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

iGA

5000 Servers

40K IOT Devices

15+ Event-Based Integrations

6500 Network Devices

750 IT Rooms

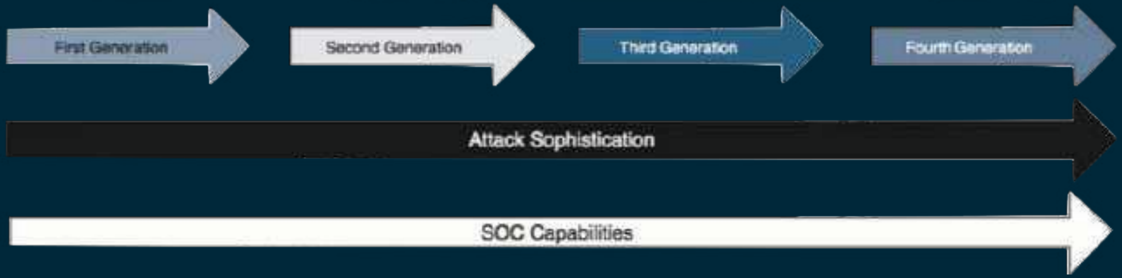
IT & IOT Service Topology

150K Metrics Monitored

100K Events/Hour

TIE III
3 Data Centers

CSOC Generations



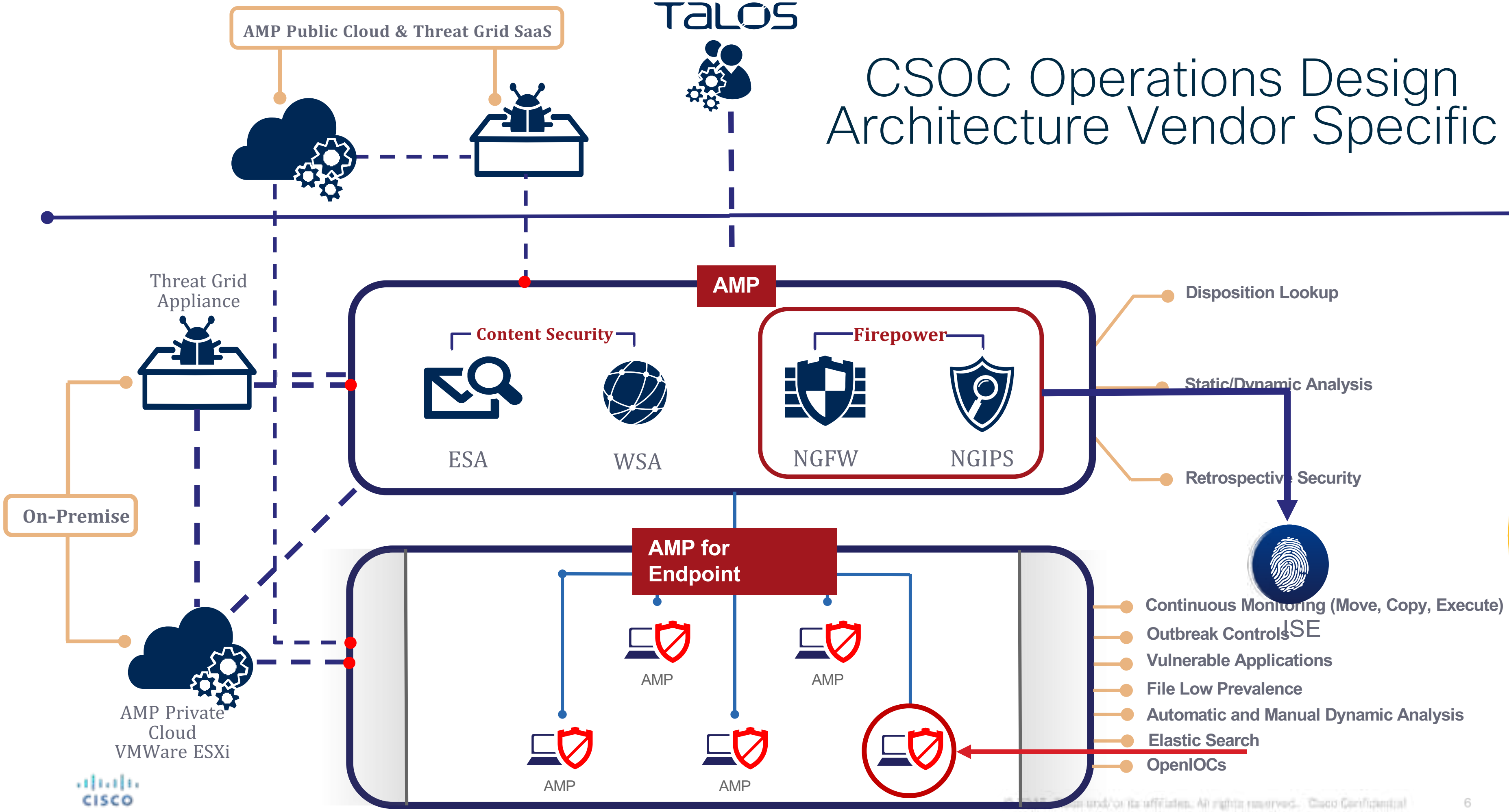
Full custom tailor-made next-gen CSOC design

Engineering

Operations

“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”

