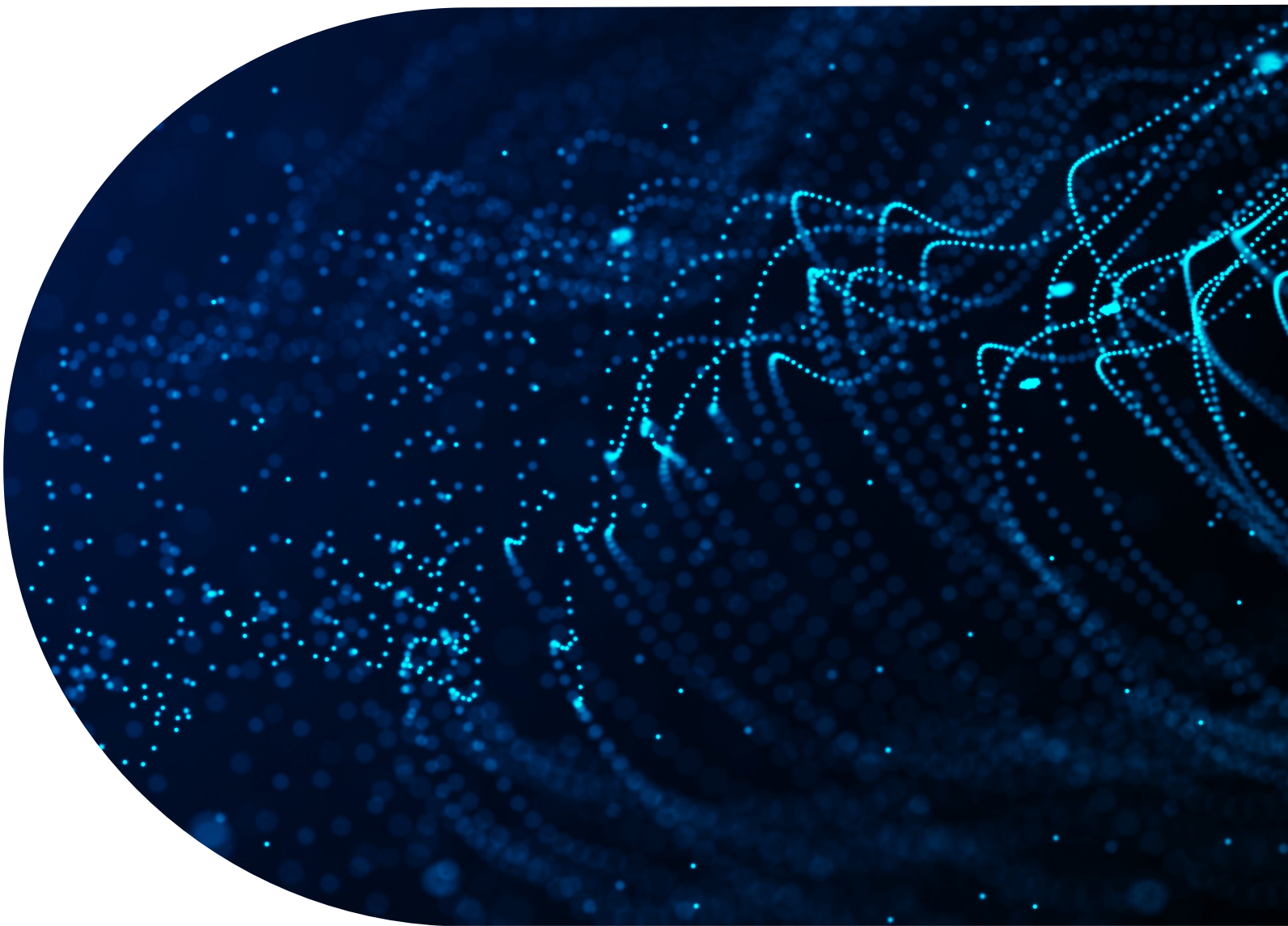
panoptica

Panoptica for Complete Cloud Application Security

Protect your complex, multi-cloud environment with a new level of precision, and scale security across all your cloud assets with Cisco's cloud native application.



As more organizations move to the cloud, there is a growing need for an integrated platform approach to cloud security. One that can comprehensively protect your cloud native applications and infrastructure while keeping up with a constantly evolving threat landscape.

Modern organizations are rapidly expanding their cloud footprint by adopting complex and hybrid multi-cloud environments. The shift to the cloud has led to the emergence of containerized and ephemeral environments with faster release cycles and modern software development practices that require a wide range of security controls. Previously, securing the cloud meant securing the infrastructure. Today, securing the cloud has evolved into protecting modern software applications that run on cloud workloads and the tooling needed to build those applications. That means optimizing cloud security and compliance by removing barriers between siloed development, operations, and security teams.

