Как мониторить безопасность и защищать приложения в частных и публичных облаках?

Mikhail Kader, mkader@cisco.com, security-request@cisco.com

20.05.2021

Applications are instrumental to modern business

Digital transformation **is “finally” here – this is the impact:**

New applications are developed infrastructure agnostic

Application modernization untangles apps from infrastructure

5-10%
of all apps
/ year

Where:
Cloud first

SaaS before PaaS before IaaS before building your own DC

Who:
Responsibility shifting

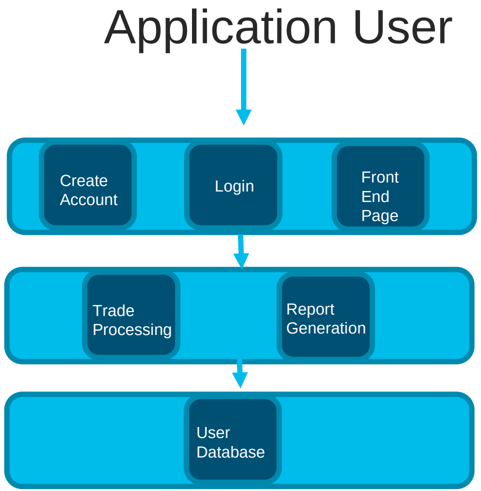
Application teams taking on security ownership – DevSecOps

How:
Development velocity

Up from months to hours, enabled by new architectures

Evolution to Micro Services

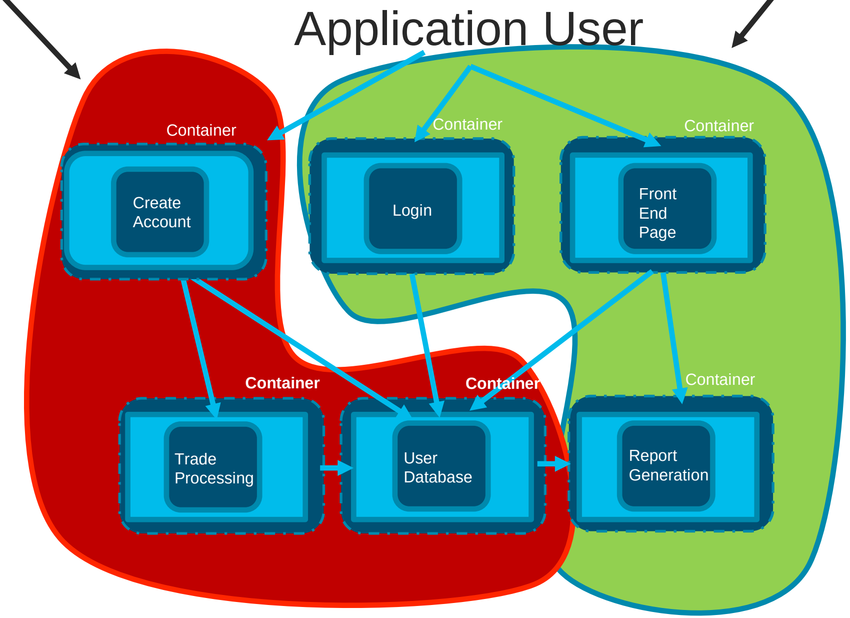
Monolithic – 3 Tier



Micro-services

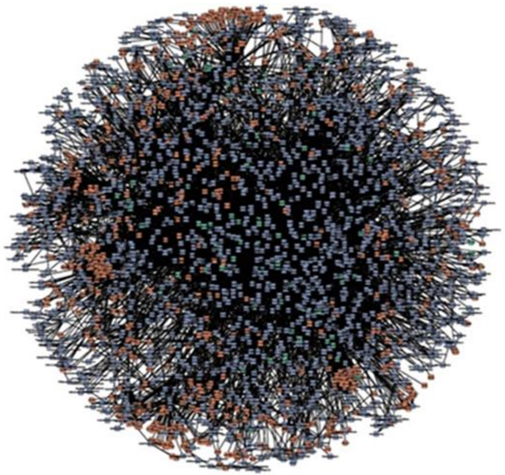
Optimized for
Security – slower rate of change

Rapid Iteration
And Development



Micro-Service Examples - Problems defined

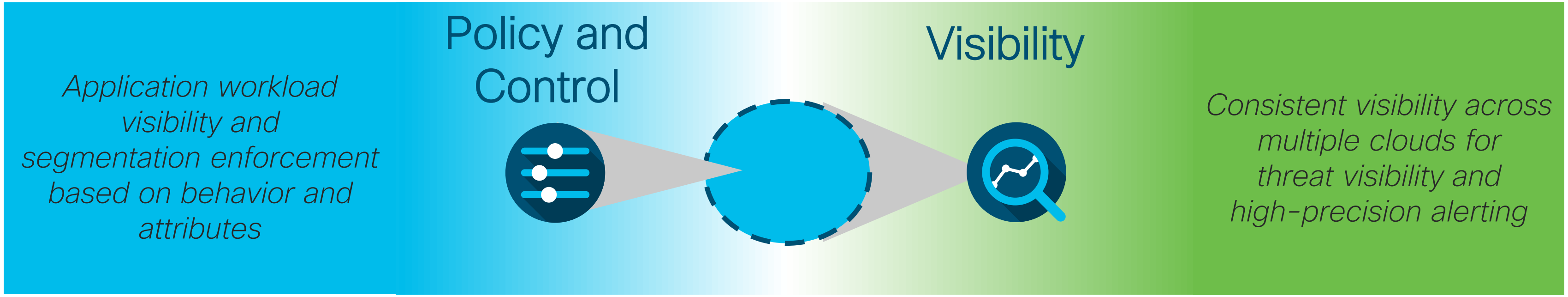
- No visibility for services
  - Unused services
  - Untrusted services
  - Dangerous services
  - Users/Services mapping
  - Services/Services mapping
- No visibility for threats
  - Data leakage
  - Malware
  - DDoS
  - Covert channels
  - Etc..



amazon.com

NETFLIX

Deep visibility & control for your workload and cloud infrastructure



Application workload visibility and segmentation enforcement based on behavior and attributes

Policy and Control

Visibility

Consistent visibility across multiple clouds for threat visibility and high-precision alerting

Continuous policy creation and control of application behavior

+

Across your entire cloud infrastructure monitor for behavior changes and threats

=

Gain wide security visibility across clouds and enables precision automated enforcement for workloads

Consistent policy and control

Cisco Secure Workload (Tetration)

Segmentation

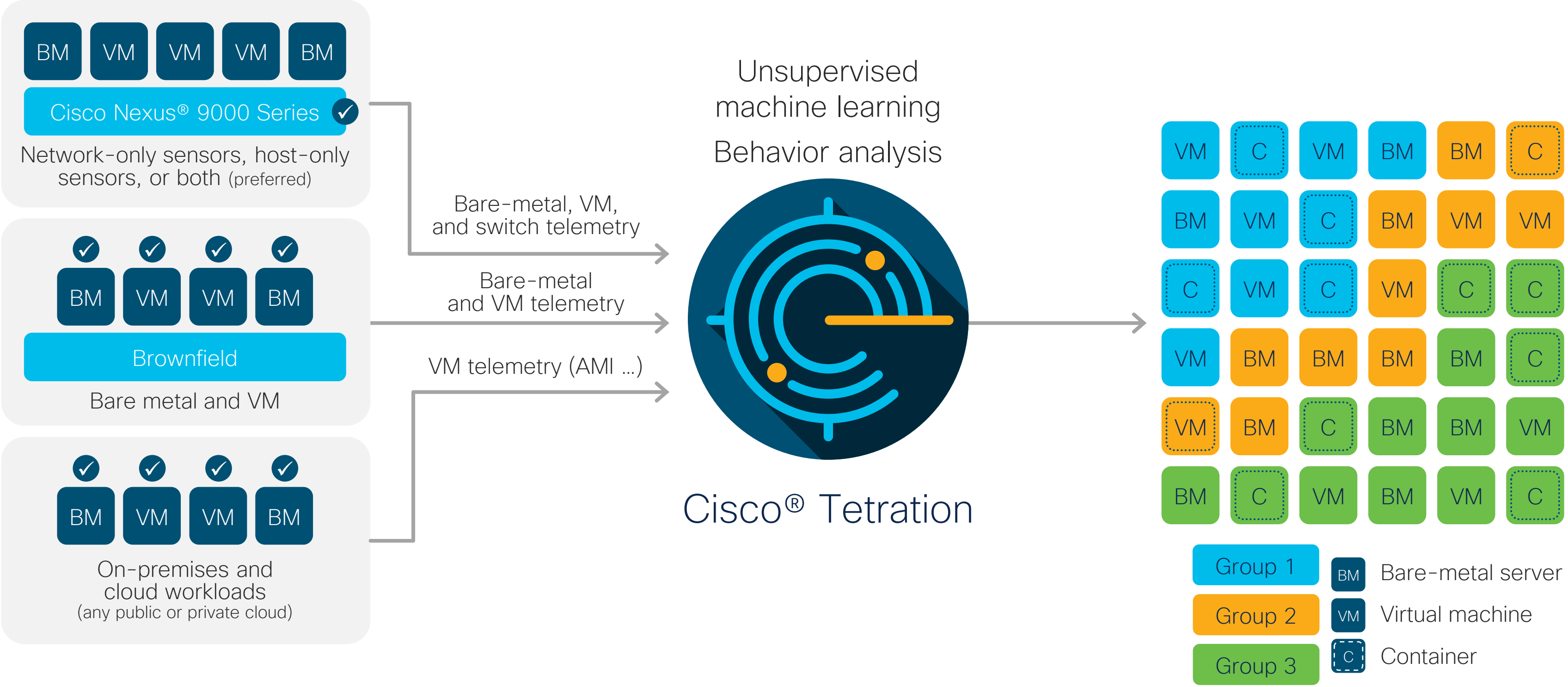
Segmentation policy elements

Autogenerated based on application behavior

Workload context and metadata

Workforce and endpoint devices

Application dependency and cluster grouping



BM VM VM VM BM

Cisco Nexus® 9000 Series ✓

Network-only sensors, host-only sensors, or both (preferred)

✓ ✓ ✓ ✓

BM VM VM BM

Brownfield

Bare metal and VM

✓ ✓ ✓ ✓

BM VM VM BM

On-premises and cloud workloads
(any public or private cloud)

Bare-metal, VM, and switch telemetry

Bare-metal and VM telemetry

VM telemetry (AMI ...)

