



# Data Center Innovation Day

## Journey to the Multicloud





# Secure Multicloud

A Path to Digitization, Speed and Visibility in an Application Centric  
Multicloud World

Nuttee Jirattivongvibul  
Technical Solutions Architect  
Data Center, ASEAN Sales

# Cisco Tetration Analytics™



- Secure Multi-Cloud with Intent-Based DC
- Secure Multi-Cloud demo
- Q&A

Tetration

$$n a = \underbrace{a^{a \dots a}}_n$$



# I've already invested in many security vendors ...

The image displays 18 security categories, each with a header and a collection of vendor logos:

- Infrastructure Security:** Network Firewall (Cisco, Palo Alto, Juniper, etc.), Network Monitoring (Blue Coat, XDR, etc.), Intrusion Prevention Systems (Cisco, Palo Alto, etc.), Unified Threat Management (Cisco, Palo Alto, etc.).
- Endpoint Security:** Endpoint Protection & Anti-Virus (McAfee, Symantec, etc.), Endpoint Detection & Response (CrowdStrike, SentinelOne, etc.), Messaging Security (Microsoft, Cisco, etc.).
- Application Security:** WAF & Application Security (Akamai, Cloudflare, etc.), Vulnerability Assessment (Qualys, Rapid7, etc.), Web Security (Cisco, Palo Alto, etc.).
- IoT Security:** Various vendors like MOCANA, Argus, etc.
- Security Operations & Incident Response:** SIEM (Splunk, LogRhythm, etc.), Security Incident Response (Phantom Cyber, etc.), Risk & Compliance (RSA, Archer, etc.).
- Threat Intelligence:** BrightPoint, DomainTools, etc.
- Mobile Security:** Lookout, MobileIron, etc.
- Data Security:** Veeva, etc.
- Transaction Security:** Feedzai, etc.
- Specialized Threat Analysis & Protection:** FortScale, etc.
- Identity & Access Management:** Okta, etc.
- Cloud Security:** Palo Alto, etc.

Source: Momentum Partners.

# ... But am I safe?



# Feeling Secure?

- Attacks are mainly driven by application vulnerabilities, not network
- In most cases the port will be legitimately open
  - Apache Struts?
- What about attacks coming from other workloads on the same hypervisor
  - Spectre / Meltdown?
- Let's see some examples in the last 12 months



Massive ransomware cyber-attack hits at least 150 countries and infected 300,000 machines

APACHE STRUTS VULNERABILITY



Oops, your important files are encrypted.



You became victim of the PETYA RANSOMWARE!

The hard disks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the xxxxxx page shown in step 2.

To purchase your key and restore your data, please follow these easy steps:

1. Download the our browser at: <http://xxxxxx.xxx/>
2. Visit one of the following pages with the our browser: <http://xxxxxxxxxxxxxxxxxxx>
3. Enter your personal decryption code there:



# EQUIFAX BREACH

- ▶ 143 MILLION AMERICANS
- ▶ NAMES, ADDRESSES
- ▶ SOCIAL SECURITY NUMBERS



MELTDOWN

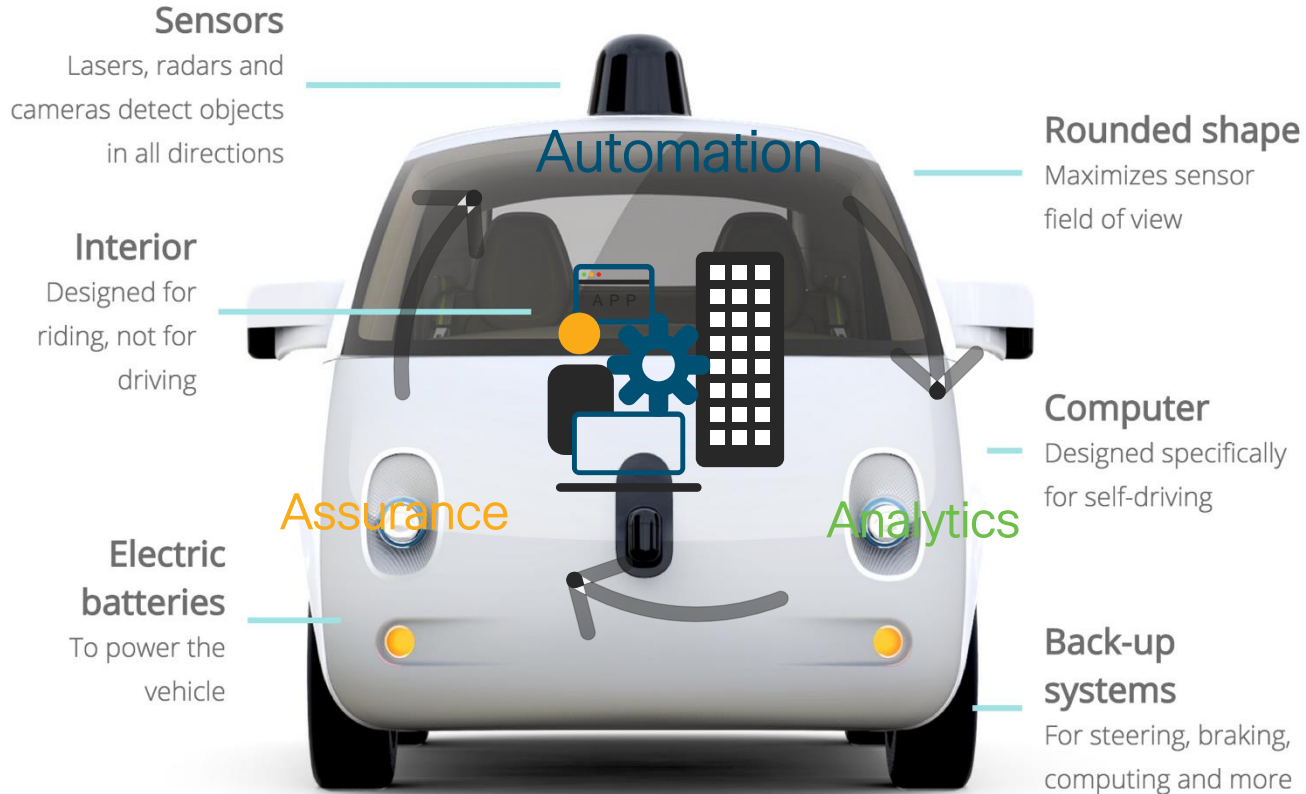


SPECTRE

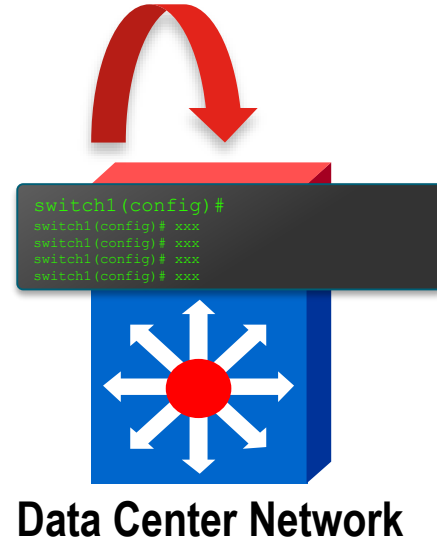
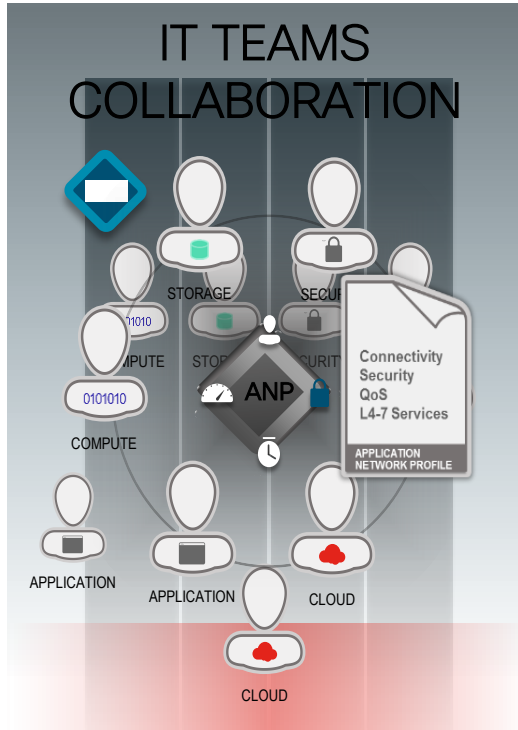
How can we effectively **secure** our workload in Multi-Cloud environment?



