WHITE PAPER

Enhance Security and Gain Comprehensive Visibility with a Cloud-native Application Protection Platform

How Cisco Panoptica Simplifies and Secures the Cloud-native Application Lifecycle

By Paul Nashawaty, Principal Analyst; and Melinda Marks, Senior Analyst
Enterprise Strategy Group

May 2023

This Enterprise Strategy Group White Paper was commissioned by Cisco and is distributed under license from TechTarget, Inc.

Contents

Executive Summary

As the demand for cloud-native applications has increased, so have the challenges around developing and managing them. Cloud-native applications are complex and designed to be highly scalable, but managing the scale can be challenging, especially when applications are distributed across multiple data centers and cloud providers. And because cloud-native applications are often built and deployed on a microservices architecture and deployed using containers and Kubernetes for orchestration, new security challenges can be easily introduced into these complex environments.

Organizations are all too aware of the negative impacts a security breach can have on the business, ranging from financial, reputation, downtime, customer loyalty, and intellectual property theft. Modern organizations are recognizing the need to take a proactive and more holistic approach to monitoring, managing, and protecting their cloud-native applications to prevent security issues and to respond quickly to them if they do occur.

Cloud-native application protection platforms (CNAPPs) are unified and tightly integrated sets of security and compliance capabilities designed to secure and protect cloud-native applications across development and production. CNAPPs consolidate a large number of previously siloed capabilities, including container and configuration scanning, cloud security posture management, infrastructure-as-code scanning, cloud infrastructure entitlement management, runtime vulnerability assessment, and cloud workload protection.

Established security tools and methods created to protect on-premises data centers and endpoints do not necessarily work for a cloud infrastructure, which is a very different architecture. Until recently, securing cloud-native applications was challenging, requiring multiple tools from multiple security vendors that were not typically well-integrated. Without a highly integrated approach, organizations only have a partial view of risk. In addition, those point solutions are often designed by security professionals not in collaboration with developers, which can unintentionally add unnecessary friction and delays to an agile development process. Clearly, cloud-native technologies require a complete lifecycle approach to simplify security, including reducing the number of security vendors.

This paper looks at how a leading-edge CNAPP can solve key challenges that organizations face with cloud-native application environments by providing a centralized platform for managing security policies and controls and by using automation to identify and remediate threats in real time. This single integrated offering identifies risk across the entire lifecycle and the various elements of a cloud-native application and puts the developer at the core of application risk responsibility. In addition to security threats, a CNAPP can provide real-time visibility into application performance and resource utilizations for faster issue resolution. Compliance with regulations such as HIPAA, PCI, and GDPR is another challenge that a CNAPP can address through automated compliance monitoring and reporting and enforcing security policies tied to those regulatory requirements.

A cloud-native application is typically defined as an application that is:

- Architected using loosely coupled microservices, interacting via APIs.
- Developed within a DevOps-style continuous integration/continuous delivery (CI/CD) pipeline with frequent updates.
- Often built using Linux containers with Kubernetes-based orchestration, supplemented with serverless functions, and platform-as-a-service (PaaS) services from a cloud provider.
- Deployed onto a cloud infrastructure.
- Updated frequently.
- Managed so that all changes are made through the development pipeline (with few or no changes to production workloads).

Introduction

CNAPP offerings integrate visibility, assessment, and remediation for modern, agile organizations leveraging DevOps strategies that need to address unknown and unexpected risks. These risks arise from the increased complexities that emerge at the intersection of automation, deployment, and orchestration of cloud-native applications. The core value of CNAPPs is their ability to identify security issues and vulnerabilities earlier in the development cycle, accelerate their remediation, and provide consistent and continuous security and compliance monitoring.

Most CNAPPs are cloud-based, as-a-service offerings, with integration into the runtime cloud environments and development pipeline tools used by the development organization. CNAPP solutions deliver an integrated set of capabilities spanning runtime visibility and control, cloud security posture management (CSPM) capabilities, software composition analysis capabilities, and container scanning. Additional capabilities may include API testing and monitoring, traditional static application security testing/dynamic application security testing, runtime web application, and API protection.

