Cloud-Native Application Security: An Integrative CNAPP Approach from Cisco

Carlos Pereira, Fellow and Chief Architect, Cisco
@capereir

Melinda Marks, Senior Analyst, Enterprise Strategy Group (ESG)
@melindamarks

BRKAPP-1115

#CiscoLive
Cisco Webex App

Questions?
Use Cisco Webex App to chat with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App (BRKAPP-1115)
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 9, 2023.

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKAPP-1115
Agenda

• ESG analyst’s view of CNAPP – what is it and what are the key concerns of the customer?

• Cisco’s Chief Architect view on an integrated cloud native application security offering and its use-case
“Use of Cloud-Native Technologies Will Be Pervasive, not Just Popular”

“More than 85% of organizations will embrace a cloud-first principle by 2025 and will not be able to fully execute on their digital strategies without the use of cloud-native architectures and technologies”

- Gartner
The Need for An Effective Cloud-native Security Platform

Melinda Marks, Senior Analyst, Enterprise Strategy Group (ESG)
Moving Production Workloads to Public Clouds

Percentage of production server workloads run on public cloud infrastructure services.

- Percentage of production workloads run on public cloud infrastructure services today (N=359)
- Percentage of production workloads run on public cloud infrastructure services 24 months from now (N=383)

NEARLY 1 IN 7 respondents reported that more than 40% of their organization’s applications run on public cloud infrastructure, which is expected to more than double two years from now.
Multi-Cloud Adoption

Number of unique public cloud infrastructure service providers currently in use.

<table>
<thead>
<tr>
<th>Number of CSPs</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5%</td>
</tr>
<tr>
<td>2</td>
<td>25%</td>
</tr>
<tr>
<td>3</td>
<td>39%</td>
</tr>
<tr>
<td>4</td>
<td>21%</td>
</tr>
<tr>
<td>5</td>
<td>6%</td>
</tr>
<tr>
<td>6</td>
<td>2%</td>
</tr>
<tr>
<td>More than 6</td>
<td>1%</td>
</tr>
</tbody>
</table>

How organizations use services from multiple CSPs.

- 31% We use multiple IaaS or PaaS CSPs in a meaningful way.
- 69% We have one primary IaaS or PaaS CSP and use other IaaS or PaaS CSPs for small, discrete purposes.
# Reaping the Benefits of Moving to the Cloud

<table>
<thead>
<tr>
<th>Area</th>
<th>Very positive impact</th>
<th>Slightly positive impact</th>
<th>No impact</th>
<th>Don’t know/too soon to say</th>
</tr>
</thead>
<tbody>
<tr>
<td>Efficiency in package deployment</td>
<td>57%</td>
<td>37%</td>
<td>6%</td>
<td></td>
</tr>
<tr>
<td>Ability to identify errors earlier in the software development lifecycle</td>
<td>56%</td>
<td>40%</td>
<td>3%</td>
<td></td>
</tr>
<tr>
<td>Efficiency in code review and collaboration cycles</td>
<td>55%</td>
<td>38%</td>
<td>6%</td>
<td></td>
</tr>
<tr>
<td>Speed of development</td>
<td>53%</td>
<td>40%</td>
<td>6%</td>
<td></td>
</tr>
<tr>
<td>Efficiency in onboarding new team members</td>
<td>53%</td>
<td>38%</td>
<td>9%</td>
<td></td>
</tr>
<tr>
<td>Efficiency during schema deployment</td>
<td>52%</td>
<td>41%</td>
<td>7%</td>
<td></td>
</tr>
</tbody>
</table>

**Question text:** What kind of impact has cloud-native application development had on your organization's application development strategy in the following areas? (Percent of respondents, N=251)
## Top Challenges for Cloud-Native Applications: Security

