



# Tetration Briefing

Workload protection with Cisco Tetration

# Modern applications...



# Cisco Zero Trust

Secure access for your workforce, workloads and workplace.

## Duo for Workforce

Ensure only the right users and secure devices can access applications.



## SD-Access for Workplace

Secure all user and device connections across your network, including IoT.

## Tetration for Workload

Secure all connections within your apps, across multi-cloud.

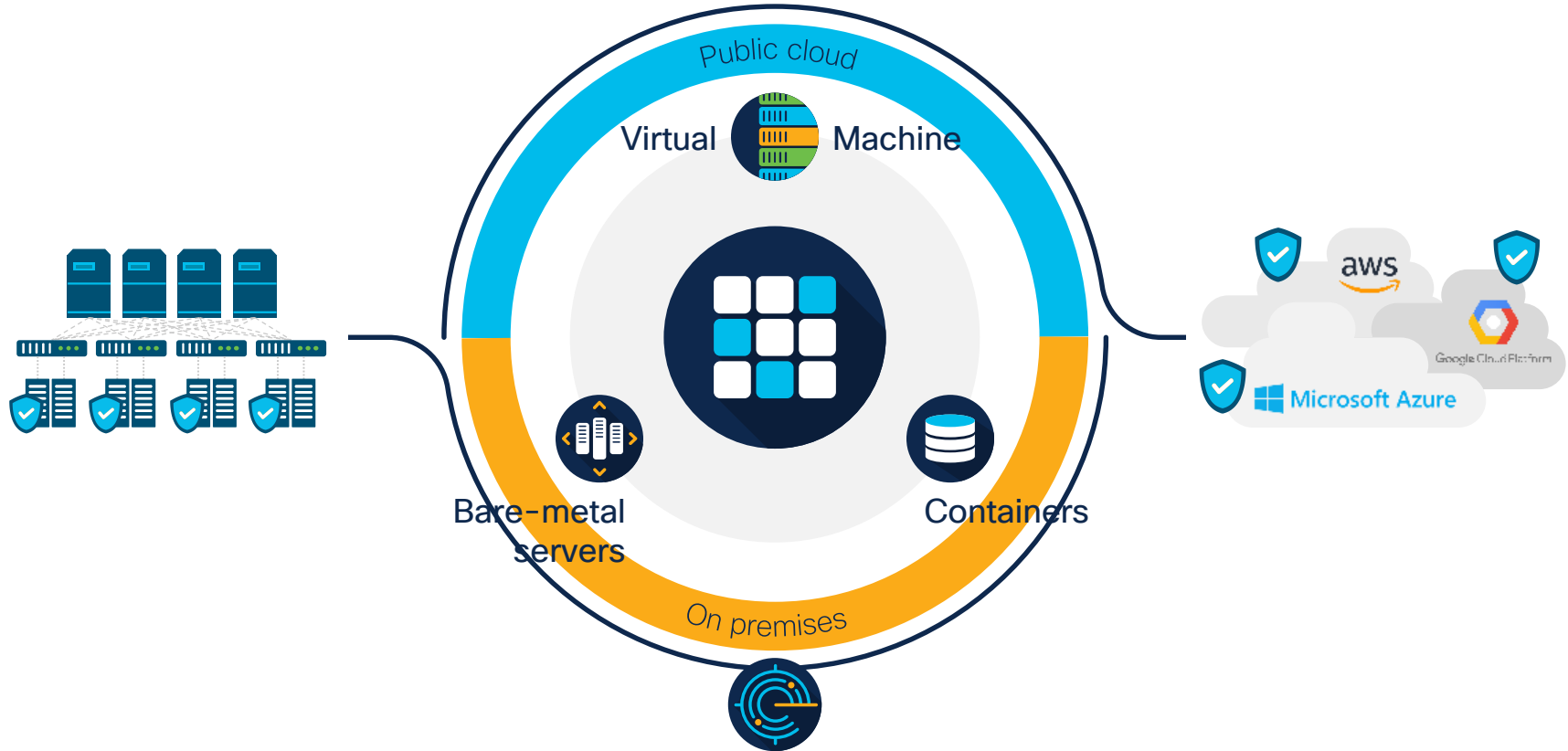
Enforce Policy-Based Controls



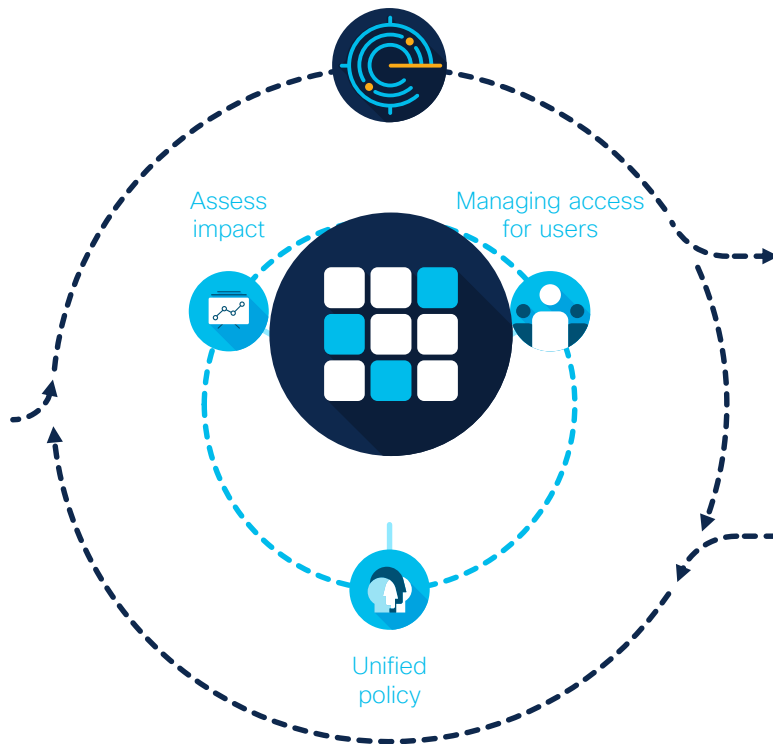
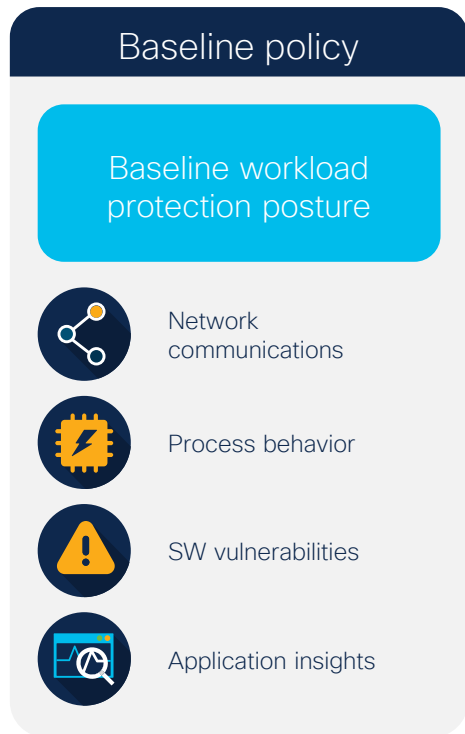
# App-first security with Cisco Tetration



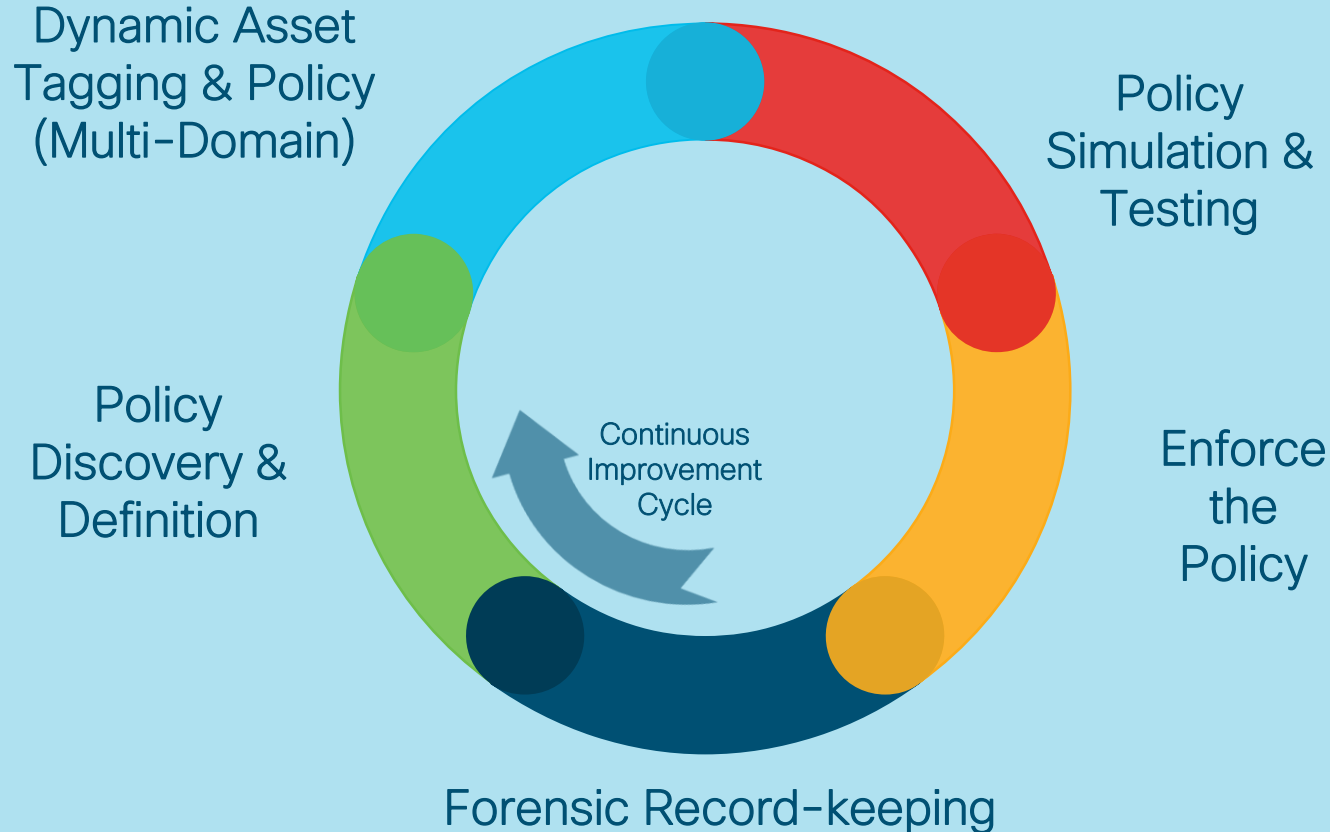
# Adaptive application segmentation



# Cisco Tetration secure any workload, anywhere



# Example: Segmentation





# Tetration Workload Protection Capabilities



## Insights



## Segmentation



## Advanced Protection



Visibility and  
Forensics



Zero Trust policy



Process Security



Process Inventory



Application  
Segmentation



Vulnerability  
Identification



Application Insights



Policy Compliance  
& Simulation



Software  
inventory baseline





Tetration  
Cloud Workload Protection  
**Customer Drivers**

**Multi-Cloud**

Consistent visibility and policy on any cloud: a key enabler for Multi-Cloud

**Compliance**

Take out time and cost. Use hard data to demonstrate compliance.