CSOC Operations Design Architecture Vendor Specific



AMP Public Cloud & Threat Grid SaaS

TALOS

Threat Grid Appliance

On-Premise

AMP Private Cloud VMWare ESXi

AMP

Content Security

ESA

WSA

Firepower

NGFW

NGIPS

- Disposition Lookup
- Static/Dynamic Analysis
- Retrospective Security

ISE

AMP for Endpoint

AMP

AMP

AMP

AMP

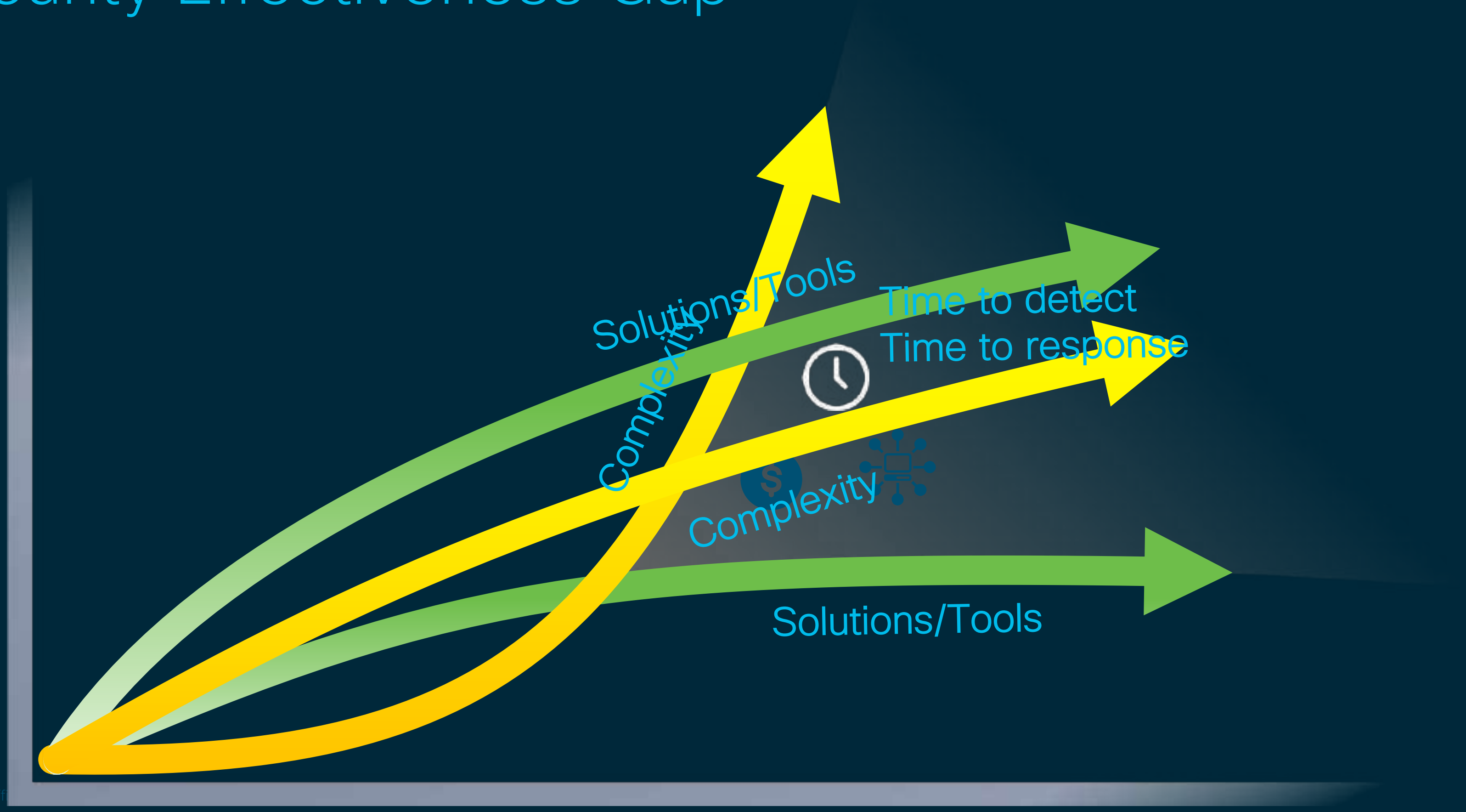
- Continuous Monitoring (Move, Copy, Execute)
- Outbreak Controls
- Vulnerable Applications
- File Low Prevalence
- Automatic and Manual Dynamic Analysis
- Elastic Search
- OpenIOCs