What is a CNAPP?

A CNAPP is a unified and tightly integrated set of security and compliance capabilities designed to secure and protect cloud-native applications across development and production.

CNAPPs consolidate a large number of previously siloed capabilities, including:

- Container scanning.
- Cloud security posture management.
- Infrastructure-as-code scanning.
- Cloud infrastructure entitlement management.
- Runtime cloud workload protection and runtime vulnerability.
- Configuration scanning.

A leading-edge CNAPP solution is a cloud security solution that provides full-stack security through three or more main components:

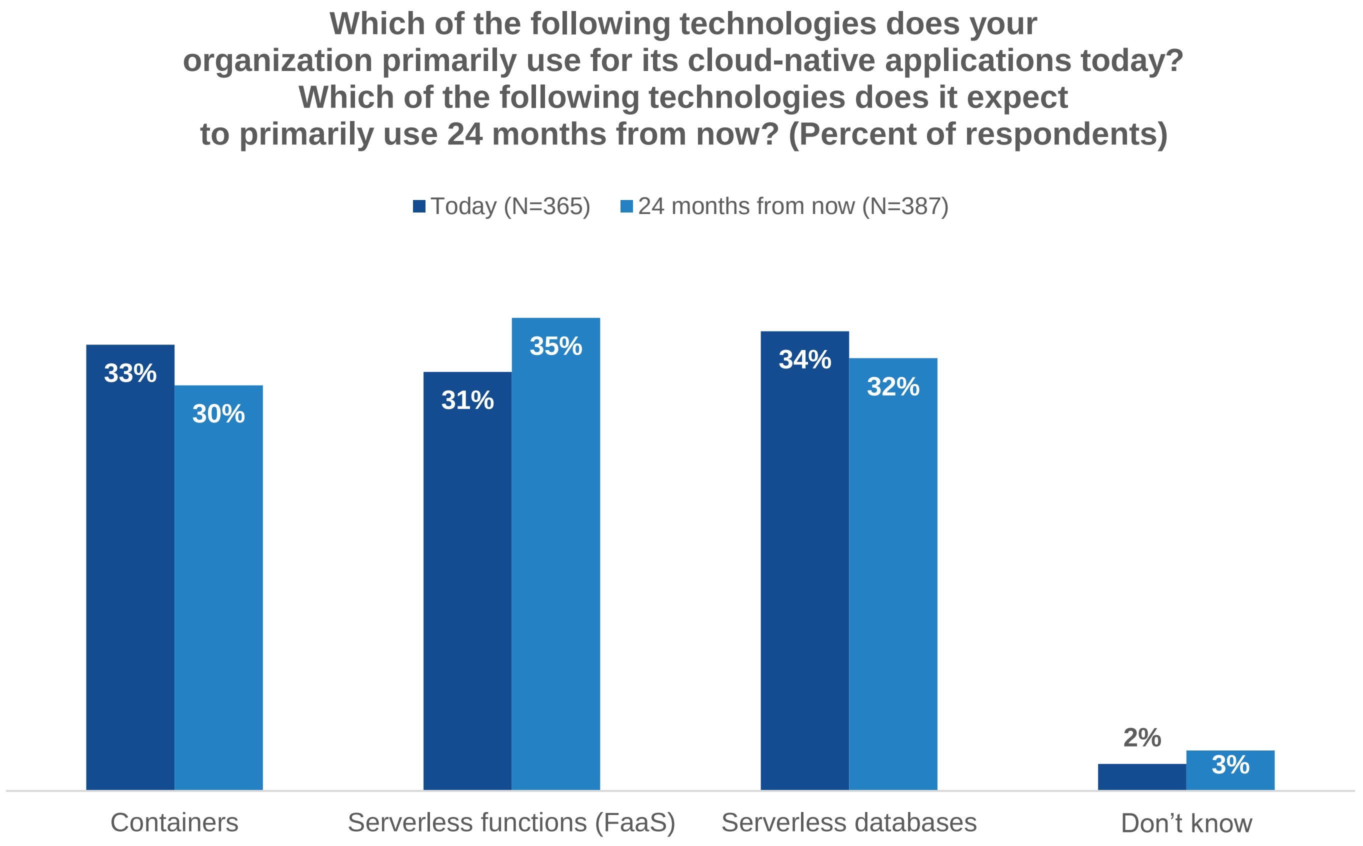
- **CSPM** monitors, identifies, and alerts organizations to compliance risks and misconfigurations in cloud environments, and remediates those risks.
- **Kubernetes security posture management** is a CSPM designed to scan, monitor, benchmark, and test Kubernetes environments and configurations.
- **Cloud workload protection platform** (CWPP) provides visibility and control for physical and virtual machines as well as containers and serverless workloads across hybrid and multi-cloud environments.
- **Cloud service network security** protects cloud infrastructure in real time through web application firewalls, web and API protection, DDOS defense, and load balancing.
- **Cloud infrastructure entitlement management** mitigates risks from public cloud data breaches by continuously monitoring permissions and activities.