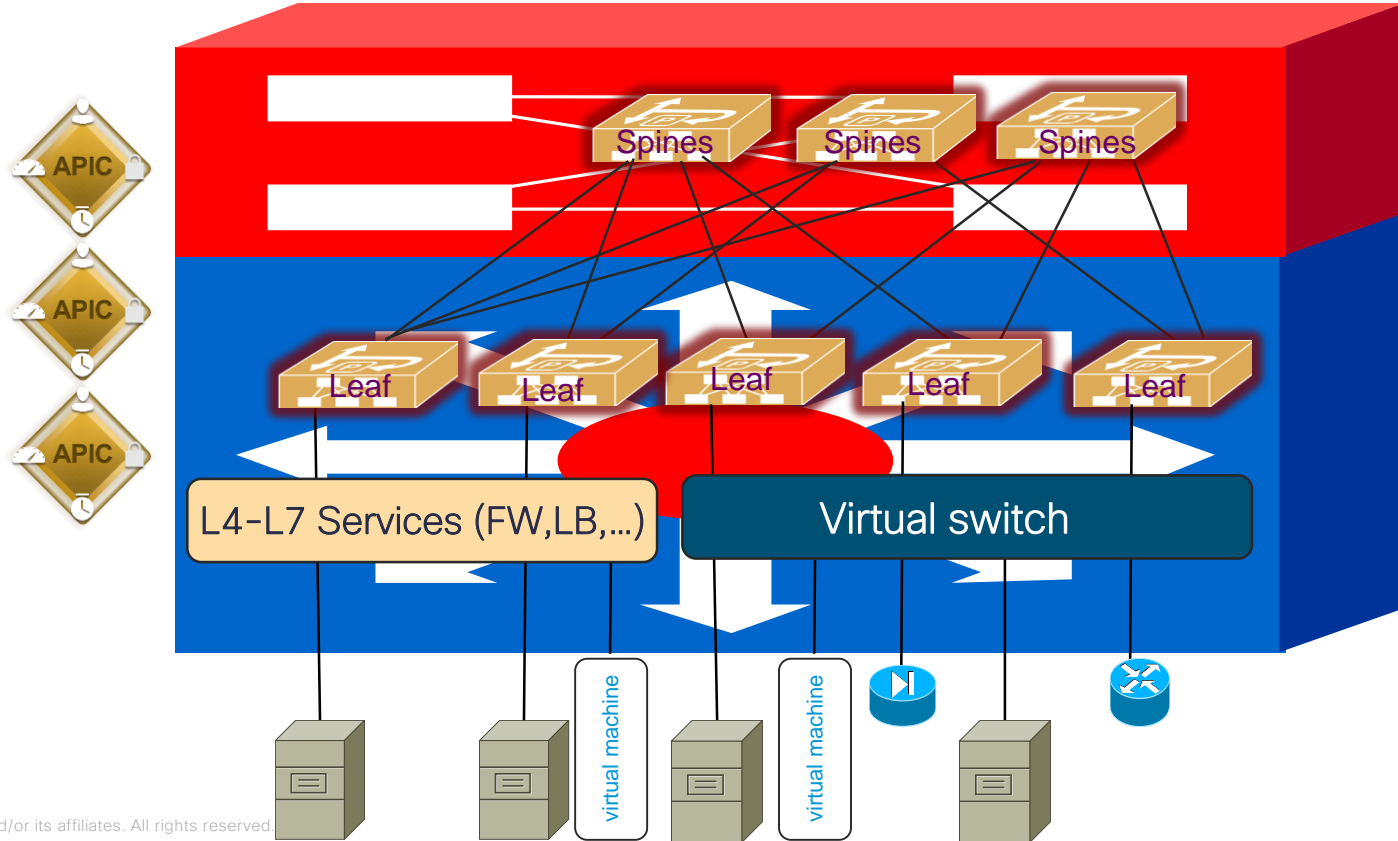
# What is Intent-Based DC?



