Global vision.
Local insight.

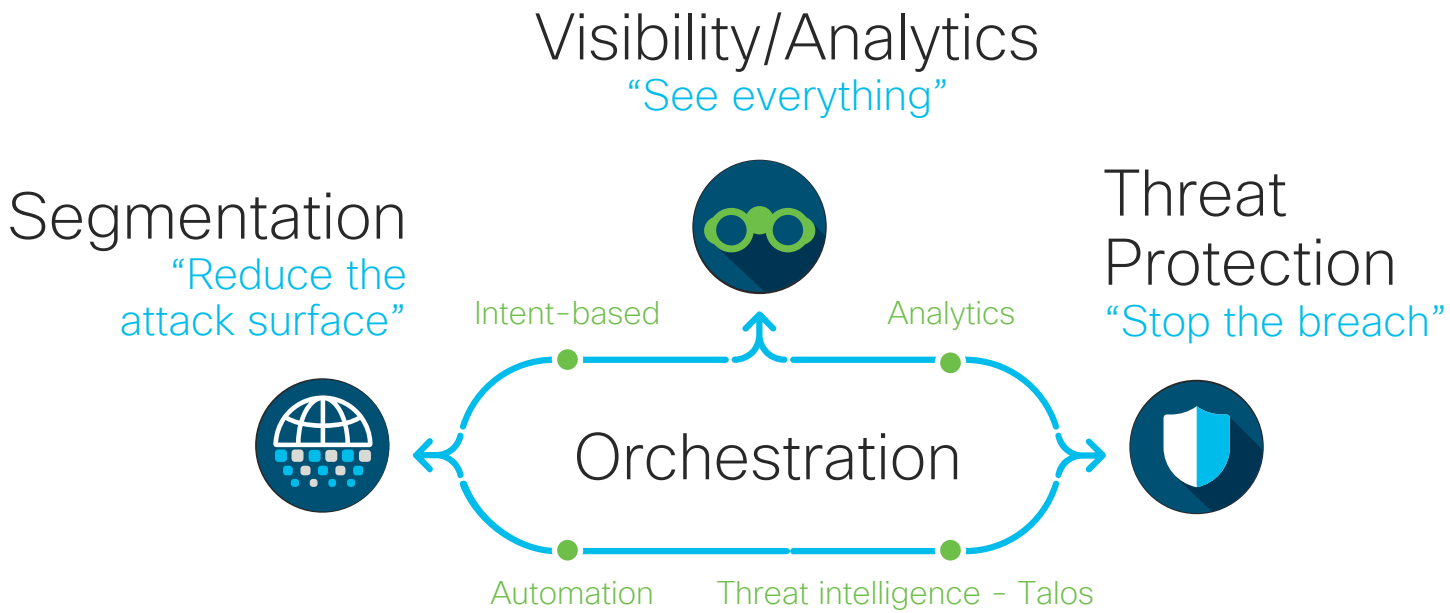
Cisco Connect Copenhagen

Denmark · 4th April 2019

Tetration Analytics

Data Center Security Architecture

Three focus areas:




Cisco
Tetration
Analytics


Cisco
Tetration
Analytics
Any Application, Any Endpoint
vmware
Hyper-V
kvm
vmware
Bare Metal
Virtual Machine
Container


