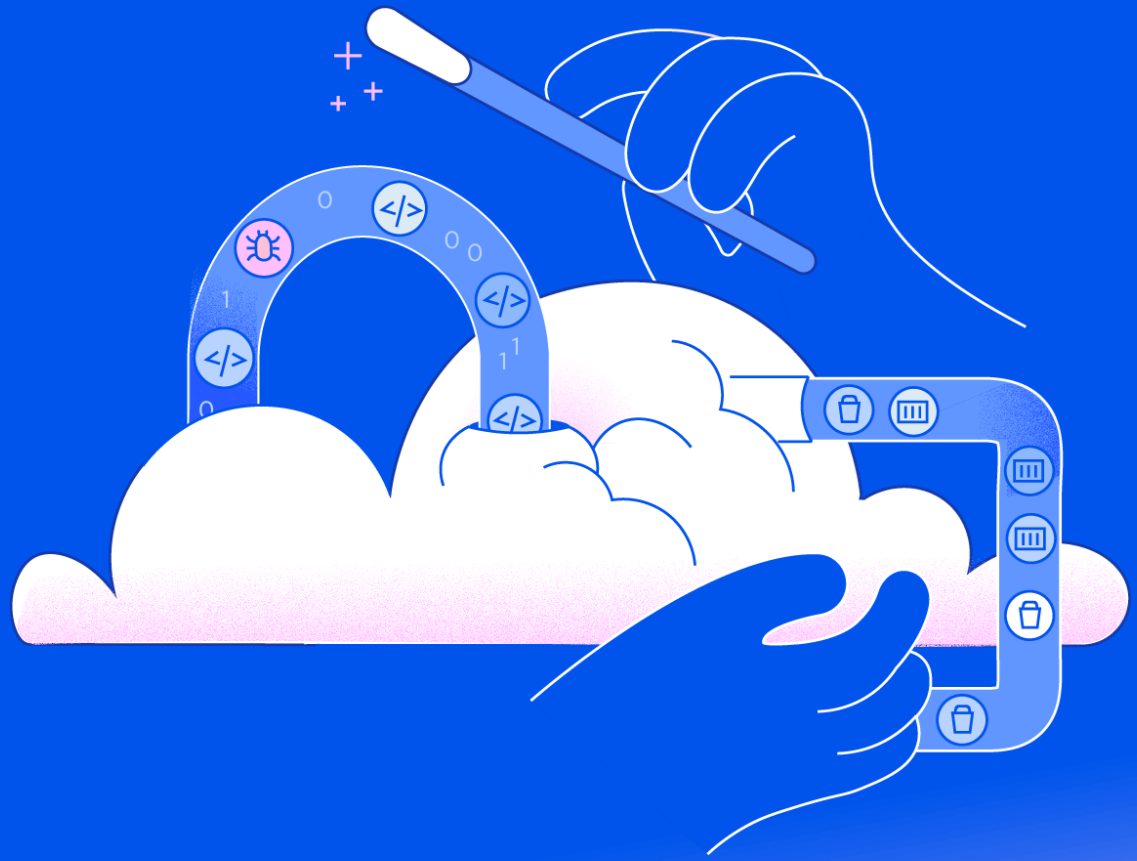
WIZ

Protect Everything You Build and Run in the Cloud



Contact :
(주)한국밸런스
영업대표 김형덕
010-7138-8889
hdkim@valence.co.kr

(주)한국밸런스

The Largest Private Cybersecurity Company

$1.9B raised

Index Ventures · THRIVE CAPITAL · INSIGHT PARTNERS · SEQUOIA · Lightspeed · andreessen horowitz

Enabling Security Impact

50% Of Customers achieve 0 Criticals

>50% Of Active Users are Devs/DevOps

The Leader in Cloud Security

G2 Grid for Cloud-Native Application Protection Platforms (CNAPP)

Industry leading global tech companies secure their cloud with Wiz

intel · Morgan Stanley · BARCLAYS · Bristol Myers Squibb · FARMERS INSURANCE · COLGATE-PALMOLIVE · Capital One · GitHub · salesforce · DELTA

Pfizer · MassMutual · Blackstone · KAISER PERMANENTE · Chick-fil-A · COSTCO WHOLESALE · slack · BMW · NBA

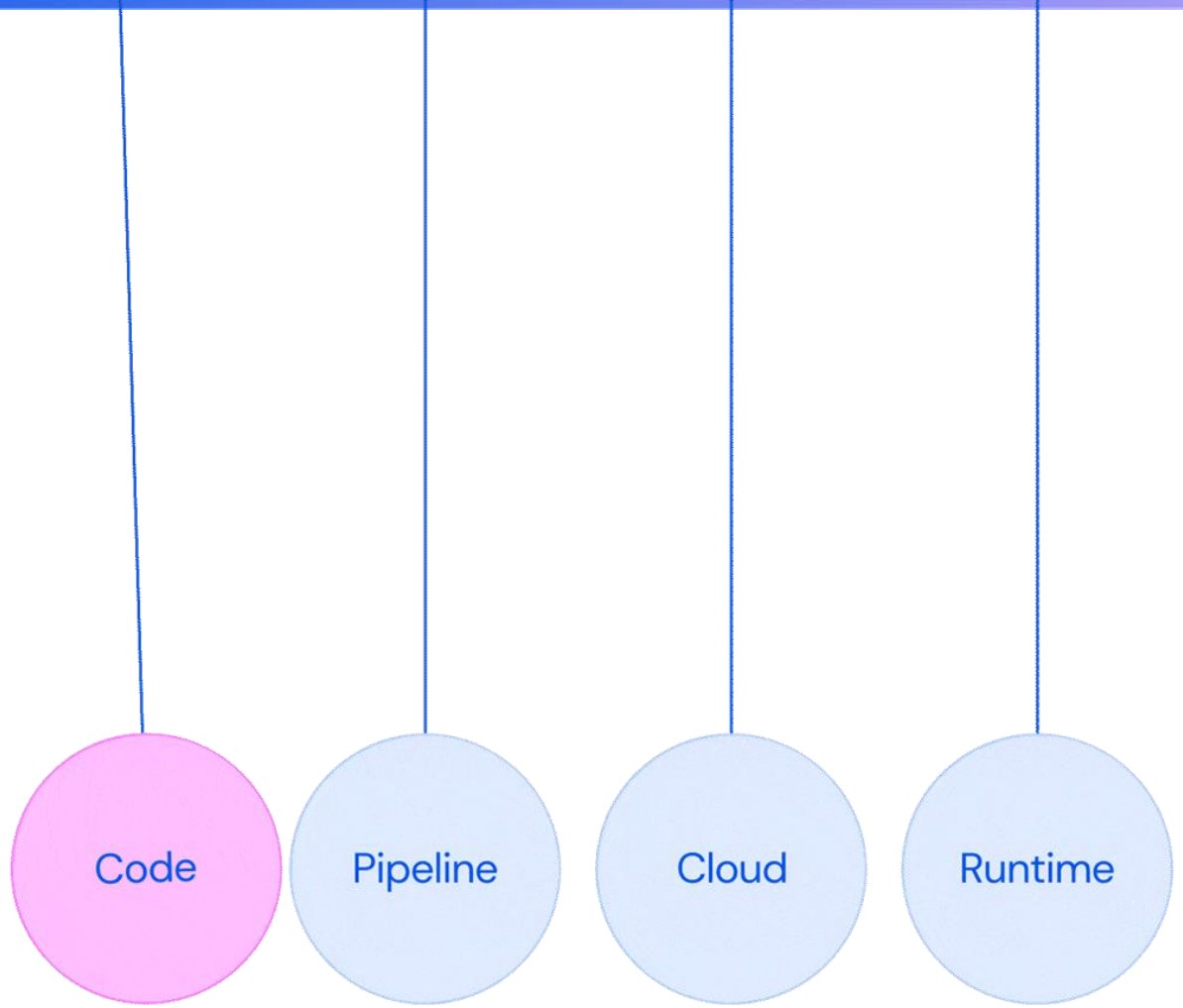
AON · JPMorgan Chase & Co. · Goldman Sachs · Elevance Health · LVMH · The Home Depot · CISCO · snowflake · Honeywell · Chevron

New York Life · Fannie Mae · MERCK · abbvie · Sysco · Chipotle Mexican Grill · EA · BlackRock · UNITED · FOX

WIZ

Cloud changes everything.

Development is now agile and continuous.