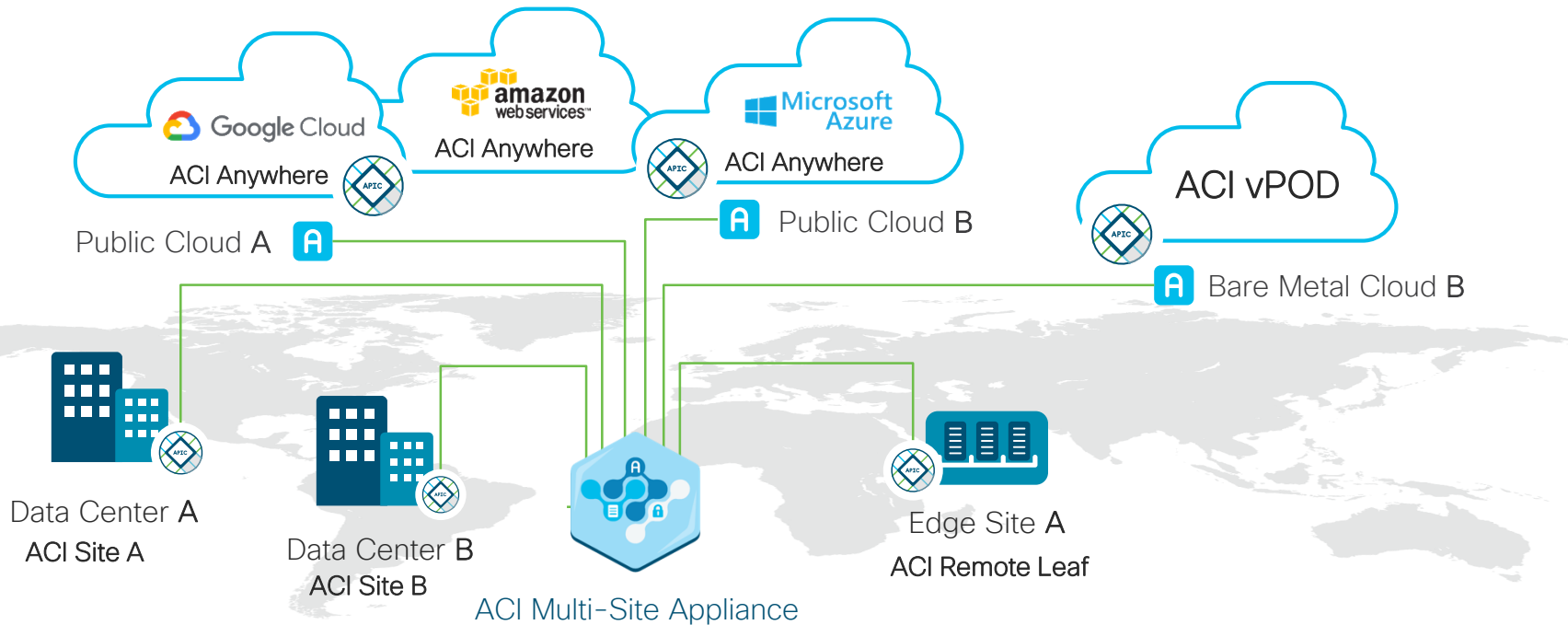
# Application Centric infrastructure



# ACI = “one big modular switch”



# ACI Anywhere - Network policy that goes where you go



Consistent Network and Policy across clouds



Seamless Workload Migration

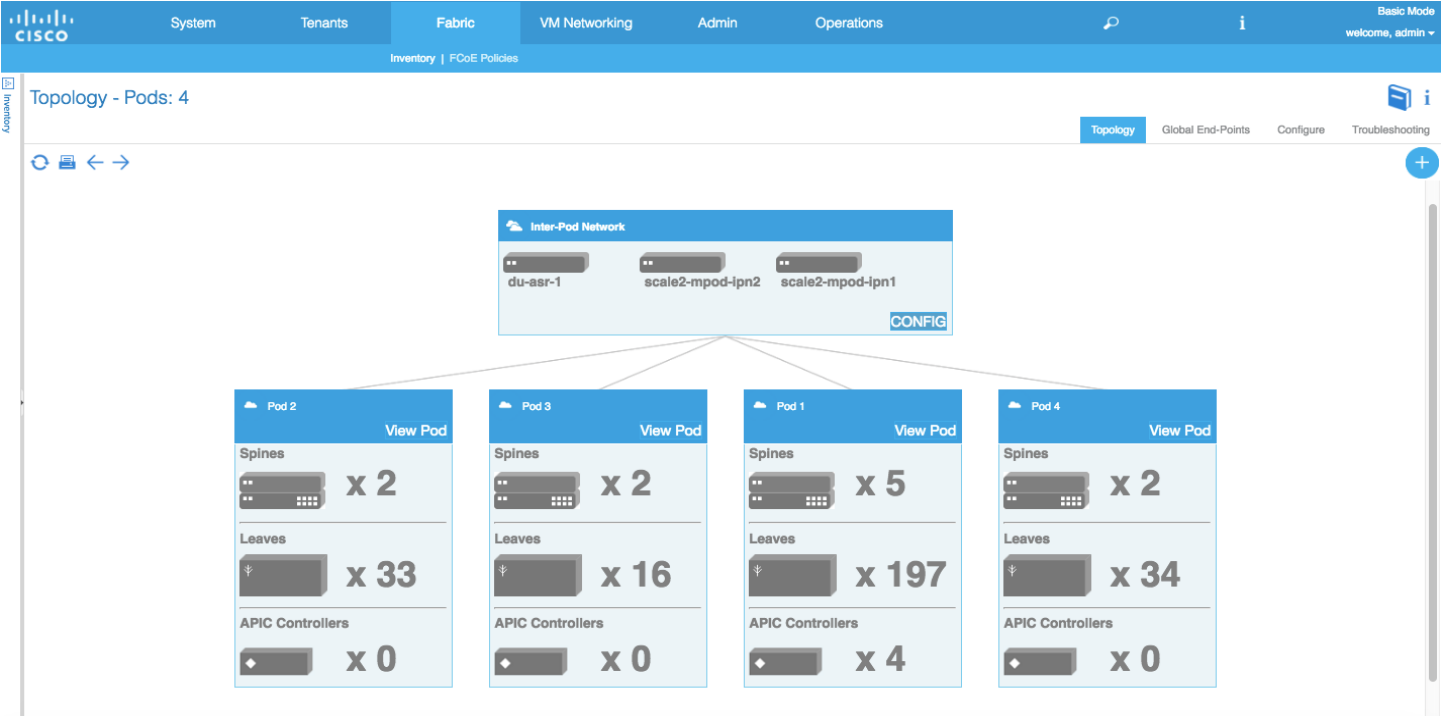