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>34%</td>
</tr>
<tr>
<td>Meeting and maintaining compliance requirements</td>
<td>30%</td>
</tr>
<tr>
<td>Lack of performance monitoring/observability</td>
<td>29%</td>
</tr>
<tr>
<td>Services purchased outside the purview of IT or other authorized decision makers</td>
<td>29%</td>
</tr>
<tr>
<td>Retaining full-featured functionality and capabilities</td>
<td>27%</td>
</tr>
<tr>
<td>Performance</td>
<td>26%</td>
</tr>
<tr>
<td>Managing costs</td>
<td>26%</td>
</tr>
<tr>
<td>Lack of resources and skills</td>
<td>25%</td>
</tr>
<tr>
<td>Lack of full automation of CI/CD pipeline integration</td>
<td>25%</td>
</tr>
<tr>
<td>API incompatibilities</td>
<td>25%</td>
</tr>
<tr>
<td>Managing across multiple clouds</td>
<td>22%</td>
</tr>
<tr>
<td>QA and testing</td>
<td>21%</td>
</tr>
<tr>
<td>Organizational barriers</td>
<td>21%</td>
</tr>
<tr>
<td>Complexity</td>
<td>19%</td>
</tr>
<tr>
<td>We don’t have any challenges</td>
<td></td>
</tr>
</tbody>
</table>

**Question text:**
What are the biggest challenges your organization has faced, or expects to face, with its cloud-native applications? (Percent of respondents, N=387, multiple responses accepted)
Security Challenges
Keeping Up with Faster Development Cycles

65% of organizations have more than 50 git repositories.

- Software is released without going through security checks and/or testing: 45%
- Security lacks visibility and control in development processes: 43%
- Lack of consistency of security processes across different development teams: 36%
- New builds are deployed to production with misconfigurations, vulnerabilities, and other security issues: 35%
- Security team can't keep pace with release cadences: 34%
- Developers are skipping security processes: 32%
- Developers don't want to work with security: 29%
Biggest Security Challenges: Around Scale

- Maintaining security consistency across our own data center and public cloud environments where our cloud-native applications are deployed: 30%
- Overly permissive service accounts: 26%
- Manual security practices and processes cannot keep pace with cloud-native application development and delivery: 25%
- Overly permissive user accounts: 25%
- Our application development and DevOps teams do not involve our cybersecurity team due to fear of being slowed down: 24%
- Customizing best practices or creating custom policies/rules that are tailored for our business: 24%
- Monitoring Kubernetes clusters for misconfigurations/vulnerabilities: 23%
- Our development and DevOps teams do not have a clear understanding of cloud security requirements: 22%
- Lack of visibility into public cloud infrastructure hosting our cloud-native applications: 22%
- Meeting prescribed best practices for the configuration of cloud-resident workloads and services: 20%
- Managing role-based access control (RBAC) for Kubernetes environments: 18%
- Lack of understanding of the threat model for our cloud-native applications and infrastructure: 18%
Cloud Application Security Incidents

- Attacks that resulted in the loss of data due to the insecure use of APIs, 38%
- Exploit(s) that took advantage of known vulnerabilities in open source software, 34%
- "Zero day" exploit(s) that took advantage of new and previously unknown vulnerabilities in open source software, 28%
- Exploit(s) that took advantage of known vulnerabilities in internally developed code, 37%
- Exploit of a misconfigured cloud service, 33%
- "Zero day" exploit(s) that took advantage of new and previously unknown vulnerabilities in internally developed code, 27%
- Compromised services account credentials, 35%
- Secrets stolen from a source code repository, 31%
- Compromised privileged user credentials, 26%
Incidents from Misconfigurations

Top five issues associated with misconfigured cloud applications/services over the last 12 months:

- 30% Externally facing server workloads
- 27% Overly permissive user accounts
- 23% Misconfigured security group permitting traffic to/from IP addresses that are not safe-listed
- 22% Overly permissive service accounts
- 22% Unprotected cloud secrets

Results of misconfigured cloud application or service:

