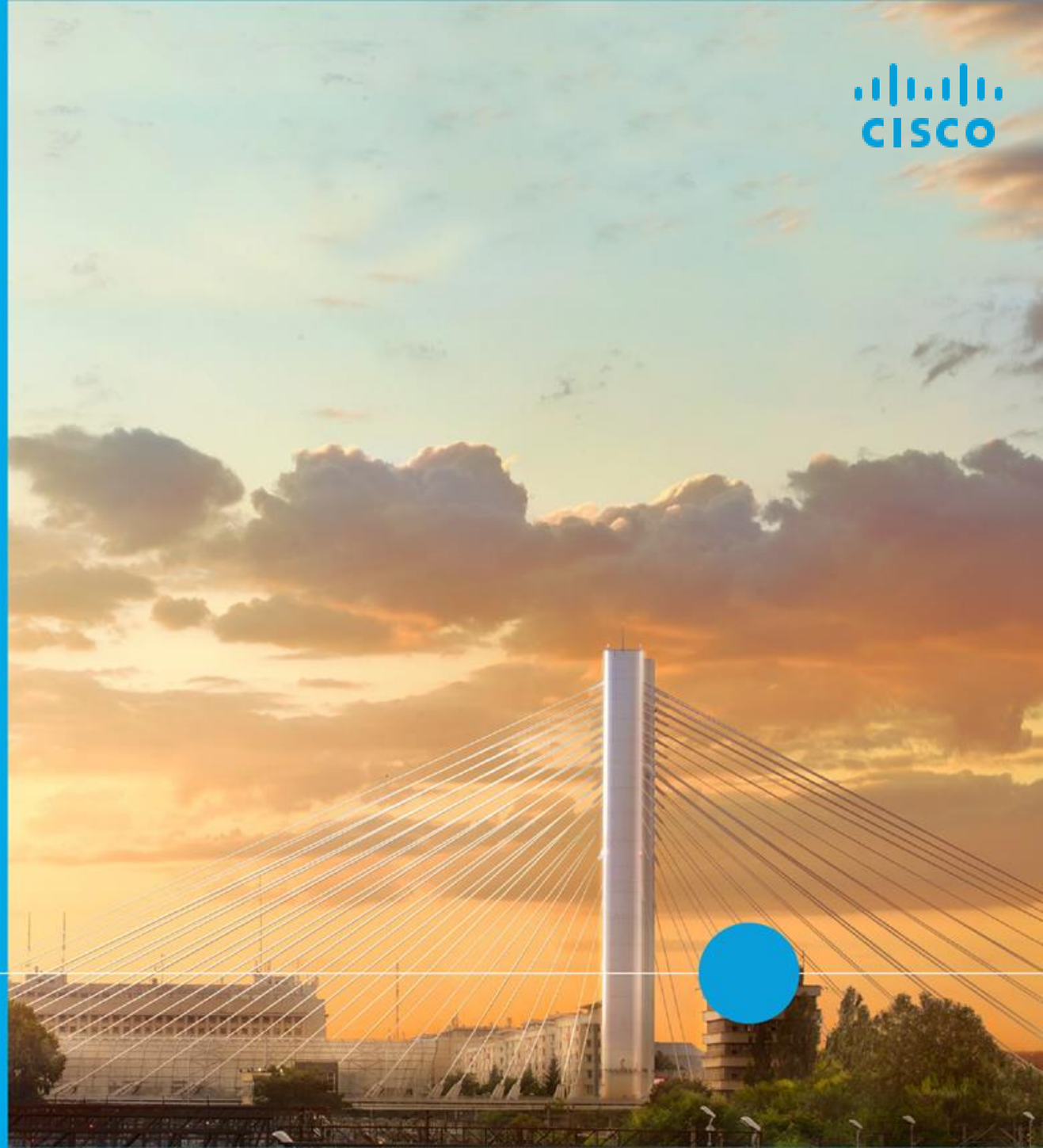
Cisco
Connect

Security ? where to ?

Adrian Aron

Consultant Systems Engineer

19 Oct



Agenda

Industry shift and trends

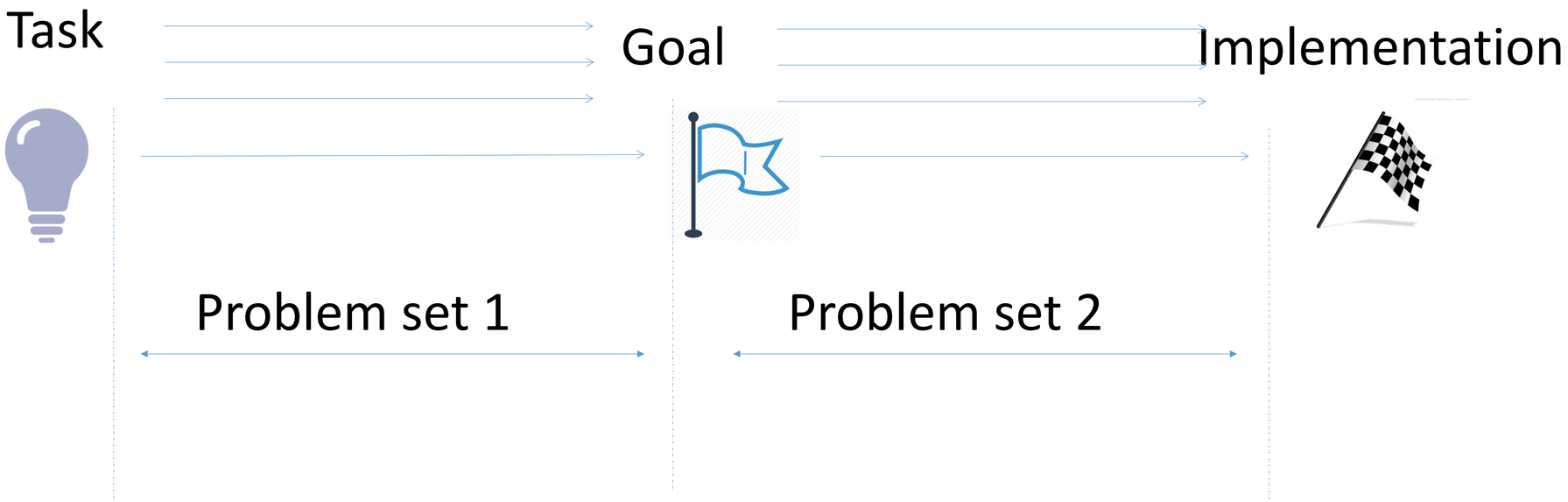
Router security, switch security

OpenDNS

Integration and automation

Q&A

Road from task to implementation



Example 1: car industry

“sustainable green cars”

Tesla S

Toyota Prius / BMW i

Mercedes F-cell

Less polution

Tesla 3

Rimac

Renault Zoe

Implementation

how? go-to market

what technology?

price, autonomy,

energy distribution

Example 2: security architecture

segregation

2FA, RBAC,
VLAN,VxLan, MPLS
ACI fabric

automate

Machine learning
pxGrid, REST, TAXII
SDA, SDP, SDN

Implementation

segment, auth
inspect, log

integrate, API
scripting, react

Router security

Integrated Security Solution for Branches

Options available on the ISR 4000 series:

Stealthwatch Learning Network

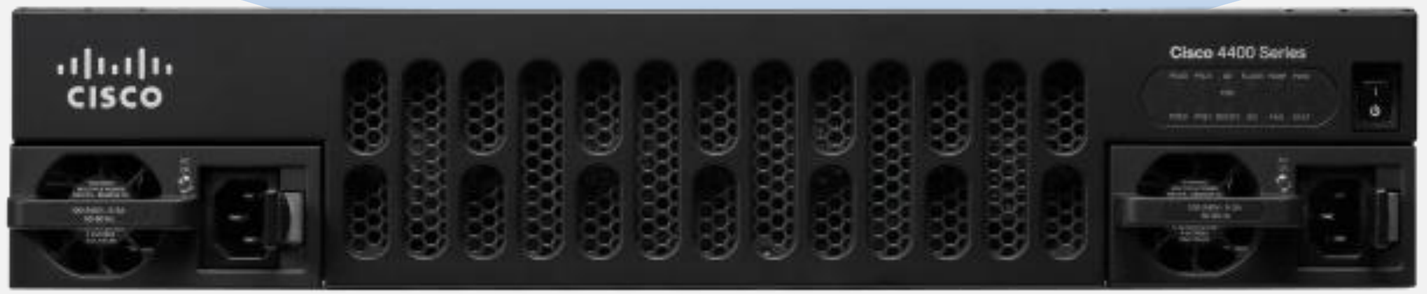
Umbrella Branch (OpenDNS)

