Change the Equation with Data Centre security

Data is currency and data centers need protecting

Suwitcha Musijaral, CISSP,CISA
Consulting System Engineer - Security
January 2018

Think about Security as what are we defending….

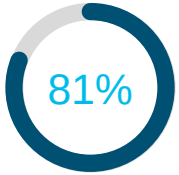
and who are we defending it from ?

Cisco UCS
with
Intel® Xeon®
processors

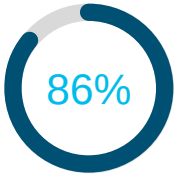
‘It’s where the money is’

Jake Davis - Anonymous

How is data being stolen? … **via** people!



of hacking-related breaches leveraged either stolen and/or weak passwords



of malicious payloads are delivered through email (73%) and web (13%)

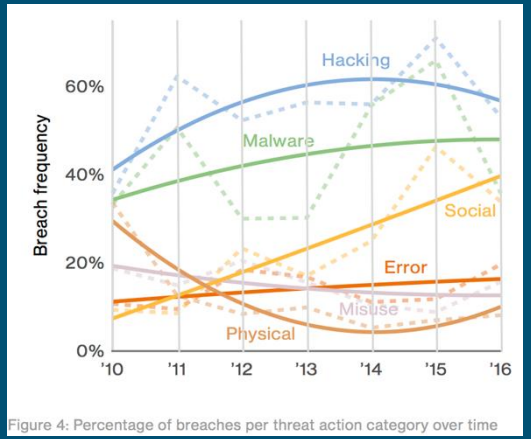


Figure 4: Percentage of breaches per threat action category over time

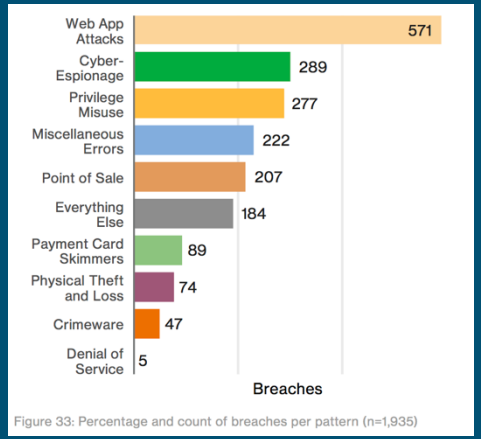


Figure 33: Percentage and count of breaches per pattern (n=1,935)

The Modern Data Center is incredibly complex

Big and Fast Data

Virtualization

Expanded attack surface

Increase in east-west traffic

Hybrid Cloud

Multi cloud orchestration

Workload portability

Zero trust model

Application Architecture

Continuous development | Micro Services | APIs

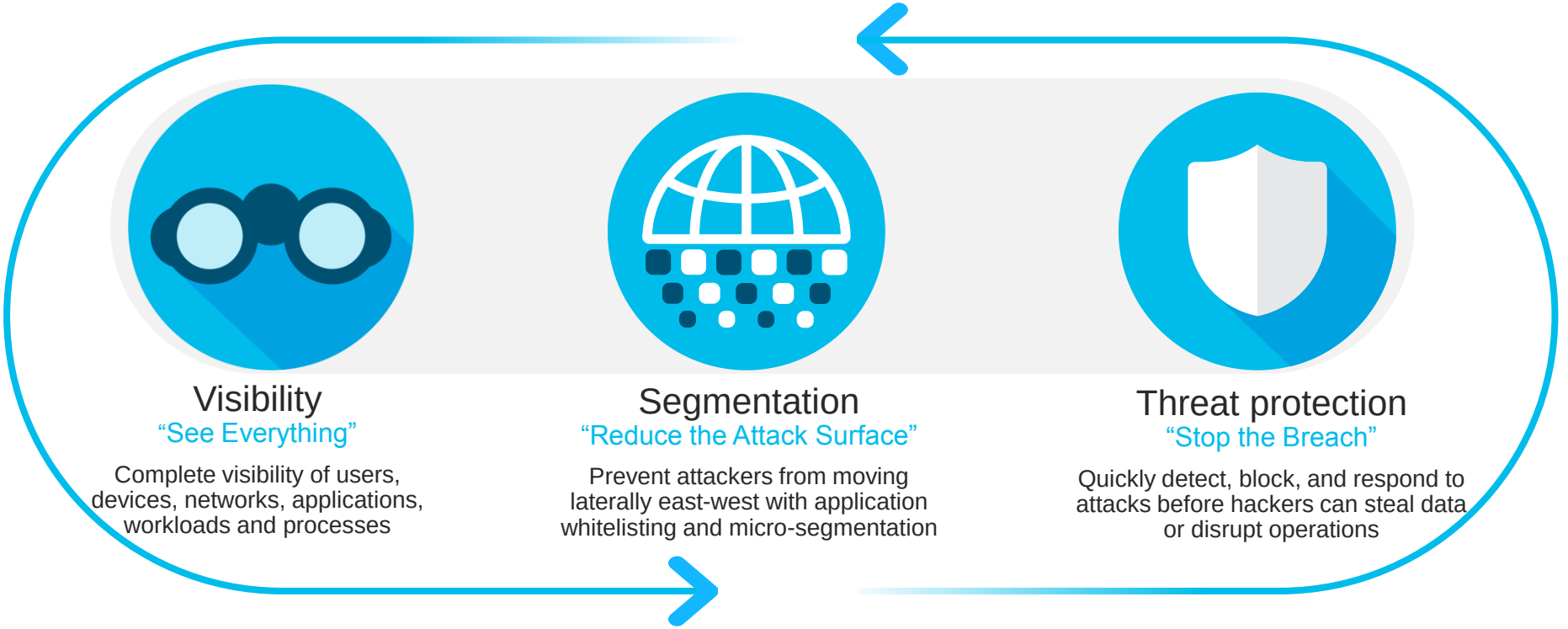
Network Challenges

- Outage/degraded service
- Insufficient visibility into the network, workload, application
- Rising security breaches and destruction of service (DeOS) attacks
- Increasing regulatory compliance requirements and audits
- Rising ACL/FW rule complexity and administration burden

- Not enough threat visibility in the network, workloads, applications
- Inconsistent policies across workloads
- Too many point security vendors
- Hackers are more sophisticated
- Attack surface is too broad

Security Challenges

Cisco Data Center Security



Visibility
"See Everything"

Complete visibility of users, devices, networks, applications, workloads and processes

Segmentation
"Reduce the Attack Surface"

Prevent attackers from moving laterally east-west with application whitelisting and micro-segmentation

Threat protection
"Stop the Breach"