Windows, Mac OSX, Linux RedHat/CentOS, Android, iOS

CISCO TALOS

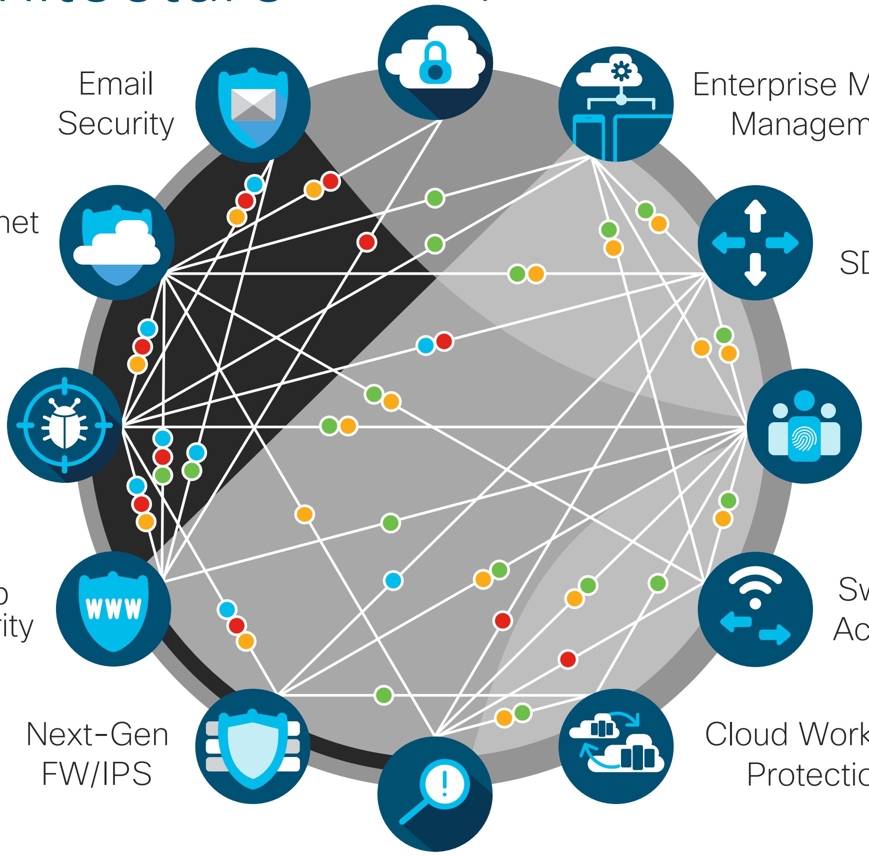
CUSTOMER SITE

The Security Effectiveness Gap



Integrated Architecture

● Cisco Threat Intelligence
● Cisco Threat Response
● Cisco Platform Exchange



Cloud Access Security

Enterprise Mobility Management

Secure SD-WAN / Routers

Identity and Network Access Control

Switches and Access Points

Cloud Workload Protection

Network Traffic Security Analytics

Next-Gen FW/IPS

Web Security

Advanced Threat

Secure Internet Gateway

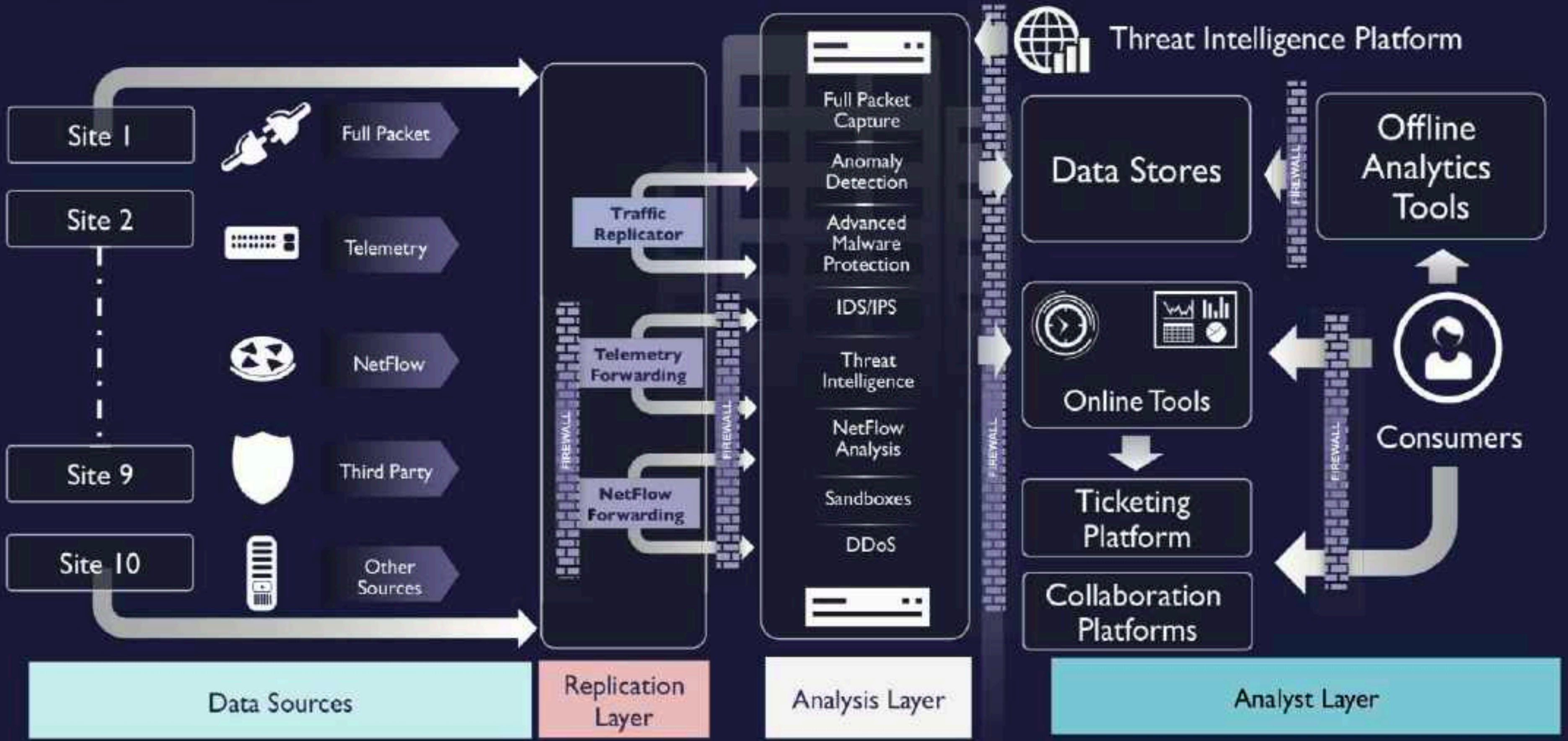
Email Security

● Threat Intel/Enforcement
● Event Visibility
● Automated Policy
● Context Awareness

Out of-the box