Application
Insight
Cisco
Tetration
Analytics

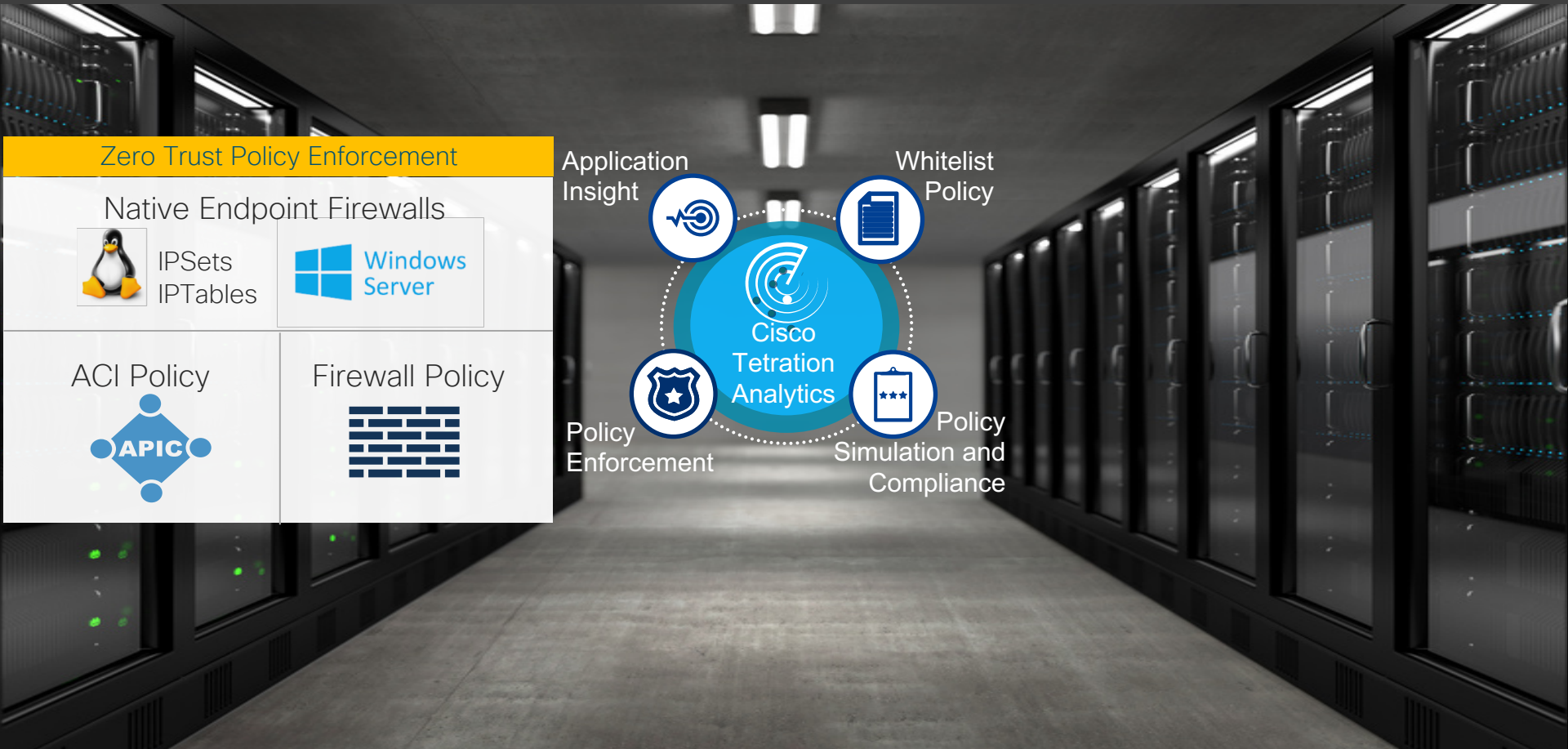
InfoSec Policy

Priority	Action	Consumer	Provider	Services
100	DENY	Production	NonProduction	Any : 0-65535
100	DENY	NonProduction	Production	Any : 0-65535

Application Whitelist Policy

Priority	Action	Consumer	Provider	Services
100	ALLOW	HAProxy	Default:Labs	TCP : 443 ...
100	ALLOW	HAProxy	Wordpress	TCP : 80 ...
100	ALLOW	Redis	Default:Labs	UDP : 123 ...
100	ALLOW	Default:Labs	Opencart	TCP : 22 ...
100	ALLOW	Default:Labs	Wordpress	TCP : 80 ...
100	ALLOW	Wordpress	Default:Labs	UDP : 53 ...
100	ALLOW	Default:Labs:APJ	HAProxy	TCP : 80
100	ALLOW	Default	Opencart	TCP : 80 ...
100	ALLOW	Opencart	Redis	TCP : 6379
Catch All Policy	DENY			


Application Insight
Whitelist Policy
Cisco Tetration Analytics
Policy Simulation and Compliance
Real-Time and Historical Compliance
Misdropped
0
Escaped
174
Rejected
73
180
160
140
120
100
80
60
40
20
0
12 PM
8/30
12 PM
8/31
12 PM
9/1
12 PM
9/2
12 PM
9/3


Zero Trust Policy Enforcement
Native Endpoint Firewalls
IPSets
IPTables
Windows Server
ACI Policy
APIC
Firewall Policy
Application Insight
Whitelist Policy
Cisco Tetration Analytics
Policy Enforcement
Policy Simulation and Compliance


Cisco
Tetration
Analytics
Any Application, Any Endpoint
vmware
Hyper-V
kvm
vmware
Bare Metal
Virtual Machine
Container

