Cisco Cloud Application Security

(Panoptica)

Cisco Partner

https://cs.co/1page

Cloud Application Security is a Cloud Native Application Protection Platform (CNAPP) that provides contextualized cloud security to identify, prioritize, and remediate security risks, vulnerabilities, and misconfigurations in complex Container, Kubernetes and Service Mesh for multi-cloud environments.

Benefits:

Scalable cloud-native solution: Cloud Application Security takes an agentless approach to securing all cloud-native architectures and it scales with your deployments. Does not require DaemonSet.

Broad Security Coverage: Cloud Application Security provides security coverage across containers, APIs, and serverless functions, generating actionable insights for security teams and developers throughout the application lifecycle.

Frictionless developer focus: Cloud Application Security promotes frictionless collaboration among DevOps, advancing them to DevSecOps at scale by shifting security to the left with declarative and automated policies using GitOps.

Seamless security in advance environments: Cloud Application Security provides seamless security coverage in new and emerging technologically complex cloud-native environments, including service meshes and Kafka / Rabbit MQ.

Supply chain security and code integrity: Cloud Application Security helps you address software supply chain requirements with SBOM generation and code signing options, enabling compliance with federal mandates.

Deep API risk assessment: Cloud Application Security analyzes risks associated with internal and external APIs and assigns risk scores. This enables you to identify and prevent breaches to your most critical assets.

Compliance and governance: Cloud Application Security's MITRE ATT&CK Framework view enables compliance from a security perspective. Kubernetes and Docker CIS risk assessment meet auditor requirements.

Conversation Starters:

Have you automated security within existing cloud native development processes?

Do you have visibility of all your images and how they interact with other services?

Are your images immutable throughout the application lifecycle (i.e., no drift)?

Do you have proper RBAC and pod security measures in place?

Works across Kubernetes platforms and in any Cloud:

AWS · Azure · GCP · Oracle OCI · RedHat OpenShift · Rancher RKE · Github · Gitlab · Bitbucket

Use Cases:

Cloud Workload Protection: Containers, Serverless, APIs

Visibility: Inventory, App to App .Communication, L7 Encryption

Compliance: Supply Chain, Docker CIS, MITRE ATT&CK

FAQs:

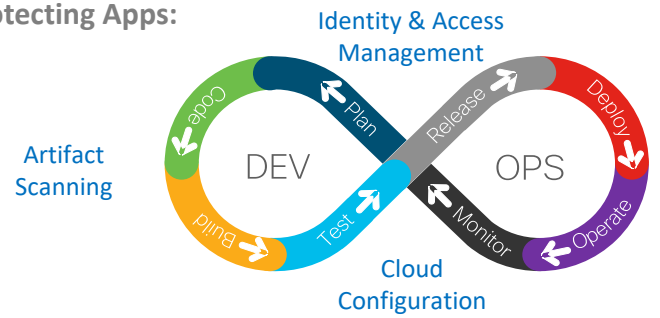
Q: What Kubernetes platforms does Cloud Application Security support?
A: All major Kubernetes flavors whether on-prem (OpenShift) or in the cloud (EKS, AKS, GKE, and OKE)

Q: What is the minimum version of Kubernetes supported?
A: Cloud Application Security supports Kubernetes 1.22.x and newer.

Q: Does Cloud Application Security require agents?
A: No, Cloud Application Security is an agentless solution that does not inject agents into the container nor require agents running on each node.

Q: Does Cloud Application Security support air-gapped operations?
A: No, currently, Cloud App Security SaaS is a requirement for operations.

Protecting Apps:



Resources:

SalesConnect
Security Suites
Ordering Guide

At-a-Glance
Best Practices
FAQs

Blog:
Attack Path Analysis
Cloud Native Security
API Security

Docs
Demo
Public page

Example SKU: **ETI-SAESSCONT-SUB**