Unsupervised machine learning

Behavior analysis

Cisco® Tetration

VM	C	VM	BM	BM	C
BM	VM	C	BM	VM	VM
C	VM	C	VM	C	C
VM	BM	BM	BM	BM	C
VM	BM	C	BM	BM	VM
BM	C	VM	BM	VM	C

Group 1

Group 2

Group 3

BM Bare-metal server

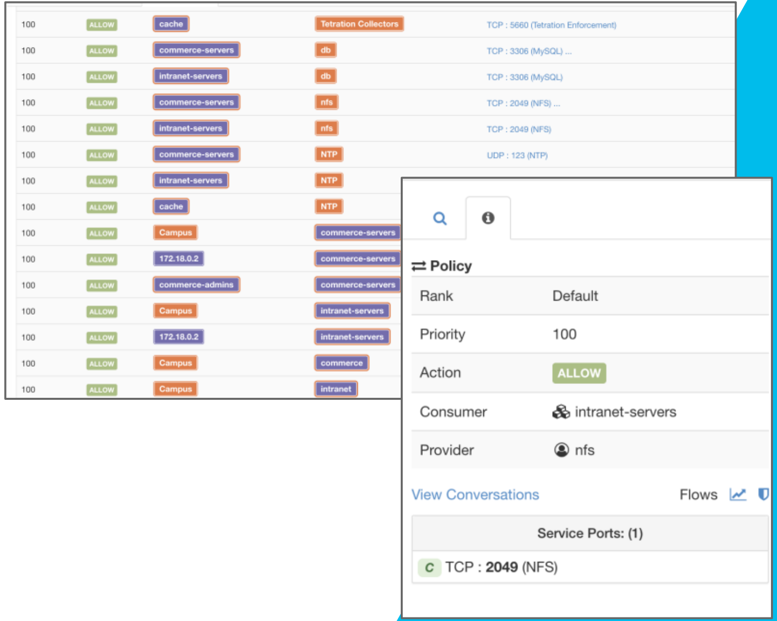
VM Virtual machine

C Container

Auto-generated segmentation policy

Automatically generated policy based on application behavior:

- Using an application dependency map as a blueprint, Tetration automatically generates the microsegmentation policy
- This policy allows the required traffic between the application components and infrastructure elements (DNS, NFS, NTP, etc.)
- The default catch-all policy is ”deny.” This can be changed to “allow” during the initial stages of enforcement to gain more confidence
    - Note: With a default catch-all of ”allow,” Tetration still detects policy compliance violations and alerts on those



100	ALLOW	cache	Tetration Collectors	TCP : 5660 (Tetration Enforcement)
100	ALLOW	commerce-servers	db	TCP : 3306 (MySQL) ...
100	ALLOW	intranet-servers	db	TCP : 3306 (MySQL)
100	ALLOW	commerce-servers	nfs	TCP : 2049 (NFS) ...
100	ALLOW	intranet-servers	nfs	TCP : 2049 (NFS)
100	ALLOW	commerce-servers	NTP	UDP : 123 (NTP)
100	ALLOW	intranet-servers	NTP	
100	ALLOW	cache	NTP	
100	ALLOW	Campus	commerce-servers	
100	ALLOW	172.18.0.2	commerce-servers	
100	ALLOW	commerce-admins	commerce-servers	
100	ALLOW	Campus	intranet-servers	
100	ALLOW	172.18.0.2	intranet-servers	
100	ALLOW	Campus	commerce	
100	ALLOW	Campus	intranet	

⇄ Policy

Rank	Default
Priority	100
Action	ALLOW
Consumer	intranet-servers
Provider	nfs

View Conversations

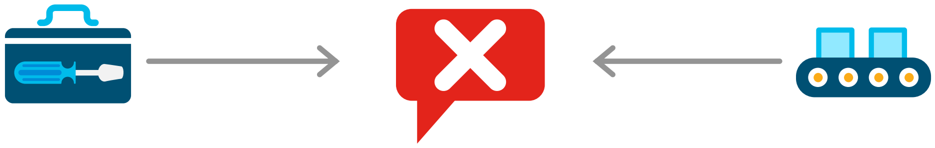
Flows

Service Ports: (1)

C TCP : **2049** (NFS)

Segmentation policies based on workload context

Public cloud workloads can’t talk to on-premises database servers



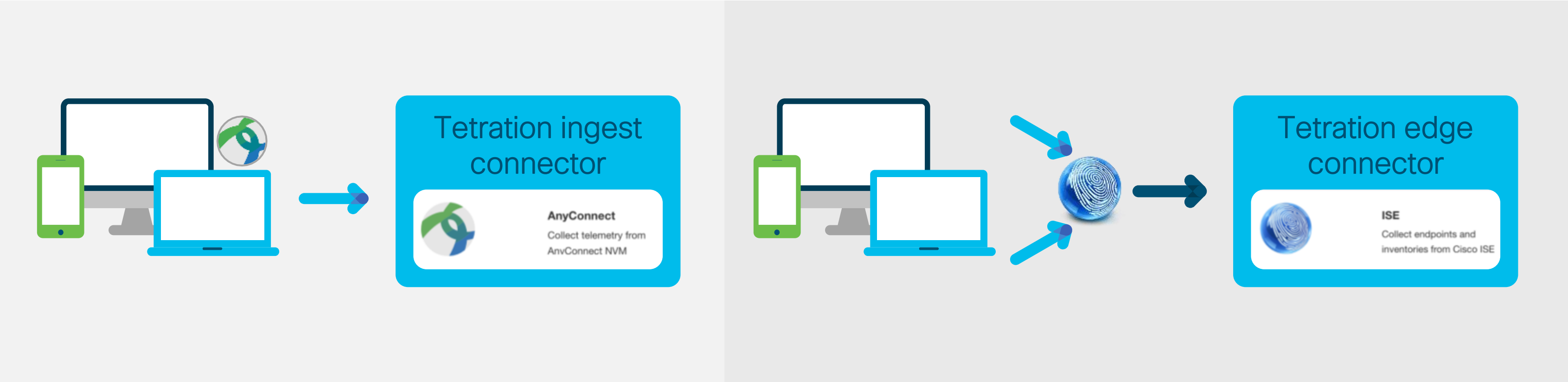
Cisco® Tetration knows which ones are public cloud workloads

Cisco Tetration knows which ones are on-premises database servers

Policies are continuously updated as new servers are added, existing servers are moved, or IP addresses change

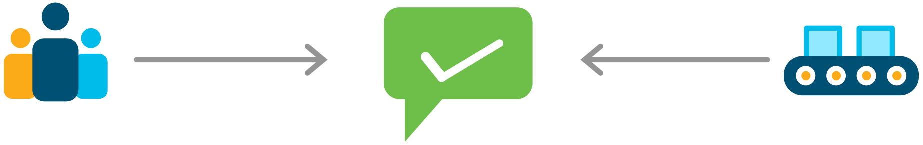
Workforce and endpoint information

- Workforce and endpoint information can come from Cisco AnyConnect® and/or Cisco® Identity Services Engine (ISE)
- Both these options require integration with Lightweight Directory Access Protocol (LDAP) to get additional user context – read-only privilege is needed

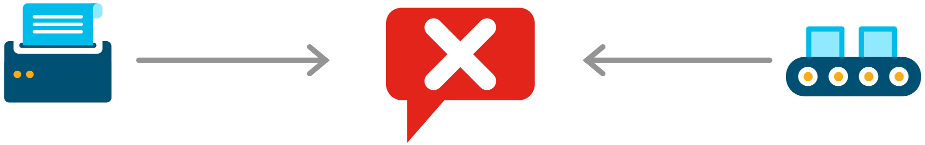

Tetration ingest connector
AnyConnect
Collect telemetry from AnvConnect NVM
Tetration edge connector
ISE
Collect endpoints and inventories from Cisco ISE

