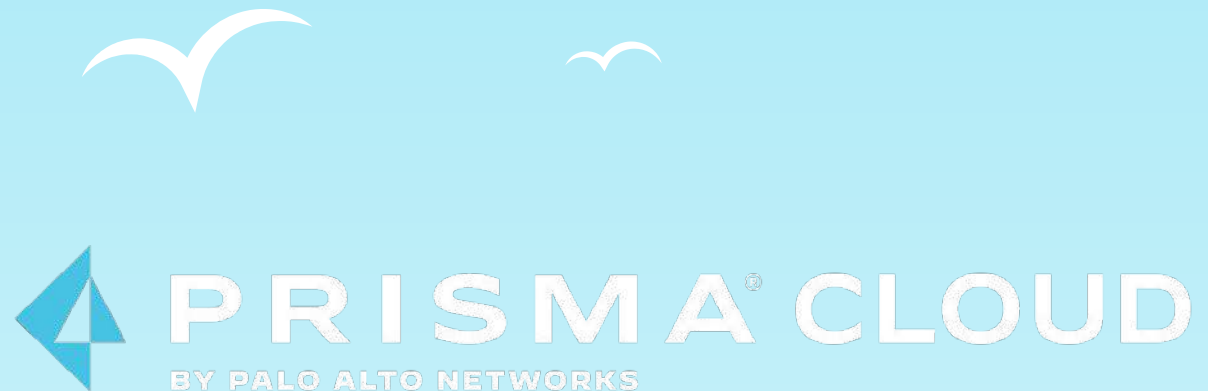




CNAPP y su rol en la Seguridad de Datos



Agenda : Today's Objectives

- 1 State of the Market and Trends**
- 2 Why move to Cloud and how app dev changed?**
- 3 Introduction to the CNAPP market category**
- 4 Prisma Cloud overview**