Code

The blueprint of every cloud application starts in code

Pipeline

That code is deployed through multiple pipelines

Cloud

Deployments replicate across scalable cloud infrastructure

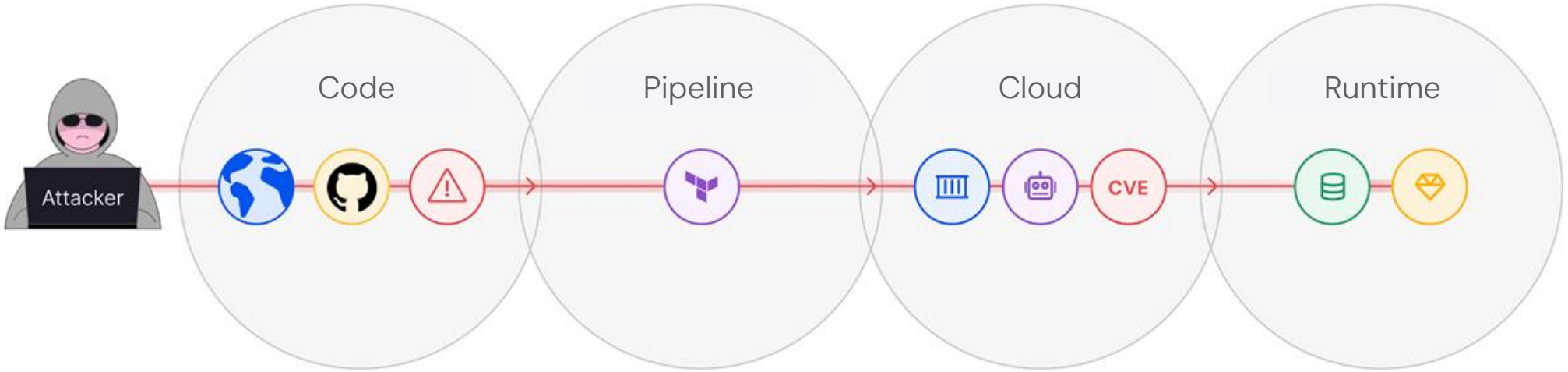
Runtime

Applications run at runtime, serving users and scaling

WIZ

Attackers target your cloud applications- not your org chart.

They don't distinguish between code, application, or infrastructure layers.



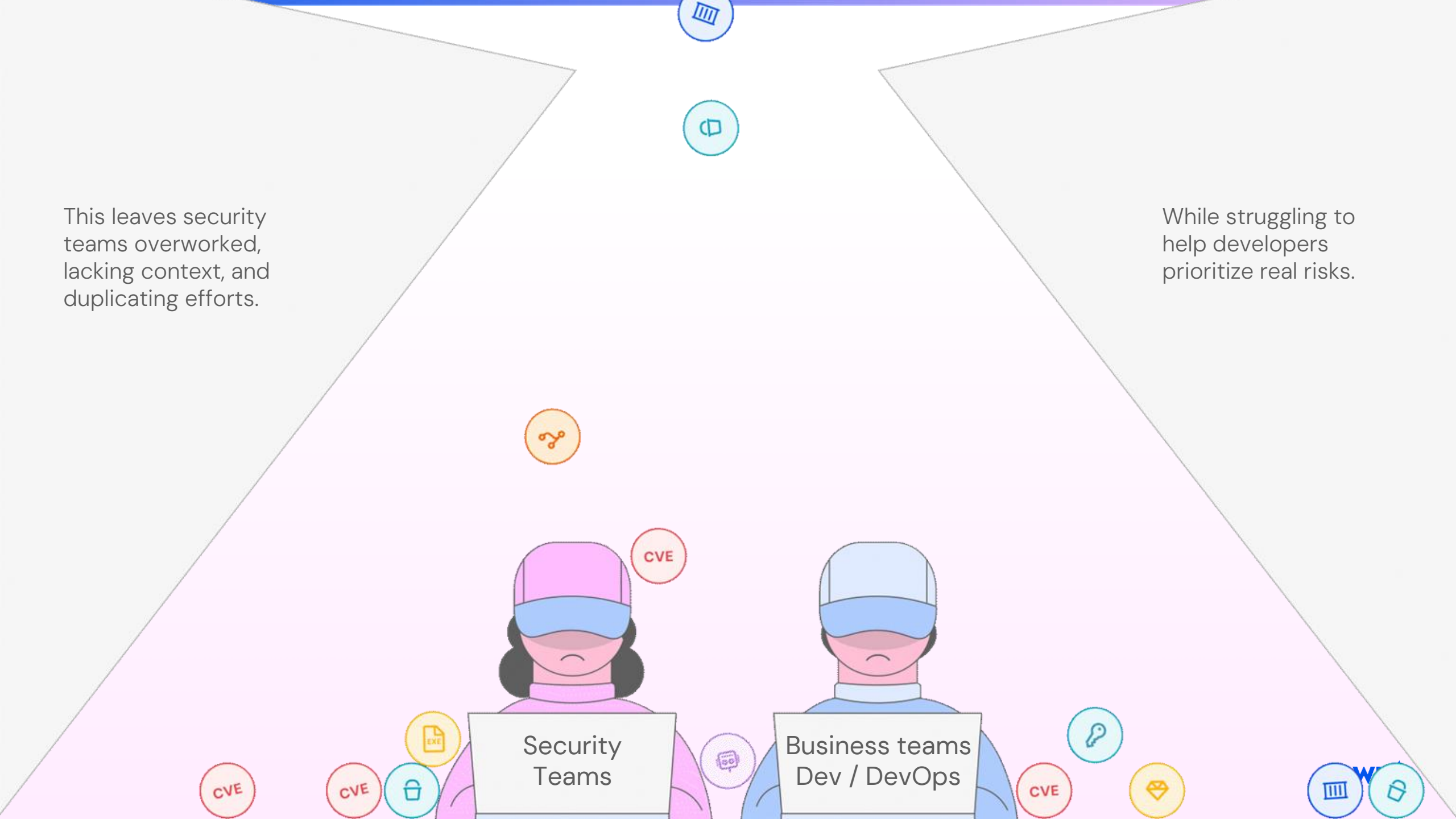
They simply look for the easiest way in.

WIZ

Yet security remains siloed, stacked vertically

This leaves security teams overworked, lacking context, and duplicating efforts.

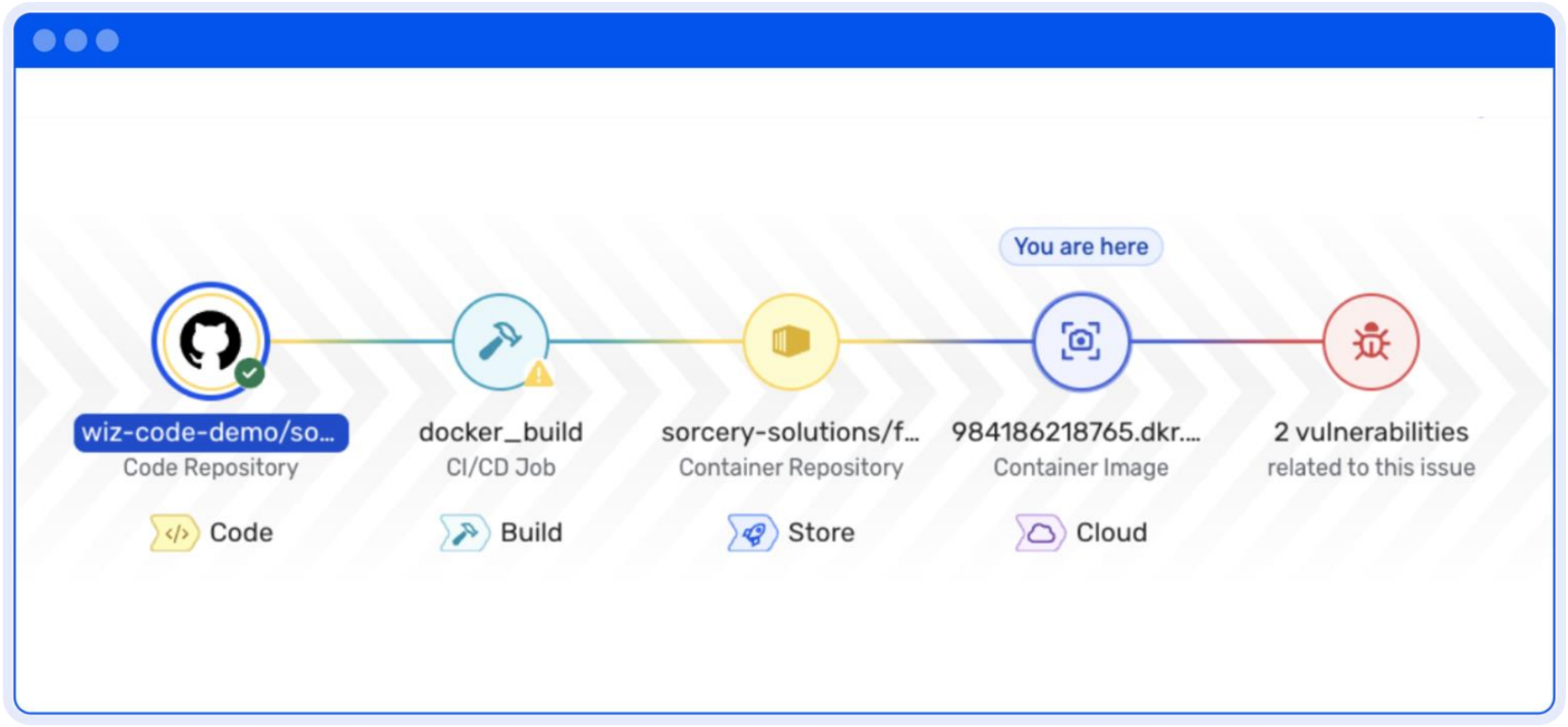
While struggling to help developers prioritize real risks.