Segmentation policies based on workforce and endpoint context

Only finance group users can access the financial reporting system



Printer devices cannot connect to any database servers

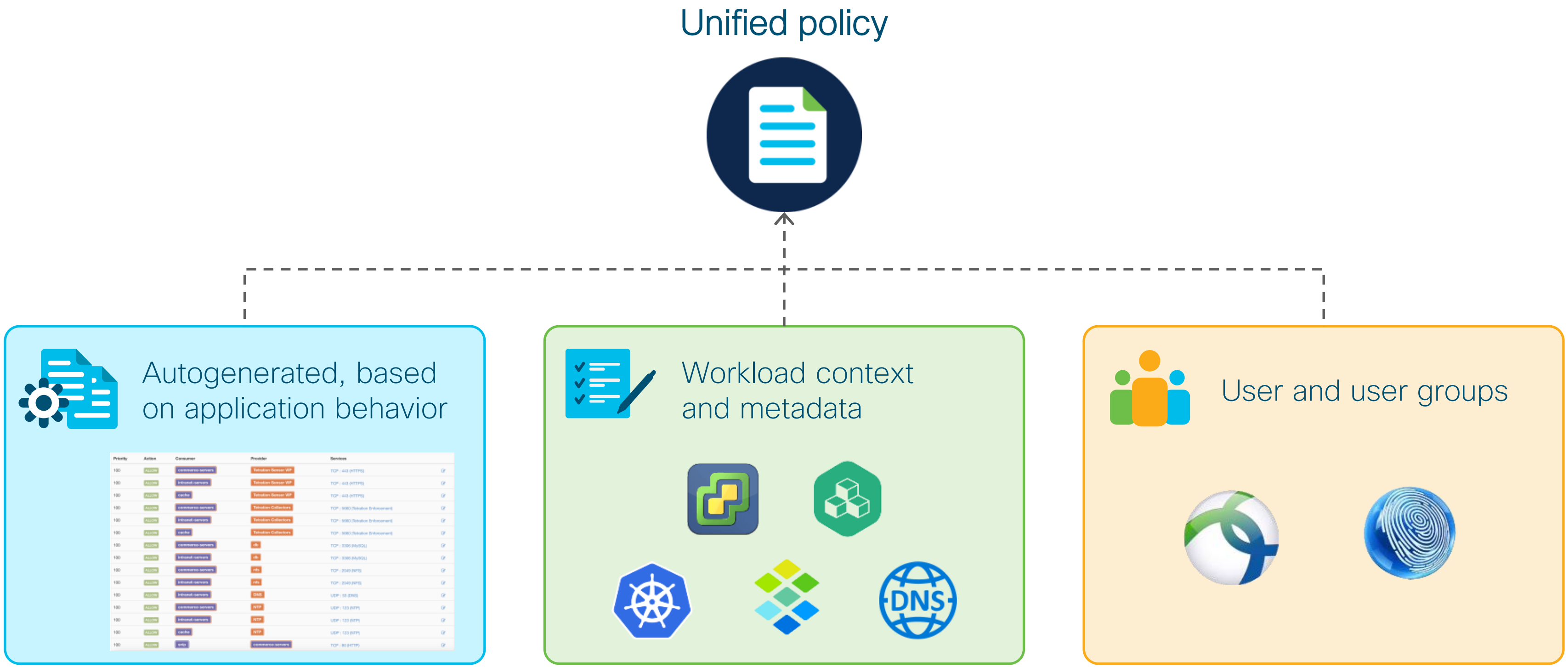


Cisco® Tetration knows about the users and devices

Cisco Tetration knows the application servers and database services

User and device memberships are maintained and updated in real time by Tetration

Generating an unified policy



Unified policy

Autogenerated, based on application behavior

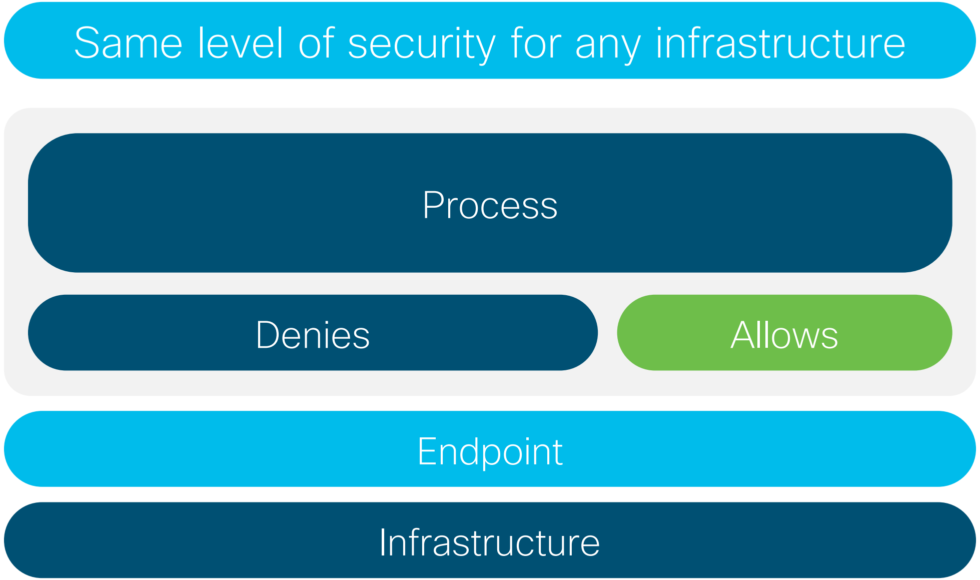
Priority	Action	Consumer	Provider	Services
100	ALLOW	commerce-servers	Tetration Sensor VIP	TCP : 443 (HTTPS)
100	ALLOW	intranet-servers	Tetration Sensor VIP	TCP : 443 (HTTPS)
100	ALLOW	cache	Tetration Sensor VIP	TCP : 443 (HTTPS)
100	ALLOW	commerce-servers	Tetration Collectors	TCP : 5660 (Tetration Enforcement)
100	ALLOW	intranet-servers	Tetration Collectors	TCP : 5660 (Tetration Enforcement)
100	ALLOW	cache	Tetration Collectors	TCP : 5660 (Tetration Enforcement)
100	ALLOW	commerce-servers	db	TCP : 3306 (MySQL)
100	ALLOW	intranet-servers	db	TCP : 3306 (MySQL)
100	ALLOW	commerce-servers	nfs	TCP : 2049 (NFS)
100	ALLOW	intranet-servers	nfs	TCP : 2049 (NFS)
100	ALLOW	intranet-servers	DNS	UDP : 53 (DNS)
100	ALLOW	commerce-servers	NTP	UDP : 123 (NTP)
100	ALLOW	intranet-servers	NTP	UDP : 123 (NTP)
100	ALLOW	cache	NTP	UDP : 123 (NTP)
100	ALLOW	smtp	commerce-servers	TCP : 80 (HTTP)

Workload context and metadata

User and user groups

Enforcing microsegmentation policy

Security



Same level of security for any infrastructure

Process

Denies

Allows

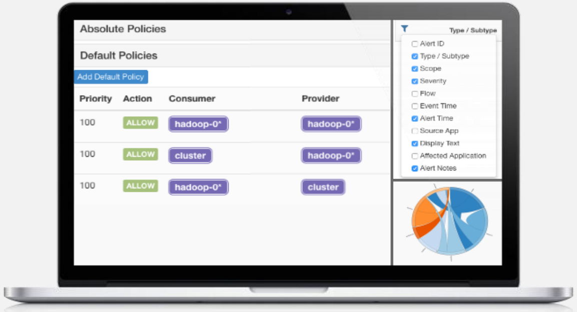
Endpoint

Infrastructure

Intent is rendered as security rules in native operating system firewalls

(IP sets in Linux and Microsoft Windows Firewall in Windows Server)

Open policy - other enforcement points



Absolute Policies

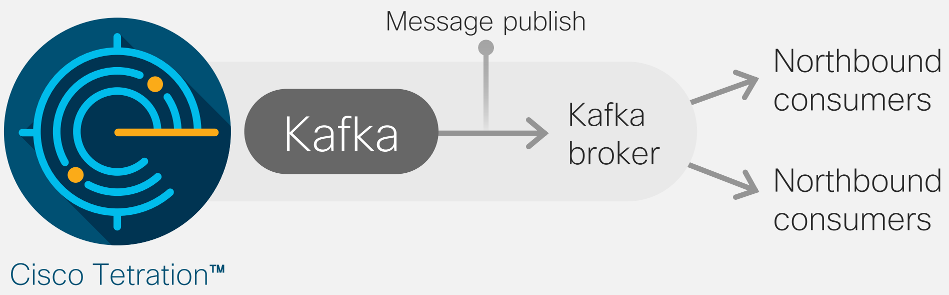
Default Policies

Add Default Policy

Priority	Action	Consumer	Provider
100	ALLOW	hadoop-0*	hadoop-0*
100	ALLOW	cluster	hadoop-0*
100	ALLOW	hadoop-0*	cluster

Type / Subtype

- ☐ Alert ID
- ☑ Type / Subtype
- ☑ Scope
- ☑ Severity
- ☐ Flow
- ☐ Event Time
- ☑ Alert Time
- ☐ Source App
- ☑ Display Text
- ☐ Affected Application
- ☑ Alert Notes



Cisco Tetration™

Publishes normalized microsegmentation policy over the Kafka interface

Updates to the policy is also sent through the same interface in real-time

Northbound systems can consume this policy and render it in other infrastructure elements such as:

- Firewalls
- Load balancers (F5/AVI)

Software vulnerabilities and exposures

Workload protection: Known vulnerabilities

Hackers exploit known vulnerabilities of software

Simple answer to protecting against exploits and threats: Patch the vulnerable servers

Identify quickly what systems are vulnerable

Detect and limit your risk: Know the impact score of CVEs and take necessary action based on that

Take action: Quarantine and block vulnerable systems to limit your attack surface and prevent lateral movement

Meet compliance needs: Regulatory standards such as PCI-DSS require that patches and updates be applied when issued

Software package inventory tracking

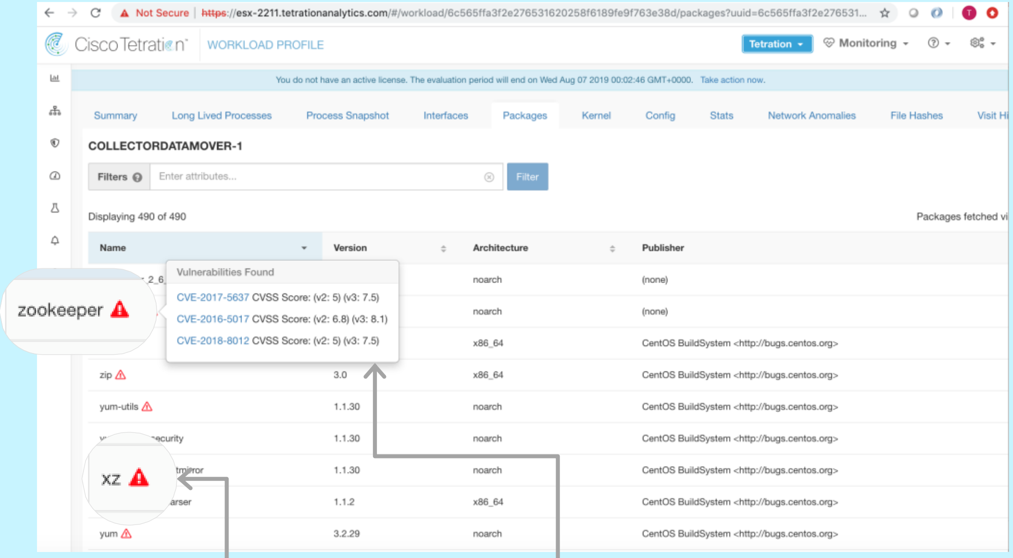
Cisco® Tetration

Inventory of all packages, along with version information installed on the server

Inventory search based on:

- Software package
- Version information
- Publisher

Quickly identify software packages that have known vulnerabilities



⚠ Not Secure | https://esx-2211.tetrationanalytics.com/#/workload/6c565ffa3f2e276531620258f6189fe9f763e38d/packages?uuid=6c565ffa3f2e276531...

You do not have an active license. The evaluation period will end on Wed Aug 07 2019 00:02:46 GMT+0000. Take action now.

COLLECTORDATAMOVER-1

Enter attributes...

Displaying 490 of 490

Packages fetched vi

zookeeper ⚠

Vulnerabilities Found

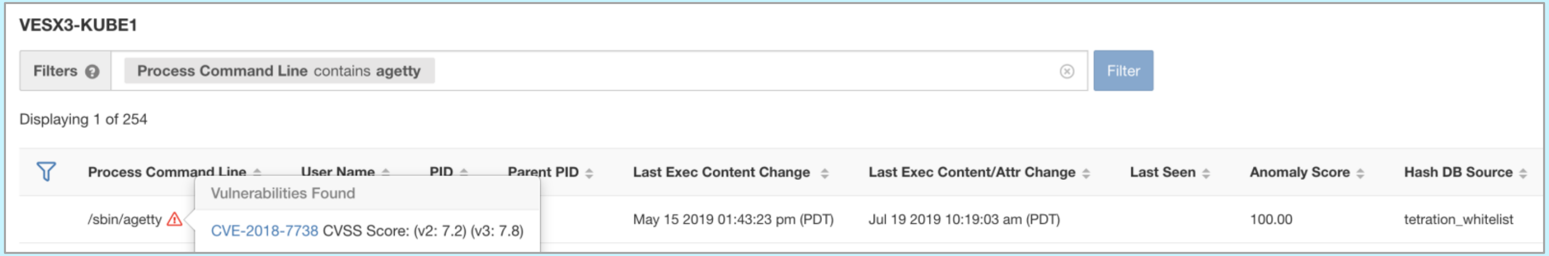
CVE-2017-5637 CVSS Score: (v2: 5) (v3: 7.5)
CVE-2016-5017 CVSS Score: (v2: 6.8) (v3: 8.1)
CVE-2018-8012 CVSS Score: (v2: 5) (v3: 7.5)

xz ⚠

Name	Version	Architecture	Publisher
2_6		noarch	(none)
		noarch	(none)
		x86_64	CentOS BuildSystem <http://bugs.centos.org>
zip ⚠	3.0	x86_64	CentOS BuildSystem <http://bugs.centos.org>
yum-utils ⚠	1.1.30	noarch	CentOS BuildSystem <http://bugs.centos.org>
y ecurity	1.1.30	noarch	CentOS BuildSystem <http://bugs.centos.org>
tmirror	1.1.30	noarch	CentOS BuildSystem <http://bugs.centos.org>
arser	1.1.2	x86_64	CentOS BuildSystem <http://bugs.centos.org>
yum ⚠	3.2.29	noarch	CentOS BuildSystem <http://bugs.centos.org>

Packages with known vulnerabilities

CVEs for running processes



VESX3-KUBE1

Filters | Process Command Line contains agetty | Filter

Displaying 1 of 254

	Process Command Line	User Name	PID	Parent PID	Last Exec Content Change	Last Exec Content/Attr Change	Last Seen	Anomaly Score	Hash DB Source
	/sbin/agetty ⚠				May 15 2019 01:43:23 pm (PDT)	Jul 19 2019 10:19:03 am (PDT)		100.00	tetration_whitelist

Vulnerabilities Found

CVE-2018-7738 CVSS Score: (v2: 7.2) (v3: 7.8)

- Tetration identifies processes that are associated with vulnerable software packages
- Administrators can immediately know whether the vulnerable software is running or is just installed and make decisions based on this information
- Attack surface score calculation now includes this information, along with the stale port and process data