READY FOR TAKEOFF



Luis Castro

| Presenter Name

**Solutions Architect Manager
Prisma Cloud**

| Title

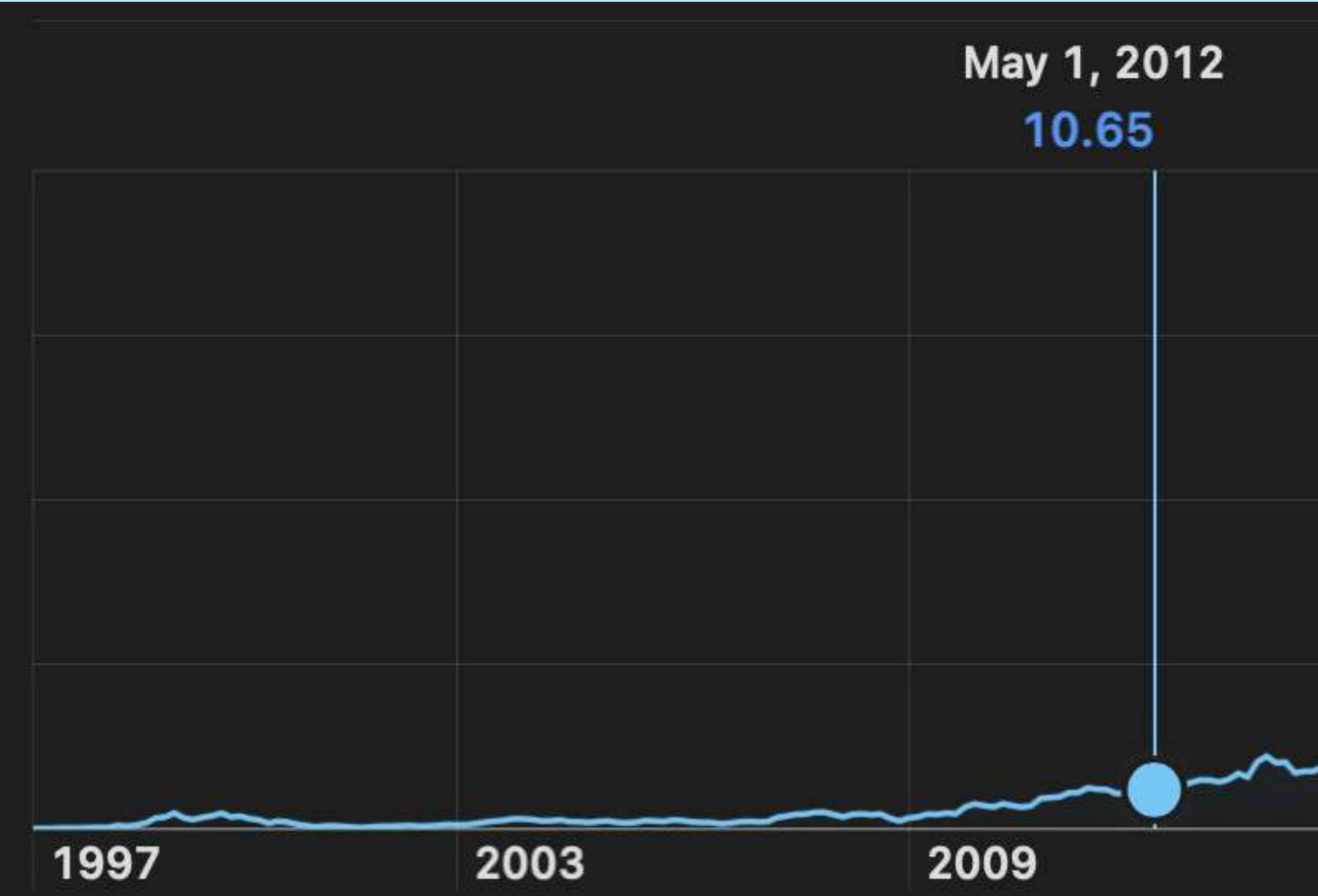
BOARDING PASS



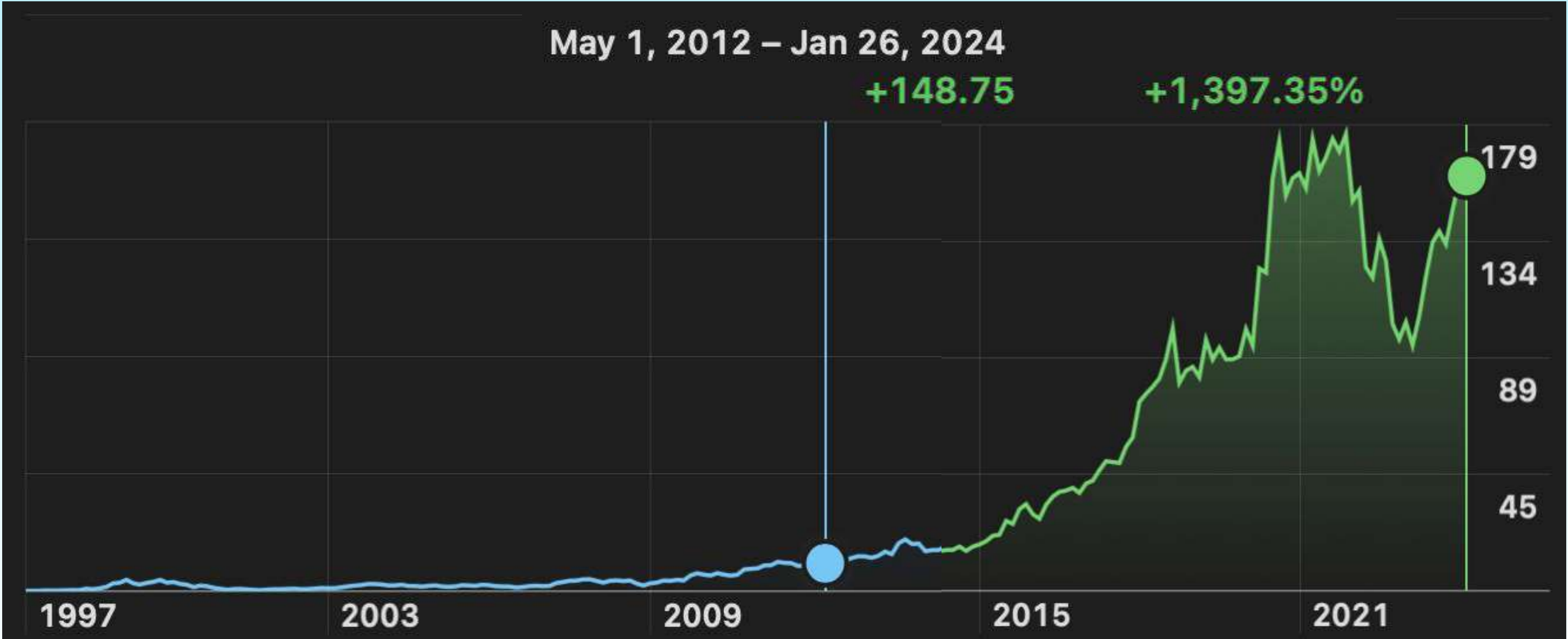
STATE OF THE MARKET



What stock is this?



What stock is this?



C N A P P

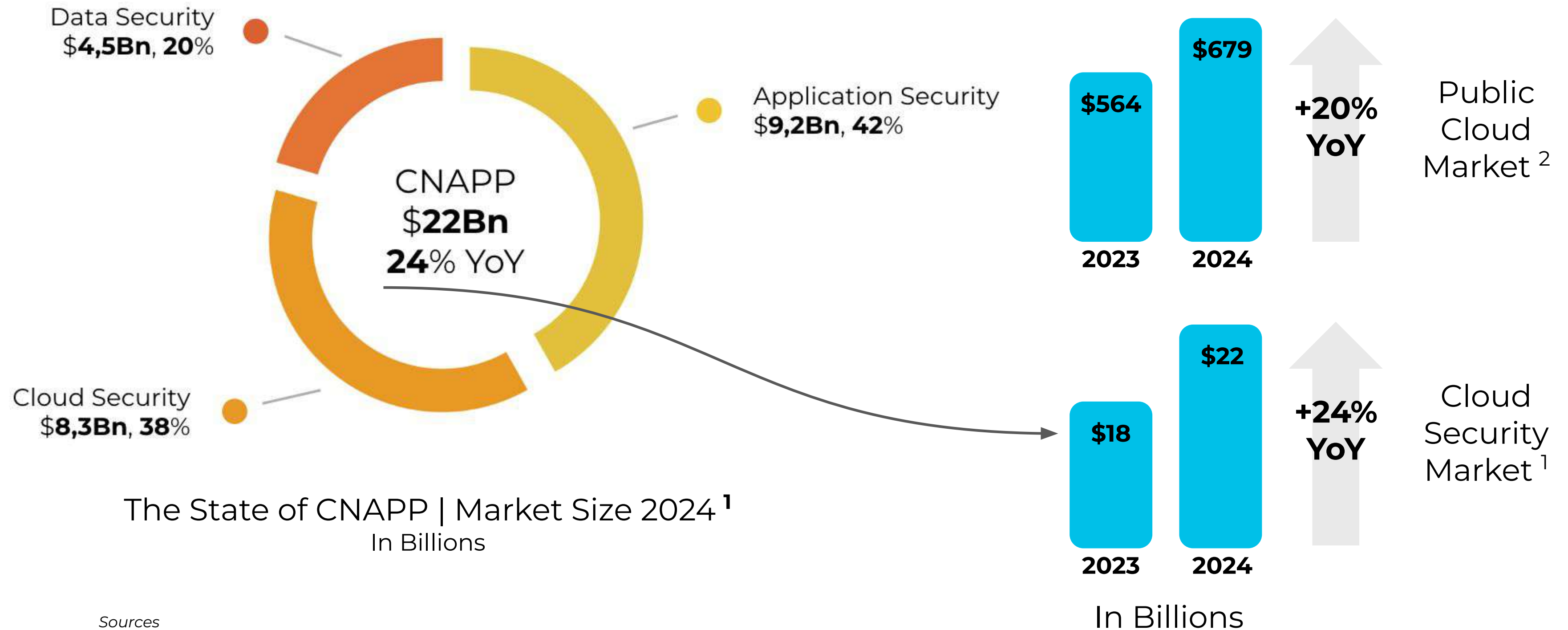
cloud-native

application protection

platform

Brought to you by **Gartner**®

CLOUD SECURITY - RAPID MARKET GROWTH



Sources

¹ Gartner: Infosec Forecast 2020 - 2026 4Q22 Update

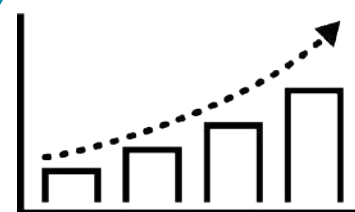
² Gartner: Public Cloud Services, Worldwide, 2021-2027, 3Q23 Update