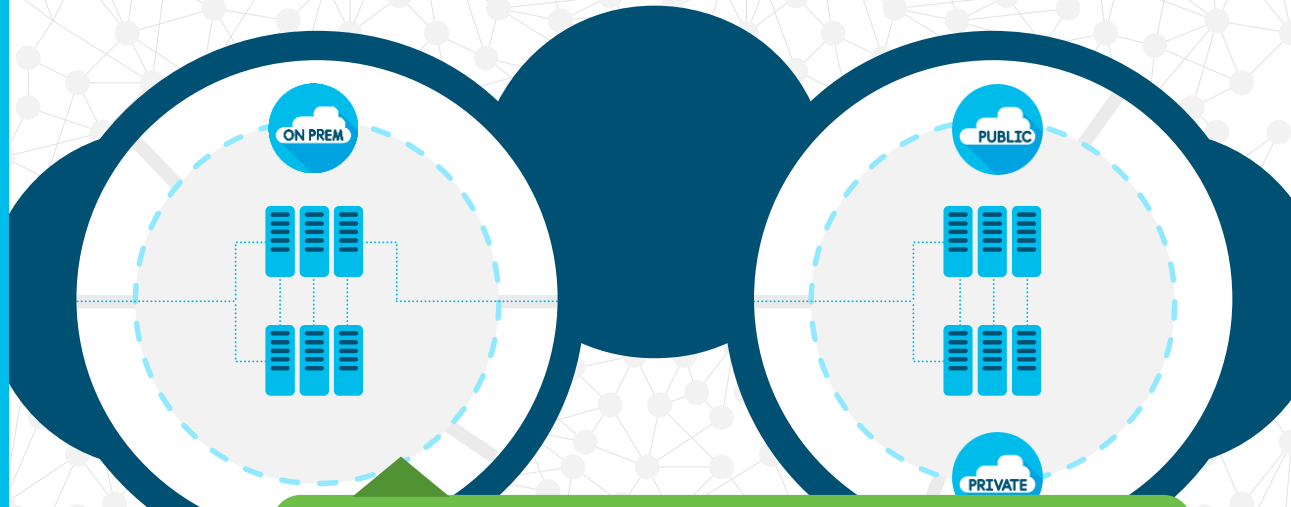
Quickly detect, block, and respond to attacks before hackers can steal data or disrupt operations

The Intent Cycle

01 02 03

Visibility:
See application components & their behavior

Cisco Tetration

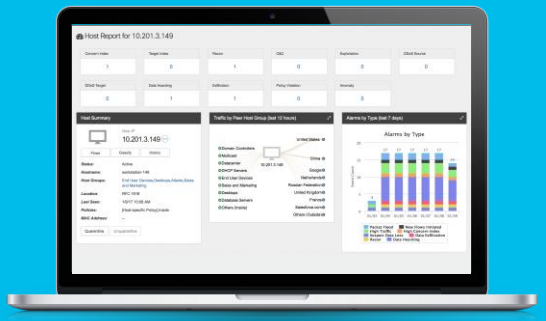


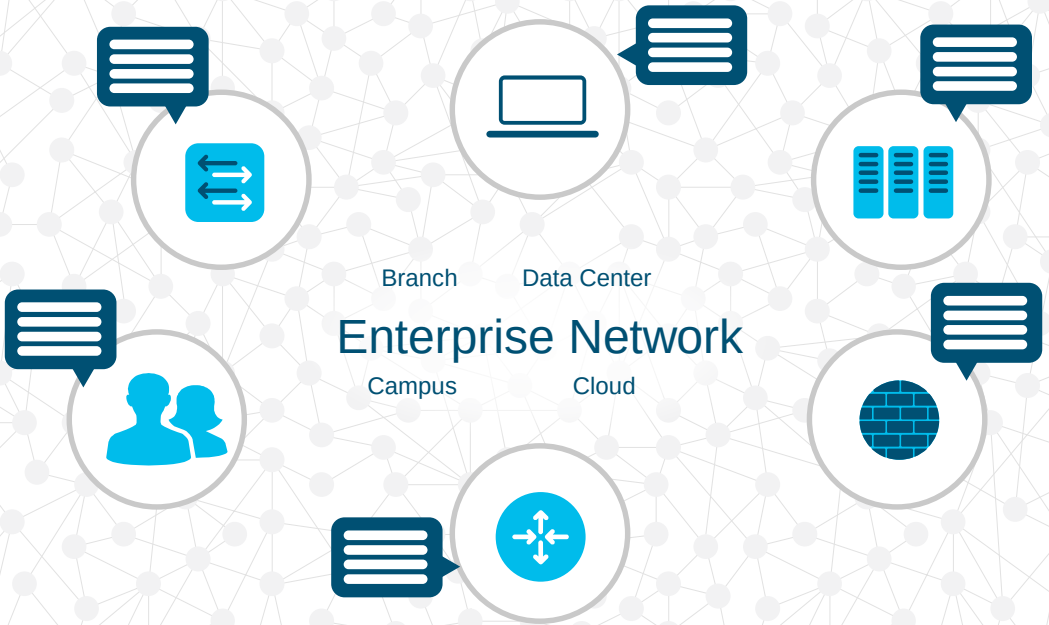
- Full visibility into application components including workloads, processes and application behavior in the data center
- Application dependency mapping
- Application segmentation policies (whitelist/blacklist)
- Forensic search and application anomaly detection

01 02 03

Visibility:
See across the enterprise network

Cisco Stealthwatch



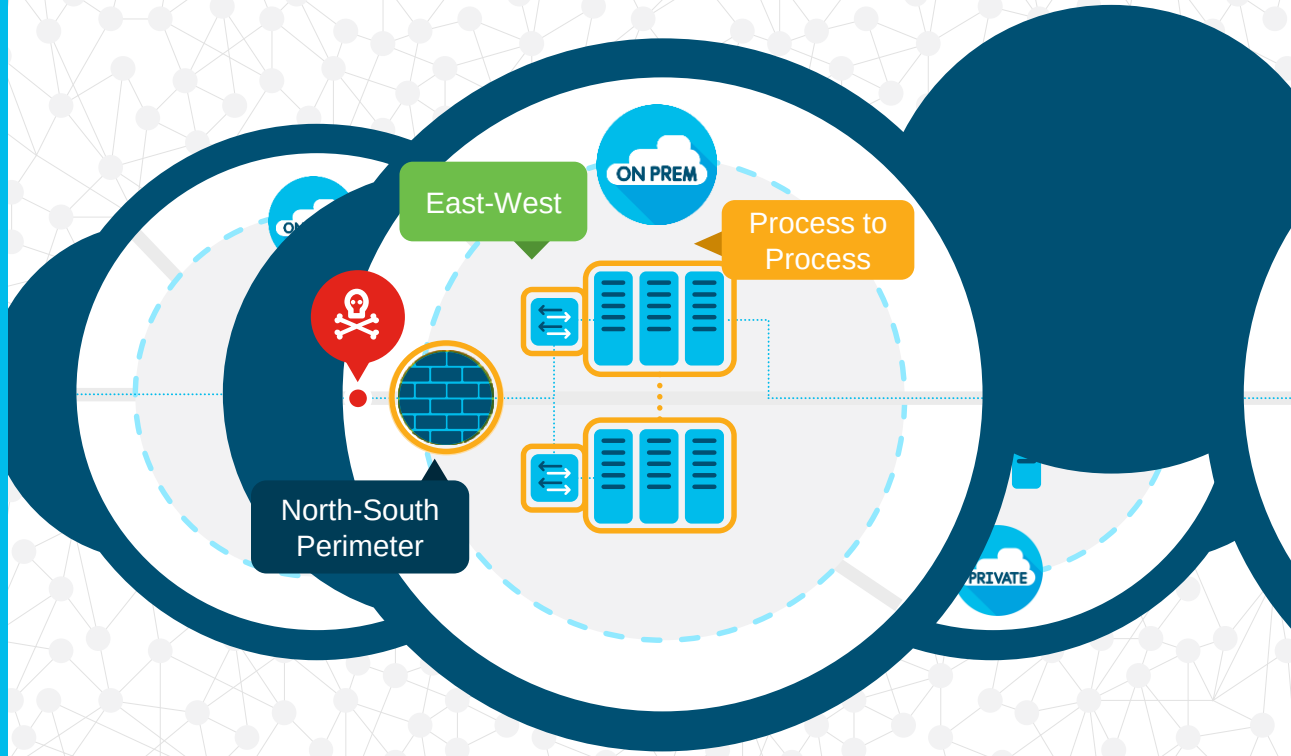


- Enterprise-wide network visibility across users, hosts, networks, and infrastructure (switches, routers, firewalls, servers)
- Collects network flow and other data to provide network visibility for understanding network wide traffic and discover threats
- Real-time situational awareness of users, devices, and applications
- Network flow monitoring of policy violations validates enterprise-wide network access to facilitate compliance and segmentation requirements

