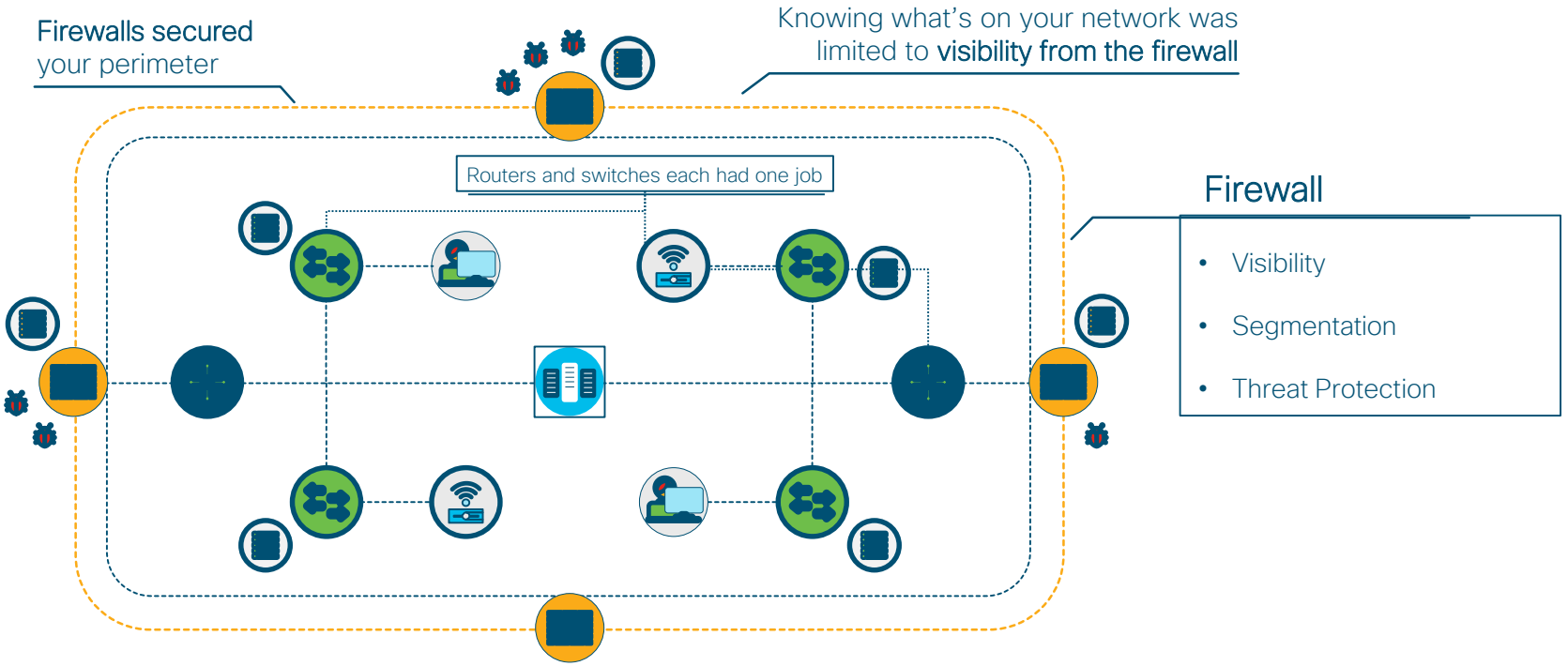
# Securing the Multicloud Gaining Full Visibility into Your Heterogeneous Environments

