



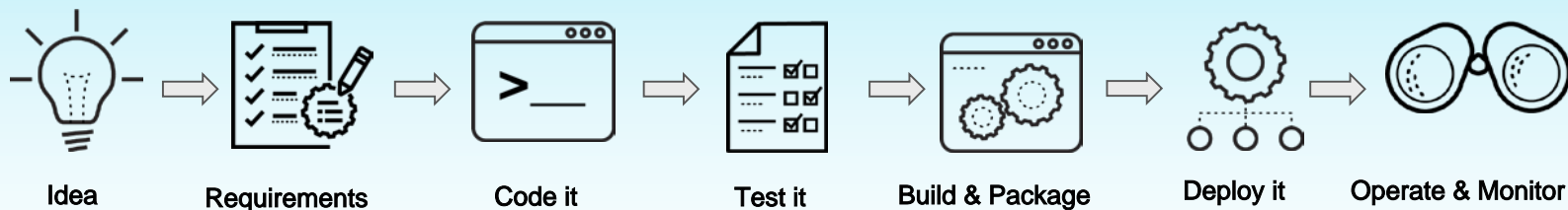
Prisma Cloud 

Agile Infrastruktur in der Cloud erfordert besondere Sicherheit

Eugen Hinz | Prisma Cloud Solutions Architect



Typical Software Release Process



Initial Launch

Digital Transformation

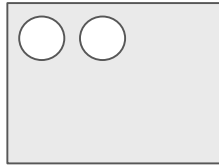
Development Process

Waterfall



Application Architecture

Monolithic



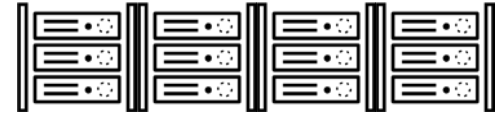
Deployment and Packaging

Physical Server

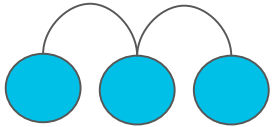


Application Infrastructure

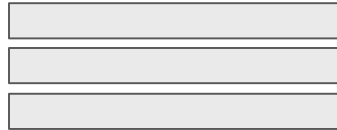
Datacenter



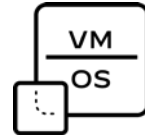
Agile



N-Tier



Virtual Servers



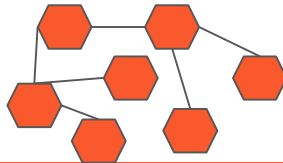
Hosted



DevOps



Microservices



Containers



Cloud

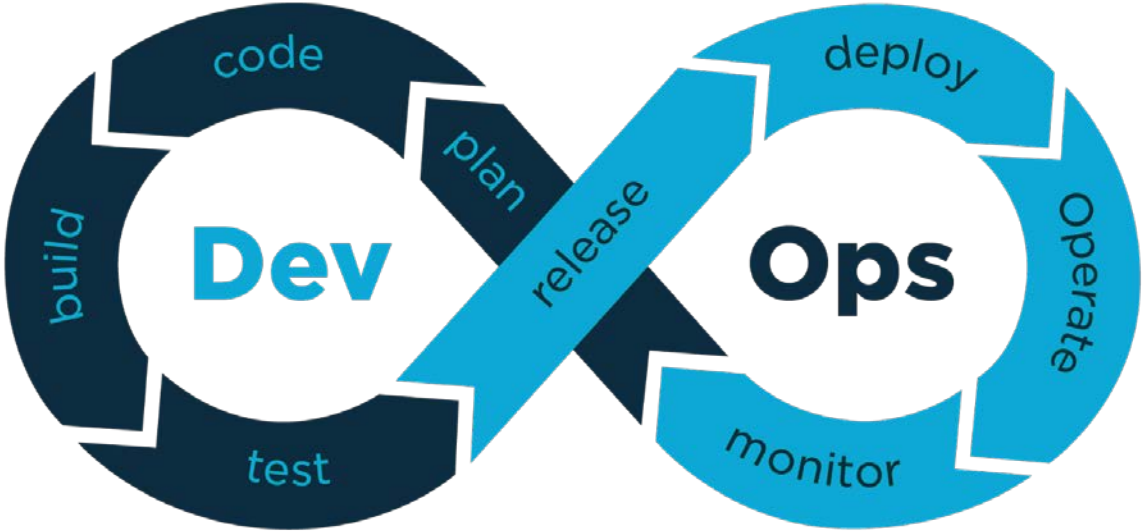


What is DevOps?