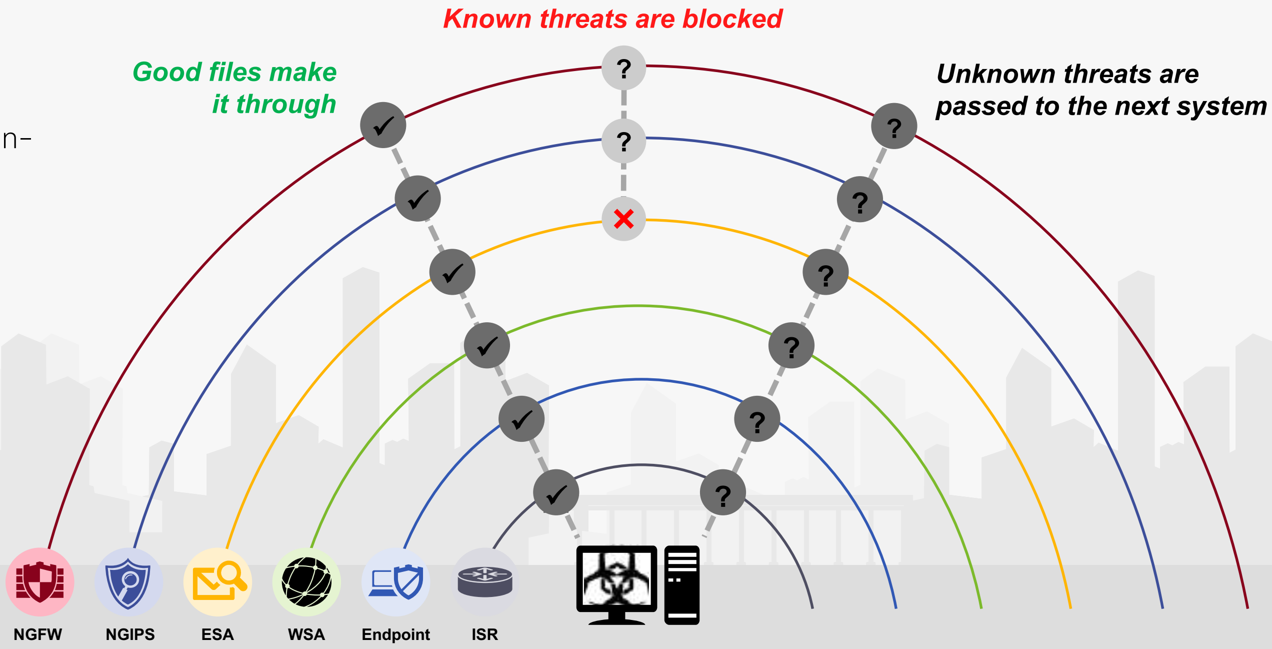
Example: Security Analytics for National Critical Infrastructure

CSOC Design Architecture



Why defense in-depth is BROKEN!

Current defense in-depth approach is built on binary detection



Known threats are blocked

Good files make it through

Unknown threats are passed to the next system

Single points of inspection have their limitations

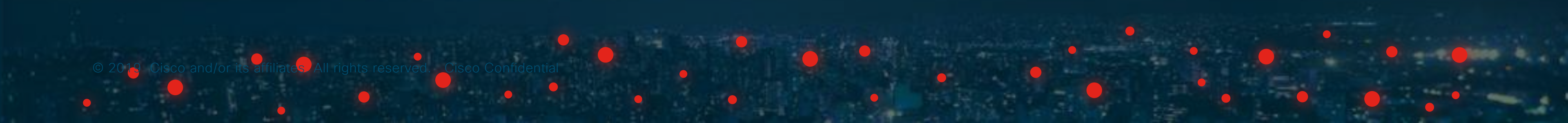
“If we are still blaming the CSOC Operation teams (incident responders, threat hunters and malware/digital forensic) people for breaches. Then we are doing a big mistake, remember human cannot protect against the threats! Technology/machines can do this to some level. So go and blame your technology!”