Simplify Cloud-native Application Management

Cloud-native applications are typically built using a microservices architecture, which can be complex to deploy and manage. These applications consist of many independent services that need to be deployed, monitored, and managed separately, sometimes across multiple clouds, which can make it difficult to get a complete picture of the application's overall health.

According to research from TechTarget’s Enterprise Strategy Group on cloud-native applications, most respondents (89%) said providing developer-ready infrastructure is essential for application deployment, with more than one in five categorizing it as critical.[1] When respondents were asked about the kind of infrastructure their organization primarily used for its cloud-native applications, it was roughly evenly split, with 33% using containers, 31% using serverless functions (such as framework-as-a-service), and 34% using serverless databases (see Figure 1).[2] Looking ahead, not much change is expected. Because developers are creating containers, serverless functions, and cloud infrastructure, CNAPP tooling needs to "shift left" into the development lifecycle in addition to providing comprehensive runtime visibility. Shifting risk visibility left requires a deep understanding of the development pipeline and artifacts and an extension of vulnerability scanning earlier into the development pipeline as these artifacts are being created.

Figure 1. Infrastructure Used for Cloud-native Applications



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

A CNAPP can simplify an IT environment in several ways:

- **Centralized management**: CNAPPs provide a centralized platform for managing security policies and controls, which can simplify the management of cloud-native applications. This "single pane of glass" can reduce the need for manual intervention and improve the efficiency of IT operations.
- **Automated security**: CNAPPs use automation to identify and remediate security threats in real time, which can reduce the workload of IT teams and improve the speed and accuracy of threat detection and response.
- **Unified visibility**: CNAPPs provide real-time visibility into application performance, resource utilization, and security threats, which can help IT teams to quickly identify and resolve issues. This unified visibility can

[1] Source: Enterprise Strategy Group Research Report, *Cloud-native Applications*, May 2022.
[2] Ibid.

simplify the management of cloud-native applications by providing a single pane of glass for monitoring and management.

- **Compliance monitoring and reporting**: CNAPPs can provide automated compliance monitoring and reporting, which can simplify compliance management and reduce the risk of non-compliance. This can help organizations to meet regulatory requirements and avoid fines and legal action.
- **Simplified deployment and scaling**: CNAPPs can automate tasks such as provisioning, deployment, and scaling, which can simplify the management of cloud-native applications. This can reduce the workload of IT teams and improve the efficiency of IT operations.

As CNAPPs simplify the cloud-native environment, improve the efficiency of IT operations, and reduce the workload for IT staff, they enable the organization to focus on higher value activities.