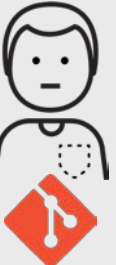
Dev Ops



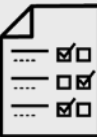
Sec



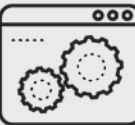
DevOps Pipeline



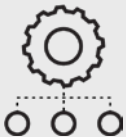
Developer



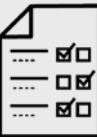
Automated Tests



Build



Deploy TEST

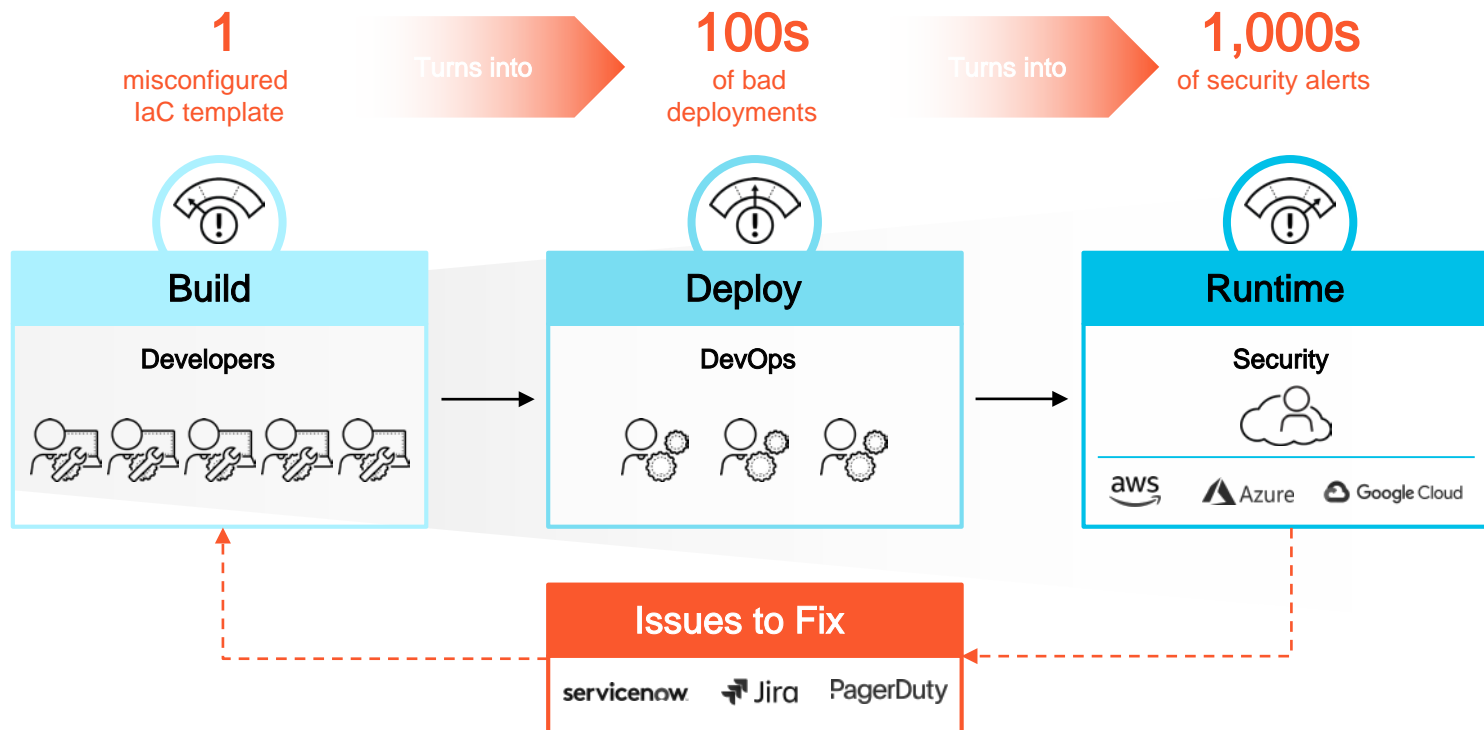


Automated Tests

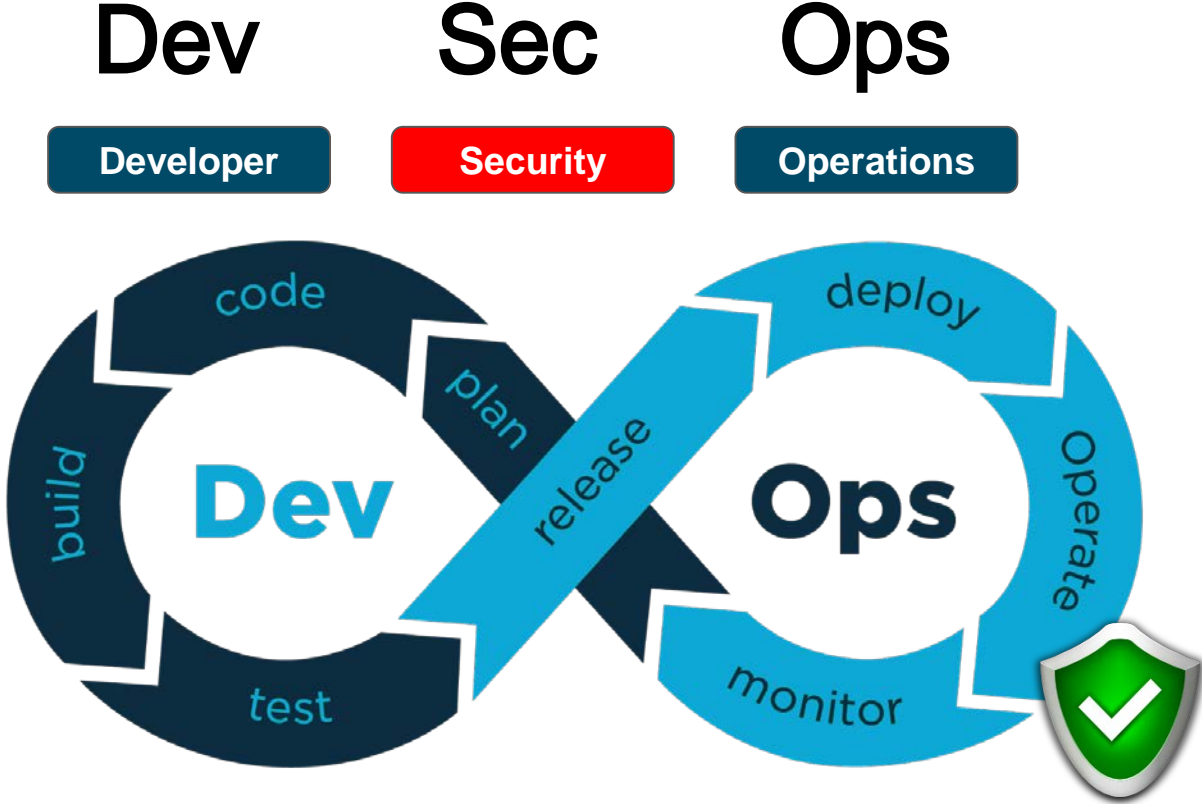


Security Tests

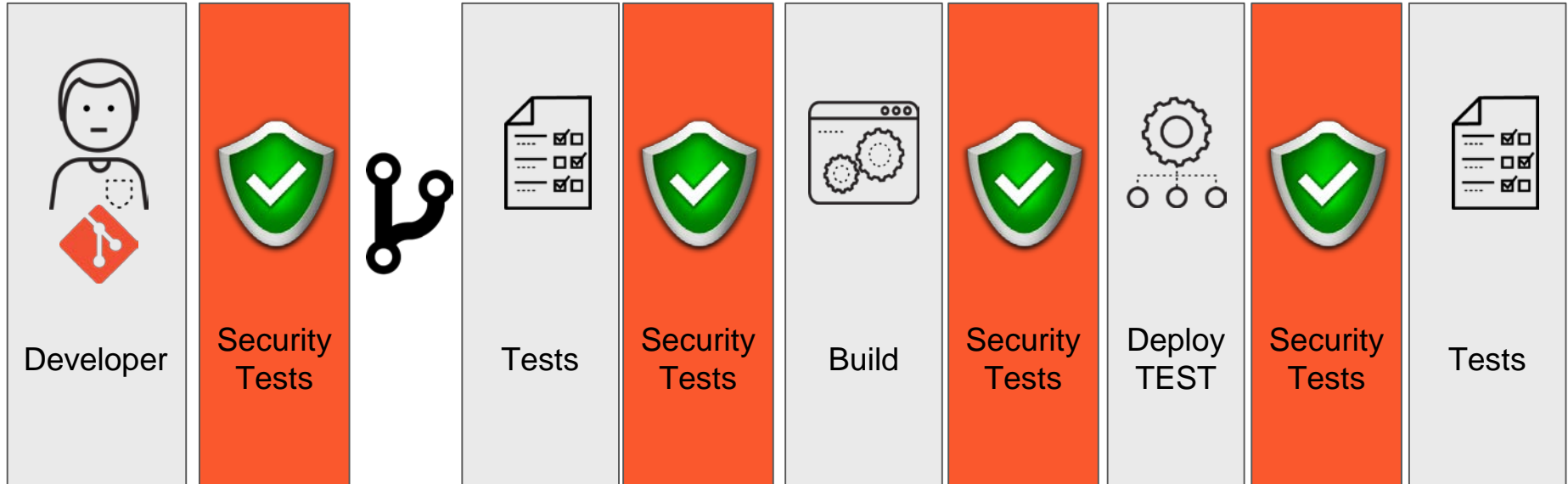
Infrastructure as Code (IaC): The Need for “Shift Left” Cloud Security



What is DevSecOps?