**Security Hardening**

Dramatically reduce risk by understanding app behavior and minimizing surface attack area

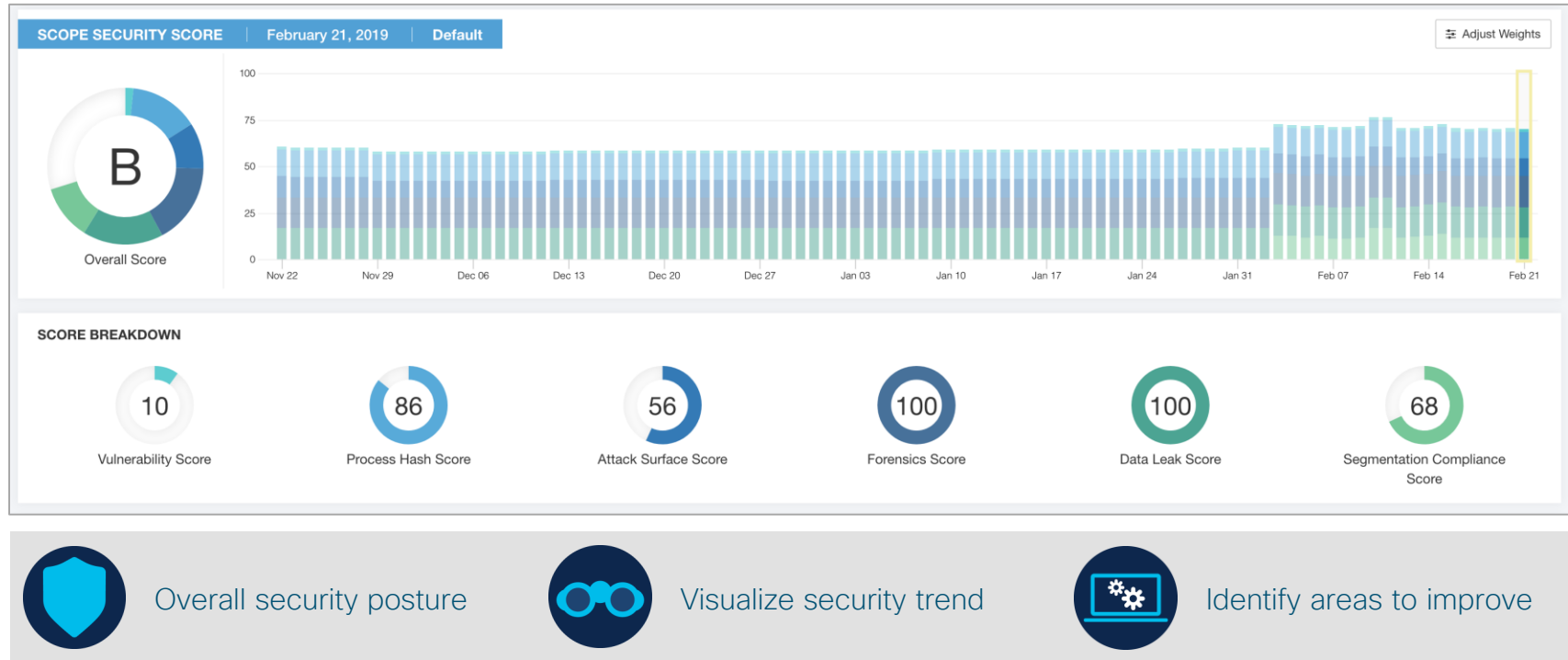
**Confidence**

Move with speed and confidence in Mission Critical Environments.

**Consolidation**

Enable shared services & new business models.

# Bringing all this together: the security dashboard





# Cisco, as open as you want it to be



Be open.

- Standard APIs and notification mechanisms
- Ecosystem of partners

Cisco Tetration™

F5  
Networks

Citrix

Avi  
Networks

Splunk

ServiceNow

AlgoSec

VMware  
vSphere

Kubernetes

OpenShift

Infoblox

# Flexible consumption models

On-premises and Software-as-a-Service (SaaS) options



Tetration™ on-premises

## On-premises options

1. Hardware-appliance-based options:
  - Form factors that support medium and large data centers
2. Virtual appliance option:
  - Suitable for smaller data centers
  - Supported on Cisco HyperFlex™ or customer-owned hardware



Tetration SaaS

## Software-as-a-Service

- Fully managed and operated by Cisco
- Suitable for any customer (small, medium, or large enterprises)
- Flexible pricing model; lower barrier to entry
- Quick turn-up and faster realization of value

Option for Partner Hosted

The software subscription license is based on the number of workloads; available in 1-, 3- and 5-year terms.

# Cisco application-first security using Tetration

Cisco empowers you to secure applications that run anywhere, change constantly, and are unique, at the speed of your digital business.



