

CISCO *Live!*



#CiscoLive



The bridge to possible

Simplify your Cyber Asset Attack Surface Management

with Cisco

Hanna Jabbour – Leader Technical Marketing Engineer – TD&R

@hanna_jabbour

BRKSEC-2346



#CiscoLive

Cisco Webex App

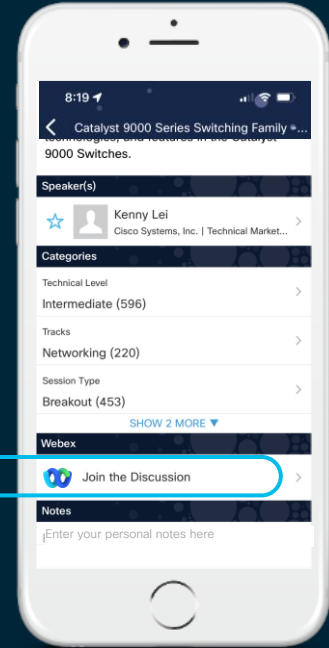
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 17, 2022.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2346>

Abstract

Securing your migration to the cloud starts with understanding your environment. Every entity within your cyber universe has the potential to either boost or diminish your security posture. These include but are not limited to **users, roles, groups, rulesets, policies, certificates, applications, workloads, containers, functions, endpoints, devices, databases**, etc.

This session will provide a **deep dive into securing these assets** through different techniques including **visibility, breach detection, policy**, and **risk management**.



Agenda

- Introduction
- Cyber Assets Visibility
- Attack Surface Management
- Cloud Security Posture Management
- Conclusion

Who Is your presenter



Hanna Jabbour

- 14 years of experience in Dev/Network/Security
- TME for Secure Analytics covering EMEAR/APJ
- Lebanese based out of the Dubai
- Yes, my name is Hanna

Lebanon



My home town



Anoubin

<https://www.youtube.com/watch?v=INiCIW2VpCI>

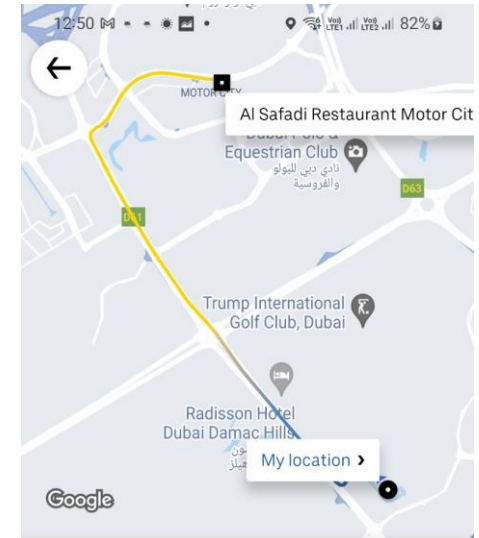


Jounieh

Dubai



CISCO *Live!*



Chopper 1 AED 520.00-624.00

Only available for Dubai city tour



Cash



No Choppers Available Now



Introduction



Accelerated Cloud Adoption increases security risk

Rapid cloud adoption with multi and hybrid cloud approach



Over 75% of midsize and large organizations will have adopted a multi-cloud and/or hybrid IT strategy¹

Expansion of the attack surface



50% increase in the number of applications supported by an organization over next two years², and sharp increase in distributed workforce

Fragmented and siloed view across cyber footprint



55% of organizations do not have an accurate inventory of assets³

Diversity pushes us to use to many many tools



Multi Cloud



Diverse Entity Types



Tools



You can't
protect

What you
can't see

Secure Cloud Insights



Asset Inventory

Entity Mapping

Security Intelligence

Data Ingest and classification



Native Data Ingestion

Integrate with data sources in the cloud or on prem natively through available APIs or data streams.

Asset discovery & mapping

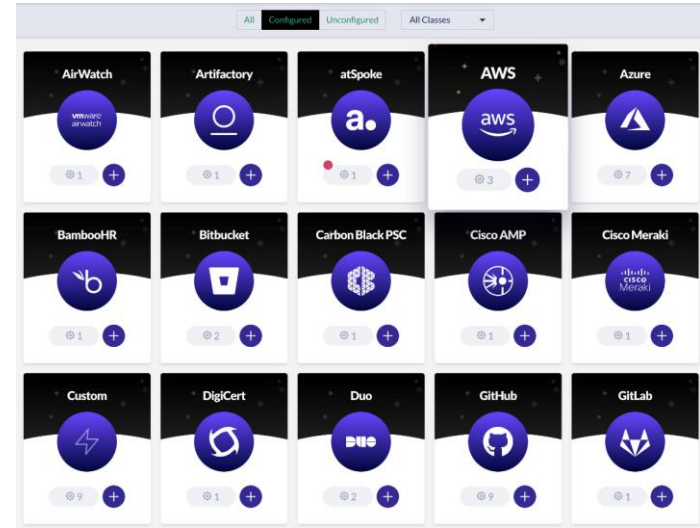
Identity assets and entities across multiple data sources. Correlate and map asset relations across multiple data sources