Cisco Tetration
Use cases

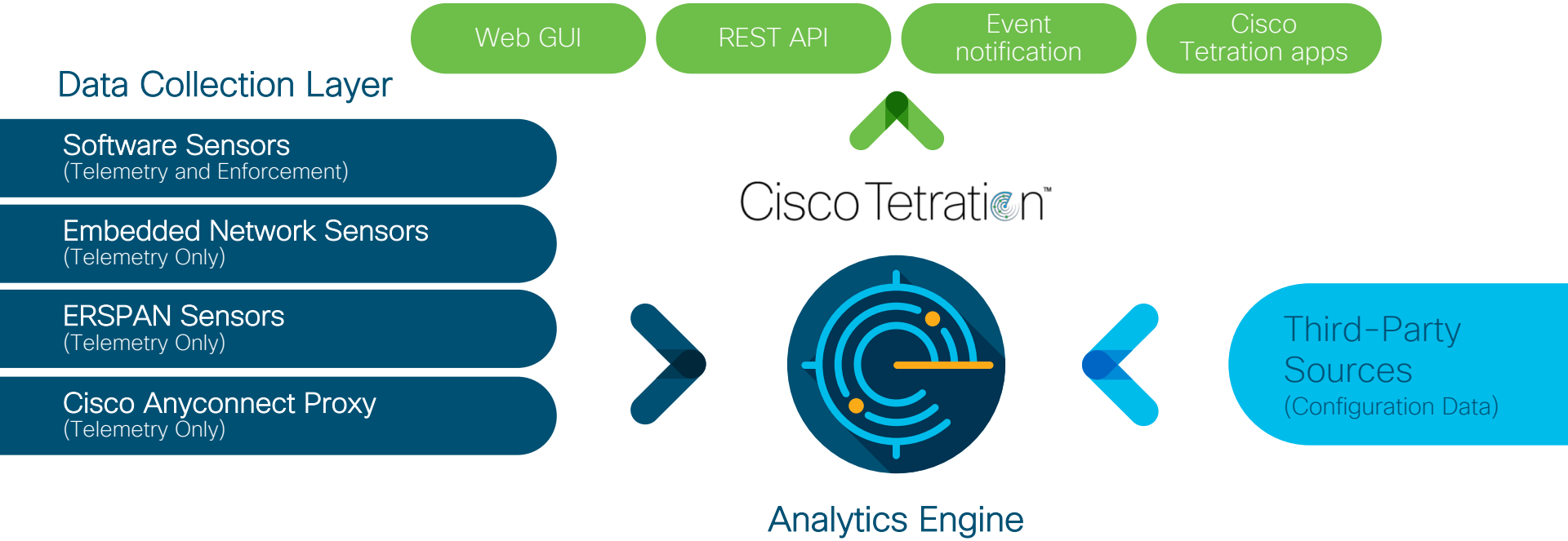
Use cases

- Data Center – change
- Application Rationalization
- Mergers and Acquisitions
- Customer Onboarding
- Automation Projects
- Application-segmentation / Micro-segmentation
- Common Issue – Visibility, dependency
- Compliance

Cisco Tetration Platform

Network Insights that enable efficient operations

Cisco Tetration Platform
Architecture overview



Cisco Tetration data sources

Software sensors

Virtual, Bare metal and Containers

- Linux servers (virtual machine and bare metal)
- Windows servers (virtual machines and bare metal)
- IBM z/Systems (IBM z/Linux operating system)
- Windows desktop VM (virtual desktop infrastructure only)
- Container host (Linux container host OS)

Network sensors

Next-generation Cisco Nexus® Series Switches

- Cisco Nexus 9300 EX
- Cisco Nexus 9300 FX
- Cisco Nexus 9000 FX2

Other sensors

Other types of sensors

- ERSPAN sensor
- Cisco Anyconnect

*Telemetry augmentation only

Main features

- Low CPU overhead (SLA enforced)
- Low network overhead
- Enforcement point (software agents)
- Highly secure (code signed and authenticated)
- Every flow (no sampling) and no payload
- Server process and software package information