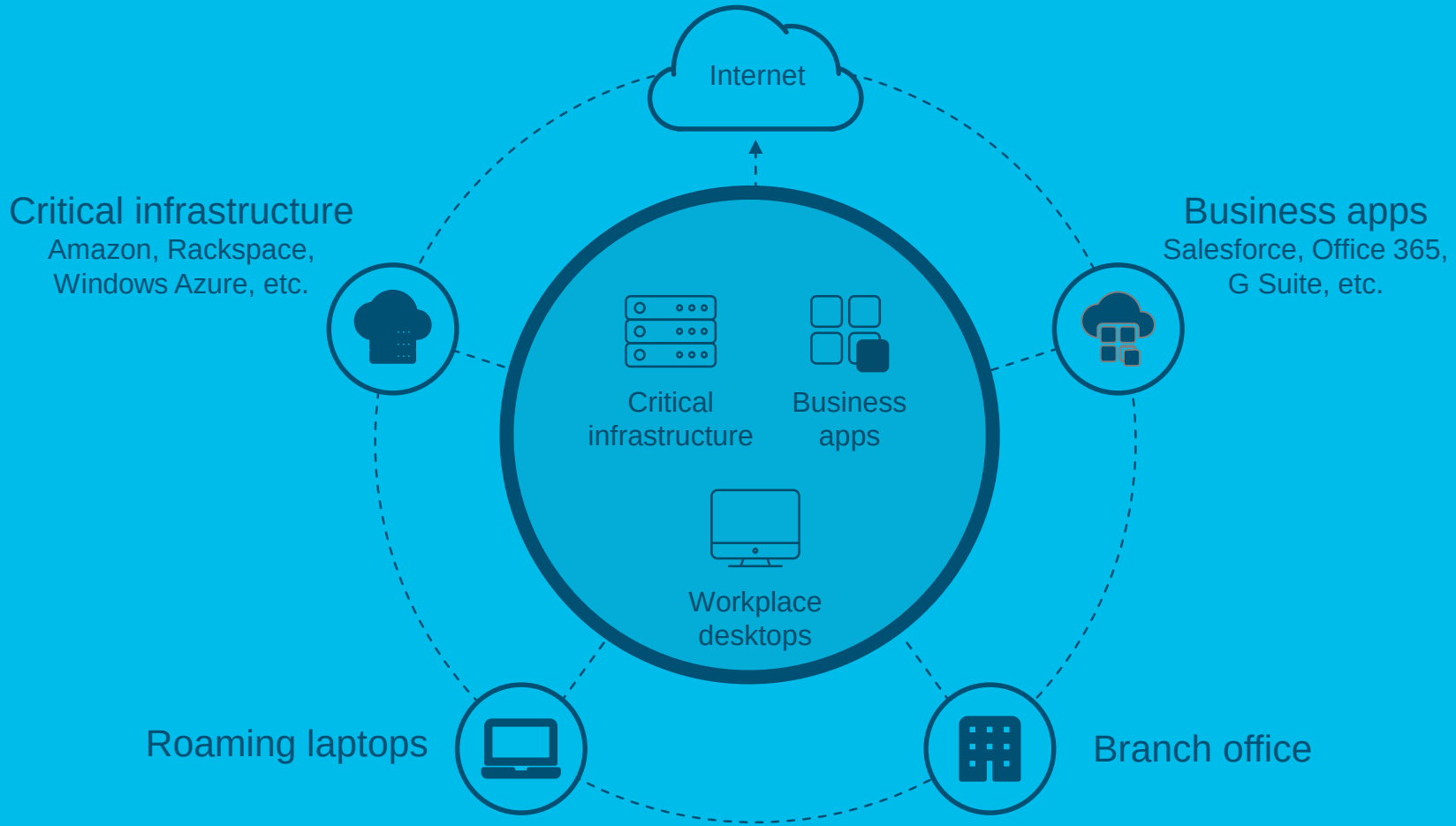
Derek Chia – Data Center Tetration lead

10 Jan 2019

# Yesterday's network security was about the perimeter



# The way we work has changed



# The Modern Data Center is Complex

## Big and Fast Data

Virtualization

Expanded attack surface

Increase in east-west traffic


## Hybrid Cloud

Multi cloud orchestration

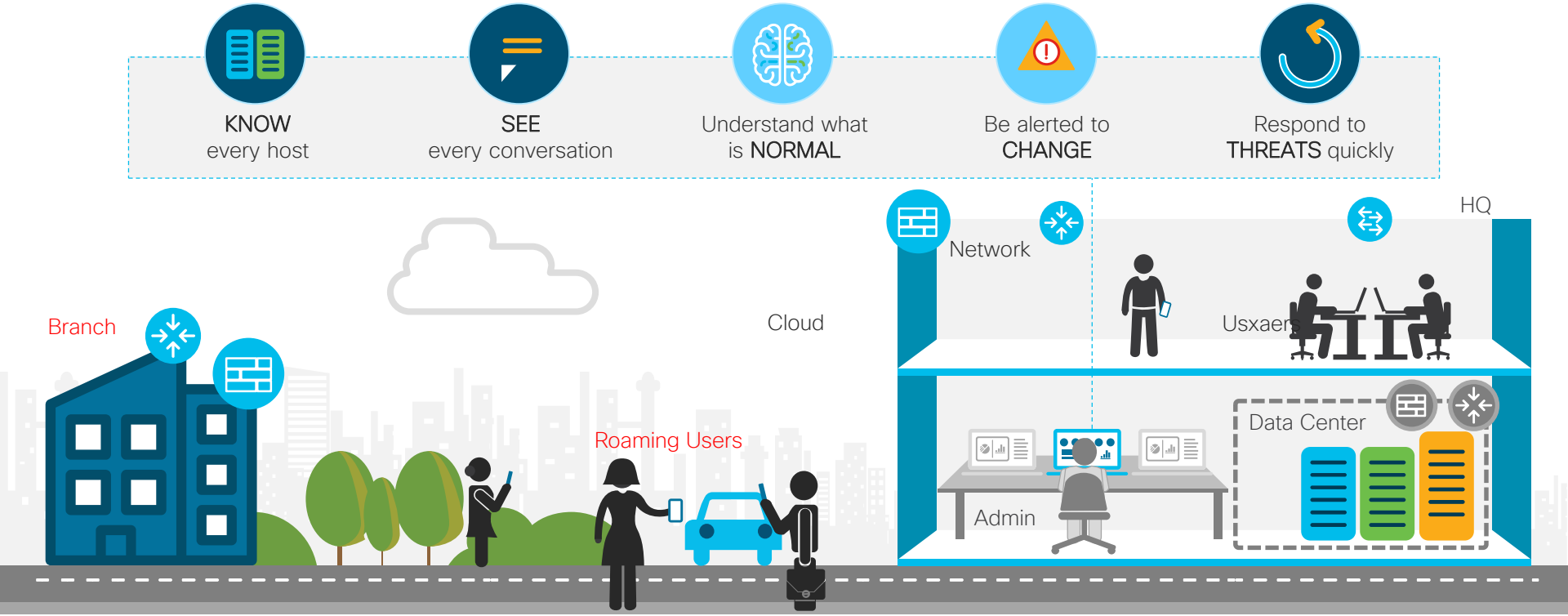
Workload portability

Zero trust model

## Application Architecture

Continuous development | Micro Services | APIs

# Effective security depends on total visibility



# National Security Agency (NSA) on securing your assets

1. When protecting your network, you have to **know everything that is going on.**

2. Decrease attack surface. **Lock down and disable services you are not using**.

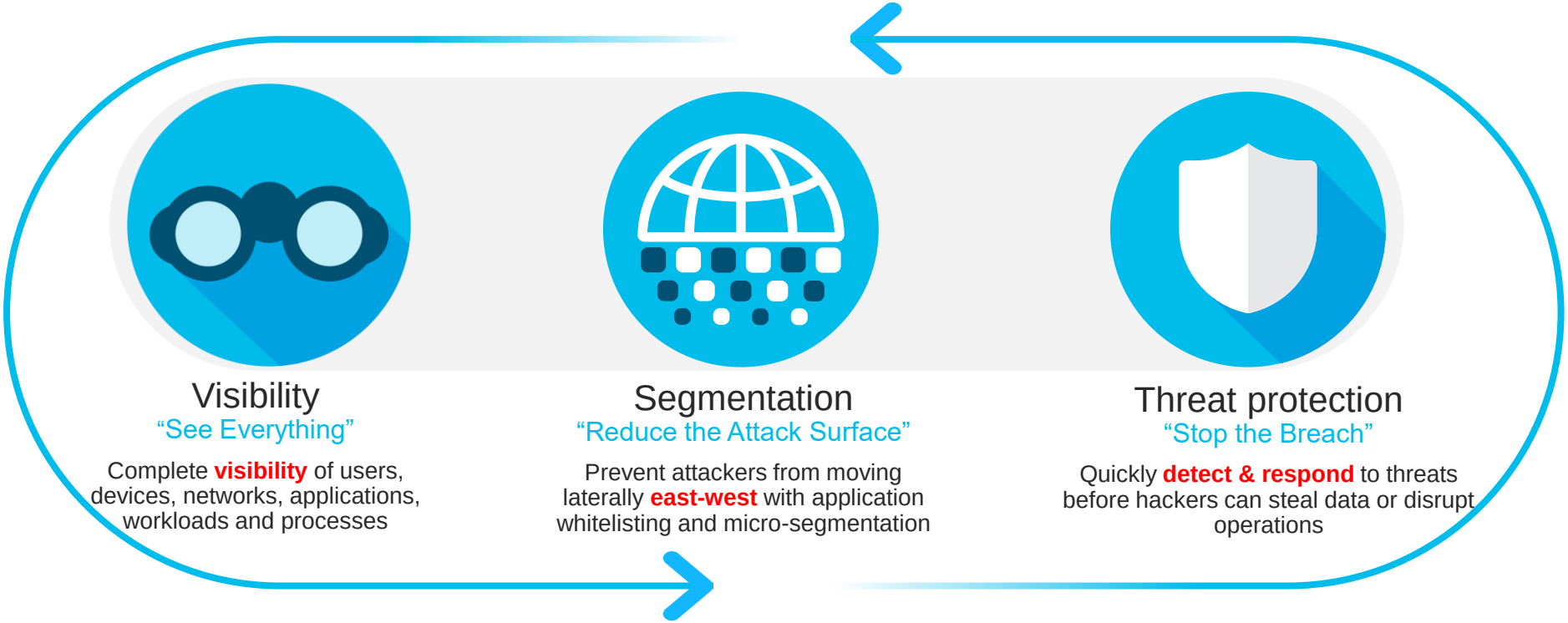
3. Identify what is routine in your infrastructure and what is not. **Monitor for deviations**.

4. **Whitelisting** is a must in today's cyber security world

"If you really want to protect your network you have to know your network, including all the devices and technology in it," he said. "In many cases we know networks better than the people who designed and run them."

