Cisco Cloud Application Security

Increased visibility and risk mitigation across cloud applications from development to runtime

The cloud offers Application Development and DevOps teams agility, autonomy, and scale to innovate more quickly; however, the dynamic nature of the cloud makes it challenging for security teams to keep pace. 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 cloud applications and the underlying infrastructure to detect and prevent a wide range of security threats plus meet compliance from development to runtime for multicloud environments. Specifically, it helps organizations:

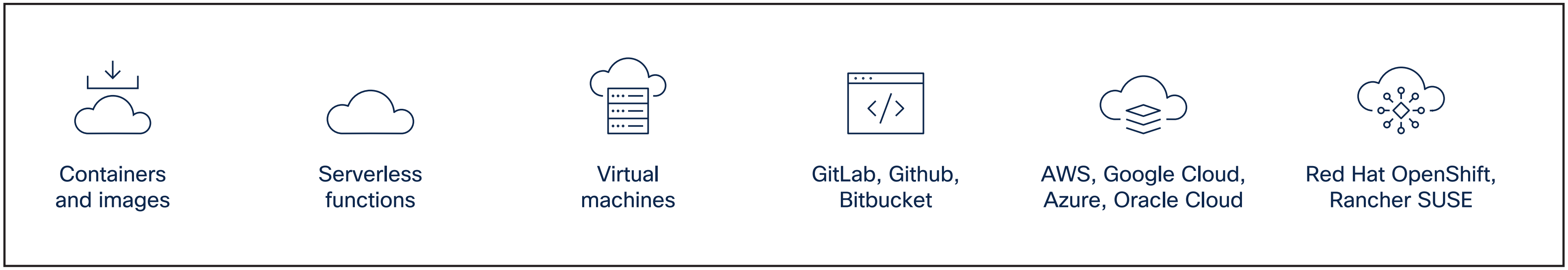
- **Monitor:** Cloud Security Posture Management (CSPM) measures compliance; Infrastructure as Code (IaC) scanning detects infrastructure misconfigurations; API security assesses risk associated with third-party APIs; and supply chain management identifies vulnerability risks.
- **Prioritize:** With the attack path analysis and visualizations, view risks from the POV of a bad actor so teams can focus on the most critical security findings, while reducing alerts.
- **Remediate:** View dynamically generated guidance, which includes step-by-step instructions and specific command lines to resolve cloud risks quickly and efficiently.

Benefits

Cisco Cloud Application Security enables you to:

- Improve visibility and protection across the cloud application lifecycle from development to runtime
- Effectively prioritize vulnerabilities and risks based on attack path analysis
- Continuously monitor cloud security posture to ensure compliance with the latest regulations and best practices
- Reduce Mean Time To Respond (MTTR) to cloud incidents with greater insights and root cause analysis
- Eliminate point tools by using a comprehensive cloud applications security service

> "Existing solutions couldn't address our transition to modern micro-services applications. Working with Cisco, we were able to insert security into our complex environment seamlessly for secure application deployment and connectivity."
>
> - Maritime Transportation Company



Containers and images

Serverless functions

Virtual machines

GitLab, Github, Bitbucket

AWS, Google Cloud, Azure, Oracle Cloud

Red Hat OpenShift, Rancher SUSE

Figure 1. Cisco Cloud Application Security provides coverage for application artifacts, CICD tools, cloud and Kubernetes environments

Cisco Cloud Application Security key differentiators

Advanced Cloud Native Application Security

Cisco Cloud Application Security unifies Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) capabilities into a unified Cloud Native Application Protection Platform (CNAPP) to centralize security management, provide end-to-end insights, and save the costs of multiple tools.

Comprehensive security coverage

Whether you build and operate your application in one or more clouds, Cisco Cloud Application Security provides comprehensive protection with coverage for the entire application lifecycle and all cloud assets, including Kubernetes clusters.

Contextual risk prioritization

Cisco Cloud Application Security adopts the attacker's point of view to identify exploitable paths that enable lateral movement and data exfiltration within your environment. These attack paths are prioritized by severity and vectors to clearly show the biggest threats to your cloud apps, without overwhelming your operators in alerts.

Multicloud compliance

Cisco Cloud Application Security enables teams to meet their cloud audits and business goals by continuously monitoring for compliance with regulations and best practices.

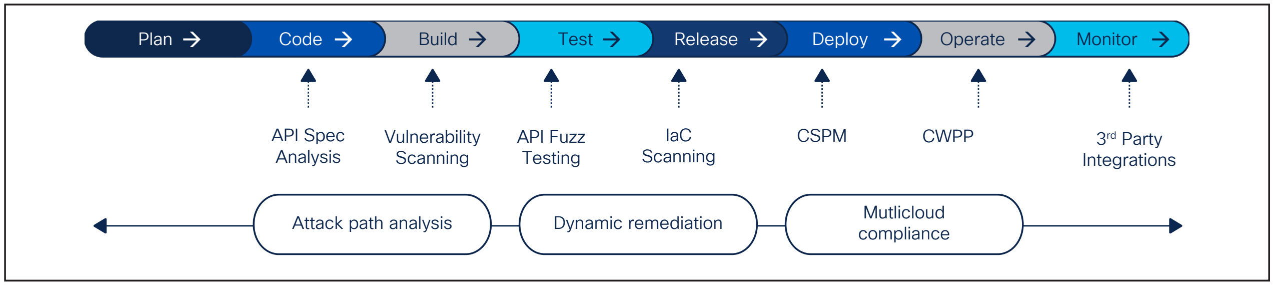


Figure 2. Cisco Cloud Application Security provides protection from code to cloud

End-to-End visualization

Cisco Cloud Application Security provides rapid and detailed visualization of the entire cloud stack, across any Kubernetes platform, in any cloud provider. Underlying graph technology provides quick and simple risk identification, prioritization, and dynamic remediations guidance for critical security gaps and vulnerabilities.

Dynamic remediation guidance

Cisco Cloud Application Security dynamically generates guidance to quickly and effectively remediate threats detected in your environment. This guidance includes both the steps to take and the specific commands lines. Cisco Cloud Application Security also summarizes the issue context, explanations, and recommended remediations via IaC, Terraform, or JavaScript Object Notation (JSON). These summaries can be integrated into your existing issue management systems and workflows to create tickets for your developers and engineers to resolve the issues quickly and effectively.

To learn more, visit cisco.com/go/cloudapplicationsecurity