
cisco Live!
ALL IN

The bridge to possible

# Complete Visibility into Your Cyber Asset Universe

## With Cisco Secure Cloud Insights

Rajat Gulati
@rajat4gulati

BRKCLD-1341

# Cisco Webex App

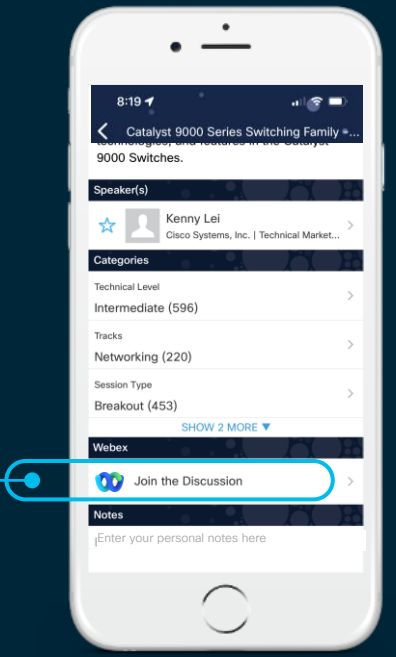
## Questions?

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/#BRKCLD-1341

# Agenda

- Challenges with modern architectures
- Introduction to Secure Cloud Insights
- How it works
- Short Demo
- Continue to engage

# Challenges with Modern Architectures

# Do you have all the answers?

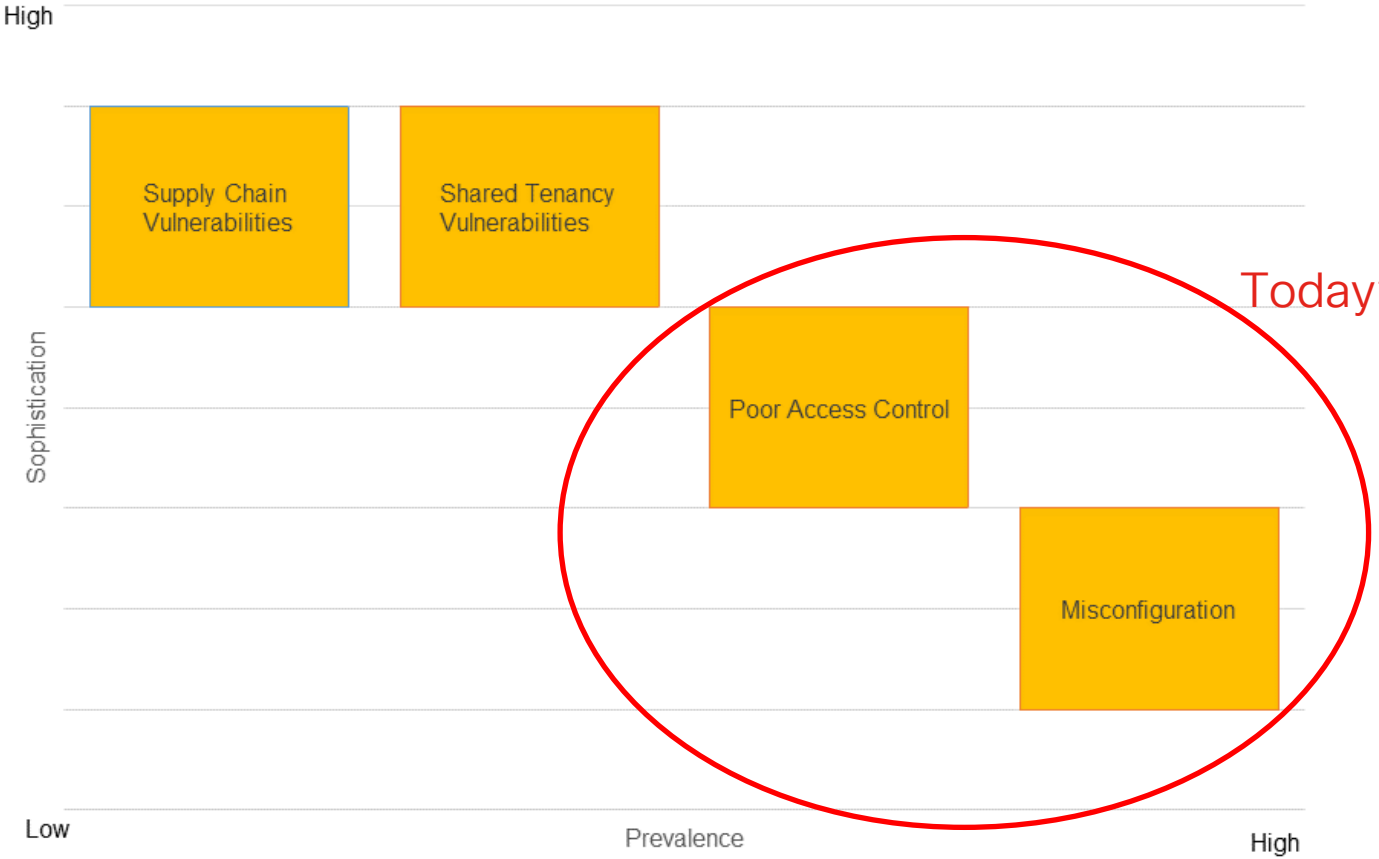
- **Normalized and unified view** of all your cyber assets?
- **Structural awareness** to augment the situational awareness of your detection and response tools?
- **Security posture** and **access entitlements** of and between your assets?
- **Real-time vulnerabilities** and **gaps** in your attack surface?
- Can you quickly understand the **full scope** and **impact** of an **attack**?
- Always on **compliance** against industry standards and security frameworks?
- Can you catch **misconfigurations**, the most common cause of breaches?

# Question 1:

In your experience, what is the #1 obstacle in the journey to the cloud?

1. No control on DevOps (software development, cloud architecture)
2. Risk of misconfigurations, and loss of visibility and context
3. Lack of insight into risks and vulnerabilities in the cloud environment
4. Regulatory obstacles, or inability to put data in the cloud
5. Other

# NSA: Misconfigurations & Access Control most Prevalent Cloud Vulnerabilities




https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF

# Introducing Secure Cloud Insights

# Cisco Secure Cloud Insights with JupiterOne

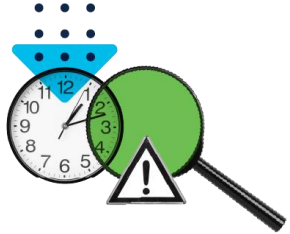
## Cyber Asset Attack Surface Management (CAASM)

### Automated Unified Asset Inventory

- Automatic discovery and normalization of cyber assets, objects, and artifacts
- Full context including configuration, access rules, and policies
- Agentless SaaS service with hybrid-cloud and premises coverage

