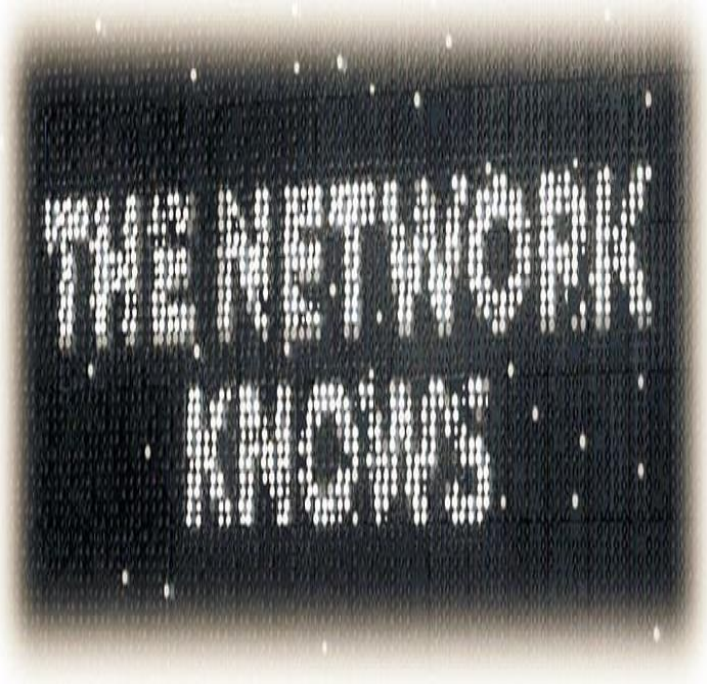

cisco
intel
Data Center Innovation Day
Journey to the Multicloud

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™



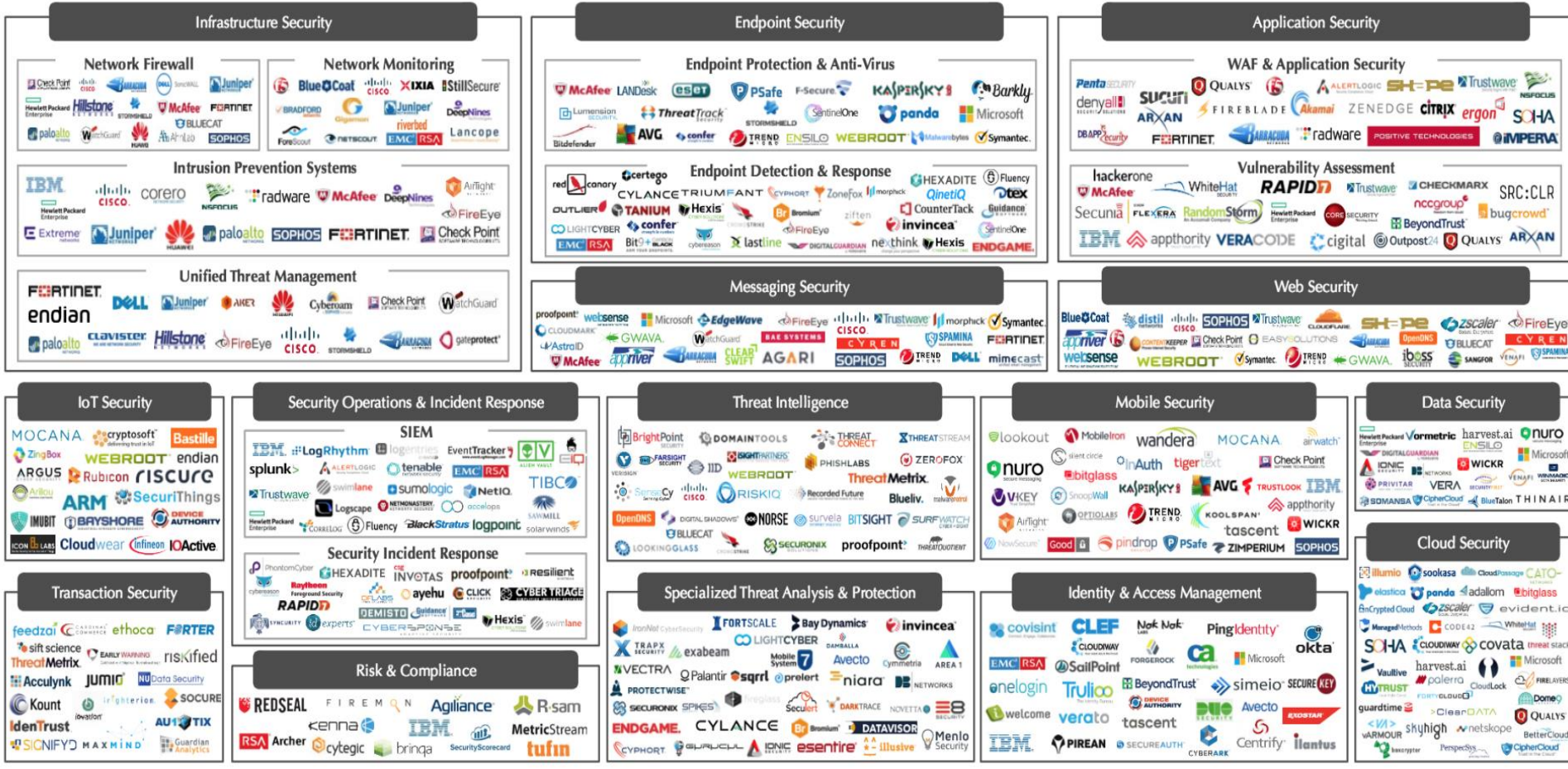
- Secure Multi-Cloud with Intent-Based DC
- Secure Multi-Cloud demo
- Q&A