Single Point of Orchestration



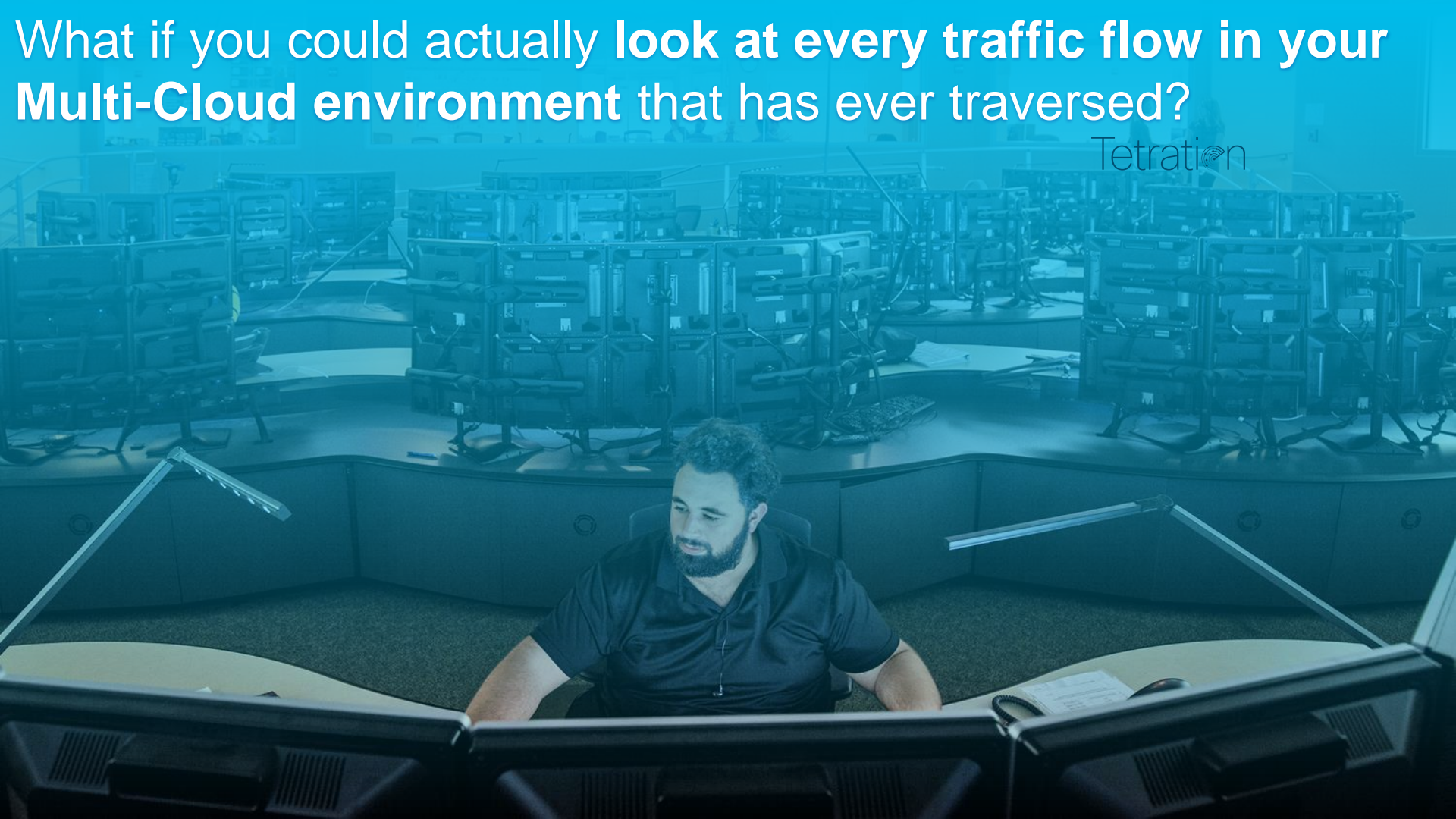
Secure Automated Connectivity

# Multi-POD practical customers



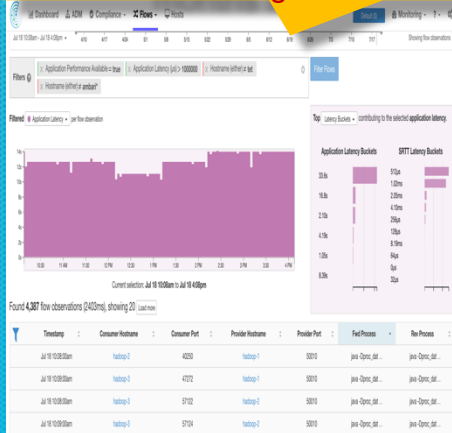
What if you could actually **look at every traffic flow** in your **Multi-Cloud environment** that has ever traversed?

Tetration