Agentless integration via API

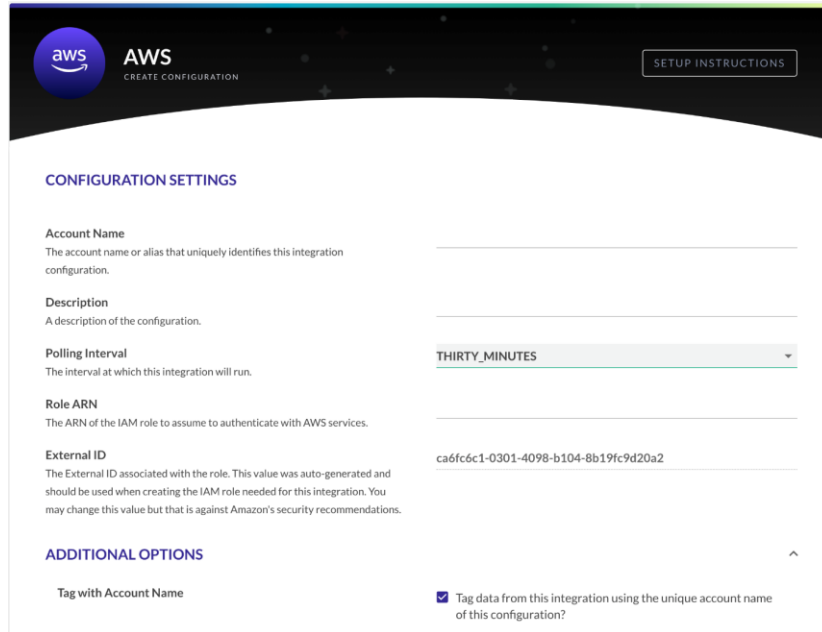
- Supply: Service account, IAM Role, or API Key on the config page
 - Read-only permissions
 - AWS/Azure/GCP can be integrated at the organization level

The screenshot shows the 'AWS' configuration page in the Cisco Duo interface. At the top, there's a header with the AWS logo and 'CREATE CONFIGURATION' button. Below this is a 'CONFIGURATION SETTINGS' section with fields for 'Account Name', 'Description', 'Polling Interval' (set to 'THIRTY_MINUTES'), and 'Role ARN'. An 'External ID' field contains the value 'ca6fc6c1-0301-4098-b104-8b19c9d20a2'. Under 'ADDITIONAL OPTIONS', there's a checkbox 'Tag with Account Name' which is checked, with a note: 'Tag data from this integration using the unique account name of this configuration?'. A 'SETUP INSTRUCTIONS' button is visible in the top right.



Polling Updates of data

- Configure polling interval 30 min, 1 hr, 4 hrs, 8 hrs, 12 hrs, 1 day, 1 week
- Automatically tag data with Account Name or Production tags

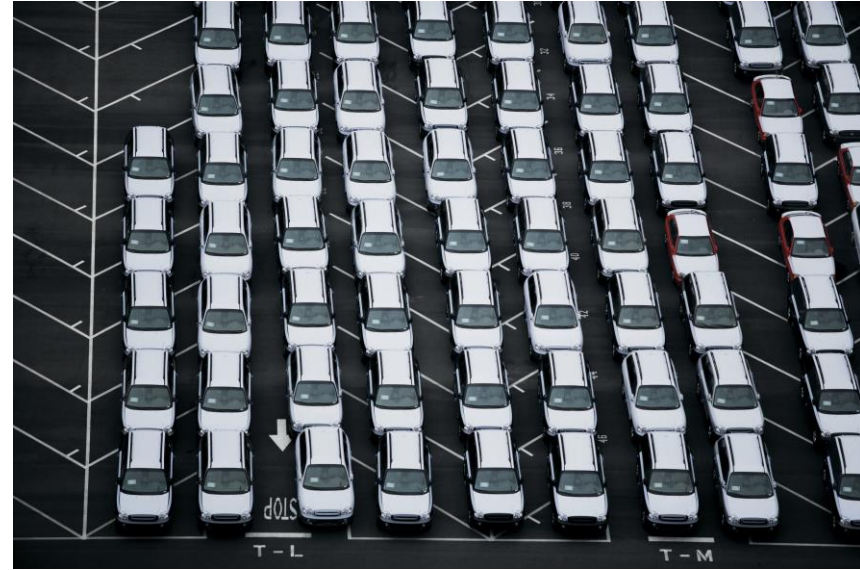


The screenshot shows the 'CREATE CONFIGURATION' page in the AWS console. The header includes the AWS logo, the text 'AWS CREATE CONFIGURATION', and a 'SETUP INSTRUCTIONS' button. The main section is titled 'CONFIGURATION SETTINGS' and contains several fields: 'Account Name' (with a description), 'Description' (with a description), 'Polling Interval' (a dropdown menu currently set to 'THIRTY_MINUTES'), 'Role ARN' (with a description), and 'External ID' (with a description and a pre-filled value 'ca6fc6c1-0301-4098-b104-8b19fc9d20a2'). Below this is an 'ADDITIONAL OPTIONS' section with a checkbox labeled 'Tag with Account Name' which is checked, and a description: 'Tag data from this integration using the unique account name of this configuration?'. An upward arrow is visible to the right of the 'ADDITIONAL OPTIONS' section.