Usenix Enigma 2016 https://www.youtube.com/watch?v=bDJb8WOJYdA
Rob Joyce, Tailored Access Operations, NSA
https://techtalk.pcpitstop.com/2016/09/07/nsa-best-practices-whitelisting/
https://www.theregister.co.uk/2016/01/28/nsas_top_hacking_boss_explains_how_to_protect_your_network_from_his_minions/

# Cisco Data Center Security



## Visibility

"See Everything"

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

## Segmentation

"Reduce the Attack Surface"

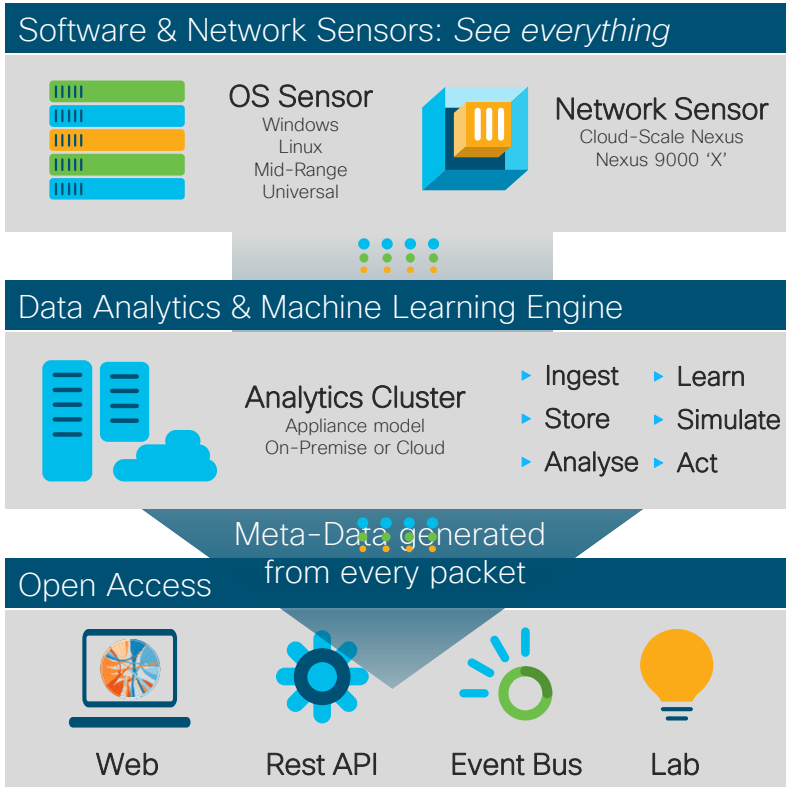
Prevent attackers from moving laterally **east-west** with application whitelisting and micro-segmentation

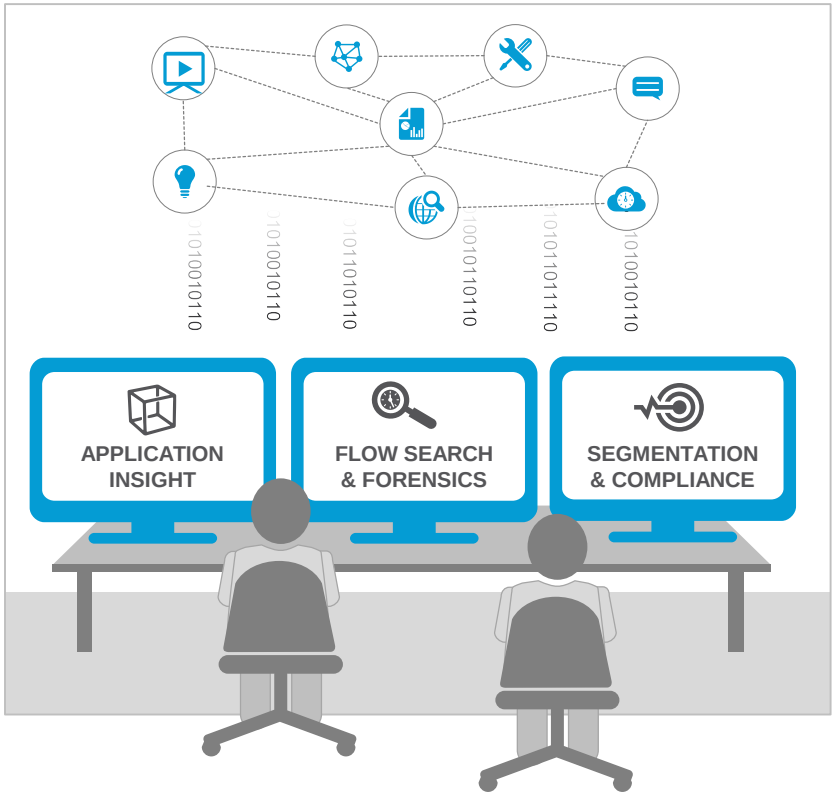
## Threat protection

"Stop the Breach"

Quickly **detect & respond** to threats before hackers can steal data or disrupt operations

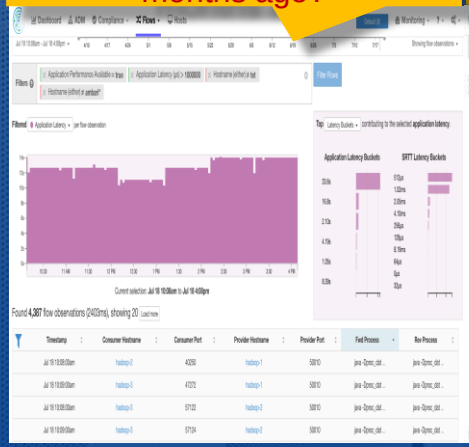
# Introducing Tetration



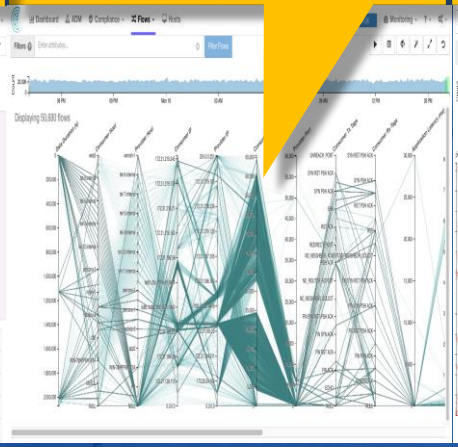



# Tetration with Machine Learning answers your Critical Questions

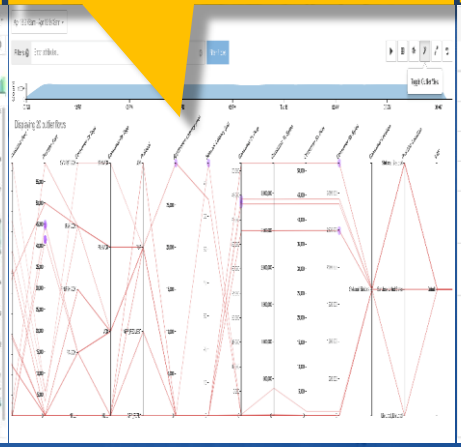
What's going on now and 6 months ago?



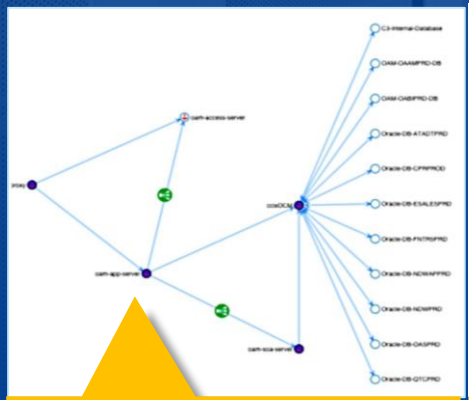
What's normal /Baseline?



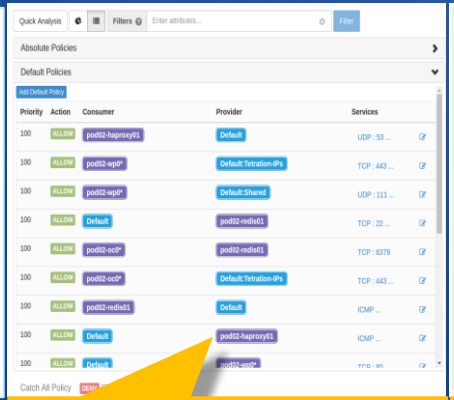
What's outlier?



