# Panoptica At A Glance

## Cisco Emerging Technologies and Incubation

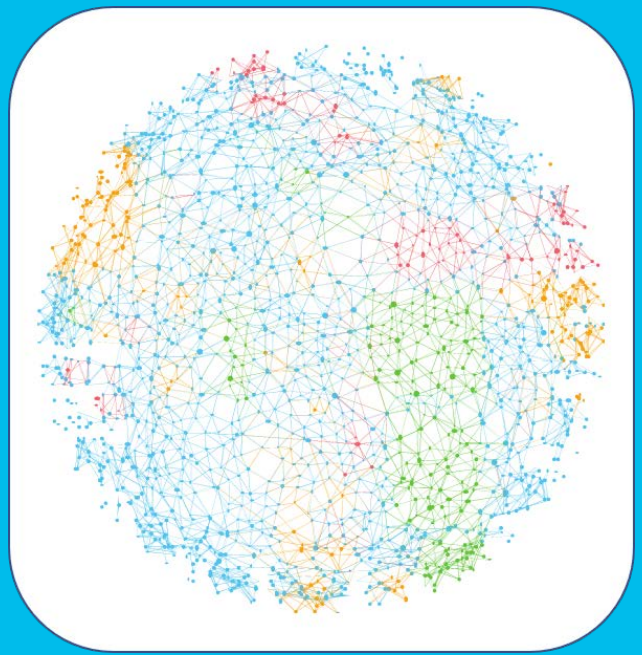
## Panoptica–The Cisco Secure Application Cloud

Businesses are increasingly adopting Cloud Native architectures, as these enable rapid application development with flexibility, stability, portability, and scale. However, microservice-based architectures also massively increase the attack surface and expose applications to new vulnerabilities and threats, thus requiring a whole new approach to application security.

This is because in Cloud Native architectures application components are disaggregated into resuable services. Each of these services are hosted in containers and pods, which are spun up, spun down, replicated and replaced as needed by container management systems, like Kubernetes. And the Application Programming Interfaces (APIs) that interconnect these services are distributed across multiple SaaS, cloud or on-premises platforms.

The interconnections of these microservices can become very complex, as shown in Figure 1, which depicts the microservice dependency graph of a typical banking application. From this graph it quickly becomes evident that traditional approaches to application security, which most often involve setting a clearly defined security perimeter around an application, do not apply in Cloud Native architectures, due to the diffused nature of these architectures.

**Figure 1: A Microservice Dependency Graph of a Cloud Native Banking Application**



It is also important to recognize that some APIs are more secure than others. As such, developers do well to consider:

- Are my internal APIs vulnerable?
- Am I using vulnerable third-party APIs?
- Do I have *indirect* dependencies on vulnerable APIs?

However, it would be burdensome to require developers to sacrifice rapid application development to perform security research and analysis on the APIs that they are considering for use.

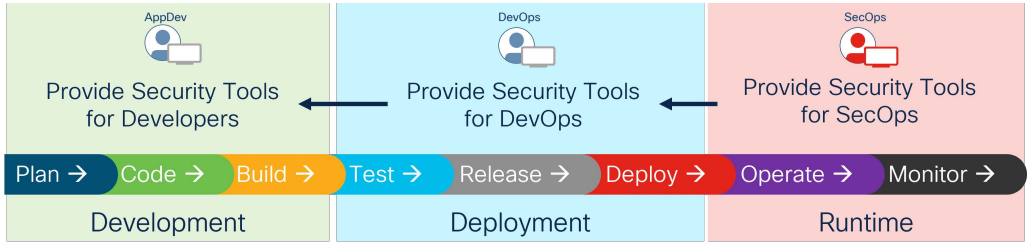
Beyond APIs, Cloud Native deployments present several additional new opportunities for vulnerabilities to be introduced and exploited, such as in container images, packages and/or dependencies, pod misconfigurations, cluster RBAC roles and even security deployment files that, due to their sheer sizes, can often contain security misconfigurations and even embedded secrets. As such, it becomes ever clearer that a new approach is needed to secure Cloud Native applications.

## Panoptica 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**" - that is, to embed security *earlier* in the Continuous Integration and Continuous Delivery (CI/CD) cycle, as shown in Figure 2.

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

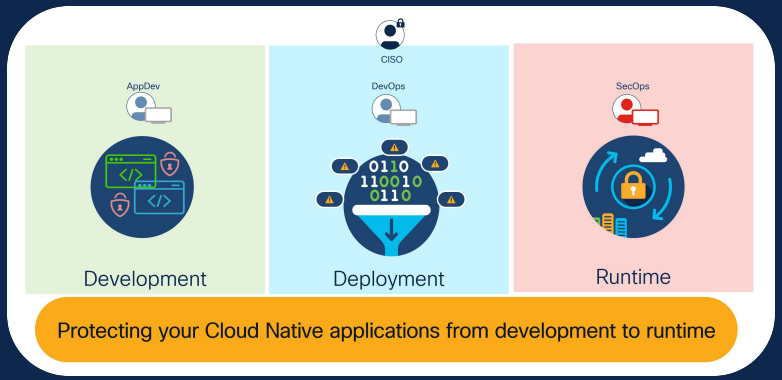



For example, returning to the API selection decision faced by developers: rather than requiring developers to perform extensive security research on APIs, Panoptica analyzes and scores all APIs (internal and external) from a security perspective, and then presents these to developers as a curated list, so that they can quickly make optimal and compliant API selections that embeds security into their apps from the very beginning. With this approach the entire process is benefited, expedited, stabilized and ultimately made more secure.

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.

In summary, to meet the comprehensive API and container security requirements of Cloud Native application architectures, Cisco has developed Panoptica, to protect and harden applications in every stage, from development, deployment and runtime.

### Figure 3: Panoptica-The Cisco Secure Application Cloud




© 2022 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

CXX-XXXXXX-00 07/21