Diverse Asset Types



- Data Stores
- Policies
- Certificates
- Containers
- Identities
- Endpoints
- Secret Keys
- Etc ...
- IAM roles
- Users



To much data

?

Data Modeling and architecture



Class: super-type or high-level definition



Type : defines what the entity is



Entity: represent a resource in your environment

Property	Type	Description
`id`	`string`, `array`	Identifiers
`name`	`string`	Name of this entity
`displayName`	`string`	Display name, e.g. a
`summary`	`string`	A summary / short de
`description`	`string`	An extended descript
`classification`	`string`, `null`	The sensitivi
`criticality`	`integer`	A number that repre
`risk`	`integer`	The risk level of t
`trust`	`integer`	The trust level of
`complianceStatus`	`number`	The compliance statu

▼ Defined Entities Table

Entity	Description
`AccessKey`	A key used to grant access, such as ssh-key, access-key, ap
`AccessPolicy`	A policy for access control assigned to a Host, Role, User,
`AccessRole`	An access control role mapped to a Principal (e.g. user, gr
`Account`	An organizational account for a service or a set of service
`Application`	A software product or application.
`ApplicationEndpoint`	An application endpoint is a program interface that eith
`Assessment`	An object to represent an assessment, including both compli
`Attacker`	An attacker or threat actor.
`Backup`	A specific repository or data store containing backup data.

Entity	Description
Everyone	The global UserGroup that represents "everyone" publicly.
Internet	The Internet -- i.e. a Network entity with CIDR "0.0.0.0/0".
Root	The entity that represents the top level organization.

<https://community.askj1.com/kb/articles/846-jupiterone-data-model>

<https://community.askj1.com/kb/articles/1165-add-enriched-or-modified-properties>

Secure Cloud Insights

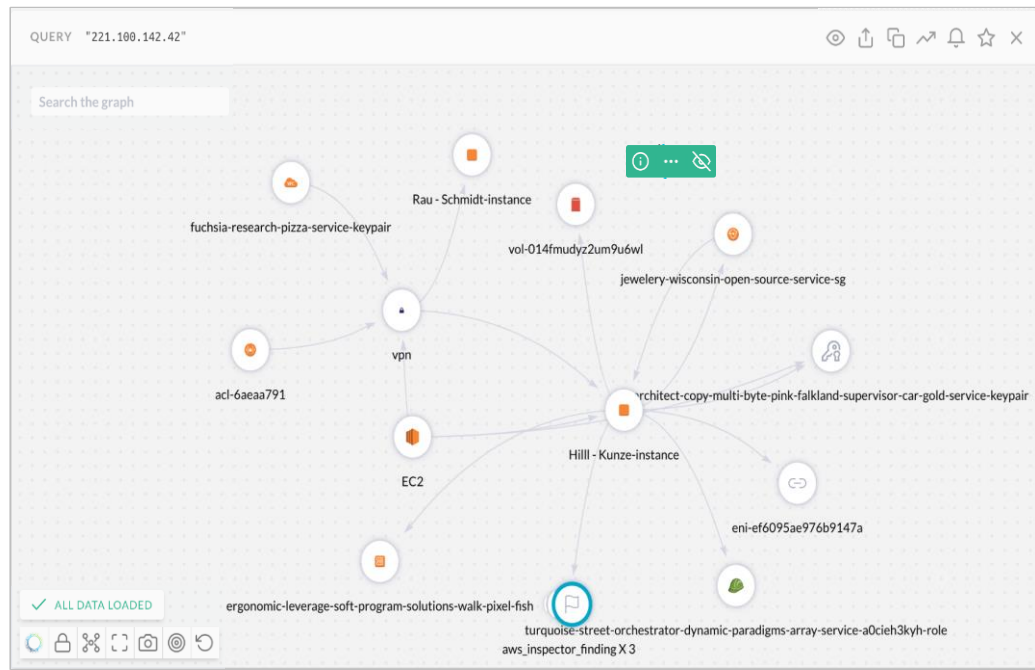


Asset Inventory

Entity Mapping

Security intelligence

Why Relationship is at the core ?



- Associate Assets with each other based on relationships

- Has / Contains
- Is / Owns
- Exploits / Impacts
- Uses
- Connects / Triggers / Extends
- Implements / Mitigates
- Manages
- Evaluates / Monitors / Protects
- Trusts
- Assigned
-

Source

Target

Relationship

Direction



Integrations & Platform Support

Vulnerability Agents

Bugcrowd
Detectify
GitLeaks
HackerOne
NowSecure
Qualys
Rapid7
Snyk
Tenable
Threat Stack
Veracode
Vuls.io
WhiteHat

Endpoints

Carbon Black
Cisco AMP
CrowdStrike
Duo
Jamf
SentinelOne
Trend Micro
AirWatch
Wazuh