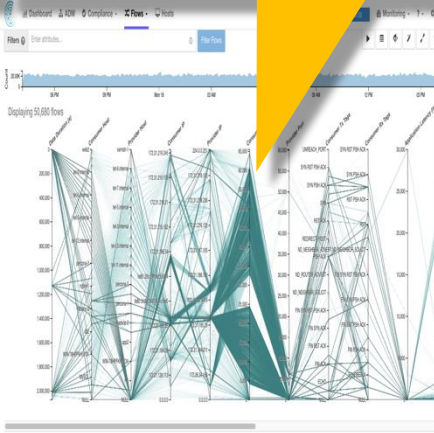


# Tetration with Machine Learning answers your Critical Questions

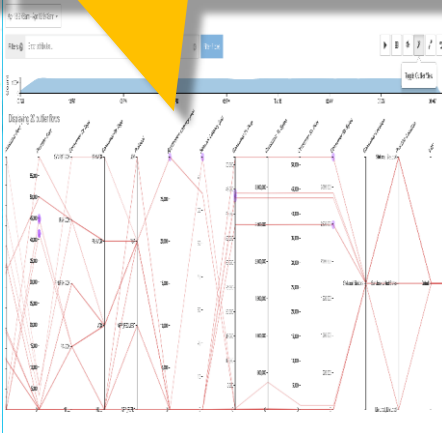
What's going on now and 6 months ago?



What's normal /Baseline?

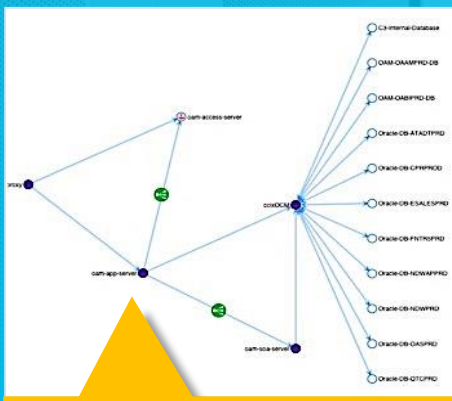


What's outlier?



How to reduce MTTI?