How Is Your Organization Approaching These Challenges Today?

Our approach - a new operating model for cloud

“Horizontal” security from code to cloud



One security platform - from code to cloud to runtime

Our approach - a new operating model for cloud

“Horizontal” security from code to cloud

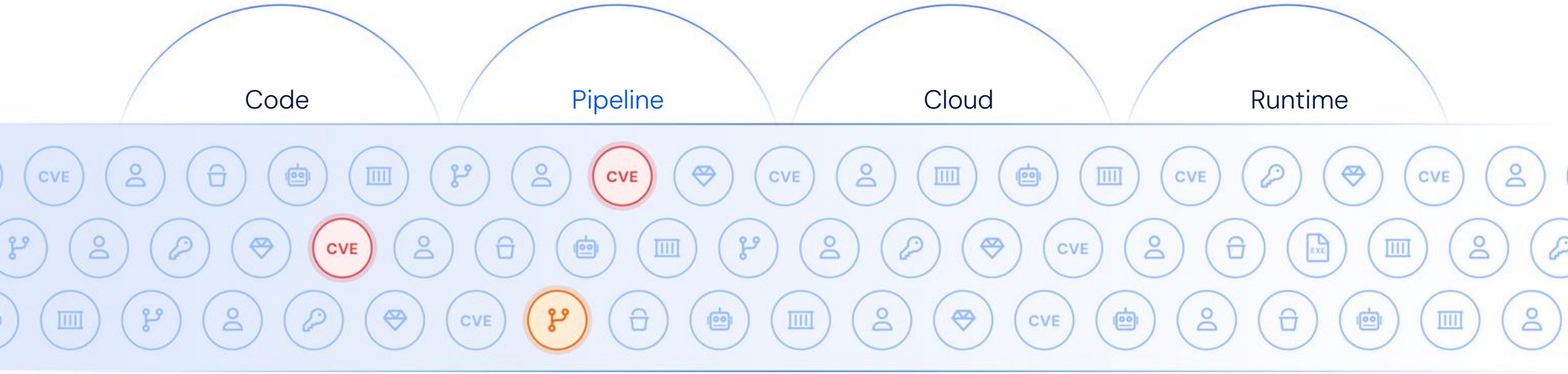
One security platform - from code to cloud to runtime

Wiz scans code directly in the IDE and pull requests, helping developers catch risks where they work and trace issues back to the root cause.

Our approach - a new operating model for cloud

“Horizontal” security from code to cloud

One security platform - from code to cloud to runtime

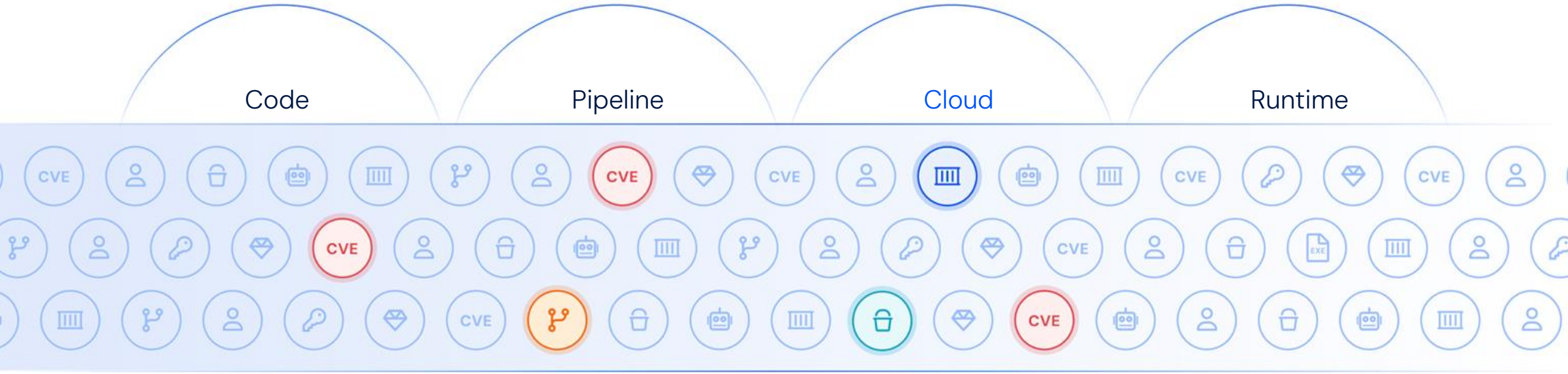


Wiz scans and maps your CI/CD pipeline, blocking risky changes before they ever reach production.

Our approach - a new operating model for cloud

“Horizontal” security from code to cloud

One security platform - from code to cloud to runtime

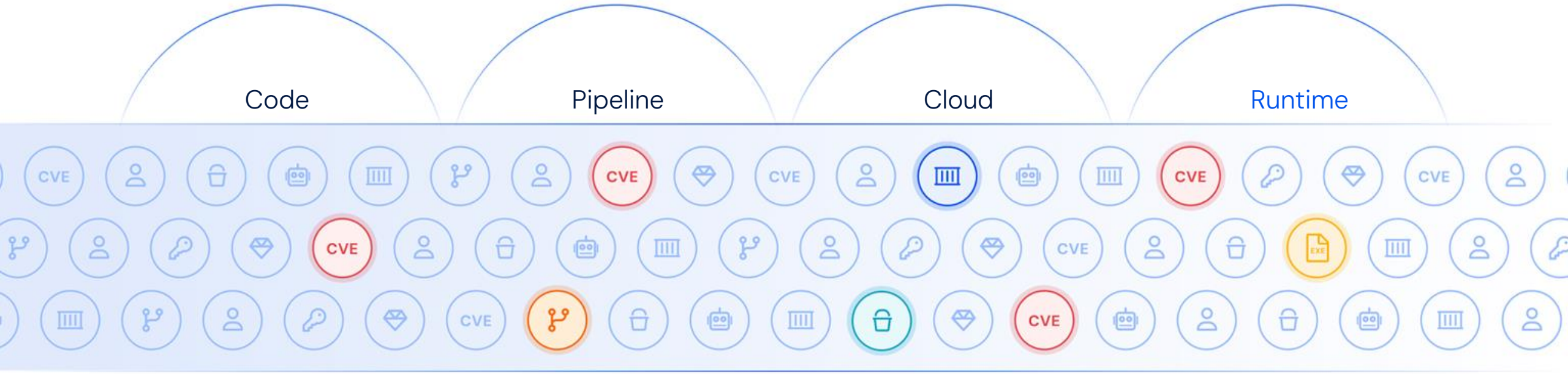


Wiz gives you a complete pictureof your cloud: mapping architecture, surfacing risks, and showing exposure, assets, and ownership.