Software package vulnerability – policy action

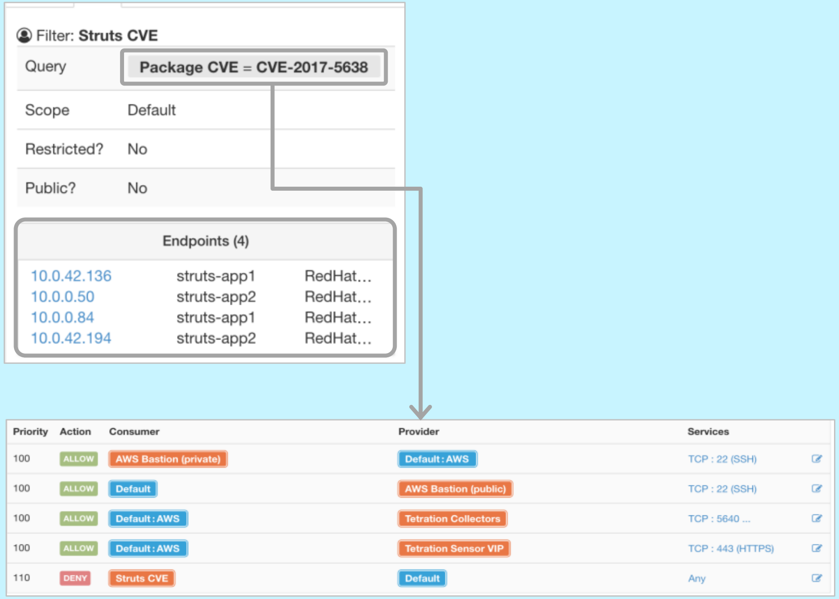
Set up filters to search for one or more vulnerabilities

Identify list of servers with the same vulnerability or software packages installed

Set up policy through UI or API to take specific action:

- Quarantine a host when servers are identified with the same vulnerability

If a new workload has the same vulnerability, its communication will be restricted as well



Filter: **Struts CVE**

Query	**Package CVE = CVE-2017-5638**
Scope	Default
Restricted?	No
Public?	No

Endpoints (4)

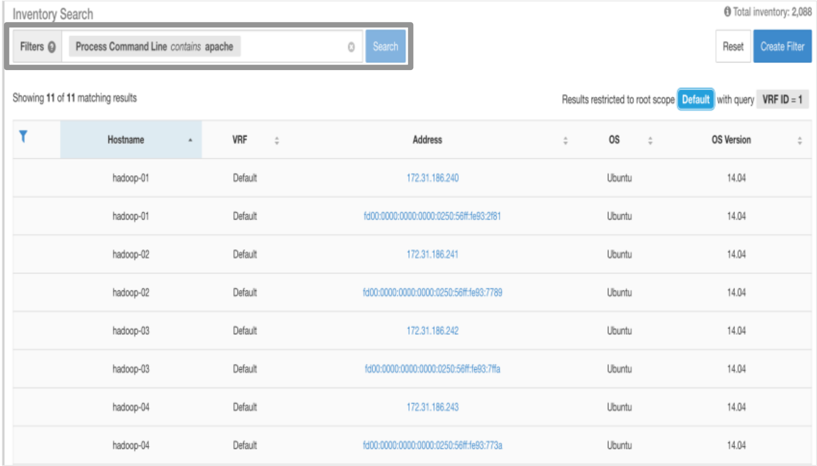
10.0.42.136	struts-app1	RedHat...
10.0.0.50	struts-app2	RedHat...
10.0.0.84	struts-app1	RedHat...
10.0.42.194	struts-app2	RedHat...

Priority	Action	Consumer	Provider	Services	
100	ALLOW	AWS Bastion (private)	Default : AWS	TCP : 22 (SSH)	✎
100	ALLOW	Default	AWS Bastion (public)	TCP : 22 (SSH)	✎
100	ALLOW	Default : AWS	Tetration Collectors	TCP : 5640 ...	✎
100	ALLOW	Default : AWS	Tetration Sensor VIP	TCP : 443 (HTTPS)	✎
110	DENY	Struts CVE	Default	Any	✎

Identify workload behavior anomalies

Search for workload with certain process and process hash

Search for process command line or binary process hash across all servers



Inventory Search

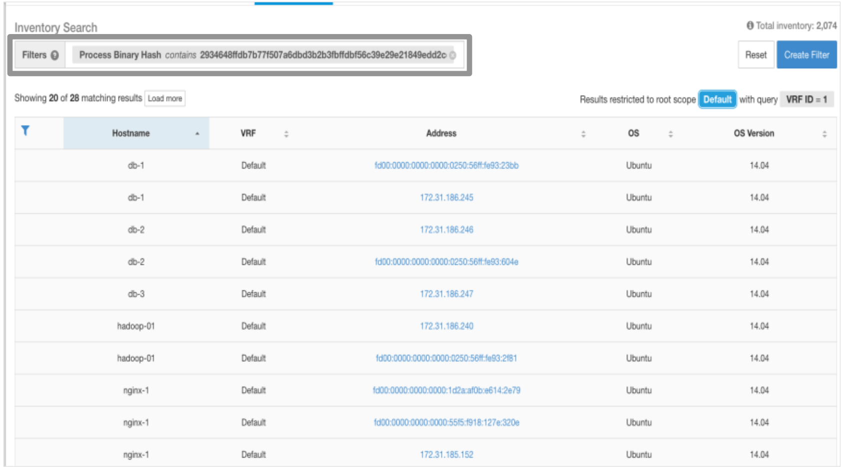
Total inventory: 2,088

Process Command Line *contains* apache

Showing **11** of **11** matching results

Results restricted to root scope **Default** with query **VRF ID = 1**

Hostname	VRF	Address	OS	OS Version
hadoop-01	Default	172.31.186.240	Ubuntu	14.04
hadoop-01	Default	fd00:0000:0000:0000:0250:56ff:fe93:2f81	Ubuntu	14.04
hadoop-02	Default	172.31.186.241	Ubuntu	14.04
hadoop-02	Default	fd00:0000:0000:0000:0250:56ff:fe93:7789	Ubuntu	14.04
hadoop-03	Default	172.31.186.242	Ubuntu	14.04
hadoop-03	Default	fd00:0000:0000:0000:0250:56ff:fe93:7ffa	Ubuntu	14.04
hadoop-04	Default	172.31.186.243	Ubuntu	14.04
hadoop-04	Default	fd00:0000:0000:0000:0250:56ff:fe93:773a	Ubuntu	14.04



Inventory Search

Total inventory: 2,074

Process Binary Hash *contains* 2934648ffdb7b77f507a6dbd3b2b3fbffdbf56c39e29e21849edd2c

Showing **20** of **28** matching results

Results restricted to root scope **Default** with query **VRF ID = 1**

Hostname	VRF	Address	OS	OS Version
db-1	Default	fd00:0000:0000:0000:0250:56ff:fe93:23bb	Ubuntu	14.04
db-1	Default	172.31.186.245	Ubuntu	14.04
db-2	Default	172.31.186.246	Ubuntu	14.04
db-2	Default	fd00:0000:0000:0000:0250:56ff:fe93:604e	Ubuntu	14.04
db-3	Default	172.31.186.247	Ubuntu	14.04
hadoop-01	Default	172.31.186.240	Ubuntu	14.04
hadoop-01	Default	fd00:0000:0000:0000:0250:56ff:fe93:2f81	Ubuntu	14.04
nginx-1	Default	fd00:0000:0000:0000:1d2a:af0b:e614:2e79	Ubuntu	14.04
nginx-1	Default	fd00:0000:0000:0000:55f5:f918:127e:320e	Ubuntu	14.04
nginx-1	Default	172.31.185.152	Ubuntu	14.04

Search for all servers that ran a certain process

Search for all servers that ran a certain process binary hash

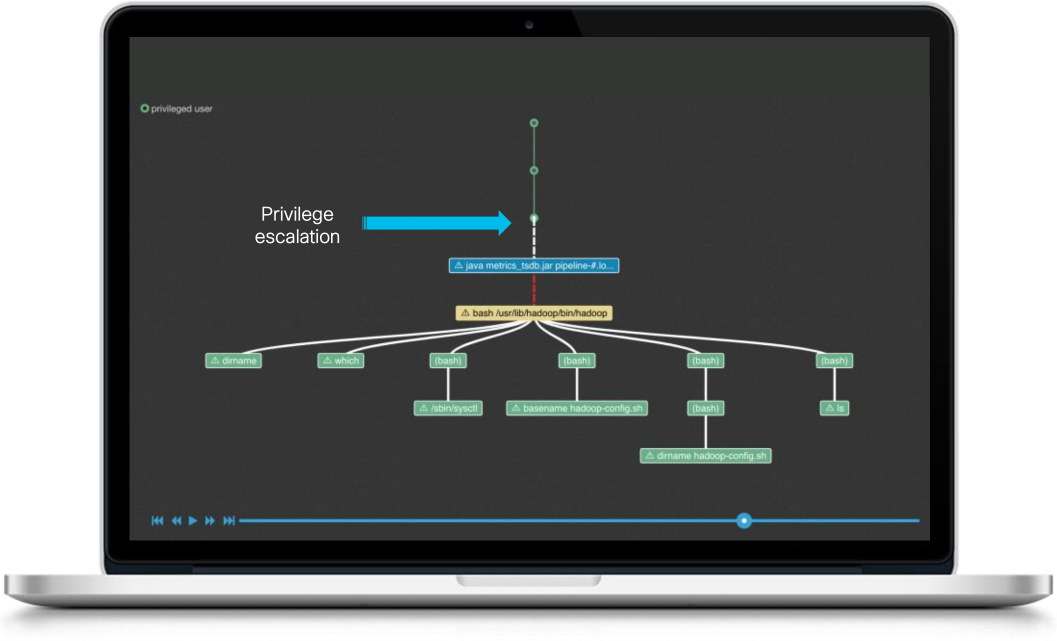
Identifying anomalous process behaviors

Cisco Tetration™

Match the process behavior deviations with malware behavior patterns to suspicious activities

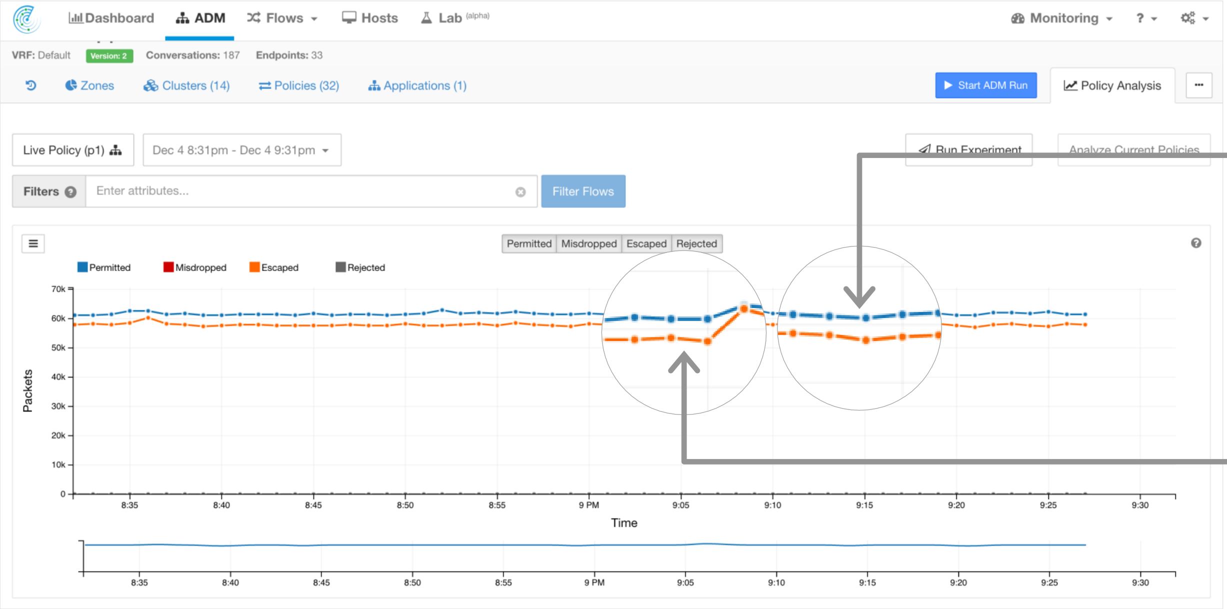
Search for specific process events and find out the details, for example:

- Privilege escalation
- Shell-code execution
- Side channel attack
- Raw socket creation
- User login activities
- File access pattern


privileged user
Privilege escalation
⚠ java metrics_tsdb.jar pipeline-#.lo...
⚠ bash /usr/lib/hadoop/bin/hadoop
⚠ dirname
⚠ which
(bash)
(bash)
(bash)
(bash)
⚠ /sbin/sysctl
⚠ basename hadoop-config.sh
(bash)
⚠ ls
⚠ dirname hadoop-config.sh

Tracking policy deviations

Policy compliance verification and simulation



VRF: Default Version: 2 Conversations: 187 Endpoints: 33

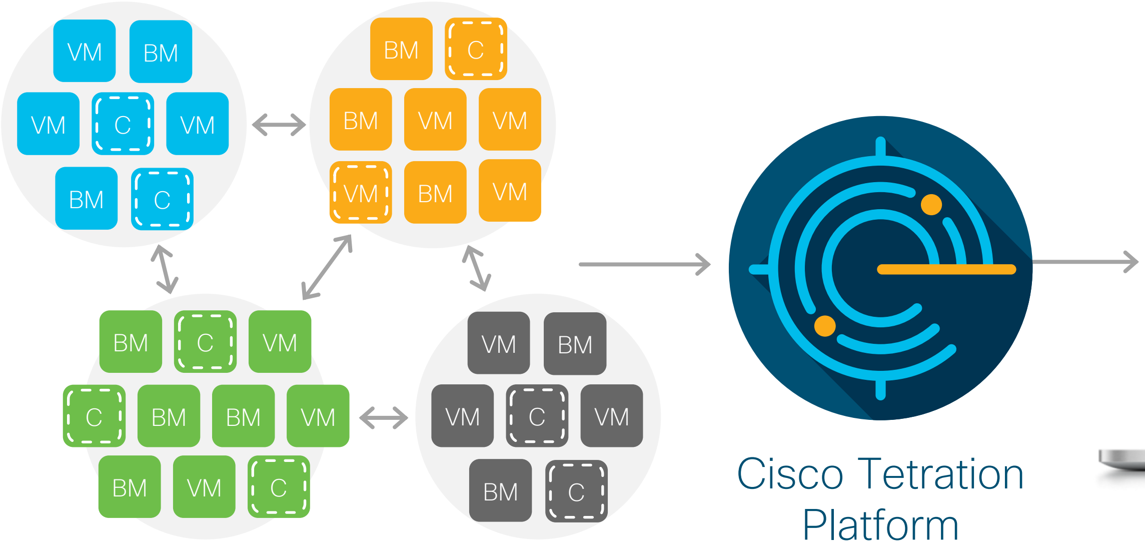
Live Policy (p1)

Dec 4 8:31pm - Dec 4 9:31pm

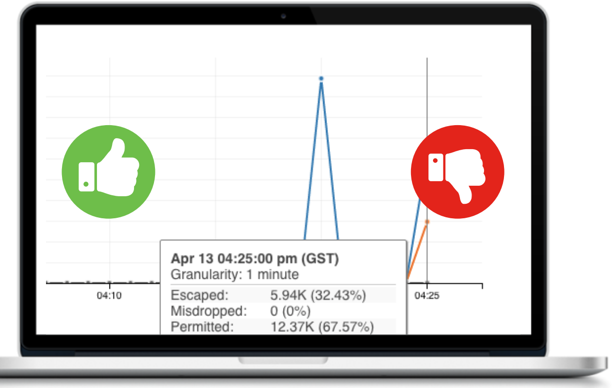
What was seen on the network that was out of compliance with policy

Permitted traffic seen on the network

Policy compliance



Cisco Tetration Platform



Apr 13 04:25:00 pm (GST)
Granularity: 1 minute
Escaped: 5.94K (32.43%)
Misdropped: 0 (0%)
Permitted: 12.37K (67.57%)

Identify policy deviations in real time

Review and update whitelist policy with one click

Perform policy lifecycle management

Container support for segmentation

Segmentation policy for containers

Integration with Kubernetes or OpenShift is mandatory for container policy generation and enforcement

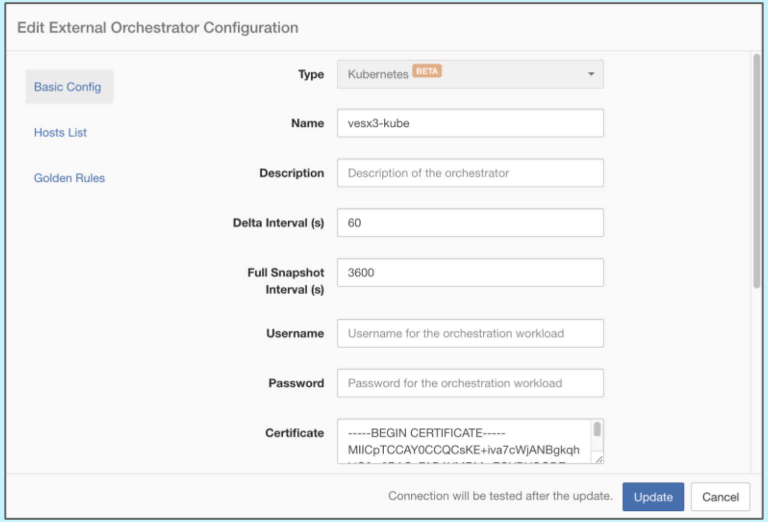
Requires only read-only access to the orchestrator

Supported version of Kubernetes and OpenShift:

- Kubernetes version 1.12.x
- OpenShift versions 3.11
  - Requires network policy plug-in
  - Should not have SDN plug-in or multitenant SDN plug-in

The following information is collected for automatic annotations:

- Container pod definitions
- Service definitions



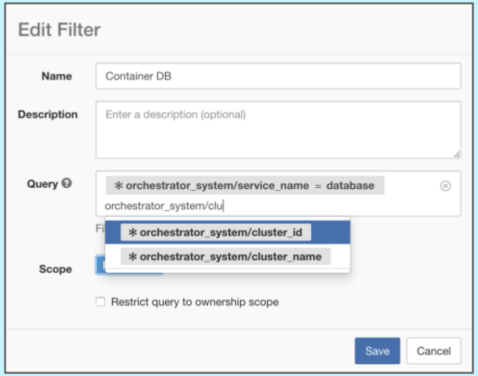
Edit External Orchestrator Configuration

Type	Kubernetes BETA
Name	vesx3-kube
Description	Description of the orchestrator
Delta Interval (s)	60
Full Snapshot Interval (s)	3600
Username	Username for the orchestration workload
Password	Password for the orchestration workload
Certificate	-----BEGIN CERTIFICATE----- MIICpTCCAY0CCQCsKE+iva7cWjANBgkqh

Connection will be tested after the update.

Container policy definitions

- Policy definitions for the container workloads also happen through the application workspace
- Policies are defined based on the tags (pod names, service names, etc.)
- Inventory filter that matches specified tag criteria will automatically get those policies when enforced
- If tag definitions match any higher-level policy definitions, such as InfoSec, container pods automatically inherit those policies



Edit Filter

Name: Container DB

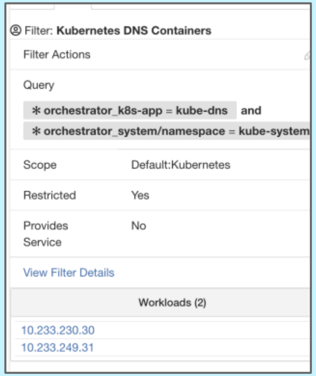
Description: Enter a description (optional)

Query: ✻ orchestrator_system/service_name = database
orchestrator_system/clu

✻ orchestrator_system/cluster_id
✻ orchestrator_system/cluster_name

Scope

□ Restrict query to ownership scope



Filter: Kubernetes DNS Containers

Filter Actions

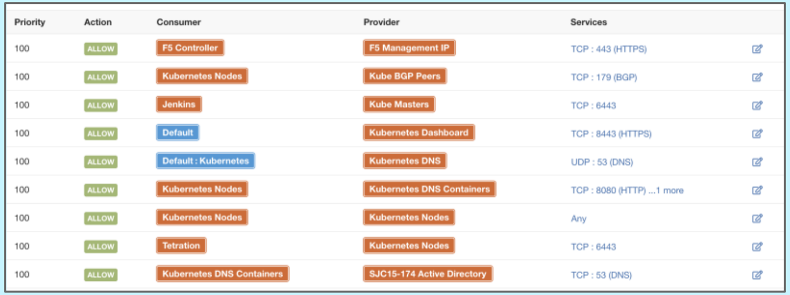
Query
✻ orchestrator_k8s-app = kube-dns and
✻ orchestrator_system/namespace = kube-system

Scope	Default:Kubernetes
Restricted	Yes
Provides Service	No

View Filter Details

Workloads (2)

10.233.230.30
10.233.249.31



Priority	Action	Consumer	Provider	Services
100	ALLOW	F5 Controller	F5 Management IP	TCP : 443 (HTTPS)
100	ALLOW	Kubernetes Nodes	Kube BGP Peers	TCP : 179 (BGP)
100	ALLOW	Jenkins	Kube Masters	TCP : 6443
100	ALLOW	Default	Kubernetes Dashboard	TCP : 8443 (HTTPS)
100	ALLOW	Default : Kubernetes	Kubernetes DNS	UDP : 53 (DNS)
100	ALLOW	Kubernetes Nodes	Kubernetes DNS Containers	TCP : 8080 (HTTP) ...1 more
100	ALLOW	Kubernetes Nodes	Kubernetes Nodes	Any
100	ALLOW	Tetration	Kubernetes Nodes	TCP : 6443
100	ALLOW	Kubernetes DNS Containers	SJC15-174 Active Directory	TCP : 53 (DNS)

In summary: Platform built for scale and flexibility

Microsegmentation

- Making the microsegmentation journey a reality
- Segmentation for thousands of applications
- Rich context based policies to support modern application deployment and access mechanisms

Comprehensive workload security

- Detect workload behavior anomalies
- Reduce attack surface by identifying software vulnerabilities
- Track application policy compliance in real time