Tetration

$$ {}^{n}a = \underbrace{a^{a^{\cdot^{\cdot^{a}}}}}_{n} $$

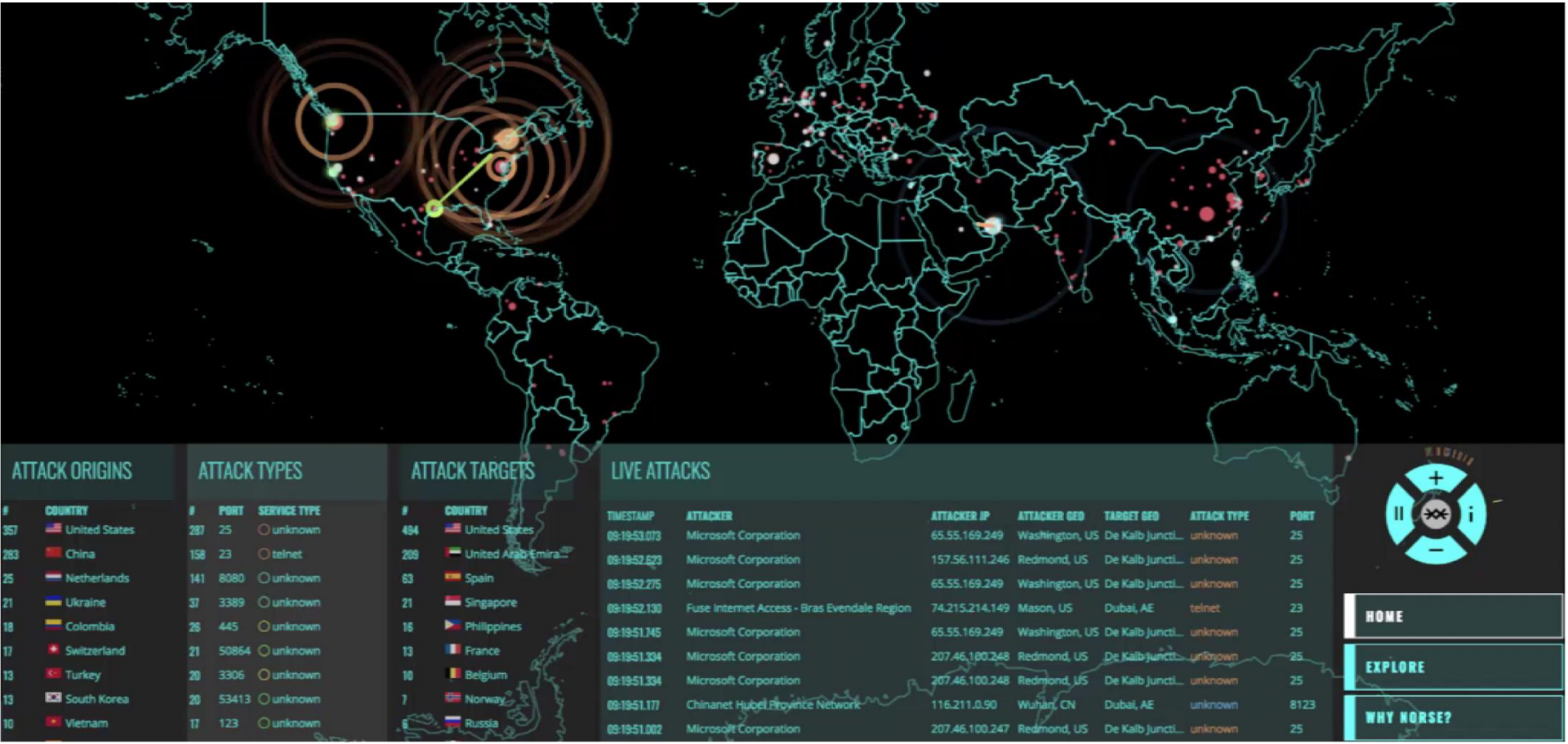
Cisco Tetration™ Systems with Intel® Xeon® Scalable processors

I've already invested in many security vendors …



Source: Momentum Partners.

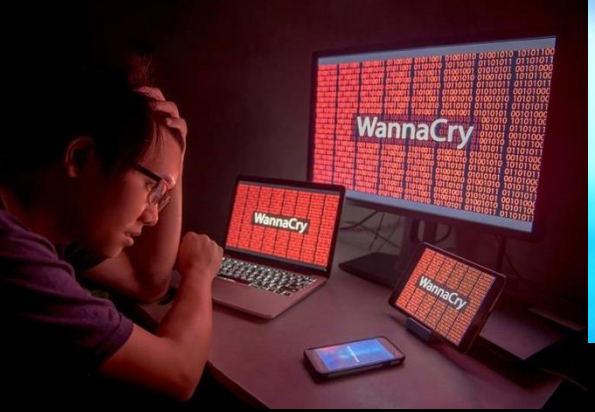
… But am I safe?