### Continuous Compliance & Posture

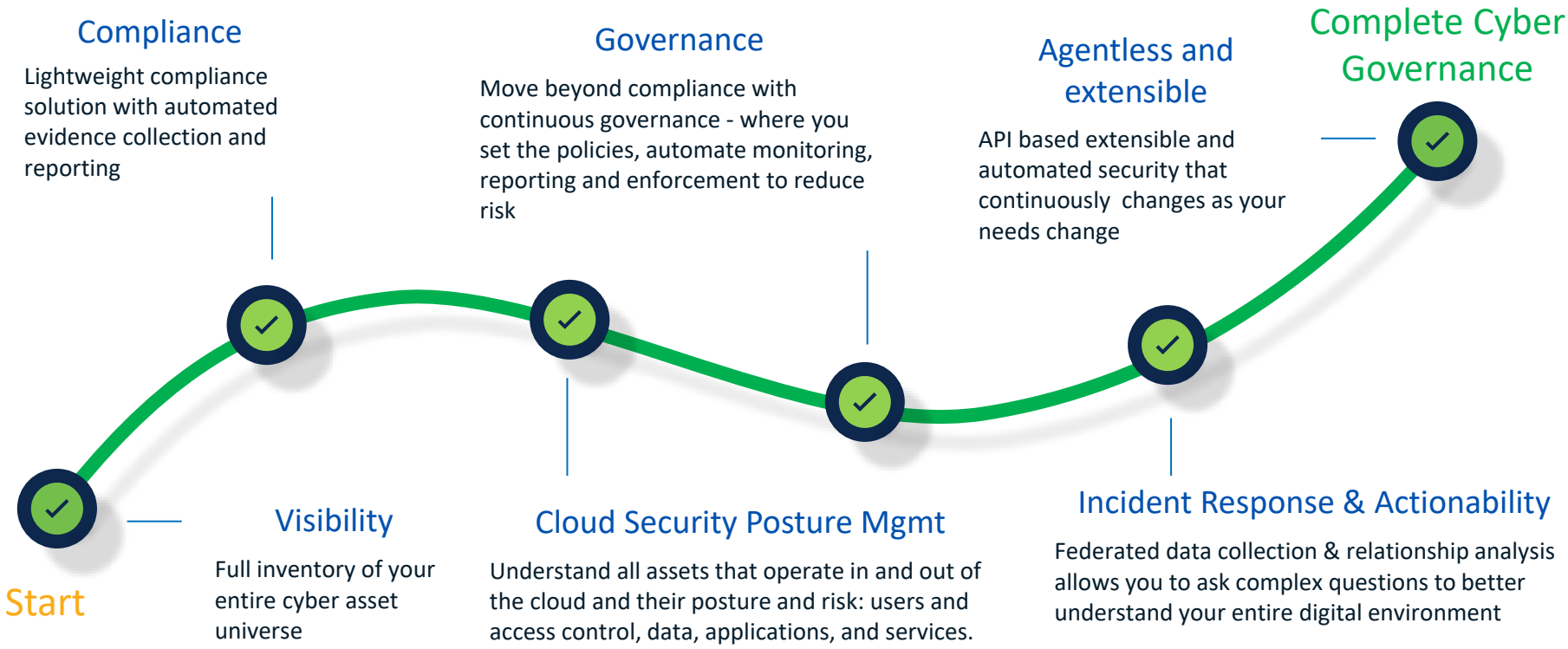
- Always-on audit against custom and regulatory benchmarks and standards
- Continuous checks allow constant awareness and alerting
- Evidence collection and tracking automated for audit purposes



### Attack Surface Visualization

- Leverages graph database technology to build intricate relationship maps
- Identify the blast radius – who and what else could be affected
- Identify the root cause – how did the attacker access this resource?

# The Journey to Complete Cyber Governance



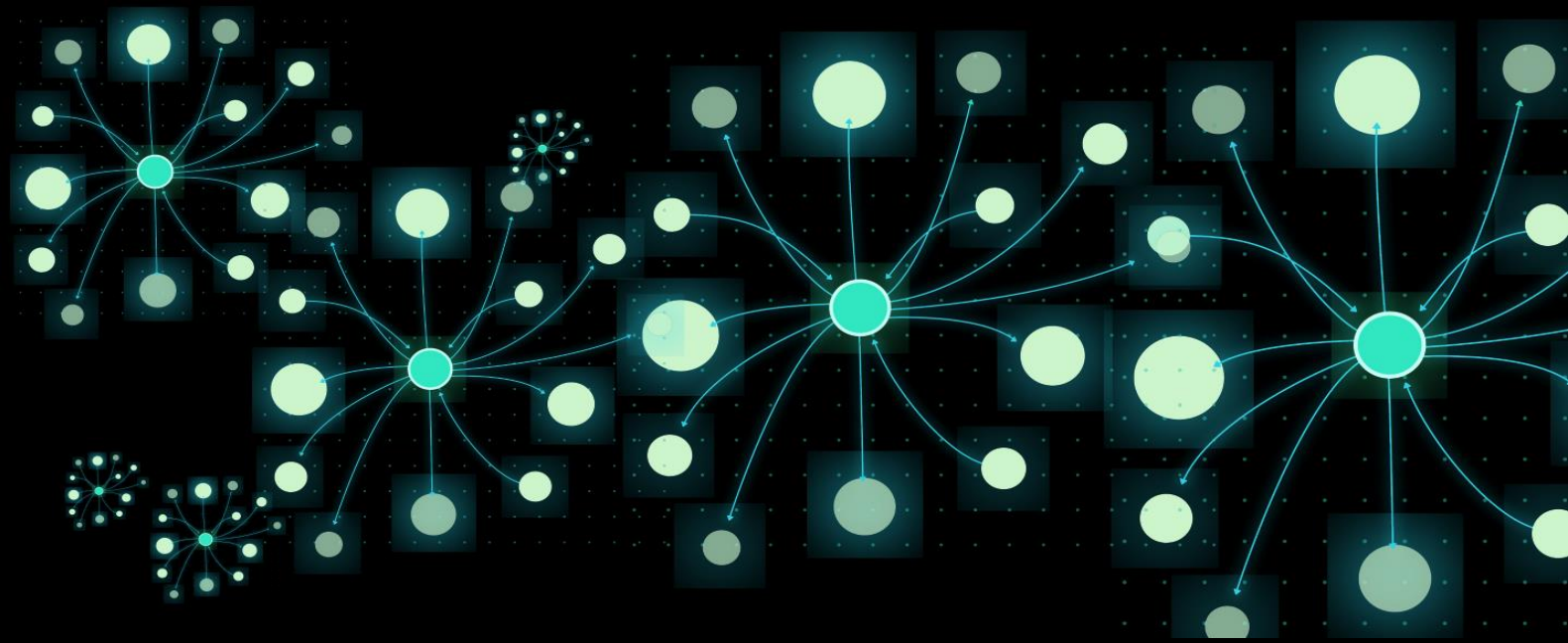
# Key use cases

Secure
Cloud Insights

| | |
|---|---|
| Hybrid cloud visibility | Natively integrate with multiple infrastructures in the public and private cloud as well as on-premises to get a unified view of the entire workload framework |
| Relationship mapping | Automatically map and visualize relationships between entities |
| Cloud Security Posture Management | Visualize and Monitor security posture of AWS, Azure and GCP environments, and easily track evidence to get complaint |
| Attack Surface Management | Contextualize every entity and track its interactions across multiple degrees of separation to achieve internal and external view of the real attack surface |
| Continuous compliance | Track compliance against 20+ pre-built compliance standards, as well as create custom standards to reduce rik |
| Fast-track investigations | Quickly get to incident root cause and blast radius to reduce time to investigate and respond |
| Cyber governance | Achieve cyber governance by remaining up to date with the risk of vulnerabilities and any security policy violations |

Defenders work with lists,

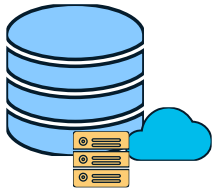
Attackers seek out connections



That is probably why attackers win so often

# How it Works

# Secure Cloud Insights High level Architecture

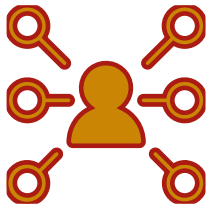


## Agentless Data Ingest

Seamlessly integrate with data sources in the cloud or on-prem natively through APIs