Run anywhere

Security controls closer to applications



Change constantly

Automated security-posture updates



Are unique

Tailored security based on application behavior



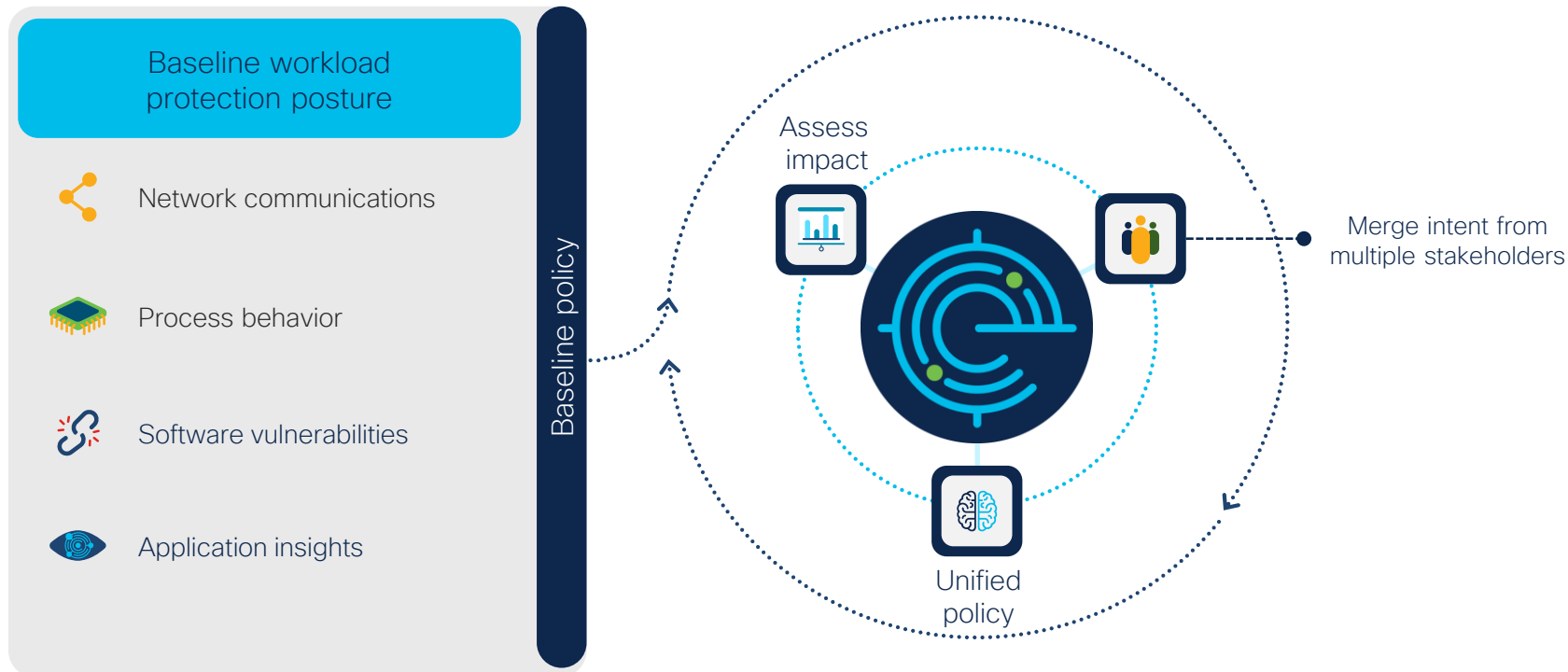
# Workload security with Cisco Tetration