Clouds

Amazon AWS
Microsoft Azure
Google Cloud

Network

Cisco Meraki
DigiCert
Nmap
Whois
Shodan

People & Access

Google G Suite
JumpCloud
Microsoft Azure AD
Okta
OneLogin

Workflows

Jira
PagerDuty
Slack
ServiceNow

Custom

GraphQL + REST API
NodeJS SDK

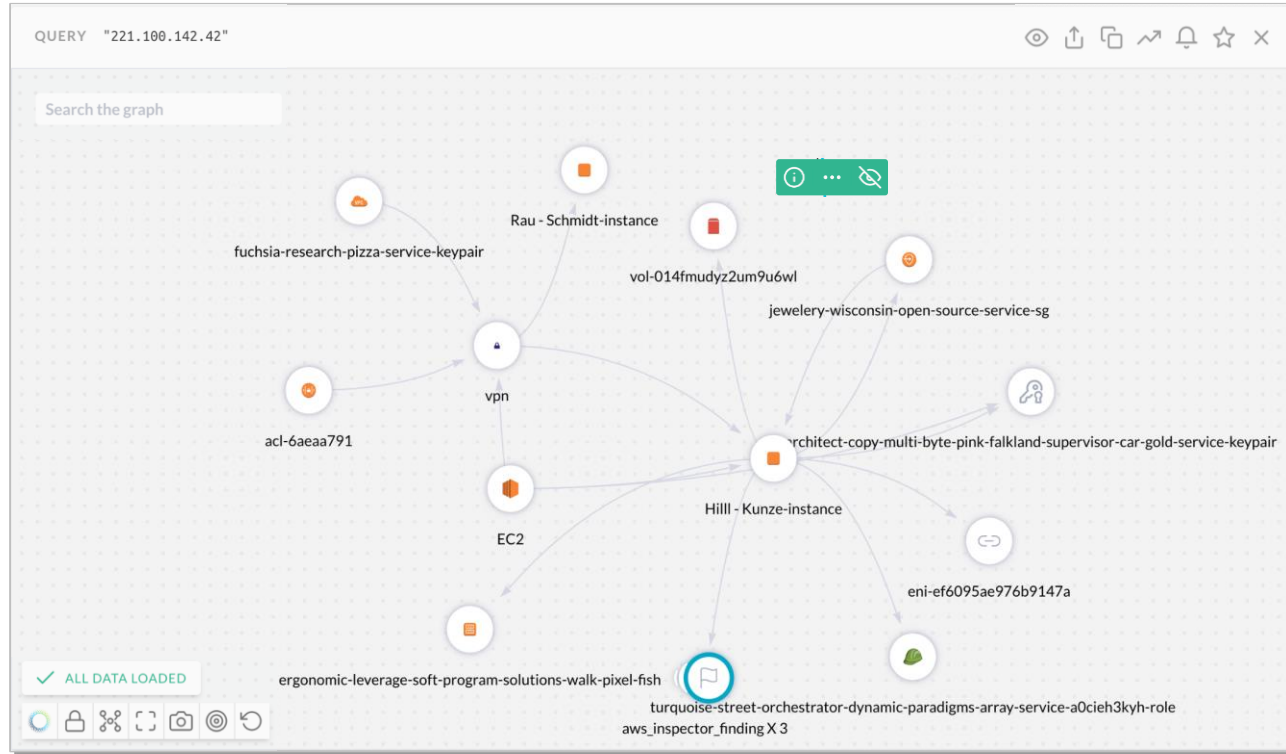
Others

Github
KnowBe4
BambooHR
GoDaddy

Demo – Visibility and relationships

Intuitive Blast Radius walk through

- Walk the graph of data by expanding nodes and view their relationships
- Identify the impact of a compromised asset and what an attacker do next
- Find relevant context to an incident in a matter of seconds



What is Next ?





How to find answers to my challenging questions ?

Simple

- *Are my S3 buckets encrypted?*
- *Which buckets do not have access logging enabled?*
- *Are there backups for configured for my databases?*

Complex

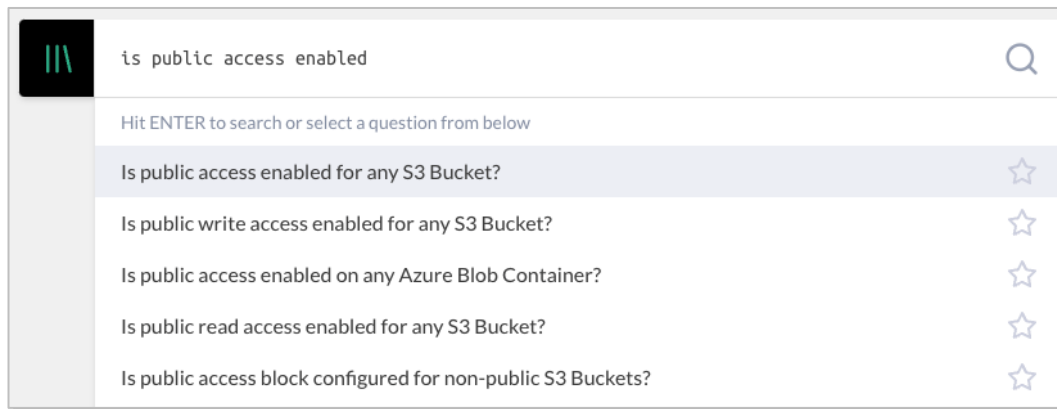
- *Are there Internet-facing EC2 instances that are allowed access to non-public S3 buckets?*
- *Are there cross-account IAM trust relationships to external / vendor accounts?*
- *Which PRs / developer introduced new vulnerability findings this past week?*

Simple Query Language

Query Language

*Find aws_s3_bucket with
classification != 'public' and
ignorePublicAcls != true and
restrictPublicBuckets != true*

Prebuilt and auto filled queries



The screenshot shows a search interface with a search bar at the top containing the text "is public access enabled". Below the search bar is a list of prebuilt queries. The first query, "Is public access enabled for any S3 Bucket?", is highlighted. Each query has a star icon to its right, indicating it can be saved or bookmarked.