There is no doubt that cloud workloads have permanently altered software development by making it possible to build flexible, resilient, and scalable applications quickly and easily. But when it comes to securing these workloads, DevOps and Security teams are left with too many moving parts to contend with. And with too many moving parts, comes the need for enforcing too many security controls.

A complex challenge facing these teams today is that they must use many security tools to enforce numerous security controls throughout the software development lifecycle. The tool sprawl resulting from this situation makes identifying and responding to security threats complex, time-consuming, and prone to errors and mismanagement. While tool sprawl is one challenge, the gaps between tools in terms of their capability or functionality is another challenge. Lastly, a lack of insights shared between tools is yet another challenge.

To bring speed and efficiency in enforcing security controls, organizations with large-scale cloud native deployments are looking to institute security during development and deployment with cloud security posture management (CSPM), cloud infrastructure entitlement management (CIEM), and cloud protection platform (CWPP) combined with application security and attack path analysis. Application security (includes code, API, and data security) is a part of this continuum because risks present in the application's logic and data must be addressed. Attack path analysis is a necessary addition as it visualizes the route an adversary takes to perpetrate an attack, thus highlighting which security vulnerabilities and attack vectors must be prioritized for remediation.

While the need is there, stitching together a full coverage enterprise-ready mechanism for complete cloud security on their own is not an easy task for organizations. That's where an end-to-end platform-approach to cloud native security has gained ground. Labeled by Gartner as a Cloud-Native Application Protection Platform (CNAPP), it consolidates previously siloed cloud security capabilities into a tightly integrated set of security and compliance solutions. With a cloud application security solution, enterprise security and risk management leaders can easily take a holistic approach to cloud security keeping these strategic planning assumptions in mind.

Gartner's Strategic Planning Assumptions

60%

Of enterprises will have consolidated CWPP and CSPM to a single vendor by 2025, up from 22% in 2022

80%

Enterprises will have adopted multiple public cloud Infrastructure-as-a-Service (IaaS) offerings, including multiple Kubernetes (K8s) offerings by 2025

