
aws
SUMMIT
INDIA | MAY 25, 2023

SECR005

Securing app life cycle via zerotrust in DevOps supply chain

Bisham Kishnani
Head of Cloud Security & DevSecOps Engineering, APAC & Japan,
Check Point Software Technologies

CHECK POINT™

Securing Application Life Cycle By Infusing Zero Trust in DevOps Supply Chain

More Context

Actionable Security

Smarter Prevention

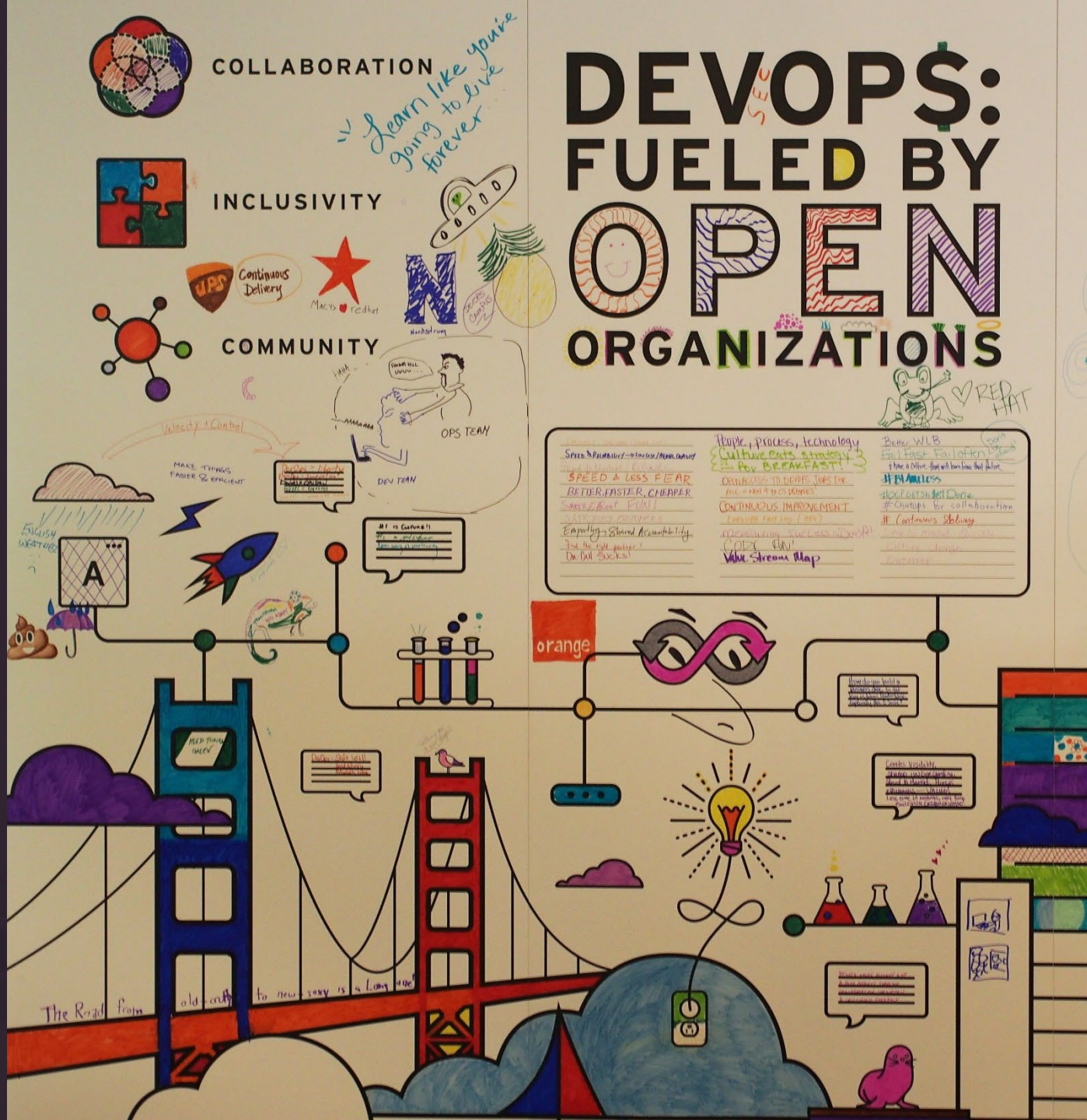
Bisham Kishnani

Head Of Systems Engineering - Cloud Security & DevSecOps (APAC)

YOU DESERVE THE BEST SECURITY

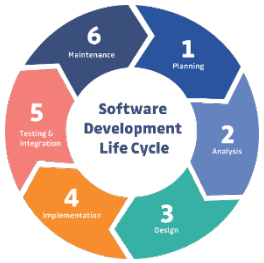
What I am going to talk about

- Recap Zero Trust
- Security incidents and trends
- Infuse Zero Trust In DevOps Supply Chain
- Solution and value proposition



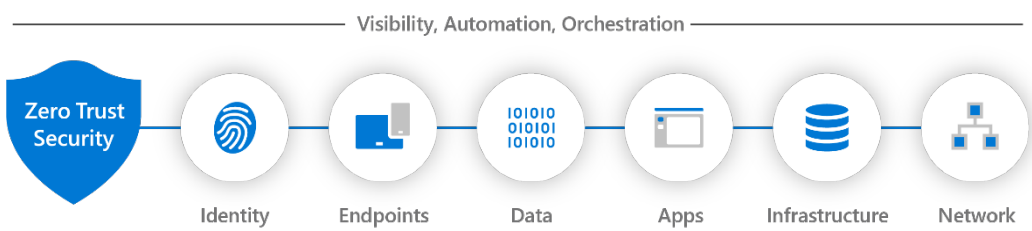
Recap zero trust

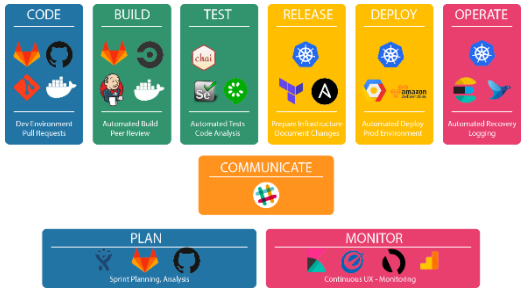
The term "Zero Trust" was coined by an analyst at Forrester Research Inc. in 2009-2010 when the model for the concept was first presented.



Zero Trust is a Security strategy with the goal to ***Eliminate Trust at all Levels***
It has the following key security principles:

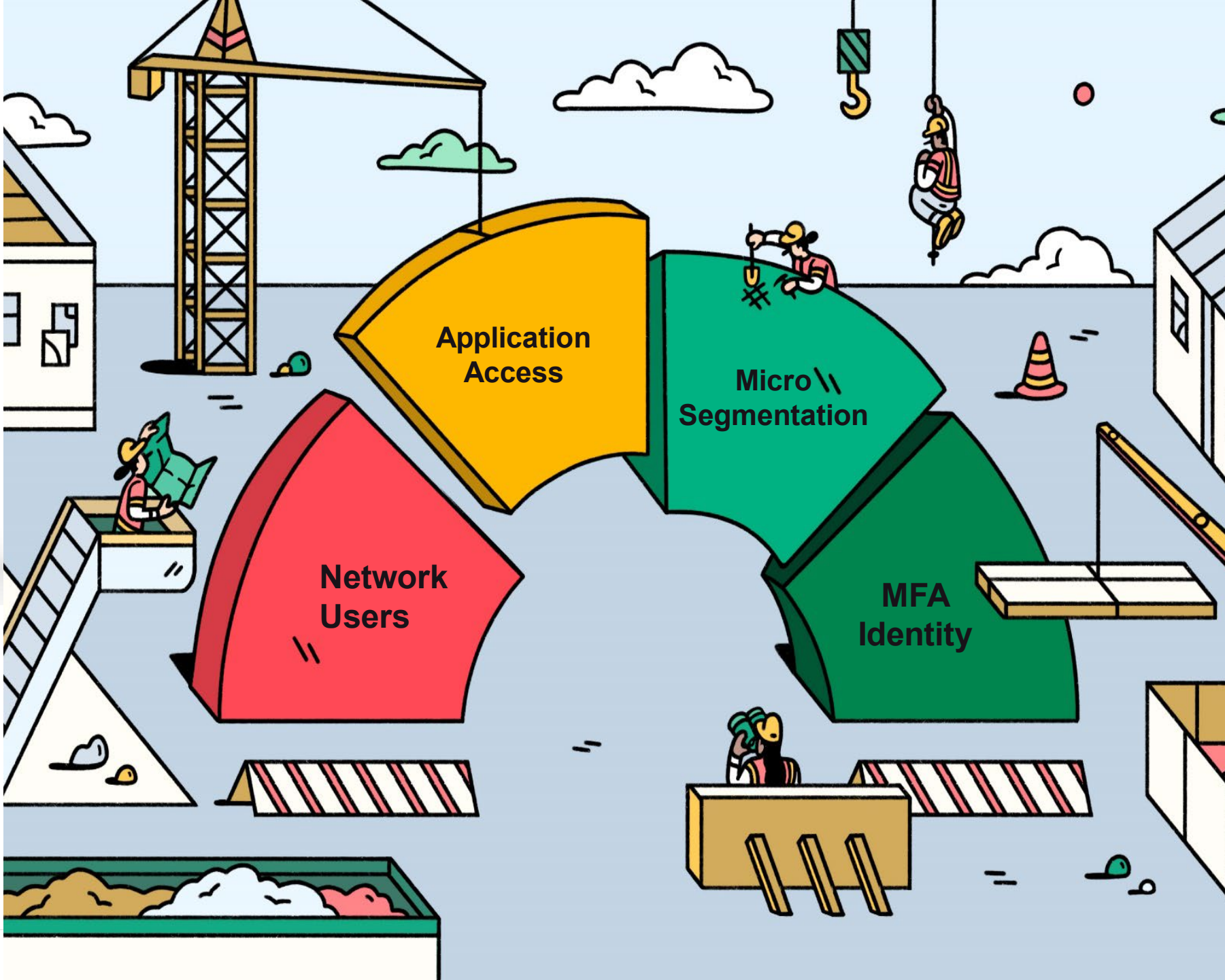
- Verify explicitly
- Use least privilege access
- Assume breach





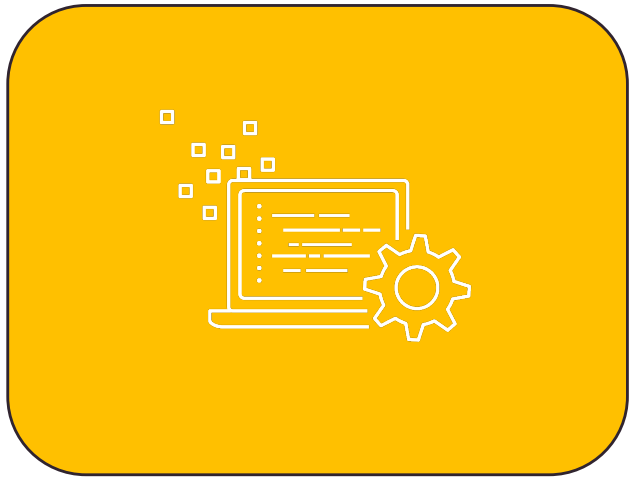
Are we eliminating trust at all levels ?


WHY
NOT

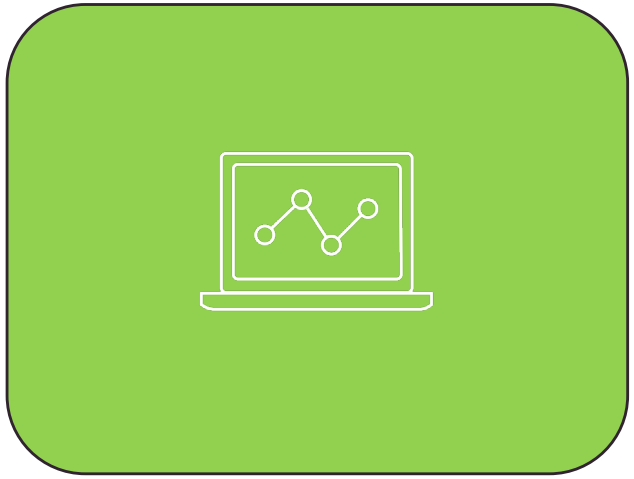

Application Access
Micro Segmentation
Network Users
MFA Identity

New attack techniques

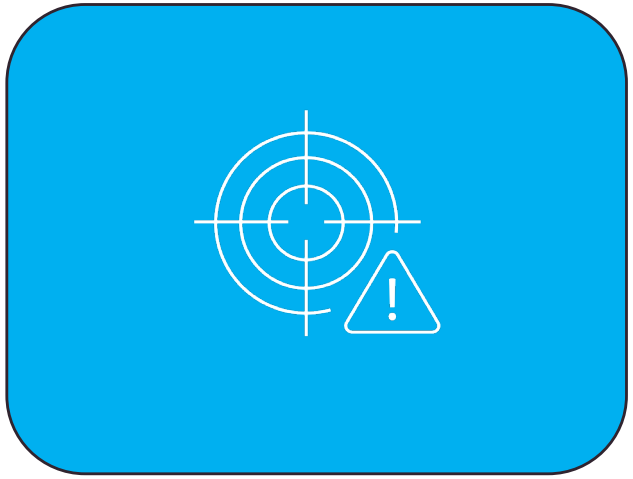
API Leaks & API Based Attacks



Supply Chain Based Attacks



Repo Jacking Based Attacks



Learn More

https://bit.ly/3VVLtFG
https://bit.ly/3Qt5NNf
https://bit.ly/3XfAdFc

EXECUTIVE SUMMARY **ngnix**

EXECUTIVE SUMMARY **nodejs**

EXECUTIVE SUMMARY **mongodb**

EXECUTIVE SUMMARY **redis**

SUMMARY OF TESTS PERFORMED

Tests Performed	Passed	Failed
411	93.43% (384)	6.57% (27)

