

# Cisco AIOps Products



- Cisco has a suite of software products which fall under the AIOps (Artificial Intelligence for IT Operations) umbrella
  - Cisco Secure Network Analytics (formerly StealthWatch)
  - Cisco Catalyst Center
  - Cisco Meraki
  - Cisco Nexus Dashboard
  - Cisco AppDynamics
  - Cisco ThousandEyes

# Cisco AIOps Products (Cont.)



- Many of the software products have overlapping ML and AI capabilities, they all support:
  - Traffic analytics
  - Anomaly detection
  - Root cause analysis
- Some of the products also provide ML and AI driven:
  - Automated configuration and management of network settings
  - Predictive maintenance

# Cisco AIOps Products (Cont.)



- There are multiple products with their own separate internal teams at Cisco
- This is because of:
  - Separate products for separate use cases, such as Data Center provisioning and monitoring (Cisco Nexus Dashboard), or monitoring of internet based applications (Cisco ThousandEyes)
  - Historical reasons such as evolution of existing software
  - Cisco purchase of new software for new capabilities

# Cisco Catalyst Center AI Features



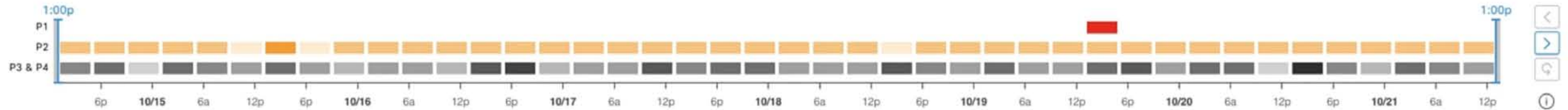
- Cisco Catalyst Center features AI Network Analytics, which continuously collects and analyzes network data.
- It aids in issue detection and provides AI driven:
  - Network traffic baselining and anomaly detection.
  - Network traffic benchmark comparison with other networks.
  - Proactive insights for pattern and trend identification.

Open Resolved Ignored

Global 7 Days

## Most Impacted Areas

By Issue Priority



Total Open: 18

All

P1: 0

P2: 0

P3: 18

P4: 0

AI-Driven: 18

Oct 14, 1:00 PM - Oct 21, 1:00 PM

Filter

Export

Priority	Issue Type	Device Role	Category	Issue Count	Site Count (Area)	Device Count
P3	[AI] Excessive failures to connect - High deviation from baseline	WIRELESS	Onboarding	15	4	
P3	[AI] Excessive time to connect - High deviation from baseline	WIRELESS	Onboarding	1	1	
P3	[AI] Drop in total radio throughput	ACCESS POINT	Application	2	1	

Open Resolved Ignored

Excessive failures to connect - High deviation from baseline &gt; Issue Instance

## Excessive failures to connect - At least 21% increase in failures

Open ▾

Is this issue helpful? 👍 👎

Problem

Impact

Root Cause Analysis

Suggested Actions

## Potential Root Causes

Network Causes

Failed Distribution

Failed Percentage

Failed Count

AAA failures: AAA-related errors observed, please verify the specific authentication failure reasons on the AAA server logs.

+ Add KPI



Probable network causes

Capacity: 4

Insights (4)

Occurrence	Insight	Category	Frequency	KPI	
Jul 27 - Aug 03	AP01 experiencing deviations in Client count over past few weeks	Capacity	5 GHz	Client count	
Jul 27 - Aug 03	AP02 experiencing deviations in Client count over past few weeks	Capacity	2.4 GHz	Client count	
Feb 24 - Mar 02	AP01-01 Band: 5 GHz experiencing deviations in Client count over past few weeks	Capacity	5 GHz	Client count	
Feb 17 - Feb 24	AP02-01 Band: 5 GHz experiencing deviations in Client count over past few weeks	Capacity	5 GHz	Client count	

Showing 4 of 4

Capacity: 4

Insights (4)

Occurrence

Jul 27 - Aug 03

Jul 27 - Aug 03

Feb 24 - Mar 02

Feb 17 - Feb 24

## INSIGHT SUMMARY

experienced Client count deviation in the 5 GHz radio. The maximum deviation observed was 34.0 clients and this occurred between the week of Feb 04-Feb 10 and Feb 25-Mar 02.