Search Query	Action
is public access enabled	🔍
Hit ENTER to search or select a question from below	
Is public access enabled for any S3 Bucket?	☆
Is public write access enabled for any S3 Bucket?	☆
Is public access enabled on any Azure Blob Container?	☆
Is public read access enabled for any S3 Bucket?	☆
Is public access block configured for non-public S3 Buckets?	☆

J1QL Good to Know and example

Selecting multiple entities or relationships:

(class/type_1 | class/type_2)

Comparing properties:

AND, OR

For string, boolean, number and date operations:

~= - Contains

^= - Starts with

\$= - Ends with

!= - Does not equal

!~= - Does not contain

!^= - Does not start with

!\$= - Does not end with

For number and date operations:

> < >= <=

Examples:

Endpoints or instances with IPs in the 10.15.0.0/16 range

- FIND (Host | Device) WITH ipAddress^='10.50'

List of devices running Linux or MacOS

- FIND user_endpoint WITH platform = ('linux' OR 'MacOS')

New hires over the last 12 months

- FIND employee WITH_createdOn > date.now-12months

<https://community.askj1.com/kb/articles/980-introduction-to-jupiterone-query-language-j1ql>

Secure Cloud Insights



Single view for diverse
assets

Entity Mapping

Security Intelligence

Hey! that is not what you described



Incident Response

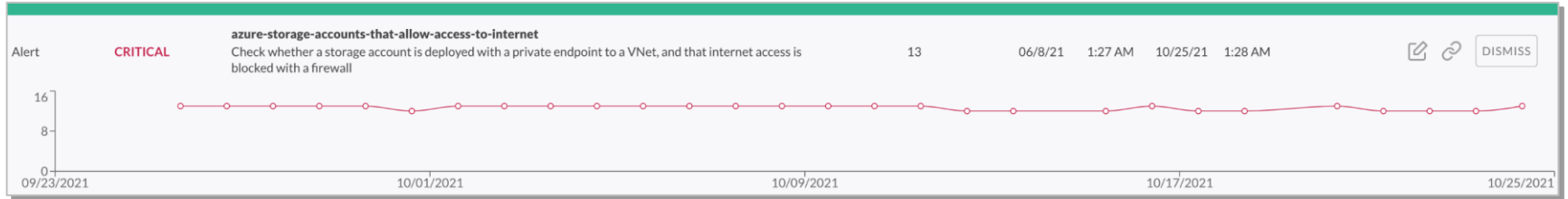


Research or Lab

Transform Queries to a detection mechanism

- Alerting and response with customisable rules.
- Leverage pre-built alert rule packs for cloud security.
- Monitor alert trends over time to identify repetitive breach

- SQS
- SNS
- Email
- Webhook
- Slack
- Etc...





68%

*of organizations believe
that misconfiguration of their cloud
platforms is the biggest threat
facing their cloud environments.*

2020 Cloud Security Report, Cybersecurity Insiders.

Be Ready With
Always On
Compliance



Compliance Status Overview

TOTAL COMPLIANCE STATUS

34% Total compliance on selected frameworks

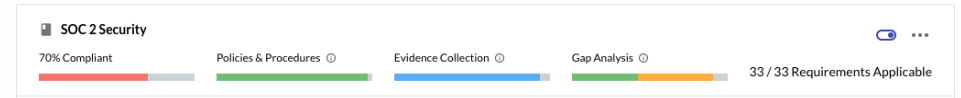
9%	CIS AWS Foundations 1.4
3%	CIS Azure Foundations v1.3.0
0%	CIS Google Cloud Foundations 1.1
8%	CIS Google Cloud Foundations
10%	CIS AWS Foundations 1.4
70%	SOC 2 Security
46%	HIPAA
0%	FedRAMP
65%	CMMC ML1
65%	CMMC ML1
0%	GDPR - example
23%	PCI DSS
0%	FedRAMP
100%	SOC 2 Confidentiality
83%	SOC 2 Availability
0%	FedRAMP
45%	HIPAA
67%	NIST CSF

- **Total Compliance Overview**
Simple compliance view of the environment and per adopted standard, framework or benchmark