CLOUD SECURITY

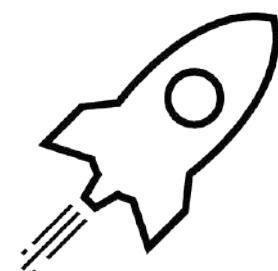




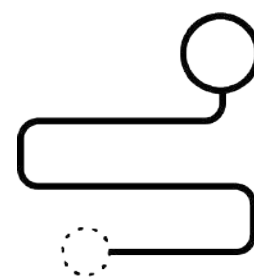
Speed, Cost and Innovation are the driving force of Cloud Adoption



**Building new
and expanding
existing products
and services**



**Increasing
efficiency and
agility**



**Creating new
processes and
workflows**



**Mitigating
business and
regulator risk**



**Expanding into
new markets**

Source:
State of Cloud Native Security Report 2023

CLOUD AND APPLICATION LANDSCAPE IS CHANGING

**3 out
of 5**

incidents in Cloud are
application specific ¹

**Legacy security solutions are
unfit to protect cloud and
cloud-native applications**

77%

of enterprises are
deploying code to
production weekly ¹

**Developers are moving fast and
security teams are left behind**

63%

of production environments
have unpatched
vulnerabilities ²

**The attack landscape
intensifies**

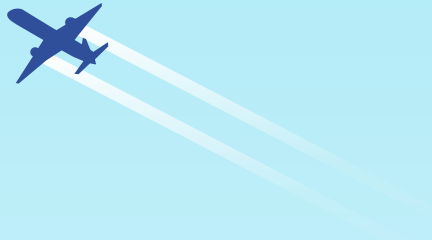
Sources:

1 State of Cloud Native Security Report 2023

2 Unit 42 Cloud Threat Report, Volume 7 2023



Public Cloud Security is a shared responsibility



Organization



Responsible
for security **in**
the cloud

Applications
Code Supply Chain
Data
Identity
Cloud Infrastructure



**Organization's
Responsibility**



Cloud Service Provider



Responsible
for security **of**
the cloud

Routers	
Switches	Hypervisor
Hubs	
Data Center	



**Cloud Service
Provider's
Responsibility**

CN

cloud-native

What is cloud-native?

AP

application protection

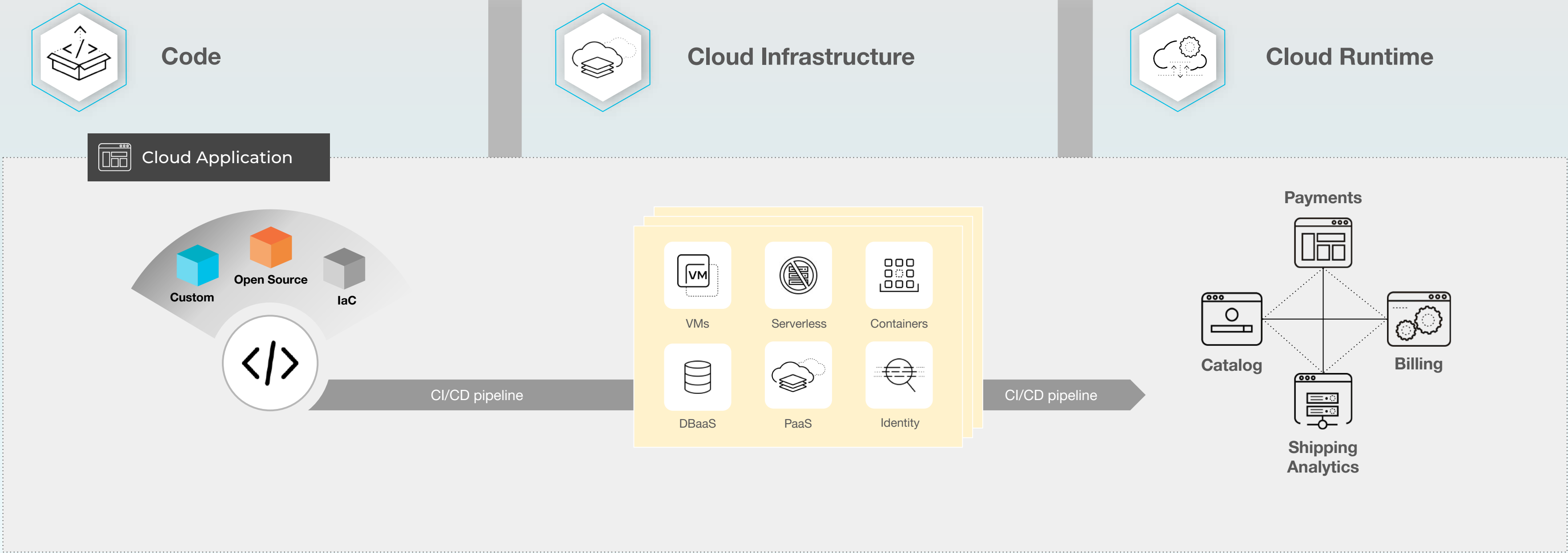
Weren't applications protected in the past, what changed?