🕒 Is this insight helpful? 👍 👎

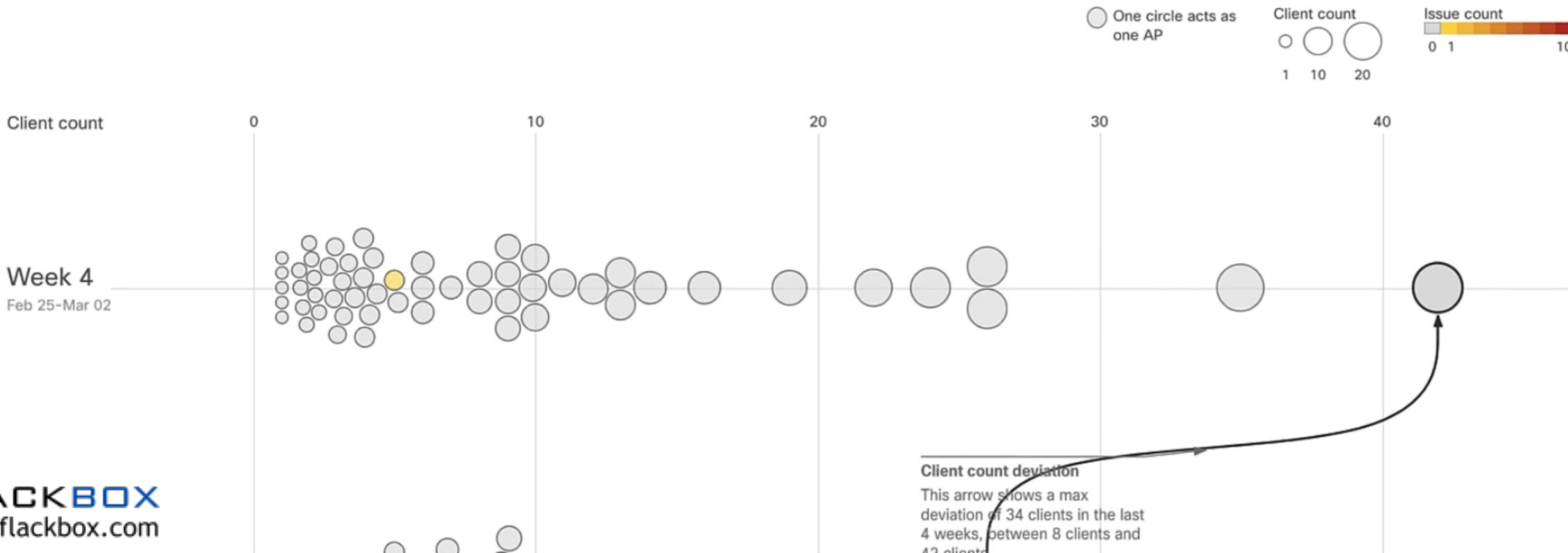
## WEEKLY CLIENT LOAD

22

clients

5% of all clients

## TROUBLESHOOT

[Network Heatmap](#) 

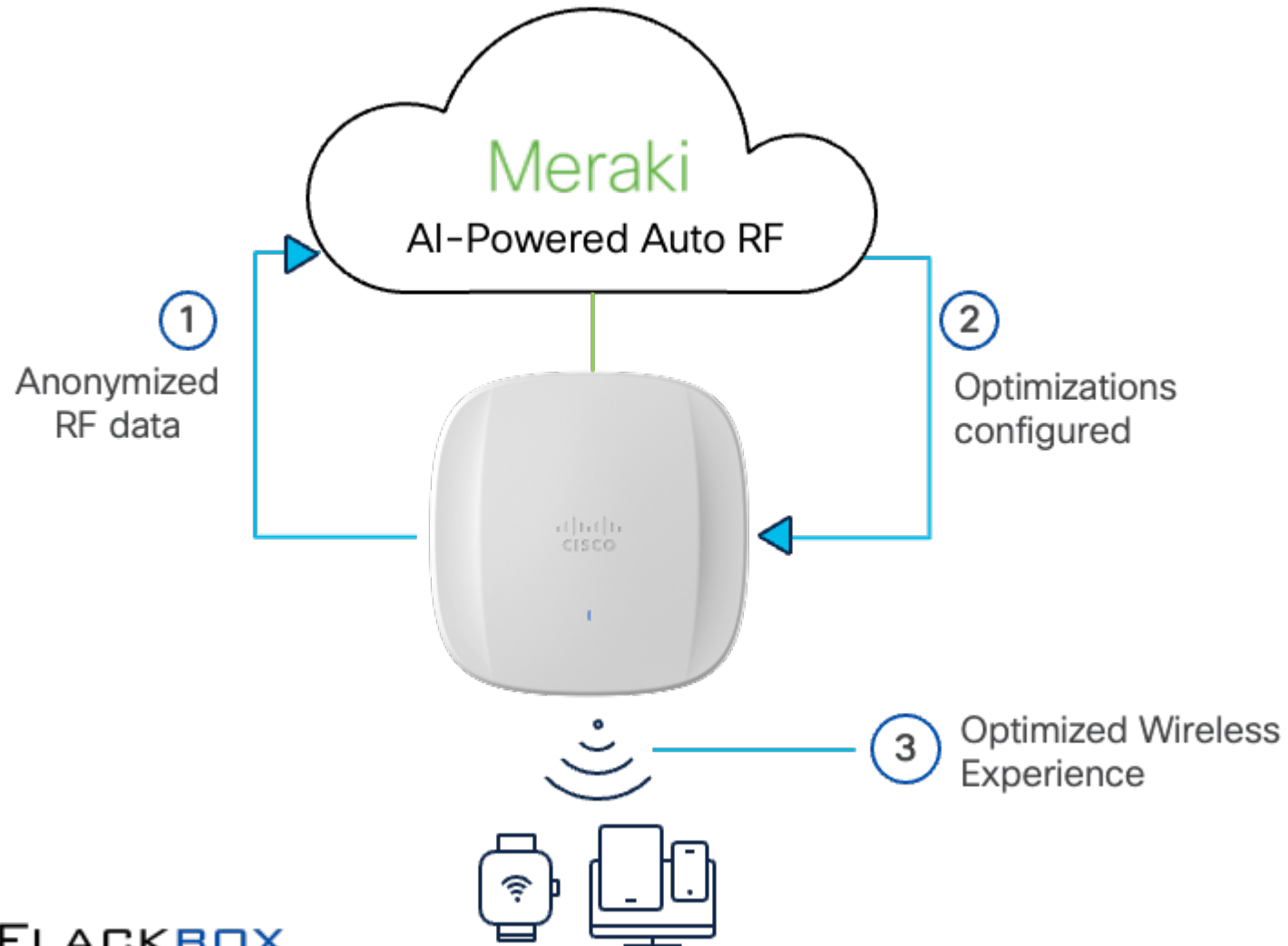


# Cisco Meraki AI Features



- The Meraki Dashboard features these AI driven capabilities:
- Meraki Wi-Fi network visualization, management and monitoring with wireless assurance.
- Meraki Wi-Fi self-optimization with visibility, historical insights and real-time data for Radio Resource Management. Auto RF selects the best channel and power level.

# Cisco Meraki Auto RF



# Cisco Meraki Auto RF (Cont.)



## Radio Settings

Overview RF Profiles

**Auto RF**

### AI channel planning

☒ AI channel planning OFF

[Download details](#)

2 RF jammed APs



2 DFS hit APs



☐ AI channel planning ON

Enhance Auto RF by leveraging artificial intelligence to optimize channel planning capabilities ⓘ

2 RF jammed APs mitigated



2 DFS hit APs mitigated



### Busy hour

☒ Minimize RF changes during busy hour

Auto RF will minimize changes during the most active hours of the day ⓘ

#### Daily busy hour

☒ Auto

Based on historical data of up to the last 6 weeks ⓘ

23:00



08:00



☐ Manual

# Cisco Nexus Dashboard










- Cisco Nexus Dashboard is a single pane of glass application designed for automated provisioning, monitoring, anomaly detection and capacity planning of data centers with NX-OS Nexus and MDS switches.
- It can be installed as a hardware appliance or virtual machine on-premises, or as cloud based SaaS
- The Fabric Controller service supports automated provisioning and monitoring.
- The Orchestrator service supports mobility and disaster recovery in multi-site environments.