VPN

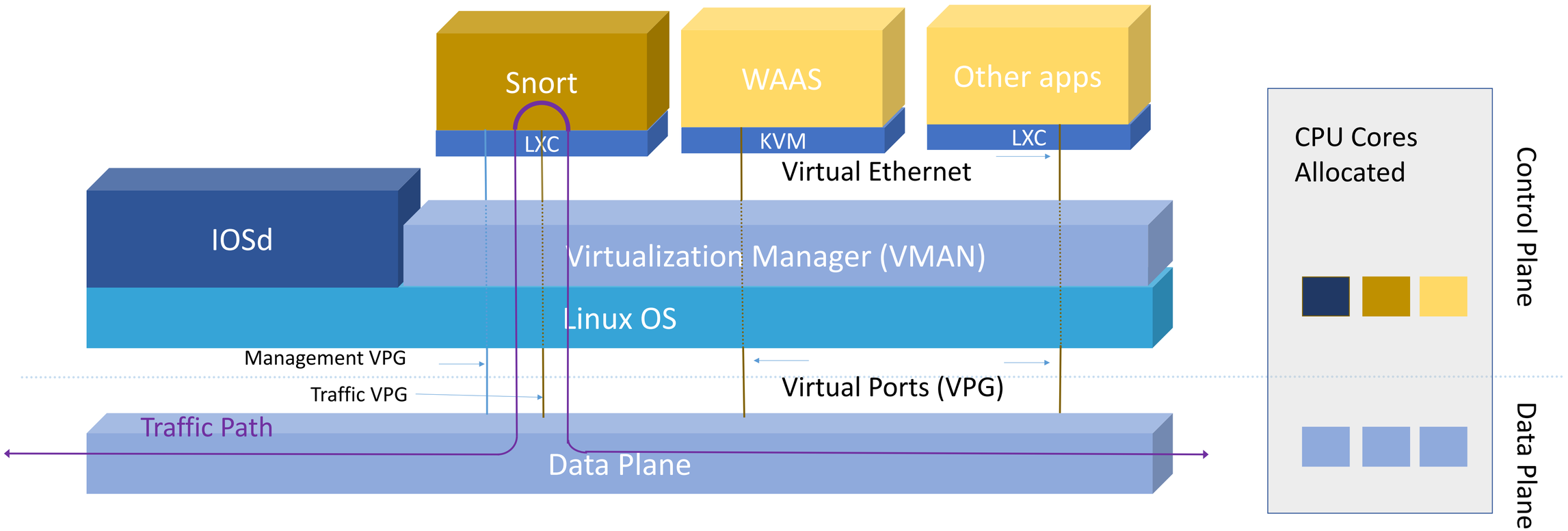
ZBFW

Snort IPS

Firepower



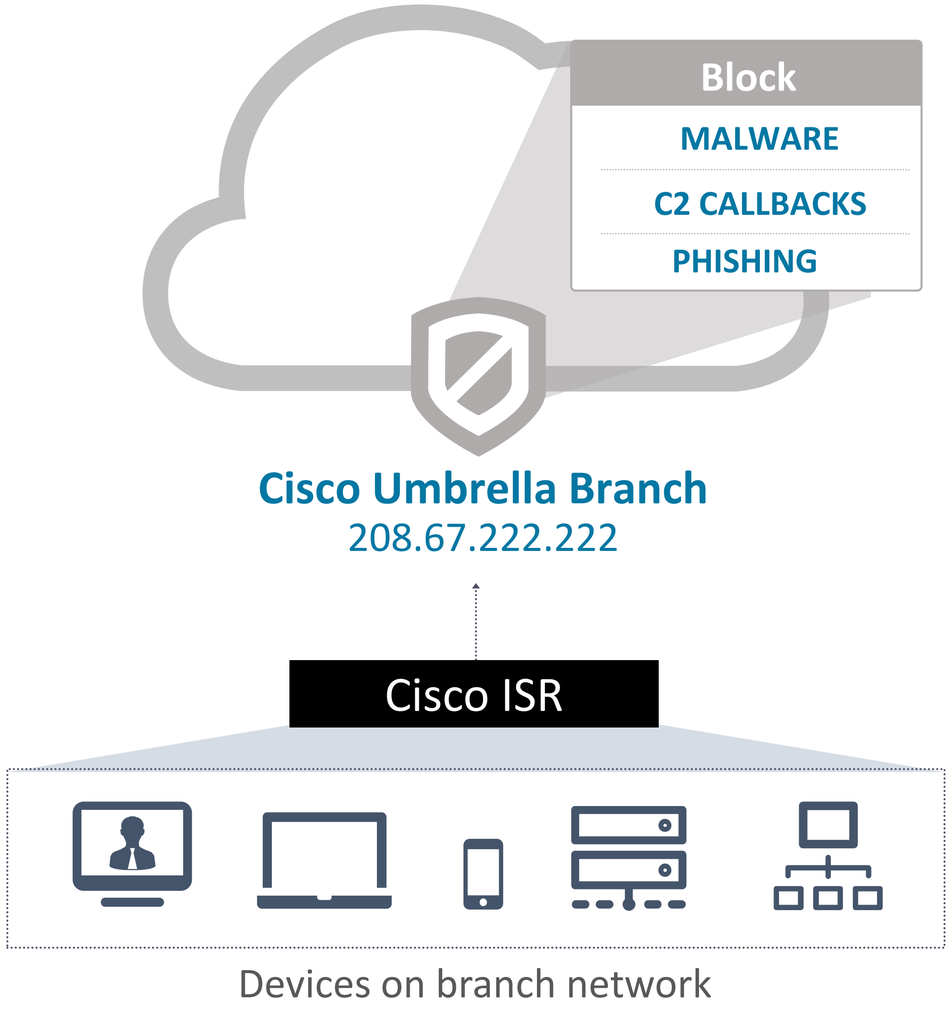
Snort IPS – Container Architecture



- Snort IPS runs on a Linux Container using control plane resources
- Traffic is punted to Snort Container using Virtual Port Group interface
- Reserved CPU and memory for Snort process enables deterministic performance