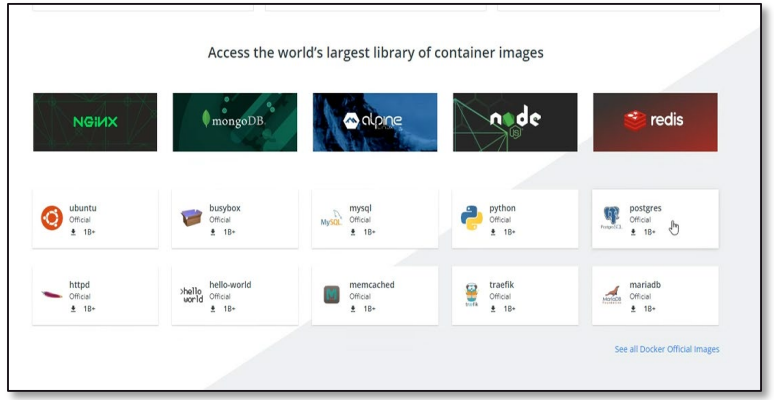
FAILED TESTS BY SEVERITY

Critical	High	Medium	Low	Informational
5	14	7	1	0

SUMMARY OF RULES TESTED

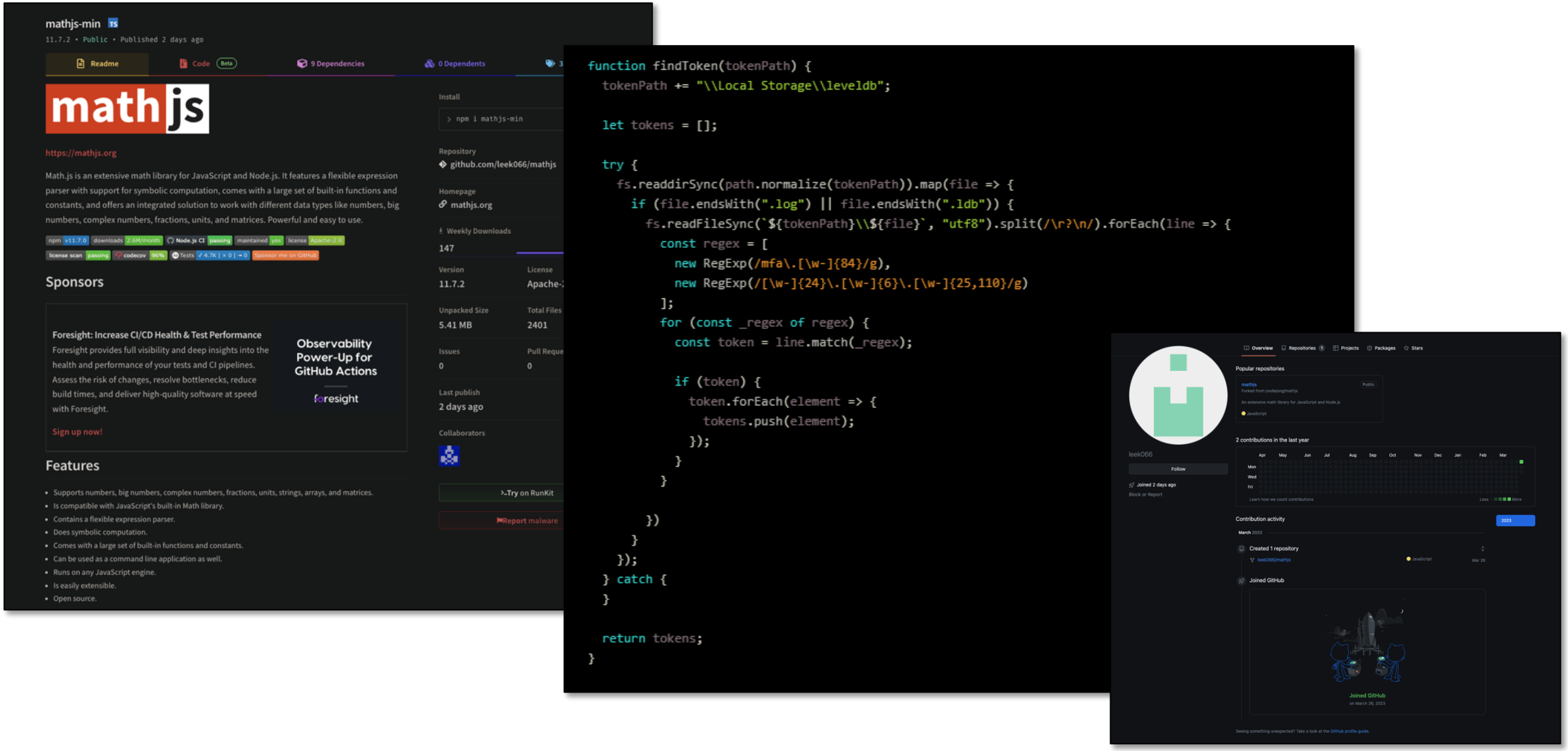
Rules Performed	Passed	Failed
20	75% (15)	25% (5)

docker



Top 10 images are downloaded more than 1B times a year

NPM package mathjs-min contains credential stealer



TRENDS

noname Products Use Cases Industries Partners Company Resources Book a Demo

451 Research
S&P Global
Market Intelligence

The 2022 API Security Trends Report

451 Research asked participants about their API landscape, API security tools, maturity level of API security within the organization, and more. In this API security trends report, we dive into the key findings.

Download Full Report

API USAGE

Companies rely on tens of thousands of APIs. For the enterprises participating in this study, the average number of APIs in use is 15,564. Large enterprises, those with more than 10,000 employees, have an even greater dependency, with an average of 25,592 APIs in place.

15,564
is the average number of APIs an organization has in place today

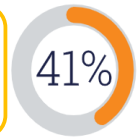
Large enterprises have an average of
25,592 APIs

API SECURITY INCIDENTS

Many API security incidents will go undisclosed unless a data breach occurs requiring consumer notifications, or there is a coordinated disclosure of API security vulnerabilities with a security researcher. Practitioners were asked whether their organizations had experienced a security incident related to an API in the past year.

41% of organizations had an API security incident in the last 12 months.

63% of those noted that the incident involved a data breach or data loss.



Gartner Information Technology Roles Experts Research & Tools Insights Events

← All Webinars

Information Technology

API Security: Protect your APIs from Attacks and Data Breaches

ON-DEMAND | 1 hour

Gartner predicts that by 2022, application programming interface (API) attacks will become the most-frequent attack vector, causing data breaches for enterprise web applications. Already, many well-publicized API security vulnerabilities affected a wide range of organizations. This complimentary webinar explores the attack paths for APIs and how your team can protect against them by building secure APIs. You will learn how API discovery and API security testing help strengthen this initiative.

Return to this web page to watch the webinar. Contact us at gartnerwebinars@gartner.com with questions about watching.

STAMFORD, Conn., February 9, 2022

Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025

Accelerating Shift to the Cloud Means the Market Opportunity for Providers Is Narrowing

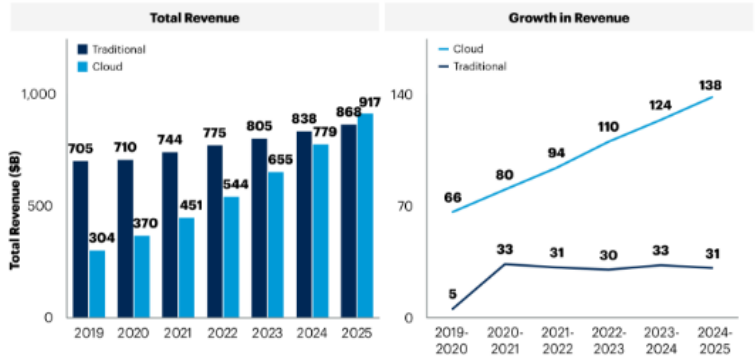
Enterprise IT spending on public cloud computing, within addressable market segments, will overtake spending on traditional IT in 2025, according to Gartner, Inc.

Gartner's 'cloud shift' research includes only those enterprise IT categories that can transition to cloud, within the application software, infrastructure software, business process services and system infrastructure markets. By 2025, 51% of IT spending in these four categories will have shifted from traditional solutions to the public cloud, compared to 41% in 2022. Almost two-thirds (65.9%) of spending on application software will be directed toward cloud technologies in 2025, up from 57.7% in 2022.

