Prioritize and remediate cloud application risks with precision

The cloud offers teams agility, autonomy, and speed to innovate more quickly; however, the dynamic nature of the cloud makes it challenging to secure. Additionally, teams often leverage open-source code and third-party APIs to speed application development time. This introduces risks that must be monitored and contained.

Cisco Cloud Application Security provides visibility into applications and the underlying infrastructure to detect and prevent a wide range of security threats plus meet compliance. After deploying Cloud Application Security, our customers report less risk and cost, plus improved productivity.

Read on to understand how Cloud Application Security secures the software development lifecycle.

### Code and Build Security
- Identify, prioritize and remediate risks like vulnerabilities and IaC misconfigurations.

### Cloud Security Posture Management
- Inventory and group assets plus automate compliance reporting.

### Cloud Workload Protection
- Continuously monitor and assess risk for all workloads including virtual machines, containers, Kubernetes and serverless.

### API Security
- Automatically inventory and analyze risks associated with APIs – internal, external and third party.

### Attack Path Analysis
- Prioritize and fix exploitable attack vectors with comprehensive attack path analysis.

### Development
- **Artifact Scanning**
  - Software Composition Analysis
  - API Security analysis
- **Software Exposure Scanning**
  - Common Vulnerabilities
  - Secrets
  - Sensitive Data
  - Malware
- **Infrastructure as Code Scanning**
  - Kubernetes Security Posture Management
  - Cloud Security Posture Management
  - Cloud Infrastructure Entitlements Management

### Runtime
- **Runtime Protection**
  - Cloud Workload Protection
  - API protection
  - Serverless Function Protection
- **Runtime Exposure Scanning**
  - Common Vulnerabilities
  - Secrets
  - Sensitive Data
  - Malware

### Operate

### Deployment
- **Test and Release**
- **Cloud Configuration Hardening**
  - Kubernetes Security Posture Management
  - Cloud Security Posture Management
  - Cloud Infrastructure Entitlements Management

### Benefits of a comprehensive solution

- 85% of organizations said a CNAPP helps drive efficiency in connecting application security processes to security posture management.
- 87% of organizations said a CNAPP will give them a consolidated approach for more efficient cloud security risk mitigation.

### Create a plan today

- 60% of network security teams have implemented a cloud-native approach to security, up from 25% in 2022.
- 80% of cloud-native teams have implemented cloud-native security measures to address 3,000 threats.
- 75% of cloud-native teams are 100% of cloud-native environments, up from 55% in 2022.


GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.