Application segmentation

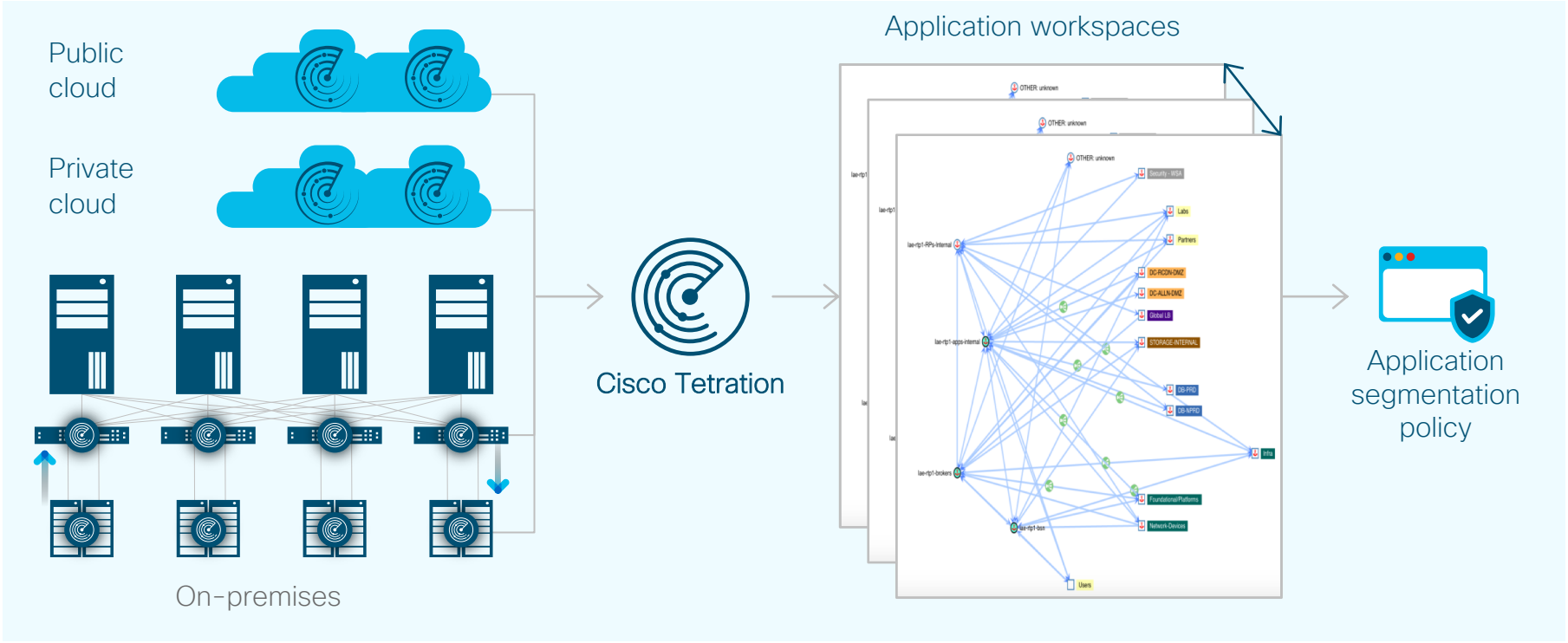
Cisco Tetration

Control communication using whitelist

Main features

- Auto generate whitelist policy based on application behavior
- Keep the policy up to date as application evolves
- Perform what-if analysis for policies using historical data

Cisco Tetration application segmentation
whitelist policy recommendation



Metadata based policy definitions

Discovered inventory

Uploaded inventory and metadata (32 arbitrary tags)

Inventory tracked in real time, along with historical trends

CMDB data sources

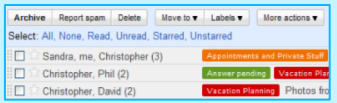
VMware vCenter (virtual machine attributes)

AWS attributes (AWS tags)

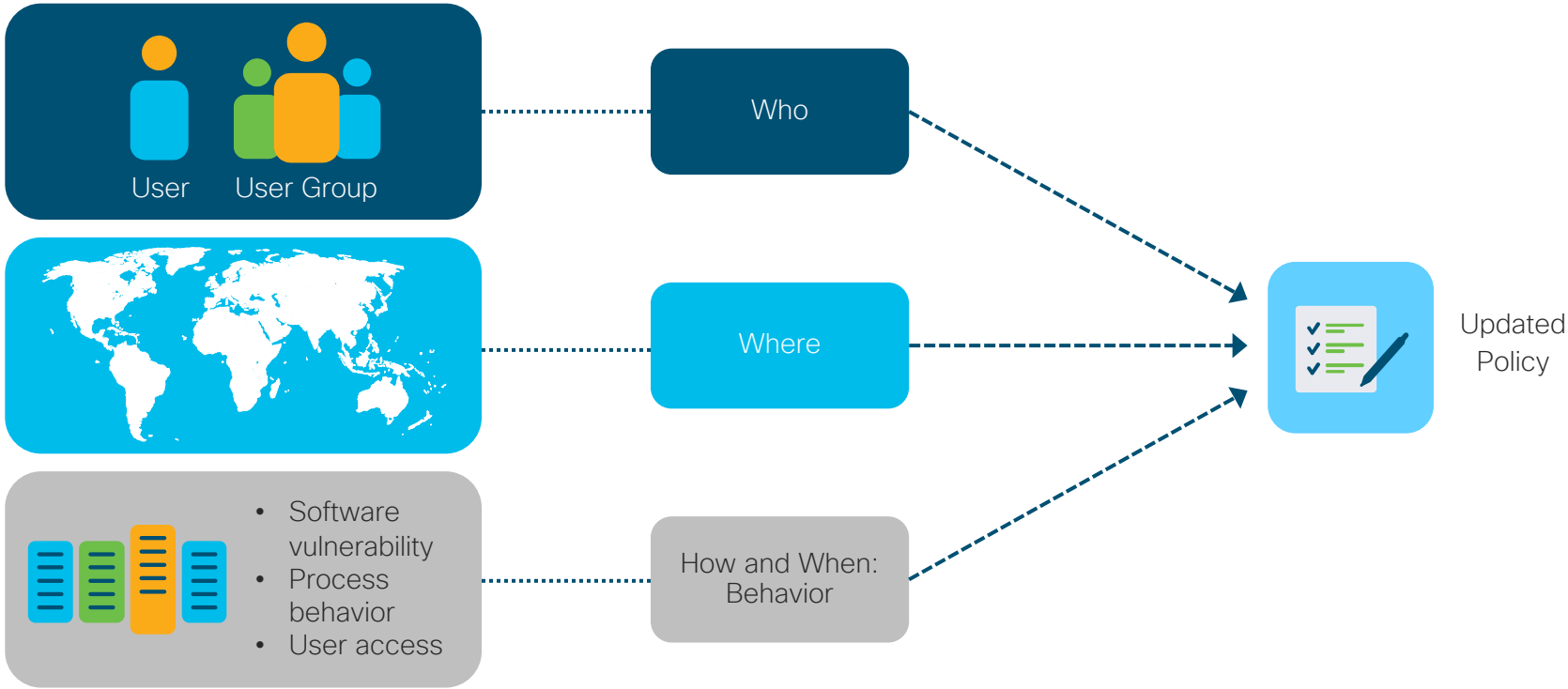
Kubernetes or Openshift (container attributes)