P

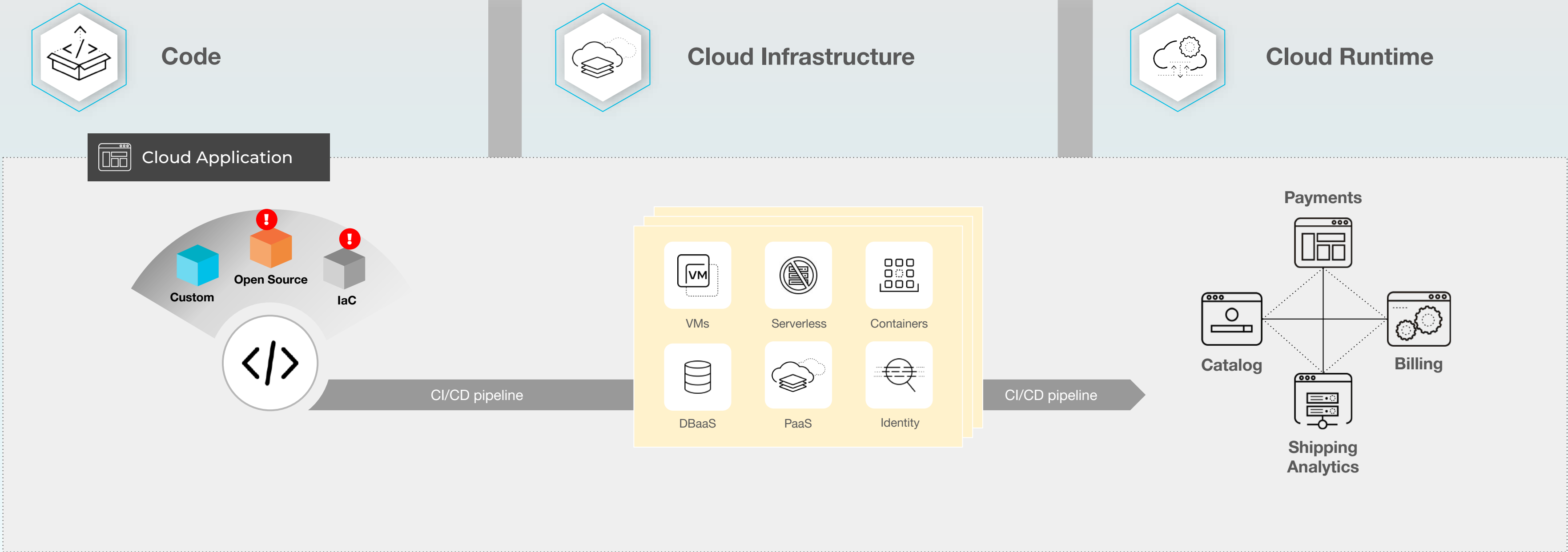
platform

Why is platform important?