## Structural Awareness

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

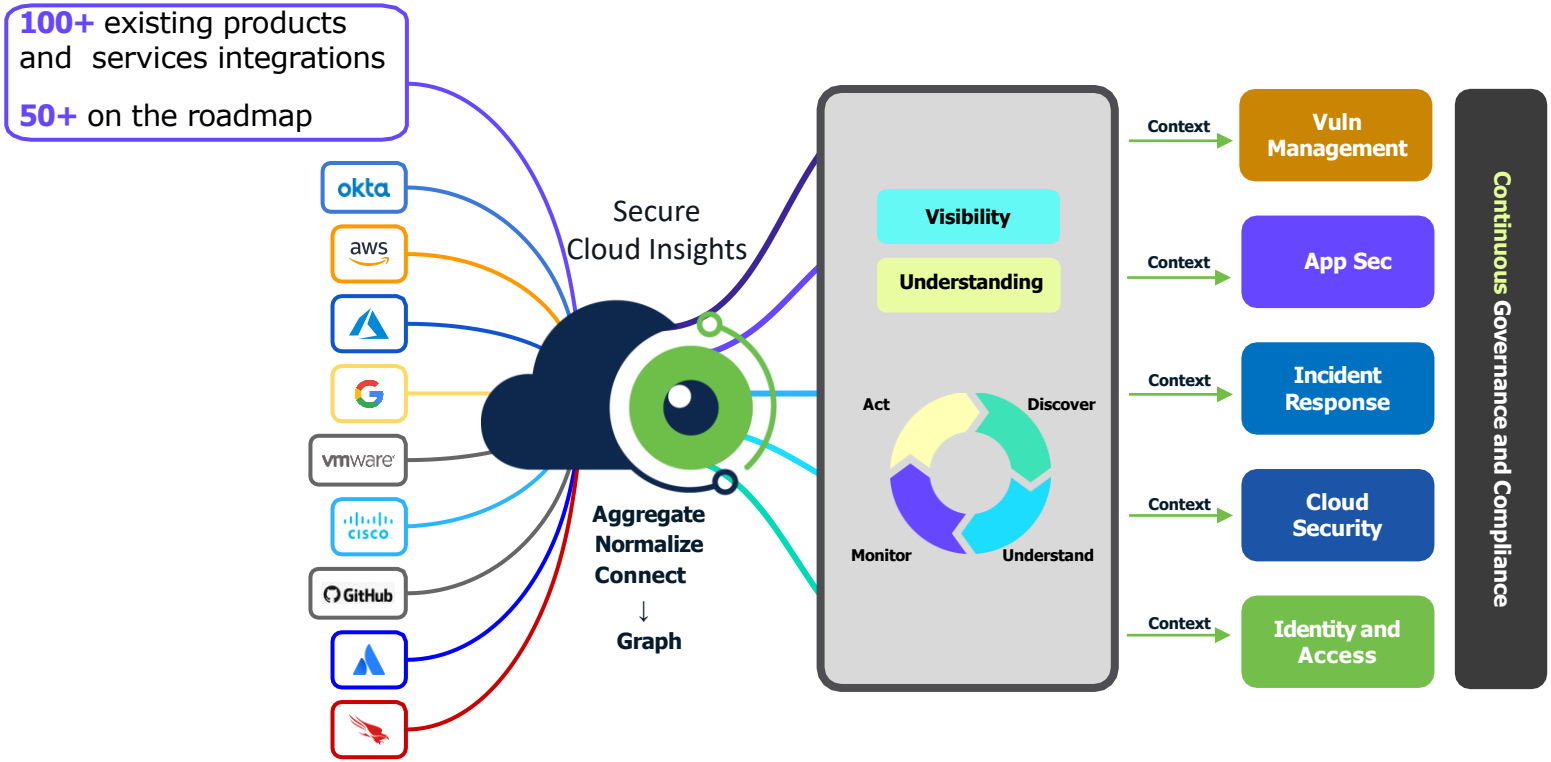


Continuous Compliance Checks
Attack Surface Visualization

## Investigate and Query

Natural language driven query engine with a simple, powerful query syntax

# Ingest, Normalize, Graph, Contextualize → Insights



# Solve complex problems with simple queries

## Continuous compliance monitoring

600+ pre-defined queries, and custom queries available

Convert any query to an alert, or add it to a compliance framework

- Are any cloud storage buckets unencrypted?
- Which storage does not have logging enabled?
- What are the production instances?
- Are internet facing compute instances accessing non-public storage?
- Are there cross-account IAM trust relationships to external / vendor accounts?
- Which PRs / developer introduced new vulnerability findings this past week?

# Pre-defined Integrations

**Cloud Infr**

- Amazon AWS
- Microsoft Azure
- Google Cloud
- Hiroku
- Snowflake
- Alibaba Cloud

**Dev & Code**

- BitBucket
- GitHub
- GitLab
- NPM
- JFrog Artifactory

**Vulnerability Management**

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

**NEW!**

- Aqua Sec
- Addigy
- Mimecast
- Rumble
- Zoom

**People & Access**

- Google G Suite
- Cisco Duo
- Microsoft AD
- Okta
- OneLogin
- JumpCloud

**Endpoint**

- Cisco Sec EP
- Carbon Black
- Crowdstrike
- Malwarebytes
- Jamf
- SentinelOne
- Trend Micro
- AirWatch
- Wazuh

**Network**

- Cisco Meraki
- DigiCert
- Nmap
- Whois
- Shodan

**Workflows**

- Jira
- PagerDuty
- ServiceNow

**Others**

- KnowBe4
- BambooHR
- GoDaddy
- DataDog
- Splunk

**Custom**

- GraphQL + REST API
- NodeJS SDK
- Custom

https://community.askj1.com/kb/categories/8-apis-and-integrations

# Question 2:

In addition to AWS, Azure, and GCP, which Clouds would you like to see supported by Cloud Native security Tools?

1. SAP Cloud
2. Oracle Cloud
3. Alibaba Cloud
4. IBM Cloud
5. Other


## Used by Cisco Security & Trust Org to solve key challenges in cloud security posture and attack surface management

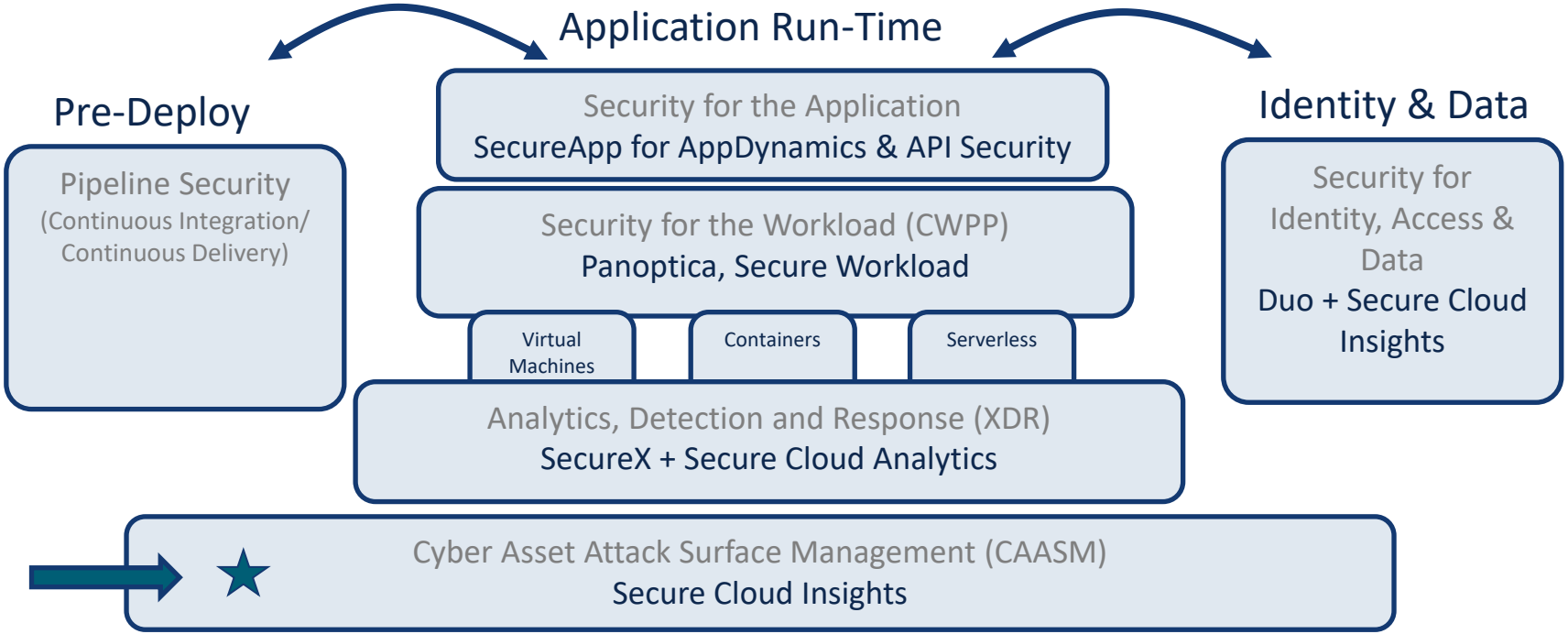
The Deployment:

- ~3,400 AWS accounts
- ~1,500 Google Cloud accounts
- ~ 800 Azure Accounts
- Automatic inclusion for all Cisco accounts in public clouds

Use Cases:

- Security & Policy monitoring
- Easily integrates with existing workflow and reporting needs
- Employee access controls

# Cisco's Cloud Native Security Capabilities



# Demo

# Continue to engage

Learn More at cisco.com/go/secure-cloud-insights

Videos: YouTube Playlist

Partner/ Seller Resources: Cisco SalesConnect Site

Free Trial: https://info.securecloudinsights.cisco.com/

Tech Session: BRKSEC-2346 : Hanna Jabbour

Reception

# 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

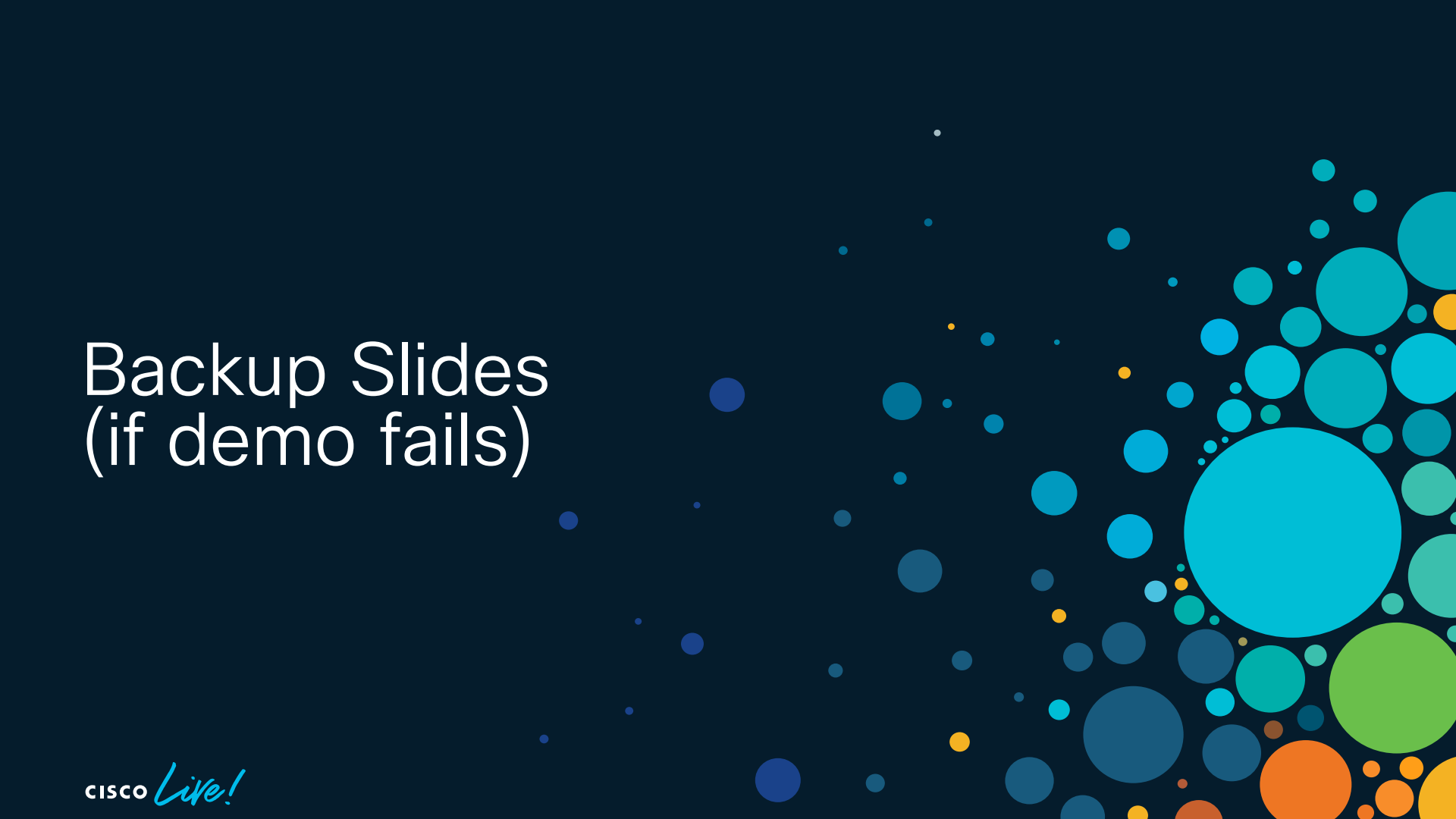
- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

cisco Live!

