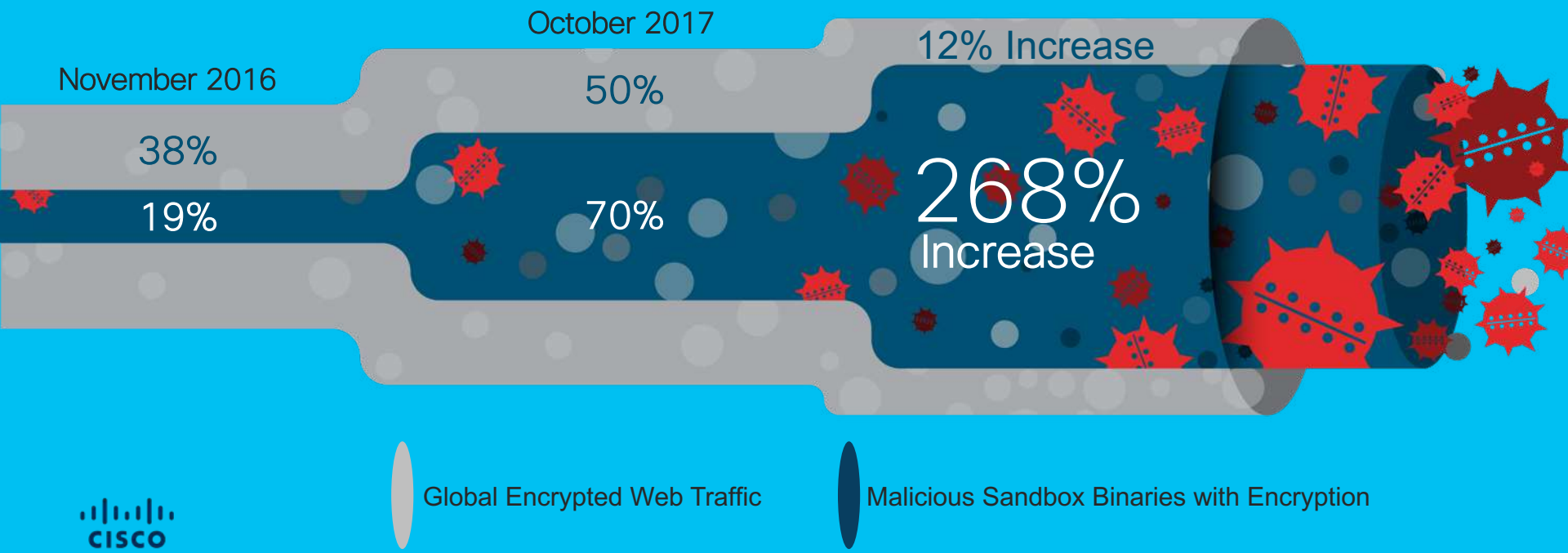
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Why endpoints is in focus… again?

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Malicious Binaries and Encryption

Attackers embrace encryption to conceal their command-and-control activity



cisco

If You Can Only Get ONE Tool

- Many organizations can get *one* tool to start.
- Which one?
- How to decide?

If you need to start hunting ASAP, the first tool to get is an endpoint focused tool (**EDR** or its open source equivalents), because **"endpoints is where the attackers are"**

EDR allows you to review the most unambiguous attacker traces:
Execution, file actions, downloads, system actions, etc.

Gartner

 © 2018 Gartner, Inc. and/or it affiliates. All rights reserved.

AMP for Endpoints

Prevent attacks and block malware in real time

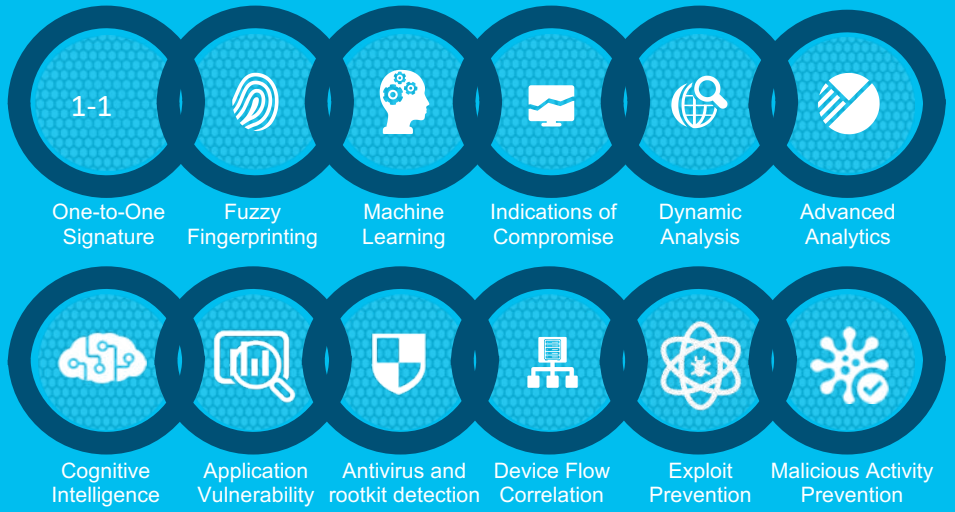
Continuously monitor all processes and activity

Accelerate investigations and remediate faster

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What is AMP for Endpoints?

Point-in-Time Detection – Plan A



All Prevention < 100%

Retrospective Security Plan B

Unique to AMP - Continuous Analysis & Retrospective Security

Cisco AMP

AMP **blocks** threats, but it trusts nothing

Hunting inside your environment

Continually exposing and **blocking**

Alerting via an **interactive, actionable history of events** that accelerates incident response

So AMP **records** events

And **continuously analyzes** each recorded event, testing it against the latest global threat intelligence

AMP **does the heavy lifting** that the IT team used to struggle with, **recapturing** 1,000s of hours each year

Demo time..

Thanks
Q/A

saruc@cisco.com


Senad Aruc


@senadaruc