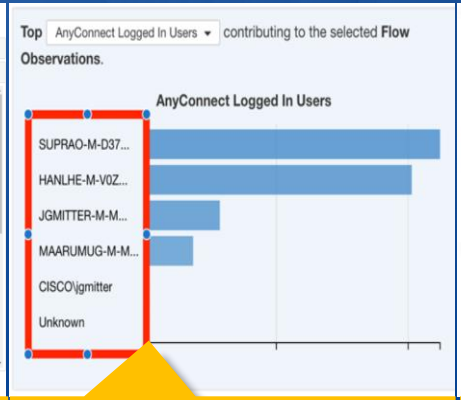
How to reduce MTTI?

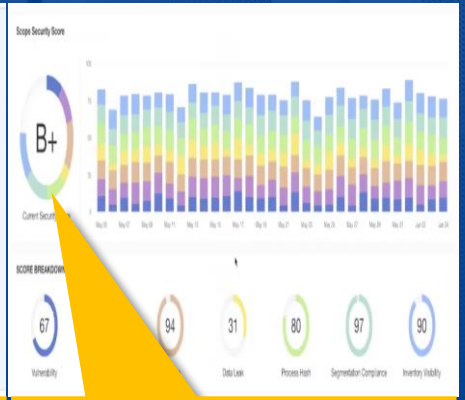
Who is talking to who for whitelist policy?



How to enforce policy to Multi-Cloud env.?



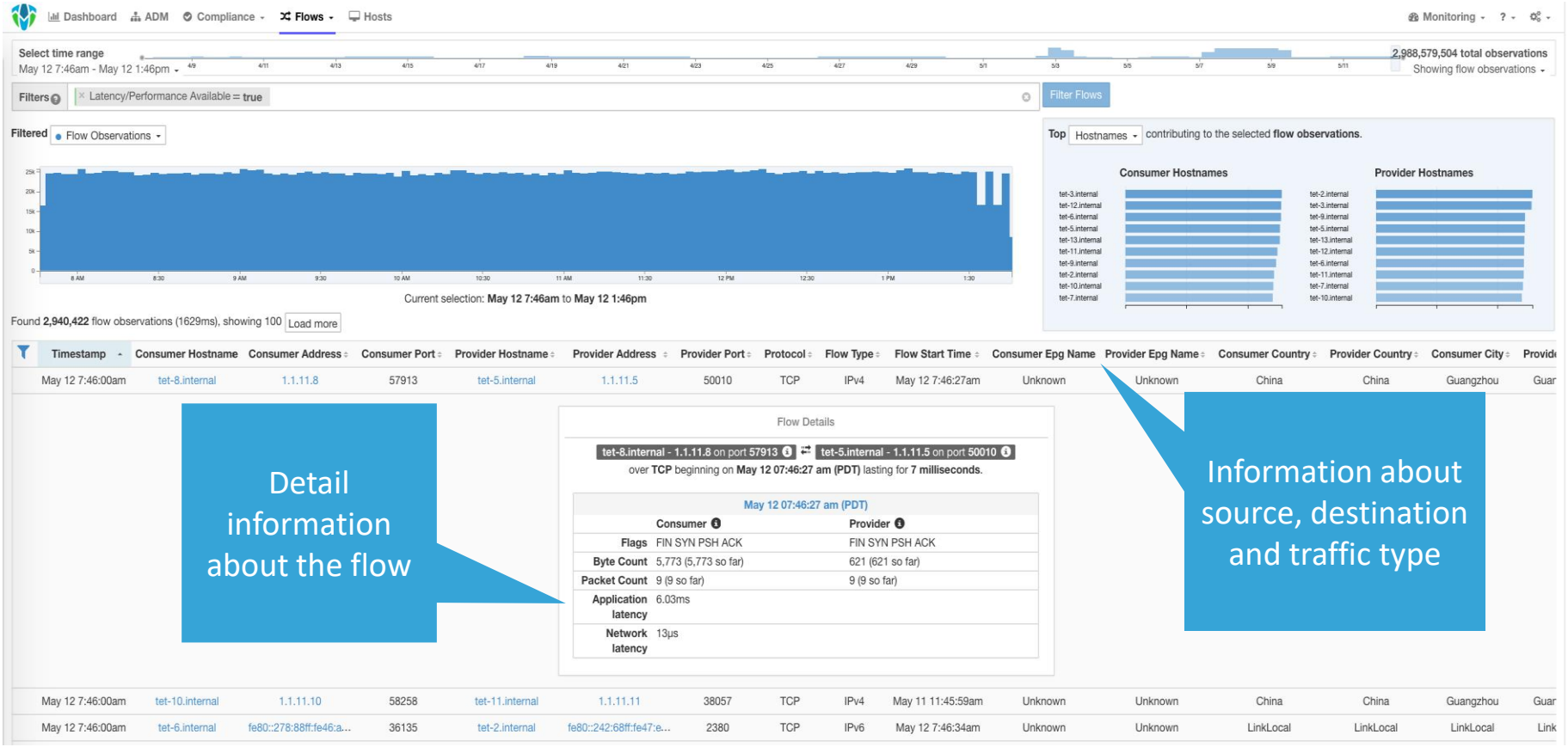

Multi-Cloud End point/client visibility?




What is my Cloud Security Grade?

# Example Use Case

# Forensics


Dashboard
ADM
Compliance
Flows
Hosts
Monitoring
Select time range
May 12 7:46am - May 12 1:46pm
2,988,579,504 total observations
Showing flow observations
Filters
Latency/Performance Available = true
Filter Flows
Filtered
Flow Observations
Current selection: May 12 7:46am to May 12 1:46pm
Found 2,940,422 flow observations (1629ms), showing 100
Load more
Top
Hostnames
contributing to the selected flow observations.
Consumer Hostnames
Provider Hostnames
Timestamp
Consumer Hostname
Consumer Address
Consumer Port
Provider Hostname
Provider Address
Provider Port
Protocol
Flow Type
Flow Start Time
Consumer Epg Name
Provider Epg Name
Consumer Country
Provider Country
Consumer City
May 12 7:46:00am tet-8.internal 1.1.11.8 57913 tet-5.internal 1.1.11.5 50010 TCP IPv4 May 12 7:46:27am Unknown Unknown China China Guangzhou
Flow Details
tet-8.internal - 1.1.11.8 on port 57913
tet-5.internal - 1.1.11.5 on port 50010
over TCP beginning on May 12 07:46:27 am (PDT) lasting for 7 milliseconds.
May 12 07:46:27 am (PDT)
Consumer
Provider
Flags FIN SYN PSH ACK FIN SYN PSH ACK
Byte Count 5,773 (5,773 so far) 621 (621 so far)
Packet Count 9 (9 so far) 9 (9 so far)
Application latency 6.03ms
Network latency 13µs
May 12 7:46:00am tet-10.internal 1.1.11.10 58258 tet-11.internal 1.1.11.11 38057 TCP IPv4 May 11 11:45:59am Unknown Unknown China China Guangzhou
May 12 7:46:00am tet-6.internal fe80::278:88ff:fe46:a... 36135 tet-2.internal fe80::242:68ff:fe47:e... 2380 TCP IPv6 May 12 7:46:34am Unknown Unknown LinkLocal LinkLocal LinkLocal
Detail information about the flow
Information about source, destination and traffic type