Flags	PSH	ACK	Provider
Byte Count	31,328	6,010 (6,084 so far)	PSH ACK
Packet Count	64 (64 so far)	63 (64 so far)	
SRTT	53.4ms		
Est. Network latency	26.9ms		
Application latency	1.35ms		
Process	tel-sensor-f-sensor.conf		/opt/tetration/collector/collector-config_file /etc/tetration/collector/collector.config -- timestamp_flow_info --logstsdem -- max_num_ssl_siv_sensors 63000 -- enable_client_certificate true --write_empty_files true



Who is talking to who for whitelist policy?

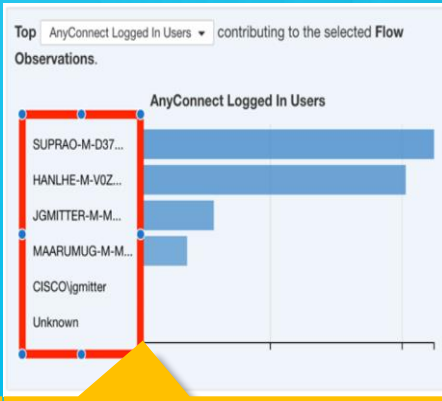
Quick Analysis Filters

Absolute Policies

Default Policies

Priority	Action	Consumer	Provider	Services
100	ALLOW	pod02-haproxy01	Default	UDP: 53 ...
100	ALLOW	pod02-ep0*	Default:Tetration-IPs	TCP: 443 ...
100	ALLOW	pod02-ep0*	Default:Shared	UDP: 111 ...
100	ALLOW	Default	pod02-reds01	TCP: 22 ...
100	ALLOW	pod02-oc0*	pod02-reds01	TCP: 6379 ...
100	ALLOW	pod02-oc0*	Default:Tetration-IPs	TCP: 443 ...
100	ALLOW	pod02-reds01	Default	ICMP ...
100	ALLOW	Default	pod02-haproxy01	ICMP ...
100	ALLOW	Default	pod02-ep00*	ICMP ...

How to enforce policy to Multi-Cloud env.?



Multi-Cloud End point/client visibility?



What is my Cloud Security Grade?

# Cisco Tetration platform

Hybrid cloud workload protection approach

## Communication control



- Visibility and ADM
- Automated whitelist policy based on application behavior
- Policy enforcement to enable segmentation
- Tracking of policy compliance
- Outlier detection
- IP Blacklist Blocking using Zeus, Bogon Cymru or manual

## App behavior detection



- Process hash, lineage, attributes
- New command, new user
- Account modification
- Privilege escalation
- Shell-code execution
- Raw sockets