Contain lateral movement  
using microsegmentation

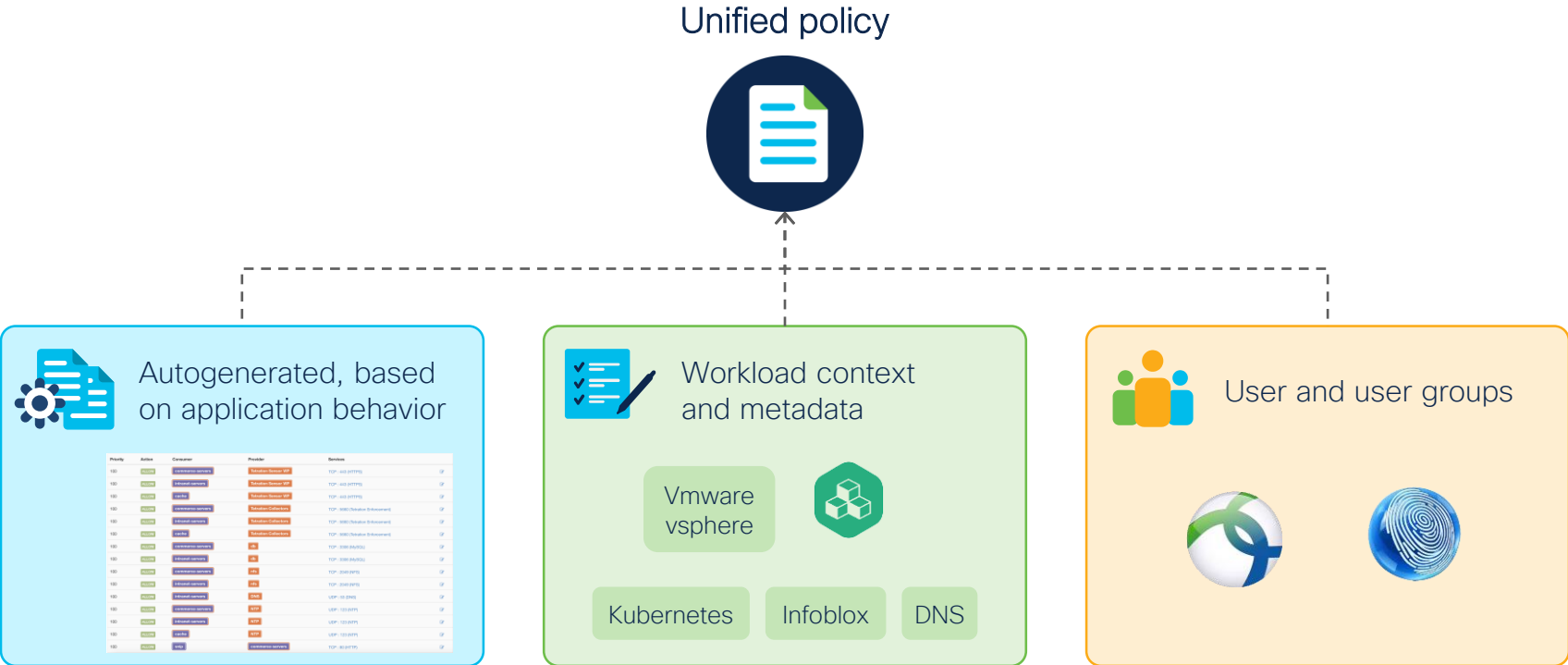
# Tetration – cloud workload protection

## Attribute- and behavior-based security policy and segmentation



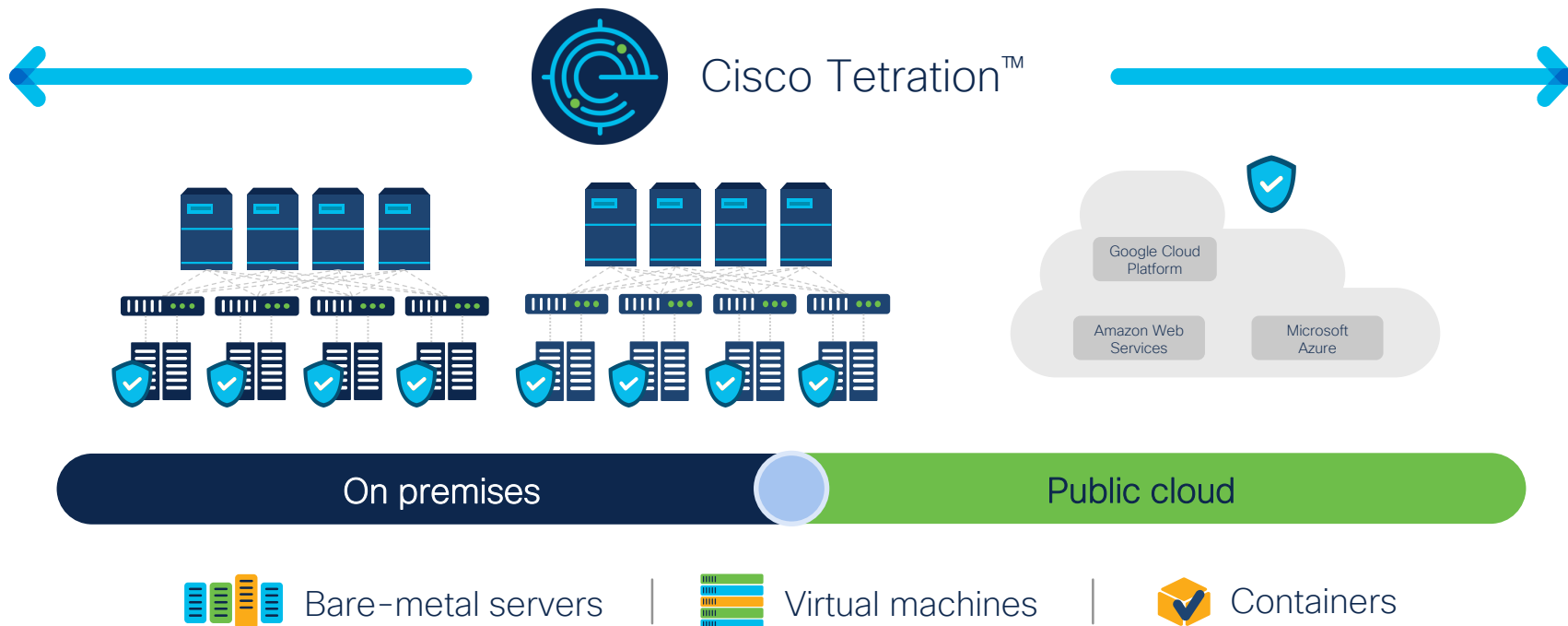


## Rich attribute set with multiple data sources



# Adaptive application segmentation

Consistent application microsegmentation: any workload, anywhere



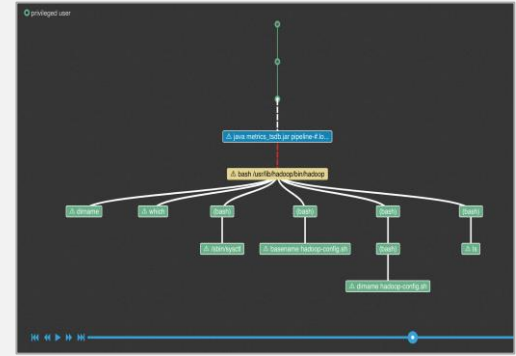
Identify workload behavior  
anomalies

# Workload process

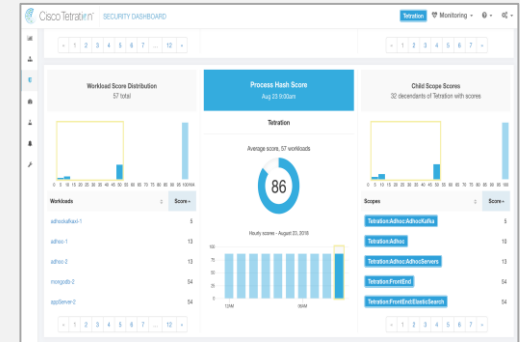


## Workload- process behavior anomalies

- Detect common anomalies based on predefined forensic rules
- Identify anomalies based on MITRE techniques and tactics