Benchmarks



Standards



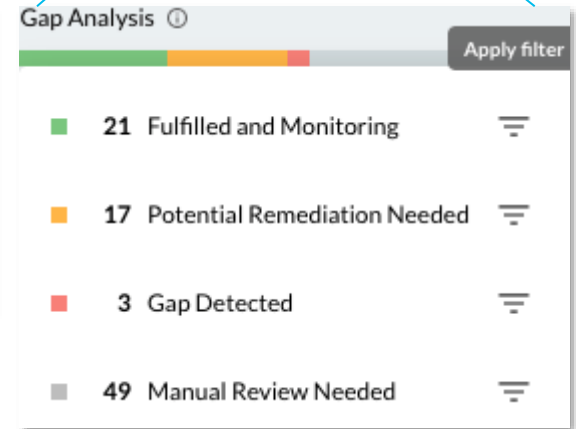
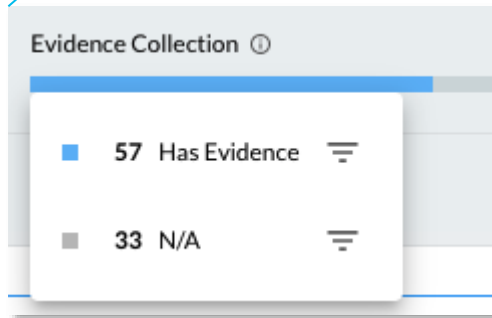
- **Per Framework View**
Simplified per framework compliance view

Filtering by gap analysis or evidence collection



- **Easier in-compliance filtering**

Filtering by gap analysis and evidence collection made easier to find compliance checks with by relevance sorting



