
Panoptica
Cloud-Native Application Security, Simplified
Cisco Panoptica for Simplified Cloud-Native Application Security
Innovate your modern cloud-native applications faster by driving simplified security automation through the entire application development lifecycle—from code to runtime.

Modern cloud-native application architectures enable rapid innovation. But when it comes to security, cloud-native architectures are fraught with complex security challenges.

Modern apps have left behind legacy application frameworks of server-centric infrastructure where development cycles and new feature releases took months or even years to complete. Unchained from monolithic on-premises infrastructure, cloud-native modern apps are built using service-based architectures that split application workloads into hundreds of smaller, more manageable units.

Cloud-native technologies provide developers with comprehensive, standards-based mechanisms for building, deploying, and managing modern applications using orchestration systems, microservices (containers and ephemeral serverless functions), declarative application programming interfaces (APIs), and service meshes. There is no denying that the move to cloud native has permanently altered software development by making it possible to build flexible, resilient, and scalable applications quickly and easily. However, when it comes to security, businesses are left with too many moving parts to contend with.

While microservices significantly reduce the speed of innovation for your DevOps teams, they complicate security for your SecOps teams by introducing new attack vectors at every stage of the app development lifecycle. Starting with the software code, the APIs used to build or integrate the application software or the Kubernetes containers themselves that host the application – in a microservices environment, all elements are subject to becoming targets of compromise.

Application vulnerabilities should be viewed in context across the application development lifecycle because risks are present in both the application's infrastructure and the application's logic.

Adding to that, the fact that Kubernetes and the one-function tools that support orchestration are not designed to be "secure by default" exacerbates the problem. API breaches are on the rise too where hackers go after software authentication, authorization, and implementation flows in the application itself. In recent times, some of the most successful companies globally have been significantly impacted by such events. Making matters even worse for SecOps is the lengthy, human-intensive model of legacy application security tools and processes. Without tight integration and frictionless collaboration, it is impossible to keep up with the speed and velocity by which DevOps teams innovate.

Threat Vectors are Exploding in Microservices Security

94%
Enterprises had a Kubernetes security incident in the last 12 months

59%
Enterprises admit to security as the biggest concern in their Kubernetes journey

55%
Enterprises had to delay application release due to a Kubernetes security issue

20%
Enterprises facing API security breaches at least once a month

286%
Quarter over quarter increase in API attacks

$4.35M
Average cost of a data breach in 2022

But there is a solution. Enter Cisco Panoptica

Advance to DevSecOps with Cisco's Panoptica

Panoptica provides a comprehensive security solution for your entire software development lifecycle (SDLC)—from development to runtime. It simplifies the task of comprehensively securing your cloud-native application development lifecycle—from build pipelines to workload runtimes of microservices running in one or more clouds. Panoptica provides visibility and remediation guidance for microservices running in containers and managed by Kubernetes, serverless functions, and declarative (APIs) that enable the microservices. It helps DevOps and SecOps teams bridge the collaboration gap more effectively, removing friction from the SDLC process.

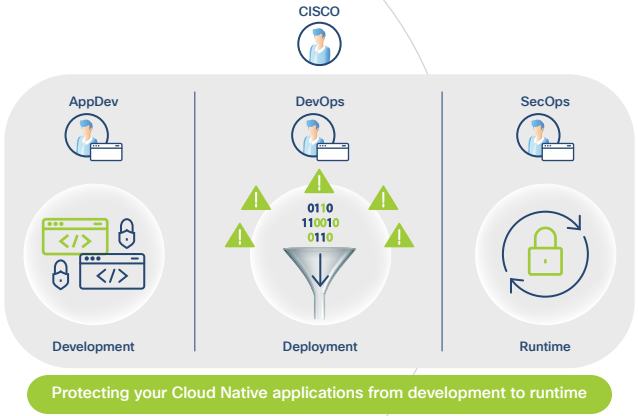

Figure 1. Panoptica – The Secure Cloud-Native Application Cloud

Panoptica's Key Value Propositions

The first security requirement in a cloud-native architecture is **visibility**, the ability to identify possible threats, vulnerabilities and policy enforcement points. However, in many cases, security teams have little or no visibility into the APIs or workloads that have been deployed, let alone what vulnerabilities these may have and which of these are currently being exploited. Panoptica provides this critical visibility.