Easy to use

- One-touch deployment
- Self-monitoring
- Self-diagnostics

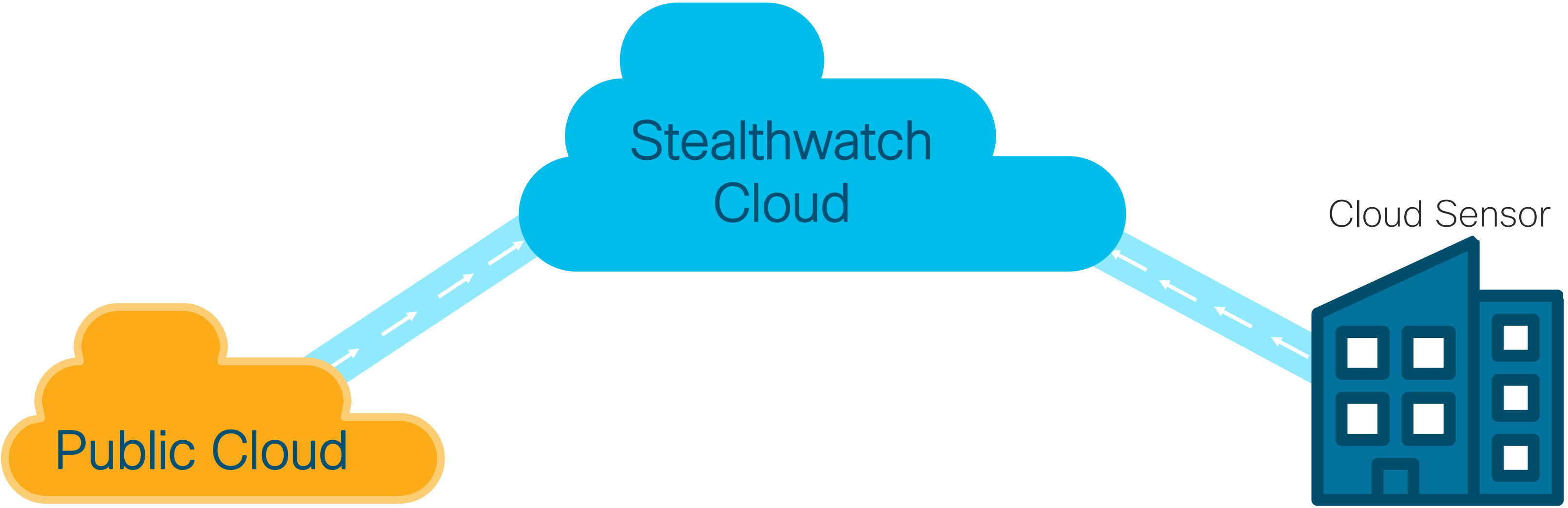
Open

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

Consistent visibility

Cisco Secure Cloud Analytics (Stealthwatch cloud)

Quick and easy security for dynamic environments

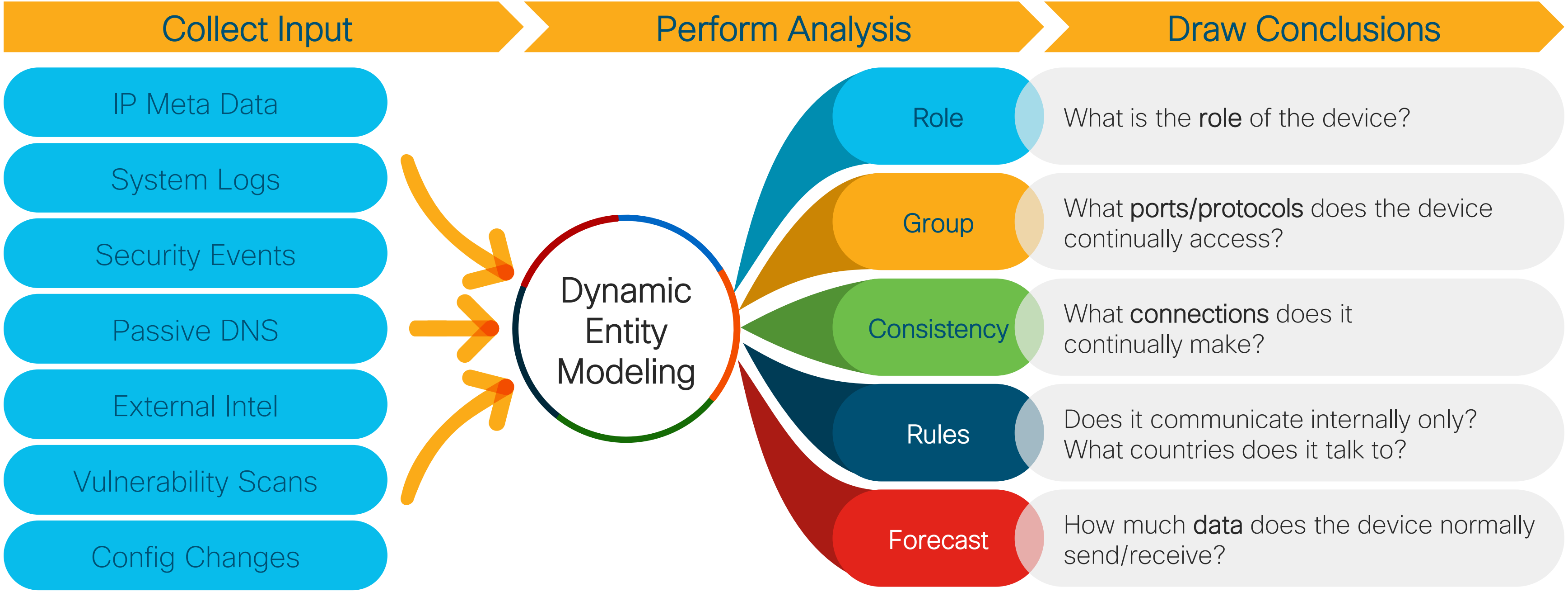


- VPC Flow Logs
- Other data sources

- NetFlow
- SPAN/TAP
- DNS

Using modeling to detect security events

Dynamic Entity Modeling



Collect Input

Perform Analysis

Draw Conclusions

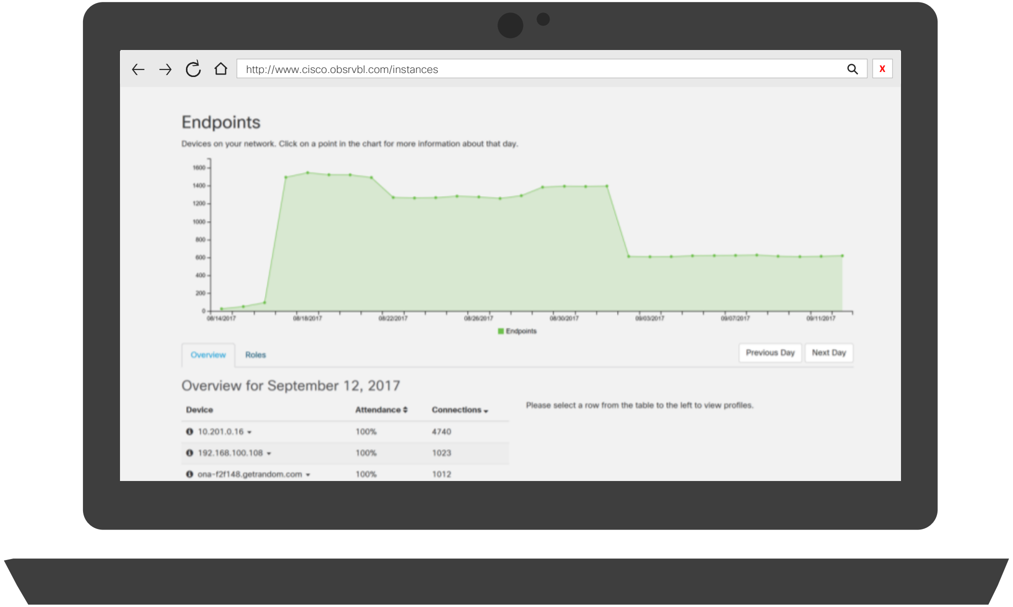
- IP Meta Data
- System Logs
- Security Events
- Passive DNS
- External Intel
- Vulnerability Scans
- Config Changes

Dynamic Entity Modeling

Role	What is the **role** of the device?
Group	What **ports/protocols** does the device continually access?
Consistency	What **connections** does it continually make?
Rules	Does it communicate internally only? What countries does it talk to?
Forecast	How much **data** does the device normally send/receive?

Identify every entity in customer networks automatically

Automated Endpoint Discovery



http://www.cisco.obsrvbl.com/instances

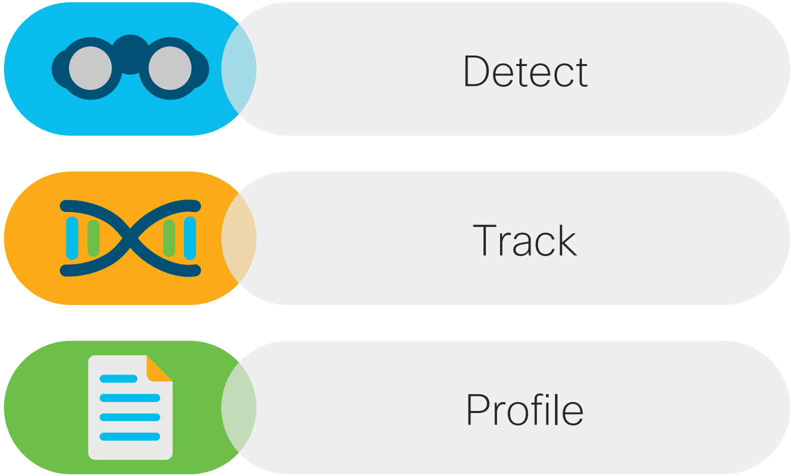
Endpoints

Devices on your network. Click on a point in the chart for more information about that day.

Overview for September 12, 2017

Device	Attendance ⇕	Connections ▾
10.201.0.16 ▾	100%	4740
192.168.100.108 ▾	100%	1023
ona-f2f148.getrandom.com ▾	100%	1012

Please select a row from the table to the left to view profiles.



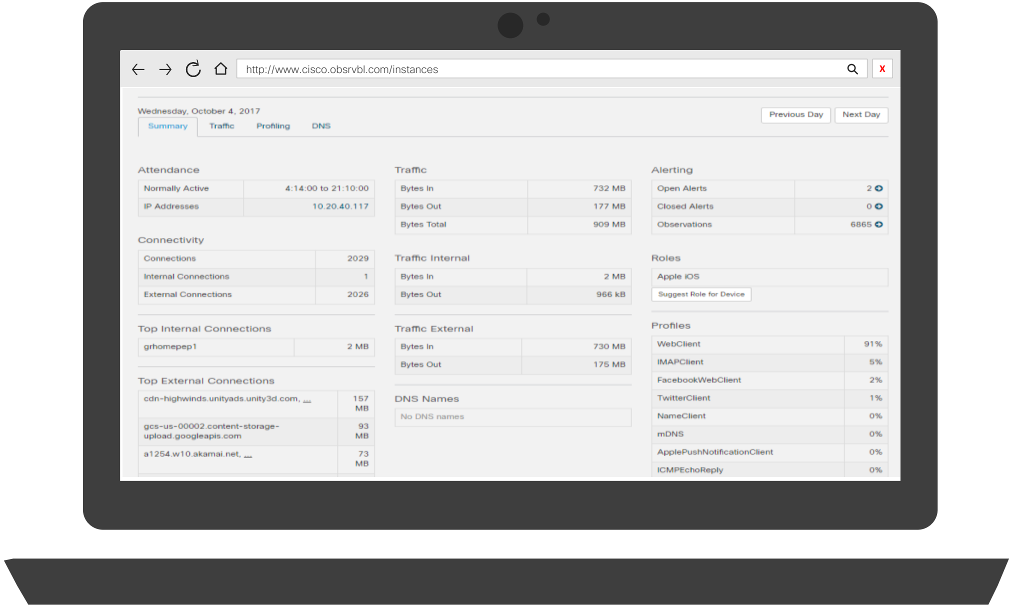
Detect

Track

Profile

Detailed visibility of every entity

Automated Entity Discovery



Wednesday, October 4, 2017

Attendance

Normally Active	4:14:00 to 21:10:00
IP Addresses	10.20.40.117

Connectivity

Connections	2029
Internal Connections	1
External Connections	2026

Top Internal Connections

grhomepep1	2 MB

Top External Connections

cdn-highwinds.unityads.unity3d.com, ...	157 MB
gcs-us-00002.content-storage-upload.googleapis.com	93 MB
a1254.w10.akamai.net, ...	73 MB