Tighten Application Security and Simplify Compliance

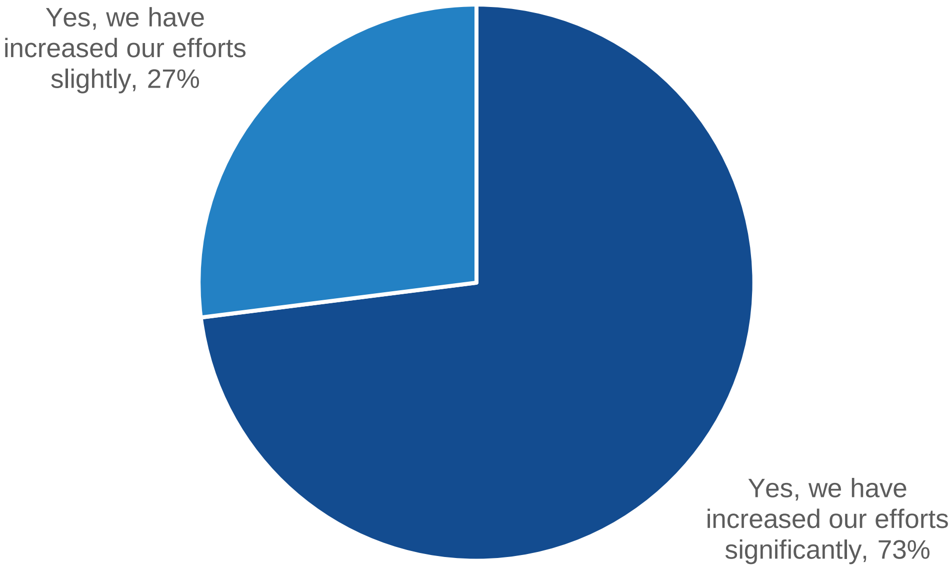
New cloud-native architectures enable teams to develop and deploy software more quickly to keep up in a fast-paced marketplace. However, this speed is not without risk to security.

In a cloud-native application development and deployment environment, containers are used to package and deploy applications. This can introduce new security challenges because containers can be vulnerable to attack, such as the injection of malicious code being injected if not properly secured. Kubernetes uses APIs to manage and orchestrate container deployments, which can also be vulnerable to attackers who are trying to gain access to the Kubernetes cluster and the containers running on it. In addition, the complex network architecture used to manage container communication can be difficult to secure. To manage access to containers and the cluster, Kubernetes also requires complex identity and access management that can lead to unauthorized access if not configured correctly. Organizations need to take proactive steps to secure their Kubernetes deployments, such as implementing security controls, conducting regular vulnerability assessments, and ensuring compliance with regulatory requirements. Enterprise Strategy Group research shows that most organizations have increased their efforts to secure open source software, containers, and third-party software components (see Figure 2).[3]

[3] Source: Enterprise Strategy Group Research Report, *Walking the Line: GitOps and Shift Left Security*, November 2022.

Figure 2. Most Organizations Have Increased Efforts to Secure Open Source Software, Containers, and Third-party Software Components

Has your organization increased its efforts to secure open source software, container images, and third-party software components as a result of recent software supply chain attacks (e.g., Log4j, SolarWinds, Kaseya, etc.)? (Percent of respondents, N=350)