"The shift to the cloud has only accelerated over the past two years due to COVID-19, as organizations responded to a new business and social dynamic," said Michael Warrilow, research vice president at Gartner. "Technology and service providers that fail to adapt to the pace of cloud shift face increasing risk of becoming obsolete or, at best, being relegated to low-growth markets."

In 2022, traditional offerings will constitute 58.7% of the addressable revenue (see Figure 1), but growth in traditional markets will be much lower than cloud. Demand for integration capabilities, agile work processes and composable architecture will drive continued shift to the cloud, as long-term digital transformation and modernization initiatives are brought forward to 2022. Technology product managers should use the cloud shift as measure of market opportunity.

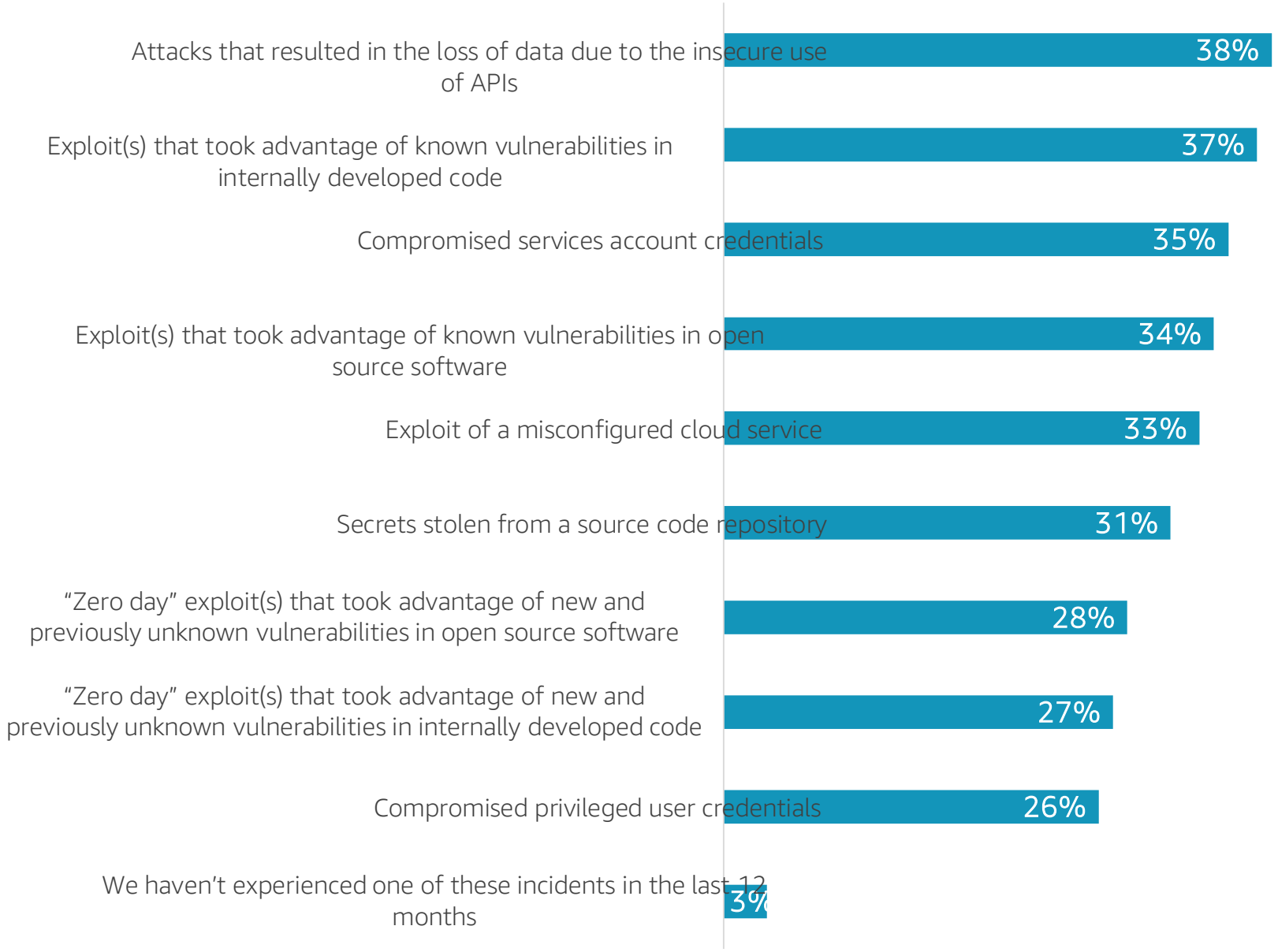
Figure 1: Sizing Cloud Shift, Worldwide, 2019 – 2025



End user and customer trends

Security incidents in past 12 months

Organizations have faced a variety of incidents and related consequences, with only 3% saying they didn't experience incidents.



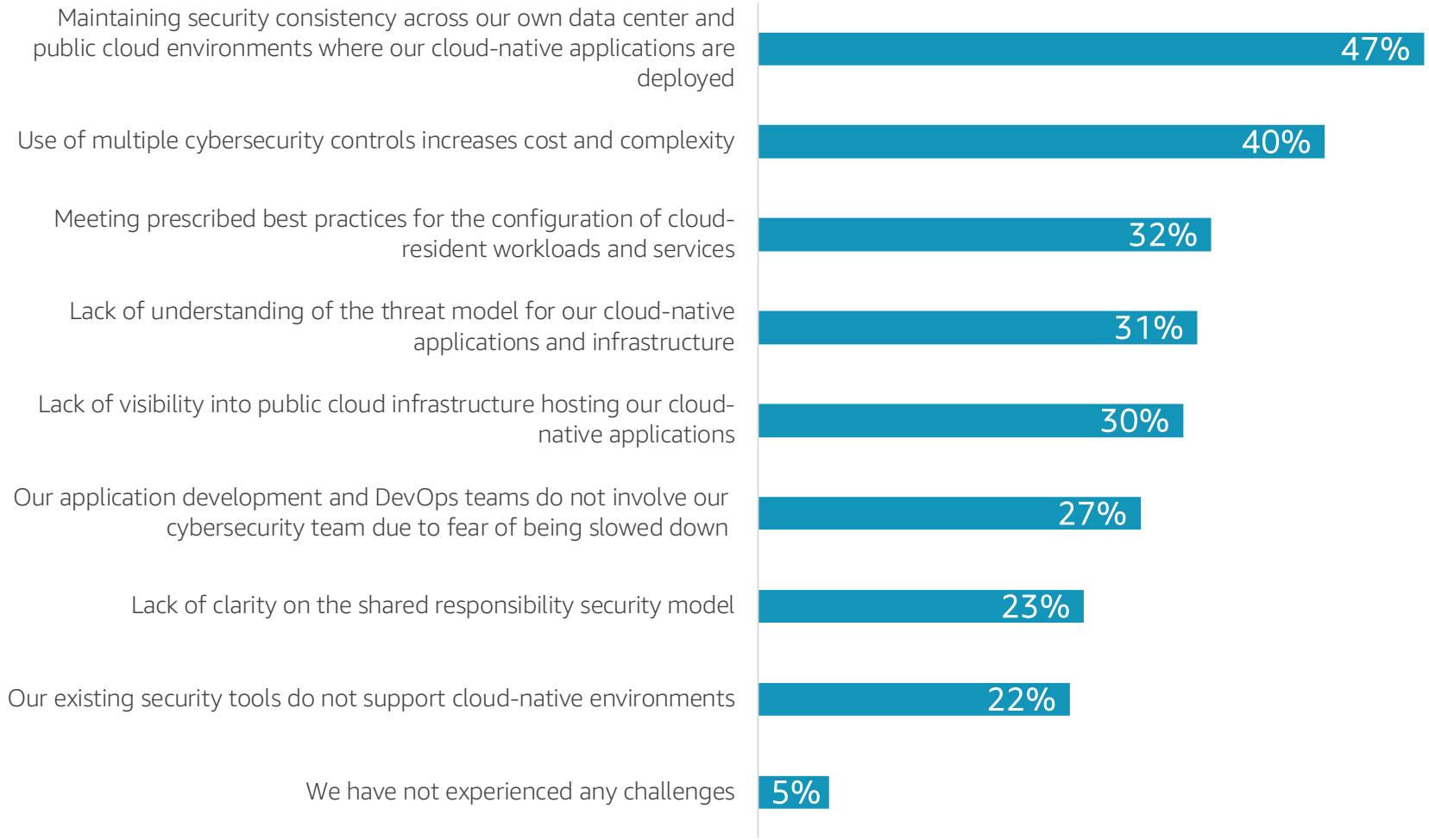
Question text:
Which of the following cybersecurity incidents, if any, has your organization experienced in the last 12 months related specifically to internally developed cloud-native applications? (Percent of respondents, N=350, multiple responses accepted)