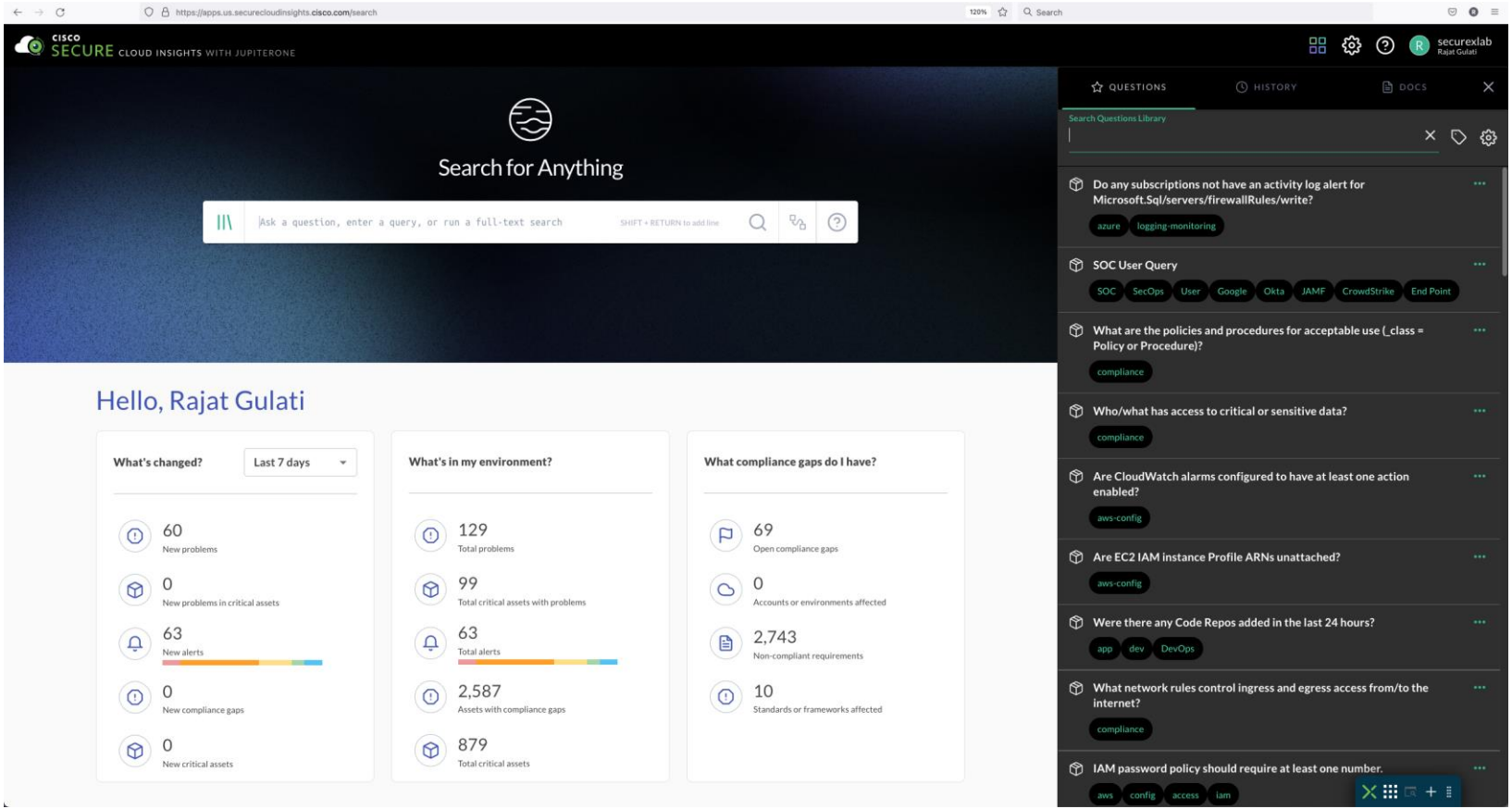

# Thank you


cisco Live!
ALL IN

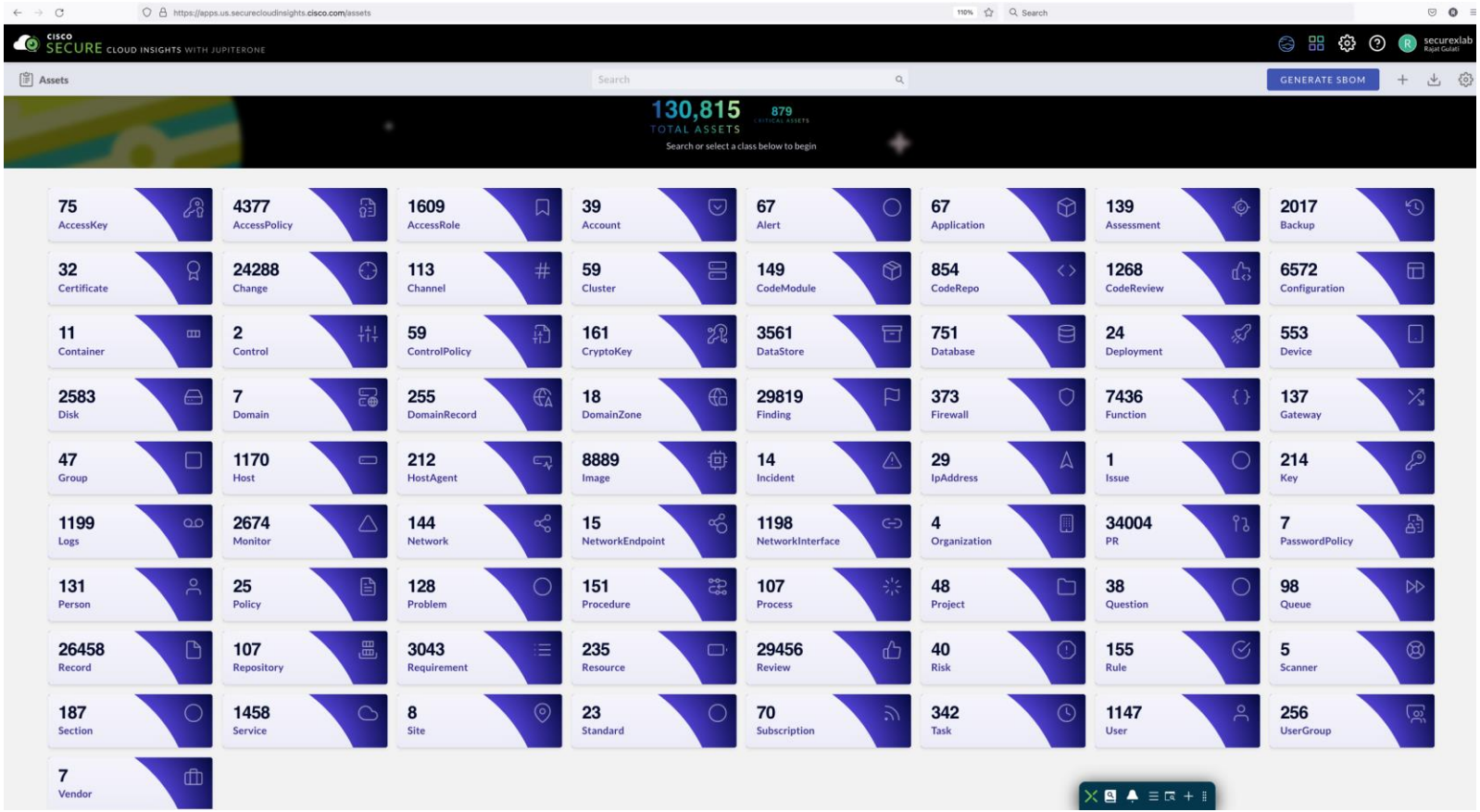
# Backup Slides (if demo fails)



