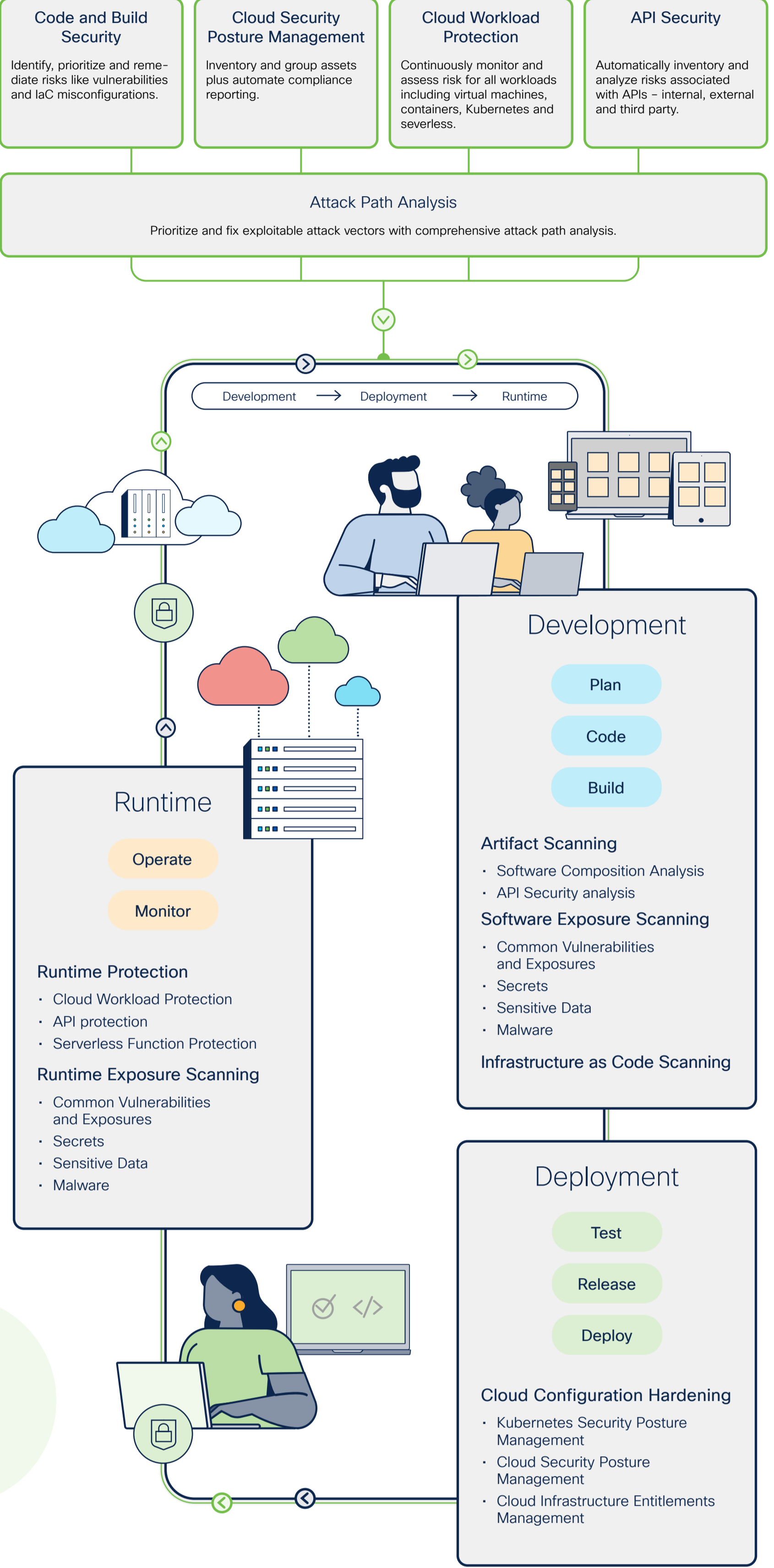# Prioritize and remediate cloud application risks with precision

The cloud offers teams agility, autonomy, and scale 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 severless.

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 → Deployment → Runtime

Development

Plan

Code

Build

Artifact Scanning
- Software Composition Analysis
- API Security analysis

Software Exposure Scanning
- Common Vulnerabilities and Exposures
- Secrets
- Sensitive Data
- Malware

Infrastructure as Code Scanning

Runtime

Operate

Monitor

Runtime Protection
- Cloud Workload Protection
- API protection
- Serverless Function Protection

Runtime Exposure Scanning
- Common Vulnerabilities and Exposures
- Secrets
- Sensitive Data
- Malware

Deployment

Test

Release

Deploy

Cloud Configuration Hardening
- Kubernetes Security Posture Management
- Cloud Security Posture Management
- Cloud Infrastructure Entitlements Management

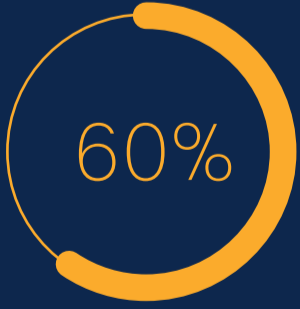## Benefits of a comprehensive solution

85%
Of organizations said a CNAPP will give them a consolidated approach for more efficient cloud security risk mitigation

87%
Of organizations said a CNAPP helps drive efficiency in connecting application security processes to security posture management
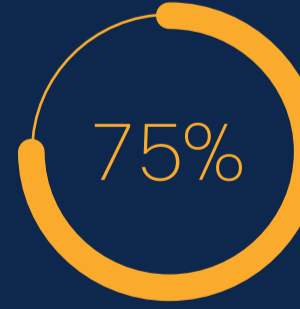
Create a plan today

60%
By 2025, 60% of enterprises will have consolidated cloud workload protection platform (CWPP) and cloud security posture management (CSPM) capabilities to a single vendor, up from 25% in 2022.

80%
By 2025, 80% of enterprises will have adopted multiple public cloud infrastructure as a service (IaaS) offerings – including multiple K8s offerings.

75%
By 2025, 75% of new CSPM purchases will be part of an integrated CNAPP offering.

Learn More

ⓘ At-A-Glance | ⓐ Learning Labs