Cisco Tetration Analytics merge operation

Real-time inventory merged with information with historical trends



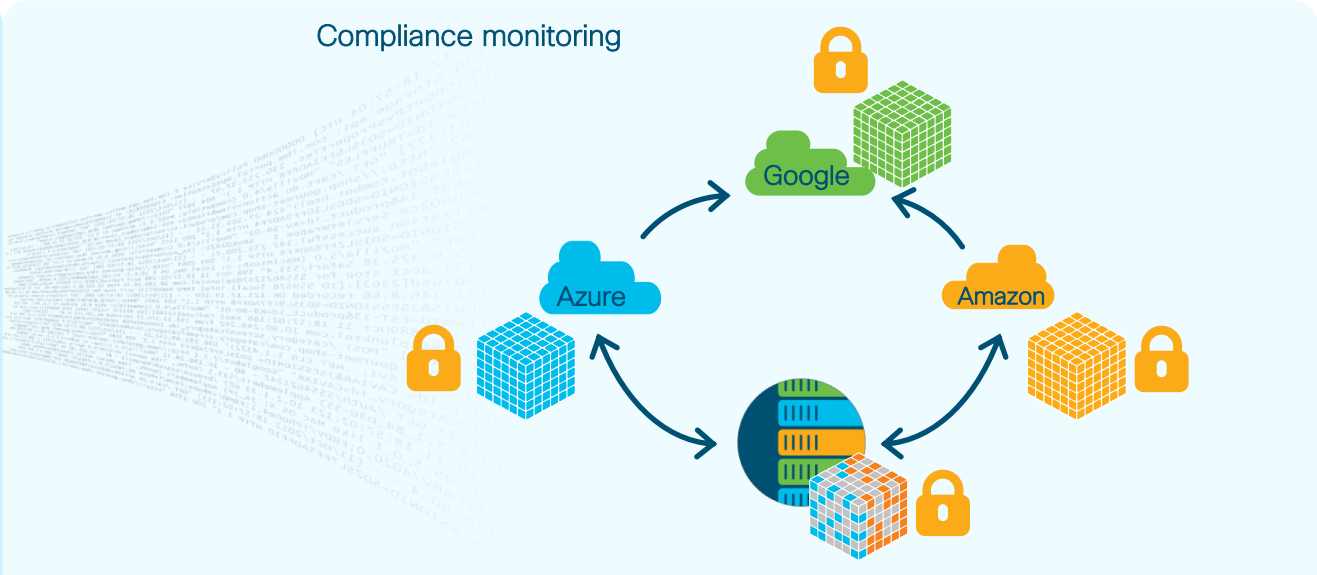
Other policy definition attributes



Enforcement of policy across any floor tile

Cisco Tetration Analytics™

1. Generates unique policy per workload
2. Pushes policy to all workloads
3. Workload securely enforces policy
4. Continuously recomputes policy from identity and classification changes