01 02 03

Segmentation:
Reduce the Attack Surface

- Cisco NGFW
- Cisco ACI
- Cisco Tetration



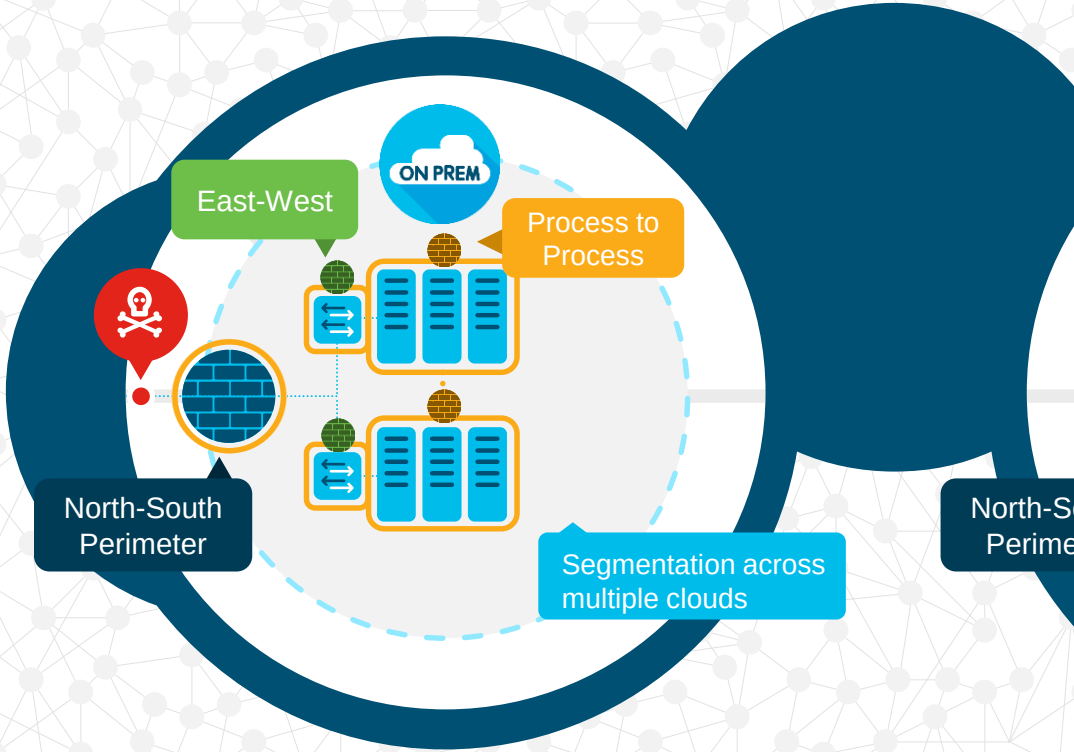
01 02 03

Segmentation:
Reduce the Attack Surface

Cisco NGFW

Cisco ACI

Cisco Tetration



01 02 03

Threat Protection: Stop the Breach

By strategically deploying threat sensors north-south, east-west

Multi-Layered Threat Sensors

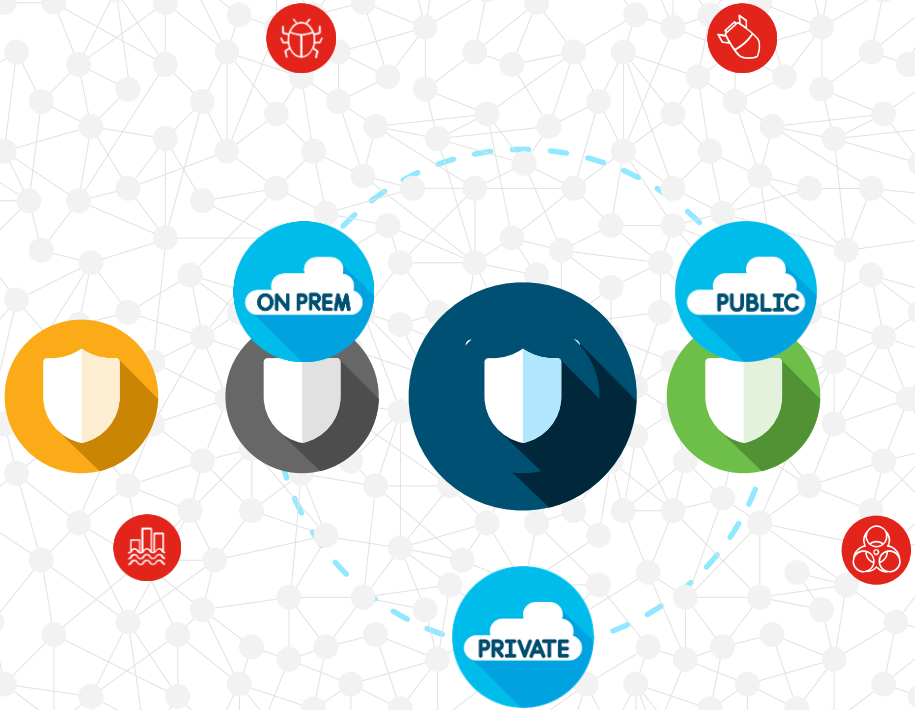
Quickly detect, block, and respond dynamically when threats arise to prevent breaches from impacting the business