Demo - Compliance and Reporting

Secure Cloud Insights

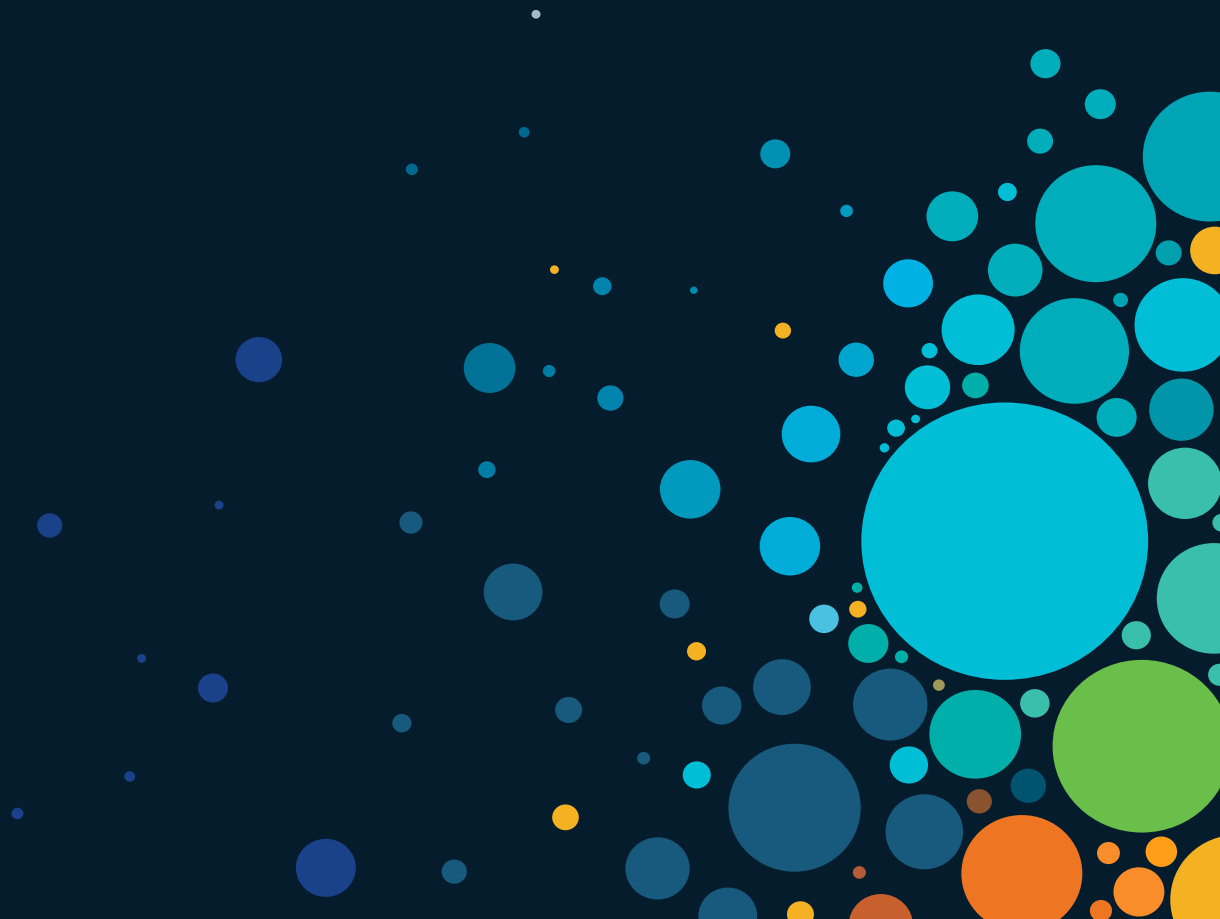


Single view for diverse
assets

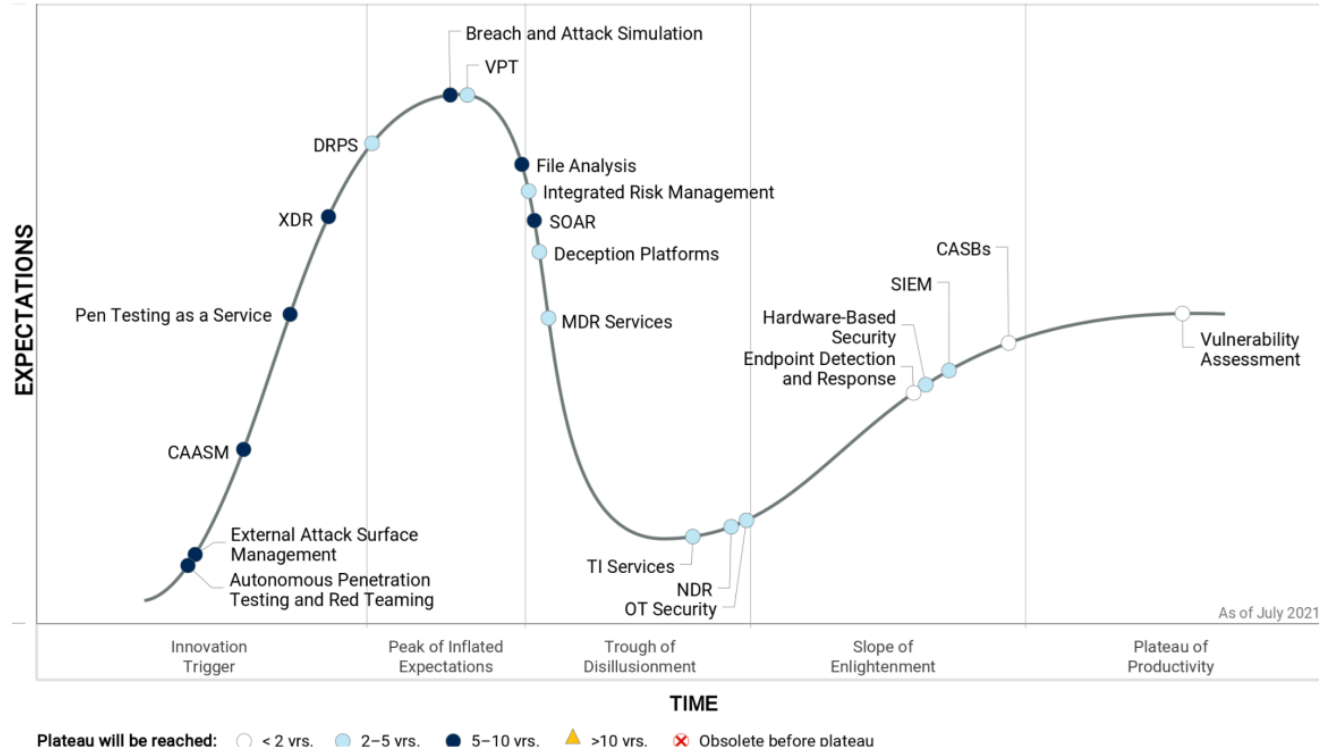
Relationship and data
correlations is at the
core

Security Intelligence


Finale



Master the technology of the future before



Source: Gartner (July 2021)



CAASM enables security teams to improve basic security hygiene by ensuring security controls, security posture and asset exposure are understood across the environment

Gartner 2021

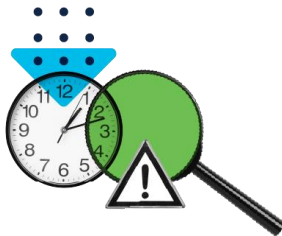
Simplified Cyber Asset Attack Surface Management



Cyber Assets Visibility

Natively detect Cyber Assets in the cloud based on multiple data types

Visualize and navigate complex relationships with ease



Attack Surface Management

Identify the blast radius – who and what else could be affected by this incident

Identify the root cause – how did the attacker access assets



Compliance and Security Reporting

Continuous audits with breadth and depth of standards out-of-box, fully customizable