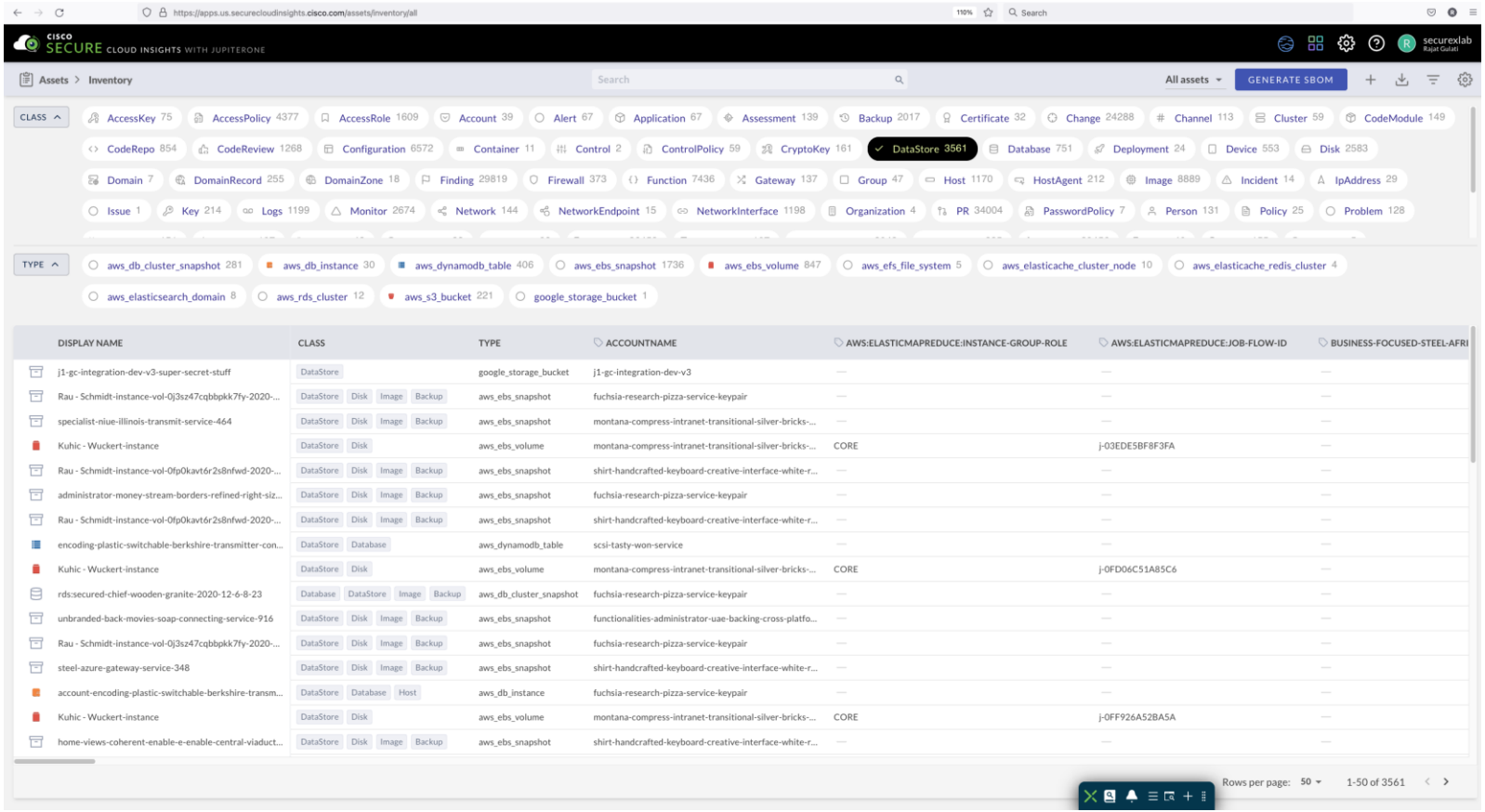
# Search Page and Statistics



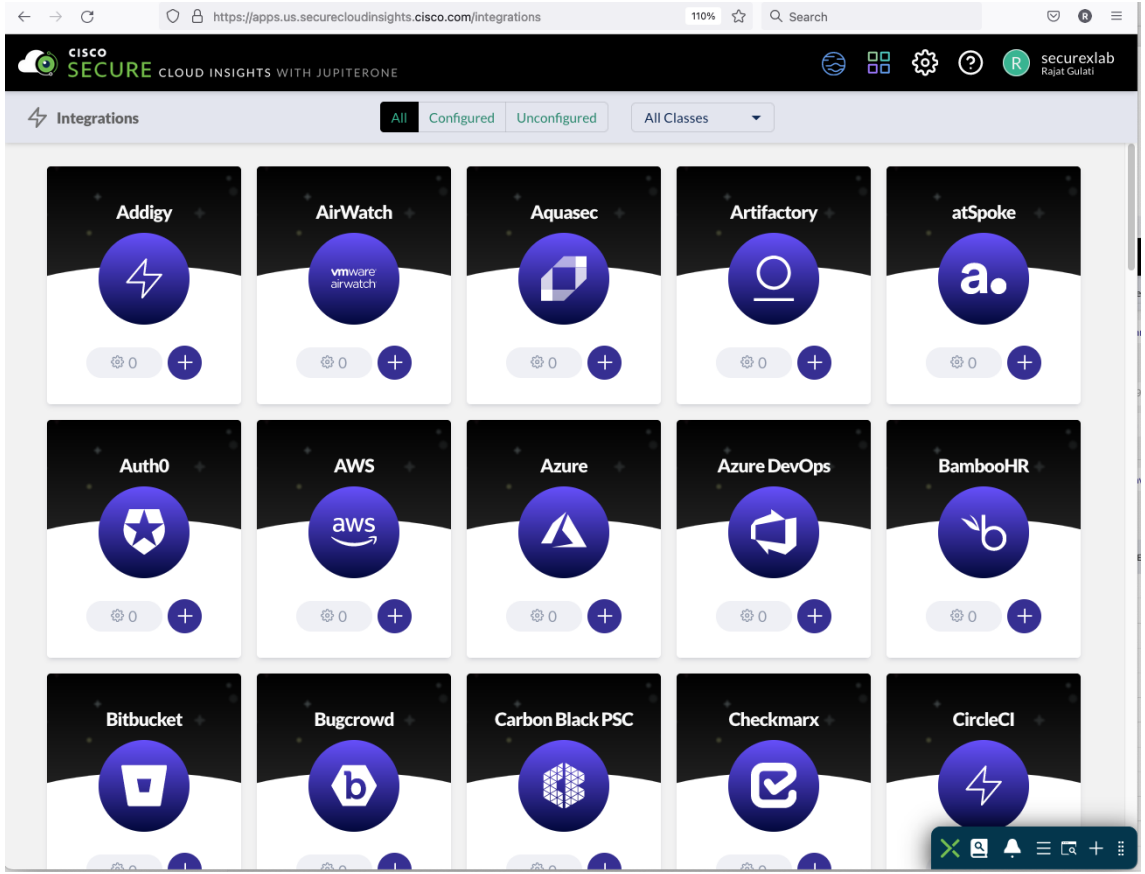
# Asset Inventory



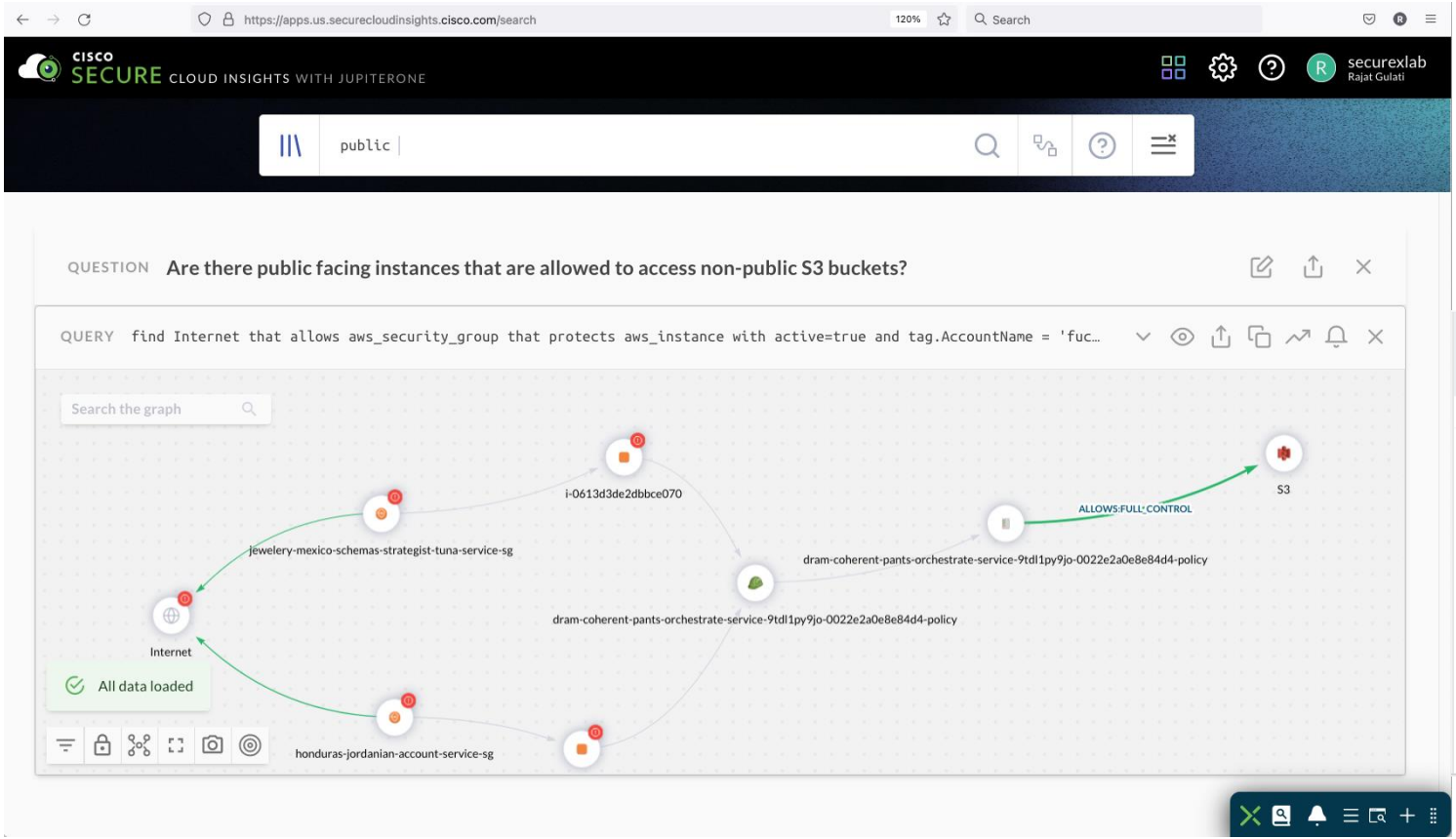
# Asset Lists


https://apps.us.securecloudinsights.cisco.com/assets/inventory/all
cisco SECURE CLOUD INSIGHTS WITH JUPITERONE
securexlab
Rajat Gulati
Assets > Inventory
Search
All assets
GENERATE SBOM
CLASS
AccessKey 75
AccessPolicy 4377
AccessRole 1609
Account 39
Alert 67
Application 67
Assessment 139
Backup 2017
Certificate 32
Change 24288
Channel 113
Cluster 59
CodeModule 149
CodeRepo 854
CodeReview 1268
Configuration 6572
Container 11
Control 2
ControlPolicy 59
CryptoKey 161
DataStore 3561
Database 751
Deployment 24
Device 553
Disk 2583
Domain 7
DomainRecord 255
DomainZone 18
Finding 29819
Firewall 373
Function 7436
Gateway 137
Group 47
Host 1170
HostAgent 212
Image 8889
Incident 14
IpAddress 29
Issue 1
Key 214
Logs 1199
Monitor 2674
Network 144
NetworkEndpoint 15
NetworkInterface 1198
Organization 4
PR 34004
PasswordPolicy 7
Person 131
Policy 25
Problem 128
TYPE
aws_db_cluster_snapshot 281
aws_db_instance 30
aws_dynamodb_table 406
aws_ebs_snapshot 1736
aws_ebs_volume 847
aws_efs_file_system 5
aws_elasticache_cluster_node 10
aws_elasticache_redis_cluster 4
aws_elasticsearch_domain 8
aws_rds_cluster 12
aws_s3_bucket 221
google_storage_bucket 1
DISPLAY NAME
CLASS
TYPE
ACCOUNTNAME
AWS:ELASTICMAPREDUCE:INSTANCE-GROUP-ROLE
AWS:ELASTICMAPREDUCE:JOB-FLOW-ID
BUSINESS-FOCUSED-STEEL-AFRI
j1-gc-integration-dev-v3-super-secret-stuff
DataStore
google_storage_bucket
j1-gc-integration-dev-v3
Rau - Schmidt-instance-vol-0j3sz47cqbbpkk7fy-2020-...
DataStore Disk Image Backup
aws_ebs_snapshot
fuchsia-research-pizza-service-keypair
specialist-niue-illinois-transmit-service-464
DataStore Disk Image Backup
aws_ebs_snapshot
montana-compress-intranet-transitional-silver-bricks-...