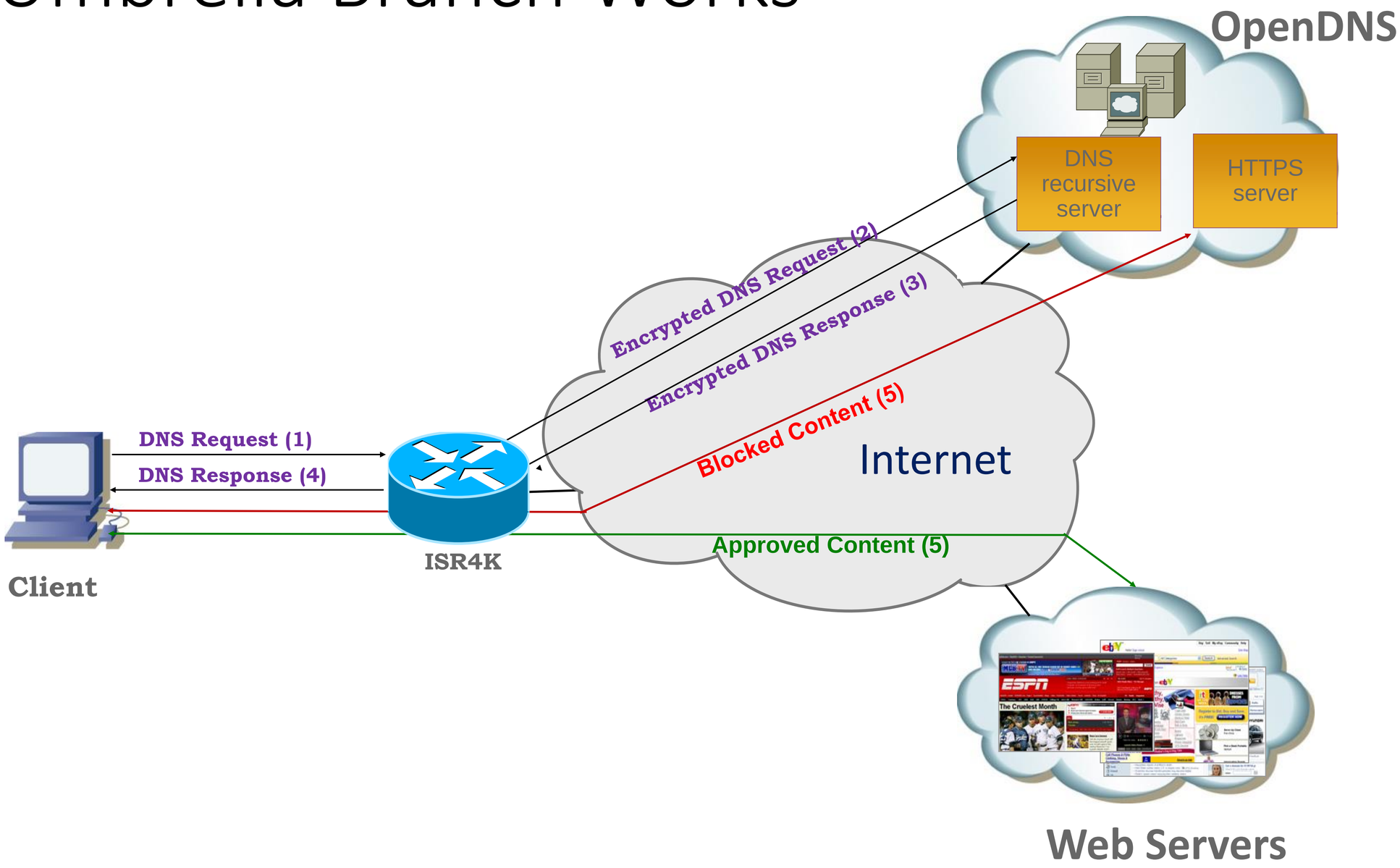
Cisco Umbrella Branch

Your first layer of defense at branch offices



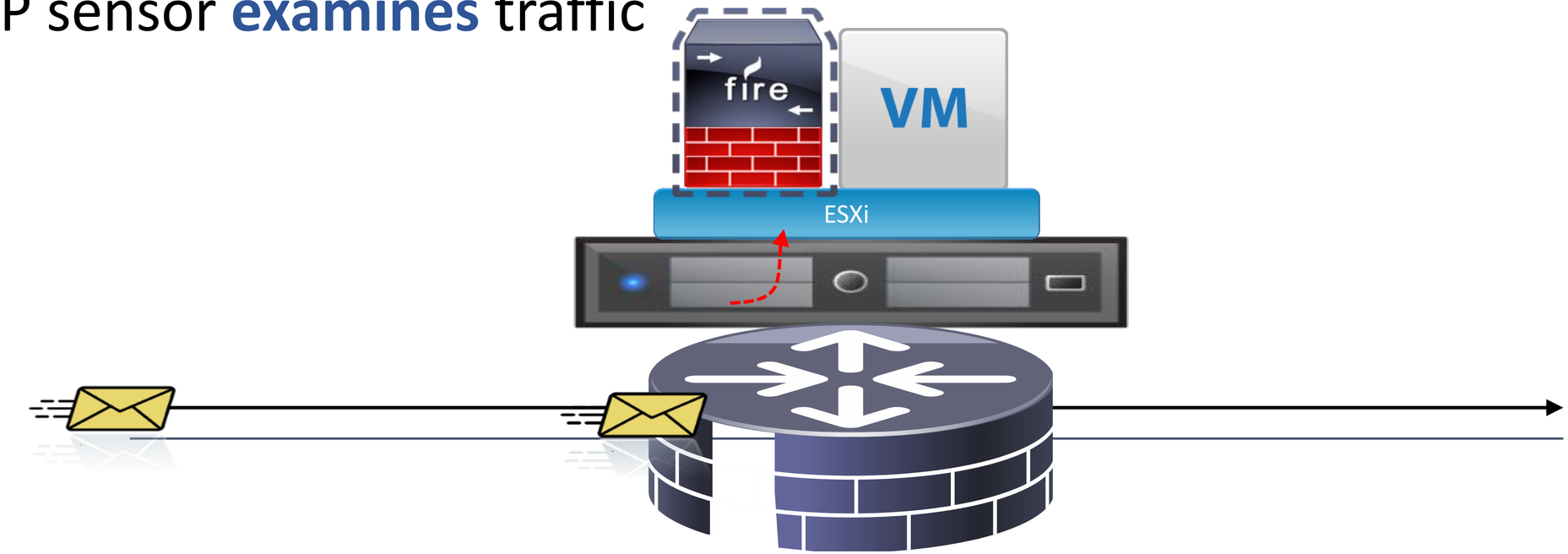
- Visibility & enforcement at the DNS-layer
- Block requests to malicious domains and IPs
- Predictive intelligence: uncover current & emergent threats
- Protect all devices on your branch network against:
  - Malware
  - Phishing
  - C2 callbacks

How Umbrella Branch Works



Firepower Threat Defense on ISR - IDS

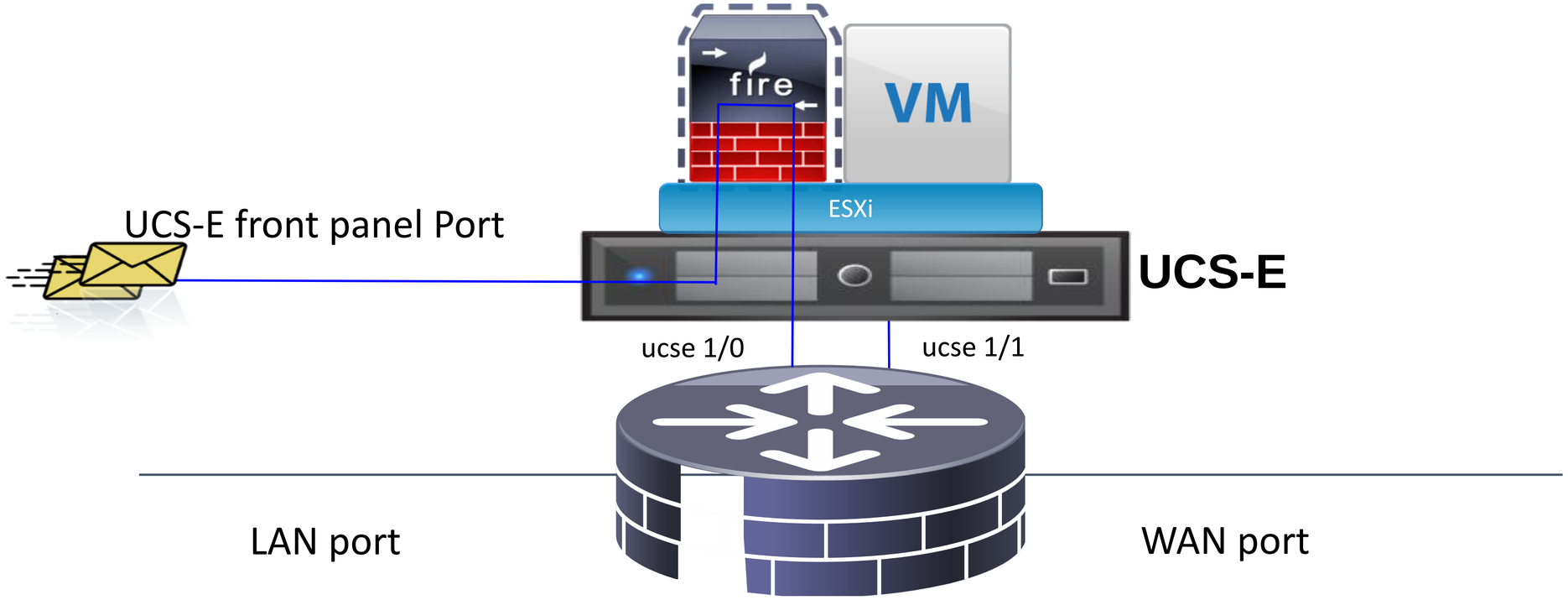
- Host the IDS Sensor on the UCS-E server colocated within router
- Replicate and push all the traffic to be inspected to the Sensor
- FP sensor **examines** traffic