Cisco ACI

Cisco Tetration

01 02 03

Protect the Workload Everywhere



Cisco Data Center Security Offers

Visibility

Network and application analytics

- Stealthwatch
- Tetration

Segmentation

Firewalls and application segmentation

- NGFW
- ACI
- Tetration

Threat prevention

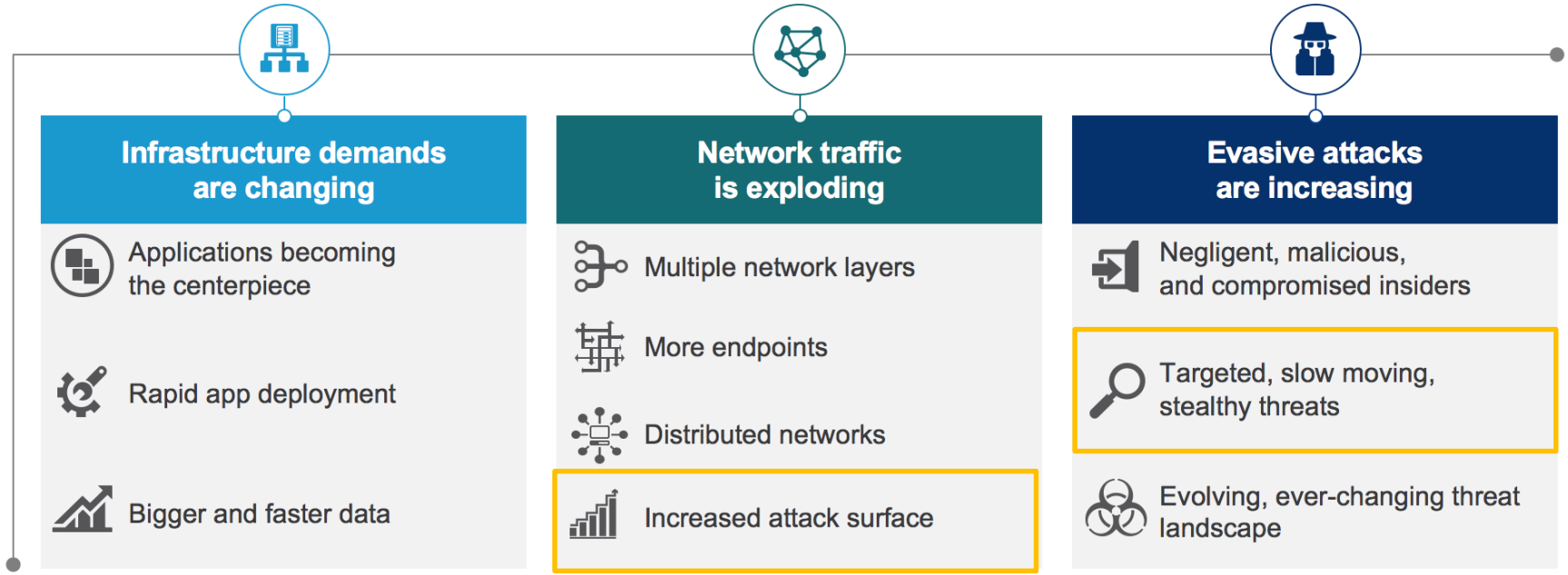
Threat detection, blocking, and automated response

- NGFW, NGIPS, & AMP
- Stealthwatch
- Tetration & ACI

Integrated

Visibility

Visibility challenges in the Data Centre



The 360º Data Centre visibility Cisco provides

Improved application understanding

Increased visibility into data center and application activities

Simplified segmentation

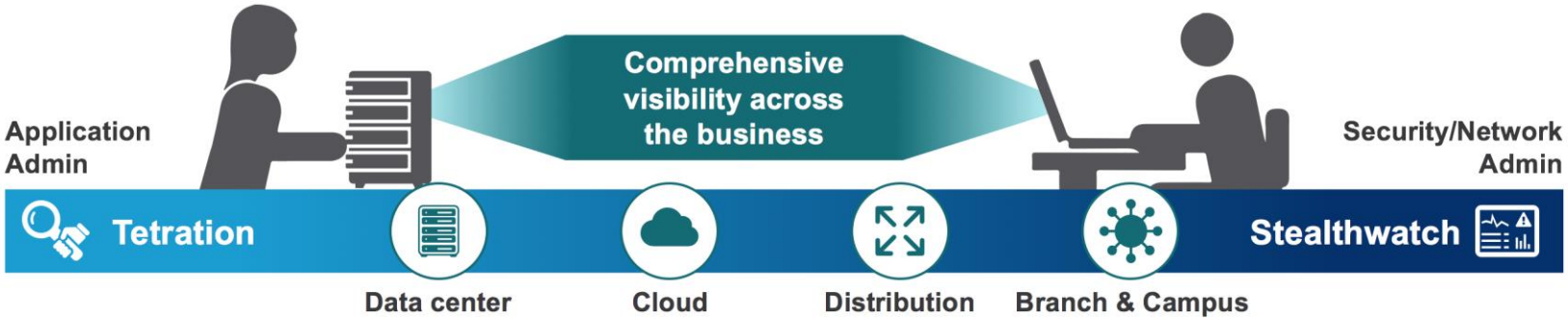
Improved compliance with application grouping and segmentation policies

Enhanced forensics

Faster forensics investigations using flow visibility

Faster threat detection

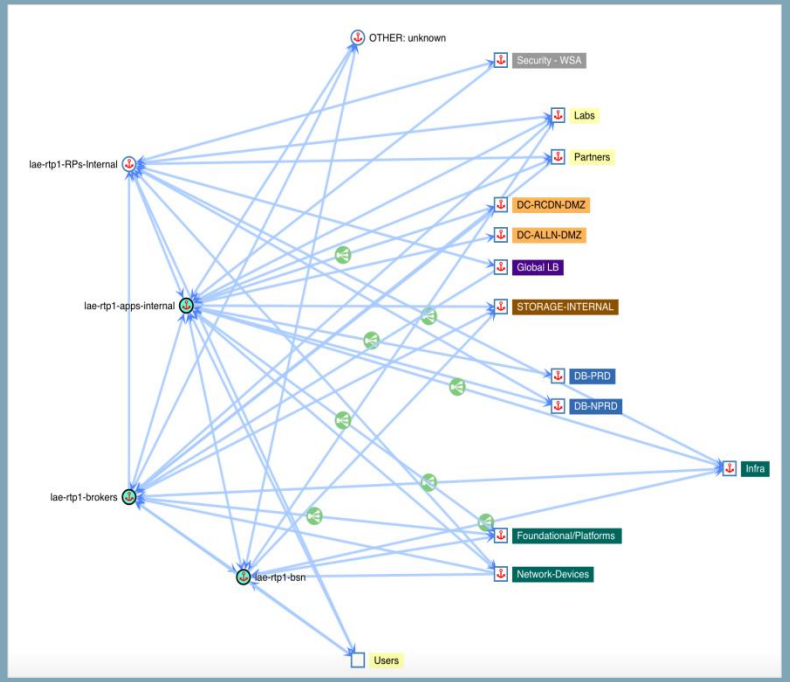
Centralized visibility and control across your entire business



What is really running on the network?

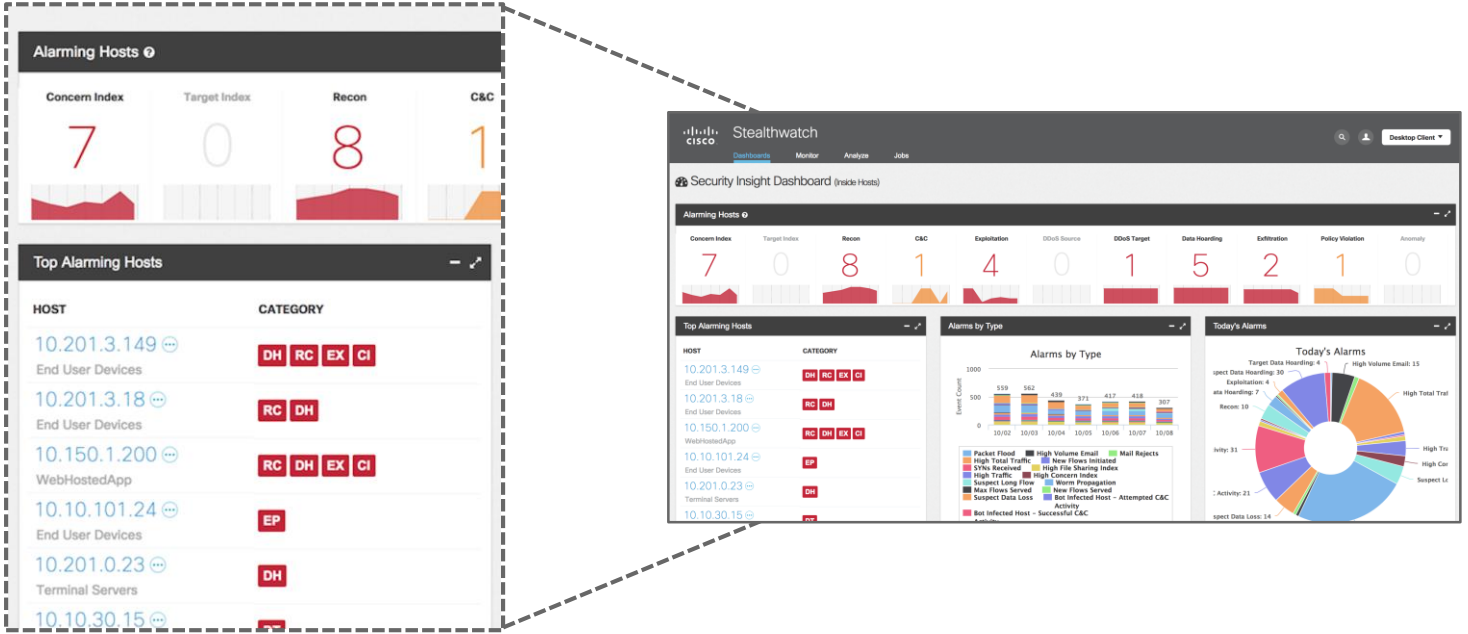
Cisco Tetration Analytics Application Insight—Dependency Map