- The introduction of crypto-jacking malware to mine cryptocurrency: 42%
- Remediation steps impacted service level agreements (SLAs): 39%
- Unauthorized access to applications and data: 36%
- Fine(s) due to non-compliance with an industry regulation: 35%
- The introduction of malware: 34%
- The introduction of ransomware: 32%
- Data loss: 27%
Driving Efficiency with a Platform Approach
## Managing Risk: Top 5 Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration with DevOps tools to enable DevSecOps use cases without disrupting developer experiences or workflows</td>
<td>28%</td>
</tr>
<tr>
<td>Deployment flexibility</td>
<td>28%</td>
</tr>
<tr>
<td>Ability to automate security posture management processes at scale</td>
<td>28%</td>
</tr>
<tr>
<td>Cloud infrastructure entitlement management (CIEM) functionality</td>
<td>25%</td>
</tr>
<tr>
<td>Breadth and depth of visibility into cloud services configuration and cloud activity</td>
<td>25%</td>
</tr>
<tr>
<td>Ability to procure via the marketplace of major cloud service providers and single billing</td>
<td>23%</td>
</tr>
<tr>
<td>Support for all types of servers and compute platforms</td>
<td>23%</td>
</tr>
<tr>
<td>Centralized access controls</td>
<td>22%</td>
</tr>
<tr>
<td>Security for the orchestration environment</td>
<td>21%</td>
</tr>
<tr>
<td>Consumption-based pricing model that aligns with the pricing of cloud services</td>
<td>21%</td>
</tr>
</tbody>
</table>
Cloud-native Application Protection Platforms (CNAPPPs)

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.

CNAPPPs 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.
What is a CNAPP?

A CNAPP unifies and tightly integrates security and compliance capabilities to secure and protect cloud-native applications across development and production.

Benefits of a Platform Approach

Cloud Native Application Protection Platform (CNAPP)

CNAPPs consolidated a number of previously siloed capabilities, including:

- Container workload protection (CWP)
- Cloud Security Posture Management (CSPM)
- Infrastructure as Code (IaC) scanning
- Cloud Infrastructure Entitlement Management (CIEM)
- Runtime cloud application protection
Using a CNAPP to Drive Efficiency by Consolidating Application Security and Posture Management

A CNAPP helps drive efficiency in connecting application security processes to security posture management

A CNAPP will help give us a consolidated approach for more efficient cloud security risk mitigation

- ESG Report: CSPM/CIEM study
Key CNAPP Attributes

• Enables them to scale security to support rapid development
• Drives efficiency of remediation to stay ahead of security incidents

- A high-level of threat detection efficacy and... 28%
- Support for all types of servers and... 28%
- A rich set of visibility capabilities from... 23%
- Preventative controls for hardening and... 21%
- Support for multiple public cloud... 21%
- Integration with DevOps tools to enable... 19%
- Deployment flexibility (i.e., offered as a... 19%
- Support for the MITRE ATT&CK framework 18%
- Agentless implementation 14%
- Centralizes workload segmentation policies... 14%
- Secures the orchestration environment... 11%
- Consumption-based pricing model that... 8%
- Ability to procure via the marketplace of... 5%
Cloud-Native Application Security from Development to Production: Cisco Panoptica

Carlos Pereira, Fellow and Chief Architect, Cisco
Problem space: What and why

Follow an attack path towards end goal
Goal is to get to Compute, Data or DoS
Attackers can compromise any asset
- APIs, SaaS
- Containers, Functions, VMs
- Configurations and identities
- Tooling

Compilers, CICD, Tooling
Modern cloud-first app
accessed from anywhere
SolarWinds attack path

- Supply chain compromise
  - Build & CICD system compromised

- Initial access, command-and-control
  - Compromised libraries infected in all SW builds

- Hands-on-keyboard attack on premises
  - Infect every node where SW is deployed

- Hands-on-keyboard attack in the cloud
  - Steal credentials and gain admin privileges

Only Cisco can provide e2e protection

- Password guessing
- Use secret key to bypass Duo and access Outlook Web App

Attacker

Initial C2

Second C2
MITRE ATT&CK framework
A Holistic View Towards Cloud App Security

One approach: capabilities for securing modern hybrid cloud apps

- Secures everything you need to worry about for modern apps
- From writing first line of code, to the tools used to produce app, to the app itself, and the cloud resources the app runs on