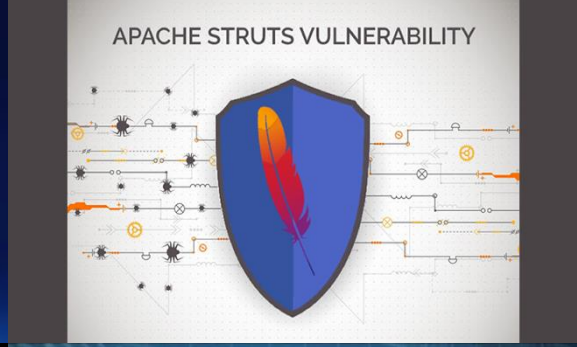
Reference: http://map.norsecorp.com/

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

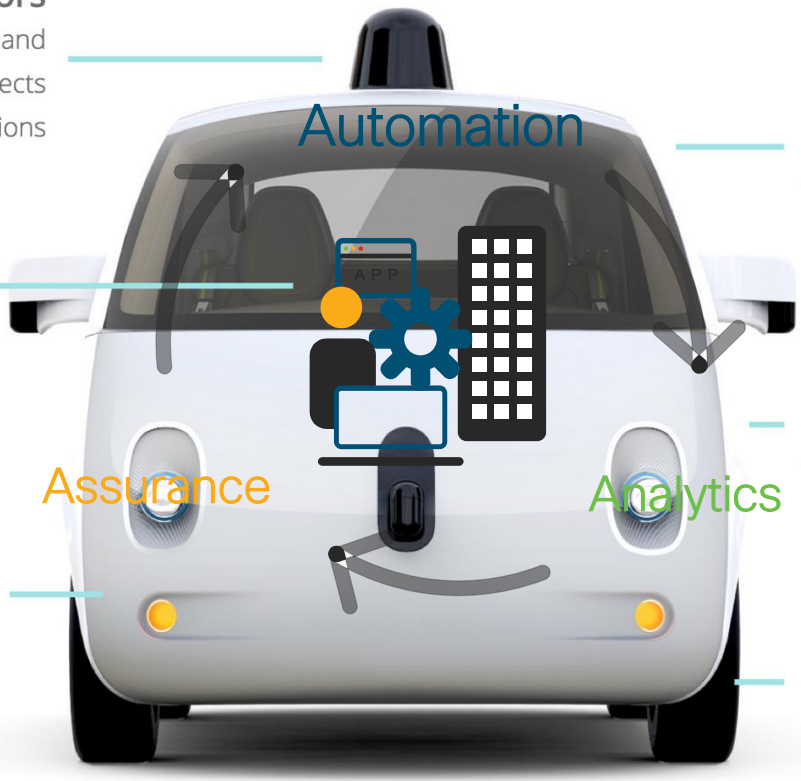


Massive ransomware cyber-attack hits at least 150 countries and infected 300,000 machines



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

What is Intent-Based DC?



Sensors
Lasers, radars and cameras detect objects in all directions

Interior
Designed for riding, not for driving

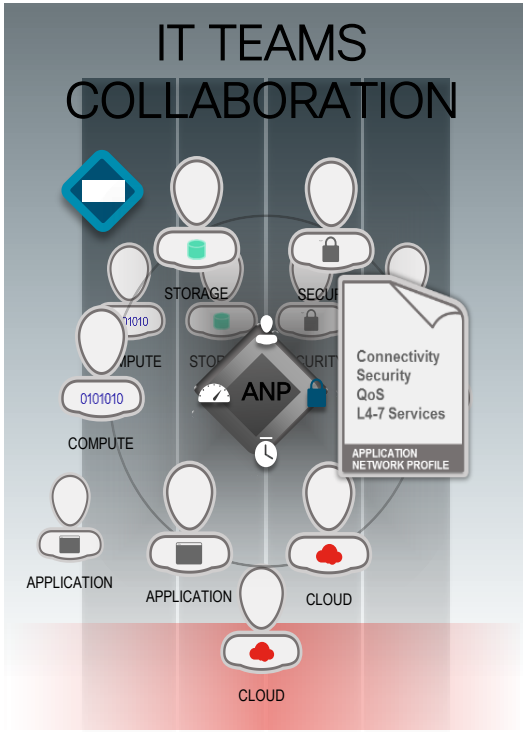
Electric batteries
To power the vehicle

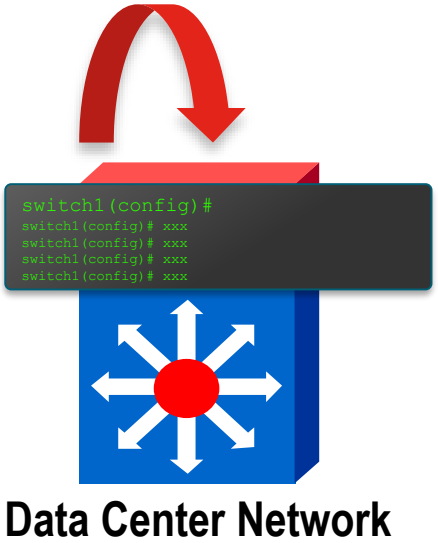
Rounded shape
Maximizes sensor field of view