Enforcement

Public cloud

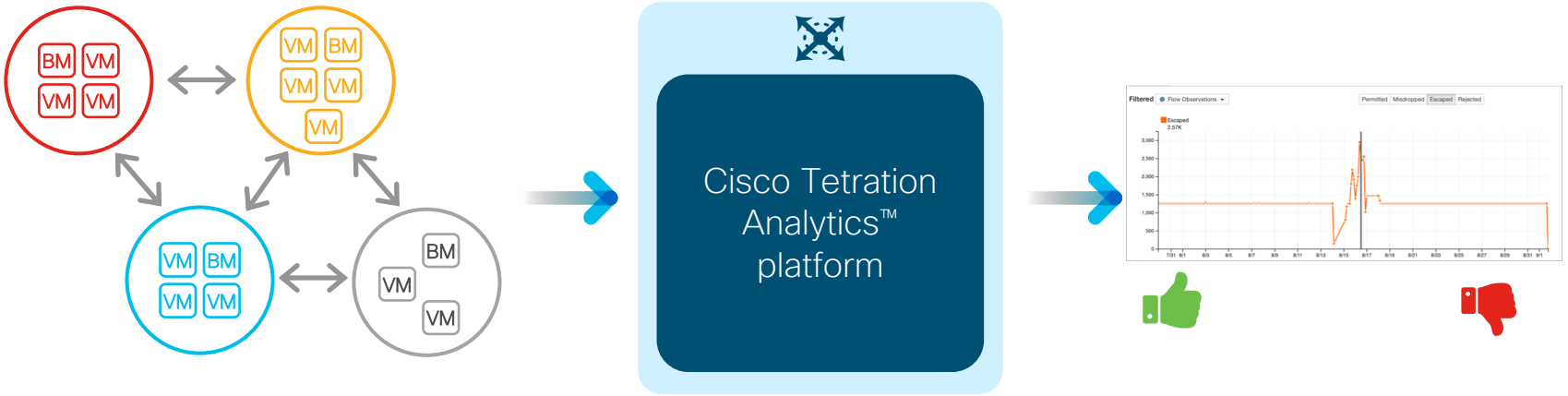
Bare metal

Virtual

Cisco ACI™

Traditional network

Policy compliance



Identify policy deviations in real time

Review and update whitelist policy with one click

Perform policy lifecycle management

Application Security assessment

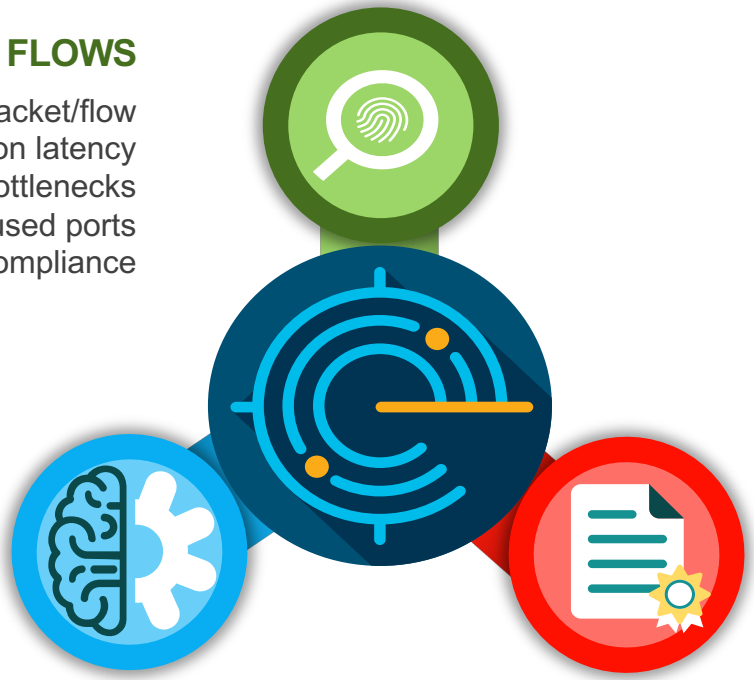
Micro-segmentation is a MUST
…but bad things can still happen

COMMUNICATION / FLOWS

Every single packet/flow
Network/Application latency
Performance Bottlenecks
Open unused ports
Compliance

PROCESS BEHAVIOUR ANALISYS

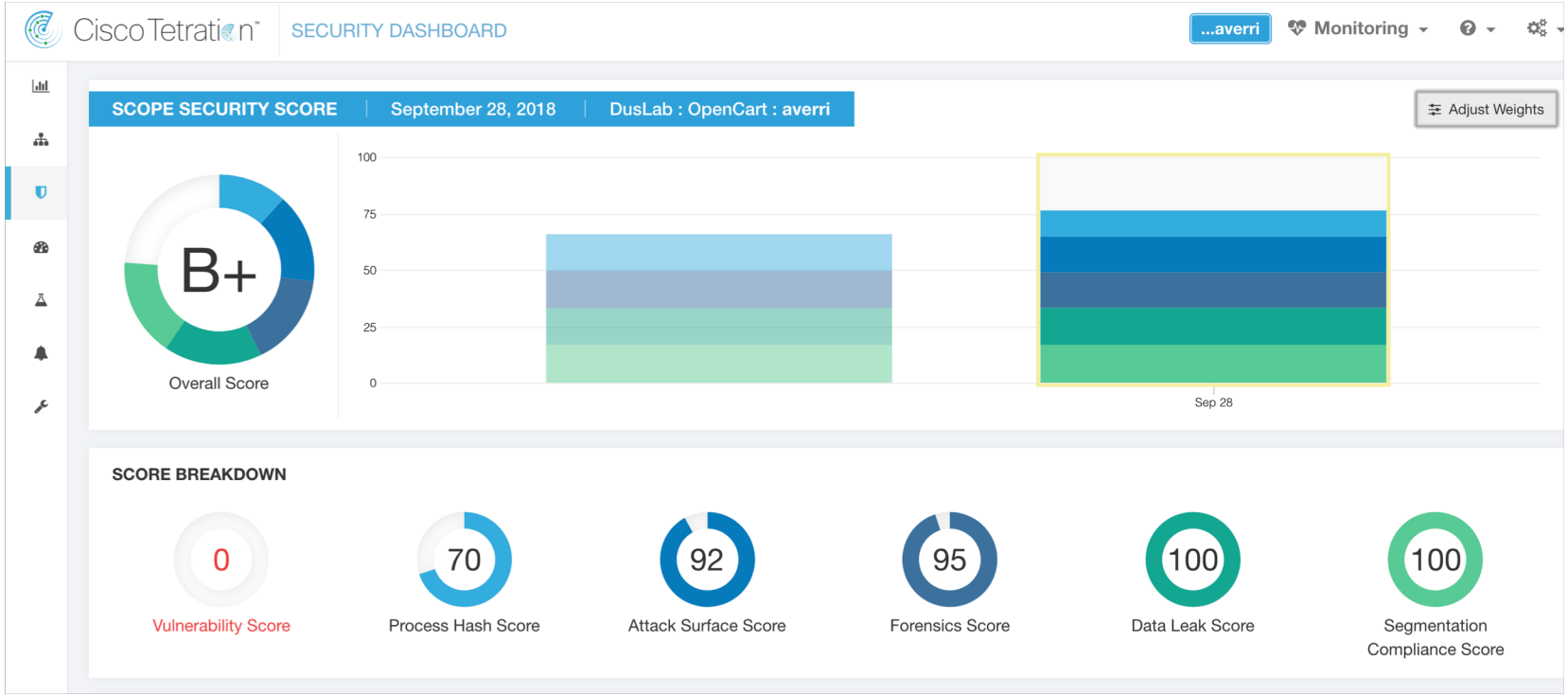
Process hash anomaly detection
Consistency
of process binary hashes
across the system
detects process hashes in a blacklist
Hash dataset as a whitelist, considered “safe” hashes