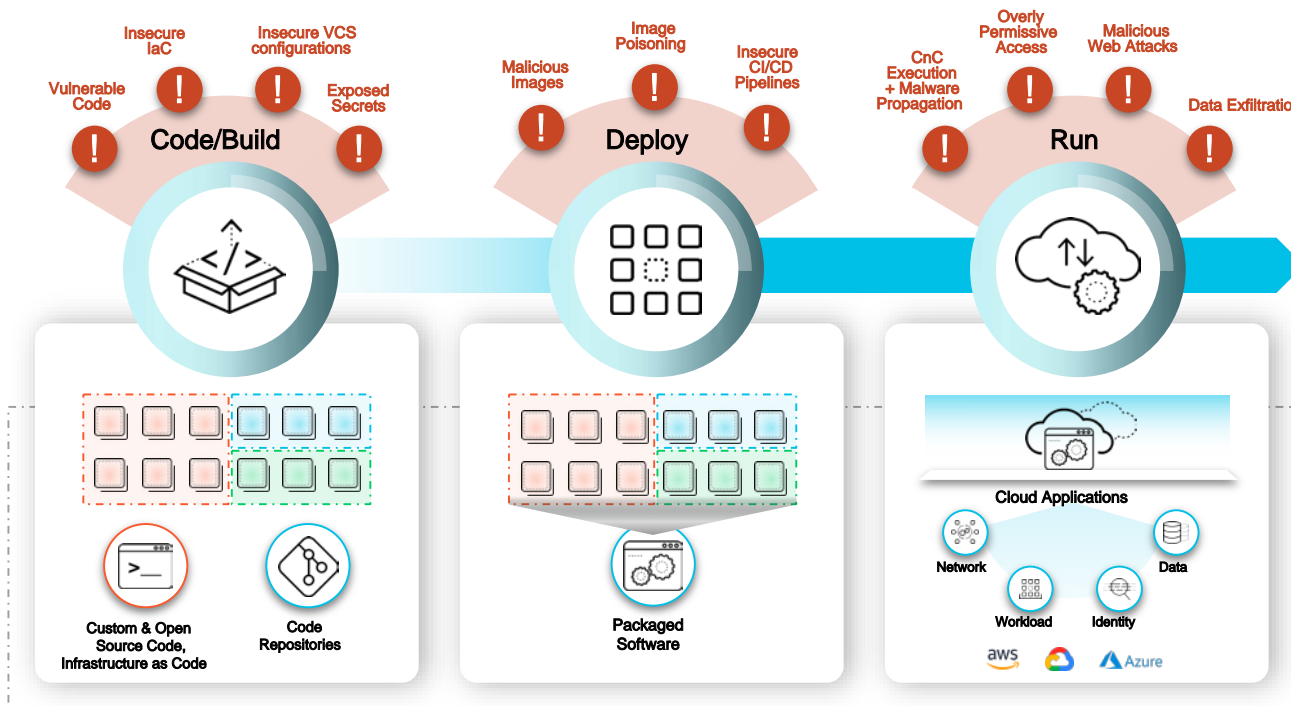


DevSecOps Pipeline

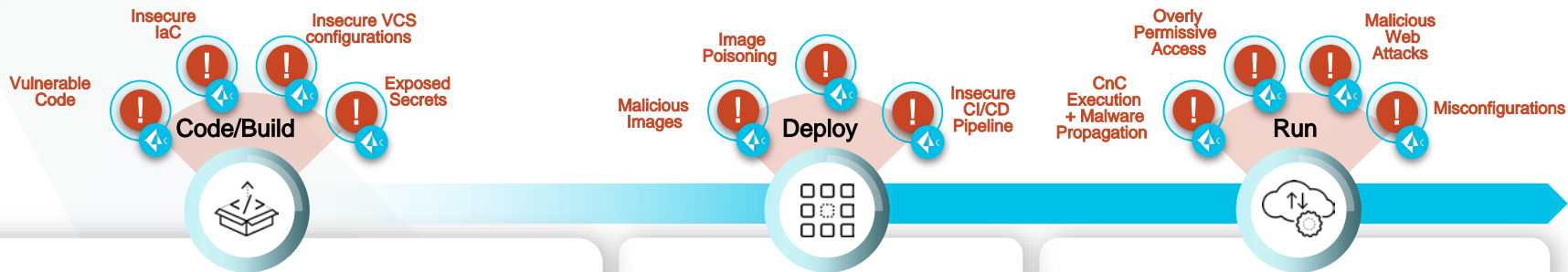


SECURITY RISKS & VULNERABILITIES AT EVERY STAGE IN CLOUD APPLICATIONS

Cloud applications are subject to various risks and vulnerabilities at every stage from Code to Runtime



PRISMA CLOUD CAPABILITIES



Repo Vulnerability Management (CCS)

Identify Vulnerabilities in Code Repos; Integrated with Host, Container, and Serverless capabilities.

IaC Security (CCS)

Find and fix misconfigurations in infrastructure as code templates.

Vulnerability Management and Compliance

Across hosts, images, containers, and serverless functions

Image Analysis Sandbox

Dynamically analyze the runtime behaviour of images before execution in production

Secrets Scanning

Identify and block secrets in IaC templates and container images ; prevent secrets exposure and account takeovers

Pipeline Configuration Management

Identify vulnerabilities in VCS configurations (e.g., branch protection rules to prevent code injection)

Access Control

Native admissions controller to prevent critical Kubernetes misconfigurations from ever being deployed.

CD Security

Continuously monitor container registries and serverless repos.

Trusted Images

Explicitly define trustworthy images, registries, repositories

Compliance & Governance

Compliance for all assets, near real time ingestion of new services / APIs.

Misconfig & Threat Detection (CSPM)

Advanced threat detection (network anomalies, UEBA) and remediation

Workload Protection (CWP)

For host, containers, serverless functions, web applications, and APIs. Agentless architecture options for vulnerability scanning and risk assessment

IAM Security (CIEM)

Enforce least privileged access, govern IAM -specific permissions, and prevent entitlement drift.