87%

of respondents believe the differences between cloud-native applications and the rest of their apps and infrastructure require a different set of security policies and technologies.

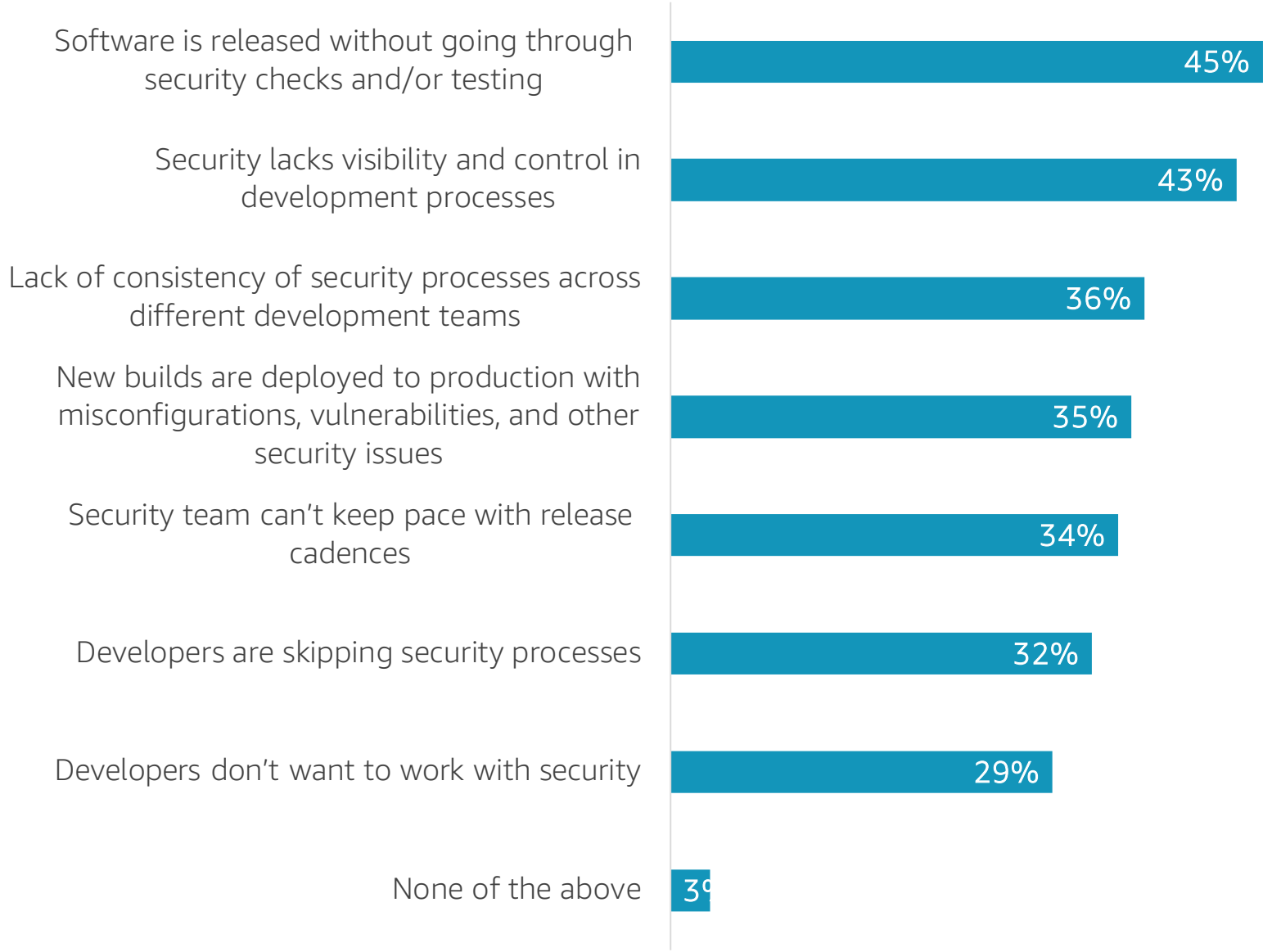
The need for a new approach to security

New challenges with cloud-native applications



Challenges with faster development

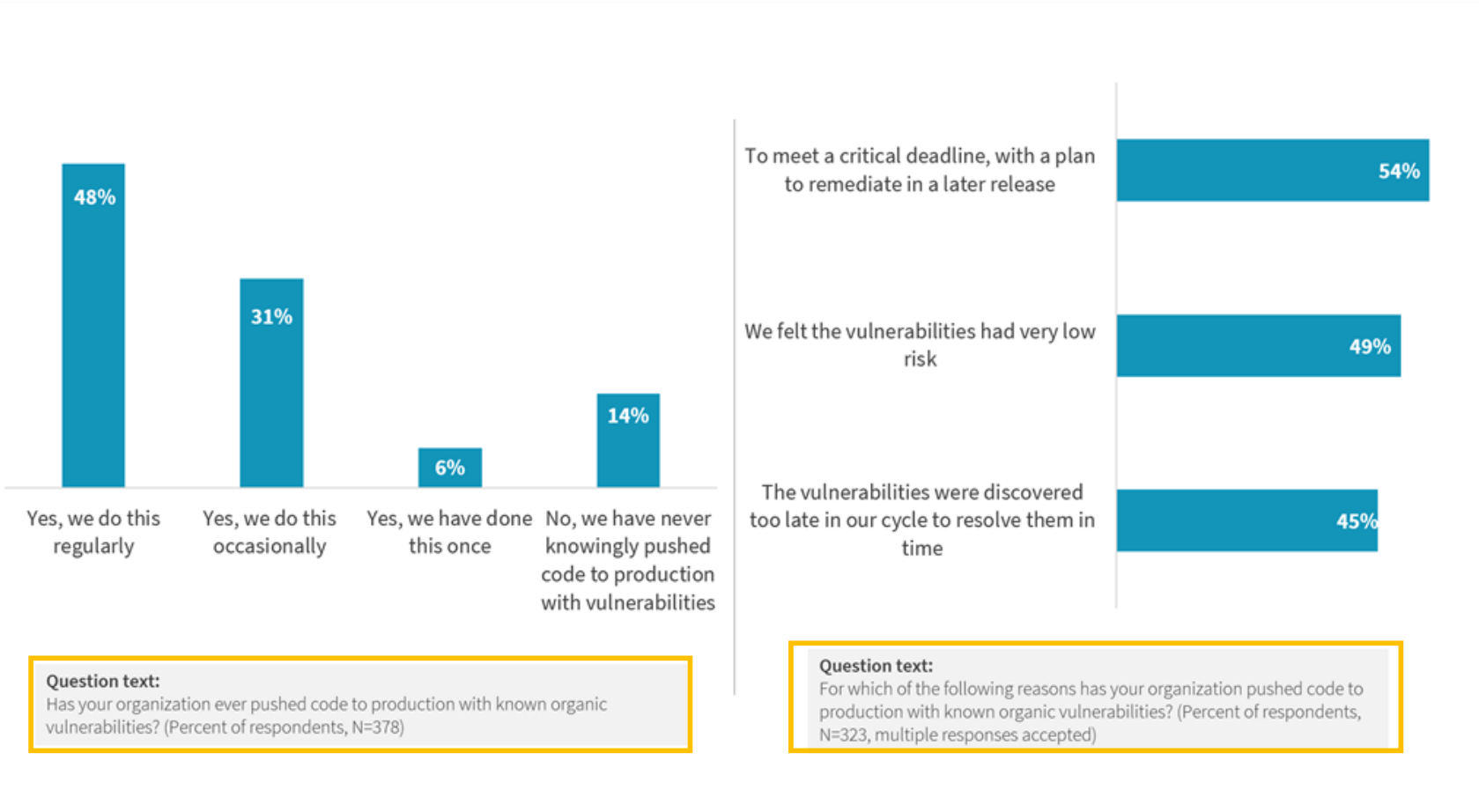
Organizations have a variety of concerns with the faster release cycles with CI/CD; the pressure to deploy means new builds get pushed with security issues. These pain points are areas that vendors can address with their solutions.