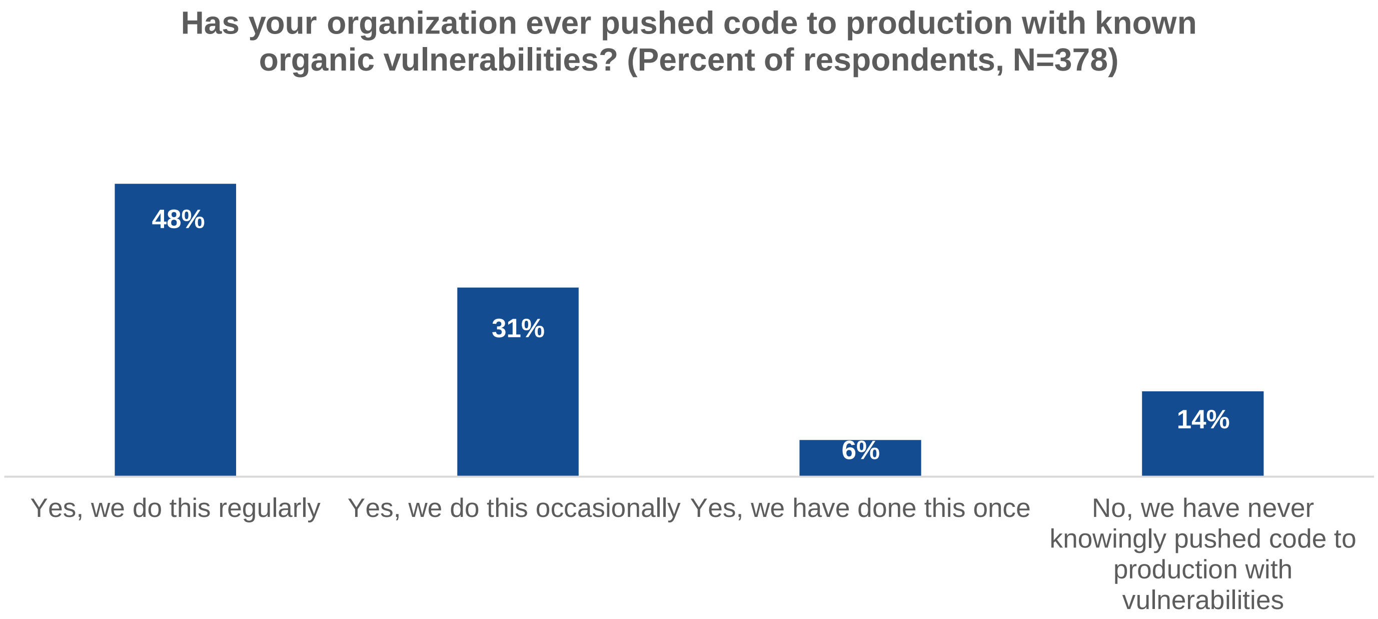


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

In spite of these efforts, organizations are under a lot of pressure to optimize and move quickly when it comes to releasing code. As a result, according to Enterprise Strategy Group research, many developers are pressured to push code to production, even with known vulnerabilities, to meet deadlines (see Figure 3).[4]

[4] Source: Enterprise Strategy Group Research Report, *Securing Modern Application Environments*, December 2020.

Figure 3. Almost Half of Developers Surveyed Say They Regularly Push Code to Production with Known Vulnerabilities