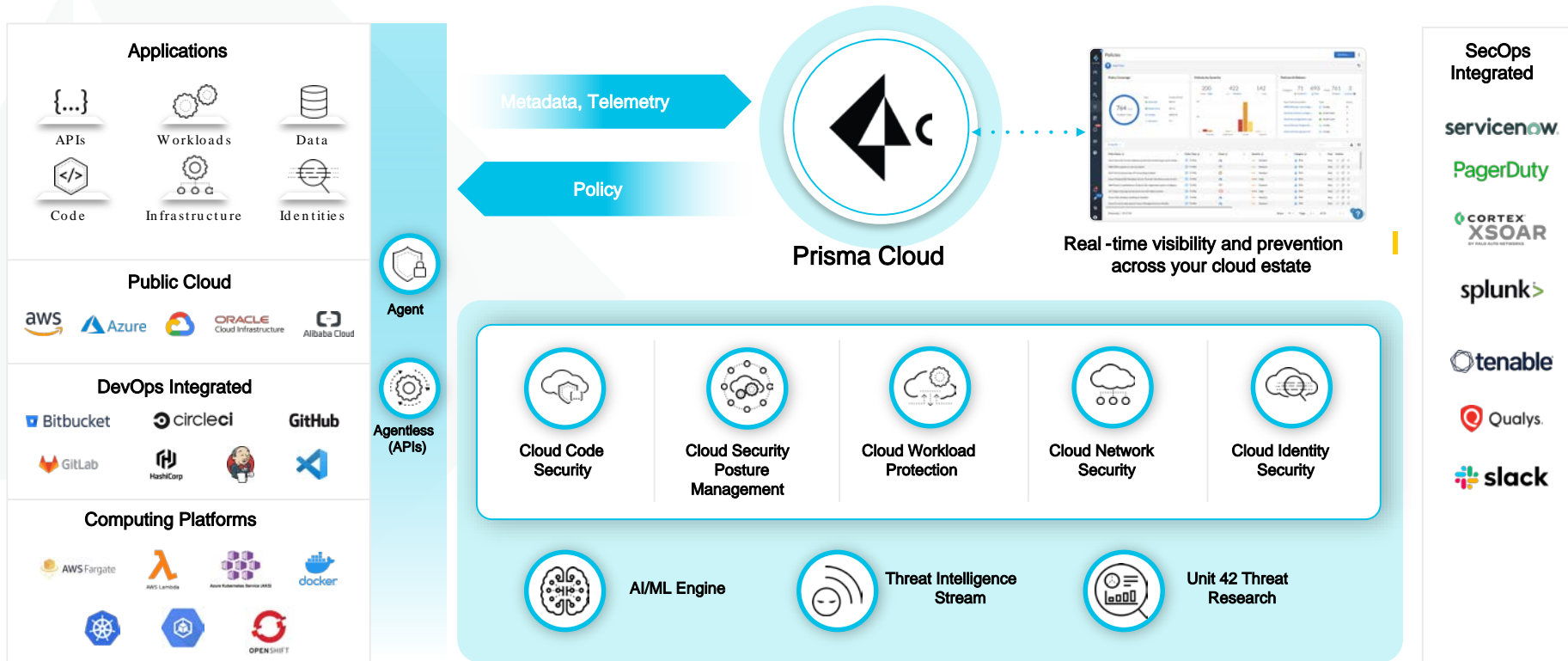
Data Security

DLP & Malware scanning for object stores

Network Security (CNS)