1. Code & Build Protection: Before the code is even deployed
2. App & API Security: Securing the application and its logic
3. Workload Security: Infrastructure for the app (CWPP++)
4. Cloud Posture: Cloud environment & configs (CSPM++)
Details: Protection from code to production

<table>
<thead>
<tr>
<th>1</th>
<th>Code &amp; Build Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Before the code is even deployed</td>
</tr>
<tr>
<td></td>
<td>- Static Analysis</td>
</tr>
<tr>
<td></td>
<td>- Infra as Code scanning</td>
</tr>
<tr>
<td></td>
<td>- Secrets scanning</td>
</tr>
<tr>
<td></td>
<td>- SSC, SBOM</td>
</tr>
<tr>
<td></td>
<td>- CI/CD Protection</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2</th>
<th>App &amp; API Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Securing the application and its logic</td>
</tr>
<tr>
<td></td>
<td>- API Security</td>
</tr>
<tr>
<td></td>
<td>- Business / app logic security</td>
</tr>
<tr>
<td></td>
<td>- Data Security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3</th>
<th>Workload Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Infrastructure for the app (CWPP++)</td>
</tr>
<tr>
<td></td>
<td>- Container workloads</td>
</tr>
<tr>
<td></td>
<td>- K8s SPM</td>
</tr>
<tr>
<td></td>
<td>- Serverless security</td>
</tr>
<tr>
<td></td>
<td>- VM security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4</th>
<th>Cloud Posture</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cloud environment &amp; configs (CSPM++)</td>
</tr>
<tr>
<td></td>
<td>- CSPM</td>
</tr>
<tr>
<td></td>
<td>- CIEM</td>
</tr>
<tr>
<td></td>
<td>- Cloud Network security</td>
</tr>
</tbody>
</table>
Planned deliverables

- Allows businesses to easily secure their modern hybrid apps by focusing on their most relevant risks across all attack paths from code to cloud.

- Intelligent Prioritization: Using AI/ML to allow SecOps to manage the most critical attack paths in modern apps regardless of attack provenance.

- Solve at Source: Lead with code-centric (shift-left) security - from the creation of the first line of code, through deployment, to production runtime.

- Integrations at Cisco Scale:
  - Cisco Secure: Allows SecOps to secure their entire environment from user to app, and app to app.
  - FSO: Allow a business owner to integrate security risks, in addition to safety risks, in Business Risk Observability.
Planned integrations

- Allows businesses to easily secure their modern hybrid apps by focusing on their most relevant risks across all attack paths from code to cloud.
- Intelligent Prioritization: Using AI/ML to allow SecOps to manage the most critical attack paths in modern apps regardless of attack provenance.
- Solve at Source: Lead with code-centric (shift-left) security – from the creation of the first line of code, through deployment, to production runtime.

Integrations at Cisco Scale:

- **Cisco Secure:** Allows SecOps to secure their entire environment from user to app, and app to app.
- **FSO:** Allow a business owner to integrate security risks, in addition to safety risks, in Business Risk Observability.
Demo
Planned integrations

Allows businesses to easily secure their modern hybrid apps by focusing on their most relevant risks across all attack paths from code to cloud.

Intelligent Prioritization: Using AI/ML to allow SecOps to manage the most critical attack paths in modern apps regardless of attack provenance.

Solve at Source: Lead with code-centric (shift-left) security – from the creation of the first line of code, through deployment, to production runtime.

Integrations at Cisco Scale:

Cisco Secure: Allows SecOps to secure their entire environment from user to app, and app to app.

**FSO:** Allow a business owner to integrate security risks, in addition to safety risks, in Business Risk Observability.
Focused on vulnerabilities & threats

App Team

Focused on velocity & user experience

Security Team
Business can’t afford Security and Applications silos.

Without both teams joining the fight, issues like the log4j JNDI vulnerability can’t be protected against in a timely fashion.
Business Risk Observability for Applications

Provides the business context needed to rapidly assess risk and align teams based on potential Impact

**Business Context Mapping**
Mapping vulnerabilities and attacks to common transactions provides the business context to help you quickly understand the location and impact of threats.