Our approach - a new operating model for cloud

“Horizontal” security from code to cloud

One security platform - from code to cloud to runtime



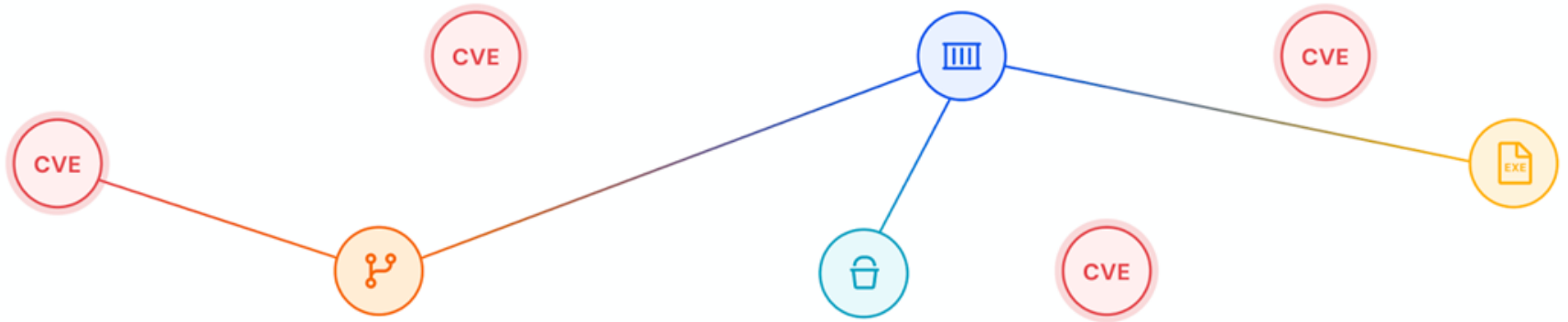
Wiz detects and blocks active attacks in runtime, giving you real-time protection for your workloads and cloud resources.

WIZ

WIZ | Security from code to cloud

Mapping this all on the Wiz C2C Security Graph allows
Wizto trace the true lineage of code and app.

For example, linking a CVE found in code to the cloud infrastructure it's deployed on, and confirming the vulnerable library is loaded and running

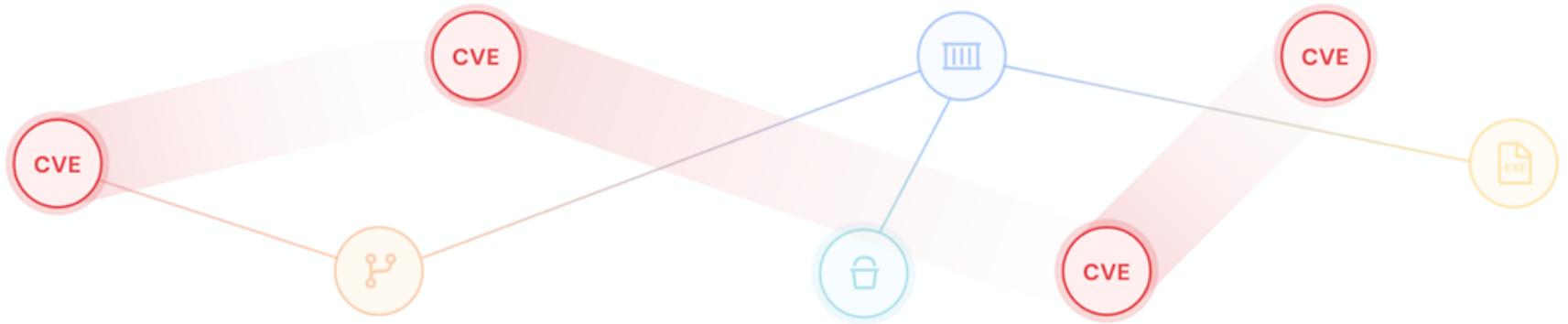


WIZ

WIZ | Security from code to cloud

Mapping this all on the Wiz C2C Security Graph allows
Wizto trace the true lineage of code and app.

For example, linking a CVE found in code to the cloud infrastructure it's deployed on, and confirming the vulnerable library is loaded and running



WIZ | Security from code to cloud

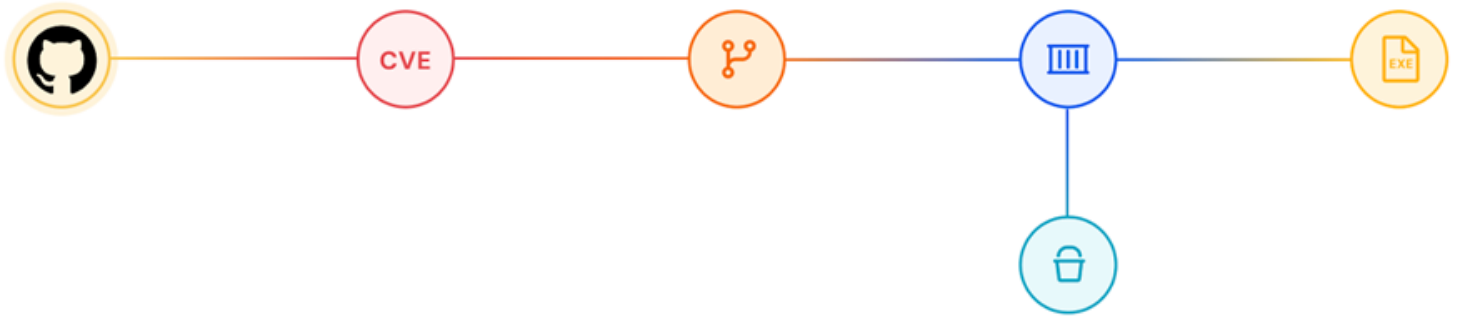
Mapping this all on the Wiz C2C Security Graph allows
Wizto trace the true lineage of code and app.

For example, linking a CVE found in code to the cloud infrastructure it's deployed on, and confirming the vulnerable library is loaded and running

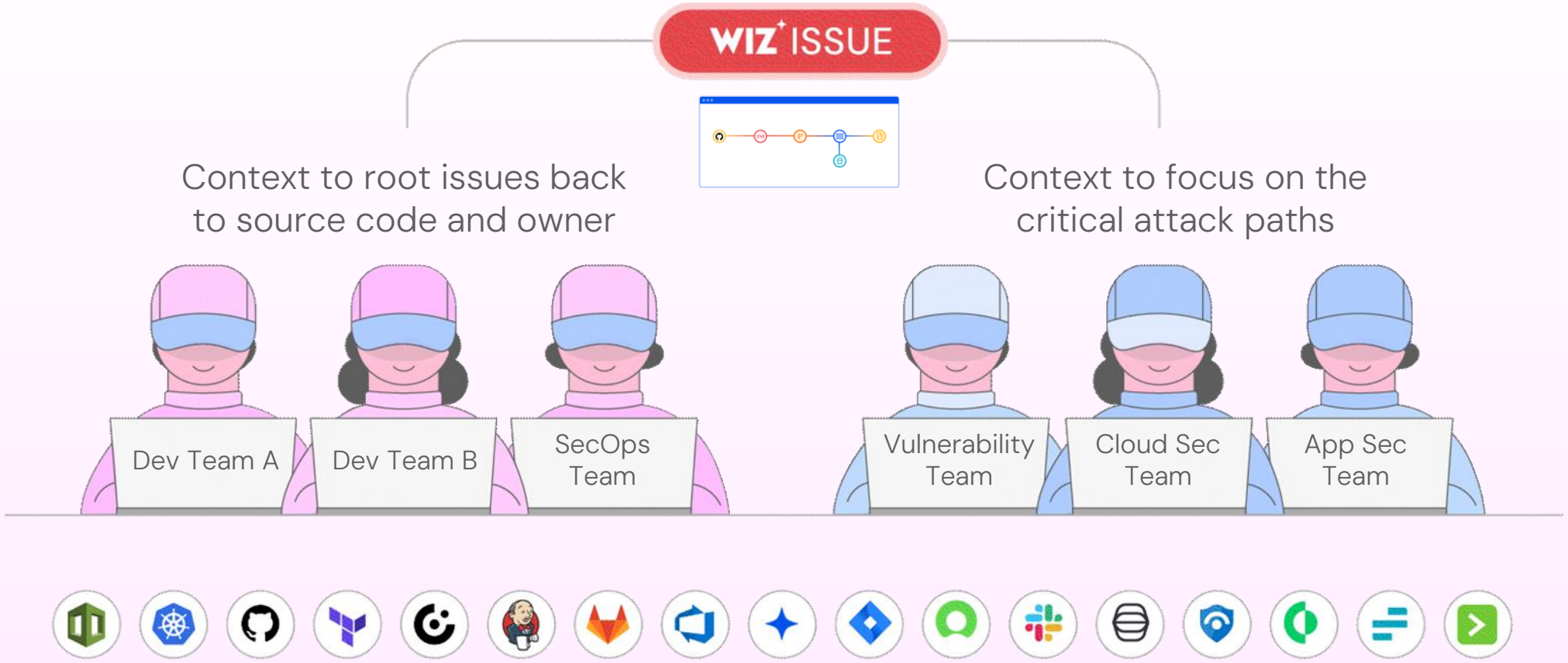
WIZ | Security from code to cloud

Mapping this all on the Wiz C2C Security Graph allows
Wizto trace the true lineage of code and app.