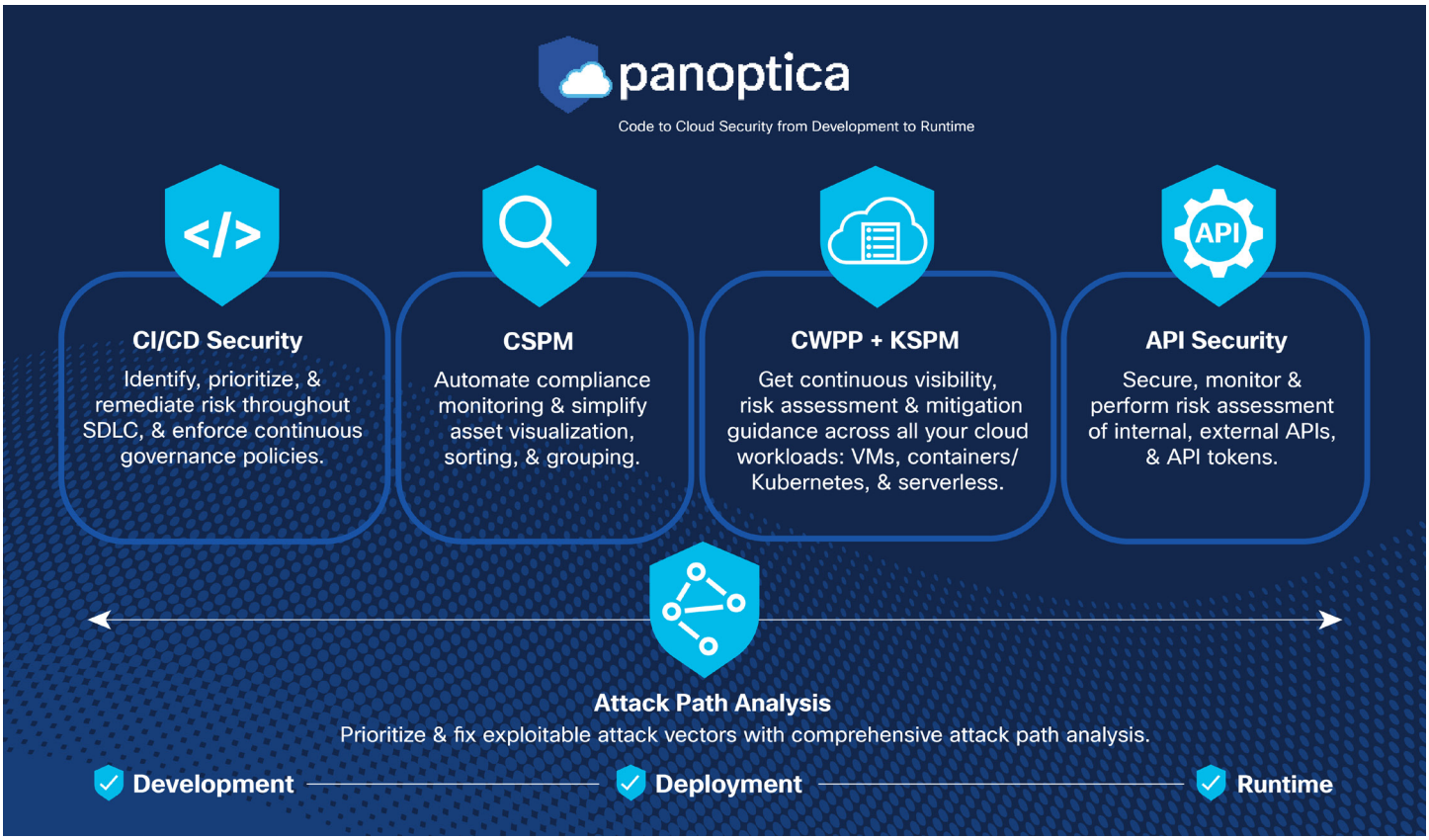
75%

Of new CSPM purchases will be part of an integrated CNAPP offering by 2025

Actionable Protection from Development to Runtime with Panoptica

Today, Cisco is connecting developer and security teams to their organization's biggest cloud threats from development to runtime.

Cisco's cloud native application protection platform Panoptica provides contextualized cloud security to identify, prioritize, and remediate security risks and misconfigurations in complex cloud environments. The unified cloud security platform makes every stage of cloud security simple. From software, artifact, and exposure scanning along with Infrastructure as Code (IaC) at build, to cloud security posture management (CSPM) including compliance benchmarks and configuration management, attack path analysis, and comprehensive cloud workload protection (CWP) across multi-cloud runtime environments—Panoptica offers a wide range of capabilities CISOs, DevOps, and Security teams need to protect their cloud-native application stack using a single simplified solution. Panoptica's "single pane of glass" approach to solving your cloud security challenges eliminates operational complexity resulting from cloud security tool sprawl. It shares deep insights across traditionally siloed tools for comprehensive security. You also get meaningful insights through its attack path analysis capability that exposes exploitable paths attackers use to breach your environment. With a fast time-to-activation through our easy set-up flow, organizations of all sizes use Panoptica to protect their infrastructure and applications in the cloud.



Panoptica is Integration Ready

Panoptica seamlessly integrates with the tools and toolchains that your DevOps teams are already using. For example:

- GitHub as a code repository
- Jenkins and CircleCI for continuous integration (CI) pipelines
- Helm for software deployments
- Terraform for the infrastructure required for applications

What's more? Your SecOps teams can take advantage of full stack observability (FSO) as an add-on to their core CNAPP experience.

Leverage the power of FSO to observe and address security vulnerabilities and threats with real-time recommendations across critical cloud assets based on business risk. Get differentiated security visibility, insights, and actions to protect cloud assets—Kubernetes clusters, workloads, and containers for public cloud applications.

On top of this, Cisco customers now have an easy path to expand their vulnerability management, thanks to Panoptica's additional integrated capabilities.

Overview of Panoptica's Cloud Application Security

Many point product competitors have invested in the cloud security space to deliver end-to-end security protection, but Cisco can offer a worthy differentiated experience. Cisco believes our customers deserve a true partner in their security strategy by providing cloud application security, which includes Gartner's CNAPP functions. Panoptica is purpose-built with the following core capabilities:

CI/CD Security

- SBOMs/Software Supply Chain

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

- Infrastructure as Code (IaC) Security

Panoptica shifts your security testing to the left by enabling your application developer teams to scan their IaC templates and scripts for potential security risks and misconfigurations before deploying them to production. Developers and DevOps teams can review the code as they build and quickly get insights into how they may be impacting production. This helps to ensure that security issues are addressed as part of the development process, rather than after deployment.

Cloud Security Posture Management (CSPM)

Posture management and compliance are essential to cloud security. Whether you are using AWS, Azure, Google Cloud, or a hybrid configuration, Panoptica takes CSPM to the next level by delivering continuous cloud security compliance at scale including attack path analysis that highlights potential attack chains.