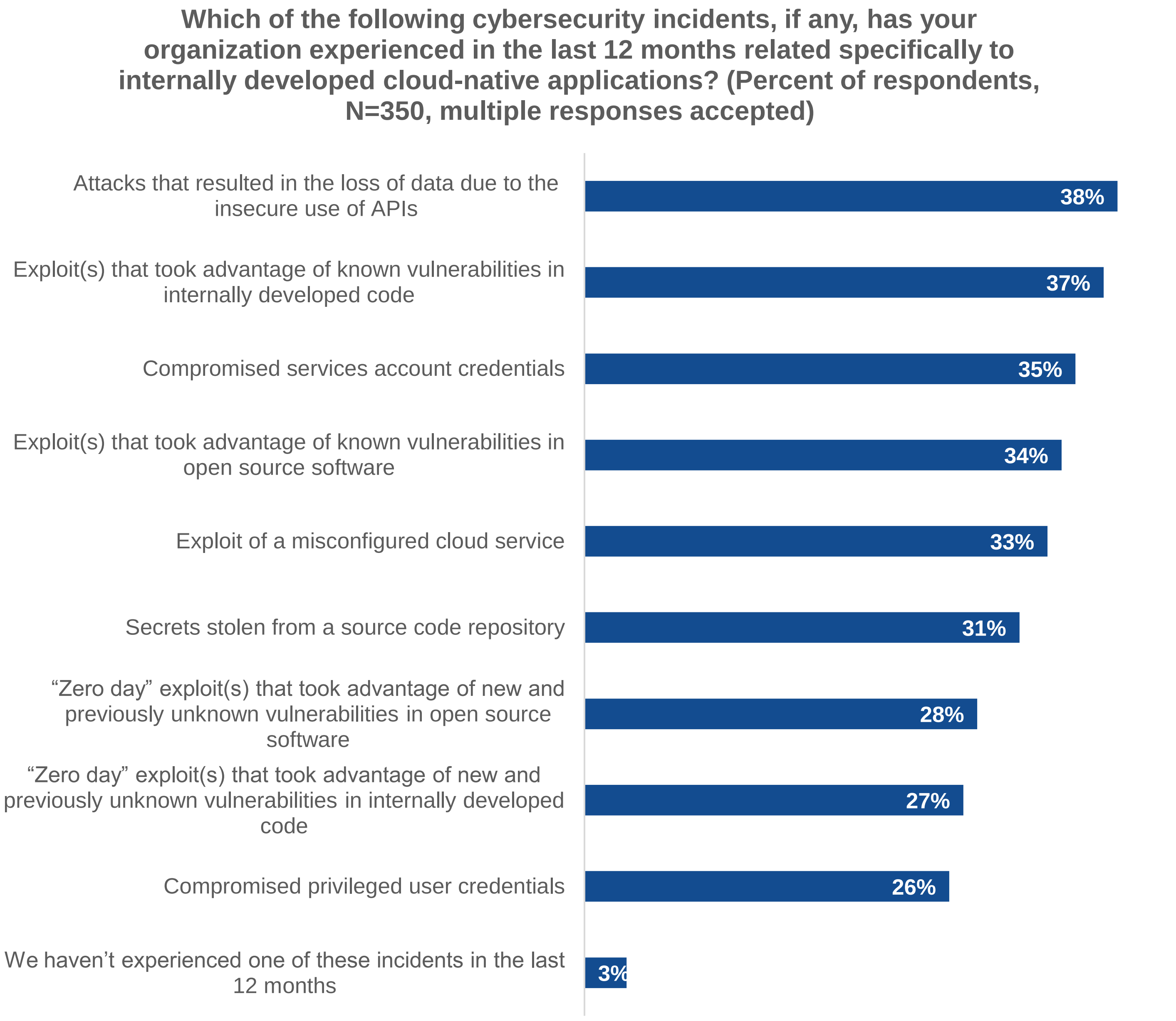


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Compounding this internal vulnerability, decentralized cloud-native architectures mean the attack surfaces are increasing. In addition, changes in the computing landscape have raised the risk of catastrophic security breaches. Attackers are targeting the misconfiguration of cloud infrastructure (network, compute, storage, identities, and permissions), APIs, and the software supply chain itself. Enterprise Strategy Group research shows 97% of organizations said they had experienced a cybersecurity incident related to internally developed cloud-native applications in the previous 12 months (see Figure 4).[5]

[5] Source: Enterprise Strategy Group Research Report, *Walking the Line: GitOps and Shift Left Security*, November 2022.

Figure 4. Types of Cybersecurity Incidents Related to Internally Developed Cloud-native Applications in the Previous 12 Months



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Security is often viewed as an obstacle to developers, so it is critical to prioritize identified risks and provide sufficient context for the developer to remediate them. CNAPP offerings bring together multiple security and protection capabilities into a single platform focused on identifying and prioritizing excessive risk of the entire cloud-native application and its associated infrastructure. As developers become increasingly responsible for operational tasks, such as addressing vulnerabilities, deploying infrastructure-as-code, and managing lifecycle implementations in production, they require tools that address this expanded scope.

In the same way that Kubernetes open source software needs to be considered as a source of vulnerability, developer-ready infrastructure, such as serverless functions, databases, and containers, needs to be considered a source of vulnerability, as well.

Improve Operational and Cost Efficiencies

A CNAPP enables a streamlined approach to security and compliance testing. By integrating testing transparently into modern DevOps (to DevSecOps), developers are able to balance security and speed in a way that doesn't unnecessarily slow down innovation, freeing developers to innovate at their desired speed with little or no friction from security unless a critical risk issue is identified. With faster testing speed comes reduced developer cost and faster speed to market.

Using a CNAPP supports a DevSecOps CI/CD pipeline by providing insights throughout the development cycle and learning from the production environment. Because risk analysis is integrated throughout cloud-native development, teams can improve not only their application's overall security posture but that of the larger team and enterprise. As lines between environments and teams blur further, a CNAPP provides an end-to-end cloud-native solution that seamlessly addresses security concerns in one source of truth and transforms an organization's IT team into a more cost-effective, efficient engine.