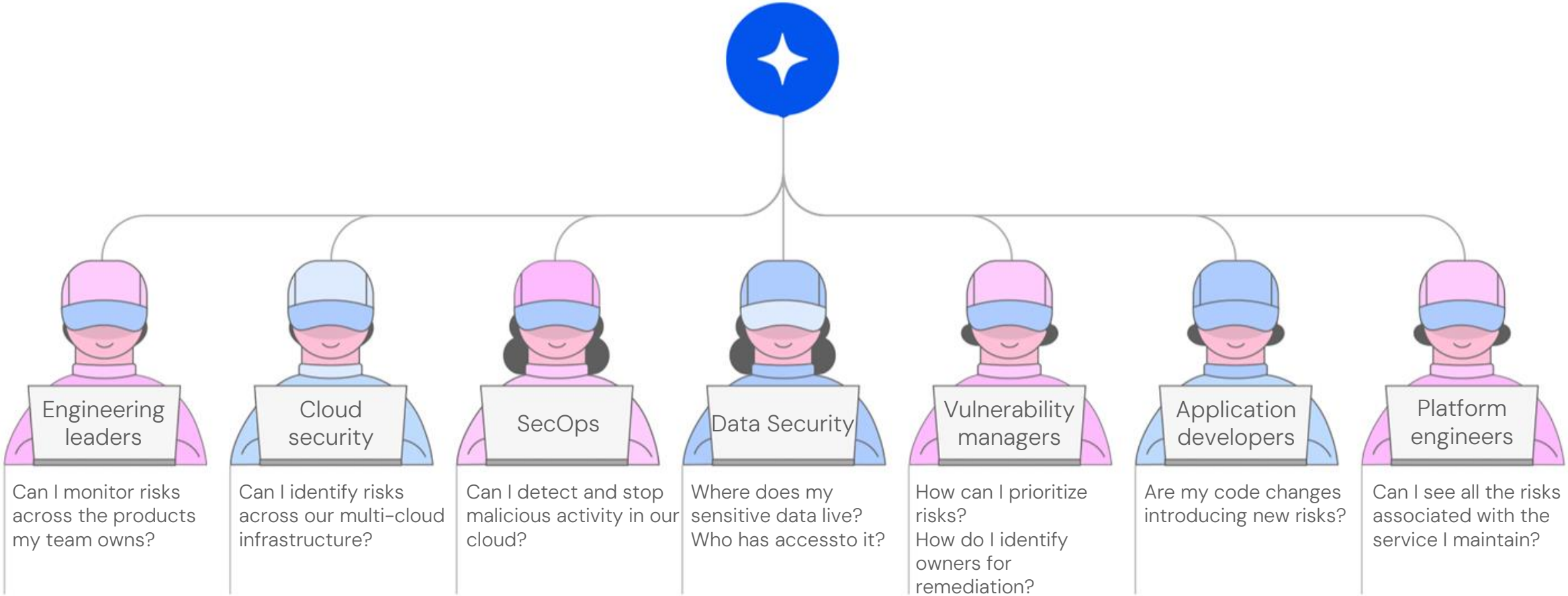
And then suggesting a CODE FIX for the vulnerability, with full context that it's actively running in production on a resource with data access.



Resulting in prioritized risks to the right team with the right context



Enable each stakeholderby democratizing security



One platform for the

Modern cloud security operating model

Code | Pipeline | Cloud | Runtime

CLOUD TO CODE
Root cause analysis for risks and threats

CODE TO RUNTIME
Anomalous behavior detection across the SDLC

Unified scanning, policy framework, and code-cloud-runtime context

WIZ Code

Secure Cloud Development

Secure every stage of your SDLC to gain visibility & prevent risks from reaching your cloud

WIZ Cloud

Manage Security Posture

Agentless visibility & risk prioritization that proactively reduces the attack surface

WIZ Defend

Respond to Cloud Threats

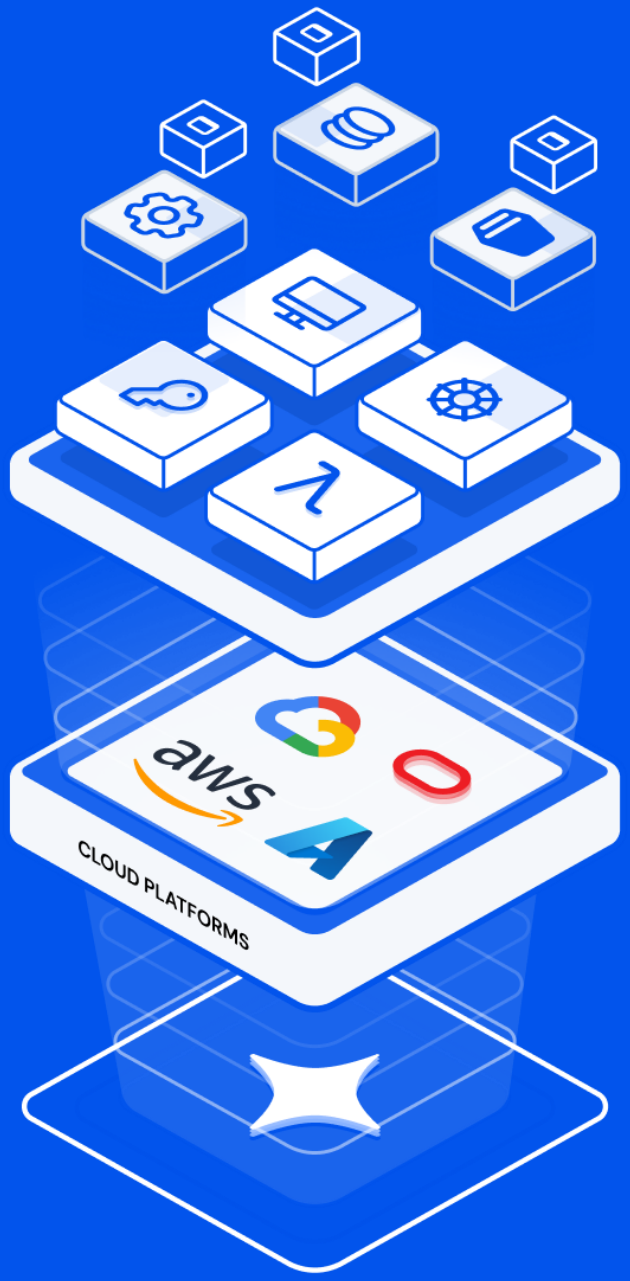
Cloud events and lightweight eBPF-based sensor to stop threats from becoming breaches

Vulnerabilities | Identity | Configuration | Data And AI | Public Exposure | Secrets