Traffic

Bytes In	732 MB
Bytes Out	177 MB
Bytes Total	909 MB

Traffic Internal

Bytes In	2 MB
Bytes Out	966 kB

Traffic External

Bytes In	730 MB
Bytes Out	175 MB

DNS Names

No DNS names

Alerting

Open Alerts	2
Closed Alerts	0
Observations	6865

Roles

Apple iOS

Suggest Role for Device

Profiles

WebClient	91%
IMAPClient	5%
FacebookWebClient	2%
TwitterClient	1%
NameClient	0%
mDNS	0%
ApplePushNotificationClient	0%
ICMPEchoReply	0%

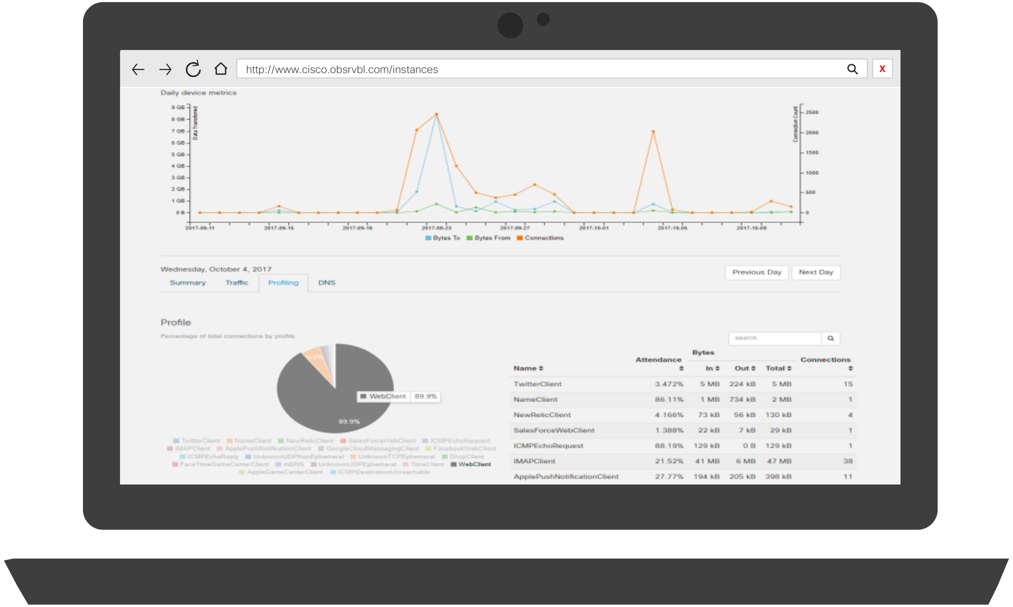
Time of Day Usage

Traffic Statistics

Active Traffic Profiles

Traffic profiling on every entity

Automated Entity Discovery



Wednesday, October 4, 2017

Profile

Percentage of total connections by profile.

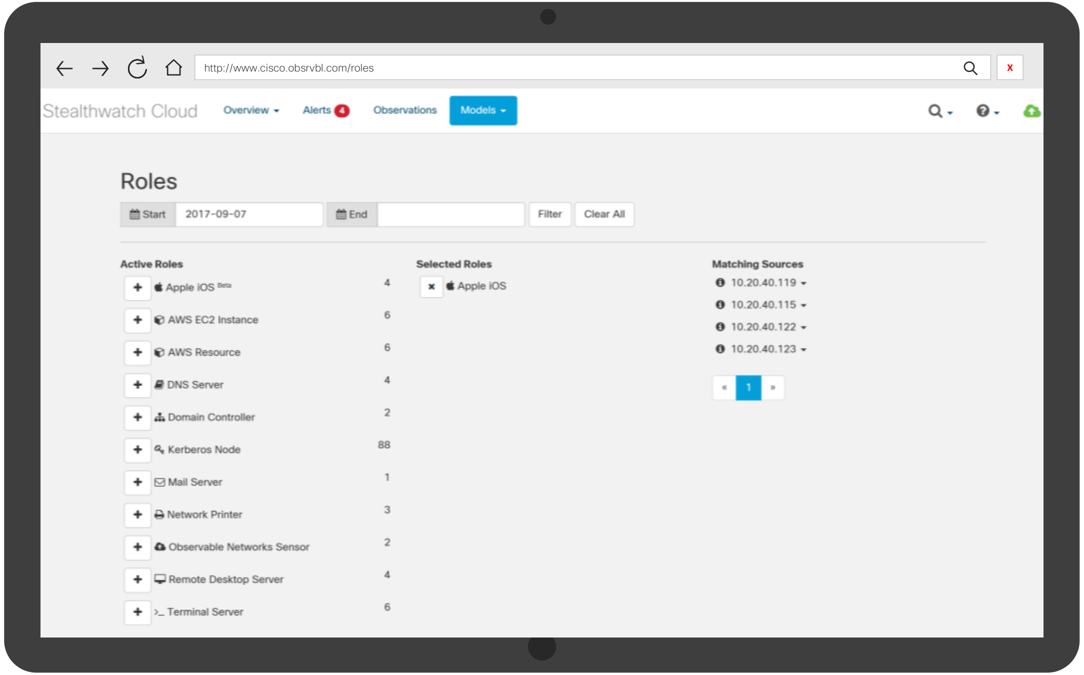
Name ⇕	Attendance ⇕	Bytes			Connections ⇕
		In ⇕	Out ⇕	Total ⇕	
TwitterClient	3.472%	5 MB	224 kB	5 MB	15
NameClient	86.11%	1 MB	734 kB	2 MB	1
NewRelicClient	4.166%	73 kB	56 kB	130 kB	4
SalesForceWebClient	1.388%	22 kB	7 kB	29 kB	1
ICMPEchoRequest	88.19%	129 kB	0 B	129 kB	1
IMAPClient	21.52%	41 MB	6 MB	47 MB	38
ApplePushNotificationClient	27.77%	194 kB	205 kB	398 kB	11

Connections by profile

Traffic Statistics by profile

Profile entity behavior

Dynamic Entity Modeling



Roles

Start 2017-09-07 End Filter Clear All

Active Roles	
+ Apple iOS Beta	4
+ AWS EC2 Instance	6
+ AWS Resource	6
+ DNS Server	4
+ Domain Controller	2
+ Kerberos Node	88
+ Mail Server	1
+ Network Printer	3
+ Observable Networks Sensor	2
+ Remote Desktop Server	4
+ Terminal Server	6

Selected Roles

× Apple iOS

Matching Sources

- 10.20.40.119
- 10.20.40.115
- 10.20.40.122
- 10.20.40.123

« 1 »

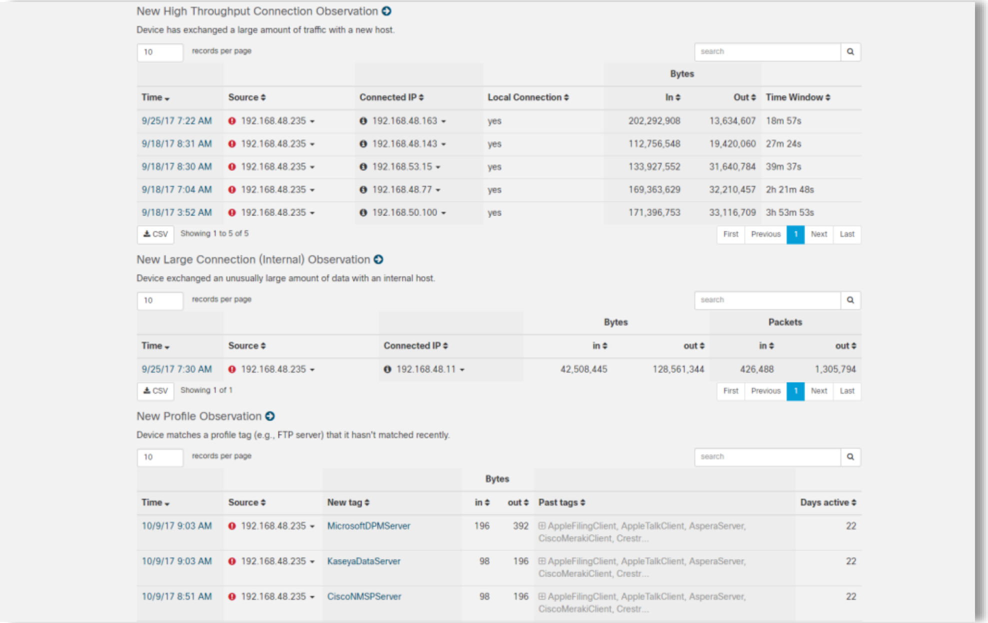
Roles include:

- Android
- Kerberos Node
- AWS Resource
- Mail Server
- Wireless LAN Controller
- Medical Imaging Client
- Citrix PVS Server
- Remote Desktop Server
- Database Server
- Terminal Server
- DNS Server
- VoIP Client
- Domain Controller
- Legacy Windows Device
- Apple iOS
- Web Server

…and 20+ more

Detecting Observations

Automatic event detection



New High Throughput Connection Observation

Device has exchanged a large amount of traffic with a new host.

10 records per page

search

				Bytes		
Time	Source	Connected IP	Local Connection	In	Out	Time Window
9/25/17 7:22 AM	192.168.48.235	192.168.48.163	yes	202,292,908	13,634,607	18m 57s
9/18/17 8:31 AM	192.168.48.235	192.168.48.143	yes	112,756,548	19,420,060	27m 24s
9/18/17 8:30 AM	192.168.48.235	192.168.53.15	yes	133,927,552	31,640,784	39m 37s
9/18/17 7:04 AM	192.168.48.235	192.168.48.77	yes	169,363,629	32,210,457	2h 21m 48s
9/18/17 3:52 AM	192.168.48.235	192.168.50.100	yes	171,396,753	33,116,709	3h 53m 53s

CSV Showing 1 to 5 of 5

New Large Connection (Internal) Observation

Device exchanged an unusually large amount of data with an internal host.

10 records per page

search

			Bytes		Packets	
Time	Source	Connected IP	in	out	in	out
9/25/17 7:30 AM	192.168.48.235	192.168.48.11	42,508,445	128,561,344	426,488	1,305,794

CSV Showing 1 of 1

New Profile Observation

Device matches a profile tag (e.g., FTP server) that it hasn't matched recently.