At a Glance: What to Look for in a CNAPP

A CNAPP should provide the following benefits:

Complete Visibility across Multi-cloud Infrastructures

A CNAPP should work across all applications, microservices, APIs, and cloud resources deployed and provide the needed level of artifact and exposure scanning. It should provide a single dashboard that spans all public cloud service providers. The platform should also prioritize mitigation, reporting on the automated steps available, as well as the actions that should be handled manually.

True "Shift Left" DevSecOps

A cloud-native application protection platform enables threat and vulnerability detection earlier in the software development lifecycle. This allows for actions to be taken earlier in the development engineering process. Alerts and data visualizations should be easy to set up and change and should trigger automated and/or manual mitigation activities.

Facilitate End-to-end Cloud Security Governance

A CNAPP should easily detect and manage vulnerabilities and security misconfigurations but also carry out runtime protection, network-based behavioral monitoring, automated compliance and governance over data, identity-based controls, and configurations.

Introducing Panoptica by Cisco

The implementation of a cloud-native application protection platform allows organizations to address development, runtime, and compliance issues as a continuum across development and operations. Additionally, it brings together insights from a wide range of data sources, visualizing those risks that should be prioritized for development, operations, and security teams. Panoptica is a leading-edge CNAPP that makes it easy to secure containers. It integrates Panoptica's core security capabilities from each stage of the software development lifecycle in unique, DevOps-friendly ways to allow IT teams to continue to innovate rapidly while allowing cloud security to scale along with the speed and complexities of their cloud-native applications.

Panoptica Overview

Panoptica offers the following sets of tools and technologies:

CWPP

Enterprises can only secure what they can 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 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 rank them by a risk score to ensure up-to-date coverage. Risk scores help set policies and specify which workloads are compliant and authorized for deployment.

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

Attack Path Analysis

Panoptica's secure assets menu lists all of the types of assets inventoried and scanned across the application domain. All of these specific elements of information are useful and necessary for security teams but can represent a massive amount of scoring and alerts that require time and attention to act on and prioritize for DevOps and SRE teams to fix. The attack path is the best way to prioritize risks and focus on the paths most likely to be exploited. When selecting a given attack path, it is flattened and can be viewed with corresponding vulnerability elements alongside detailed attack flow steps.

Infrastructure as Code (IaC) Security

With IaC, organizations can manage and provision their cloud infrastructure using code, allowing them to automate the deployment and configuration of their cloud resources. IaC scanning is key to ensuring cloud infrastructure code is secure from the start. Panoptica shifts an organization's security testing to the left by enabling the 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 get insights in real time 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. Panoptica also offers secrets and supply chain security with software bill of materials generation during code/build.

API Security

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 teams 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 an organization's declarative policies. It helps Ops teams perform fuzz testing and spec analysis and reconstruct specs that are broken. It can also establish policies that govern which API calls the gateway will permit based on specific app components. In addition, Panoptica lets risky APIs that don't adhere to specifications be disabled.

Panoptica benefits include:

- **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 analyzes risks from multiple touchpoints throughout the software development lifecycle 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 private, public, and hybrid multi-cloud environments.
- **Tighter end-to-end security controls:** Panoptica integrates with the CI/CD toolchains DevOps teams already use and provides add-on integrations with AppDynamics for full stack observability, Cisco SecureX, and Cisco Cloud Analytics platforms.
- **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 and more time for security priorities.

Conclusion

Cisco Panoptica offers unique features and value to protect today's expanded and complex application architectures. The decision to move to a "shift left" mentality with DevSecOps and modern data security focuses on protecting applications that run on containers, workloads, and microservices, which are foundational to cloud-native development. CNAPPs identify security issues and vulnerabilities earlier in the development cycle, accelerate their remediation, and offer consistent and continuous security and compliance monitoring.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

About Enterprise Strategy Group
Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community. © TechTarget 2023.

✉ contact@esg-global.com
🖥 www.esg-global.com