Data sheet

Cisco public

Cisco Cloud Application Security

Contents

Application trends

Cloud applications are the future of digital business. In fact, by 2025, organizations will be running more than 750 million cloud applications, which is nearly three times as many as they are running today. Additionally, more than 85% of organizations have plans to adopt cloud development principles, redefining application architecture standards and the security practices needed to protect these new environments.

Cloud applications are built differently, and as a result, require an innovative approach to securing them. Cloud applications:

- Are hosted on serverless infrastructure, instead of running on fixed server hardware in a local corporate data center.
- Are designed as small, interdependent services instead of as an application comprised of a large block of monolithic code.
- Use APIs (Application Programming Interface) and open-source code as reusable application building blocks, instead of libraries of custom programmed sub-routines written for a specific application.

New security approach needed

API's and open-source code are cloud application 'building blocks' that can be used over and over, speeding application development time. While a great time-saver and development accelerator, this reuse can expose organizations to tainted code built into third-party artifacts. The origins of these artifacts are often hard to validate, which means organizations without the right tools will, at some point, unwittingly import bad code into applications. This risk shifts the importance to focus on a security strategy centered on unified security platform that **thinks like an attacker**, using several different techniques to secure the entire cloud application process from development to cloud deployment.

Cisco Cloud Application Security overview

Cloud Application Security is a unified security platform that brings together Cloud Security Posture Management (CSPM), Cloud Workload Protection (CWPP), API security, and Infrastructure as Code (IaC) security to minimize visibility gaps and provide centralized management. Unlike the use of multiple security point products common today, Cloud Application Security is an all-in-one security solution from Cisco, designed to substantially reduce risk and cost, while improving productivity in the following ways:

- **Comprehensive code to cloud coverage.** Whether you build and run your applications 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.** The Cloud Application Security attack path engine actively analyzes misconfigurations, network exposure, secrets, vulnerabilities, malware, and overly permissive identities to find exploitable paths that could be used to get into an environment and move laterally. These attack paths are prioritized by severity to clearly show the biggest threats without overwhelming operators in countless alerts.
- **Dynamic remediation guidance.** Cloud Application Security dynamically generates guidance to quickly and effectively remediate threats detected in your environment. This guidance includes the remediation steps and specific commands for each step. This guidance 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.

Features and benefits

Listed below are the key features and benefits of Cloud Application Security.

Table 1. Features and benefits

Feature	Benefit
Agentless Scanning	• Agentless technology scans any cloud environment—Azure, AWS, GCP, OCI, Kubernetes, or a combination thereof.
API security	• Analyzes risk associated with untrusted external and internal APIs used by your workloads. • Automatically uploads external or internal API specs for inspection. • Performs trace analysis on API traffic (both external and internal) to identify security issues that influence risk scores.
Attack Path Analysis	• Focuses on the most critical risks by viewing the environment from an attacker's perspective. • Reduces non-critical security findings and improve team productivity.
CI/CD Security	• Drives security automation throughout the application development process, enabling developers to assess and mitigate security risks. • Mitigates risks including code vulnerabilities, IaC misconfigurations, and API security.
Cloud Security Posture Management (CSPM)	• Ensures security checks pass all audits and meet business goals by monitoring for compliance standards and best practices. • Enforces PCI-DSS, HIPAA, GDPR, SOC2, and CIS (Center for Internet Security) benchmarks. • Goes beyond compliance by inventorying all cloud assets and identifying all misconfigurations plus following identity risks: ◦ Common Misconfigurations ◦ Dangerous Defaults ◦ Dangling Domains ◦ Detecting Exposed Secrets ◦ Effective Permissions Evaluation ◦ Identifying Public Exposure ◦ Neglected Resources ◦ Risky and Weak Configurations ◦ Risky Permissions ◦ Shadow Admin ◦ Unsupported Software • Understands misconfigurations connected to vulnerabilities and other security issues associated with attack paths to further prioritize issues.
Cloud Workload Protection (CWP)	• Helps minimize your attack surface, prevent administrator errors, and protects against common attack vectors. • Enables security and compliance teams to enforce policy-driven security configurations and governance. • Helps secure the essential orchestration layer of cloud applications with continuous security risk assessment and remediation.
Infrastructure as Code (IaC) Security	• Scans IaC files to find security vulnerabilities and infrastructure misconfigurations before deploying them to production.

Feature	Benefit
Kubernetes Security Posture Management (KSPM)	• Provides continuous visibility and monitoring of Kubernetes clusters for security risks and compliance violations. • Uses contextual mapping to identify the relationships between Kubernetes objects, providing an accurate and up-to-date view of the cluster's security posture. • Ensures the secure configuration of Kubernetes clusters, detects vulnerabilities and misconfigurations, and reduces the risk of a security breach. • Provides actionable insights by scanning multi-cloud Kubernetes workloads for vulnerabilities and common misconfigurations. • Enables declarative policy automation.
Root Cause Analysis	• Goes beyond surface level insights to find issues such as a singular root cause that enables multiple attack paths. • Save countless hours of manual work on analysis.
Serverless security	• Frees developers to focus on developing and deploying cloud features and services faster, without managing infrastructure.
Software Supply Chain security	• Generates a Software Bill of Materials (SBOM) for each image. • Identifies the vulnerabilities for each layer. • Analyzes deployment templates for configuration risk. • Ensures best practice conformity via CIS Benchmarks. • Ensures application developers stay compliant with federal mandates. • CI/CD security feature drives security automation in the application development process, enabling developers to assess and build security policies from the IDE, Terraform, and GitOps tooling.

"Upon implementing Cisco Cloud Application Security, we significantly enhanced the security posture of our cloud application ecosystem. By integrating this platform into our testing and production environments, we've accelerated our application deployment process which has given us a significant competitive edge."

– Financial Services Company

Cloud Application Security licensing options

The Cloud Application Security solution is available as a standalone solution or part of the Cisco Cloud Protection Suite:

- **Cloud Application Security Solution:** As a standalone solution, the single security platform enables DevSecOps best practices and protects cloud applications from development through runtime. The subscription includes comprehensive protection of Virtual Machines (VM), APIs, Kubernetes clusters, serverless environments, and developer coding environments. It enables developers to fix vulnerabilities faster while boosting security team's ability to measure compliance and prioritize findings.
- **Cisco Cloud Protection Suite:** A purpose-curated group of security solutions to address specific security concerns that are introduced as organizations migrate through the process of digitalization, which often presents profound security challenges associated with the adoption of multiple cloud infrastructure elements and the evolution of traditional applications to cloud applications.

Ordering information

To subscribe, contact your certified Cisco partner or Cisco sales agent. If you need help finding a partner in your area, use the Partner Locator tool. Your partner or Cisco sales agent can also aid with any modifications to your subscription after your initial order is placed.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

Learn more about Cloud Application Security

To learn more about how the Cisco Cloud Application Security solution can provide a comprehensive, easy to deploy solution for protecting your cloud applications and the underlying infrastructure that they are built upon, contact your Cisco sales representative or access more information from the Cloud Application Security webpage.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-4153002-00 04/24