# Zero-Trust Policy Lifecycle

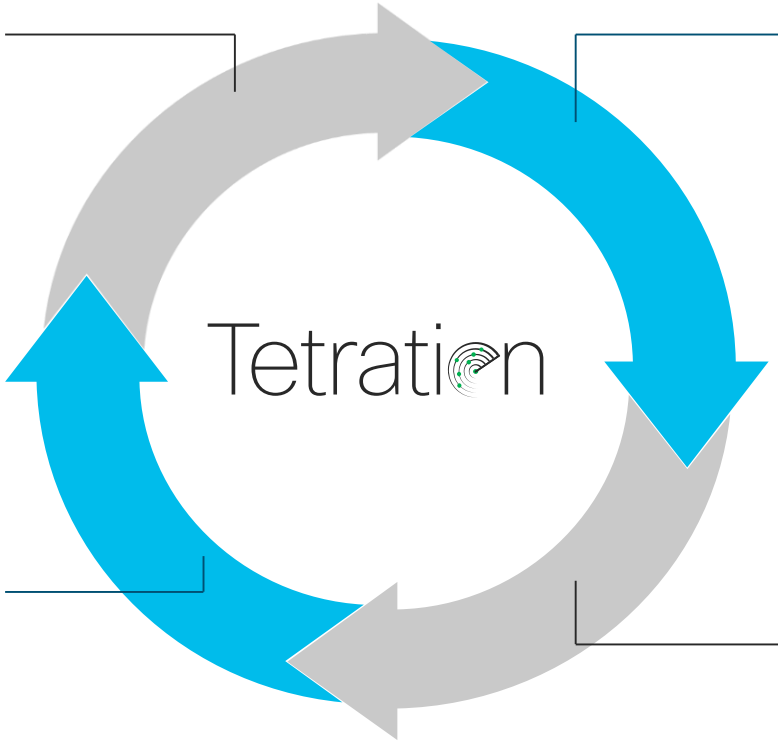
Cisco Tetration™ with Intel® Xeon® Platinum processor

**Discover** and **Map** all applications and dependencies

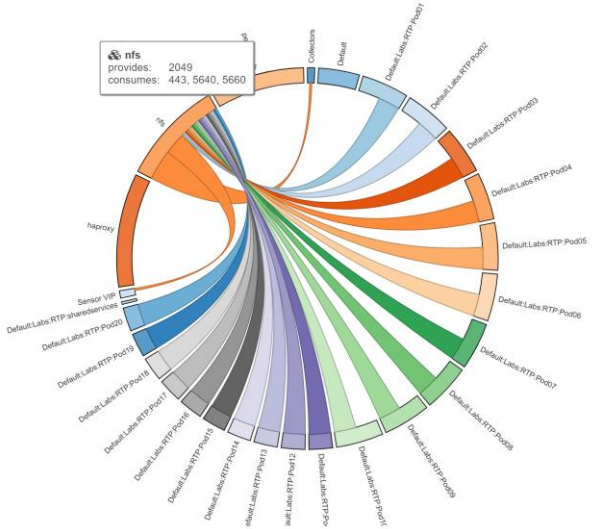
**Create** and test segmentation and security policy

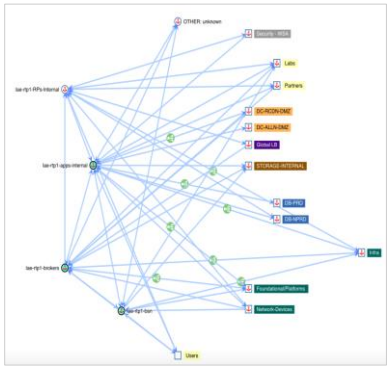
**Enforce** policy across public and private cloud applications

Monitor for compliance and remediate



# Discovery, Map and automatic policy creation



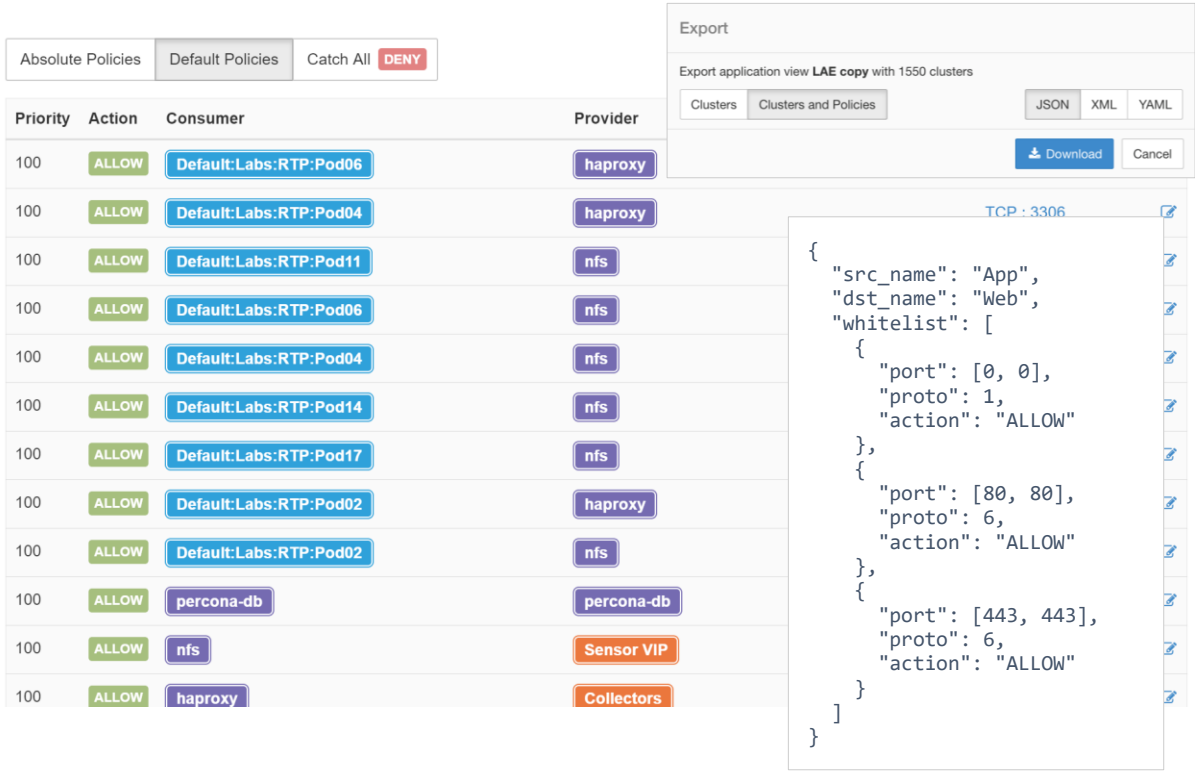
Absolute Policies | Default Policies | Catch All DENY

+ Add Default Policy

| Priority | Action | Consumer | Provider | Services |
|---|---|---|---|---|
| 100 | ALLOW | Default:Labs:RTP:Pod06 | haproxy | TCP : 3306 |
| 100 | ALLOW | Default:Labs:RTP:Pod04 | haproxy | TCP : 3306 |
| 100 | ALLOW | Default:Labs:RTP:Pod11 | nfs | TCP : 2049 |
| 100 | ALLOW | Default:Labs:RTP:Pod06 | nfs | TCP : 2049 |
| 100 | ALLOW | Default:Labs:RTP:Pod04 | nfs | TCP : 2049 |
| 100 | ALLOW | Default:Labs:RTP:Pod14 | nfs | TCP : 2049 |
| 100 | ALLOW | Default:Labs:RTP:Pod17 | nfs | TCP : 2049 |
| 100 | ALLOW | Default:Labs:RTP:Pod02 | haproxy | TCP : 3306 |
| 100 | ALLOW | Default:Labs:RTP:Pod02 | nfs | TCP : 2049 |
| 100 | ALLOW | percona-db | percona-db | TCP : 4567 ... |
| 100 | ALLOW | nfs | Sensor VIP | TCP : 443 |
| 100 | ALLOW | haproxy | Collectors | TCP : 5640 ... |