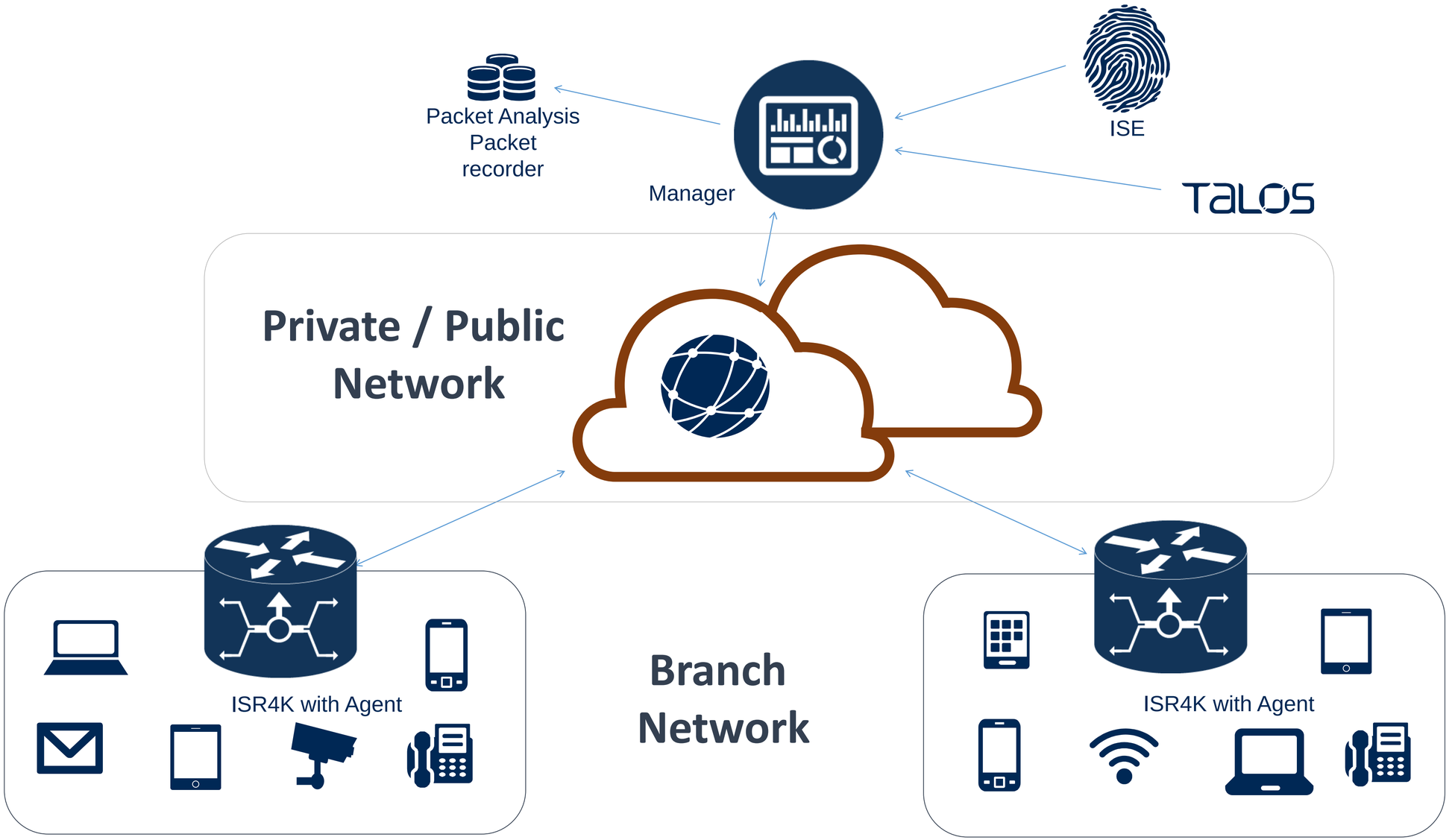
WARNING: It is not recommended to install FP sensor and Firepower Management Center VMs on the same UCS-E unless it is for testing purpose

Firepower Threat Defense for ISR- IPS (front panel port)

- Host the Sensor on the UCS-E server
- IPS is in inline mode
- Packets ingress via the UCS-E front panel port
- SF sensor examines traffic; **allowed** packets egress the WAN interface



Automating Security in your Branch Offices



Basic Operation of the Learning Network

1 Discovers traffic paths

2 Builds map of IP addresses to learn about its environment

3 Identifies applications on NBAR and DPI

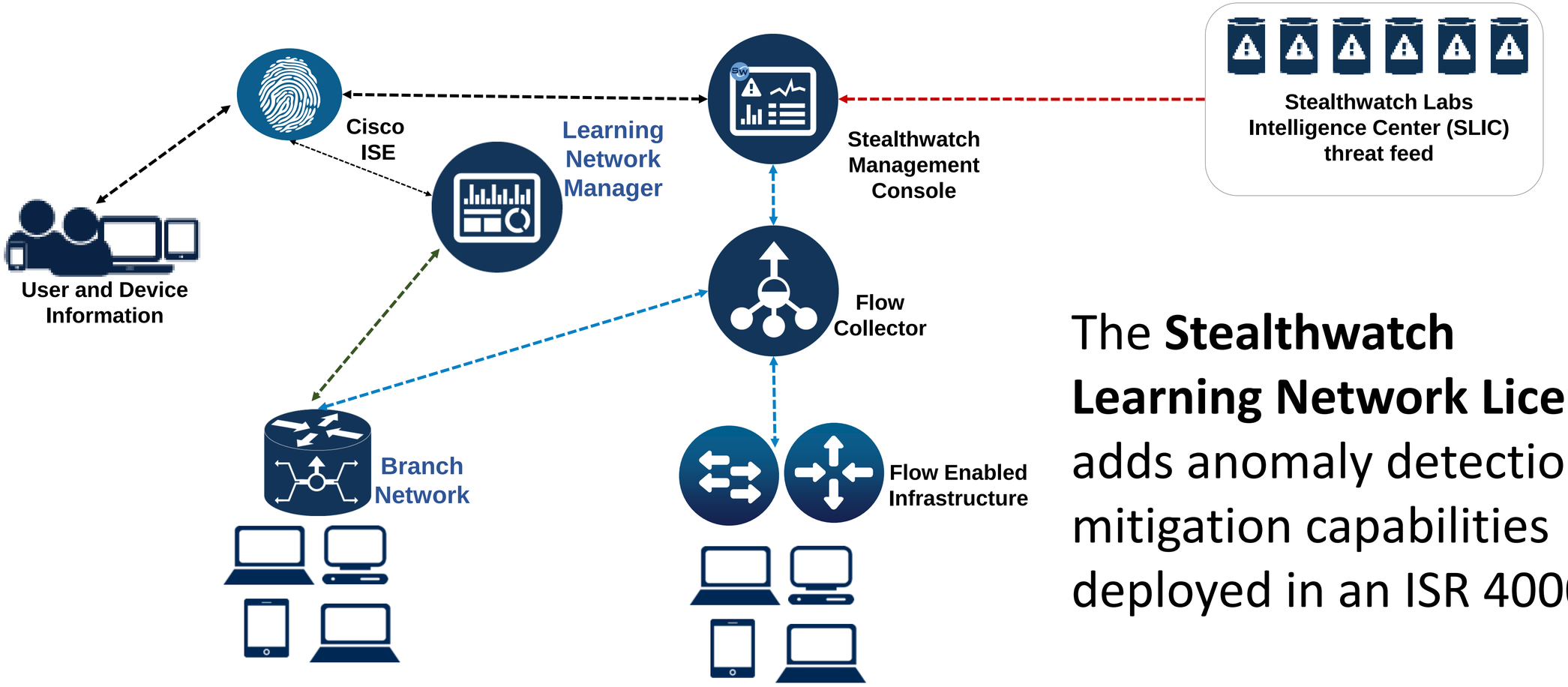
4 Studies traffic movement, volumes, patterns, times of day