AI Agents, Engines, and Assistants

WIZ

The Technology



The cloud security operating platform

Scan your cloud without agents and build the graph

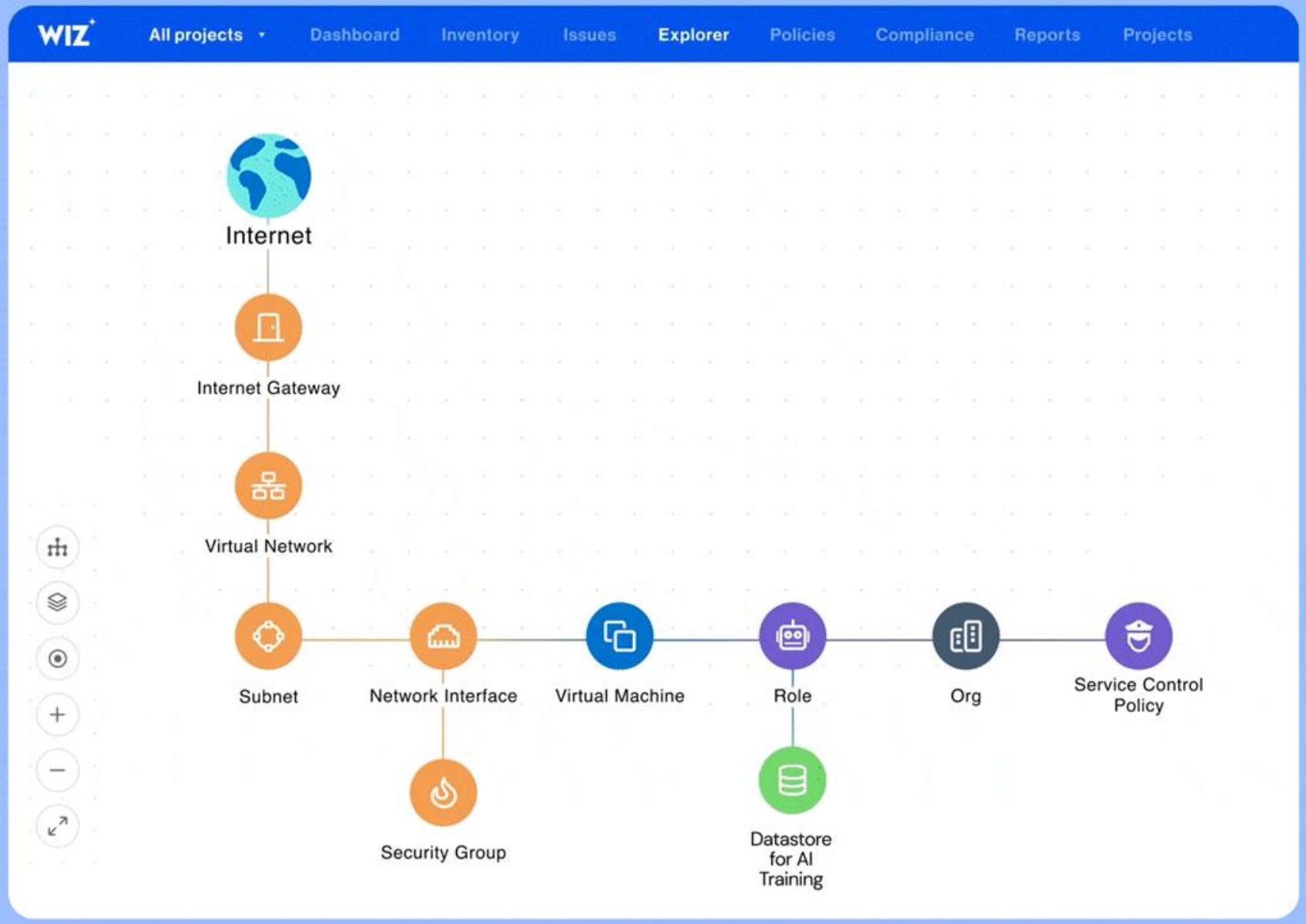
- Serverless
- Containers
- VMs
- PaaS

1 **Cloud operating path**
Gain visibility

The cloud security operating platform

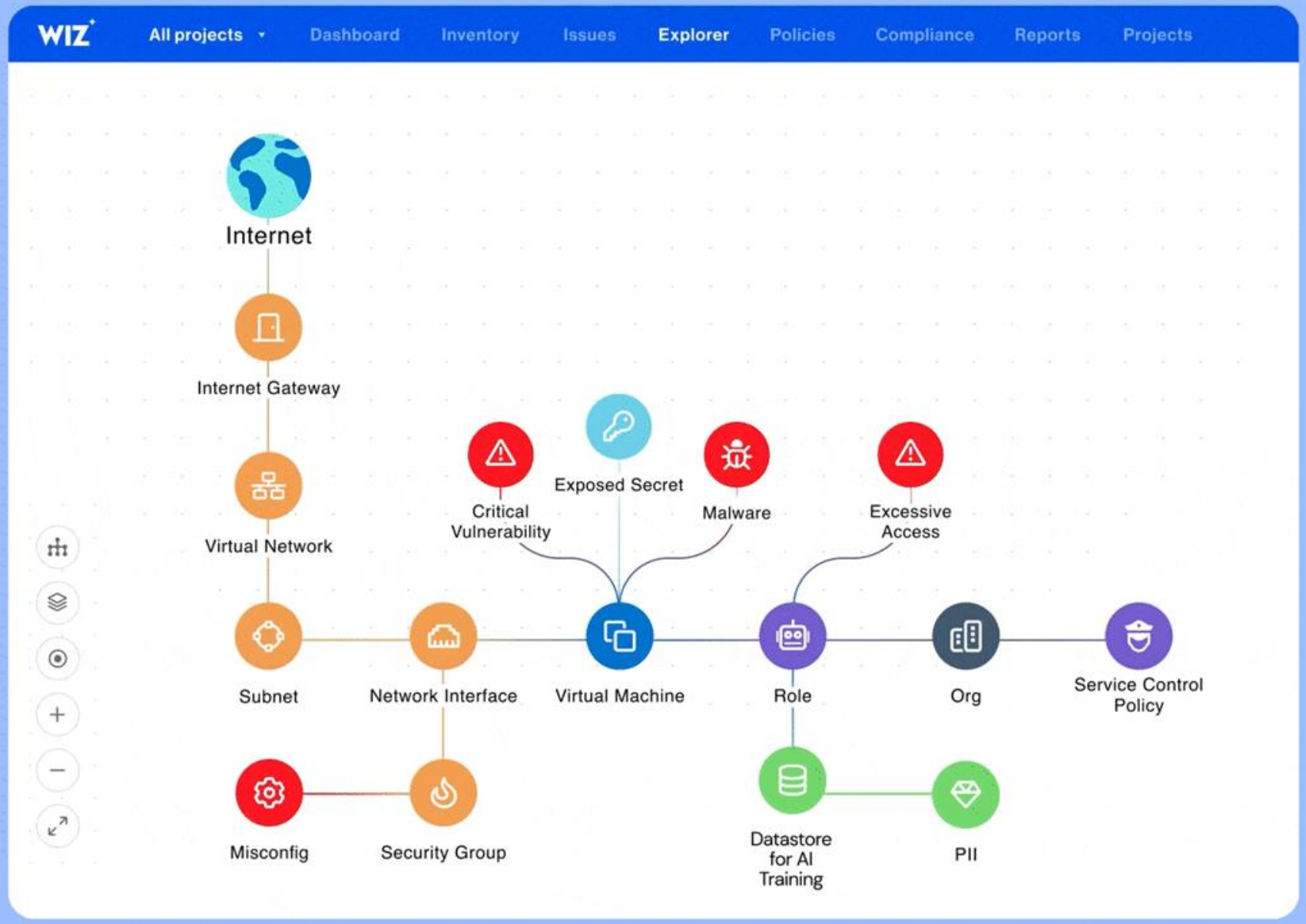
Identify risks

- Misconfigurations
- Vulnerabilities
- Malware
- Sensitive data
- External exposure
- Excessive permissions
- Exposed secrets
- Lateral movement
- AI risks
- Novel vulnerabilities and attacks
- Business impact