Computer
Designed specifically for self-driving

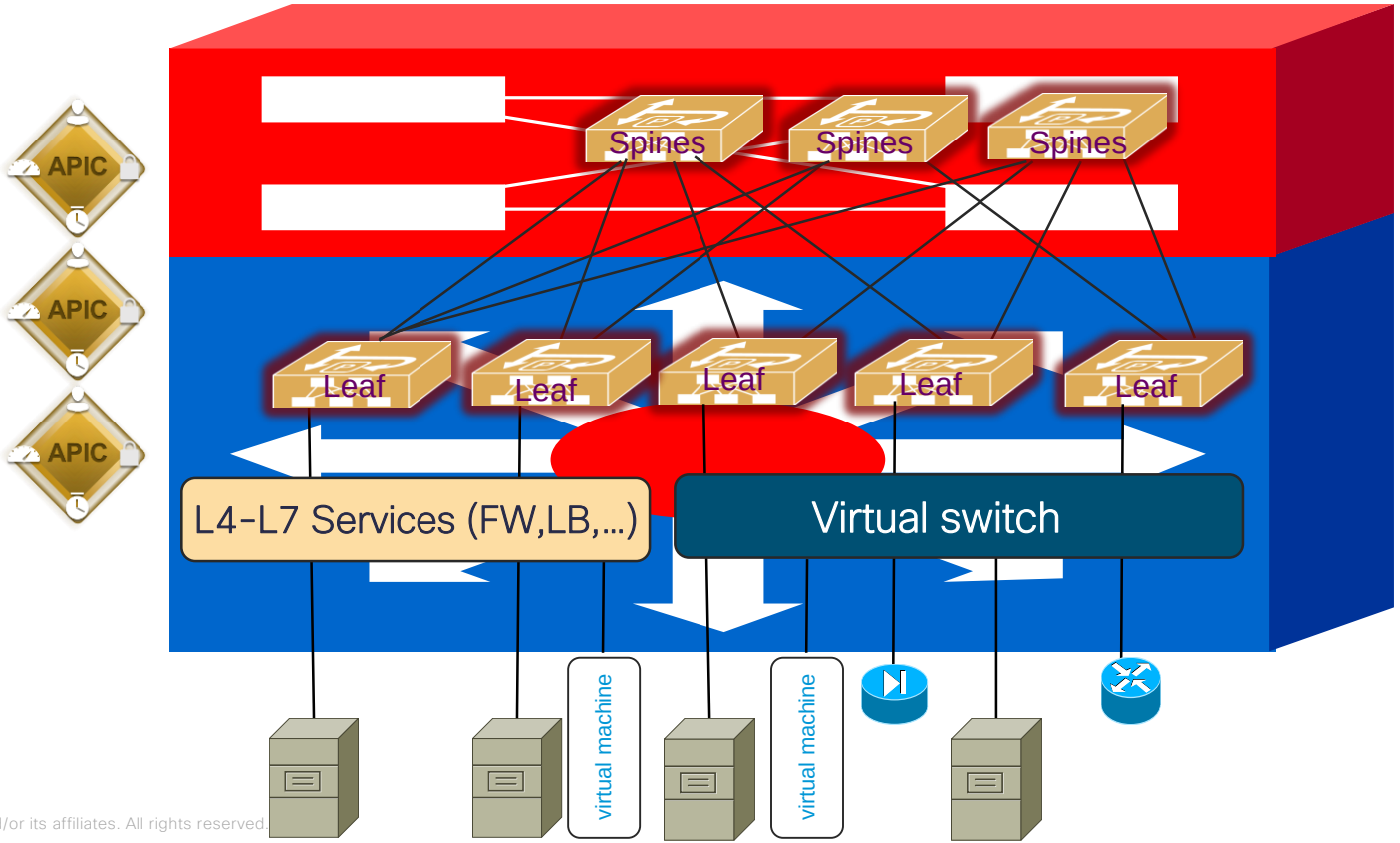
Back-up systems
For steering, braking, computing and more

Application Centric infrastructure

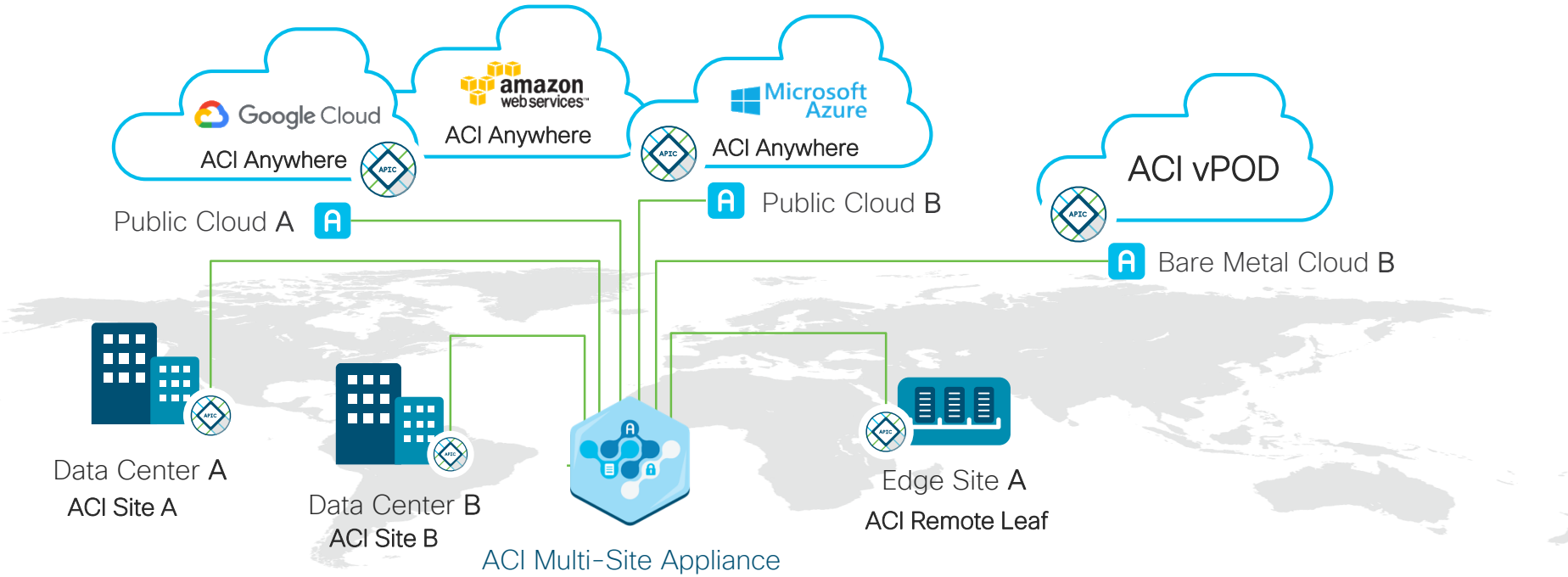




ACI = “one big modular switch”