5 Learns to distinguish normal from anomalous

6 Precisely identifies anomaly; allows operator to take action to remediate

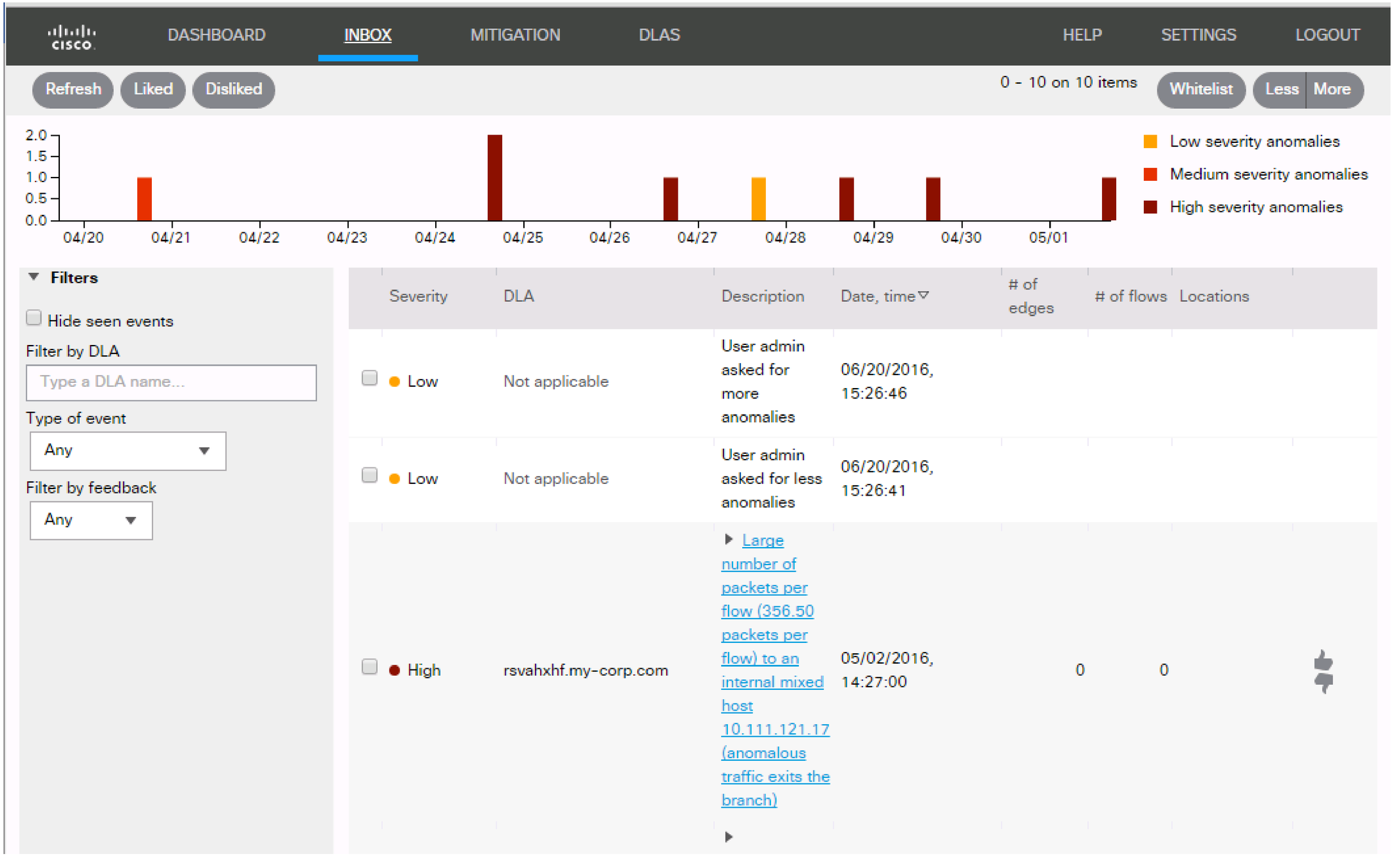
Learning Network Agent

Stealthwatch Portfolio: Learning Network



The **Stealthwatch Learning Network License** adds anomaly detection & mitigation capabilities deployed in an ISR 4000.

Inbox Top Level view



Inbox Conversations

INBOX | MITIGATION | DLAS | USERS | HELP | SETTINGS | LOGOUT

…ber of bytes (4.37 MiB) for an internal http client and windows host X.125.81.111 in United States

Like | Dislike | Whitelist | Get PCAP files

…e 07/13/2016, 21:07:00 Severity ● High Seen: 07/20/2016, 16:51:22

Display hostnames when possible

Facts

The other correspondent is an external dns server znpexo.my-corp.com in United States

Host X.125.81.111 also communicates with 22 other hosts in 8 clusters: new external hosts in United States, external ntp servers, external dns servers, new external hosts in United States (OR), new external hosts in United States (CA), new external hosts in United States (MA), external windows hosts, new external hosts in United Kingdom

Host X.125.81.111 has been involved in 1 anomalies in the past

They communicate bidirectionally using the following application(s): dns

99.9% of the number of bytes for the graph dns are between 31.00 bytes and 256.00 KiB.

Host X.125.81.111 is alone in its cluster

There are 2 other external dns servers

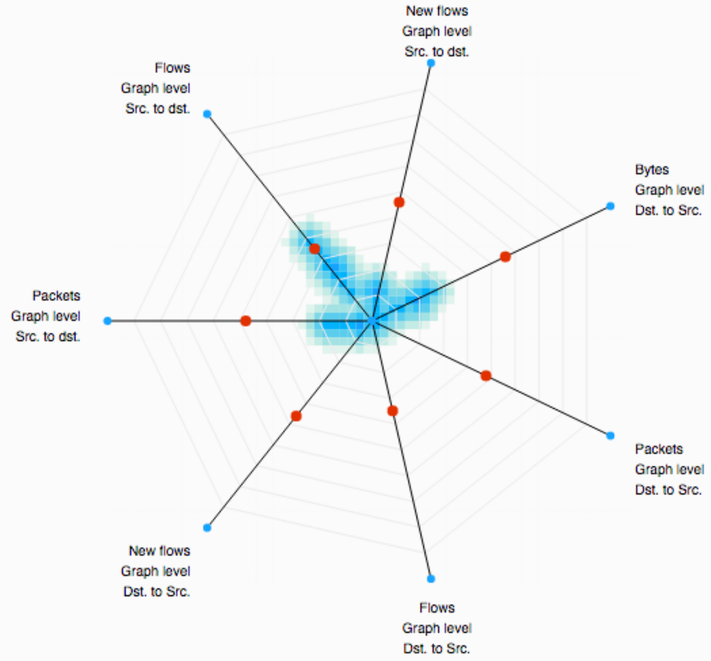
Conversations

Expand all | Collapse all

App. group	Source	Destination	21:00:00	21:11:00
DNS	X.125.81.111 Internal http clients and windows hosts	znpexo.my-corp.com External dns servers		
Anomalous feature(s):	Packets ⇢ (15 K)	Flows ⇢ (12 K flows)	New flows ⇢ (10 K flows)	Bytes ⇠ (3.49 M)	Packets ⇠ (30 K)	Flows ⇠ (12 K flows)	New flows ⇠ (10 K flows)
DNS	X.125.81.111 Internal http clients and windows hosts	zvcvnmt.my-corp.com External dns servers		

23 conversation(s) hidden Show all

Anomalous features graph



Previous Play Next

Between 21:07:00 and 21:08:00, 7 features were anomalous:

Packets ⇢ (15 K)
Compared to all other conversations of the graph : 99.99% of the packets for graph dns are between 0 and 2 K

Flows ⇢ (12 K flows)
Compared to all other conversations of the graph : 99.99% of the flows for graph dns are between 0 flow and 1 K flows

New flows ⇢ (10 K flows)
Compared to all other conversations of the graph : 99.99% of the new flows for graph dns are between 0 flow and 1 K flows

Bytes ⇠ (3.49 M)
Compared to all other conversations of the graph : 99.99% of the bytes for graph dns are between 15 B and 512 K

Packets ⇠ (30 K)
Compared to all other conversations of the graph : 99.99% of the packets for graph dns are between 0 and 2 K

Flows ⇠ (12 K flows)
Compared to all other conversations of the graph : 99.99% of the flows for graph dns are between 0 flow and 1 K flows

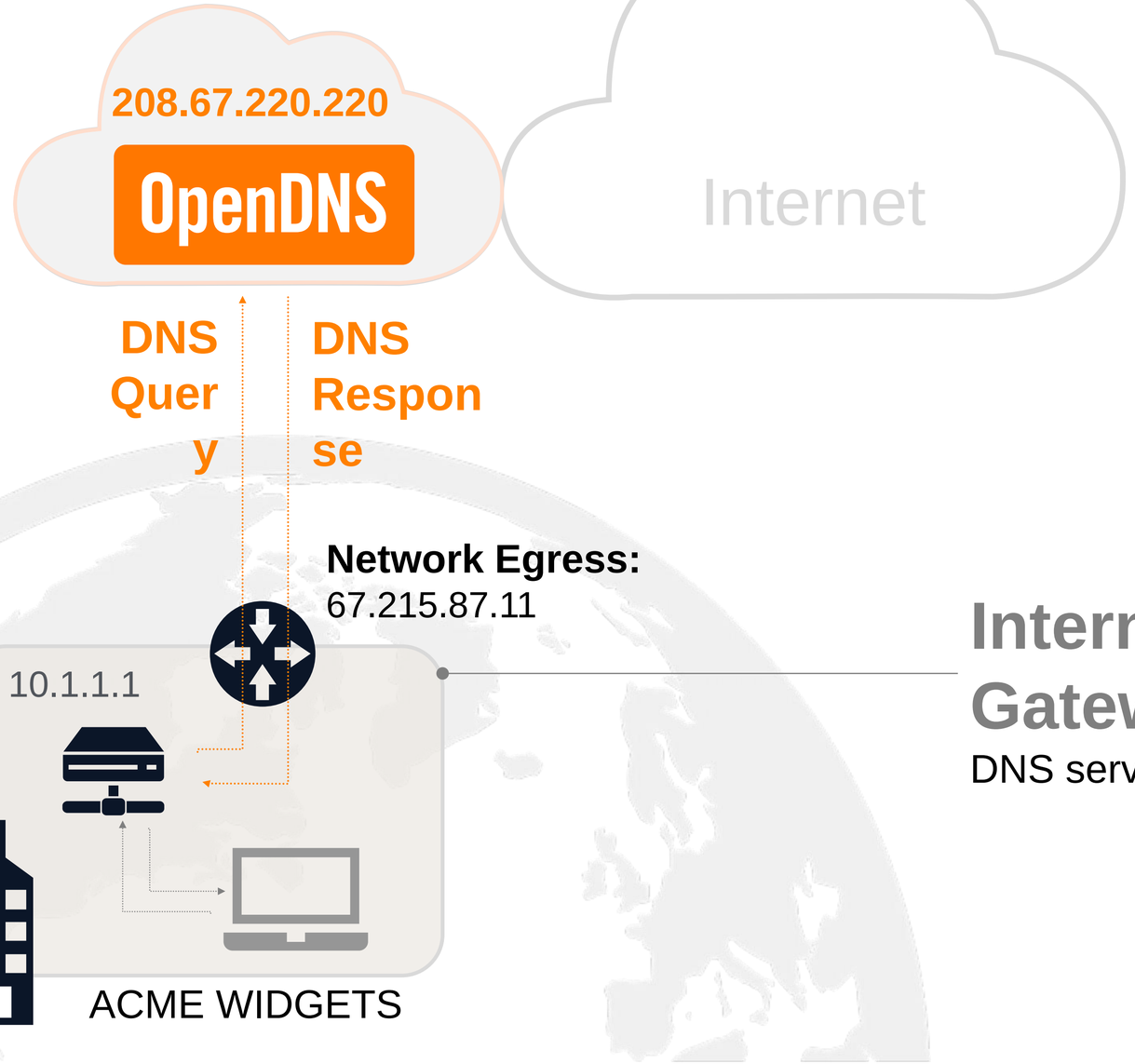
New flows ⇠ (10 K flows)
Compared to all other conversations of the graph : 99.99% of the new flows for graph dns are between 0 flow and 1 K flows