# Cisco Nexus Dashboard Insights



- Cisco Nexus Dashboard Insights uses ML and AI to provide traffic analysis, anomaly detection and root cause analysis.
- Assurance ensures device configurations comply with the organization's policies.
- Event Analytics includes control plane event analysis.

-  Overview
-  Operate
-  Analyze
-  Configure
-  Admin
-  Explore
-  Bookmarks

ACI

## Bruxelles-Fabric1

[View in Topology](#)

[Site Details](#)



**Anomaly  
Level  
Critical**

1 total critical anomaly,  
out of which 1 occurred  
in the last week



**No  
Advisories**

No advisories  
found

### External Traffic

Last 7 Days



- Received  
0.17% of total traffic
- Sent  
99.83% of total traffic

**2.05 TB** Total Data Transferred

### Connectivity

**64**  
Endpoints


**11**  
L3 Neighbors




### Inventory

Controllers  
**1**

Switches  
**3**


 Overview

 Operate

 **Analyze**

 Configure

 Admin

 Explore

 Bookmarks

Analyze ▸ Analysis Hub

## Analysis Hub

Analyze and troubleshoot your network with advanced analytics tools optimized for you to gain valuable insights into the performance and health of your network.



### Compliance

Monitor your fabric's compliance with custom anomaly rules



### Conformance

Keep track of your hardware and software life cycles



### Policy CAM

Monitor your network's policies



### Connectivity

Analyze flows from one endpoint to another



### Log Collector

Collect and analyze logs from your devices



### Sustainability

Explore your site's energy usage, cost, and emissions



### Delta Analysis

Compare configurations and differences in your site(s) between two points in time




### Pre-Change


View the potential impact of configuration changes


© Cisco Systems, Inc.


Current date and time is Thursday, December 7, 11:07 PM (CET)




 Overview

 Operate

 **Analyze**

 Configure


 Admin

 Explore

 Bookmarks

## Anomalies

[Refresh](#)

 Online Sites ▾

All Anomalies **Grouped** ▾  Active Now ▾

Filter









### Anomaly Level



■ Critical 10  
■ Major 3  
■ Other

### Category

Configuration 7 Connectivity 5 Hardware 3  
Integrations 1 Active bugs 3

Title	Anomaly Level	Category	Count	
<a href="#">Interface Down</a>	 Critical	Connectivity	5	
<a href="#">Bugs Currently Impacting Site</a>	 Major	Active bugs	3	
<a href="#">Environmental Power Supply Equipment Psu Missing</a>	 Warning	Hardware	2	
<a href="#">Incomplete VPC Backup VLAN Configuration</a>	 Major	Configuration	2	
<a href="#">VPC Peer Keep Alive Error</a>	 Critical	Configuration	2	
<a href="#">Contract Has No Consumers</a>	 Warning	Configuration	1	
<a href="#">Environmental Power Supply Equipment Psu Down</a>	 Warning	Hardware	1	



# Cisco AppDynamics



- AppDynamics monitors applications and their infrastructure.
- It can be installed on Linux or Windows on-premises, or as cloud based SaaS
- Agents on the application servers report their statistics to the AppDynamics controller.
- It uses Machine Learning and AI to perform baselining, anomaly detection, and root cause analysis.
- It learns historical data, time-of-day and seasonal variations, and integrates log analysis tools.






# Cisco AppDynamics (Cont.)



Getting Started Wizard



What do you want to monitor?