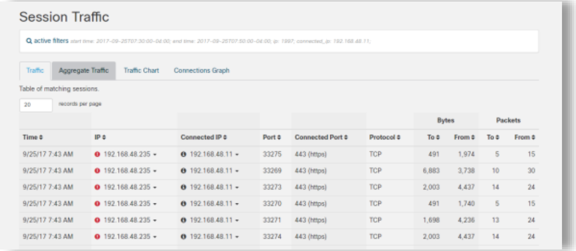
10 records per page

search

			Bytes			
Time	Source	New tag	in	out	Past tags	Days active
10/9/17 9:03 AM	192.168.48.235	MicrosoftDPMServer	196	392	⊞ AppleFilingClient, AppleTalkClient, AsperaServer, CiscoMerakiClient, Crestr...	22
10/9/17 9:03 AM	192.168.48.235	KaseyaDataServer	98	196	⊞ AppleFilingClient, AppleTalkClient, AsperaServer, CiscoMerakiClient, Crestr...	22
10/9/17 8:51 AM	192.168.48.235	CiscoNMSPServer	98	196	⊞ AppleFilingClient, AppleTalkClient, AsperaServer, CiscoMerakiClient, Crestr...	22

View observations for a a specific host

See Observation details



Session Traffic

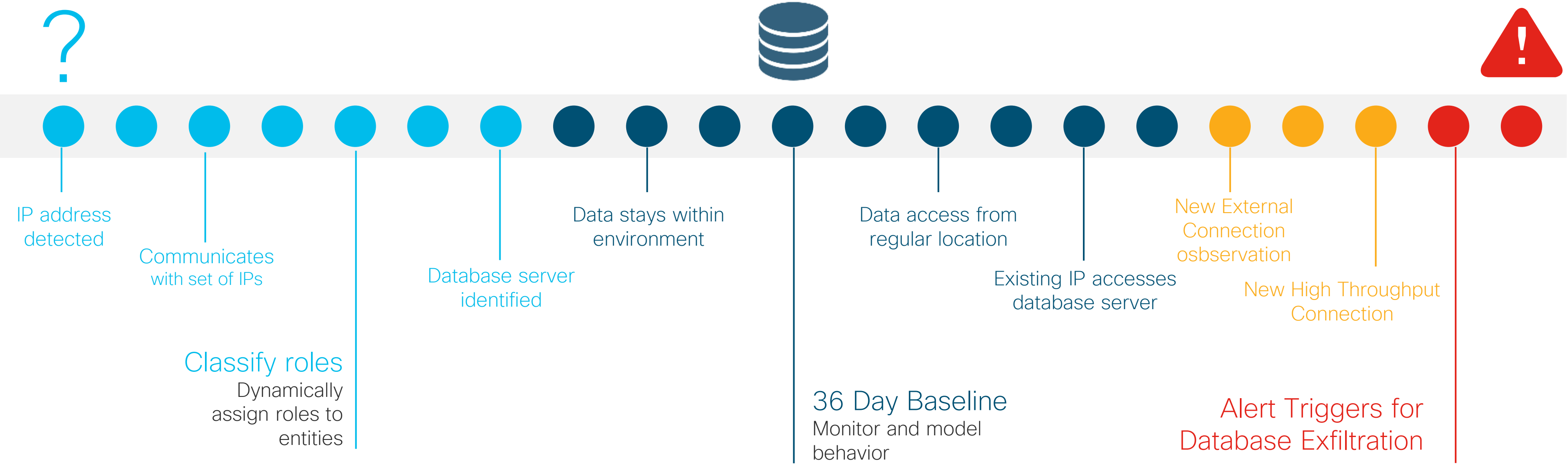
active filters start time: 2017-09-25T07:30:00-04:00; end time: 2017-09-25T07:50:00-04:00; ip: 1997; connected_ip: 192.168.48.11;

Table of matching sessions.

20 records per page

						Bytes		Packets	
Time	IP	Connected IP	Port	Connected Port	Protocol	To	From	To	From
9/25/17 7:43 AM	192.168.48.235	192.168.48.11	33275	443 (https)	TCP	491	1,974	5	15
9/25/17 7:43 AM	192.168.48.235	192.168.48.11	33269	443 (https)	TCP	6,883	3,738	10	30
9/25/17 7:43 AM	192.168.48.235	192.168.48.11	33273	443 (https)	TCP	2,003	4,437	14	24
9/25/17 7:43 AM	192.168.48.235	192.168.48.11	33270	443 (https)	TCP	491	1,740	5	15
9/25/17 7:43 AM	192.168.48.235	192.168.48.11	33271	443 (https)	TCP	1,698	4,236	13	24
9/25/17 7:43 AM	192.168.48.235	192.168.48.11	33274	443 (https)	TCP	2,003	4,437	14	24

Detect abnormal activity using entity modeling



IP address detected

Communicates with set of IPs

Classify roles

Dynamically assign roles to entities

Database server identified

Data stays within environment

36 Day Baseline

Monitor and model behavior

Data access from regular location

Existing IP accesses database server

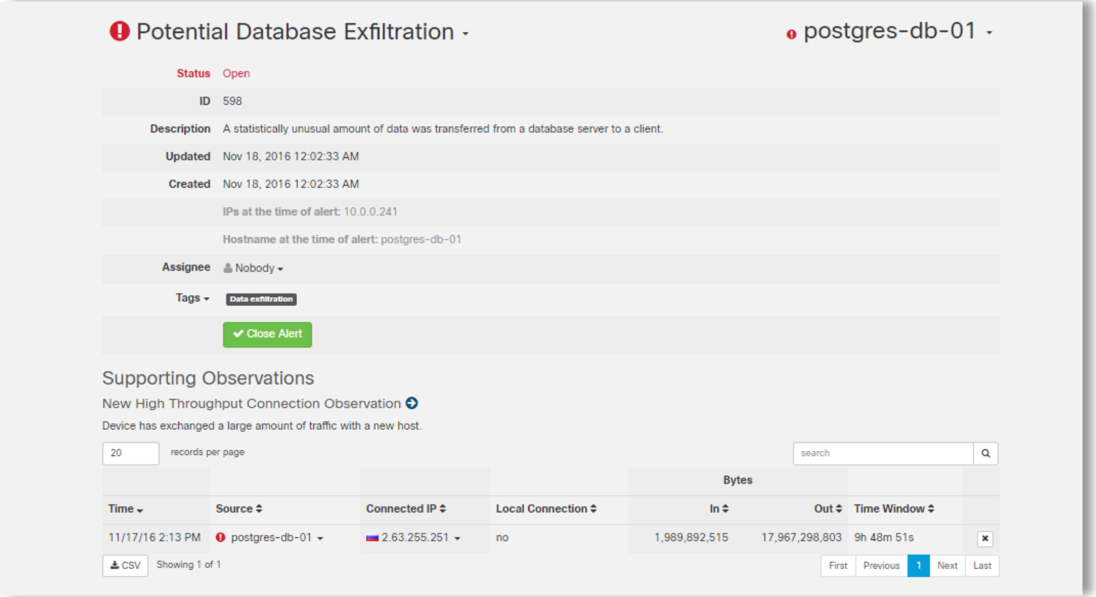
New External Connection osbservation

New High Throughput Connection

Alert Triggers for Database Exfiltration

Alerts reference Observations

Automatic event detection



Potential Database Exfiltration

postgres-db-01

Status Open

ID 598

Description A statistically unusual amount of data was transferred from a database server to a client.

Updated Nov 18, 2016 12:02:33 AM

Created Nov 18, 2016 12:02:33 AM

IPs at the time of alert: 10.0.0.241

Hostname at the time of alert: postgres-db-01

Assignee Nobody

Tags Data exfiltration

Supporting Observations

New High Throughput Connection Observation

Device has exchanged a large amount of traffic with a new host.

20 records per page

				Bytes		
Time	Source	Connected IP	Local Connection	In	Out	Time Window
11/17/16 2:13 PM	postgres-db-01	2.63.255.251	no	1,989,892,515	17,967,298,803	9h 48m 51s

Showing 1 of 1

High throughput to new host

Suspicious country identified

Low-noise alerts help you solve problems

Dynamic Entity Modeling

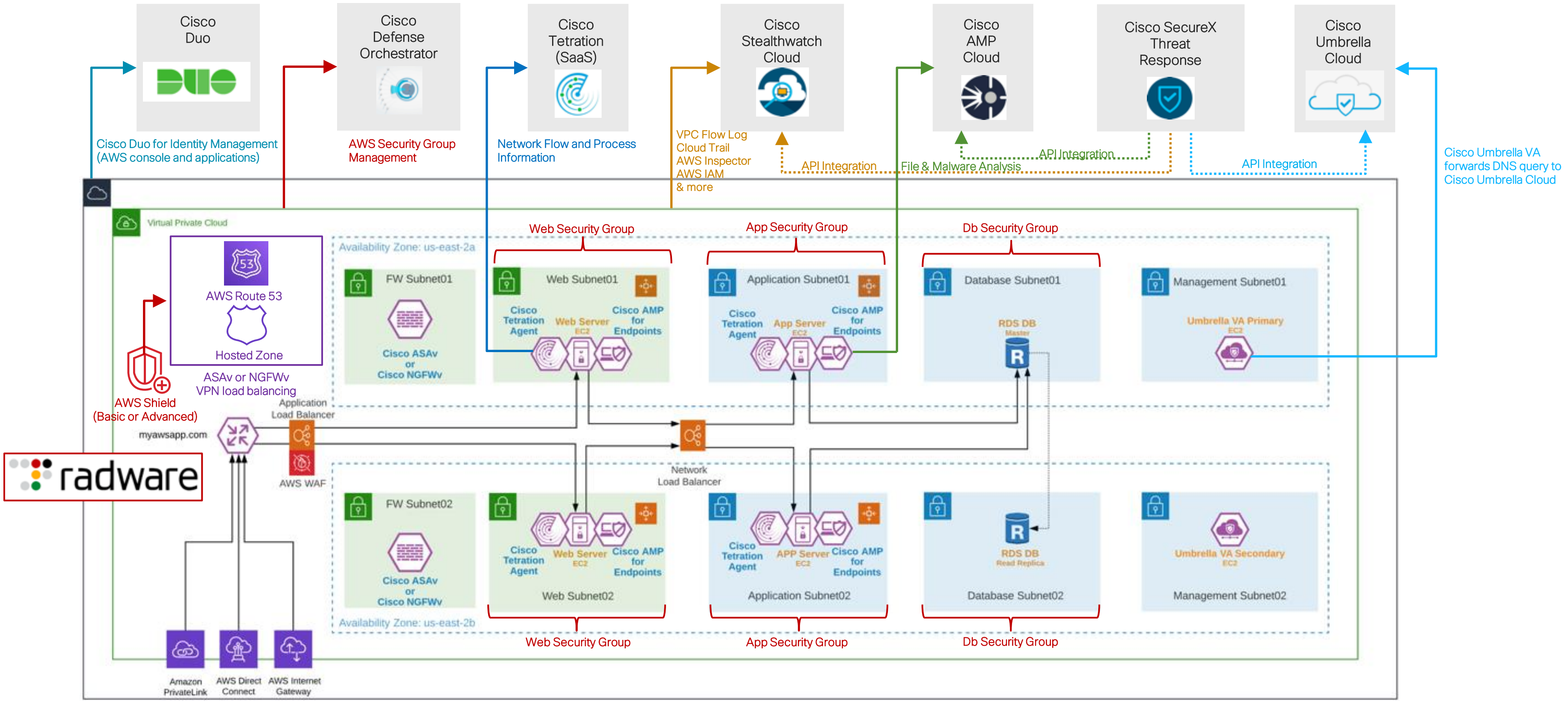
ALERT: Anomaly detected

96% of Stealthwatch Cloud alerts rated as "helpful" by current customers

- Excessive failed access attempts
- DDoS and amplification attacks
- Potential data exfiltration
- Geographically unusual remote access
- Suspected botnet interaction

Secure Cloud Architecture

Cisco Secure Cloud Architecture for AWS



cisco