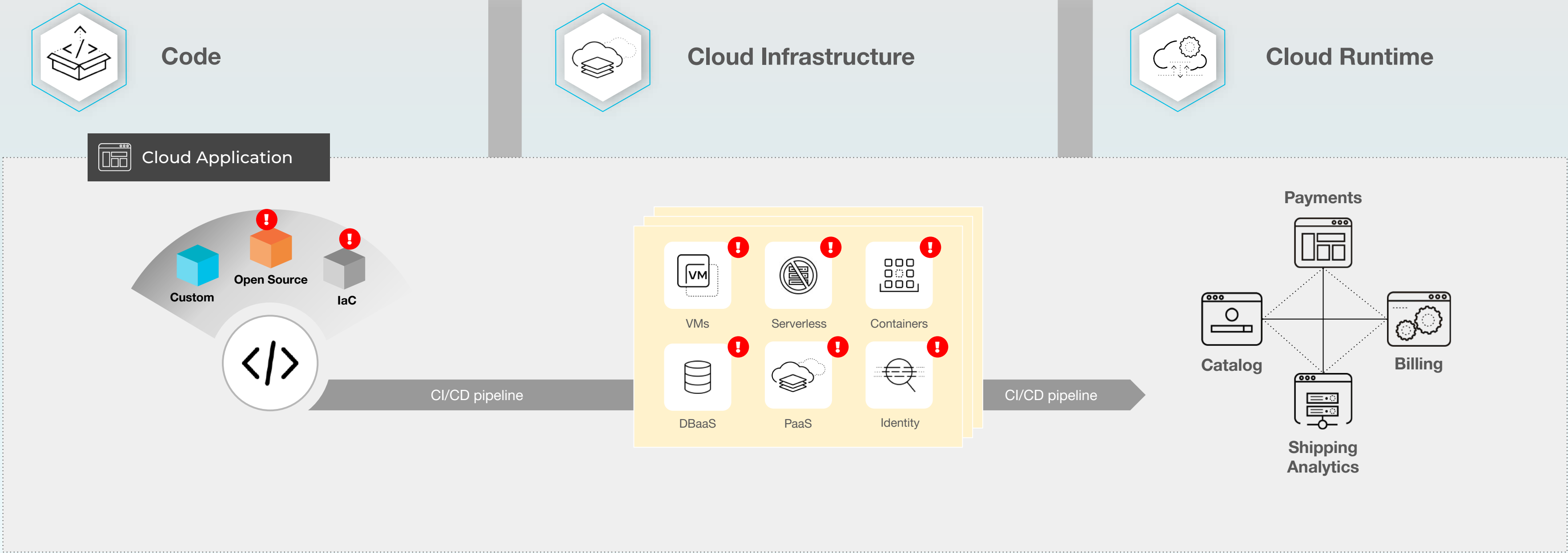
Everything Cloud Starts as Code



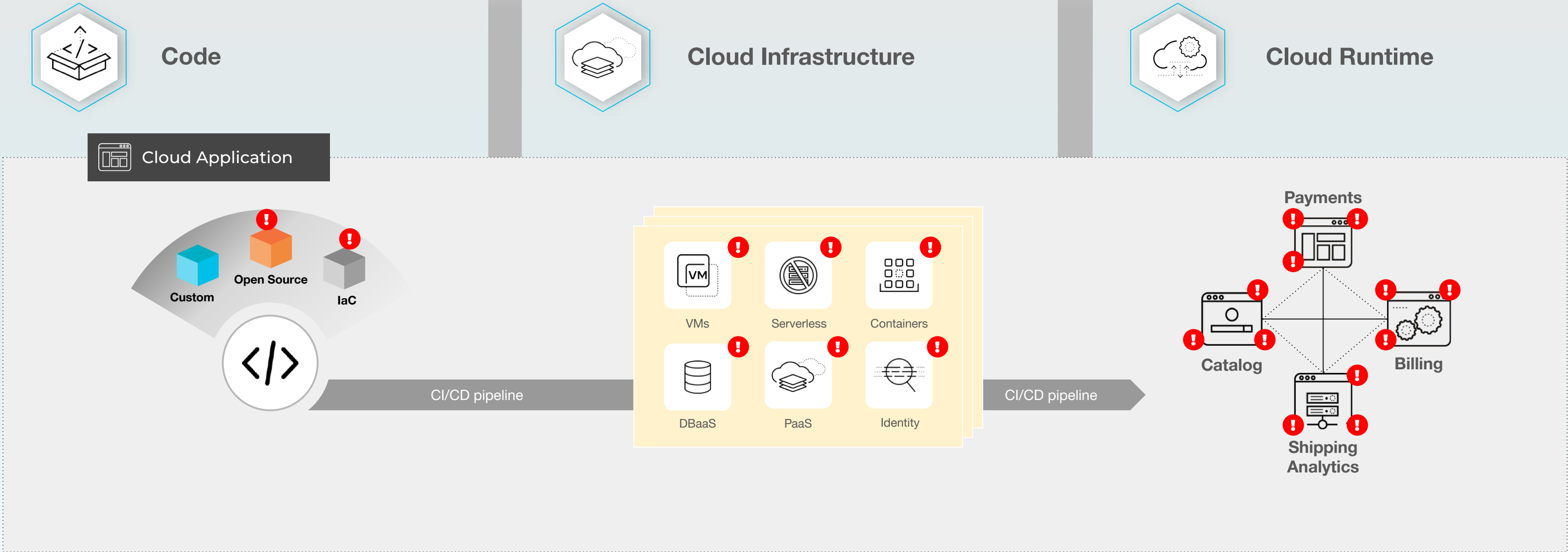
Everything Cloud Starts as Code, Where 1 issue ...



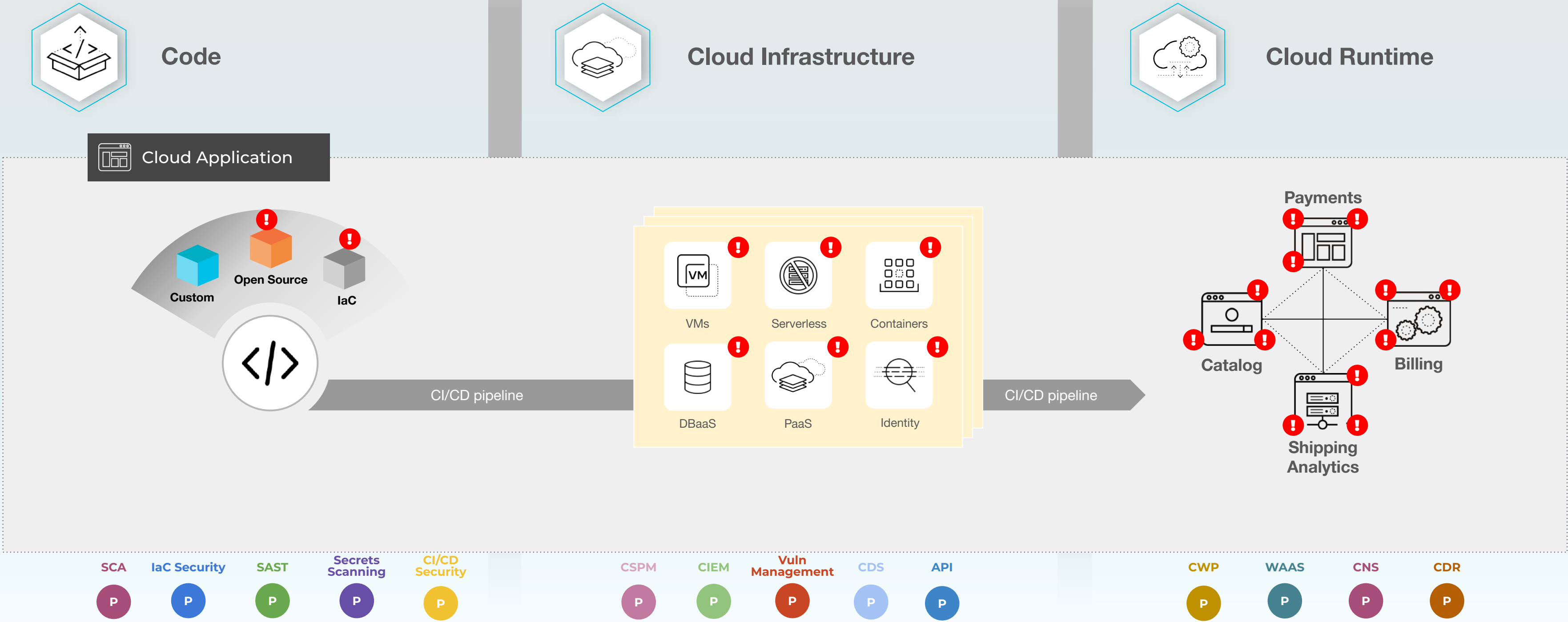
Everything Cloud Starts as Code, Where 1 issue Becomes Hundreds in Runtime