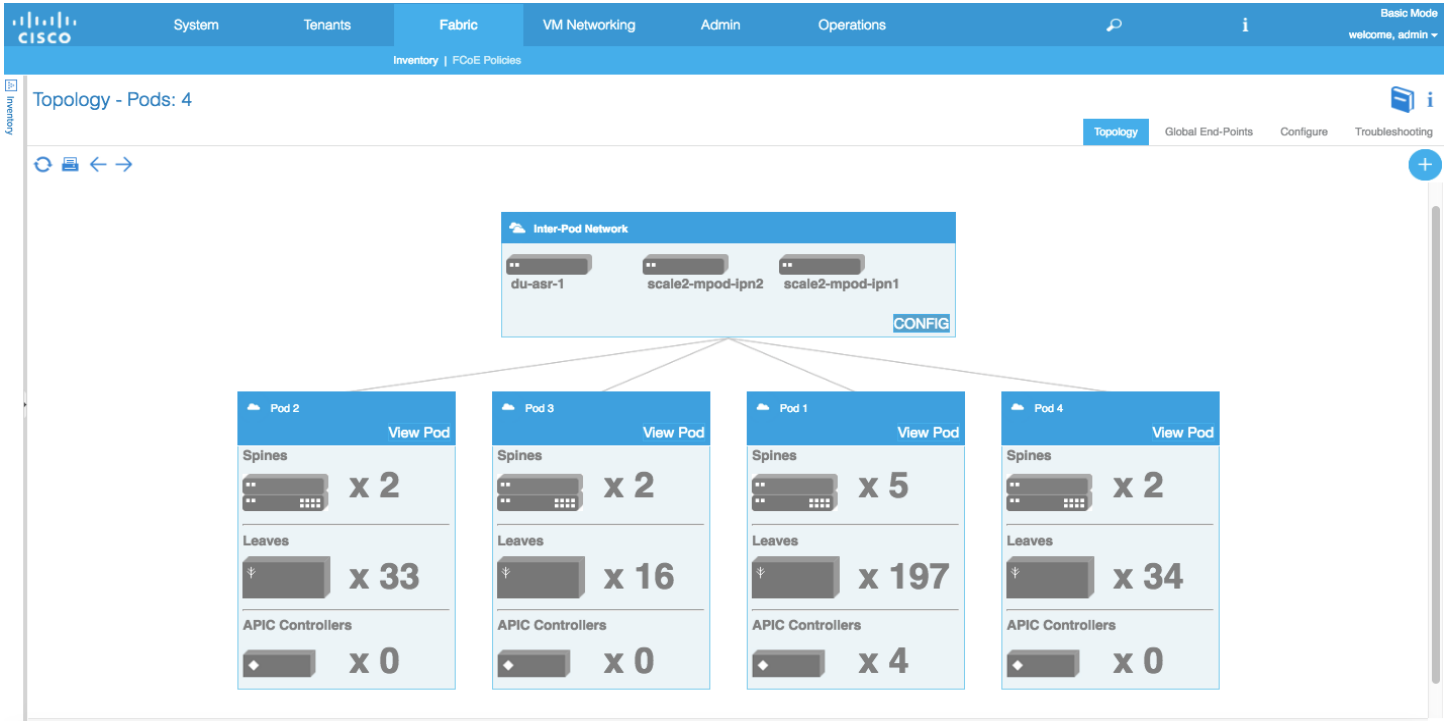


ACI Anywhere – Network policy that goes where you go



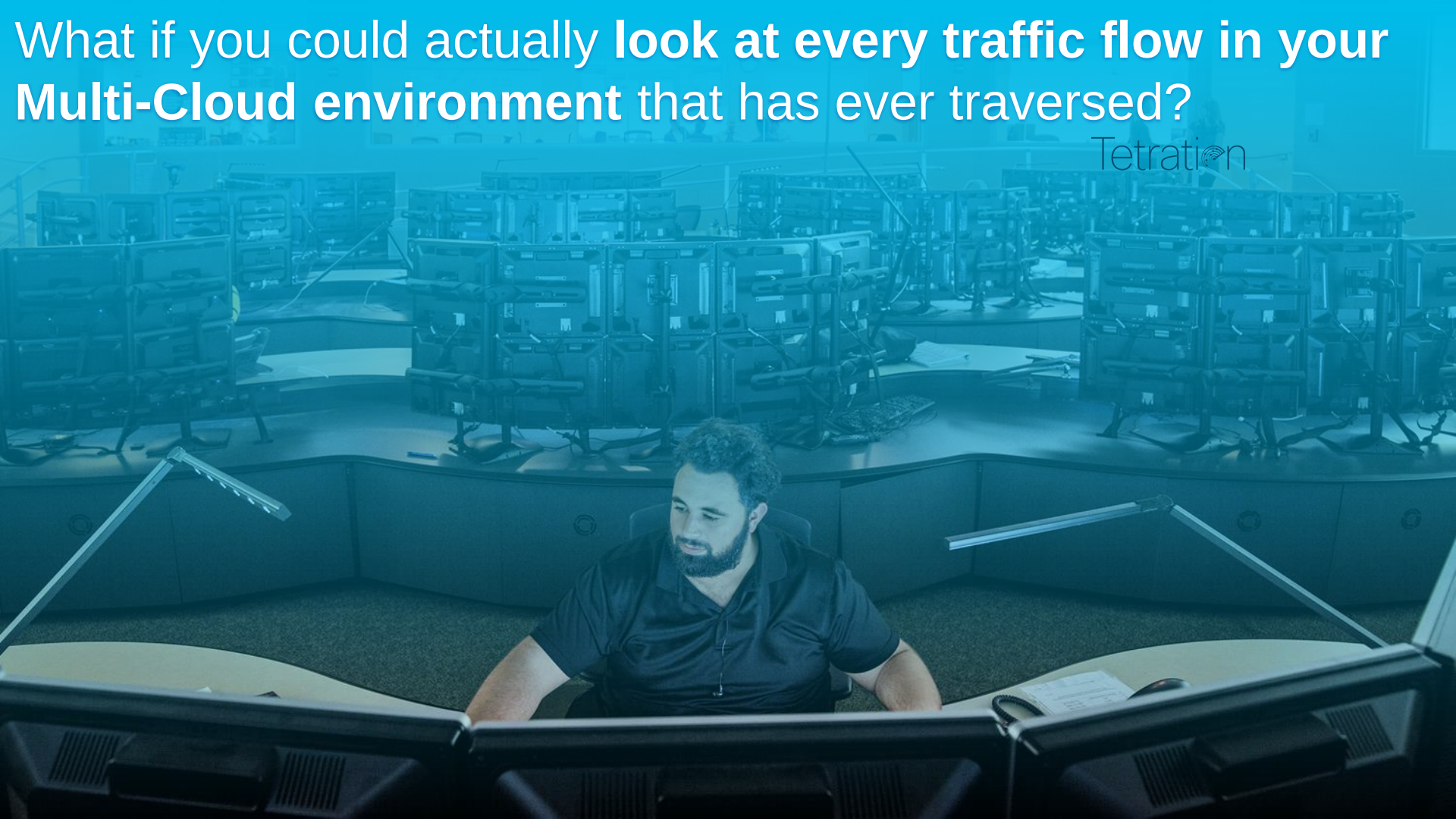
- Consistent Network and Policy across clouds
- Seamless Workload Migration
- Single Point of Orchestration
- Secure Automated Connectivity