Zero Trust Policy Dynamically Discovered

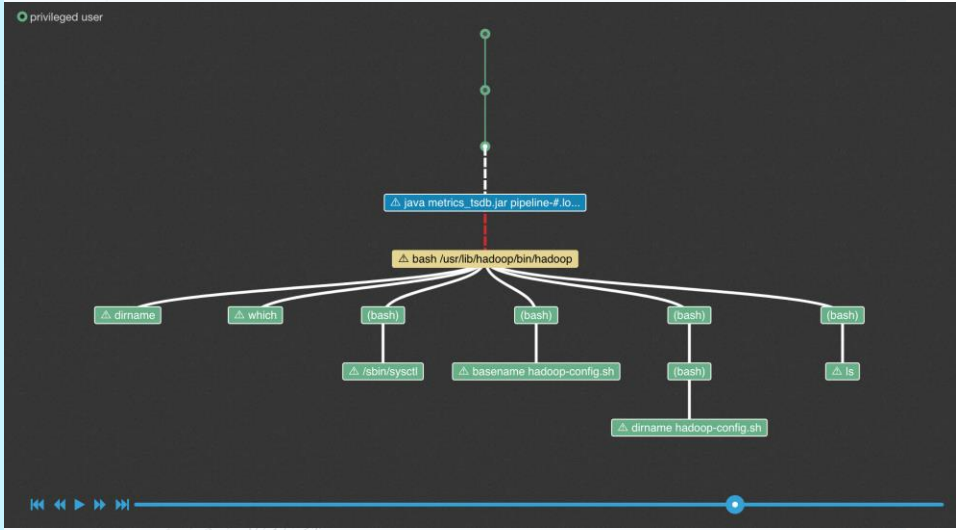
# Discovery, Map and automatic policy creation



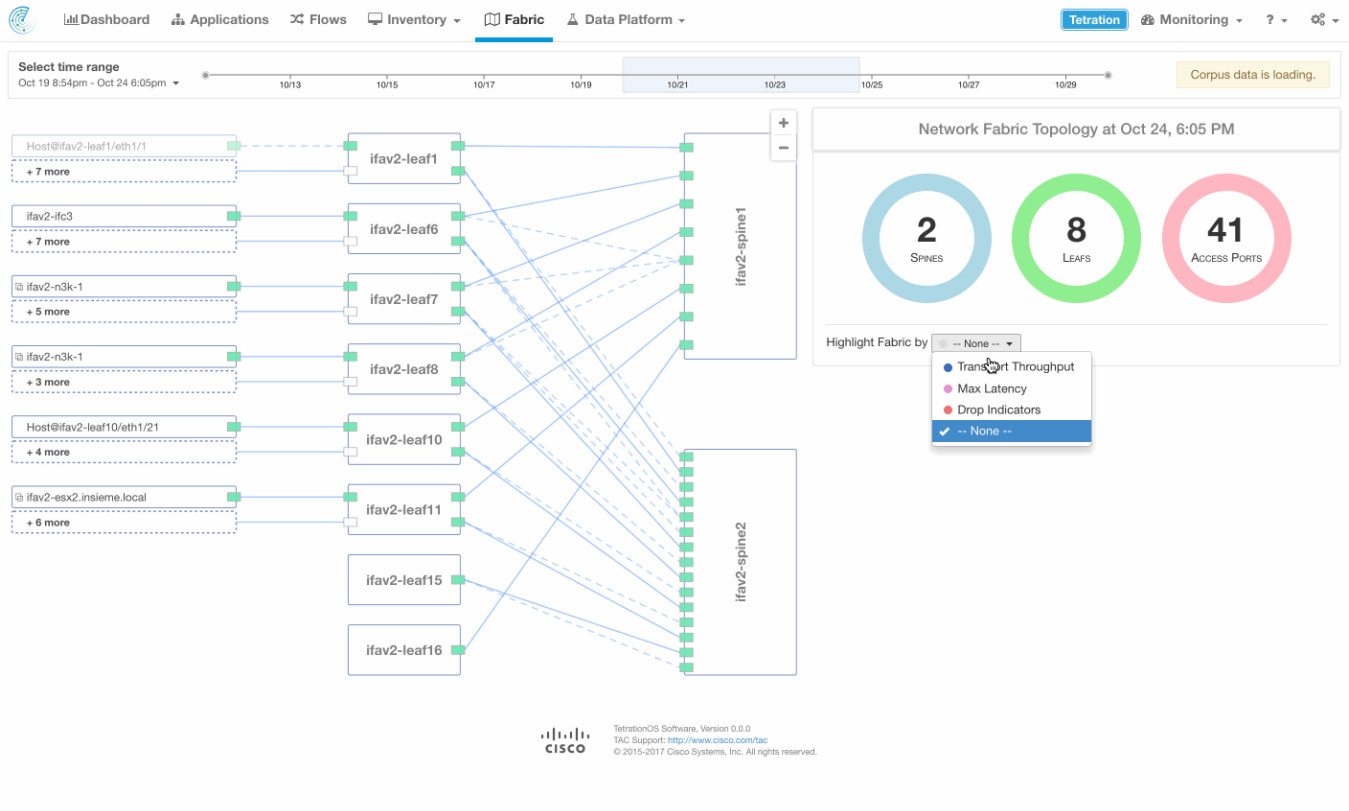
# Cloud Workload protection

Process baseline and behavior analysis

- Gain visibility into critical activities of a process: **Detect and alert** when a particular process deviates from its **normal** behavior
- Automatically **detect suspicious behavior** based on process behavior deviations
- **Proactive analysis**: Quickly search and visualize process tree and timelines to identify threats
- **See** what happened at each stage of the attack: Full time-series view of process hierarchy and behavior changes