Applications




-  Java
-  .NET
-  PHP
-  Node.js
-  Python

User Experience


Browser

-  Real User
-  Synthetic


Mobile

-  iOS
-  Android
-  Cross Platform


Connected Devices

-  IoT SDK

Databases

-  Databases

Analytics

-  Analytics

# Cisco AppDynamics – App Dashboard

Supercar-Trader

Supercar-Trader

Dashboard

Network Dashboard

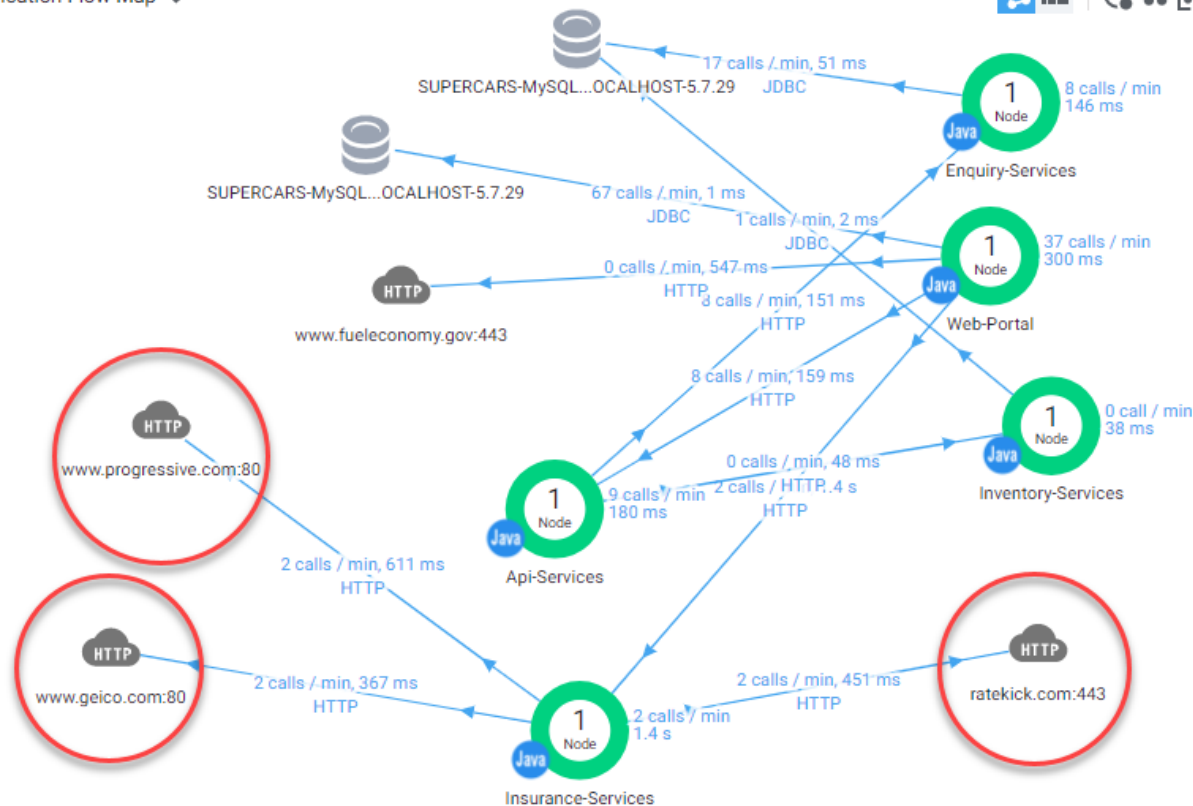
Events

Top Business Transactions

Transaction Snapshots

Transaction Score

Application Flow Map



Legend

Not comparing against Baseline data

Application Dashboard

Business Transactions

Service Endpoints

Tiers & Nodes

Servers

Containers

Database Calls

Remote Services

Troubleshoot

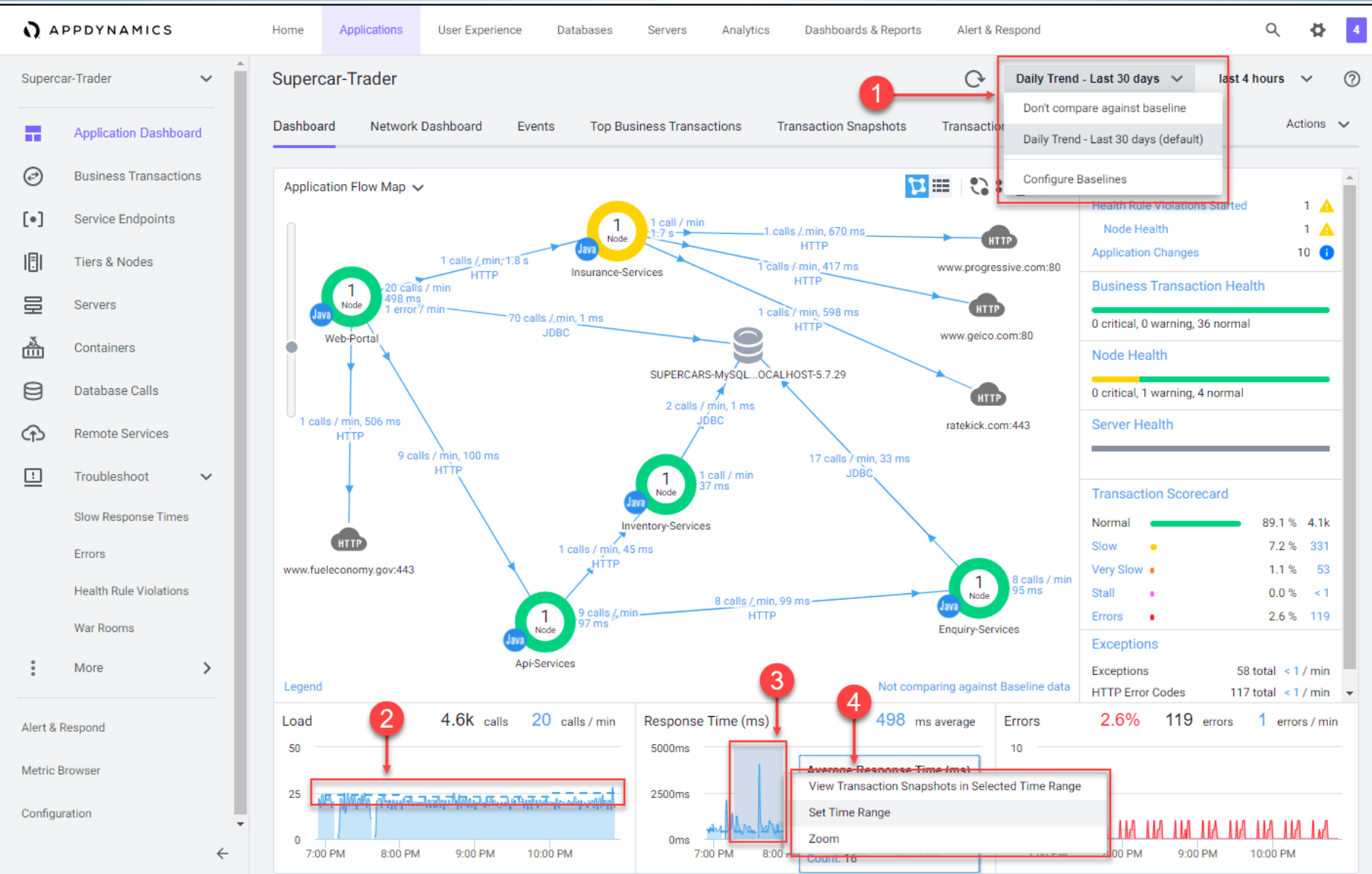
More

Alert & Respond

Metric Browser

Configuration

# Cisco AppDynamics - Baselining



# Cisco AppDynamics - Transactions



Supercar-Trader

## Business Transactions














last 2 hours



Details Filters Actions View Options Configure



Showing 11 of 30

Name	Hea...	Transaction Score	Response Time (ms)	Max Response Time (ms)	Calls	Calls / min	Slow Transacti...	Very Slow Transacti...
 /Supercar-Trader/car.do	✓	<div><div></div></div>	243	4,295	1,056	9	5	9
 /Supercar-Trader/insurance.do	✓	<div><div></div></div>	2,580	6,272	92	1	1	4
 /Supercar-Trader/home.do	✓	<div><div></div></div>	1,088	2,119	60	1	10	3
 /Supercar-Trader/search.do	✓	<div><div></div></div>	558	1,317	565	5	-	-
 /Supercar-Trader/cars.do	✓	<div><div></div></div>	505	1,011	180	2	-	-
 /Supercar-Trader/sell.do	✓	<div><div></div></div>	496	973	60	1	1	-
 /Supercar-Trader/enquire.do	✓	<div><div></div></div>	459	985	120	1	0	-
 /Supercar-Trader/about.do	✓	<div><div></div></div>	543	990	60	1	11	-
 /Supercar-Trader/deleteRecord.jsp	✓	<div><div></div></div>	0	1	28	0	-	-
 /Supercar-Trader/updateRecord.jsp	✓	<div><div></div></div>	0	1	28	0	-	-
 /Supercar-Trader/supercars.do	✓	<div><div></div></div>	547	1,019	84	1	0	-

Application Dashboard

Business Transactions

Service Endpoints

Tiers & Nodes

Servers

Containers

Database Calls

Remote Services

Troubleshoot

More

Alert & Respond

Metric Browser

Configuration

# Cisco ThousandEyes



- ThousandEyes is a cloud managed monitoring and troubleshooting platform which is designed for organisations with complex distributed networks and applications on cloud or across the internet.
- It monitors internal and external (ISP and cloud provider) network availability and performance for applications.
- It helps identify the root cause of application performance problems as originating from the network, the application or external dependencies.