Open DNS

1: Provision On-Network Devices via DNS Server

Acme Widgets Policy

enforce all security settings for 67.215.87.11



Internal DNS Server

external DNS resolution = 208.67.220.220

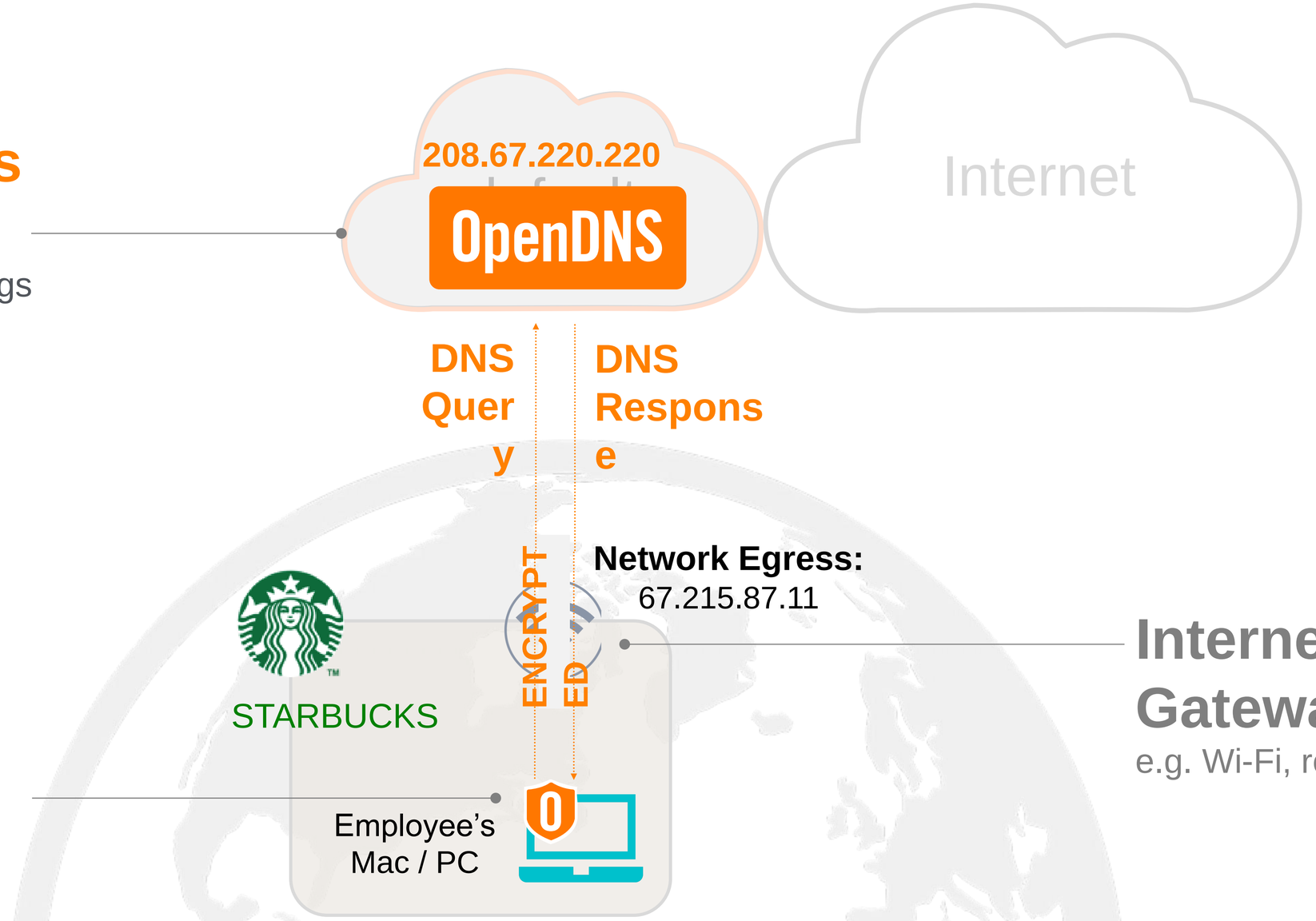
Internet Gateway

DNS server = 10.1.1.1

2: Provision On or Off-Network Mac / PCs via Roaming Client

Acme Widgets Policy

enforce all security settings for GUID = Acme employee's Mac



Roaming Client

inserts GUID & Org ID in EDNS request, encrypts and forwards

Internet Gateway

e.g. Wi-Fi, router

A Single, Correlated Source of Intelligence

INVESTIGATE

- Passive DNS database
- WHOIS record data
- Malware file analysis
- ASN attribution
- IP geolocation
- Domain & IP reputation scores
- Domain co-occurrences
- Anomaly detection (DGAs, FFNs)
- DNS request patterns/geo. distribution