Question text:
What security challenges does your organization face with faster development cycles of CI/CD? (Percent of respondents, N=350, multiple responses accepted)

Push vulnerable code to meet deadlines

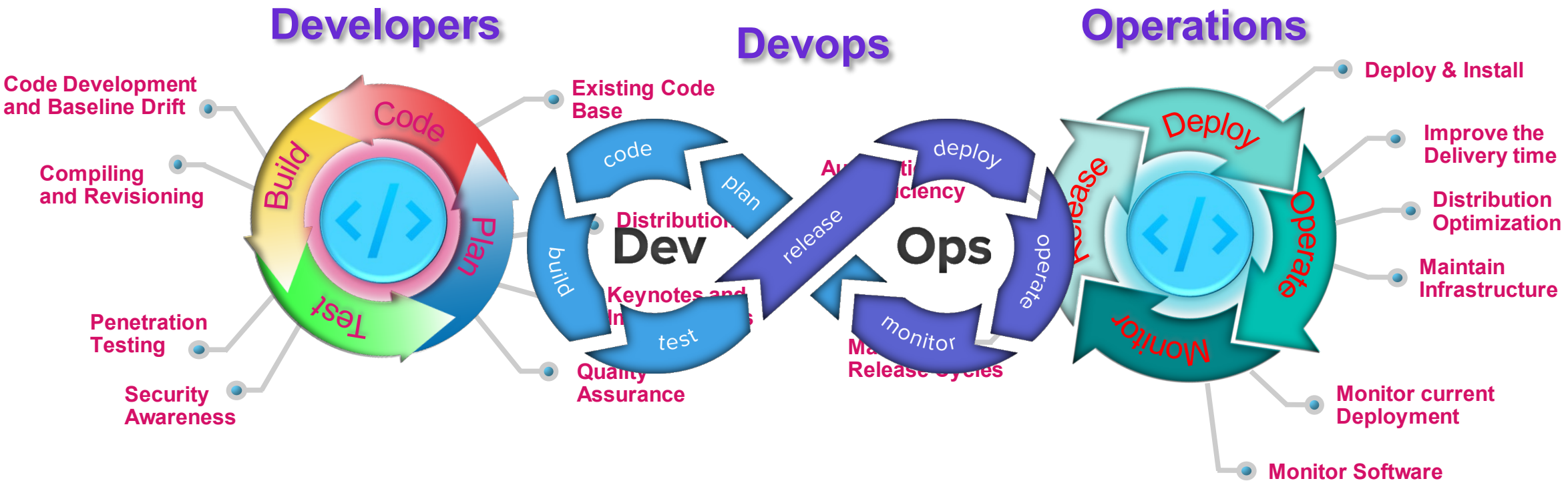
Security can’t keep up; they need a way to help developers efficiently secure their code