Multi-POD practical customers



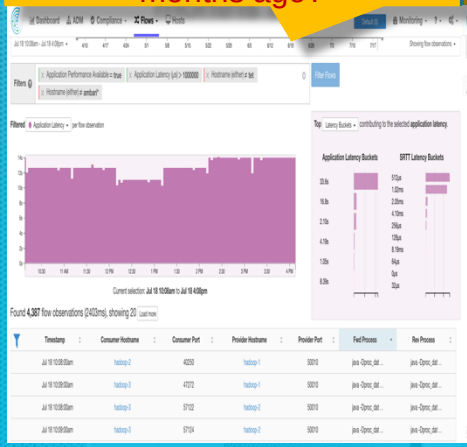
What if you could actually **look at every traffic flow in your Multi-Cloud environment** that has ever traversed?

Tetration

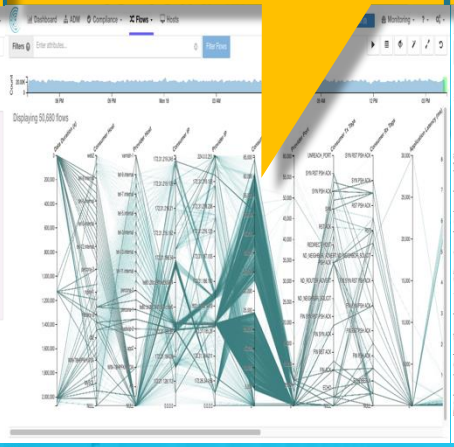


Tetration with Machine Learning answers your Critical Questions

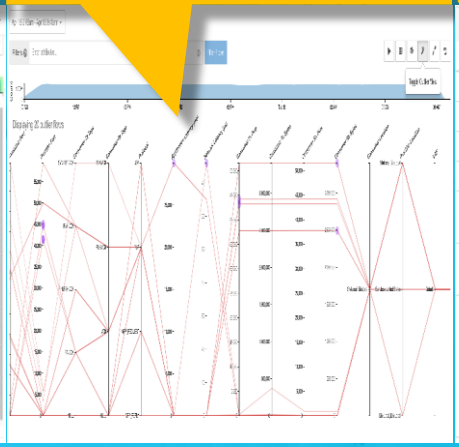
What's going on now and 6 months ago?



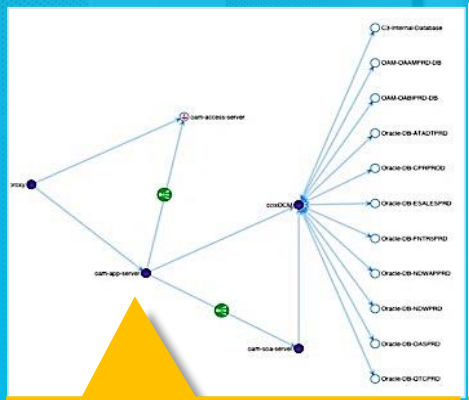
What's normal /Baseline?



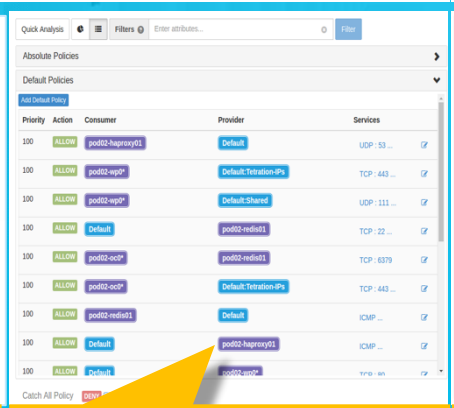
What's outlier?



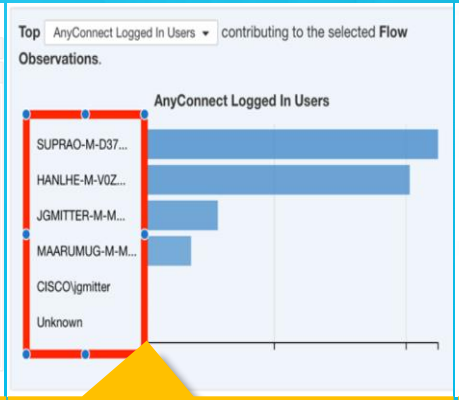
How to reduce MTTI?



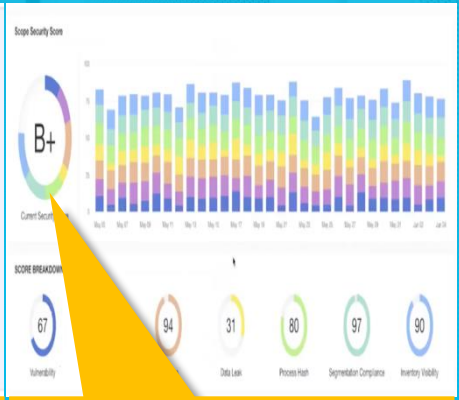
Who is talking to who for whitelist policy?