“Protection = Machines where Detection Response = Humans”

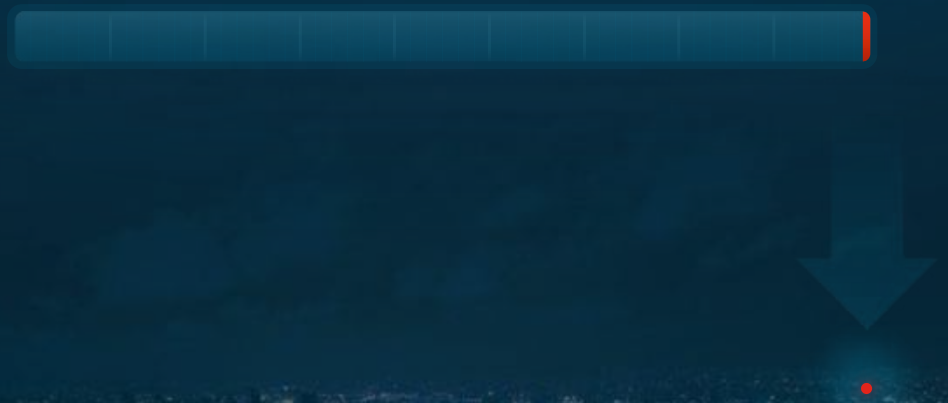
Preventing Malware Attacks is **Ideal**

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

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



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



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

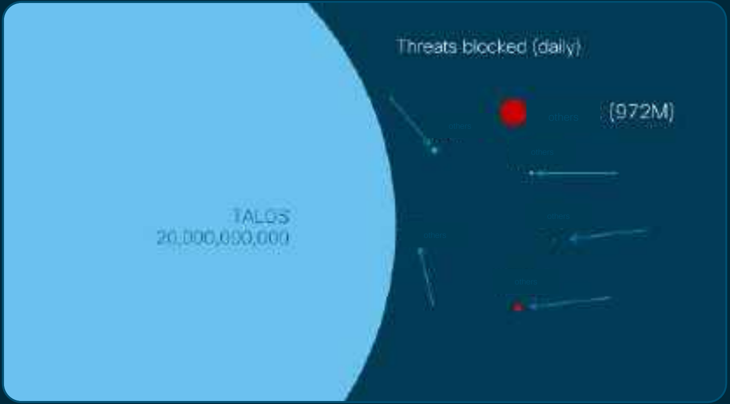
Using Advanced Evasion Techniques

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

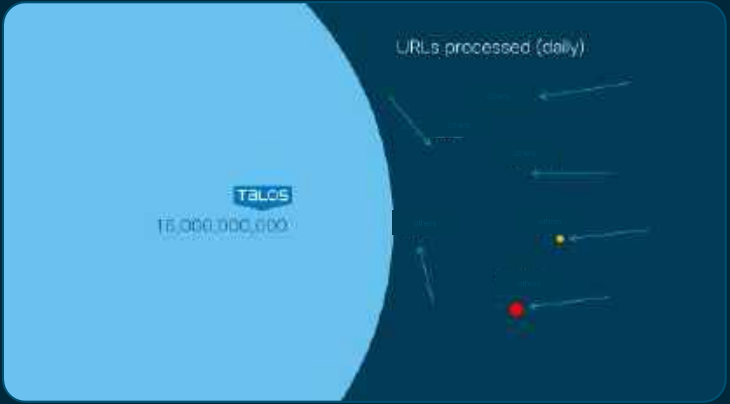
Finding Them Is **Not Easy**

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

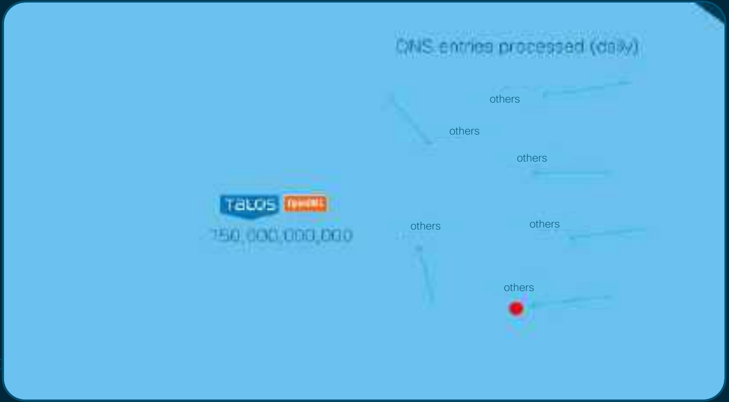
THREATS BLOCKED



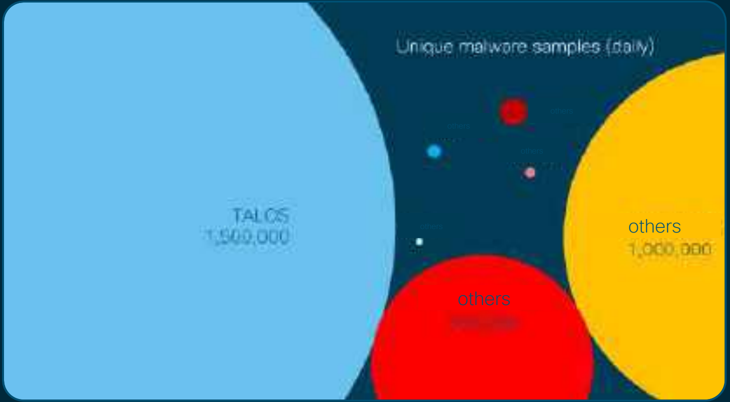
URLS PROCESSED



DNS ENTRIES PROCESSED



UNIQUE MALWARE SAMPLES



It Takes a **Whole Lot of Time**

Security Analyst

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

Incident Responder

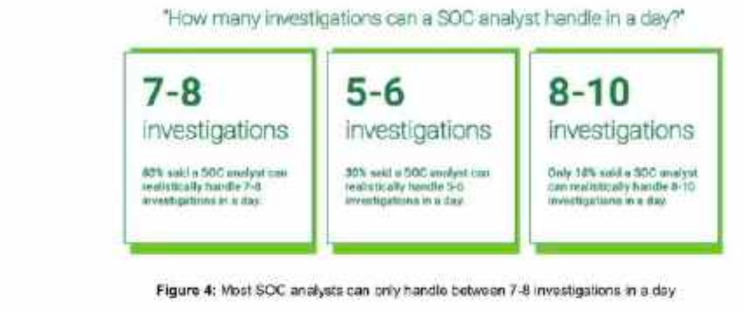
- Sifting through disparate data
- Lack of contextual info
- Gather/present evidence

IT Security Director

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

Automation & Orchestration

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



"How many investigations can a SOC analyst handle in a day?"