**Vulnerability and Threat Intelligence**
Threat intelligence feeds from multiple yet complementary sources provide the threat context to understand the likelihood of threat exploits.

**Business Risk Scoring**
Scoring composited from analysis of runtime behavior + business impact + intelligence provides complete business risk context to instantly assess and prioritize action across ITOps and SecOps teams.
### Cisco Business Risk Observability in action, NOW!

<table>
<thead>
<tr>
<th>Per business-transaction</th>
<th>Real-time Score: Estimate of the likelihood of exploitation based on what is happening in real-time.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High risk of exploitation with a correlated high business impact. Operator must act due to active nature of threat.</strong></td>
<td><strong>CVSS Score:</strong> Qualitative ratings of Public Disclosed Vulnerabilities</td>
</tr>
<tr>
<td><strong>Differentiate between what’s important versus what’s urgent. High severity, but low likelihood of exploitation or business impact.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Operator often ignore this case due to low CVSS score, but must act because of high business risk and impact potential.</strong></td>
<td></td>
</tr>
</tbody>
</table>

---


- **Kenna Score:** 100
- **CVSS Score:** 9.8
- **Kenna Intelligence:**
  - 3 Active
  - 1 Inactive


- **Kenna Score:** 33
- **CVSS Score:** 9.8
- **Kenna Intelligence:**
  - 3 Active
  - 1 Inactive

#### Vulnerabilities: HTTP Request Smuggling (CVE-2022-42252)

- **Kenna Score:** 64
- **CVSS Score:** 3.7
- **Kenna Intelligence:**
  - 1 Active
  - 3 Inactive

---

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

#CiscoLive BRKAPP-1115

---

36
Extend Cisco’s industry-first and unique Business Risk Observability approach to Cloud native workloads through the Panoptica Integration at the Cisco FSO Platform

The proposed integration of Cisco’s Full Stack Observability (FSO) platform and Panoptica provides security visibility, insights, and actions to protect cloud assets - Kubernetes (K8S), workloads, and business focused application security visibility and control.

This integration is part of the overall Business Risk Observability on Cisco FSO platform, and it has been announced at Cisco Live FY23. The key value proposition will be Cisco Business Risk Observability mapped across the entire modern application stack, including infra security insights and business application data insights to provide prioritized end-to-end security visibility.

Initial integration phase will focus on findings of container vulnerability and Kubernetes workloads.
Business Risk Observability

Use case 1: Threats and Vulnerabilities Across Cloud-Native Kubernetes and Containers

Integrated view on FSO
Detect, prioritize, and address container vulnerabilities and security threats right from your observability dashboard

Factor in business risk
Combine findings into your application context for business-level risk scoring

Announce: Cisco Live June GA: August ‘23
Business Risk Observability

Use case 2: Prioritize and align across security issues based on business context

Create your own customized view of security risk

Changes in security & app graphs are evaluated to reflect real-time risk

Prioritize remediation and mitigation efforts by what matters to the biz

Announce: Cisco Live June GA: August ’23
What’s next?
Next Steps: Start Using Panoptica for free

Simplified Cloud-Native Application Security for DevSecOps, Platform, and DevOps teams

Panoptica makes it easy to secure your containers, APIs, and serverless functions, and manage software bills of materials.

Panoptica.app
Continue Your Cloud Native Security Learning

Emerging Technologies & Incubation

Cloud Native Security

Explore why a new approach to security is needed for cloud native applications and learn how Cisco is meeting these rapidly evolving security requirements.
Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

**These points** help you get on the leaderboard and increase your chances of winning daily and grand prizes.
Continue your education

• Visit the Cisco Showcase for related demos

• Book your one-on-one Meet the Engineer meeting

• Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

• Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand
Gamify your Cisco Live experience!
Get points for attending this session!

How:
1. Open the Cisco Events App.
2. Click on ‘Cisco Live Challenge’ in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:
Thank you