Microsegmentation for cloud -native workloads

PRISMA CLOUD ARCHITECTURE



Product Highlights

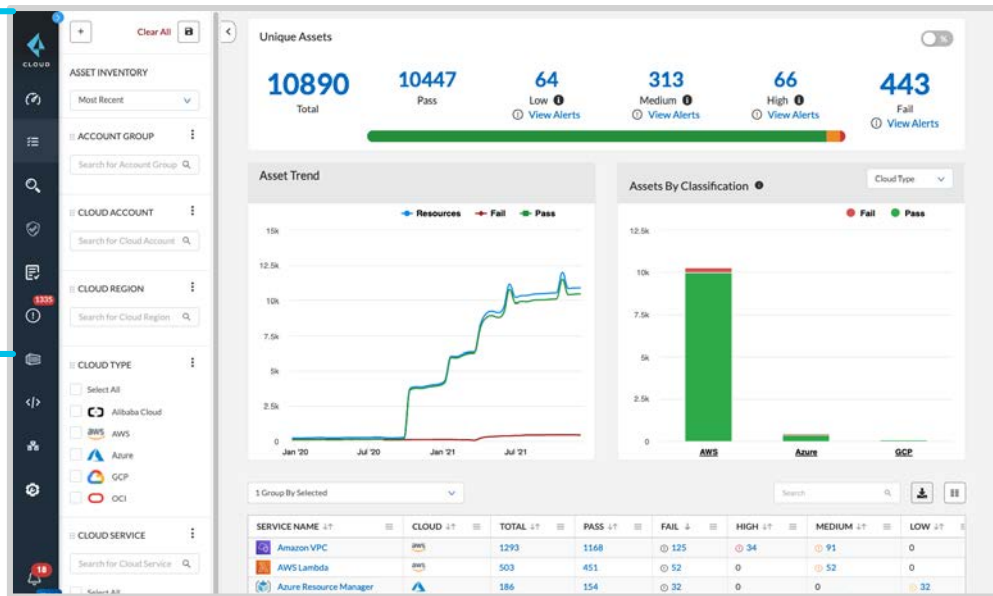
Cloud Security Posture Management to achieve compliance and secure multi -cloud environments

Multi -cloud visibility and security

Support for the world's 5 largest clouds, including AWS, Azure, Google Cloud, Alibaba Cloud, and OCI

Optimized compliance

Real-time and historical compliance with over 40 pre-build frameworks



Integrated threat detection

Monitor and analyze cloud audit logs and network flow logs to detect and prevent threats

Scan and secure public cloud data

Audit cloud storage and identify personal information and malware, integrated with WildFire

Easy onboarding and proven scalability

Unify users and cloud accounts in a single UI for managing and enabling cloud security

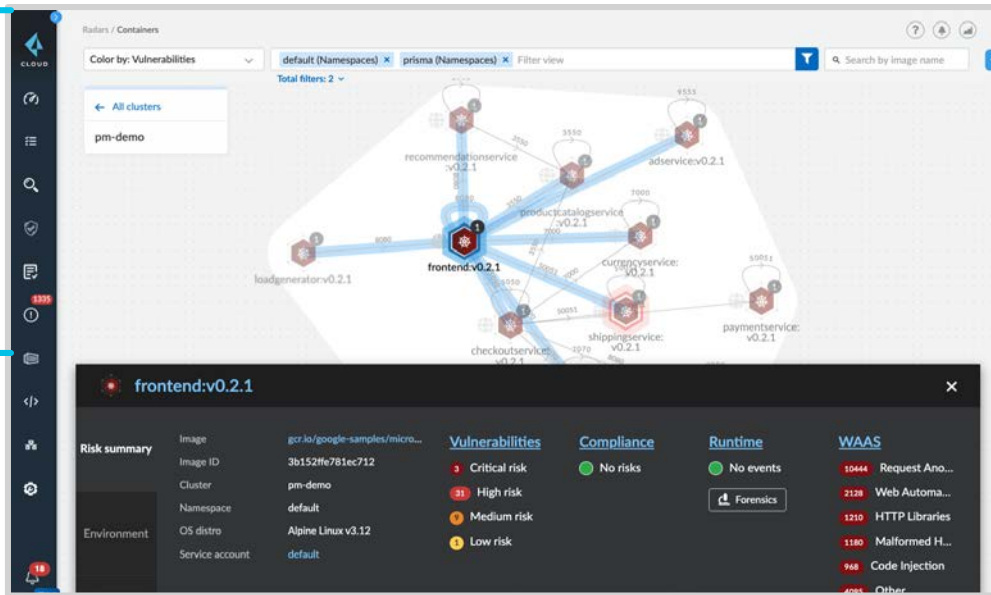
Cloud Workload Protection to secure hosts, containers, and serverless Functions

Agent -based protection and Agentless scanning

Protect hosts, containers, and serverless all from a central Console

Accurate vulnerability management

Recognized Leader in vulnerability management and risk prioritization across OS, images, and functions



Runtime protection and forensics

Secure all application tech stacks and investigate events and incidents

Cloud native compliance

400+ checks covering the Linux, Docker, and Kubernetes CIS Benchmarks, plus Windows and Istio

Integrated Web Application & API Security

Protection including OWASP Top 10, API protection, bot risk management, and more

Thank you