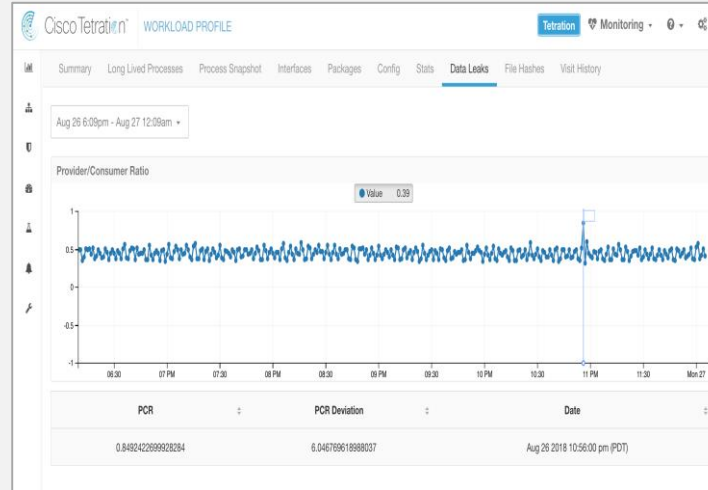
- Quickly detect malicious processes running in the workloads based on the hash
- Whitelist processes that can run in the workload and get alerts if a new process spins up



# Network communication

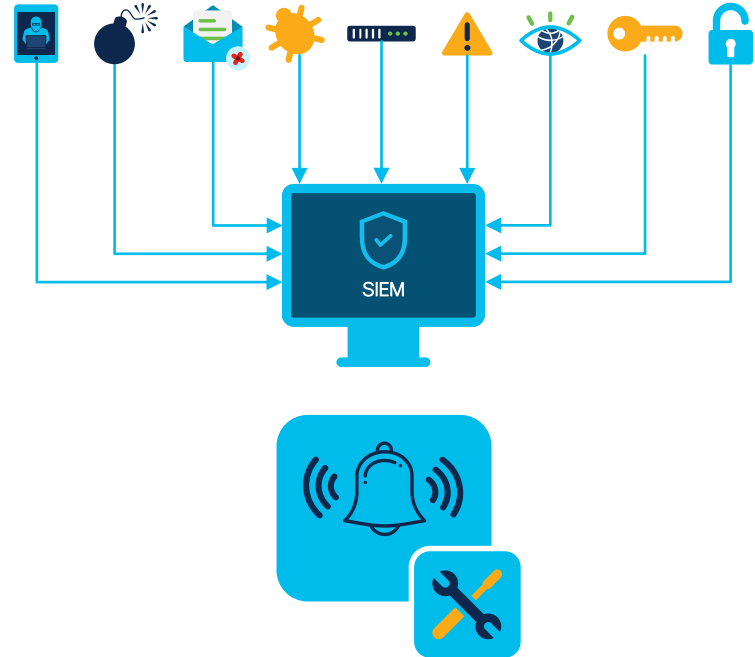
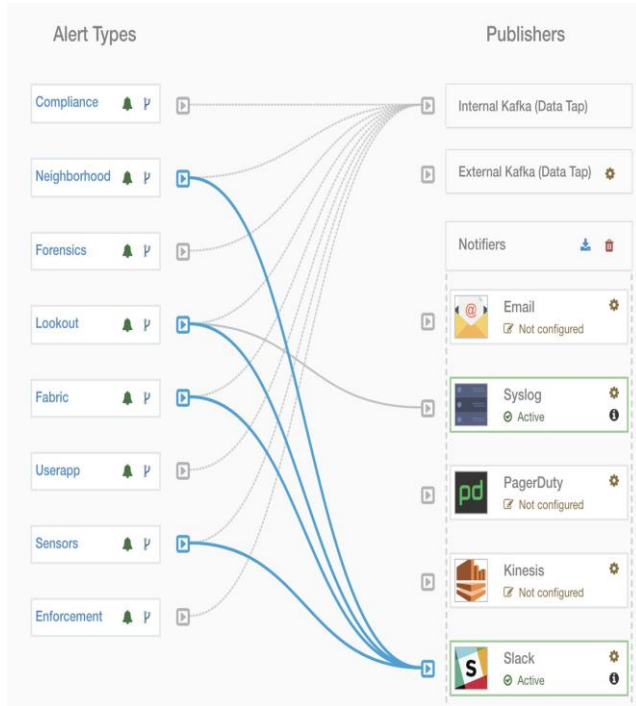


Network  
communication  
anomalies




- Proactively detect network communication anomalies and receive alerts
- Correlate with other forensic events to determine if there is a potential data leak event

# Alerts to other northbound systems

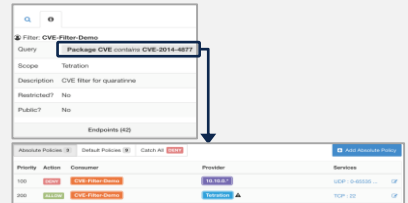
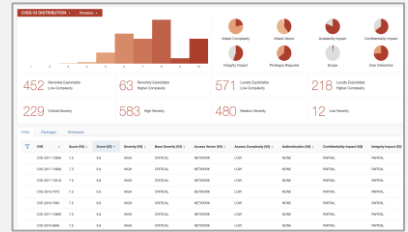
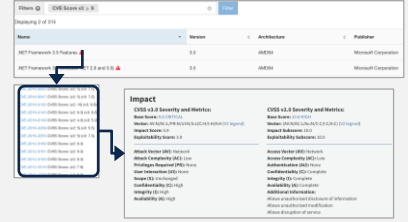