# Discovering Important Fabric Links



# Cisco Tetration Analytics: Ecosystem

Cisco Tetration™ with Intel® Xeon® Platinum processor

**Cisco Tetration Analytics™**

## Application Dependency

servicenow

## Layer4-7 Services

f5 CITRIX AVI Networks

## Enforcement

tufin algosec

## Visibility and Optimization

Vnomic Workloads Control Center for Hybrid Clouds™ turbonomic VEEAM

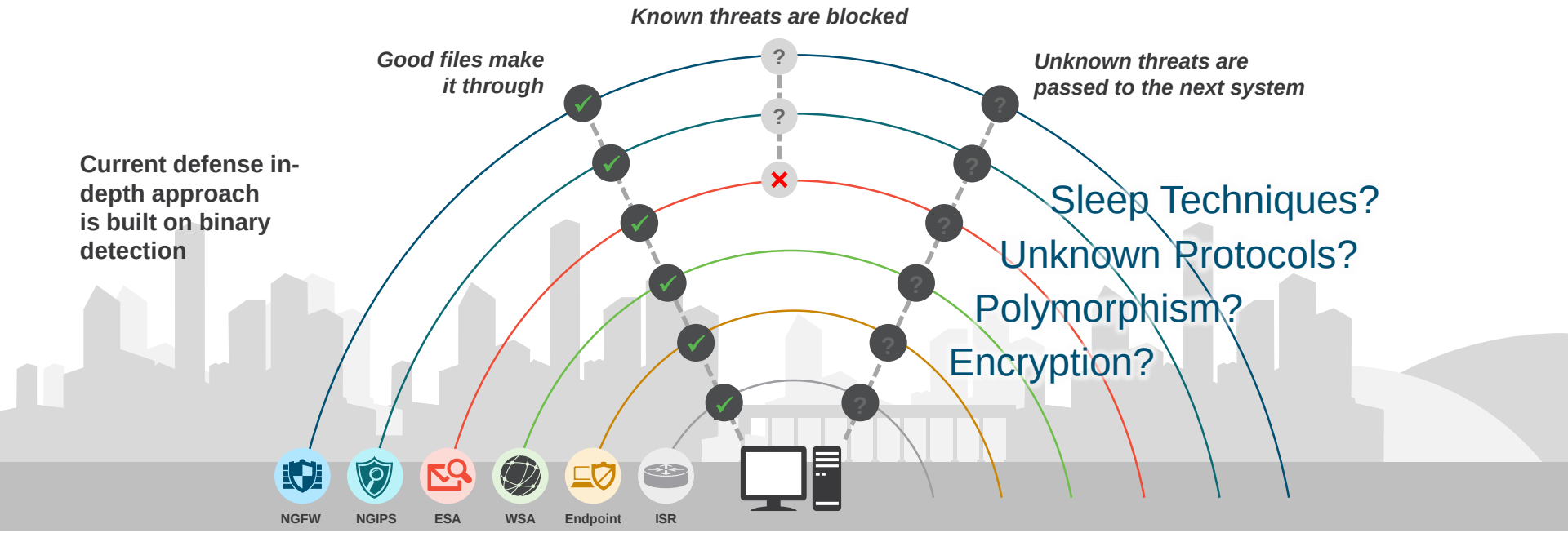
## Insight exchange

splunk> servicenow ExtraHop Corvil IBM Radar LogRhythm Infoblox

# Cisco Secure DC Architecture

## in summary

# It’s Impossible to Block 100% of Threats 100% of the Time

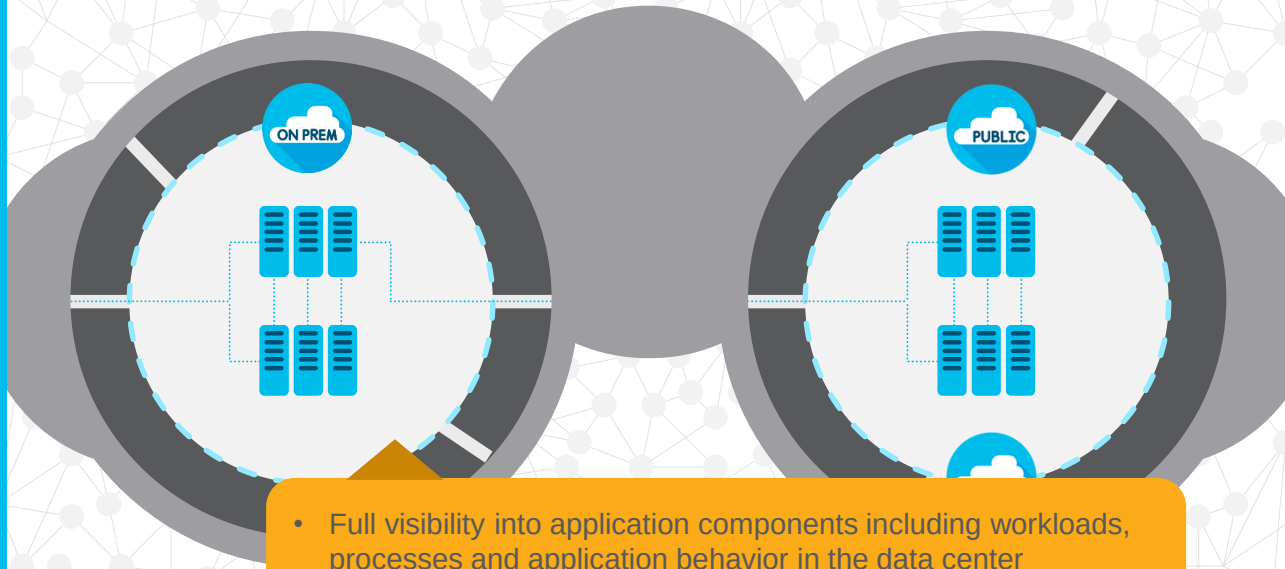