While surfacing the relevant compliance benchmarks, Panoptica also ensures your cloud stack runs securely from end to end by scanning it continuously for any new vulnerabilities and misconfigurations. As your cloud stack expands and grows, Panoptica helps you visualize, sort, and group your assets easily through its dashboard to get full visibility into your entire inventory of cloud assets.

Kubernetes Security Posture Management (KSPM)

Panoptica provides continuous visibility and monitoring of Kubernetes clusters for security risks and compliance violations. Our KSPM capability uses contextual mapping to identify the relationships between Kubernetes objects and provide an accurate and up-to-date view of the cluster's security posture. Leverage Panoptica to ensure the secure configuration of Kubernetes clusters, detect vulnerabilities and misconfigurations, and reduce the risk of a security breach. 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 it across clusters.

Cloud Workload Protection (CWP)

Enterprises can only secure what they see, and for that they need comprehensive visibility across all cloud native workloads and applications. Panoptica provides visibility and remediation guidance for applications running on virtual machines (VMs), for microservices

running in containers and managed by Kubernetes, and for event-based microservices that use ephemeral serverless functions to perform highly specific roles within an application. Panoptica's scanning capabilities inspect workloads for vulnerabilities and ranks them by a risk score to ensure up-to-date coverage. Risk scores help set policies specifying which workloads are compliant and authorized for deployment. Beyond just scanning, it lets you drill down into common vulnerability exposures (CVEs) to get deeper context on the most urgent threats while giving you access to instant remediation to clear the vulnerability.

API Security

Panoptica helps discover API endpoints giving Ops teams a clear picture of all API connections—including segmented views of internal and external APIs. Panoptica analyzes and scores OpenAPI/REST-based APIs from a security perspective, and then presents these to developers and SecOps as a curated list so that they can quickly make compliant API selections to embed security into their microservices from the beginning. Panoptica monitors the APIs for vulnerabilities in runtime to ensure their compliance with your declarative policies. It helps your team perform fuzz testing, spec analysis, and reconstructs 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.

Attack Path Visualization and Analysis

Siloed tools can simply not chart out the route an adversary takes to perpetrate an attack as these attack paths often cross over from one area (for example, an API vulnerability) and then exploit a completely different area (for example, a software vulnerability).

A platform-based approach to cloud-native security with attack path analysis capabilities is necessary here because while the relative risks in one isolated view may not be severe on their own, the combination of exploits may present serious exposure.

Panoptica's proprietary attack path analysis engine quickly and accurately discovers and helps remediate exploitable attack vectors in your cloud stack. Using techniques such as comprehensive attack path analysis, root cause analysis, and dynamic remediation, you can now uncover new and known risks by looking through the lens of a potential attacker. Use attack path analysis to surface critical attack paths to better understand the impact of potential risks.

Determine the root cause with the help of our root cause analysis algorithm that presents you with easy-to-understand foundational issues that impact your cloud environment. Leverage dynamic remediation with ready-made IaC built for you. Simply review and deploy to close security gaps faster than ever.

Panoptica Enables Comprehensive Cloud Application Security at Scale

We integrate our core security capabilities from each stage of the software development lifecycle in unique, DevOps friendly ways to allow your teams to continue to innovate rapidly while allowing cloud security to scale along with the speed and complexities of their cloud native applications.

Streamlined and Consolidated Cloud Security:
Panoptica provides a holistic security solution across multiple cloud native workloads eliminating the need for disjointed point solutions.

Complete and Cohesive Visibility:
Panoptica analyses risks from multiple touchpoints to provide a cohesive and prioritized view of threats, vulnerabilities, and compliance issues.

Complex Multi-Cloud Environment Support:
Panoptica encompasses scanning, monitoring, and remediating risks and compliance issues across public and hybrid multi-cloud environments.

Tighter End-to-End Security Controls:
Panoptica integrates with the CI/CD toolchains DevOps already use and provides add-on integrations for full stack observability and vulnerability management.

Lower Cloud Security Overhead and Complexity:
Panoptica provides an economy of scale not found through a patchwork of individual solutions. Less disjointed effort translates into less operational overhead for CISOs and DevOps leads and more time for security priorities.

Outshift by Cisco is paving the way with "DevOps-friendly" cloud native security solutions that fundamentally simplify conventional offerings.

Built from the ground up to meet the needs of business-critical modern applications, our Panoptica solution simplifies cloud native application security by combining the collective strengths of its existing capabilities with organic development. As a result, what you get is a solution that makes embedding cloud security simple yet comprehensive into the application development lifecycle.

Experience Panoptica Free!

Simply go to www.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.

Learn More and Get Started

Visit panoptica.app

Sign up for a Free Trial

Access Additional Resources

Read Our Blogs

Get More Content