- It's security monitoring features include detection of anomalies and DDoS and DNS based attacks.

# Cisco ThousandEyes Agents



- Monitoring agents provide statistics and different vantage points for tests:
- **Enterprise agents** operate within the enterprise infrastructure.
- **Endpoint agents** are installed on end user machines.
- **Cloud agents** are managed by ThousandEyes and are distributed throughout ISPs and cloud providers. They provide inbound remote monitoring of the enterprise apps and infrastructure.

# Cisco ThousandEyes AI and ML



- ThousandEyes agents located across the Internet perform billions of measurements each day, creating a massive data set on when and where traffic flows are disrupted at the network interface and application server levels.
- IT teams can rapidly identify, escalate and remediate issues with providers using Internet telemetry data.



## Remote ADP sales staff report their web application is not working

Agent

All agents

### Views

WEB

Page Load

HTTP Server

NETWORK

Overview

Path Visualization

ROUTING

BGP Route Visualization

Target URL

<https://www.adpwebdesking.com>

Map

Table

Waterfall

Details for all 38 agents

DOM Load Time 933 ms

Page Load Time 1203 ms ⓘ

Errors from 4 agents

Metric

Page Load Time

24h 7d 14d



Showing data from Thu, Jan 26 15:30 - 15:45 CST (Jan 27, 2017)

Latest



Page Load

24h 7d 14d

HTTP Server

NETWORK

Overview

Path Visualization

ROUTING

BGP Route Visualization

Target Server

www.adpwebdesking.com:443

Showing data from Thu, Jan 26 15:30 - 15:40 CST (Jan 27, 2017)

Latest

## Path Visualization

Showing: 1 of 1 Test 8 of 38 Agents (Show All) 1 of 1 Server Hide IP Address labels

Grouping: Agents by Agent Interfaces by IP Address Destinations by Domain

Highlighting: Forwarding Loss &gt; 10 % ( 6 nodes ) Link Delay &gt; 100 ms ( 1 link )

Selecting: Click a node or link Info (2)

Outage Detected ( 1 node )



WEB

Page Load  
HTTP Server

NETWORK

Overview  
Path Visualization

ROUTING

**BGP Route Visualization**

Target Prefix  
207.186.144.0/21

Showing data from Thu, Jan 26 16:00 - 16:15 CST (Jan 27, 2017)

Average Path Changes

**BGP Route Visualization**Showing: Monitor Atlanta, GA ☐ Add a filter ☐ Remove allPaths active for more than 0s ☐Related: 1 covering prefix ☐Grouping: Monitors by Monitor ☐Selecting: Click a node or link Quick selections by Warning (2) ☐3 hops  2 hops

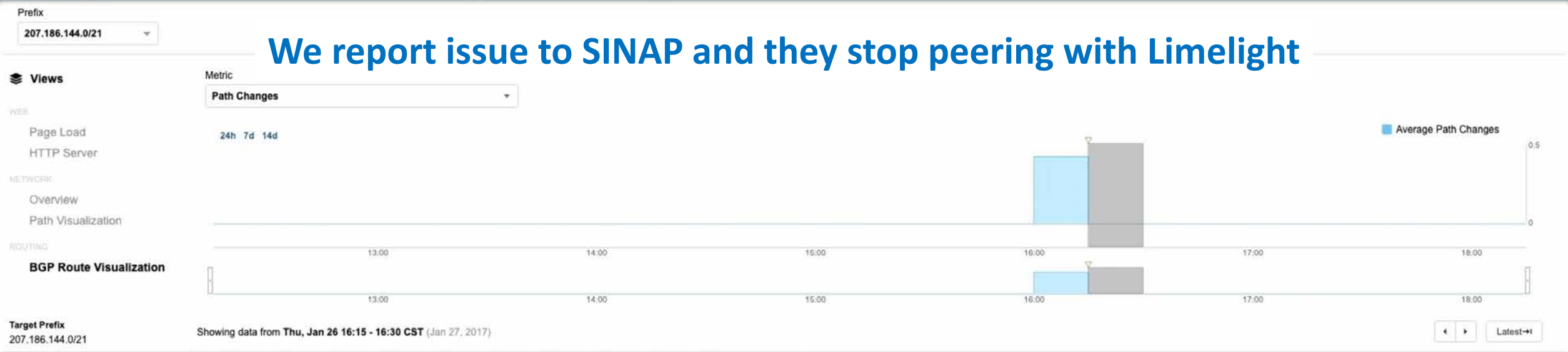
Highlight nodes that match all / any

Search on Network, Country, IP address, Prefix, or Title...