The cloud security operating platform

Prioritize attack paths



2 **Cloud operating path**
Reduce critical risks

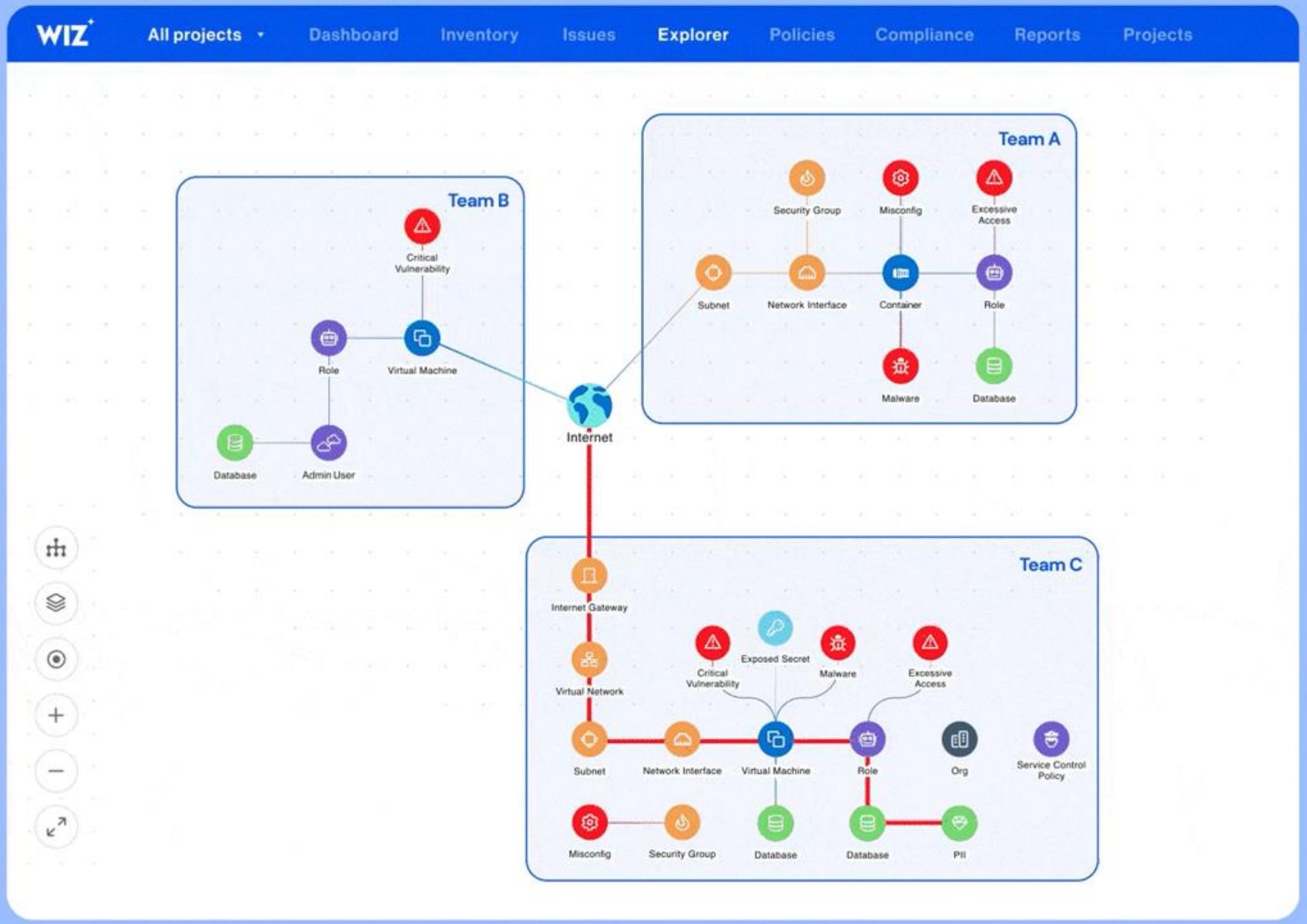
The cloud security operating platform

Determine ownership for democratization

3 Cloud operating path
Democratize security

The cloud security operating platform

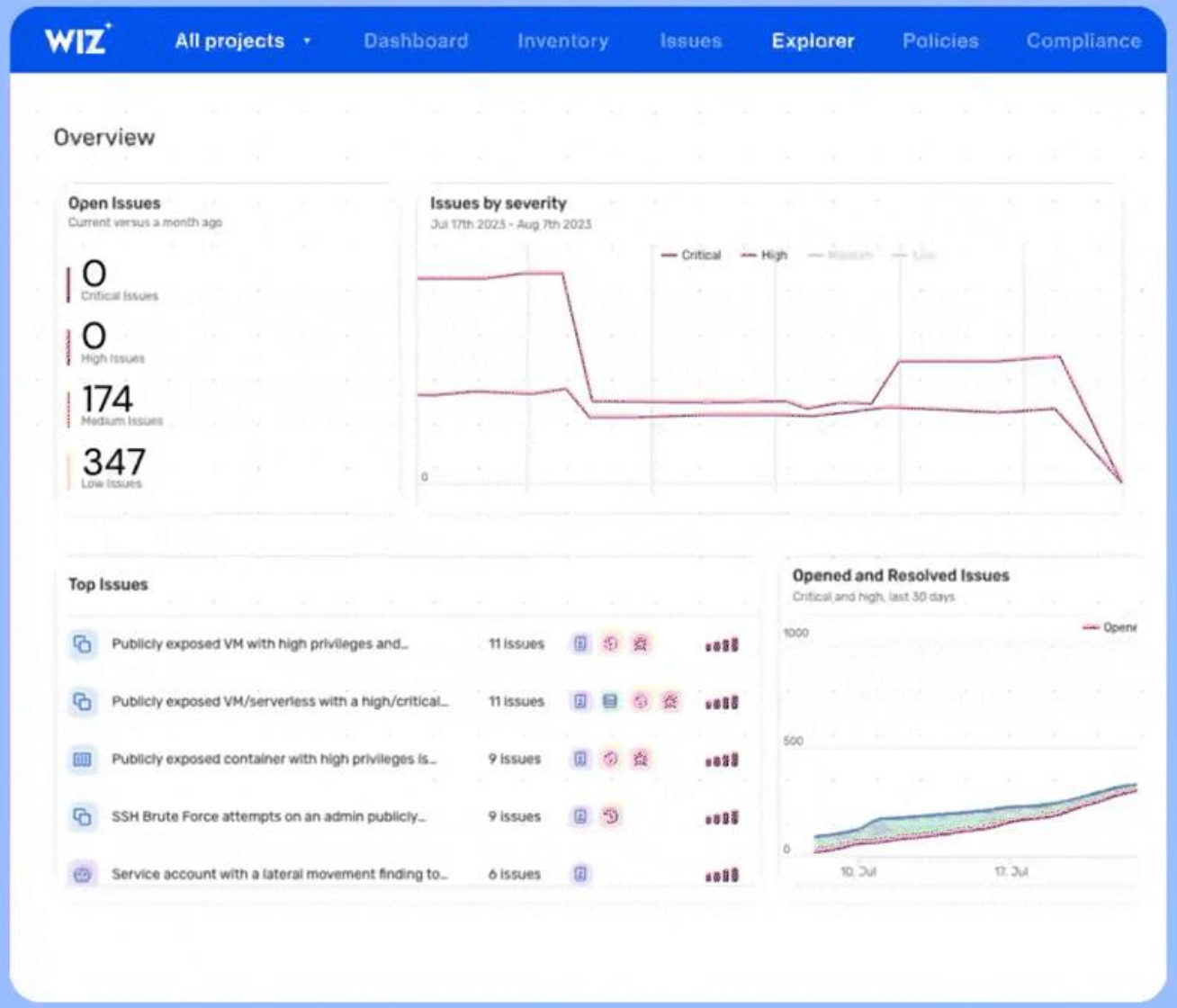
Automate workflows to speed remediation



3 **Cloud operating path**
Democratize security

The cloud security operating platform