Use Cisco Tetration Analytics™ outcome to generate white-list policies

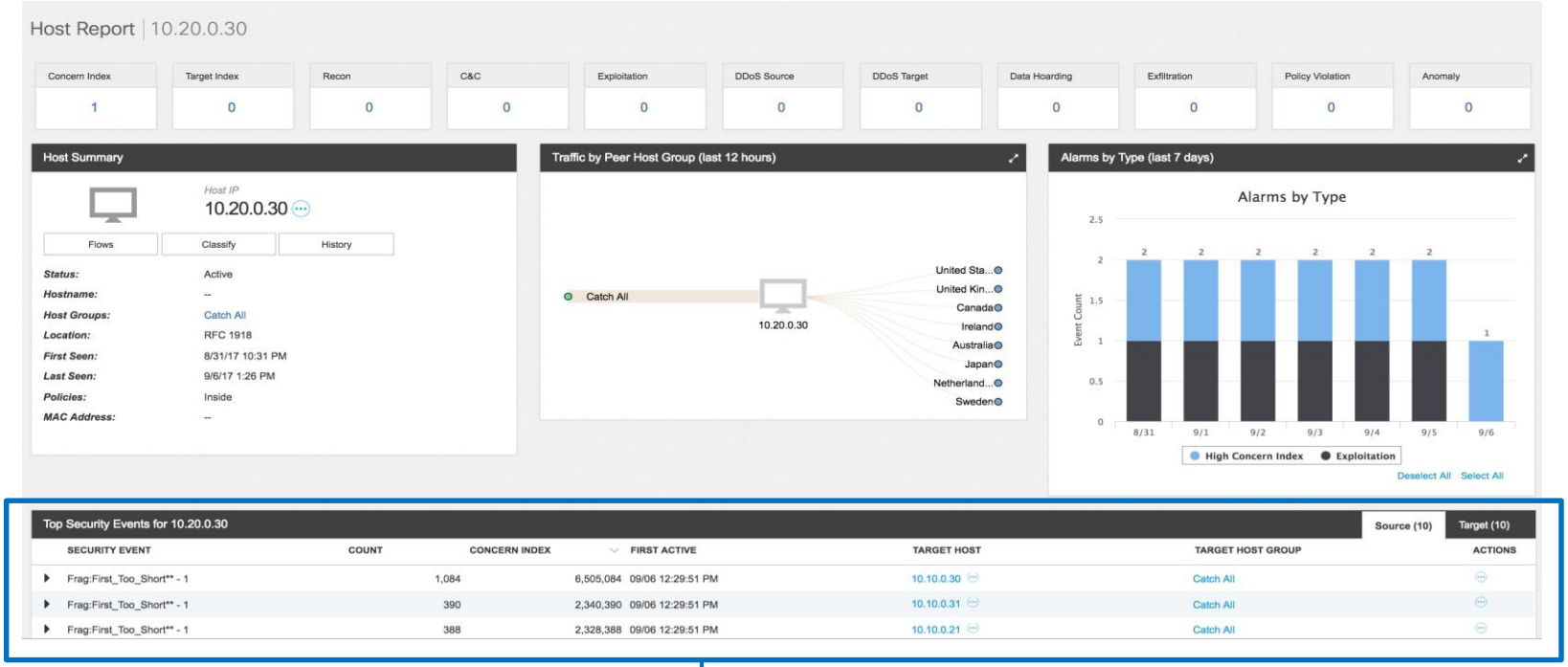


- (Service Owner)
- Service Category
- Service
- Service Offering
- Application
- Dependencies
- Security

Forensics & Incident Handling (Reactive)



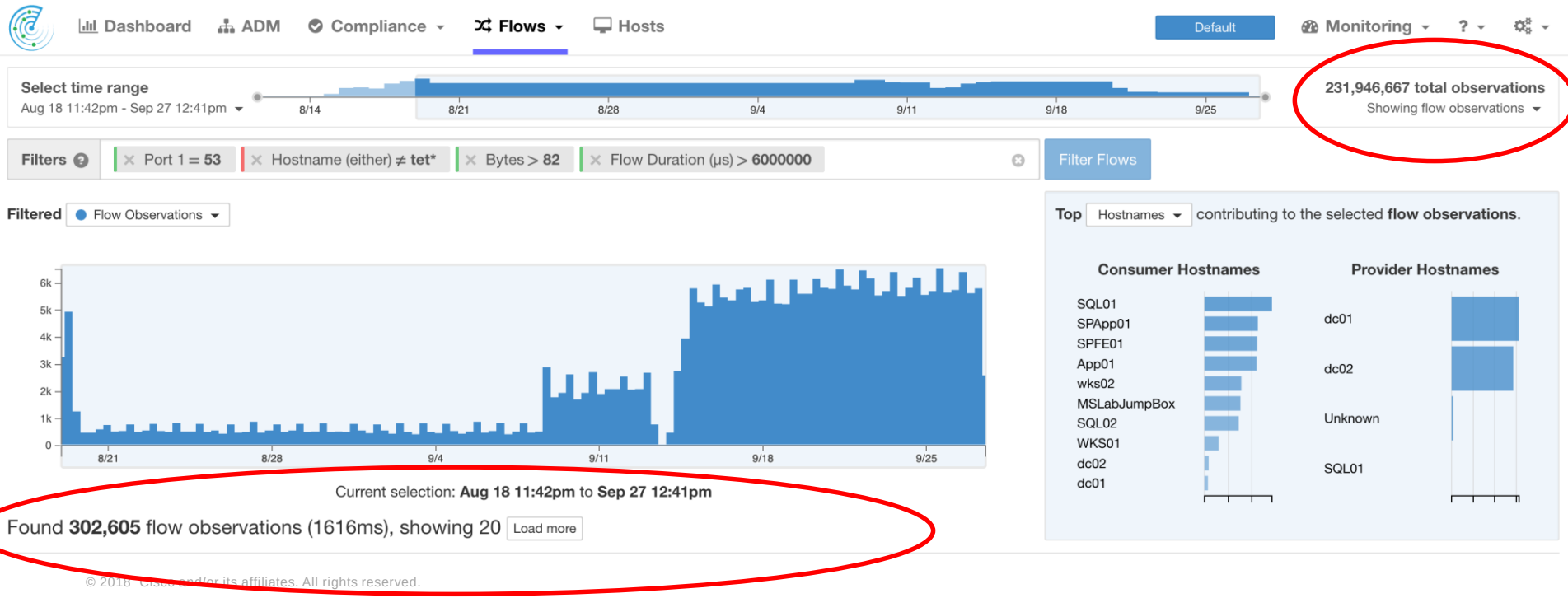
Forensic Detail (Collected & Correlated)