7-8 investigations

80% said a SOC analyst can realistically handle 7-8 investigations in a day.

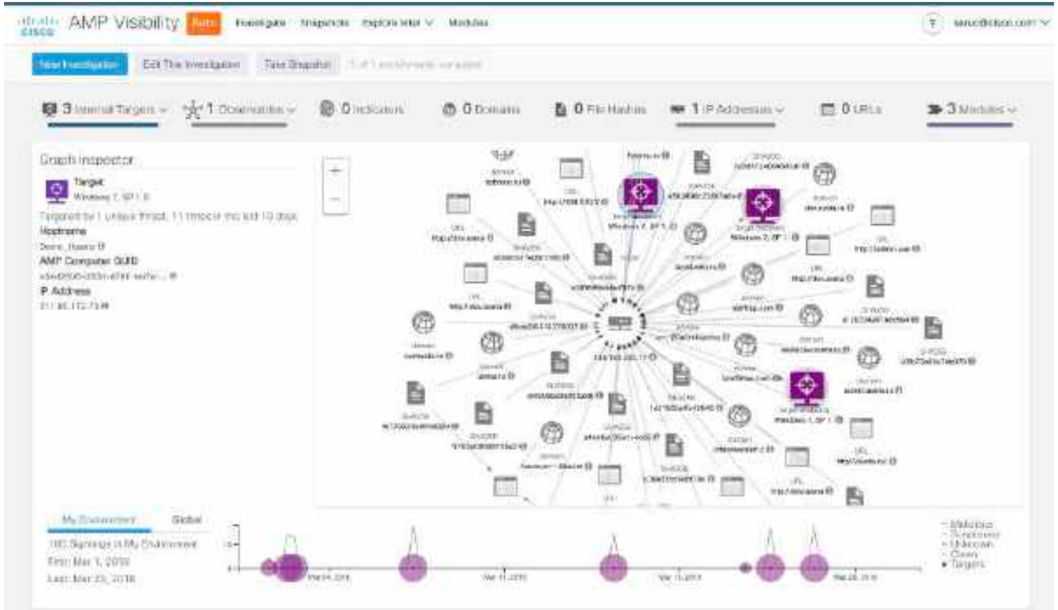
5-6 investigations

30% said a SOC analyst can realistically handle 5-6 investigations in a day.

8-10 investigations

Only 14% said a SOC analyst can realistically handle 8-10 investigations in a day.

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

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

Stop Malware

Using multiple detection and protection mechanisms

What to have..

Prevent

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

Detect

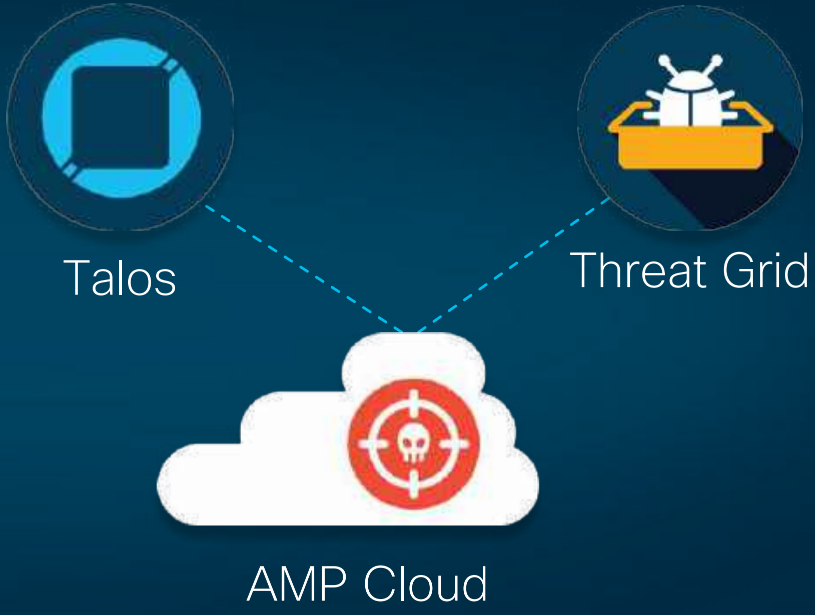
- Static analysis
- Sandboxing
- Malicious Activity Protection
- Machine learning
- Device flow correlation
- Cloud Indicators of Compromise

Reduce Risk

- Vulnerable software
- Low prevalence
- Proxy log analysis

Cloud-based Analysis and Threat Intelligence

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



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.

Protect Against Ransomware

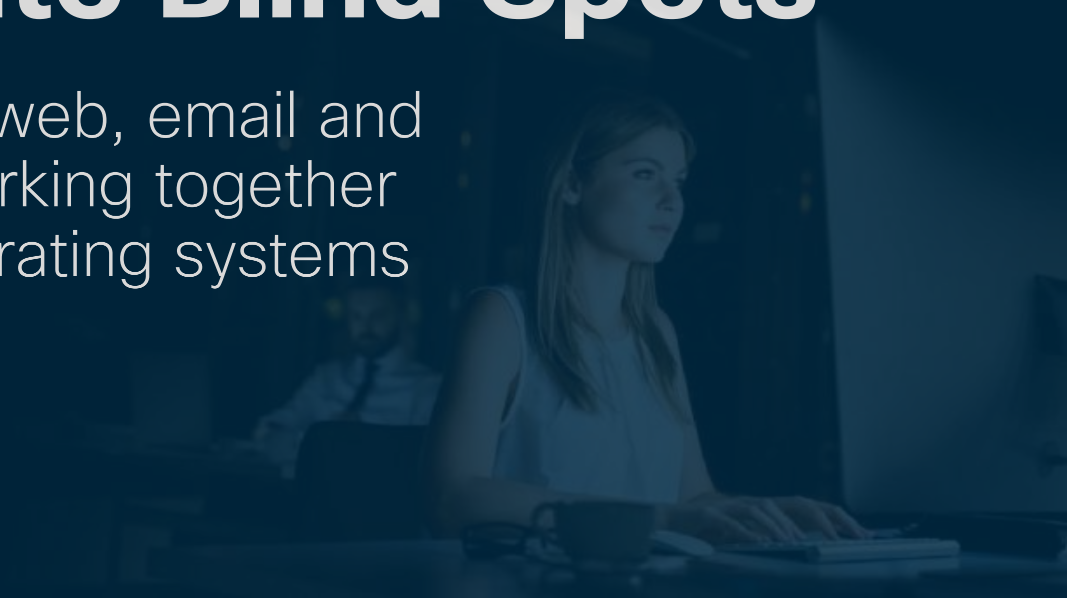
Malicious Activity Protection

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

Ooops, your files have been encrypted!
What Happened to My Computer?
02:23:57:37
05:23:57:37
bitcoin
Check Payment
Decrypt