Top Ways to Add OpenDNS to Customer's Security Stack

OFF-NETWORK SECURITY

Umbrella
+
ASA / AnyConnect

SECURE DIRECT-TO-NET OFFICES

Umbrella
+
ISR / Meraki

NEW LAYER OF PREDICTIVE SECURITY

Umbrella
+
AMP for Endpoints

AUTOMATE ENFORCEMENT & VISIBILITY

Umbrella
+
Threat Grid

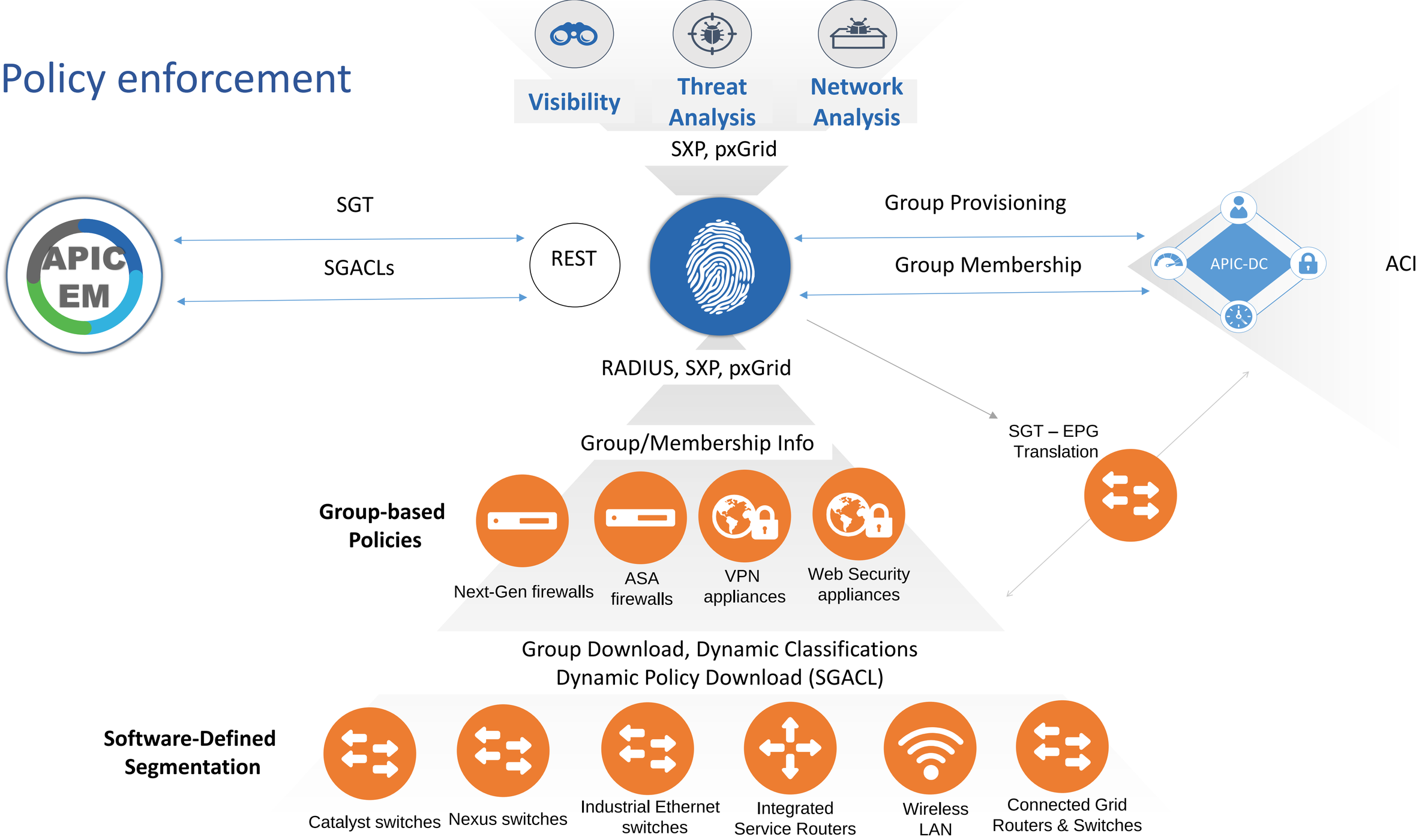
SPEED UP INCIDENT RESPONSE

Investigate
+
Threat Grid

Integration looking forward

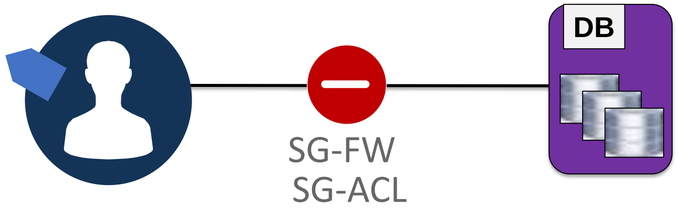
Automation is a consequence

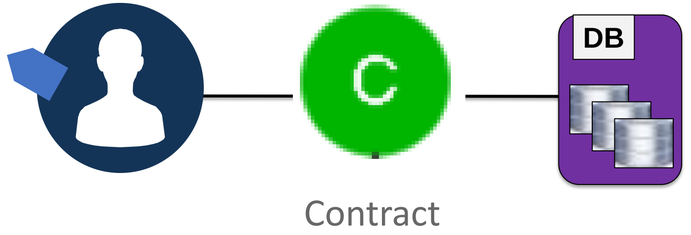
Policy enforcement

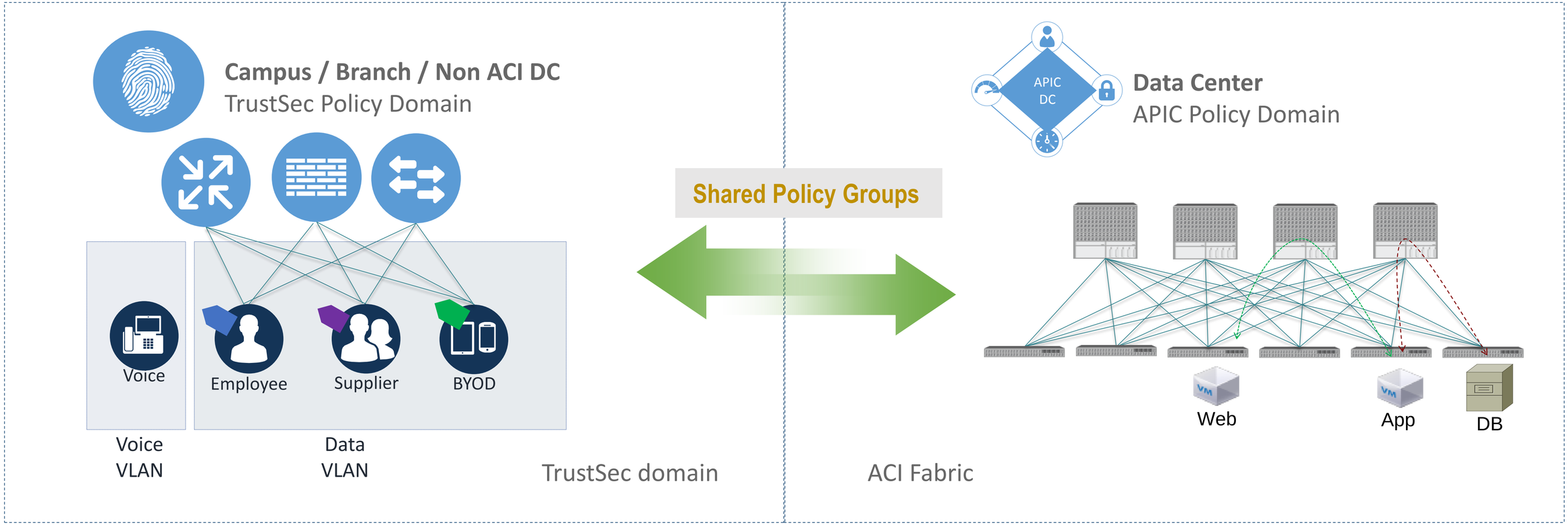


Enabling Group-based Policies across the Enterprise

Policy corelation







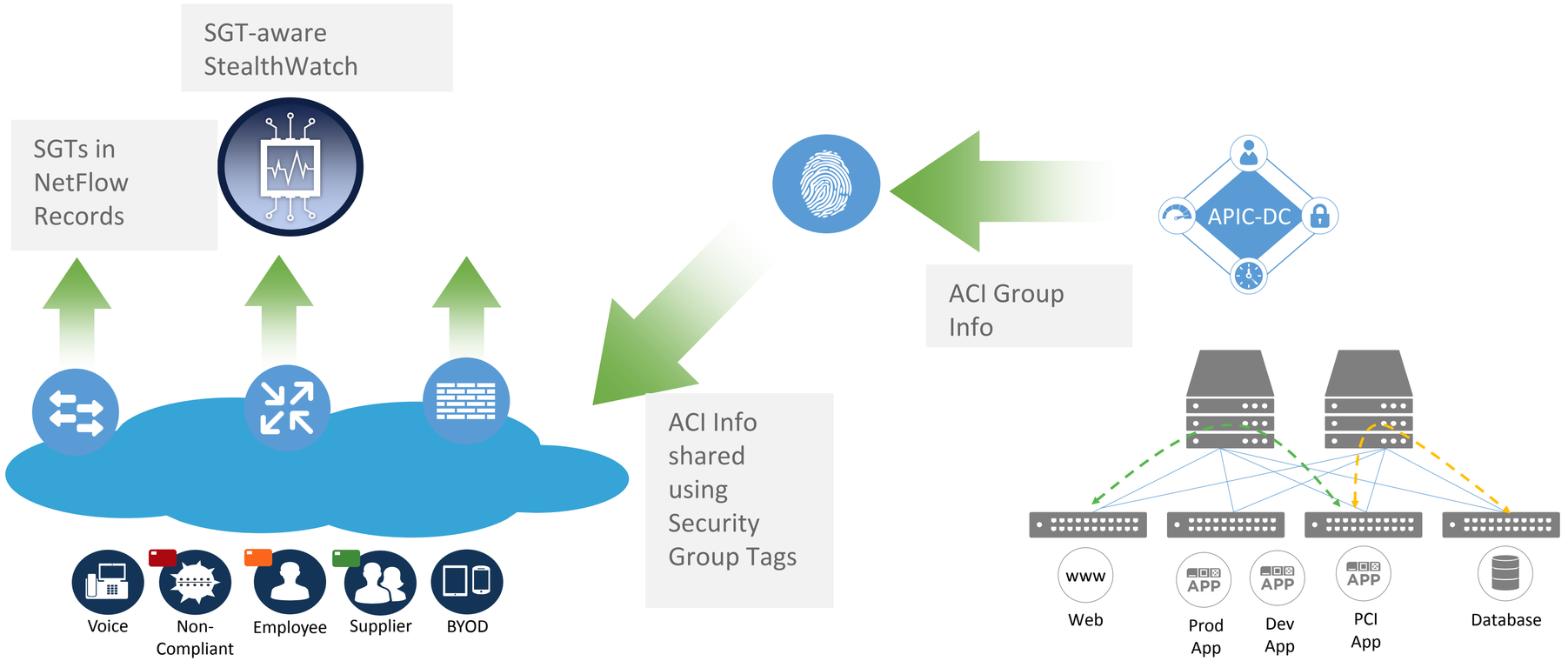
Making StealthWatch Aware of ACI Groups

Policy enrichment and adjustoment

What's new?