***Single points of inspection have their limitations***

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

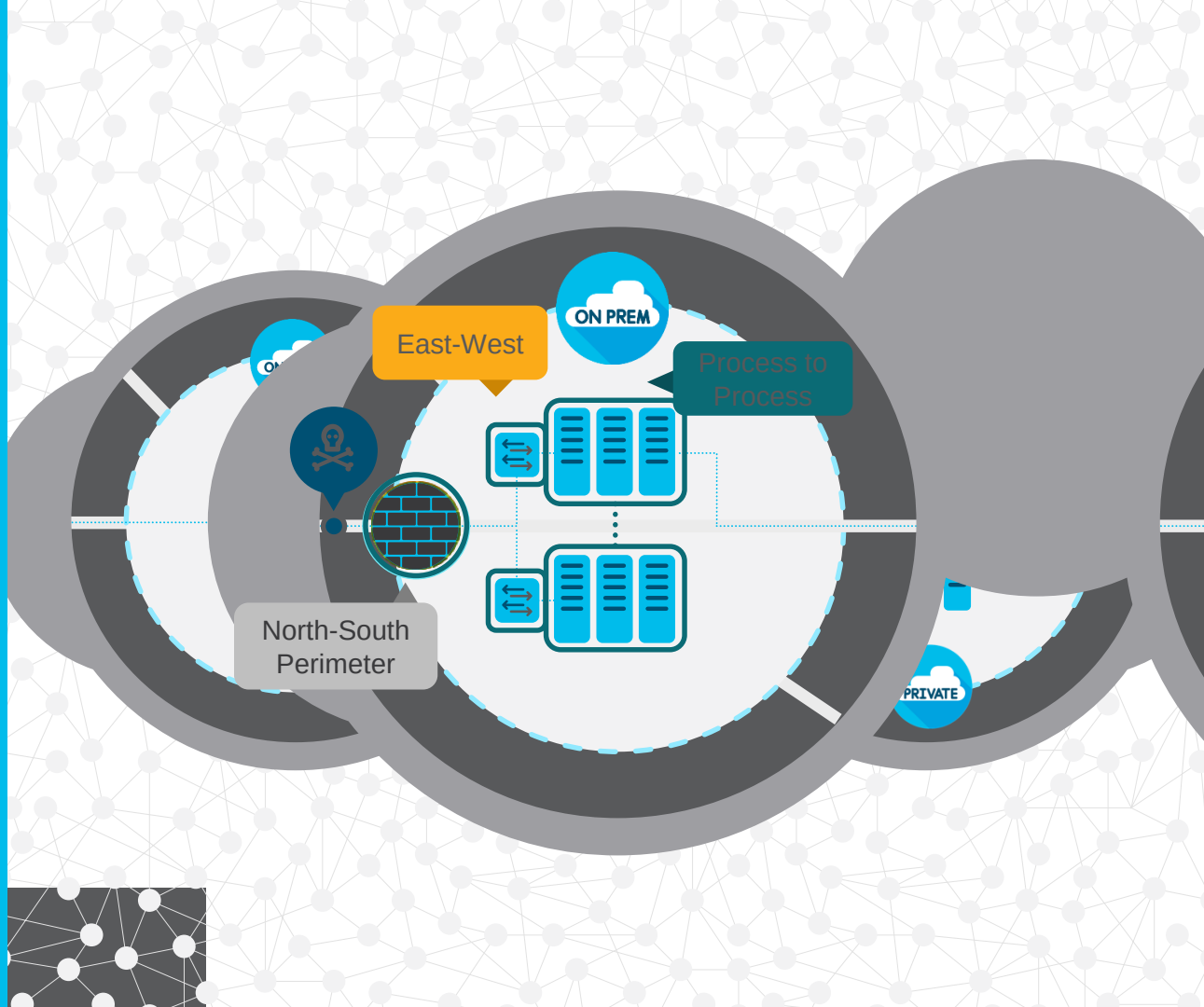
01 02 03

# Segmentation:
## Reduce the Attack Surface

Cisco NGFW

Cisco ACI

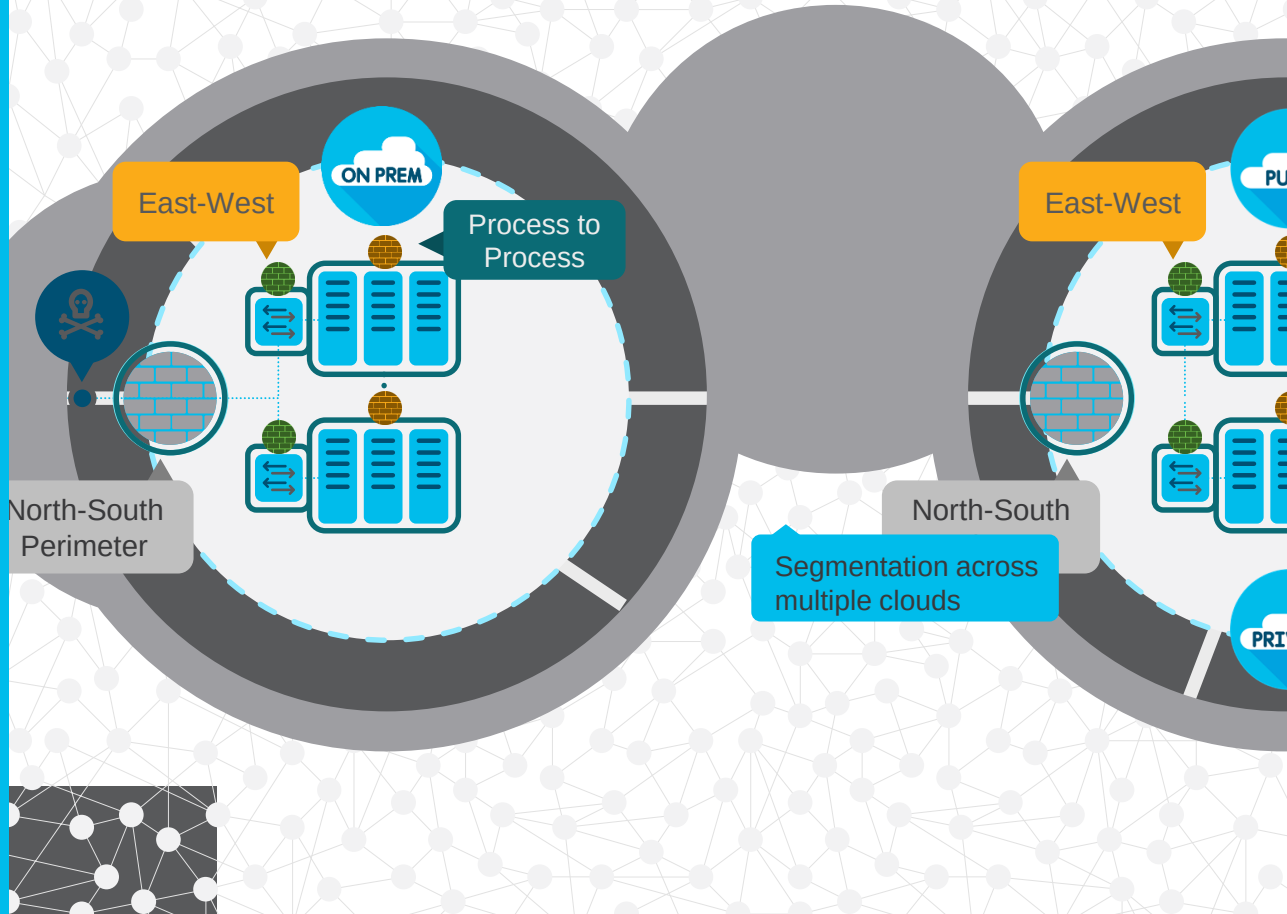
Cisco Tetration



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

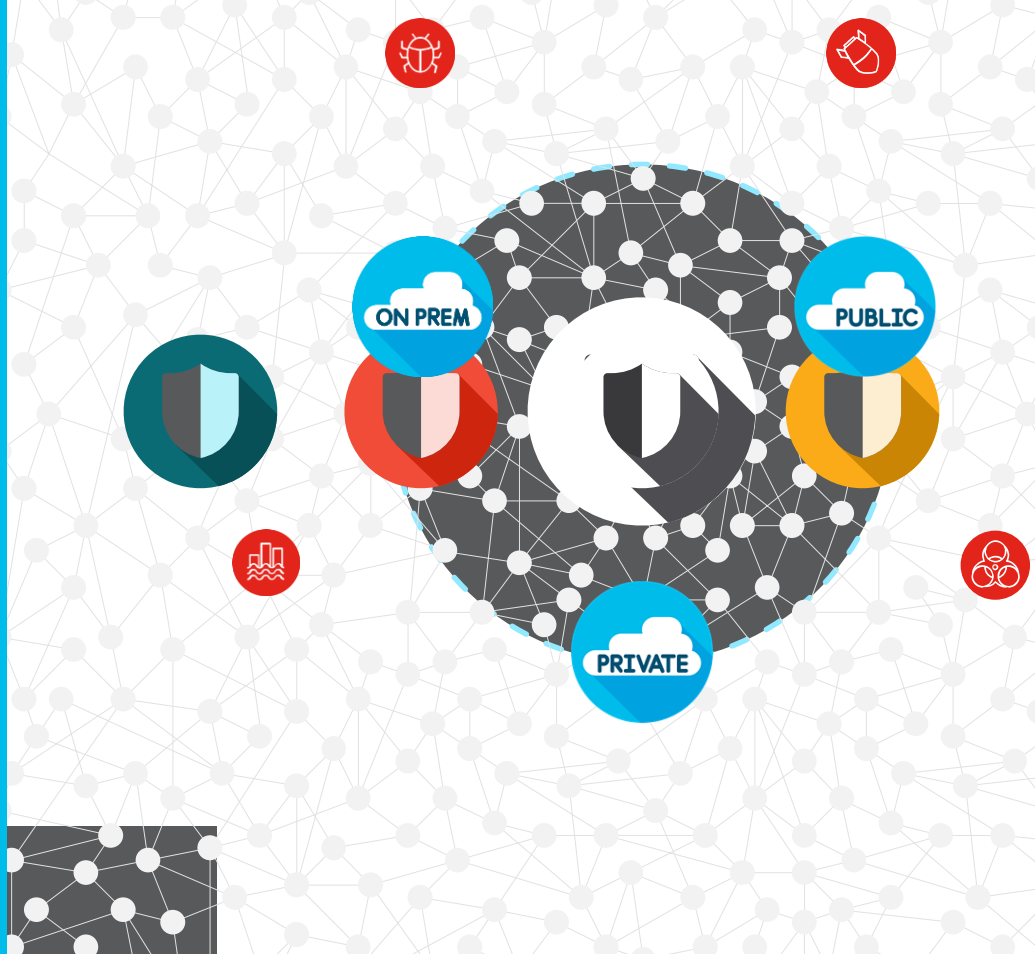
Quickly detect, block, and respond dynamically when threats arise to prevent breaches from impacting the business


Cisco ACI

Cisco Tetration

01 02 03

# Protect the Workload Everywhere




CISCO