Reducing the attack surface



# Software vulnerabilities

- Identify known vulnerabilities associated with software packages and the OS kernel
  - Find out how many workloads have a given vulnerability
- 
- Get more information about the nature of vulnerabilities, for prioritization
- 
- Set up policy through UI or API to take specific actions
  - Quarantine a host when servers are identified with given vulnerability



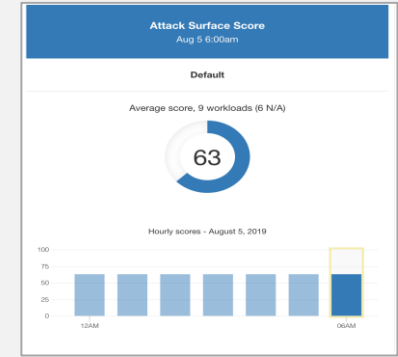


# Stale ports, processes, and vulnerability correlation



## Stale ports and processes

- Determine if there are open ports and processes without any activity
- Find out which application, workloads, and processes are part of this security exposure



- Determine if this process is associated with a software with known vulnerability

**Attack Surface Details - EC2AMAZ-HHIF4L3**  
Aug 5 7:00am to Aug 5 9:00am

28 Total Ports (26 unused ports on this workload)

Unused Ports Only

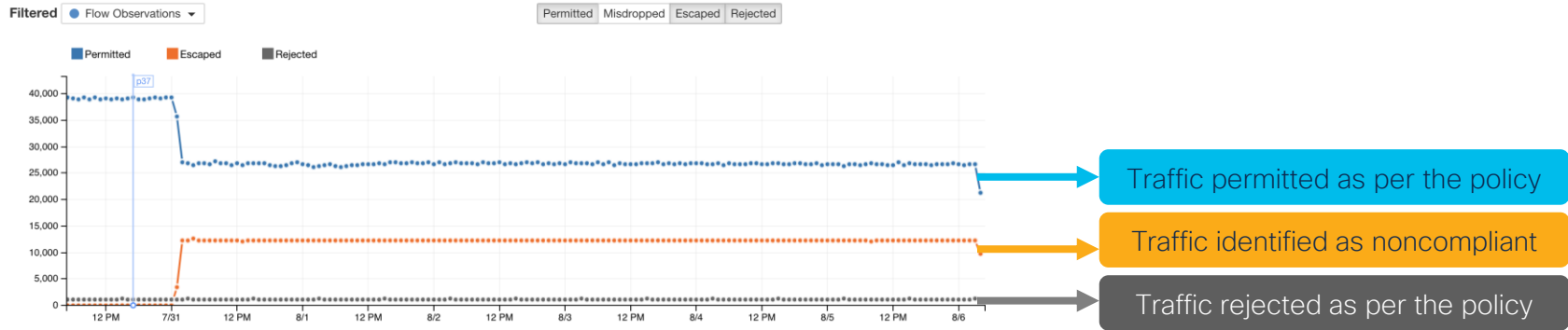
These are open ports and interfaces that haven't had traffic in the last 15 days (see help for specifics). Consider closing them to reduce your attack surface (and increase your Attack Surface Score) if they aren't needed.

Port	Package Name	Total Permitted	CVE Max Score	Process Hash	Interfaces	Package Publisher
123 (NTP)	None	N/A	None		2	N/A
135	None	N/A	None	..Office?	1	N/A
137 (NetBIOS Name Service)	None	N/A	None		1	N/A
138 (NetBIOS Datagram Service)	None	N/A	None		1	N/A
139 (NetBIOS Session Service)	None	N/A	None		1	N/A
445 (Microsoft-lls)	None	N/A	None		1	N/A
500 (ISAKMP)	None	N/A	None	..Office?	2	N/A
546	None	N/A	None		1	N/A
1800	None	N/A	None		2	N/A
3389 (Remote Desktop)	None	37238	None	..Office?	2	N/A

Segmentation policy  
compliance

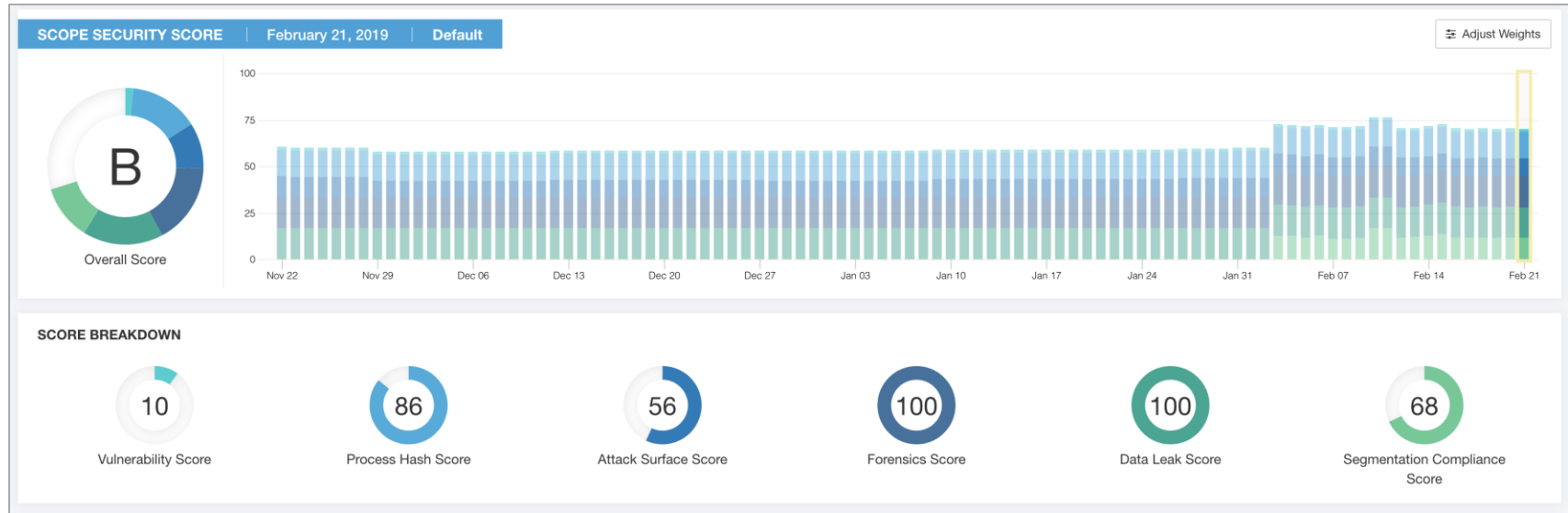
# Policy compliance with Cisco Tetration