Kuhic - Wuckert-instance
DataStore Disk
aws_ebs_volume
montana-compress-intranet-transitional-silver-bricks-...
CORE
j-03EDE5BF8F3FA
Rau - Schmidt-instance-vol-0fp0kavt6r2s8nfwd-2020-...
DataStore Disk Image Backup
aws_ebs_snapshot
shirt-handcrafted-keyboard-creative-interface-white-r...
administrator-money-stream-borders-refined-right-siz...
DataStore Disk Image Backup
aws_ebs_snapshot
fuchsia-research-pizza-service-keypair
Rau - Schmidt-instance-vol-0fp0kavt6r2s8nfwd-2020-...
DataStore Disk Image Backup
aws_ebs_snapshot
shirt-handcrafted-keyboard-creative-interface-white-r...
encoding-plastic-switchable-berkshire-transmitter-con...
DataStore Database
aws_dynamodb_table
scsi-tasty-won-service
Kuhic - Wuckert-instance
DataStore Disk
aws_ebs_volume
montana-compress-intranet-transitional-silver-bricks-...
CORE
j-0FD06C51A85C6
rds:secured-chief-wooden-granite-2020-12-6-8-23
Database DataStore Image Backup
aws_db_cluster_snapshot
fuchsia-research-pizza-service-keypair
unbranded-back-movies-soap-connecting-service-916
DataStore Disk Image Backup
aws_ebs_snapshot
functionalities-administrator-uae-backing-cross-platfo...
Rau - Schmidt-instance-vol-0j3sz47cqbbpkk7fy-2020-...
DataStore Disk Image Backup
aws_ebs_snapshot
fuchsia-research-pizza-service-keypair
steel-azure-gateway-service-348
DataStore Disk Image Backup
aws_ebs_snapshot
shirt-handcrafted-keyboard-creative-interface-white-r...
account-encoding-plastic-switchable-berkshire-transm...
DataStore Database Host
aws_db_instance
fuchsia-research-pizza-service-keypair
Kuhic - Wuckert-instance
DataStore Disk
aws_ebs_volume
montana-compress-intranet-transitional-silver-bricks-...
CORE
j-0FF926A52BA5A
home-views-coherent-enable-e-enable-central-viaduct...
DataStore Disk Image Backup
aws_ebs_snapshot
shirt-handcrafted-keyboard-creative-interface-white-r...
Rows per page: 50
1-50 of 3561