&lt; Undo



# We report issue to SINAP and they stop peering with Limelight



## BGP Route Visualization

Showing: Monitor **Atlanta, GA**  Add a filter  Remove all

Paths active for more than **0s**

Related: 1 covering prefix

Grouping: Monitors by **Monitor**

Selecting: Click a node or link

Node

**SINAP-TIX, LLC (AS 22911)**

Primary Country

Global Network Rank

Prefixes Announced

United States

1787

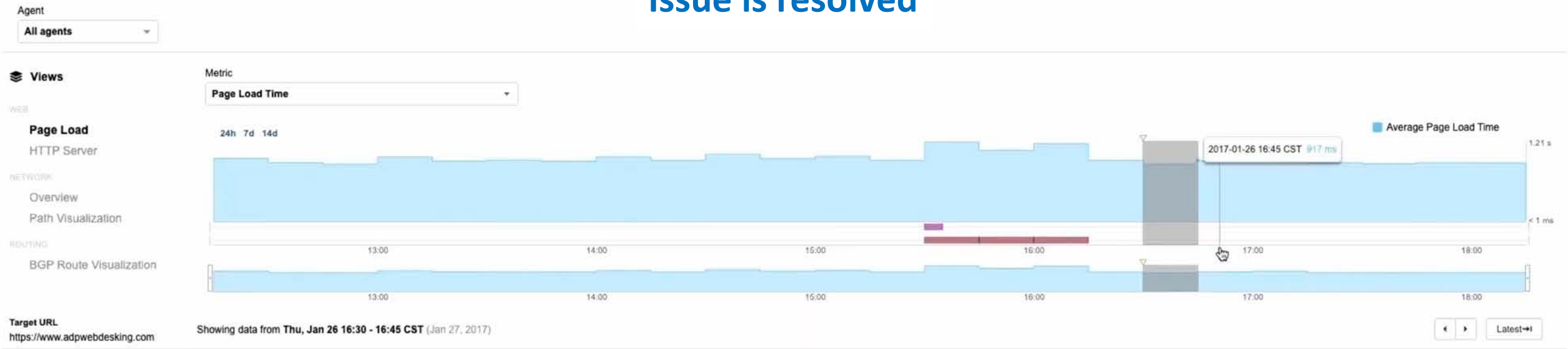
15

Show only routes passing through this AS

3 hops  2 hops



# Issue is resolved



# Cisco Secure Network Analytics



- Cisco Secure Network Analytics was formerly named StealthWatch
- It is security software which analyzes network traffic to create a baseline of normal network behavior
- It is also aware of malicious external domains and servers globally
- Machine Learning and advanced analytics identifies anomalies and threats and responds in real- time

# Cisco Secure Network Analytics (Cont.)

- Threats include Command-and-Control (C&C) attacks, ransomware, DDoS, unknown malware and insider threats.
- Automated responses to threats include quarantining the affected host with ISE Identity Services Engine integration.
- It can be installed as a hardware appliance or virtual machine on-premises, or as cloud based SaaS



# ML in Cisco Secure Network Analytics

- Cisco Secure Network Analytics uses Machine Learning for:
  - Contextual network-wide visibility
  - Predictive analytics
  - Automated detection and response



## Security Insight Dashboard | Inside Hosts

### Alarming Hosts

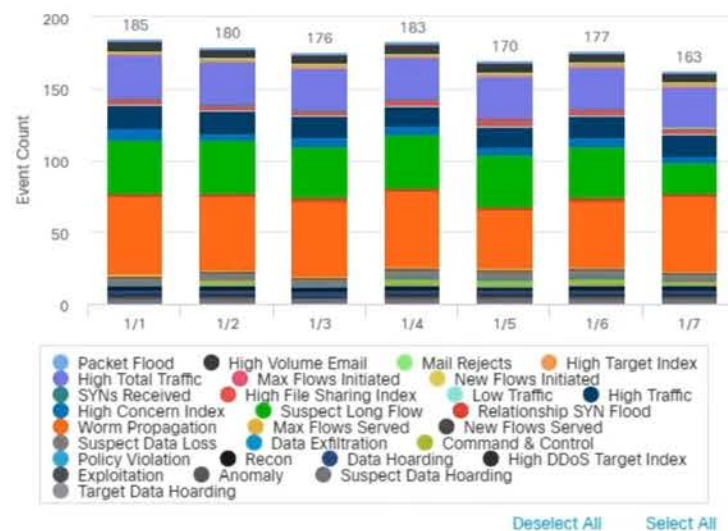


### Top Alarming Hosts

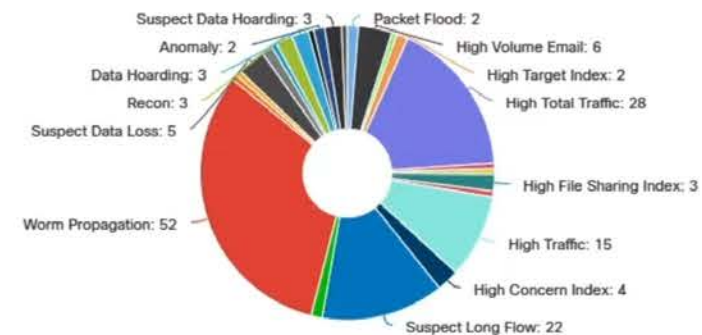
Host	Category
10.201.3.149 ... End User Devices	DH CI RC
10.201.3.18 ... End User Devices	DH CI
10.10.30.11 ... End User Devices	AN
10.201.0.23 ... Terminal Servers	DH TI
10.201.3.83 ... End User Devices	CI RC
10.10.30.15 ... DNS Servers	TI DT
10.201.3.50 ... End User Devices	CI RC

[View All Hosts >](#)

### Alarms by Type



### Today's Alarms



Host Report | 10.201.3.149

## Automatic Grouping

### Alarm Categories

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
1	0	1	0	0	0	0	1	0	0	0

### Host Summary



Host IP  
10.201.3.149 ...