VULNERABILITIES

Software or modules installed in workloads
Validation against NIST CVE

Security Dashboard
Score per Application

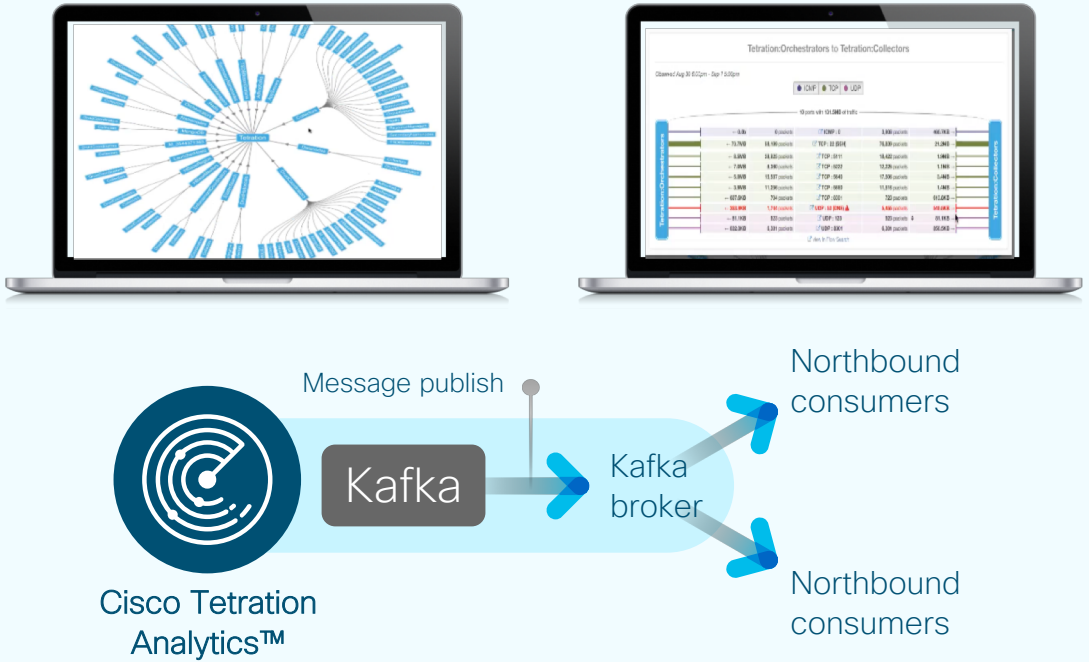


Neighborhood Graphs

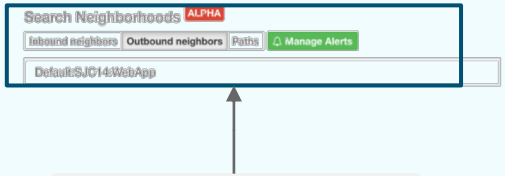
Insight-based notification: Neighborhood graphs

Neighborhood graphs

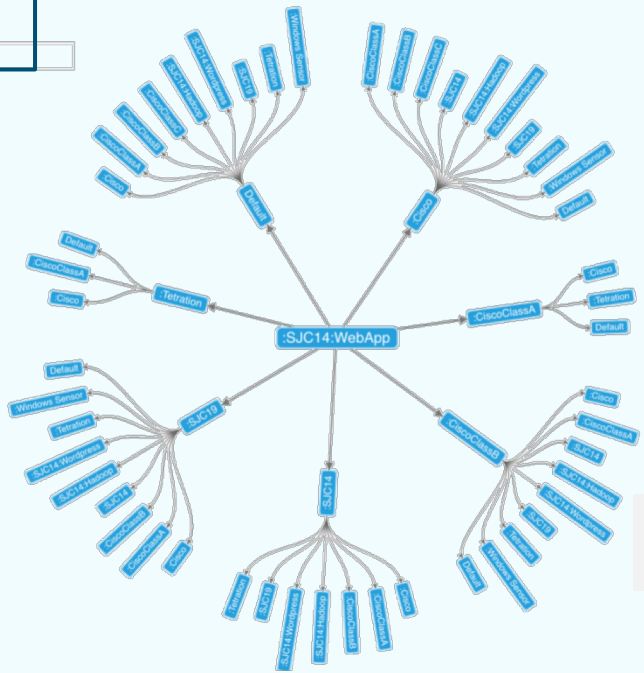
- Find up to two-hop communication neighbors for a selected workload
- Drill down into details about communication between these neighbors
- View dashboard display using graph database
- Determine the number of server hops between two workloads
- Get out-of-the-box and customer alerts through Kafka