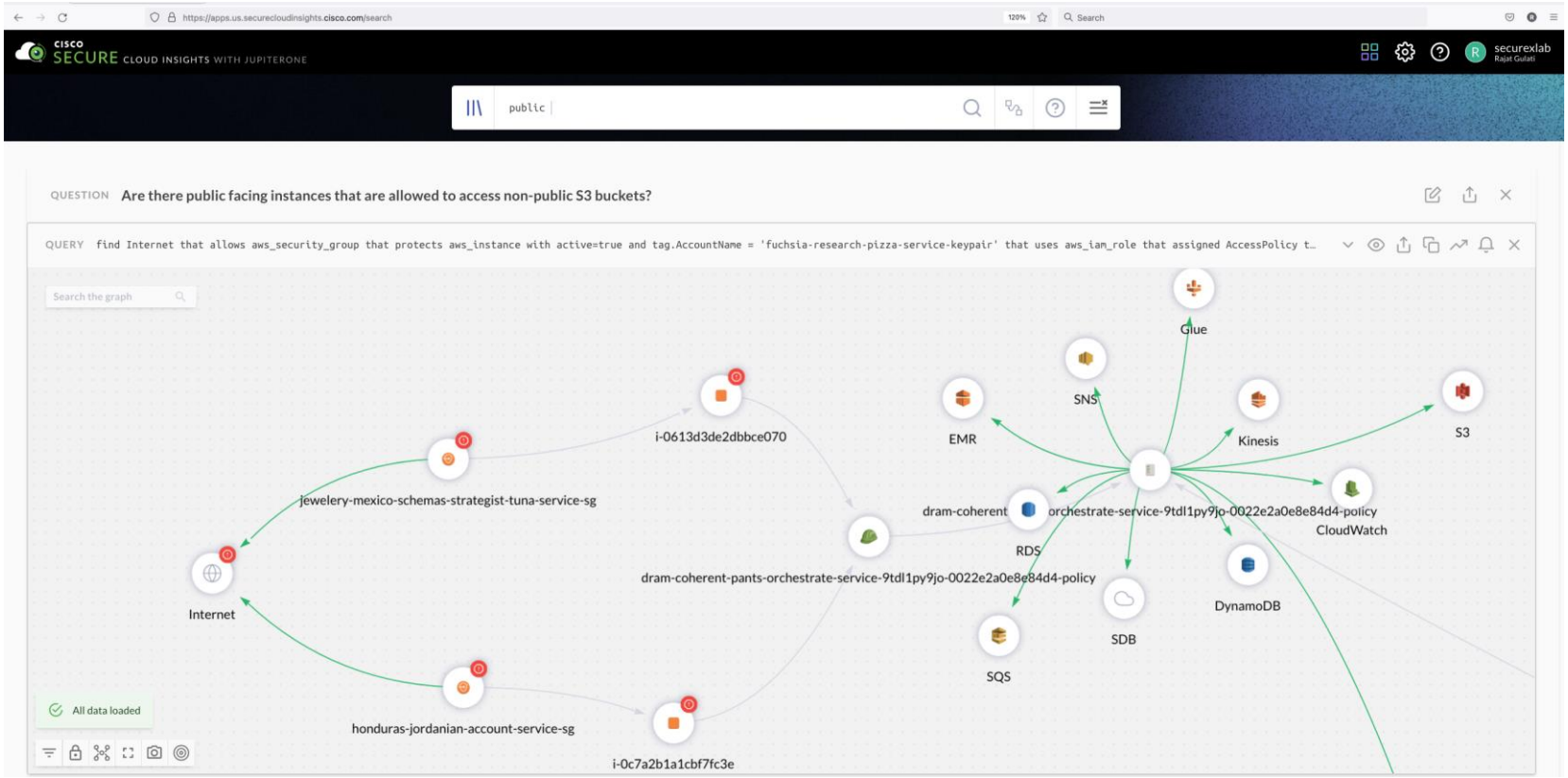
# Integrations Page



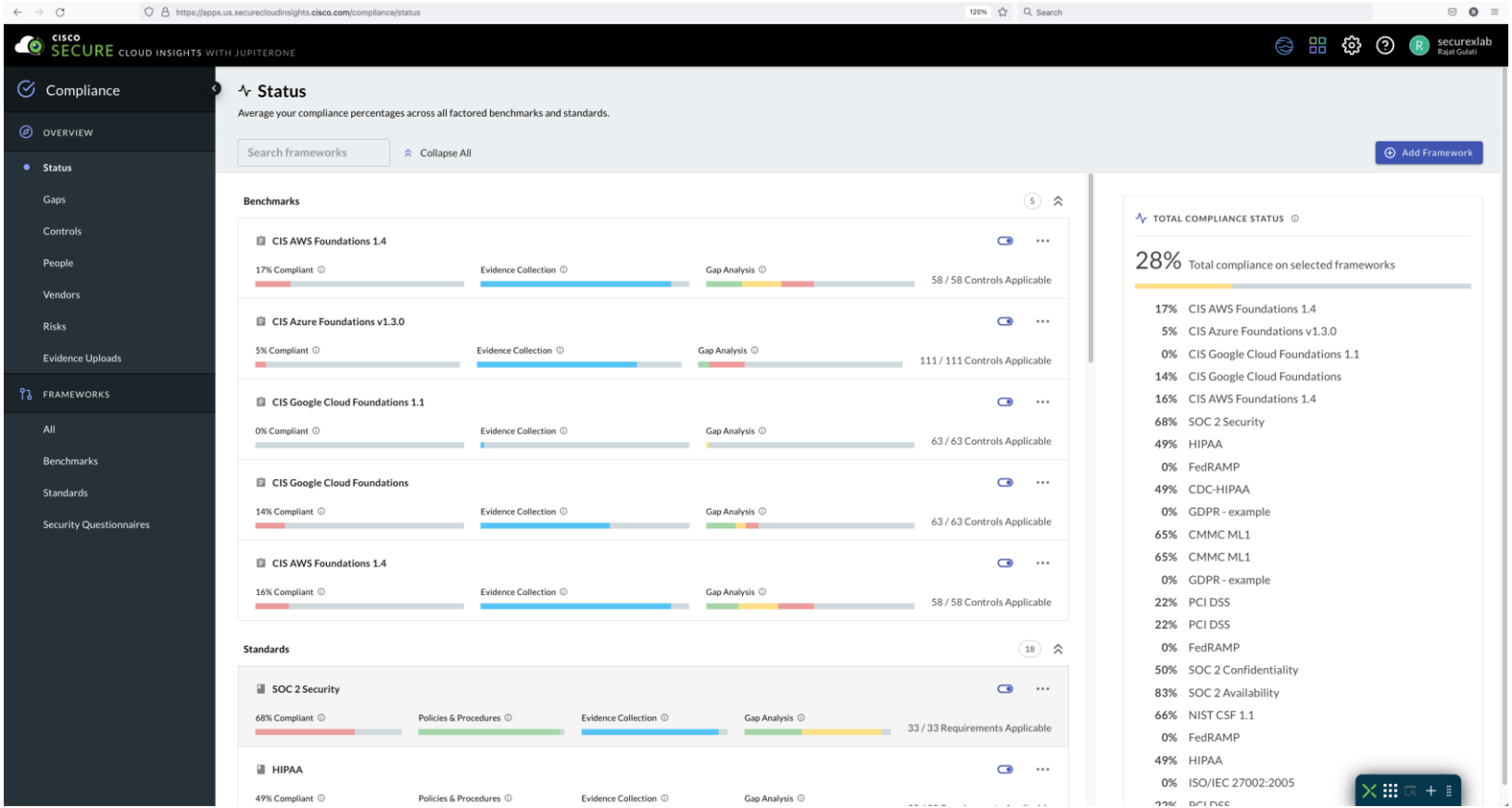
# Relationship Maps



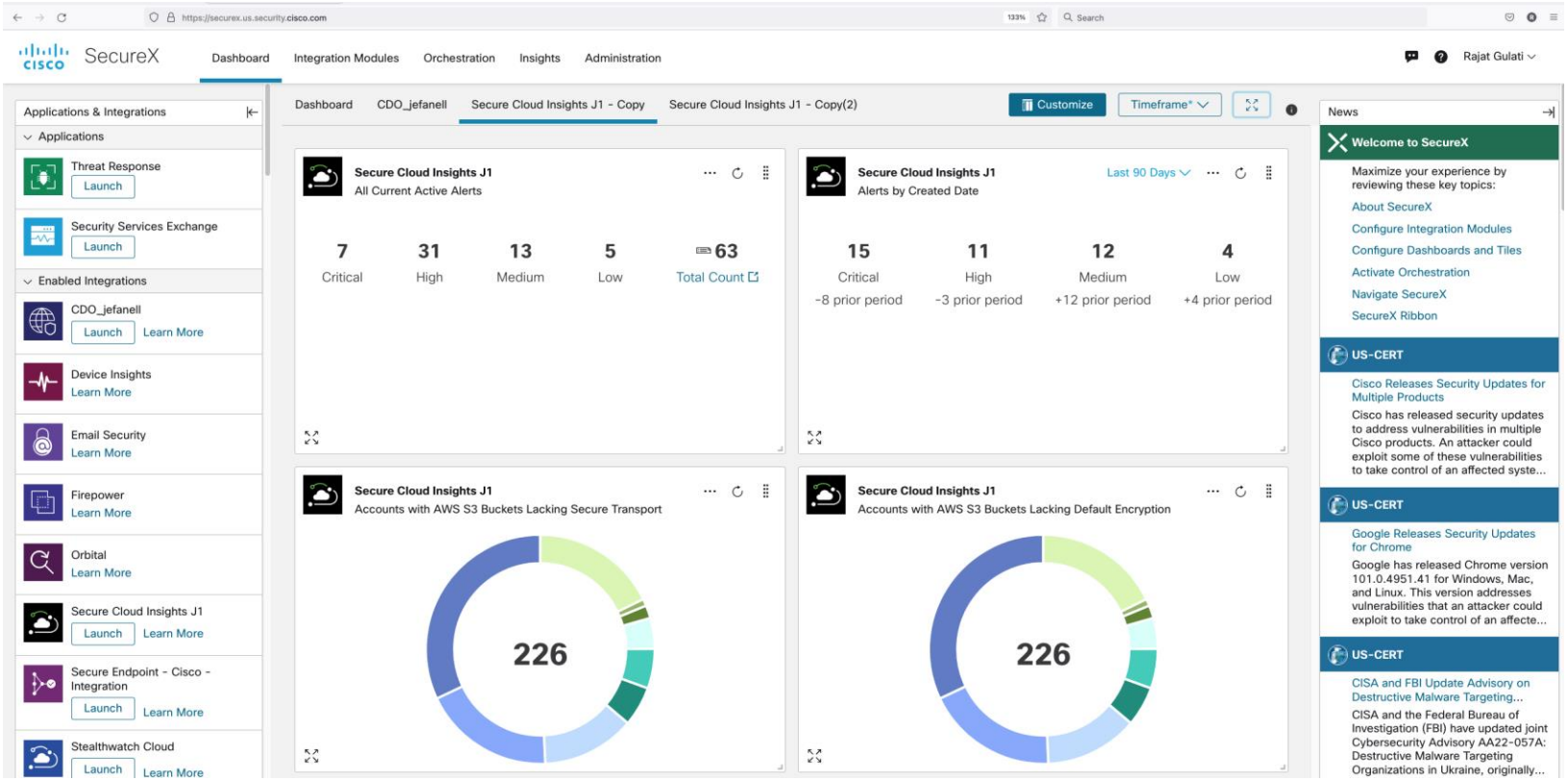
# Dynamic build-out of graph



# Compliance Status Page



# SecureX Integration via Tiles, Ribbon and Posts




cisco Live!
ALL IN