How to enforce policy to Multi-Cloud env.?



Multi-Cloud End point/client visibility?



What is my Cloud Security Grade?

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

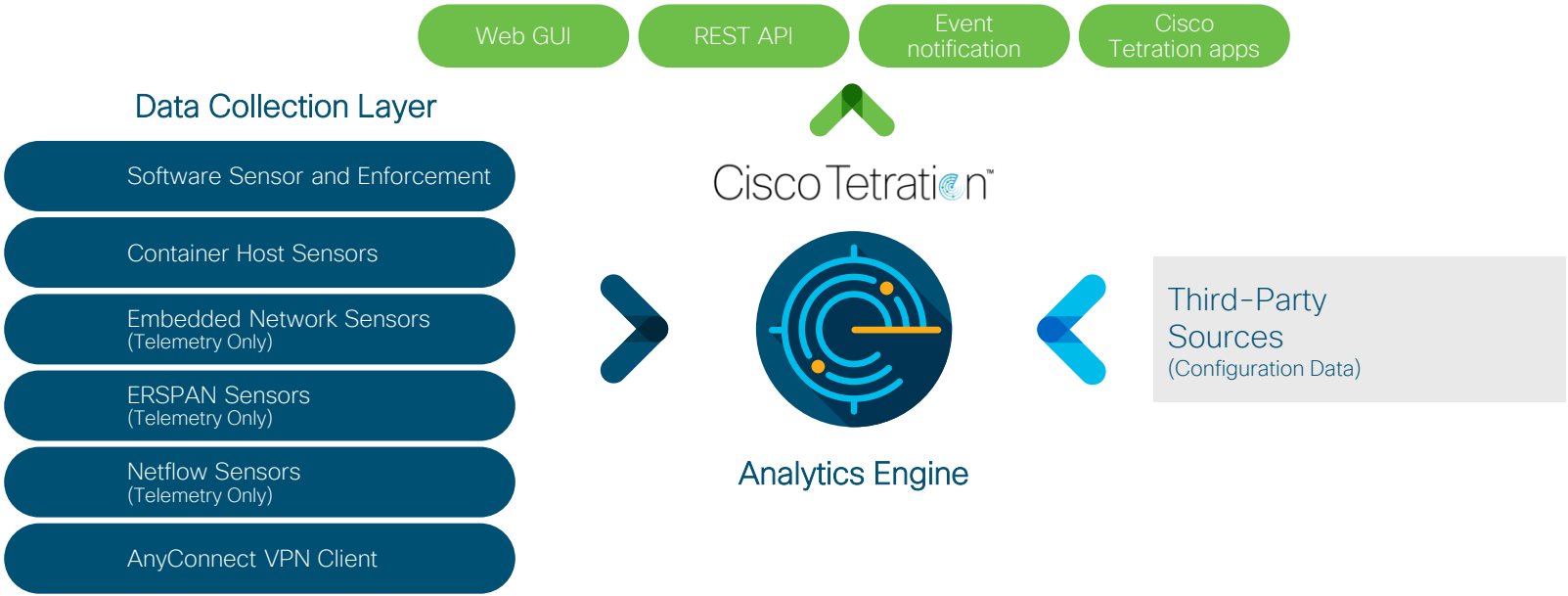
Vulnerability detection

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

Cisco Tetration™ Systems with Intel® Xeon® Scalable processors

Cisco Tetration Platform

Architecture Overview



Cisco Tetration™ Systems with Intel® Xeon® Scalable processors

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?

Cisco Tetration™ Systems with Intel® Xeon® Scalable processors

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

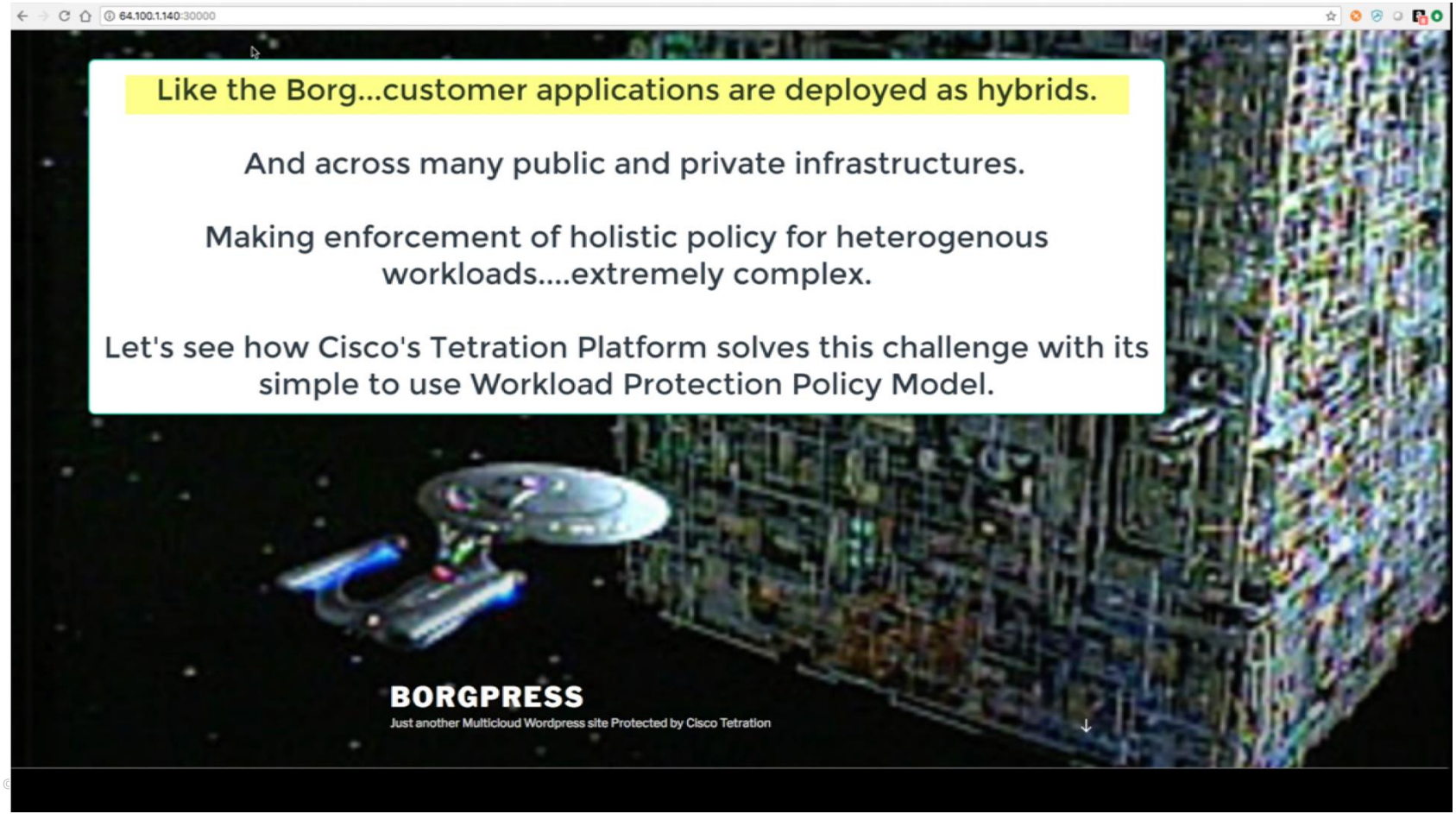
"Tetration provided more value in the first 30 days with 100 sensors deployed than 3 years of investing with G (a Data Broker Vendor)"
- An US Customer