Everything Cloud Starts as Code, Where 1 issue Becomes Hundreds in Runtime



Too often siloed point product tools are used for cloud security



CLOUD COMPLEXITY



No matter the cloud maturity, Prisma Cloud has it covered



36
%

Lift-and-shift Applications

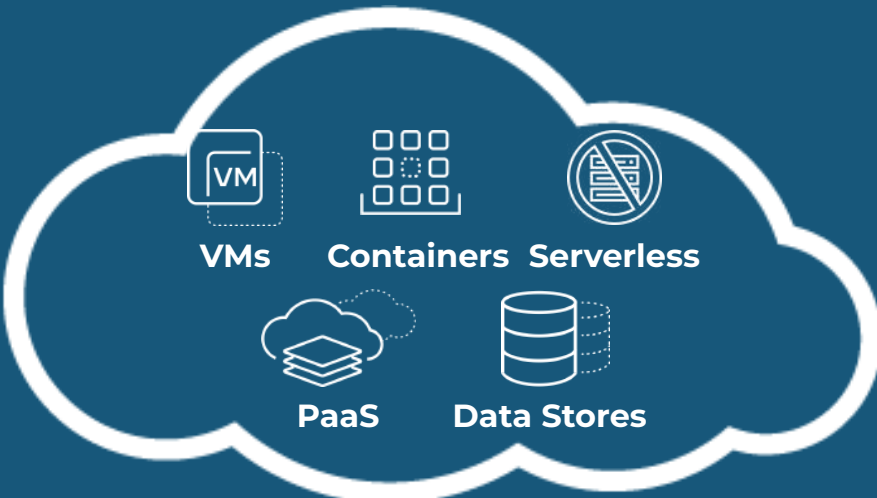


On-Premise Data Center
Applications



27
%

Re-Factor Applications

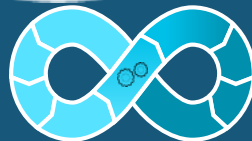
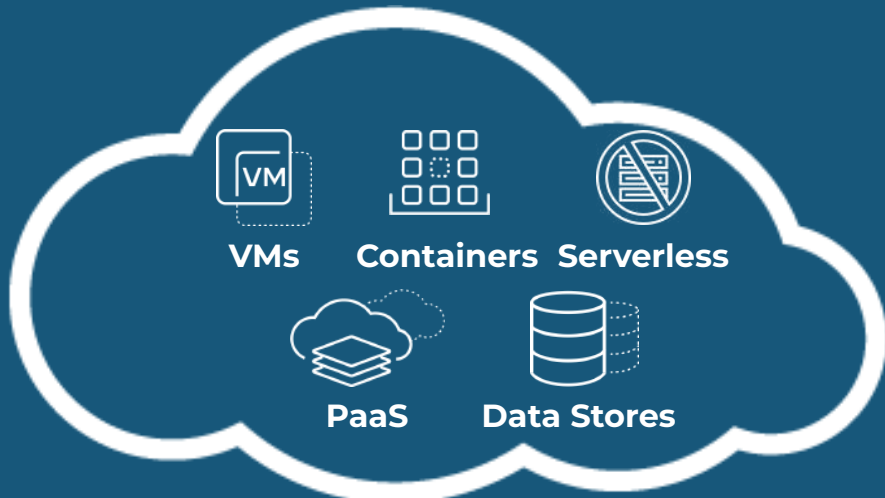


On-Premise Data Center
Applications



37
%

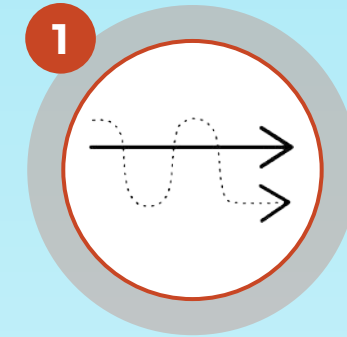
Build Cloud Native Applications



On-Premise Data Center
Applications

TOP 5 CHALLENGES IN MOVING TO THE CLOUD

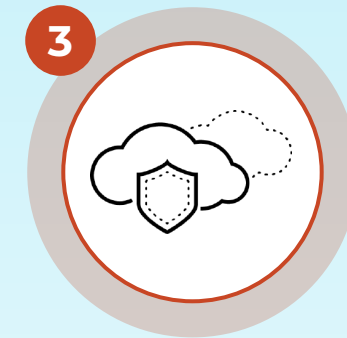
Complexity is the common denominator behind otherwise disparate challenges.



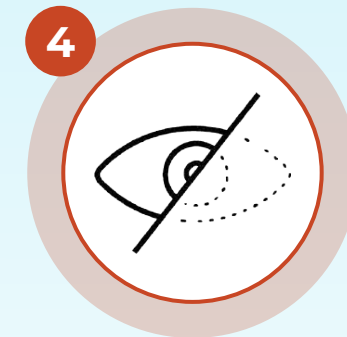
Technical complexity



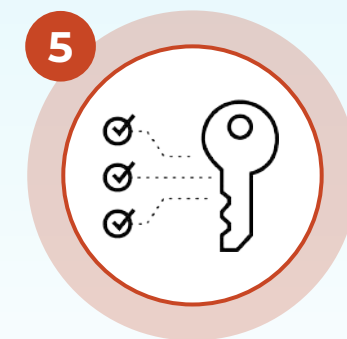
Lack of talent and/or consulting services



Maintaining comprehensive security



Lack of visibility across services and providers



Meeting compliance requirements

CLOUD SECURITY CONCERNS



TOP 5 CHALLENGES TO PROVIDE COMPREHENSIVE CLOUD SECURITY



Managing holistic
security

75%

Reported blind spots
due to high number
of tools



Security across app
lifecycle

35%

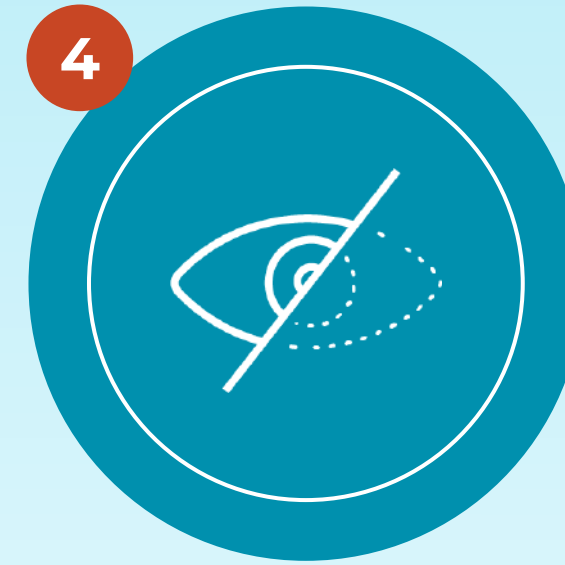
Can't provide
comprehensive
coverage due to
siloed teams