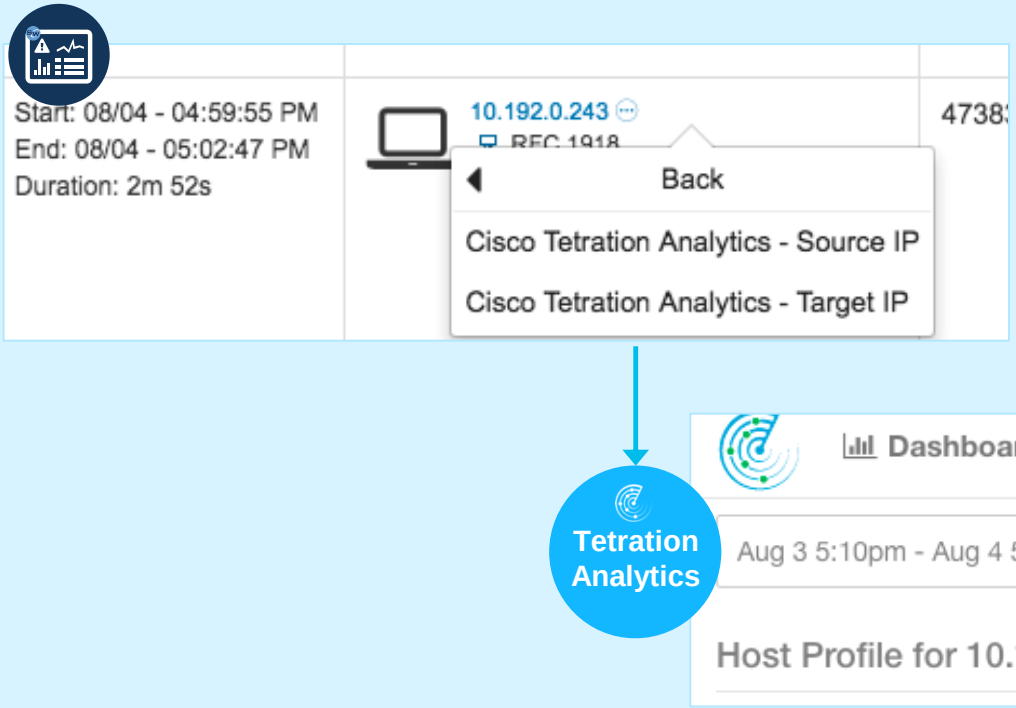
Host Report Security Events Widget

Tetration Threat Hunting (Pro-active)

Show all DNS traffic with packets larger then 82 bytes and a flow duration of greater then 6 secs.

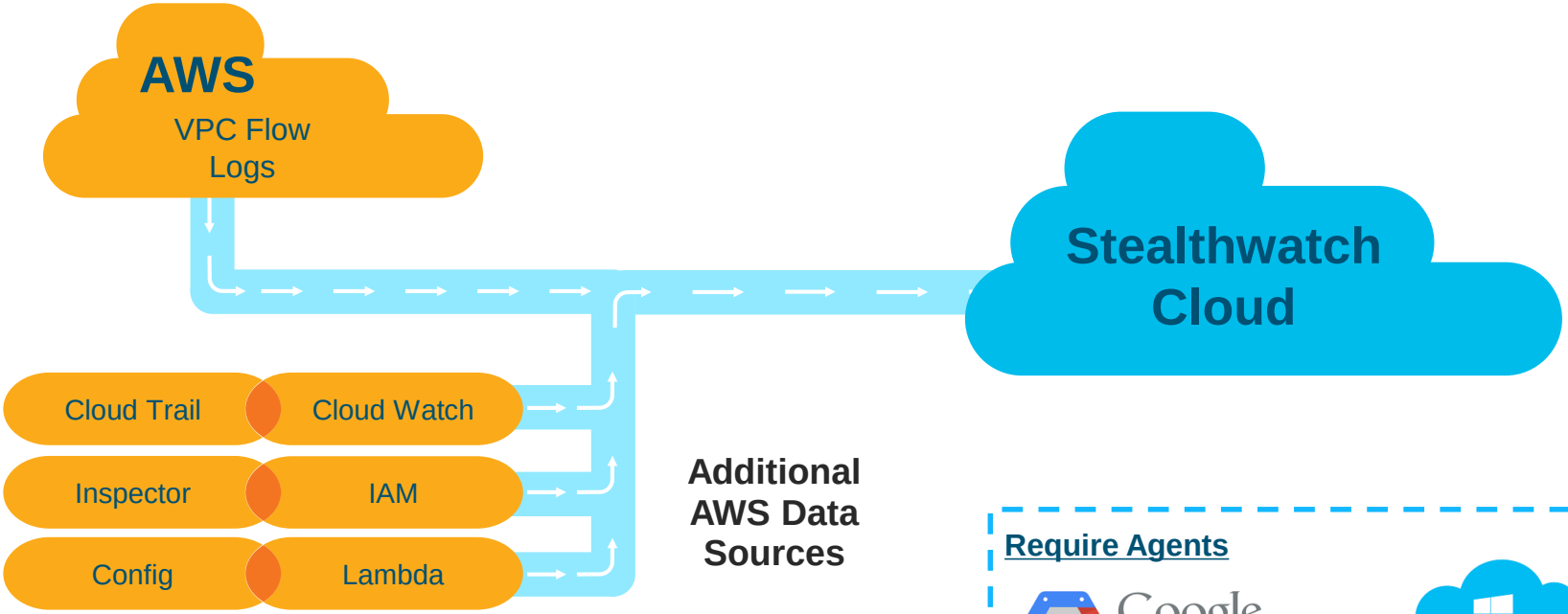


Stealthwatch & Tetration working together



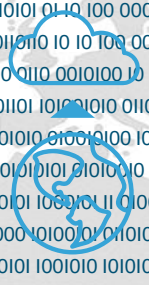
Pivot from Stealthwatch to Tetration interface during an investigation

See all public cloud activity through telemetry.



Global visibility like no one else….

TALOS



24 • 7 • 365 Operations

Cisco
Cognitive Threat Analytics (CTA)

AMP
Advanced Malware Protection

ThreatGRID
Malware Threat Intelligence Platform

Cisco Umbrella

STEALTH WATCH

Segmentation

Segmentation

ACCESS ALL AREAS

(Edge Security)

BUILDING ACCESS ONLY

(Segmentation)

ROOM ACCESS ONLY

(Micro-Segmentation)

ZERO TRUST

01 02 03

Segmentation:
State of the Market

Deep Dive

Application Segmentation

Powered by Tetration

Different, how exactly?