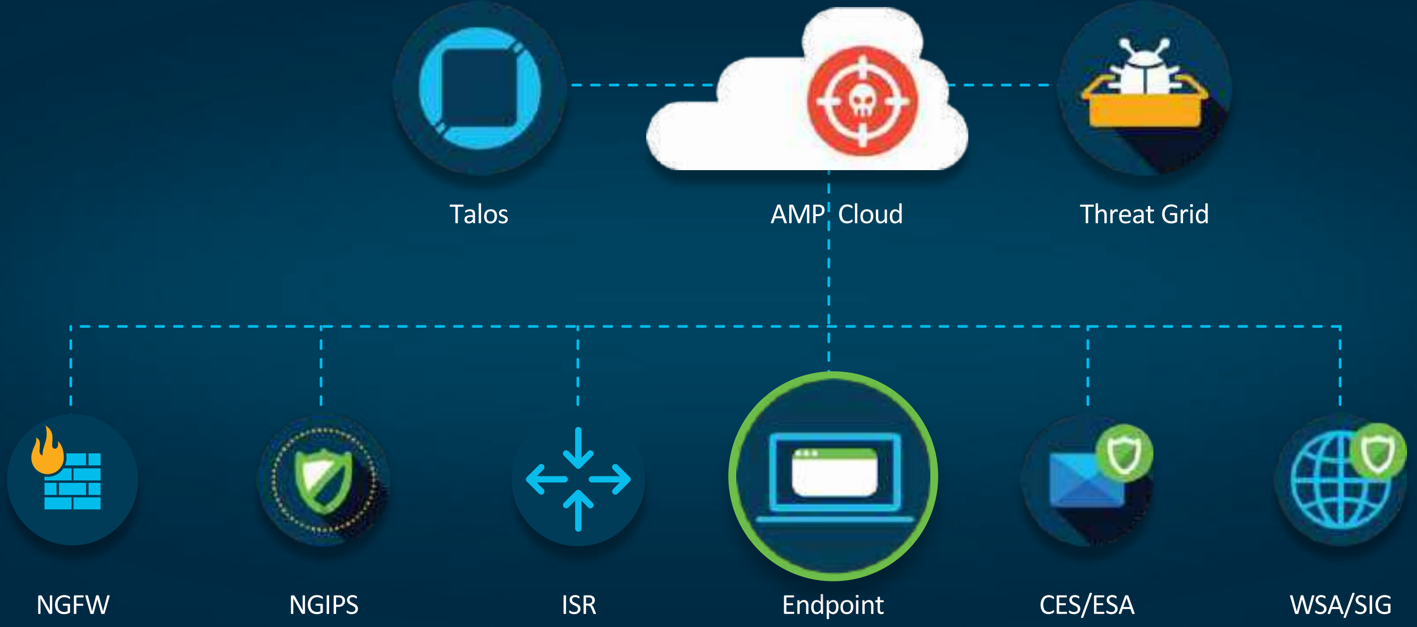
Eliminate Blind Spots

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



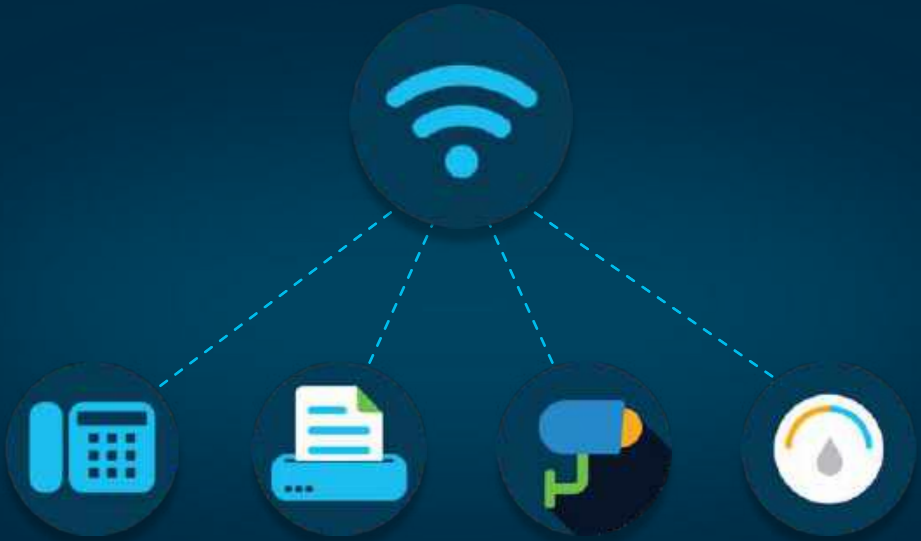
See Once, Block Everywhere

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



Agentless Detection with Proxy Analysis

Identify Anomalous Traffic Occurring Within Your Network



VoIP Phones

Printers

Security Cameras

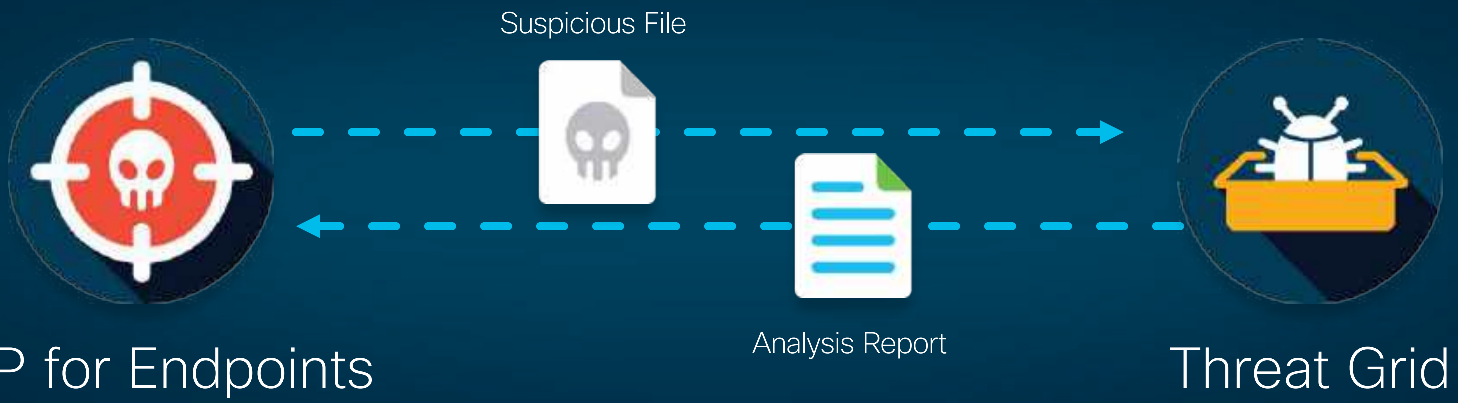
Thermostats

Discover Unknown Threats

With proactive threat hunting

Dynamic and Behavioral Analysis with Sandboxing

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



Suspicious File

AMP for Endpoints

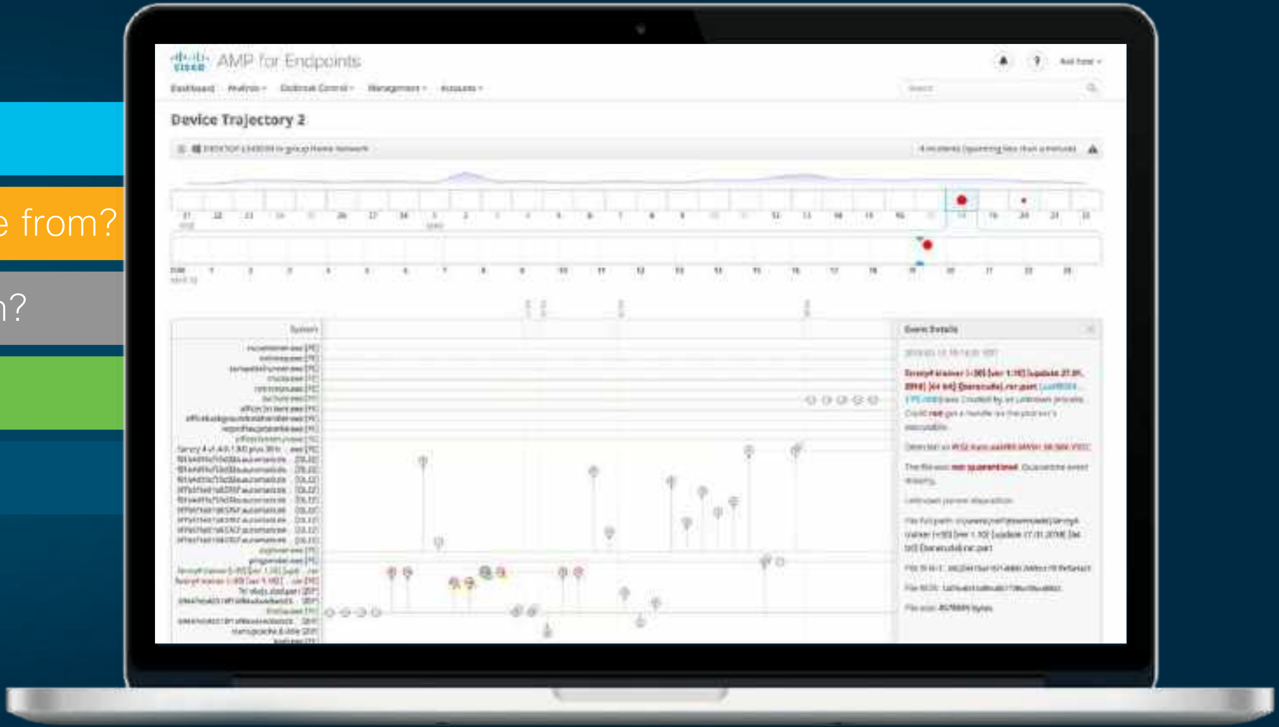
Analysis Report

Threat Grid

“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”