Training all staff

84%

Don't have large
teams -need to be
very efficient



Lack of visibility

96%

Container apps
contain known
vulnerabilities



Finding the right
tools

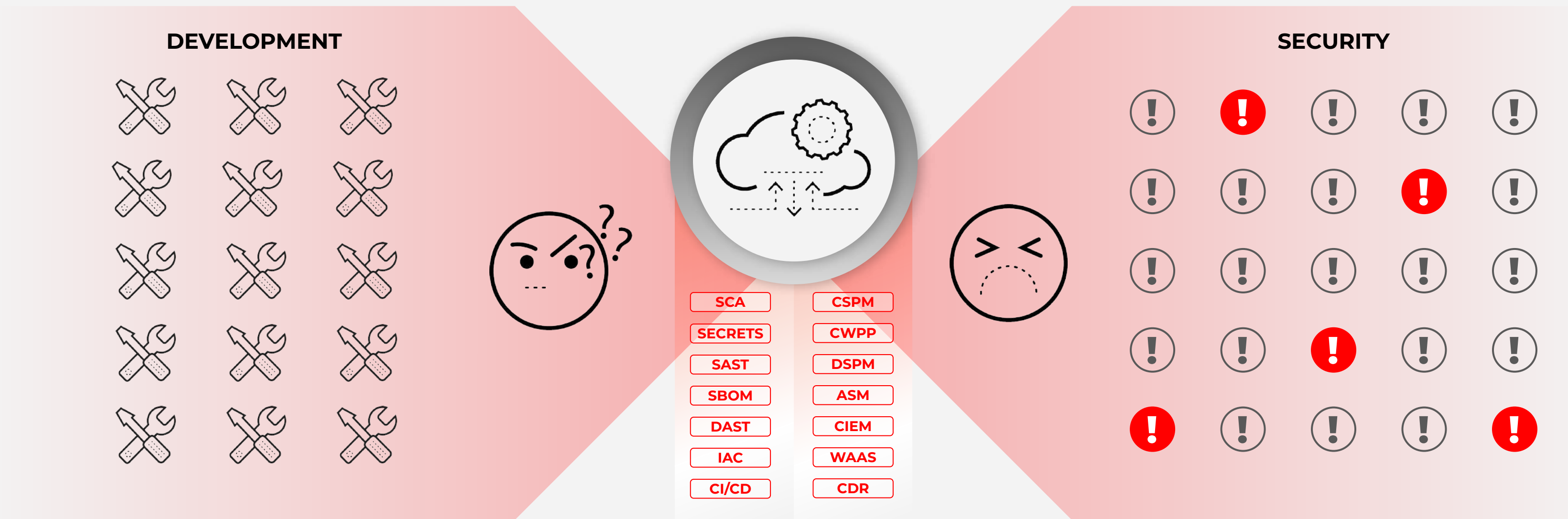
78%

struggle to identify
tools needed to
achieve security goals

SUMMARY

- 1.** Legacy systems are unfit to protect cloud native environments - 3 out of 5 incidents in Cloud are application specific
- 2.** Developers are moving fast: 77% of enterprises are deploying code to production weekly
- 3.** Rise of point products creates blind spots
- 4.** 90% of organizations cannot detect, contain, and resolve cyber threats within an hour
- 5.** Protecting Cloud native environments requires integrated end to end system

Today: Disintegrated security fosters adversarial relationships between security and development



Poor Developer Experience

Wasted cycles on too many low-risk alerts to fix. Insufficient context makes remediation efforts confusing and frustrating.

Siloed security tools

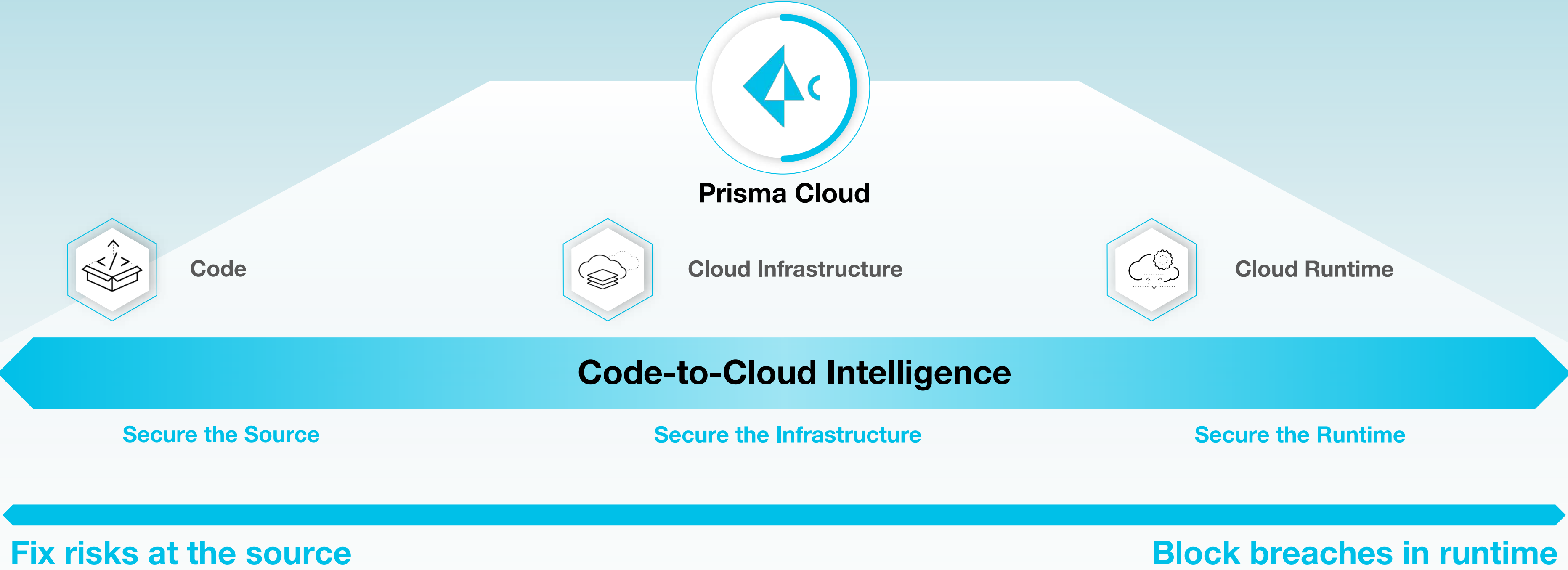
Point tools don't share security state and generate siloed alerts.