Next Generation Segmentation

Cisco ACI | Cisco NGFW | Cisco Tetration

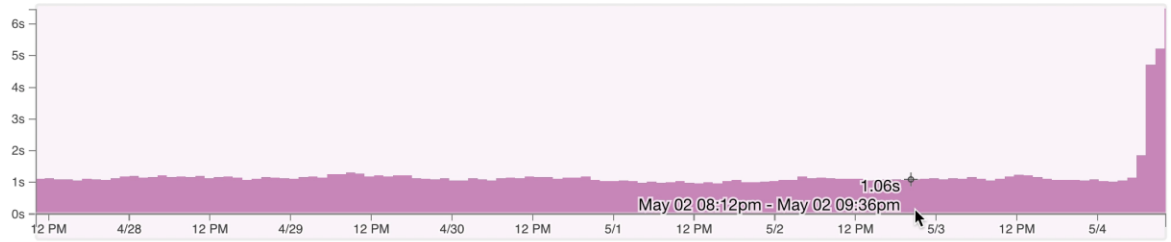
Dashboard | ADM | Flows | Hosts | Default | Monitoring | ? | ⚙

Select time range
Apr 27 10:09am - May 4 10:09am

1,621,596,002 total observations
Showing flow observations

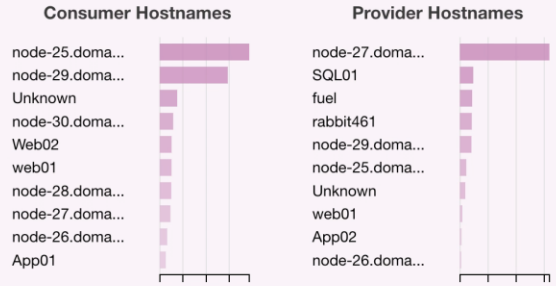
Filters | Enter attributes... | Filter Flows

Filtered Application Latency average



Current selection: **Apr 27 10:09am** to **May 4 10:09am**

Top Hostnames contributing to the selected **application latency**.



Found **42,405,981** flow observations (115ms), showing 20 Load more

Timestamp	Consumer Hostname	Consumer Address	Consumer Port	Provider Hostname	Provider Address	Provider Port	Protocol	Flow Type	Flow Start Time	Fwd Packets	Re
Apr 27 10:09:00am	tet-14.internal	172.26.46.37	0	Unknown	172.26.46.1	0	ICMP	IPv4	Apr 20 5:24:28am	2	
Apr 27 10:09:00am	node-27.domain.tld	192.168.0.4	56281	node-25.domain.tld	192.168.0.6	80 (HTTP)	TCP	IPv4	Apr 27 10:09:21am	6	
Apr 27 10:09:00am	node-27.domain.tld	192.168.1.2	37897	node-25.domain.tld	192.168.1.4	6000	TCP	IPv4	Apr 27 10:09:05am	6	
Apr 27 10:09:00am	node-25.domain.tld	192.168.1.4	40921	node-27.domain.tld	192.168.1.2	6001	TCP	IPv4	Apr 27 10:09:39am	6	
Apr 27 10:09:00am	web01	7.0.0.41	63421	tet-11.internal	172.26.46.33	5640	TCP	IPv4	Apr 25 6:20:01am	20	
Apr 27 10:09:00am	cloudcenteramqp4.6.1.novalocal	192.168.111.13	34930	tet-8.internal	172.26.46.30	5640	TCP	IPv4	Apr 25 6:20:13am	4	
Apr 27 10:09:00am	Unknown	240.0.0.2	36835	node-29.domain.tld	192.168.0.3	9191	TCP	IPv4	Apr 27 10:09:36am	0	
Apr 27 10:09:00am	Web02	7.0.0.42	58447	Unknown	7.0.0.13	88	TCP	IPv4	Apr 27 10:09:59am	5	

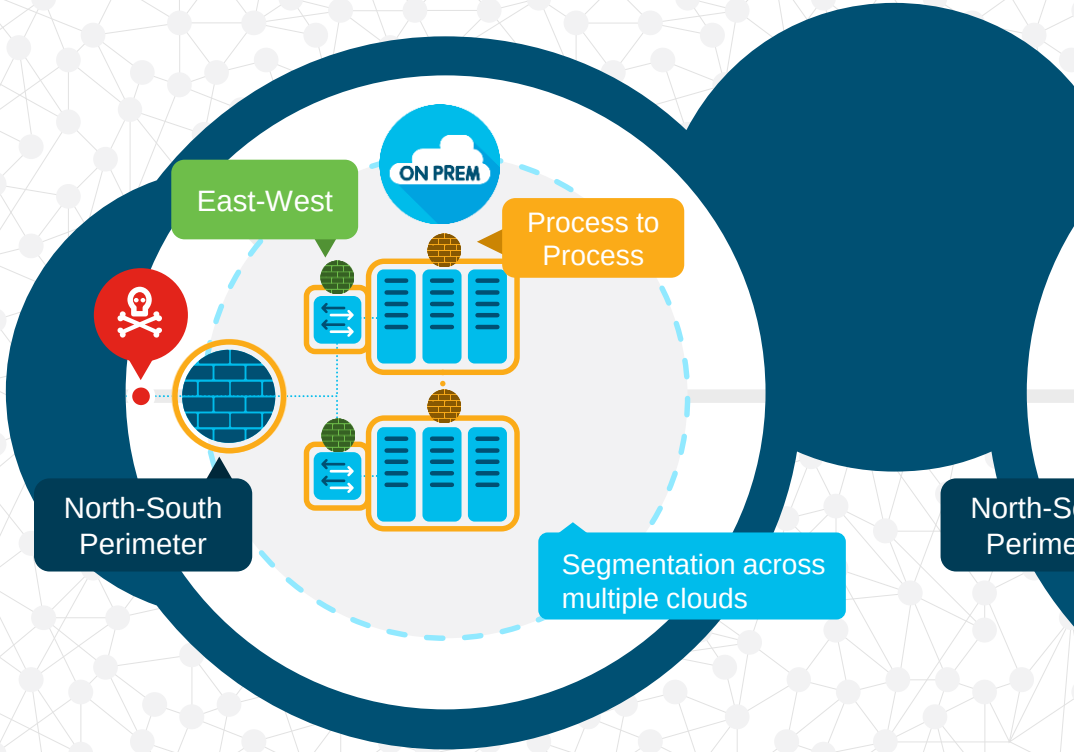
01 02 03

Segmentation:
Reduce the Attack Surface

Cisco NGFW

Cisco ACI

Cisco Tetration



01 02 03

Threat Protection: Stop the Breach

By strategically deploying threat sensors north-south, east-west

Multi-Layered Threat Sensors

Quickly detect, block, and respond dynamically when threats arise to prevent breaches from impacting the business

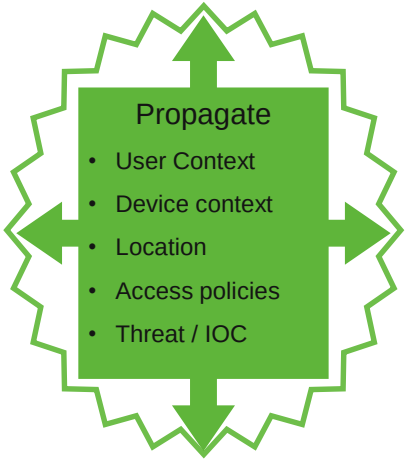
Dynamic Access Control with open framework