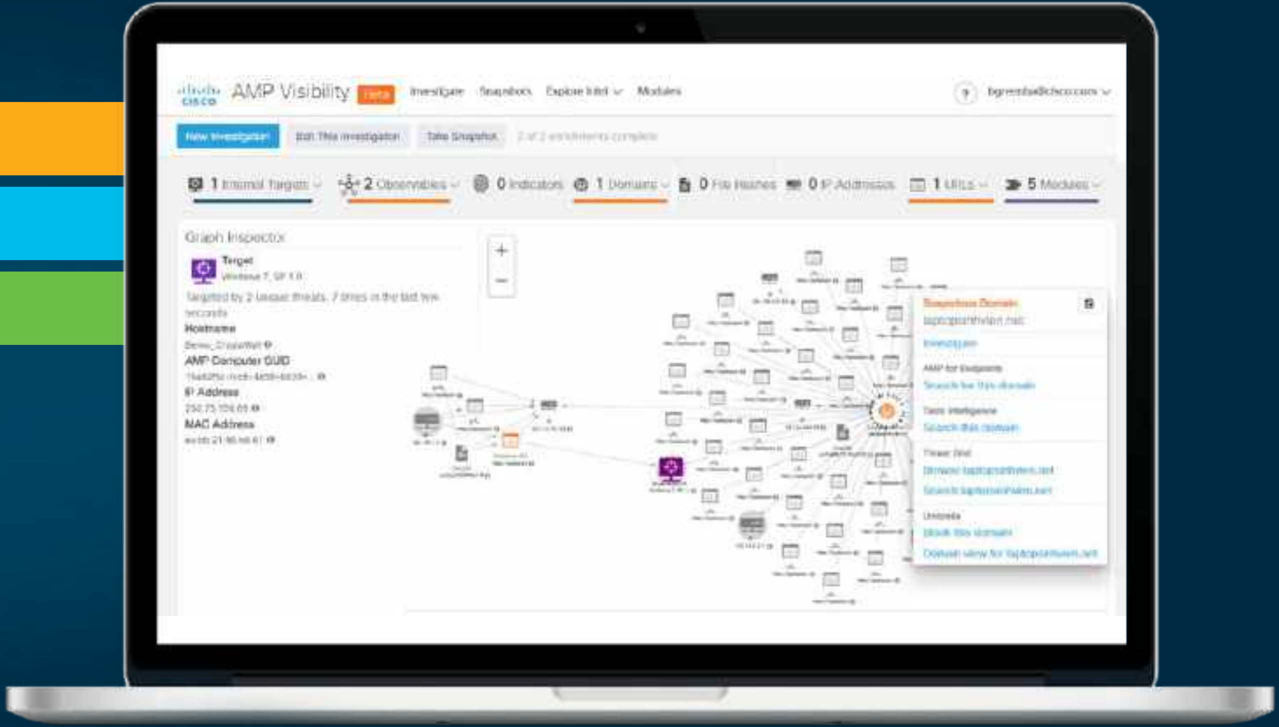
Capability to Continuous Monitoring

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



Capability to Perform In-depth Investigations

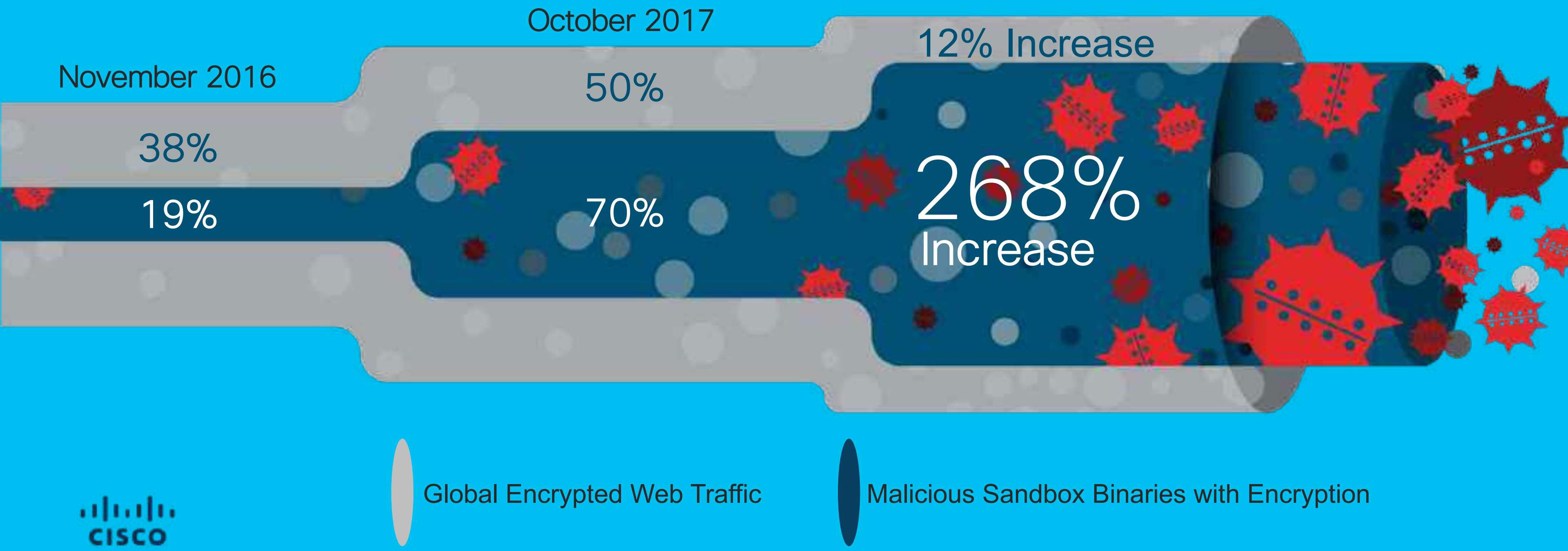
- Threat Hunting
- One Click Remediation
- Intelligence Correlation



Why endpoints is in focus… again?

Malicious Binaries and Encryption

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



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.

AMP for Endpoints

Prevent attacks and block malware in real time

Continuously monitor all processes and activity

Accelerate investigations and remediate faster

What is AMP for Endpoints?

Point-in-Time Detection – Plan A

1-1

One-to-One Signature

Fuzzy Fingerprinting

Machine Learning

Indications of Compromise

Dynamic Analysis

Advanced Analytics

Cognitive Intelligence

Application Vulnerability

Antivirus and rootkit detection

Device Flow Correlation

Exploit Prevention

Malicious Activity Prevention

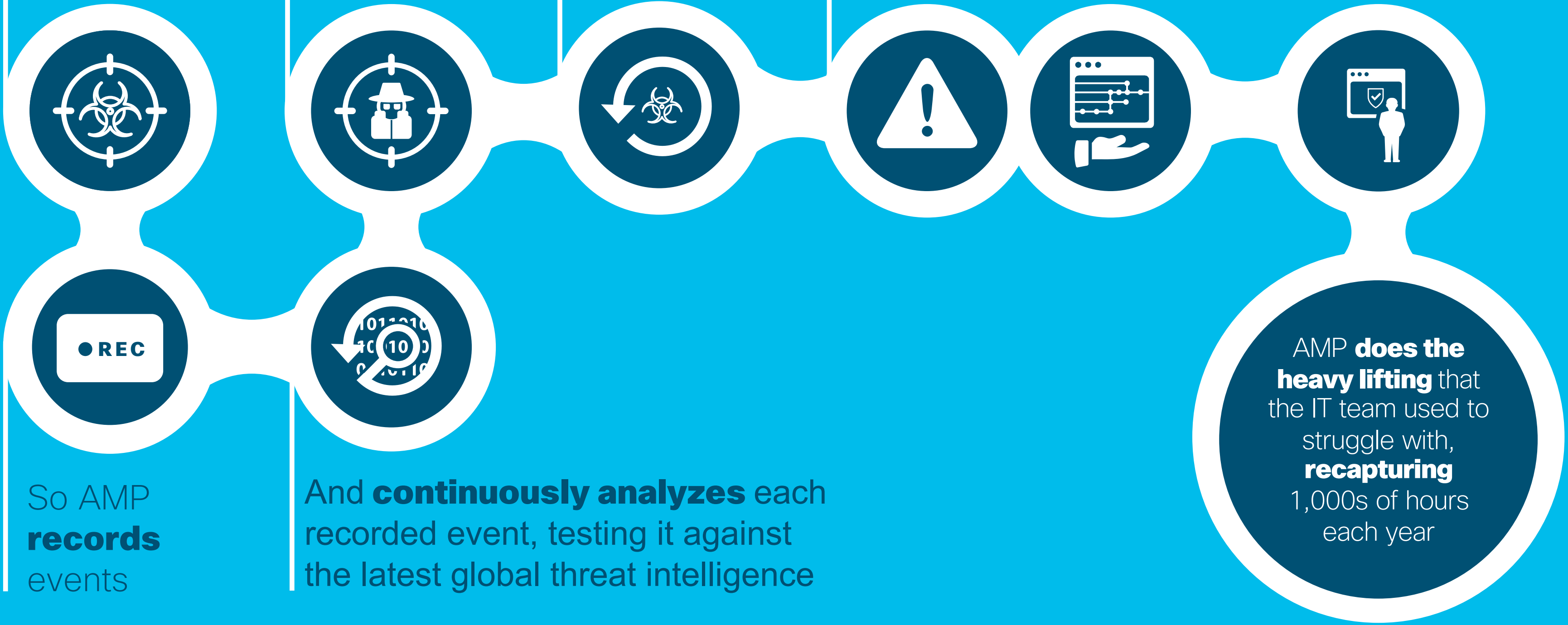
All Prevention < 100%

Retrospective Security Plan B

∞

Unique to AMP - Continuous Analysis & Retrospective Security

Cisco AMP



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

So AMP **records** events

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

Hunting inside your environment

Continually exposing and **blocking**

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

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

in Senad Aruc

@senadaruc

cisco