Another key security requirement particularly relevant to cloud-native is the need to "**shift-left**" by embedding security earlier in the software delivery lifecycle (SDLC).

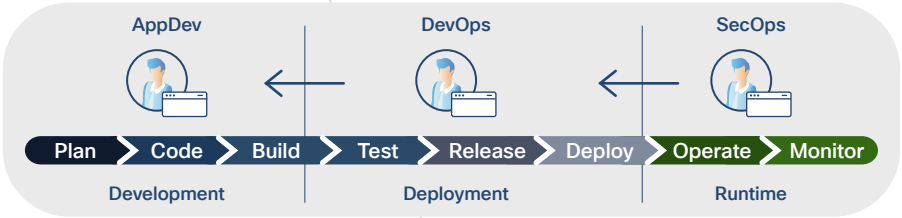

Figure 2: Shifting Security Left in the CI/CD Cycle Cloud

Panoptica enables SecOps teams to develop and harden application security at the earliest stages in the development lifecycle so they can identify and fix security vulnerabilities at the very onset, before deployment. Doing so helps with considerable cost savings because remediating breaches in production can cost substantially more than remediating potential risks earlier in the development lifecycle.

A third key requirement is the ability to **enforce policy**. While knowing about a vulnerability is obviously helpful, this alone is insufficient. Actions need to be enforceable to prevent and remediate threats, whether these threats are introduced when developing, deploying, interconnecting or running containerized applications and microservices. Panoptica provides policy-based remediation guidance to protect your application from security attacks.

Part of the Cisco SecOps toolset, Panoptica serves as a key enabler to let your SecOps professionals join the world of DevSecOps to bring secure modern apps to market faster.

The Cisco Panoptica Difference

Panoptica protects the full application stack from code to runtime by scanning for security vulnerabilities in the cloud infrastructure, microservices (Containers or Serverless), the software bill of materials, and the interconnecting APIs. And best of all, Panoptica integrates with the tools that your application development and SecOps teams are already using like GitHub as a code repository, Helm for software deployments, and Terraform for the infrastructure required for their applications.

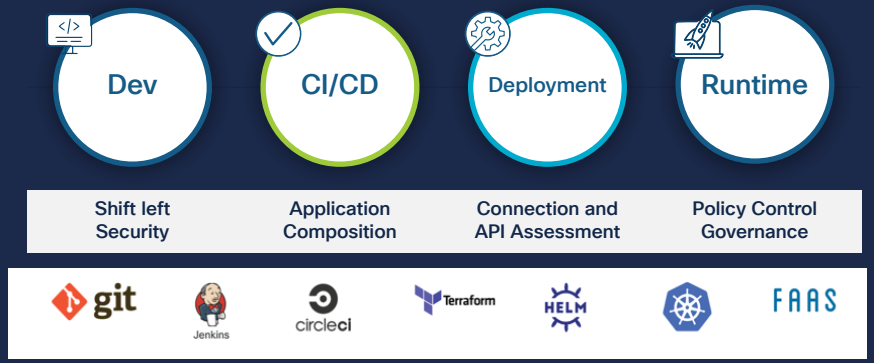

Figure 3. Panoptica enables security across the full SDLC Stack – from code to runtime, seamlessly integrating with all DevOps tools and toolchains

How Panoptica Solves Security Issues at Each SDLC Stage

Shift-Left Security (Development): Panoptica adds shift-left security to your cloud-native environment by detecting and prioritizing risks associated with your application, stopping preventable security risks from reaching production. It allows you to build security policies and analyze risks within the most popular Dev tools you already use such as Git, Jenkins, Helm, and Terraform.