## Vulnerability detection

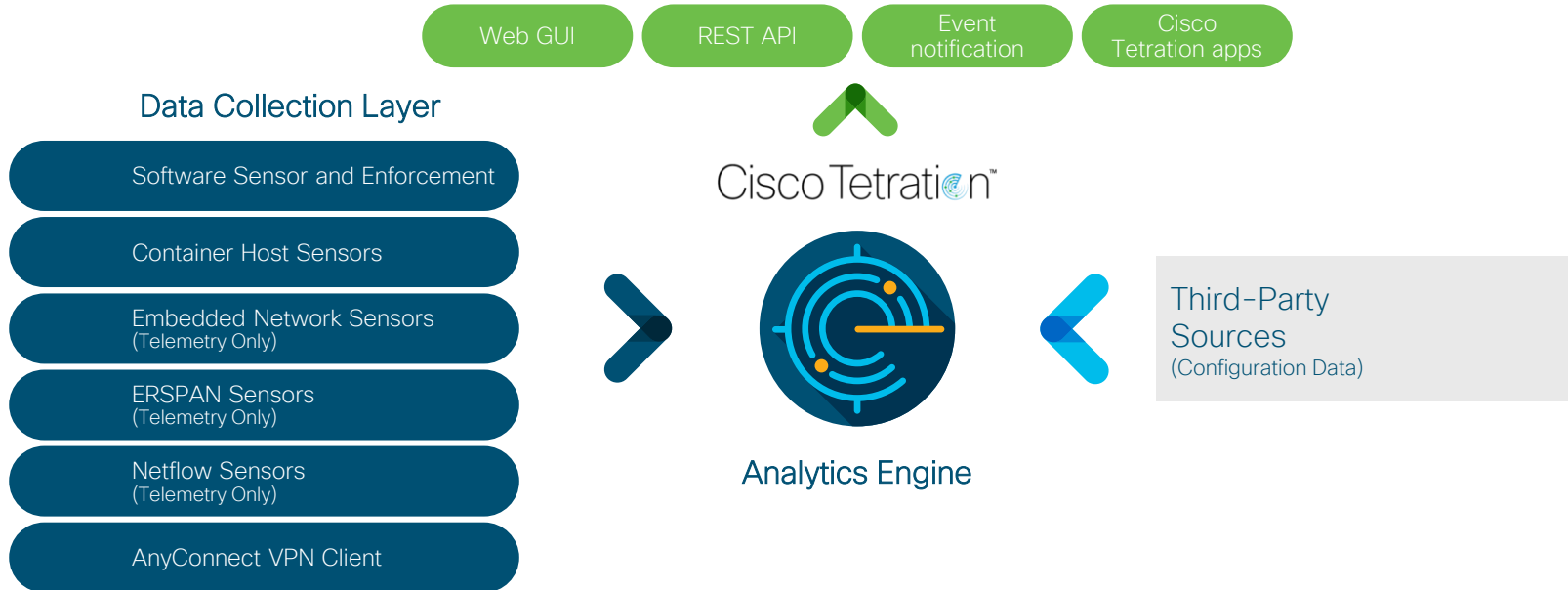


- Installed package tracking
- Weekly CVE tracking
- Vulnerability scoring
- Threat intelligence ingestion
- Process Inventory and outlier



# Cisco Tetration Platform

## Architecture Overview



# Cisco Tetration: On-premises deployment options

## On-premises options

### Cisco Tetration™ Platform (large form factor)

- Suitable for deployments of more than 5000 workloads
- Built-in redundancy
- Scales to up to 25,000 workloads

#### Includes:

- 36 Cisco UCS® C220 servers
- 3 Cisco Nexus® 9300 platform switches

### Cisco Tetration-M (small form factor)

- Suitable for deployments of less than 5000 workloads

#### Includes:

- 6 Cisco UCS C220 servers
- 2 Cisco Nexus 9300 platform switches

## Public cloud

### Cisco Tetration Cloud

- Software deployed in AWS
- Suitable for deployments of less than 1000 workloads
- AWS instance owned by customer

Amazon  
Web Services

Microsoft  
Azure

## Virtual appliance option

### Cisco Tetration Virtual

- Suitable for deployments of less than 1000 workloads
- Published system specification (CPU cores, memory, storage, etc.,)
- Supported in VMware ESXi-based environment

Software subscription license based on number of workloads; available in 1-, 3-, and 5-year terms

# Why Tetration is better?



# In Summary – Did we help (NSA)?

- ✓ 1. When protecting your network, you have to **know everything** that is going on.  
TA: end-to-end visibility
- ✓ 2. Decrease attack surface. **Lock down and disable services you are not using.**  
TA: You will know unused ports, un-patch vulnerabilities,... in each workloads
- ✓ 3. Identify what is routine in your infrastructure and what is not. **Monitor for deviations.**  
TA: You can see the network baseline and outlier
- ✓ 4. **Whitelisting** is a must in today's cyber security world  
TA: We set the scene by segmenting application tiers and build the policy in real time

“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.”

# In summary - Did we help (ASD)?

1. Application Whitelisting
  - ✓ • **TA:** We set the scene by segmenting application tiers
2. Patching Systems
  - ✓ • **TA:** We identified Vulnerable systems and were able to take action on them
3. Restricting Administrative Privileges
  - ✓ • **TA:** We identified and alarmed on privilege escalation
4. Creating a Defense in Depth System
  - ✓ • **TA:** We've setup the first stages of our defense in depth approach with multi-level segmentation

# Cisco Tetration Analytics



“**Tetration** provided **more value** in the **first 30 days** with **100 sensors** deployed than **3 years** of investing with G (a Data Broker Vendor)”  
– An US Customer



Demo



**KEEP  
CALM  
IT IS  
DEMO  
TIME**

# Multicloud Enforcement

Like the Borg...customer applications are deployed as hybrids.

And across many public and private infrastructures.

Making enforcement of holistic policy for heterogenous workloads....extremely complex.

Let's see how Cisco's Tetration Platform solves this challenge with its simple to use Workload Protection Policy Model.



**BORGPRESS**

Just another Multicloud Wordpress site Protected by Cisco Tetration

# Security Dashboard