Source: ESG Master Survey Results: Modern Application Development Security

The most privileged user

Developers, operations & devops



And This Pipeline is Built on Trust which the Threat Vectors are exploiting

Value Proposition

Go Deep Shift Left

Zero Trusted DevOps Supply Chain

Eliminate Trust At Every Point Of Pipeline

CODE

Dev Environment
Pull Requests

BUILD

Automated Build
Peer Review

TEST

Automated Tests
Code Analysis

RELEASE

Prepare Infrastructure
Document Changes

DEPLOY

Automated Deploy
Prod Environment

OPERATE

Automated Recovery
Logging

COMMUNICATE

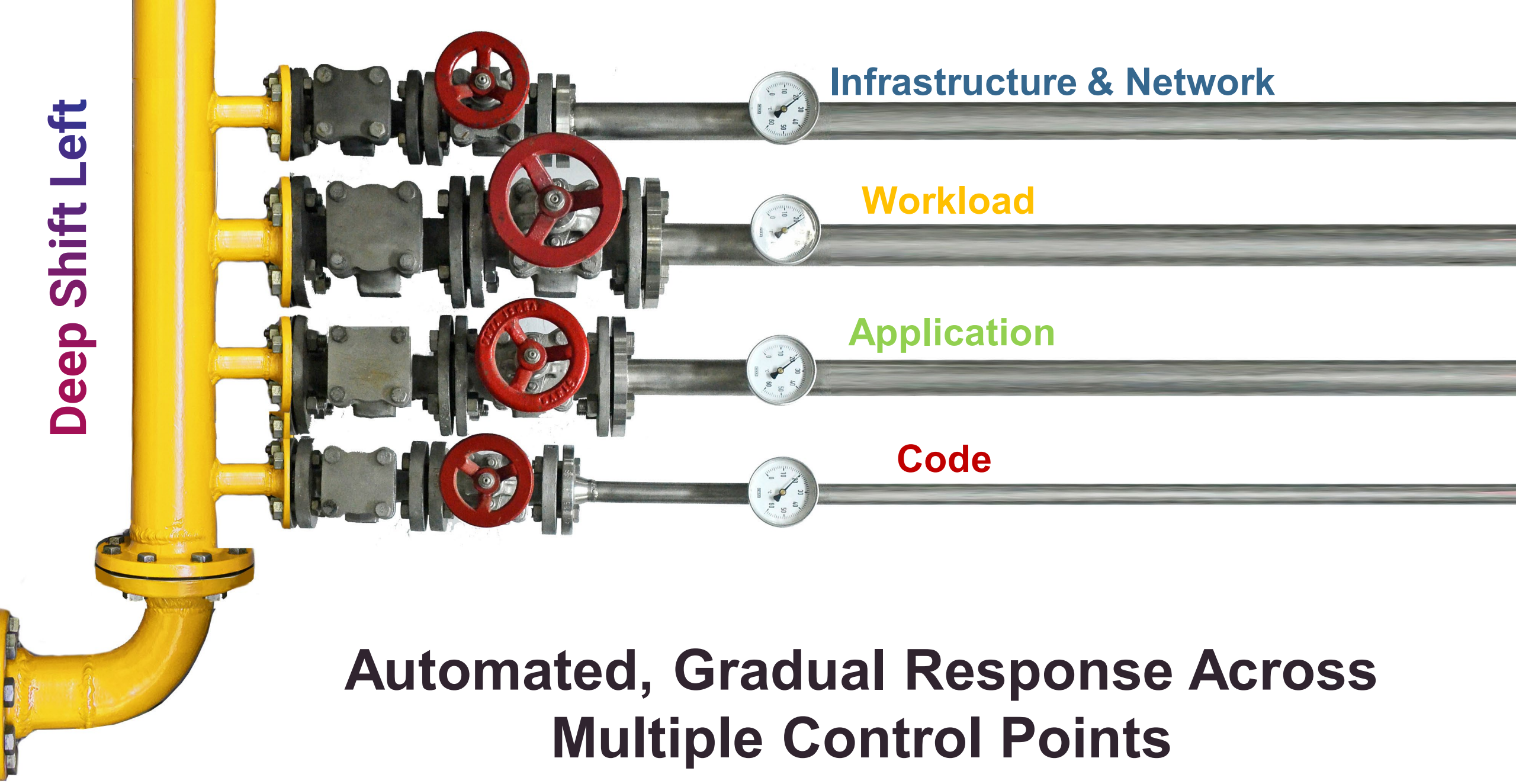
PLAN

Sprint Planning, Analysis

MONITOR

Continuous UX - Monitoring

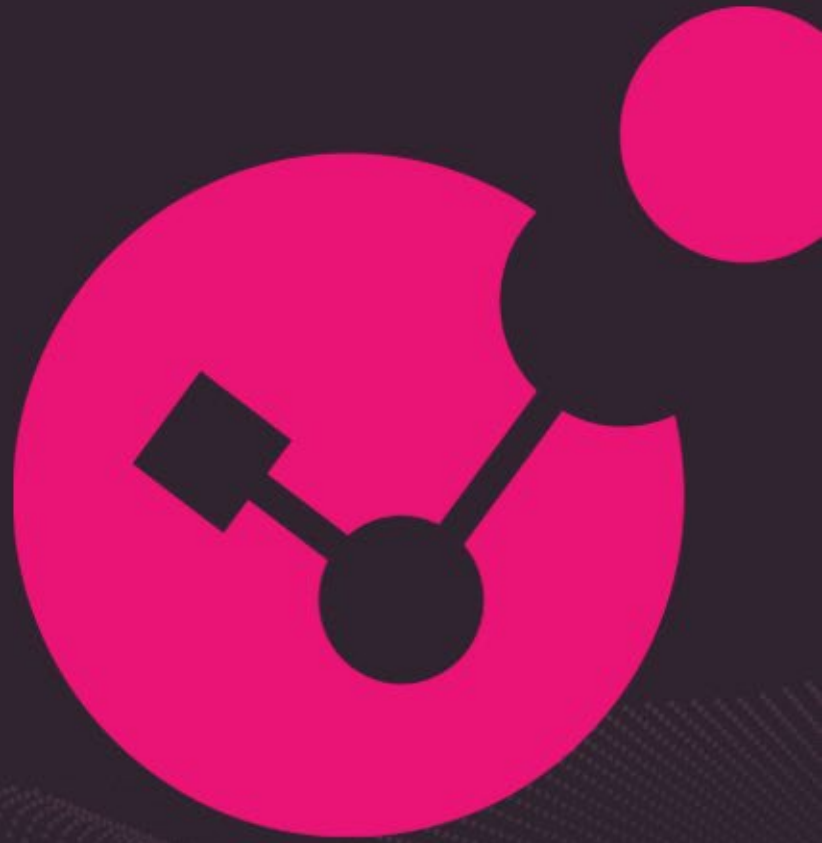
Shift Left = Closing the valve stops EVERYTHING



Automated, Gradual Response Across Multiple Control Points

Deploy separate tools to fix issues

Misconfigured Code	IAC Security & Code Scanning
Overly Permissive Users	Cloud Entitlement Management
Compliance & Misconfigurations	Cloud Posture Management
Threat Monitoring	Cloud Detection & Response
Malware & Vulnerabilities	Container & Agentless Scanning
Web, API, & Bot Attacks	WAF, API SecGW & Bot Mitigation



Alert Fatigue

Gartner's **c**loud **n**ative **a**pplication **p**rotection **p**latform

Integrated set of security and compliance capabilities designed to help secure and protect cloud-native applications across development and production

CNAPPs consolidate:

Large number of **previously siloed capabilities**, including:

- Container scanning, CSPM, Infrastructure as Code scanning,
- Cloud Infrastructure Entitlement Management,
- Runtime Cloud Workload Protection platforms

Gartner®

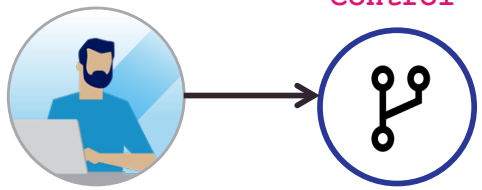
CloudGuard

PREVENTION-FIRST CNAPP

More Context ▶ Actionable Security ▶ Smarter Prevention

Infusing zero trust security into devops - born from left

Code | Build | Deploy | Operate



Version Control

Enforce Security and compliance standards

- Zero Trust Permission
- K8s & Workload configuration

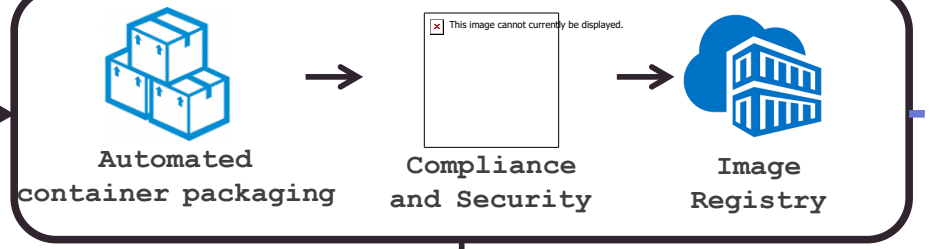
CloudGuard

Continusous Image Scan

- Image vulnerability by severity
- Image file reputation and secrets

CloudGuard

CI



Effective Risk Management

- Complete visibility
- CSPM
- Workload Risk
- API Security

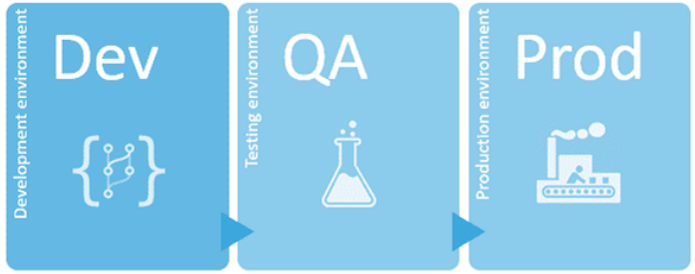
CloudGuard

Developer-First Security

- Static Code Analysis
- Infrastructure as a Code Scanning
- Secrets
- API Tokens
- Misconfigurations