Poor Security Outcomes

Excessive alerts and poor prioritization due to lack of context

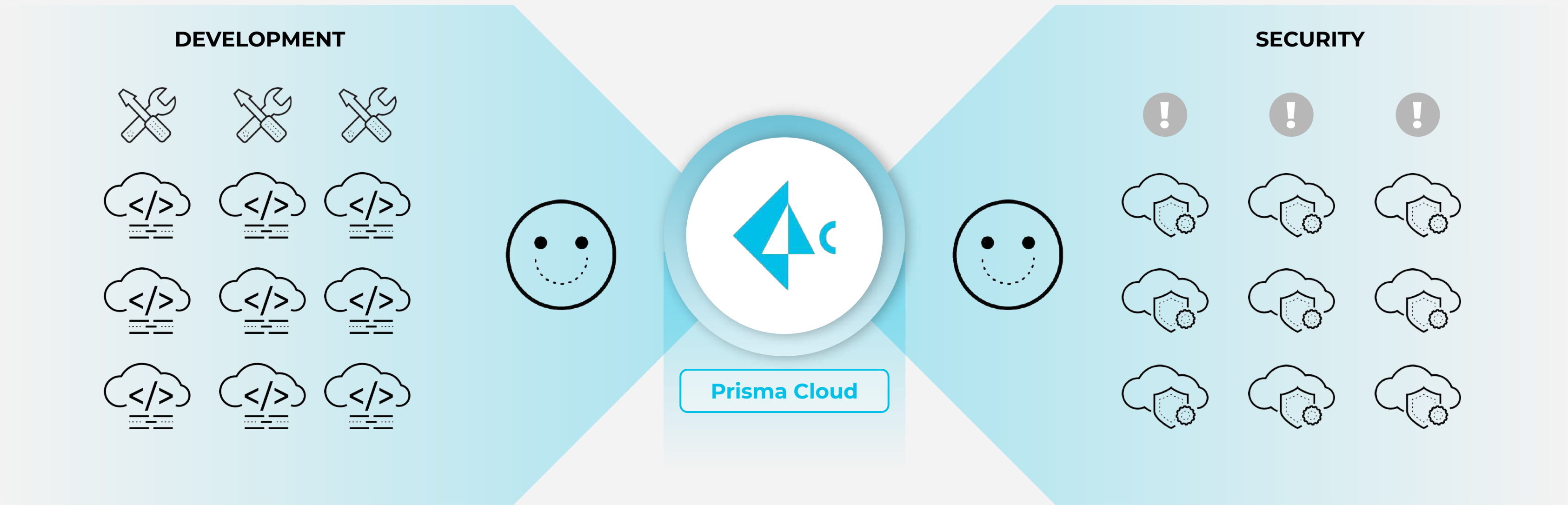
Solution

What's Required: Integrated Context to Prioritize, Fix at Source, Block in Runtime



Prisma Cloud Helps Bridge Siloes

to Protect Applications from Code to Cloud



Improved Developer Experience

Actionable remediation information for only critical issues saves developer time

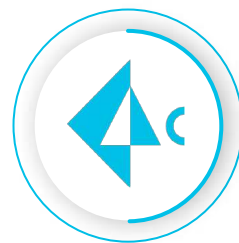
Code to Cloud Intelligence

Connects insights from the developer environment to application runtime to prevent risks and stop breaches.

Better Security Outcomes

Enhanced prioritization and improved risk management raises security posture in less time

Prisma Cloud is the industry's first Code to Cloud™ platform



Code to Cloud Platform



Secure the Source *Risk Prevention*

- Find and protect secrets **Secrets Security**
- Scan and secure open source software **SCA**
- Protect the delivery pipeline **CI/CD Security**
- Ship secure infrastructure **IaC Security**

Fix risks at the source



Secure the Infrastructure *Visibility & Control*

- Ensure correct cloud configurations **CSPM**
- Manage vulnerabilities **CWPP**
- Maintain least privileged access **CIEM**
- Find and secure sensitive data **DSPM / DDR**
- Discover and control ungoverned assets **CDEM**



Secure the Runtime *Runtime Protection*

- Detect advanced runtime threats
- Protect Kubernetes **CWP**
- Protect all running workloads **CWP**
- OWASP Top 10 protection **WAAS**
- API discovery and security **WAAS**

Block breaches in runtime

Broadest Cloud Service Coverage



40%

greater coverage than
the nearest competitor

11 Hosting Locations

Multi-geo support: NA (US & Canada), EMEA (UK, Germany, France),
JAPAC (Australia, China, Singapore, Japan, India), GovCloud

Support your DEVELOPERS' CHOICE of cloud services

Prisma Cloud: Protection from Code to Cloud

A Complete Platform that Integrates Best of Breed Capabilities

CNAPP
LEADER

Cloud Workload Security Wave

FORRESTER

CNAPP
LEADER

Global CNAPP Radar

FROST & SULLIVAN

CNAPP

Top Reviewed Product
Gartner Peer Insights CNAPP

Gartner



Secure the Source

DevSecOps
LEADER

Developer Security Tools Radar

GIGAOM

Code Security
LEADER

Policy as Code Radar

GIGAOM



Secure the Infrastructure

CSPM

Top Reviewed Product
Gartner Peer Insights CSPM

Gartner

CSPM

LEADER
CSPM Radar

GIGAOM



Secure the Runtime

CWPP

Ranked #1
Top CWPP Products

PeerSpot

CWPP

LEADER
Global CWPP Radar

FROST & SULLIVAN

CN

cloud-native

Driven by cloud computing, cloud-native defines frameworks for deploying and operating applications at speed and scale

AP

application protection

Secure applications and networks that deliver them. Workloads have more degrees of freedom = larger attack surface

P

platform

Multi disciplinary approach to security from code to cloud

Thank You!!!