Automated evidence collection

Insights and Analytics together



Cloud Security Posture
Management

Attack Surface
Management

Continuous Compliance

Relationship Mapping

Multi Cloud

Visibility

SaaS Delivered

Native Integration

Entity Detection



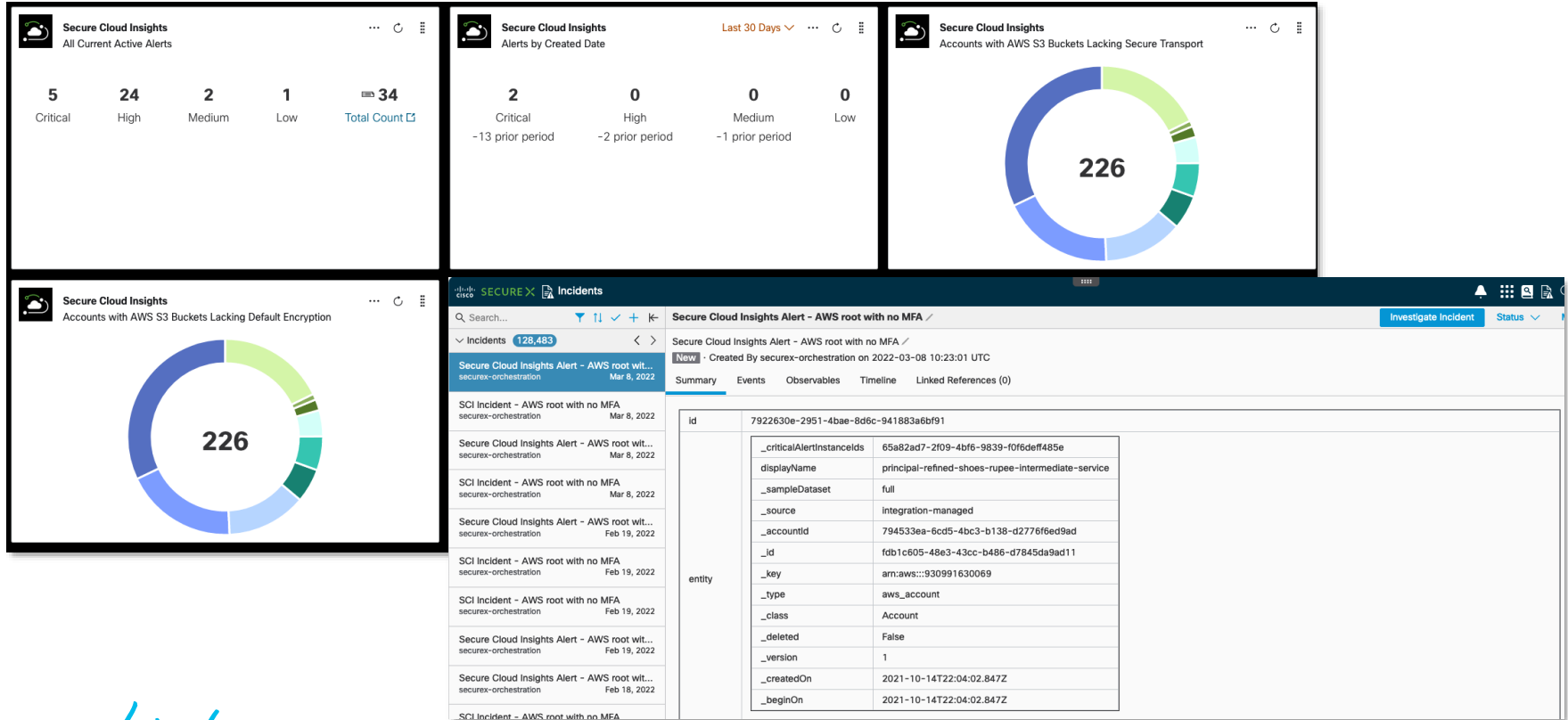
Behavioral threat
detection

Network segmentation

Threat Response

Event risk visibility

Secure Cloud Insights and SecureX Integration



References

- Data Modeling
- Relationship Model
- J1QL
- Troubleshooting

- <https://community.askj1.com/kb/articles/846-jupiterone-data-model>
- <https://community.askj1.com/kb/articles/1165-add-enriched-or-modified-properties>
- <https://community.askj1.com/kb/articles/847-jupiterone-entity-relationship-mappings>
- <https://community.askj1.com/kb/articles/980-introduction-to-jupiterone-query-language-j1ql>
- <https://support.jupiterone.io/hc/en-us/sections/360002319333-FAQs>
- <https://support.jupiterone.io/hc/en-us/articles/1500003848502-Troubleshooting-and-Reporting-Common-Data-Issues>

Video References

- J1QL Intro: <https://youtu.be/bcWjuMO-YcE>
- Insights: <https://youtu.be/98OI0se225s>
- Compliance: <https://youtu.be/v-Vj1tPLVmQ>
- J1QL Intro
<https://youtu.be/B0mHXa0SUXw>
- Policies & Procedures: <https://youtu.be/mpMOueb-ot10>
- Compliance
10/12: <https://www.youtube.com/watch?v=YSSBAwVaaTY>



*The Power to ask questions is the basis
of all Human Progress* by making everything visible

Hanna Jabbour

Indira Gandhi

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.



Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with
Cisco Learning Credits

(CLCs) are prepaid training
vouchers redeemed directly
with Cisco.



Learn

Cisco U.

IT learning hub that guides teams
and learners toward their goals

Cisco Digital Learning

Subscription-based product, technology,
and certification training

Cisco Modeling Labs

Network simulation platform for design,
testing, and troubleshooting

Cisco Learning Network

Resource community portal for
certifications and learning



Train

Cisco Training Bootcamps

Intensive team & individual automation
and technology training programs

Cisco Learning Partner Program

Authorized training partners supporting
Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product,
technology, and certification courses



Certify

Cisco Certifications and Specialist Certifications

Award-winning certification
program empowers students
and IT Professionals to advance
their technical careers

Cisco Guided Study Groups

180-day certification prep program
with learning and support

Cisco Continuing Education Program

Recertification training options
for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



The bridge to possible

Thank you

CISCO *Live!*



#CiscoLive