Application Composition (CI/CD): During application composition, Panoptica generates a software bill of materials (SBOM) for each image, identifies the vulnerabilities associated with each layer, analyzes deployment templates for configuration risk, and ensures best practice conformity via CIS Benchmarks.

With Panoptica, application developers can stay compliant with federal mandates by easily identifying open-source software components that may be vulnerable to attacks and require patching.

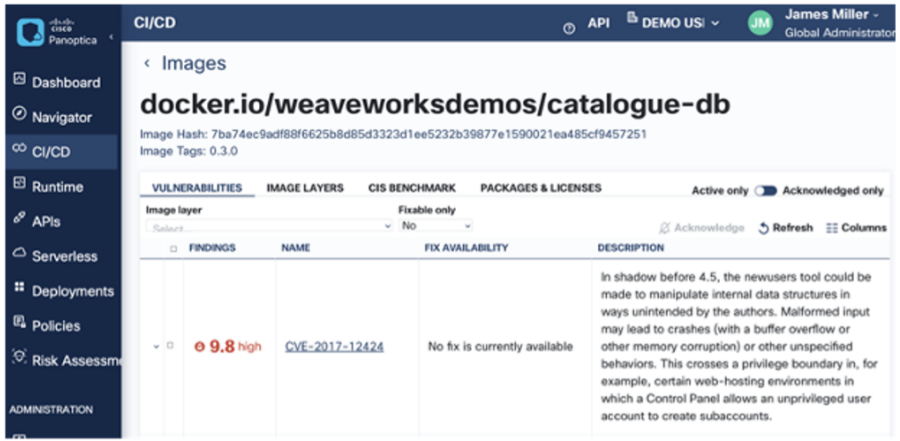

Figure 4. Panoptica identifies vulnerabilities across each layer

Connection and API Assessment (Deployment): Rather than requiring developers to perform extensive security research on APIs, Panoptica helps discover the API endpoints giving Ops teams a clear picture of all API connections including segmented views of internal and external APIs. Panoptica analyzes and scores the APIs from a security perspective, and then presents these to developers and SecOps as a curated list, so that they can quickly make optimal and compliant API selections to embed security into their microservices from the very beginning. Panoptica monitors the APIs for vulnerabilities to ensure their compliance with your declarative policies.

It can help your Ops teams perform fuzz testing, spec analysis and reconstruct specs that are broken. It can establish policies that govern which API calls the gateway will permit, based on specific app components. It lets you disable risky APIs that don't adhere to specifications.