Flows

Classify

History

Status:

Hostname: --

Host Groups: End User Devices,Desktops,Atlanta, Sales and Marketing

Location: RFC 1918

First Seen: 1/25/20 1:36 AM

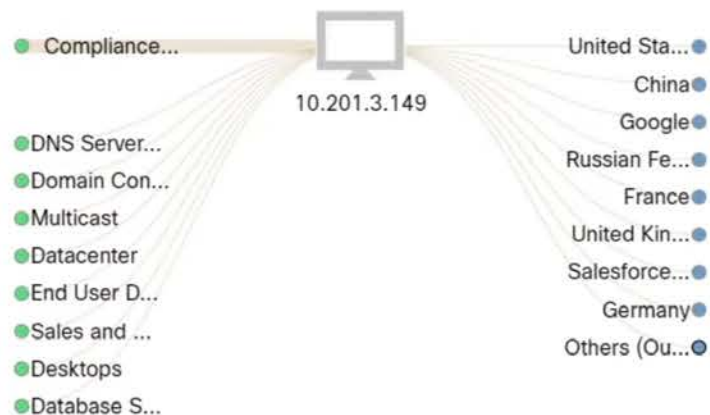
Last Seen: 1/7/21 4:07 PM

Policies: Insider Threat Event (10.201.3.149),Client IP Policy,Inside

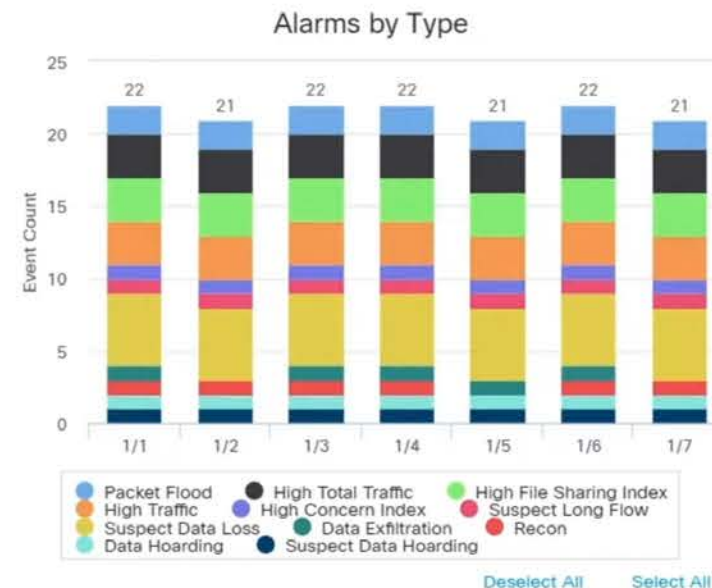
MAC Address: --

ISE ANC Policy: -- Edit

### Traffic by Peer Host Group (last 12 hours)



### Alarms by Type (last 7 days)



[Flows](#)
[Classify](#)
[History](#)
**Status:**
**Hostname:** --

**Host Groups:** End User Devices,Desktops,Atlanta, Sales and Marketing

**Location:** RFC 1918

**First Seen:** 1/25/20 1:36 AM

**Last Seen:** 1/7/21 4:07 PM

**Policies:** Insider Threat Event (10.201.3.149),Client IP Policy,Inside

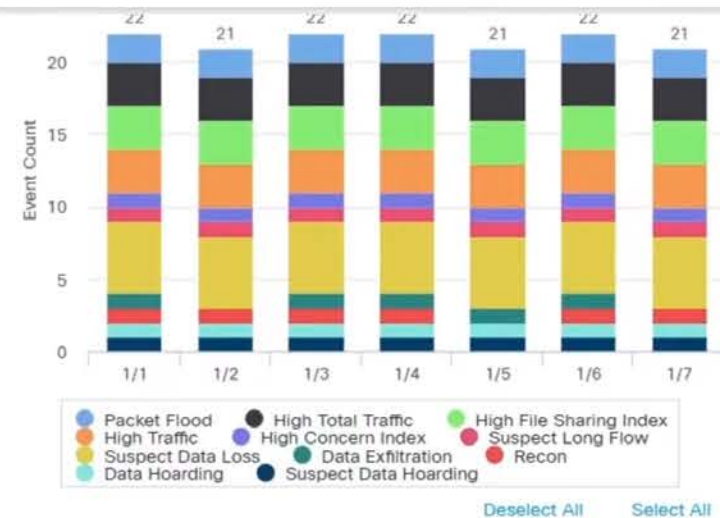
**MAC Address:** --

**ISE ANC Policy:** -- [Edit](#)

10.201.3.149

- DNS Server...
- Domain Con...
- Multicast
- Datacenter
- End User D...
- Sales and ...
- Desktops
- Database S...

- China
- Google
- Russian Fe...
- France
- United Kin...
- Salesforce...
- Germany
- Others (Ou...



## Top Security Events for 10.201.3.149

[Source \(10\)](#)
[Target \(4\)](#)

Security Event	Count	Concern Index	First Active	Target Host	Target Host Group	Actions
▶ Suspect Data Hoarding	31	45,731,106	01/07 2:35:00 AM	Multiple Hosts	--	...
▶ High Total Traffic	38	554,634	01/07 8:30:00 AM	Multiple Hosts	--	...
▶ High Traffic	28	452,974	01/07 2:35:00 AM	Multiple Hosts	--	...
▶ Addr_Scan/tcp - 22	252	168,000	01/07 6:49:58 AM	10.201.0.0/24 ...	--	...
▶ Addr_Scan/tcp - 22	252	168,000	01/07 6:50:00 AM	10.201.2.0/24 ...	--	...
▶ Addr_Scan/tcp - 22	276	156,000	01/07 6:49:59 AM	10.201.1.0/24 ...	--	...
▶ Addr_Scan/tcp - 22	186	124,000	01/07 6:50:02 AM	10.201.3.0/24 ...	--	...



MALWARE RANSOMWARE **ENCRYPTED**

100% confidence, in #CWNC01

★ NEW / TRIAGE ...

Add notes...