Integration of TrustSec and ACI policy groups allows us to make NetFlow aware of Groups from the DC

StealthWatch then receives NetFlow with SGT information based on the DC groups from ACI



Cisco Platform Exchange Grid (pxGrid)

Any-to-Any Platform Data & Service Exchange

Rapid Threat Containment Use Cases

Benefits

Detect threats early
ANC Mitigation actions sent to ISE for real-time response

Automate alerts
Leveraging ISE ANC to alert the network of suspicious activity according to policy

Leverage a growing ecosystem
of partners that provide rapid threat containment by integrating with ISE

Rapid Threat Containment with Ecosystem Partners and ISE

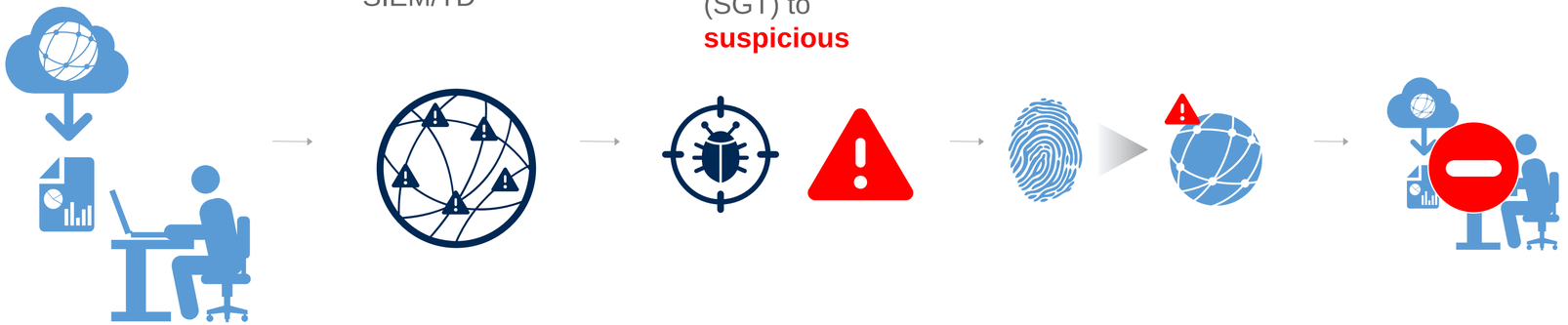
- Corporate user downloads file
- Malware detected on device

- Scans user activity and file
- Behavioral Analysis
- Vulnerability Scans
- SIEM/TD

- Detects suspicious file and alerts ISE using pxGrid by changing the Security Group Tag (SGT) to **suspicious**

- Based on the new tag, ISE enforces policy on the network

- Access based on organizations security policy

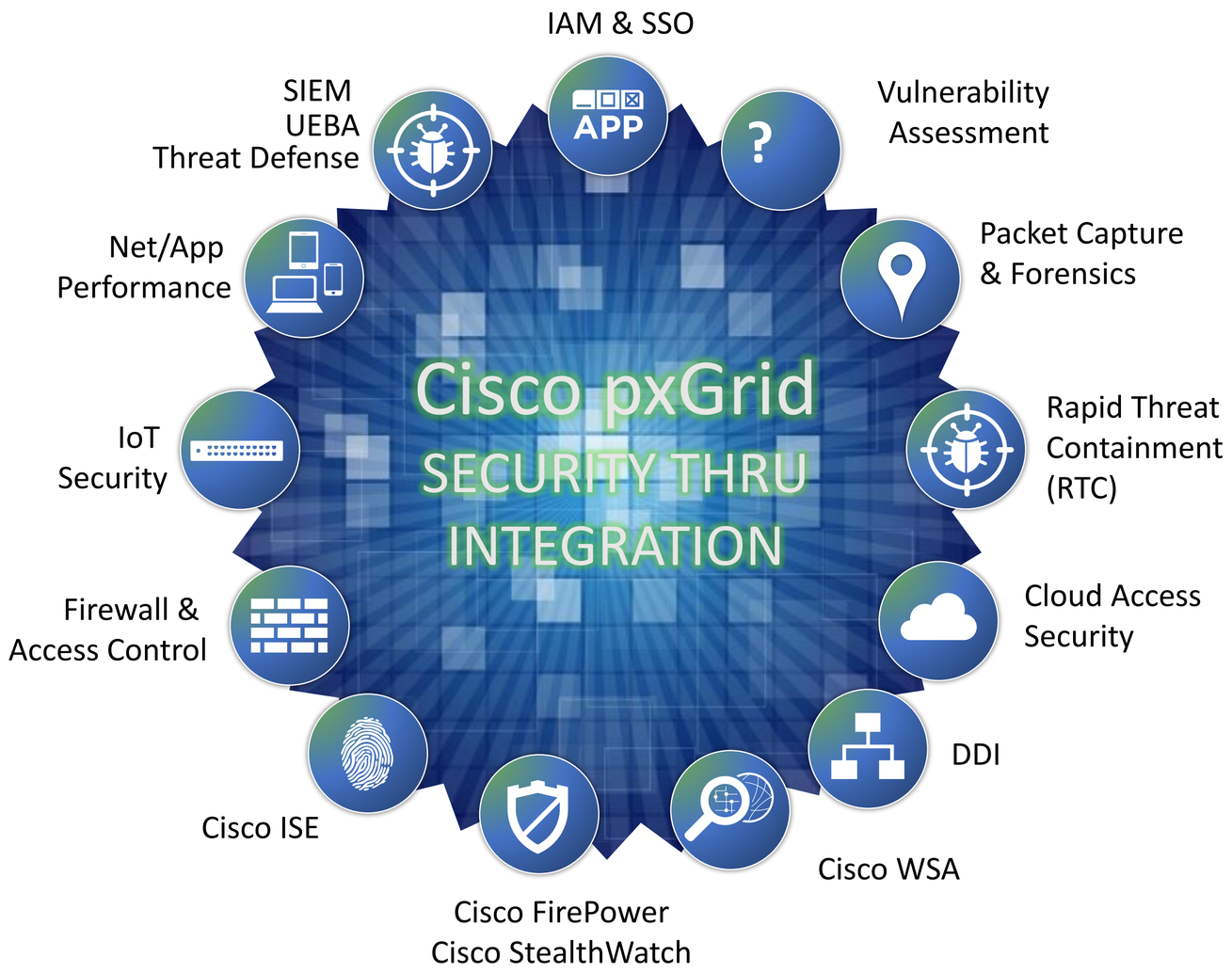


ANC Mitigation Actions

- ISE EPS RESTful API
- pxGrid (EndpointProtectionService/AdaptiveNetwork Control
- STIX- Threat Centric NAC- AMP/Qualys

pxGrid – Industry Adoption Critical Mass

40+ Partner Product Integrations and 12 Technology Areas in 18 Months Since Production Release



pxGrid-Enabled Partners:

- Cisco: WSA, FirePower, ISE, StealthWatch
- RTC: Cisco FirePower, Cisco StealthWatch, Attivo, Bayshore, E8, Elastica, Hawk, Huntsman, Infoblox, Intelliment, Invincea, Lemonfish, LogRhythm, NetIQ, Rapid7, RedShift, SAINT, Splunk, Tenable, ThreatTrack, TrapX
- Firewall: Check Point, Infoblox, Intelliment, Bayshore
- DDI: Infoblox
- CASB: Elastica, Netskope, SkyHigh
  Net/App: Lumeta, Savvius
- SIEM/TD: LogRhythm, NetIQ, Splunk
  UEBA: E8, FortScale, Niara, Rapid7
- IAM: NetIQ, Ping, SecureAuth, Situational
- Vulnerability: Rapid7, SAINT, Tenable
- IoT Security: Bayshore Networks
- P-Cap/Forensics: Emulex

Conclusions

Infrastructure takes many forms to ensure telemetry and detection

Time to detection becomes critical

Router security, switch security, no longer a switch / router

DNS is a tool used for attacking and defending

Integration and automation, contains a breach

, if time to detection !

Q&A