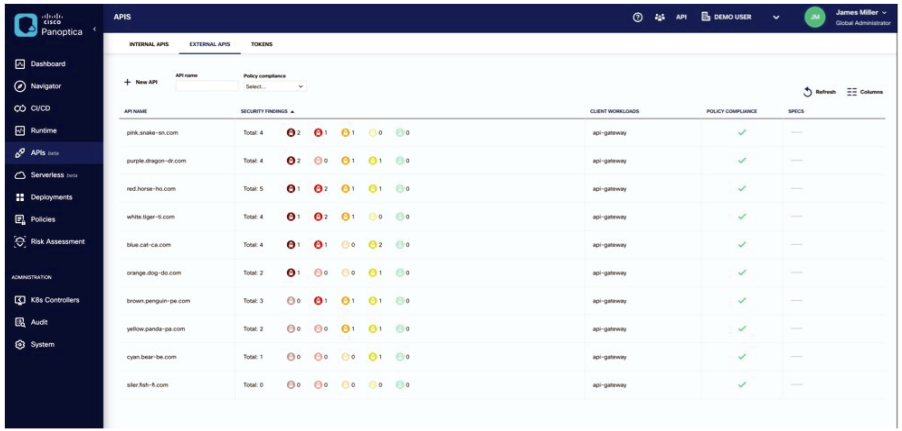

Figure 5. Panoptica provides segmented views of internal and external APIs

Policy Control Governance (Runtime): Hardening your Kubernetes infrastructure is crucial to prevent breaches, attacks and leaks of information. Panoptica provides seamless security to the entire cloud infrastructure stack—from code to runtime—enabling your SecOps teams to identify suspicious behavior in the entire cluster. It runs on any cloud—public or private. By scanning multi-cloud Kubernetes workloads for vulnerabilities and common misconfigurations, Panoptica provides actionable insights from its dashboards. It enables declarative policy automation—meaning you just write one access or permissions policy and propagate across clusters. With Panoptica, you can set seamless controls and understand who has what permissions to ensure permissions aren't overly permissive.

Panoptica's scanning capabilities also inspect serverless functions for vulnerabilities and ranks them by a risk score to ensure up-to-date coverage. Risk scores help set policies specifying which serverless functions are compliant and authorized for deployment.

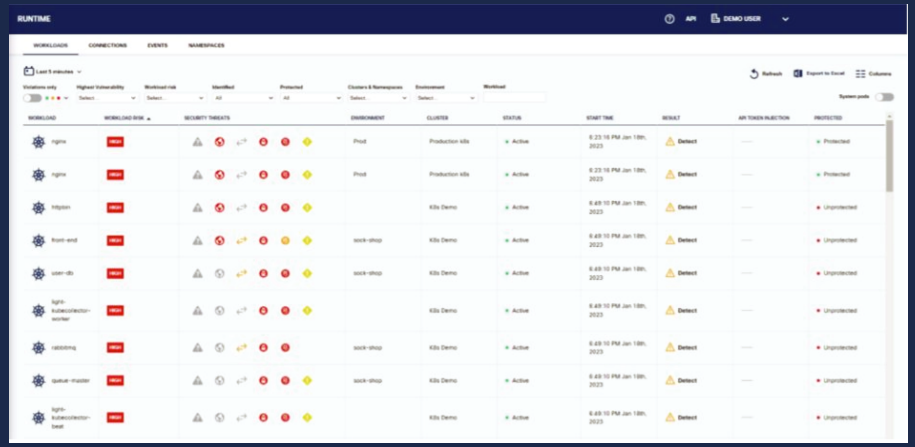

Figure 6. Panoptica analyzes the pods in the cluster and give you an overview of the current risks and vulnerabilities

Panoptica Enables DevSecOps at Scale

We integrate our core security capabilities from each stage of the SDLC in unique, developer friendly ways to allow your developers to continue to innovate rapidly while permitting security to scale along with the speed and complexities of cloud-native applications.

Policy Automation

Panoptica lets you automate the updating of your policies. Write one policy and propagate across containers or code deployments to ensure new code has less risk. Free yourself from having to manually search for individual security policies across your Kubernetes infrastructure and manually make updates and changes.

Actionable Insights

Panoptica gives you actionable incident response with a dashboard highlighting what MITRE Att&ck vectors you have that are aligned to your Kubernetes and container risks.

Agentless Approach

Panoptica's agentless approach lets the application run on single pod that covers your environment—even across clouds.

Panoptica Works Across All Kubernetes Platforms

Experience Panoptica Free!

Simply go to panoptica.app. Sign-ups are without time restrictions and don't require credit card information. Panoptica's free tier version protects up to 10 nodes, 1 cluster, & unlimited pods.

Page 1 Data Sources:
https://www.redhat.com/en/blog/state-kubernetes-security-2022-1
https://www.ibm.com/downloads/cas/3R8N1DZJ
https://www.forbes.com/sites/forbestechcouncil/2022/07/25/how-to-address-growing-api-security-vulnerabilities-in-2022/?sh=7baebdf55a9e
https://www.gartner.com/en/webinarsfl:~:text=Gartner%20predicts%20that%20by%202022,a%20wide%20range%20of%20organizations.