Cisco Tetration™ Systems with Intel® Xeon® Scalable processors

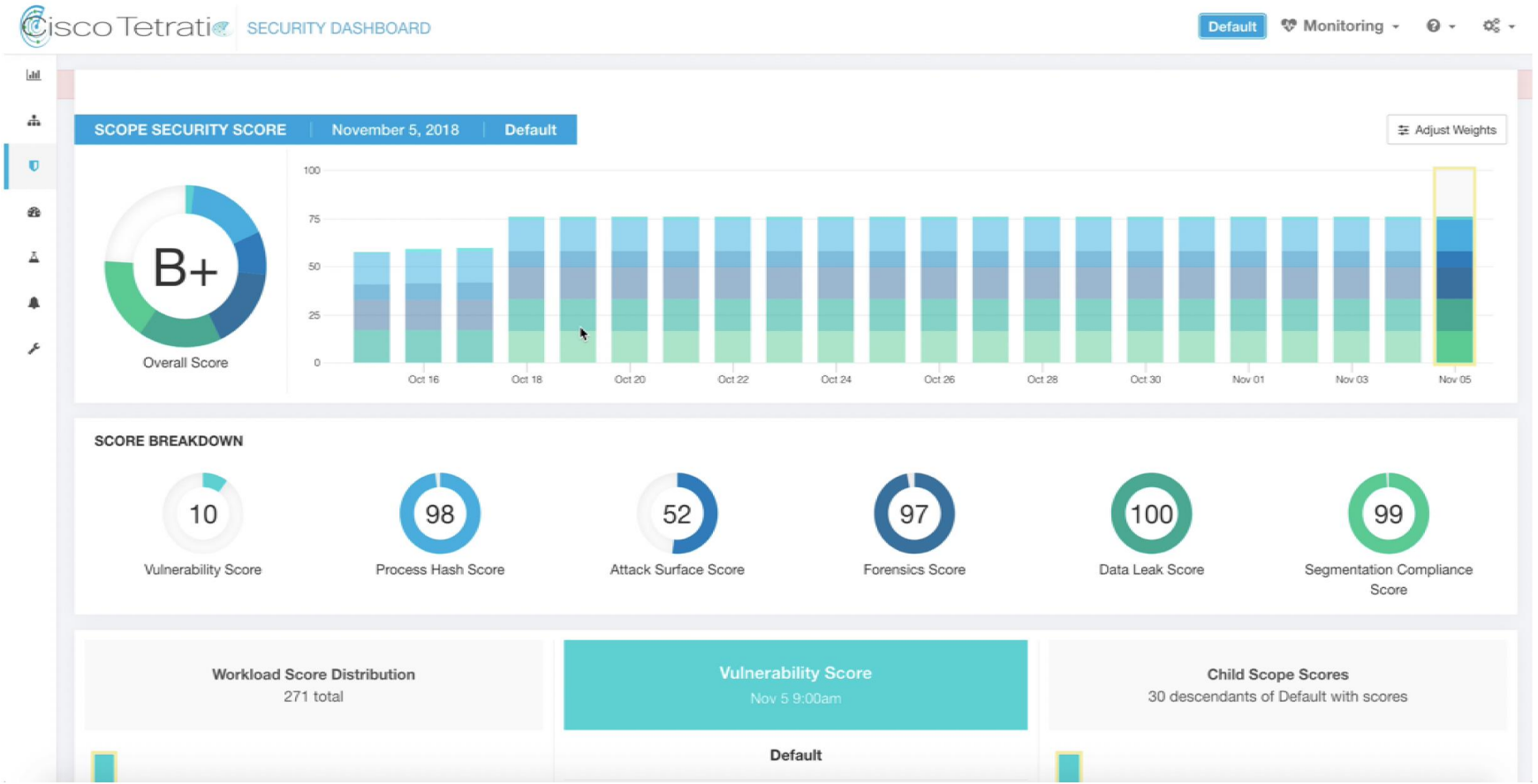
Demo

KEEP
CALM
IT IS
DEMO
TIME

Multicloud Enforcement



Security Dashboard




CISCO