## Malicious External Server

▼ OCCURRENCE

7 days

Dec 31 - Jan 7

### ANOMALIES AND FLOWS

RISK FACTOR FILTER: ☒ Critical ☒ High ☐ Medium ☐ Low

Anomaly

Domain

Server IP

Autonomous System

☒ malicious host  
Communication with  
hostname  
[luqerfsodp9ifjaposdfjh...](#)  
known to be indicative of  
CWNC01

☐ tor relay  
Communication with IP  
addresses [176.9.39.218](#),  
[212.47.244.38](#), and  
[217.112.131.98](#) known  
to be Tor nodes

☐ [luqerfsodp9ifjaposdfjh...](#)  
Inferred: 83%

☐ 104.17.41.137

☐ Cloudflare Inc

☐ 212.47.244.38

☐ 212.47.244.38

☐ Solar Communications GmbH

☐ 27mqgnjrmhhypy7k6.com

☐ 46.28.207.19

☐ Online S.a.s.

☐ 98-131-112-217.hu.xe...

☐ 217.112.131.98

☐ 23VNet Kft.

☐ wuat27zyqlo.com

☐ 162.173.201.62

Feedback





Applying ANC policy

Select the ANC Policy to apply to ISE cluster for this host: 10.201.3.149

ISE Server: **Tradeshow ISE**  
Username: ken  
MAC: 64:80:99:51:f6:88  
ANC Policy:

No policy applied

No policy applied

SW\_Quarantine

SW\_Port\_Bounce

SW\_Shutdown

Source Host	Source Host Group	Target Host	Target Host Group	Actions
10.201.3.149 ...	End User Devices , Desktops , Atlanta , Sales and Marketing	Multiple Hosts	--	...
has downloaded an unusual amount of data from one or more hosts.				
10.201.0.72 ...	Atlanta , Compliance Systems	10.201.3.149 ...	End User Devices , Desktops , Atlanta , Sales and Marketing	...
10.201.3.149 ...	End User Devices , Desktops , Atlanta , Sales and Marketing	Multiple Hosts	--	...
10.201.3.149 ...	End User Devices , Desktops , Atlanta , Sales and Marketing	Multiple Hosts	--	...
10.201.3.149 ...	End User Devices , Desktops , Atlanta , Sales and Marketing	10.201.0.0/24 ...	--	...
10.201.3.149 ...	End User Devices , Desktops , Atlanta , Sales and Marketing	10.201.2.0/24 ...	--	...
10.201.3.149 ...	End User Devices , Desktops , Atlanta , Sales and Marketing	10.201.1.0/24 ...	--	...



## Response Management

## Automated Response Management

Rules Actions Syslog Formats



## Rules

Add New Rule ▾

Name ↑	Type	Domain	Description	Enabled	Actions
Block Rogue DHCP server from the Network	Host Alarm	IT	This rule will block network access for a Host when the Unauth DHCP server CSE is triggered	<input type="checkbox"/>	...
FlowCollector System Alarm	FlowCollector System Alarm	SP	This rule will send an email message to users populated within the "Send email" action. To send additional alarm types, edit this rule to add/remove alarm types.	<input checked="" type="checkbox"/>	...
FlowCollector System Alarm	FlowCollector System Alarm	IT	This rule will send an email message to users populated within the "Send email" action. To send additional alarm types, edit this rule to add/remove alarm types.	<input checked="" type="checkbox"/>	...
Host Group Relationship Alarms to Threat Response	Host Group Relationship Alarm	IT		<input checked="" type="checkbox"/>	...
Quarantine End User Devices Violating PCI Policy	Host Alarm	IT	Quarantine End user Devices violating PCI Policy by connecting to PCI servers	<input checked="" type="checkbox"/>	...
SMC System Alarms	Stealthwatch Management Console System Alarm	All	This rule will send an email message to users populated within the "Send email" action. To send additional alarm types, edit this rule to add/remove alarm types.	<input type="checkbox"/>	...
StealthWatch Host Alarms - Inside Hosts as the Source of alarm	Host Alarm	SP	This rule will send an email message to users populated within the "Send email" action. To send additional alarm types, edit this rule to add/remove alarm types.	<input checked="" type="checkbox"/>	...
StealthWatch Host Alarms - Inside Hosts as the Source of alarm	Host Alarm	IT	This rule will send an email message to users populated within the "Send email" action. To send additional alarm types, edit this rule to add/remove alarm types.	<input checked="" type="checkbox"/>	...
StealthWatch Host Alarms - Outside Hosts as the Source of alarm	Host Alarm	SP	This rule will send an email message to users populated within the "Send email" action. To send additional alarm types, edit this rule to add/remove alarm types.	<input checked="" type="checkbox"/>	...
StealthWatch Host Alarms - Outside Hosts as the Source of alarm	Host Alarm	IT	This rule will send an email message to users populated within the "Send email" action. To send additional alarm types, edit this rule to add/remove alarm types.	<input checked="" type="checkbox"/>	...
Threat Response	Host Alarm	IT		<input checked="" type="checkbox"/>	...
Trapped Host Alarm	Host Alarm	SP	Send alarm for any hosts that communicate with the honeypot host group	<input type="checkbox"/>	...



## Response Management

Rules

Actions

Syslog Formats

### Actions

[Add New Action](#) ▾

Name ↑	Type	Description	Used By Rules	Enabled	Actions
Create Threat Response Incident	Threat Response Incident		2	<input checked="" type="checkbox"/>	...
ISE Port Bounce	ISE ANC Policy		0	<input checked="" type="checkbox"/>	...
ISE Port Shutdown	ISE ANC Policy		0	<input checked="" type="checkbox"/>	...
ISE Quarantine	ISE ANC Policy	Quarantine a host	2	<input checked="" type="checkbox"/>	...
Send email	Email	Send email message Edit to add recipients within the "To:" field	2	<input checked="" type="checkbox"/>	...

# Further Learning Resources on cisco.com

- DevNet Sandbox

<https://devnetsandbox.cisco.com>

- DevNet Learning Labs

<https://developer.cisco.com/learning/>