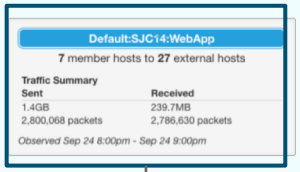


Neighborhood graph and summary information



Search for an Inventory filter, scope, or cluster





Two-hop communication summary with network traffic details

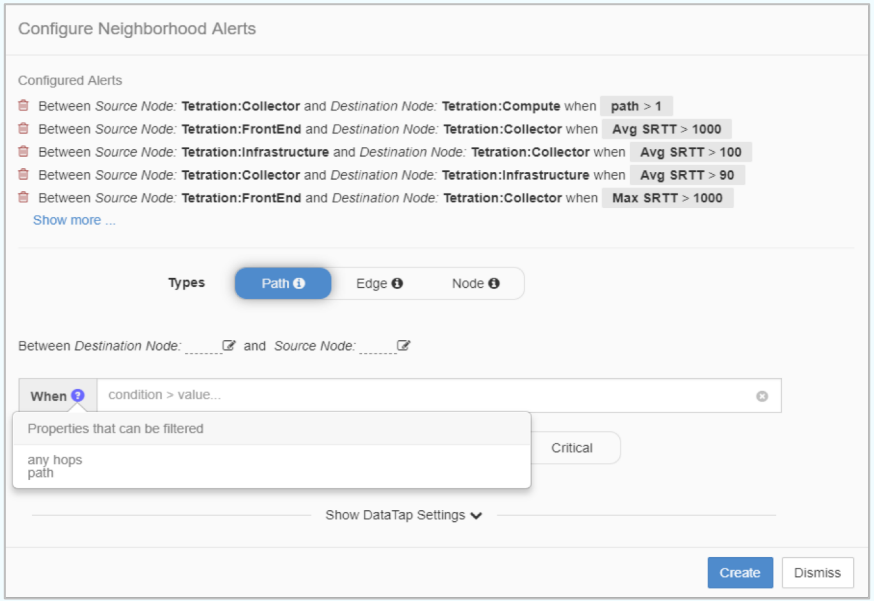
Nodes in radial tree are clickable for exploration

Paths from Default:SJC14:WebApp

Neighborhood application: Alerts

Allows users to configure alerts in three scenarios:

- Path between two nodes has decreased below some minimum hop count
  - Example: “Database should never be directly communicate to Scope X”
- Edge performance characteristics
  - Example: “Average round trip latency between source and destination is > X”
- Node characteristics
  - Example: “Number of cluster members or adjacency count is > X”



Deployment options

Cisco Tetration: On-premises deployment options

On-premises appliance 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

Virtual appliance options

Cisco Tetration Virtual

- Suitable for deployments of up to 1000 workloads
- Supported in VMware ESXi-based environment
- Customers provide their own hardware and storage to run Tetration-V
- Simplified deployment process
- Faster realization of Tetration benefits

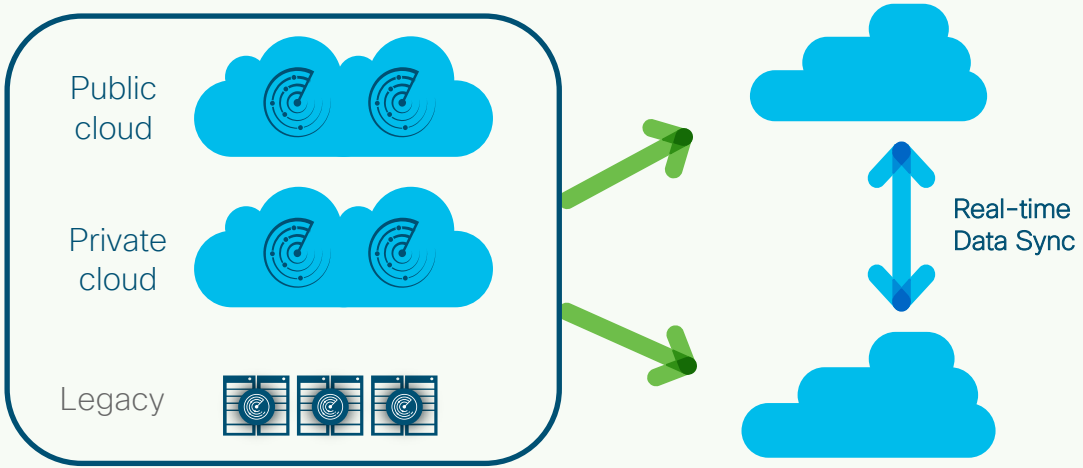
vmware ESXi

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

Cisco Tetration software-as-a-service option

Cisco Tetration™ SaaS

- Software-as-a-service model: No need to purchase, install and manage hardware or software
- Fully managed and operated by Cisco
- Suitable for commercial customers and SaaS-first/SaaS-only customers
- Flexible pricing model; lower barrier to entry
- Quick turn up
- Scales to up to 25,000 workloads



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

In summary: Platform built for scale and flexibility

Real time and scalable

- Every packet, every flow
- Application segmentation for 1000s of applications
- Extends visibility to process and software packages
- Long term data retention

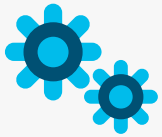
Holistic workload protection

- Consistent application segmentation
- Any workload, anywhere
- Process behavior deviations
- Software package vulnerability

Easy to use

- One touch deployment
- Self monitoring
- Self diagnostics

Open



- Standard web UI
- REST API (pull)
- Event notification (push)
- Tetration applications


CISCO