# Cisco Attack Surface Management with JupiterOne

*(formerly Cloud Insights)*

Cisco Partner

https://cs.co/1page

**Cisco Attack Surface Management (CASM)**: A Cyber platform to identify, map, analyze, and secure your cyber assets and attack surface. Gain full visibility beyond Cloud Security Posture Management (CSPM) into managed cloud environments to uncover threats, close compliance gaps, and prioritize risk.

## Benefits:

- **Complete Cloud Visibility:** Gain complete visibility and understanding of your cloud security posture across multiple clouds.
- **Continuous Cloud Security:** Continuously monitor cloud environments to detect policy violations, compliance requirements or misconfigurations.
- **End-to-End Attack Surface Insights:** Understand your entire attack surface by mapping relationships between assets.
- **Fast Investigation & Response:** Quickly investigate and remediate impacted assets by pinpointing your blast radius.

## Use Cases:

- **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 & 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 risk.
- **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.

## High Level Architecture:

- **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.
- **Alert and Respond:** Shares alert findings to ticketing correlating systems upon detection.

## Questions / Conversation Starters:

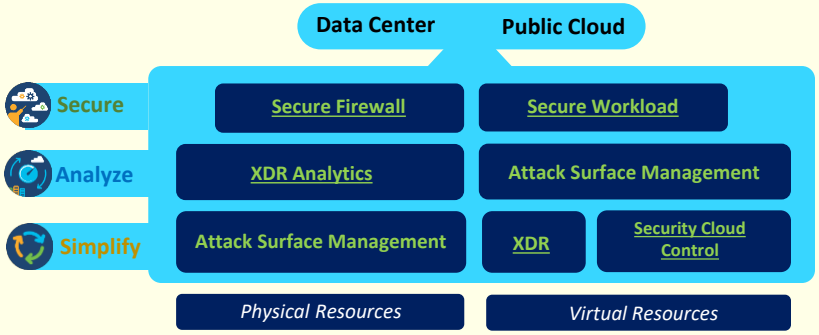
- Do you have a single and unified view of your entire cloud asset universe?
- What and where are your most critical cyber assets this moment (People, Data, Hosts, Networks, Infrastructure, Applications)?
- What is the security posture, attack surface and inter-relationships of your assets?
- What are the real-time vulnerabilities and gaps in your security controls?
- Can you quickly understand the full scope and impact of an attack or breach of your cloud assets?
- Can you assess just-in-time compliance with security standards and best practices?

## Cloud Security Process:

**Secure:**
Securing network, workload, and application environments with multi-use firewall and workload protection.

**Analyze:**
Detect indicators of compromise or unusual behaviors including insider threat activity, malware, and policy violations.

**Simplify:**
Enabling cloud configuration confidence Deploy automation to scale.




## Resources:

- At-a-Glance
- Ordering Guide
- CASM FAQ
- JupiterOne Updates
- System Status
- YouTube Playlist
- Public page

Example SKU: ***SCA-INS***

WO-03232025