Pervasive Enforcement with NGFW + Identity Services Engine (ISE)

ISE + NGFW

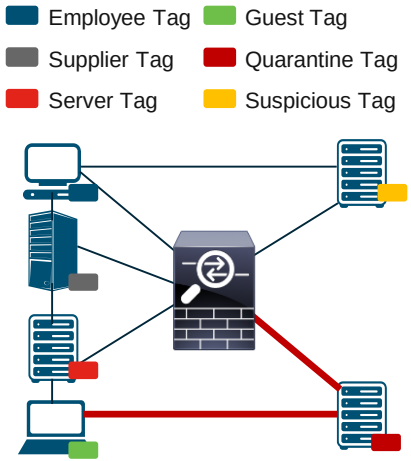
Set access control policies

pxGrid



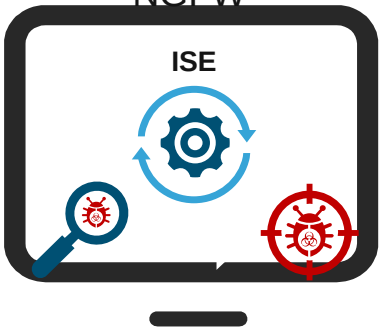
Propagate rules and context

TrustSec + NGFW



Establish a secure network

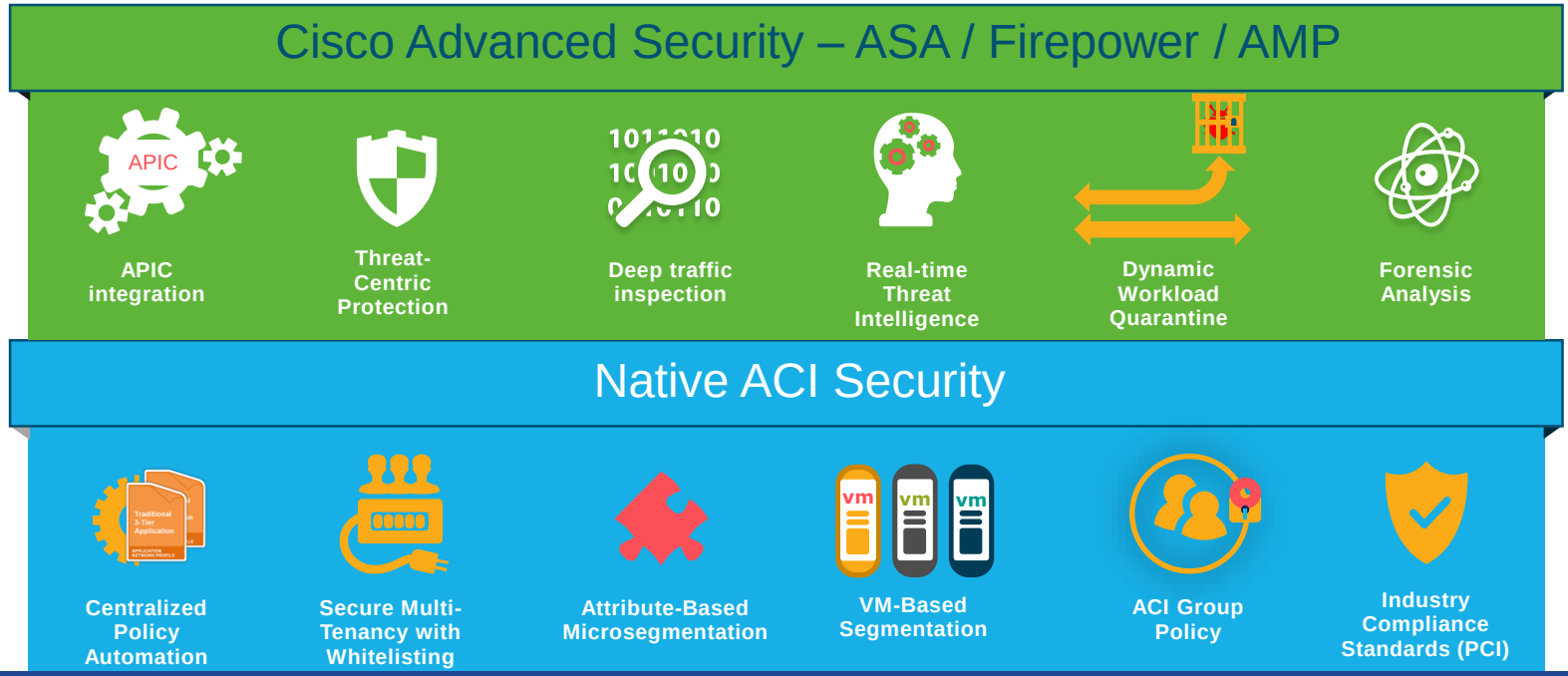
ISE + pxGrid + TrustSec + NGFW



Policy automation

Remediate breaches automatically

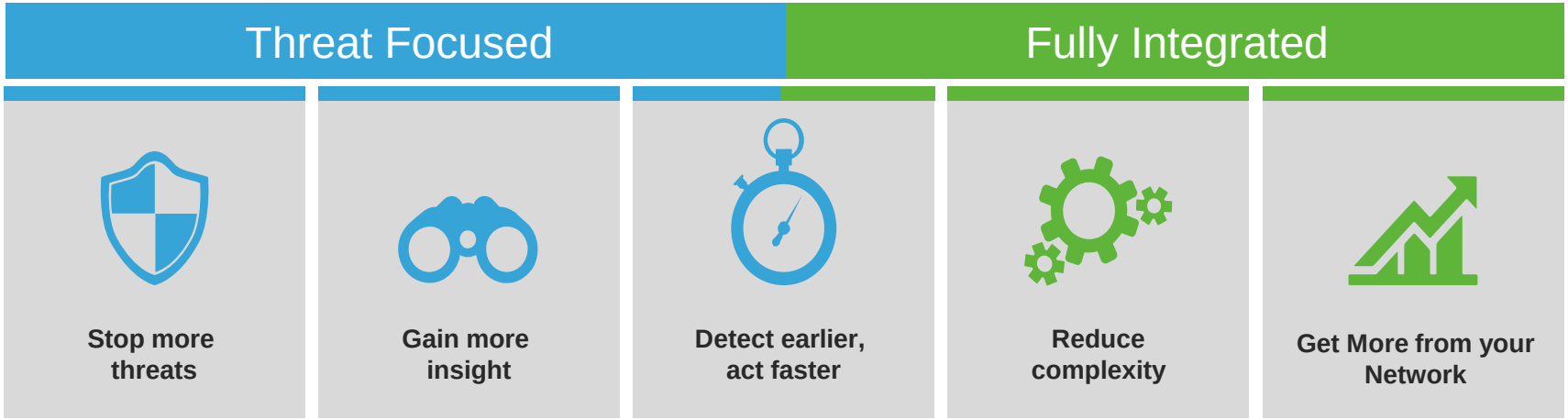
Cisco ACI and Advanced Security



Cisco ACI + Cisco Advanced Security Advantages:

- Addresses key DC challenges: threat-centric, visibility, compliance
- The only approach with kill chain approach to the threat lifecycle
- Industry's most comprehensive threat intelligence with TALOS
- Pervasive security offering between on premise and cloud
- Elastic scale with pay-as-you-grow model

Only Cisco delivers



… superior protection and visibility to address new demands, more things, and specialized threats


CISCO