CloudGuard

CD



Containers & Serverless Self-Protection

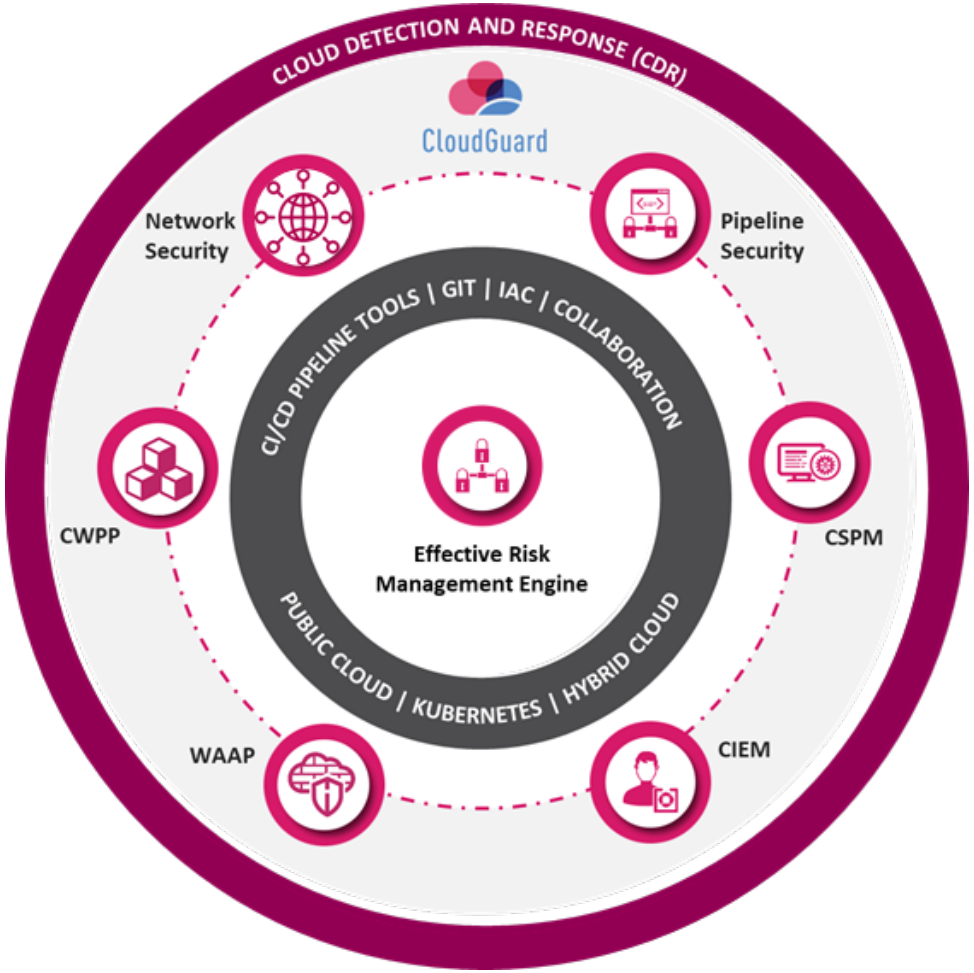
- Agentless Posture Management
- CIEM
- Workload Protection

CloudGuard

SecDev | DevSec | SecOps | OpsSec

More Context | Actionable Security | Smarter Prevention

ONLY CLOUDGUARD OFFERS SMARTER CLOUD THREAT PREVENTION...

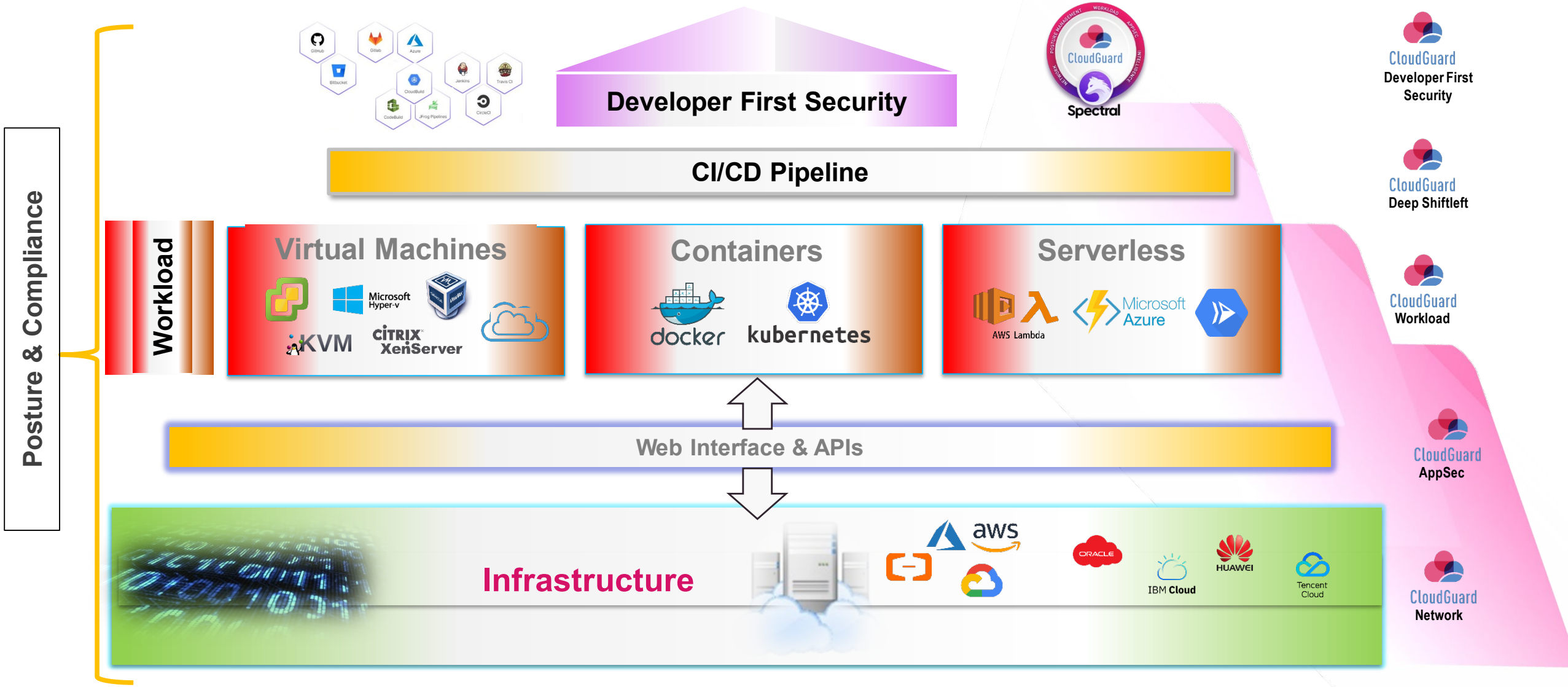


Comprehensive, Consolidated, & Collaborative

- From code to cloud
- From workload to application
- From intelligent remediation to runtime prevention
- Across the broadest number of use cases

More Context – Actionable Security – Smarter Prevention

Implementing structured multilayer security



More Context

Actionable Security

Smarter Prevention

- **Deep Visibility At All Layers**
- **Layered Security Approach**
  - Code Protection, Application & API Security (api is the new data path), Workload Protection & Network Security
- **Implement Developer First Security**
  - Integrate Code Quality Gates
  - Build Gates At Every Junction / Point Of The Pipeline
- **Security Posture Management & Compliance**
- **Threat Intelligence**

Thank you!

Please complete the session survey

Bisham Kishnani

Head of Cloud Security & DevSecOps Engineering, APAC & Japan,
Check Point Software Technologies