With Cisco Tetration™, you can, in near real-time, detect applications that are trying to communicate outside of a set segmentation policy.



Generate notifications to SIEM or other systems when such an event occurs.

# Bringing all this together: the security dashboard



Overall security posture



Visualize security trend



Identify areas to improve

# Achieve the workload security required for successful digital transformation



Any cloud



Any application



Any workload



Anywhere

Ecosystem integrations



# Cisco, as open as you want it to be



Be open.

- Standard APIs and notification mechanisms
- Ecosystem of partners

Cisco Tetration™

F5  
Networks

Citrix

Avi  
Networks

Splunk

ServiceNow

AlgoSec

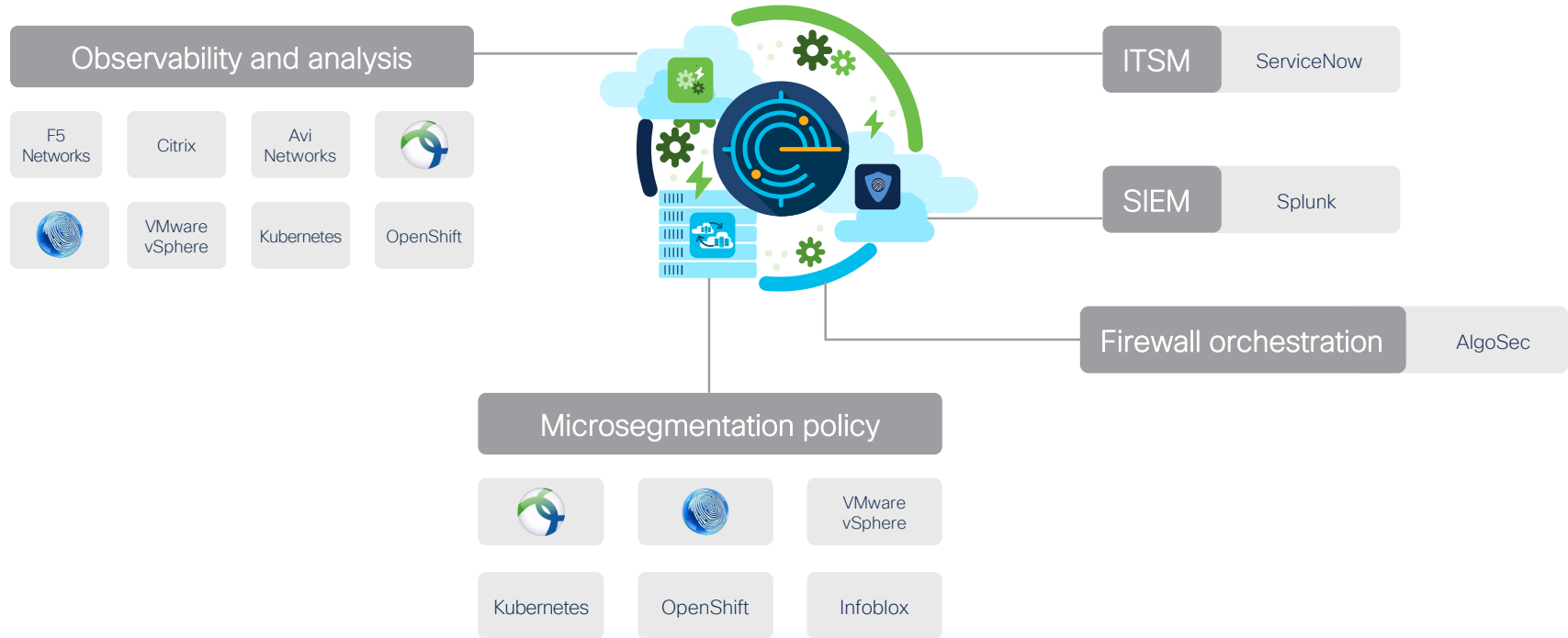
VMware  
vSphere

Kubernetes

OpenShift

Infoblox

# Furthering your reach with Tetration integrations





Deployment options

# Flexible consumption models

On-premises and Software-as-a-Service (SaaS) options



Tetration™ on-premises

## On-premises options

1. Hardware-appliance-based options:
  - Form factors that support medium and large data centers
2. Virtual appliance option:
  - Suitable for smaller data centers
  - Supported on Cisco HyperFlex™ or customer-owned hardware



Tetration SaaS

## Software-as-a-Service

- Fully managed and operated by Cisco
- Suitable for any customer (small, medium, or large enterprises)
- Flexible pricing model; lower barrier to entry
- Quick turn-up and faster realization of value

The software subscription license is based on the number of workloads; available in 1-, 3- and 5-year terms.