Build securely by design, all the way from IDE to deployment



Team A

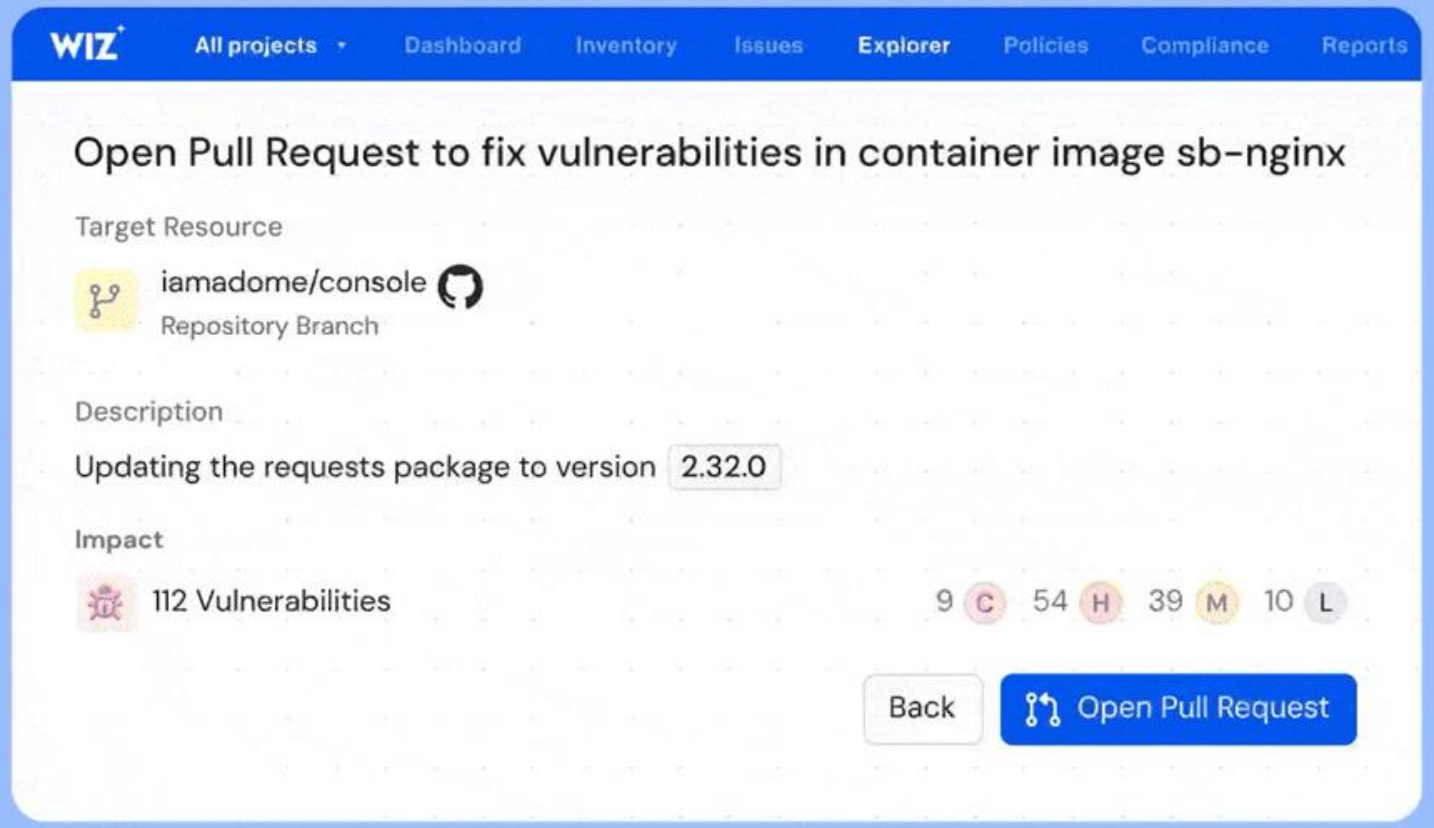
Team B

Team C

4 Cloud operating path
Develop securely

The cloud security operating platform

Code-to-cloud context enables efficient remediation at root cause - code

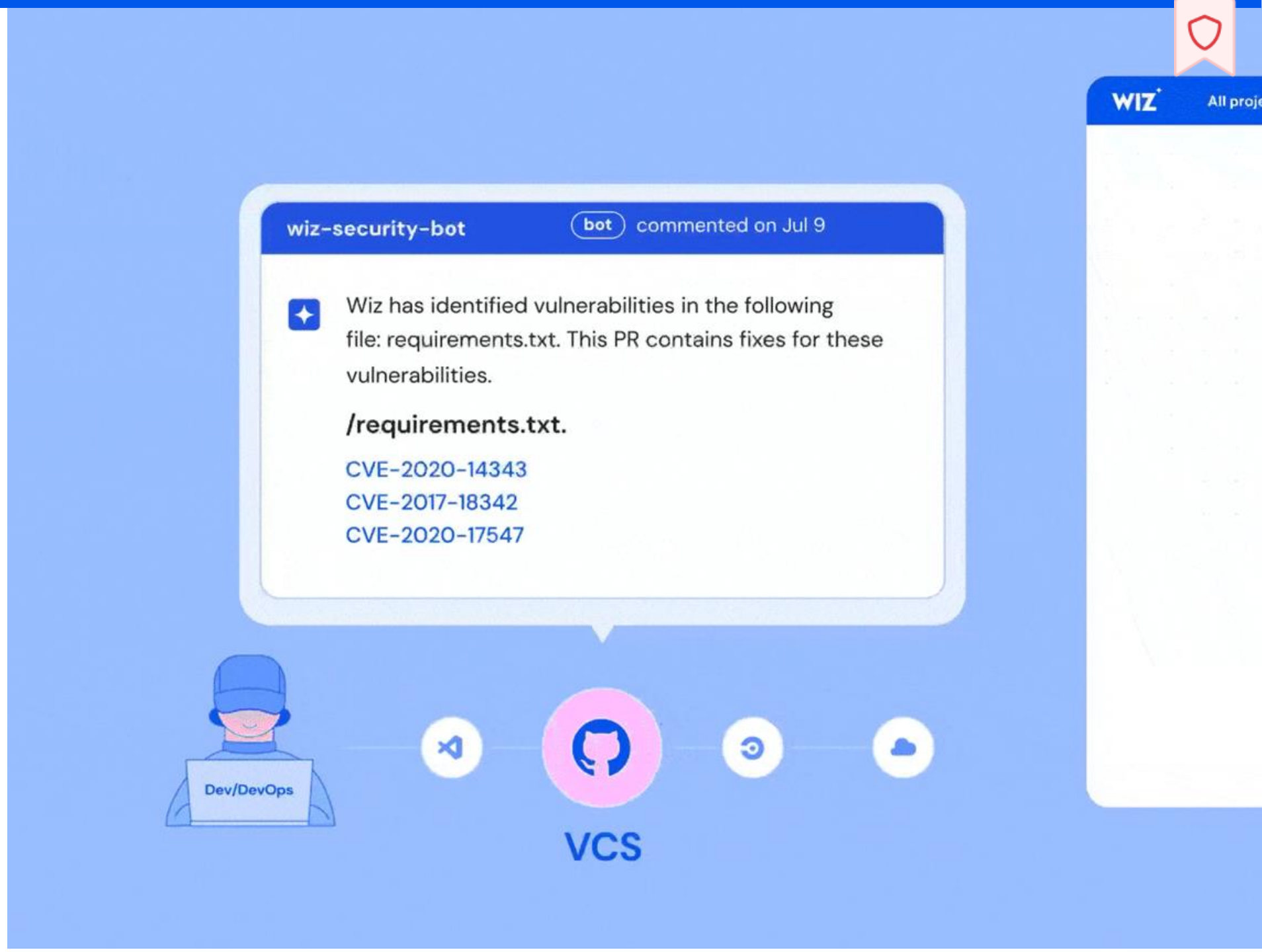


4 Cloud operating path
Develop securely

Cloud

The cloud security operating platform

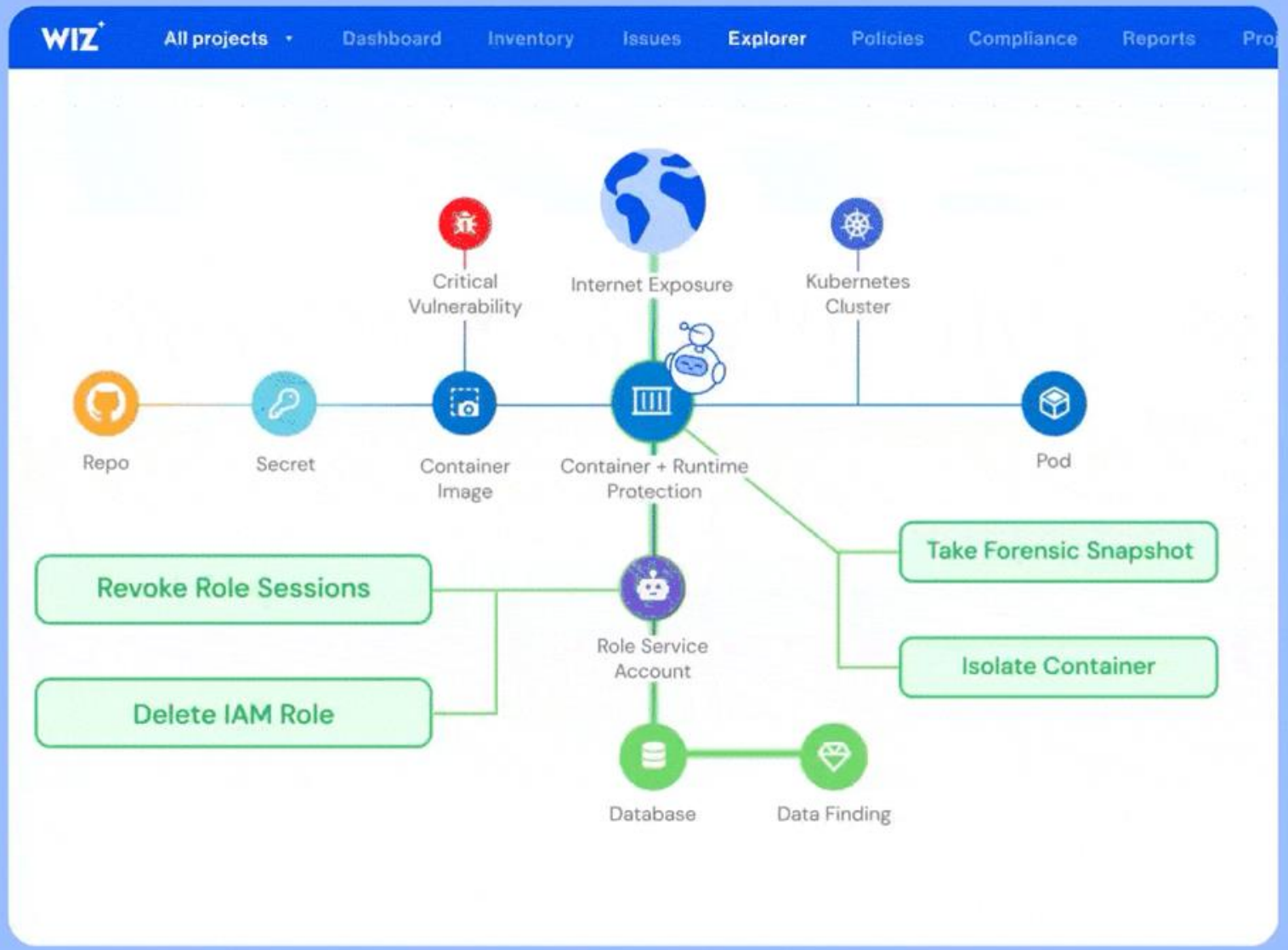
Detection and response born for cloud workloads



5 Cloud operating path
Transform cloud SecOps

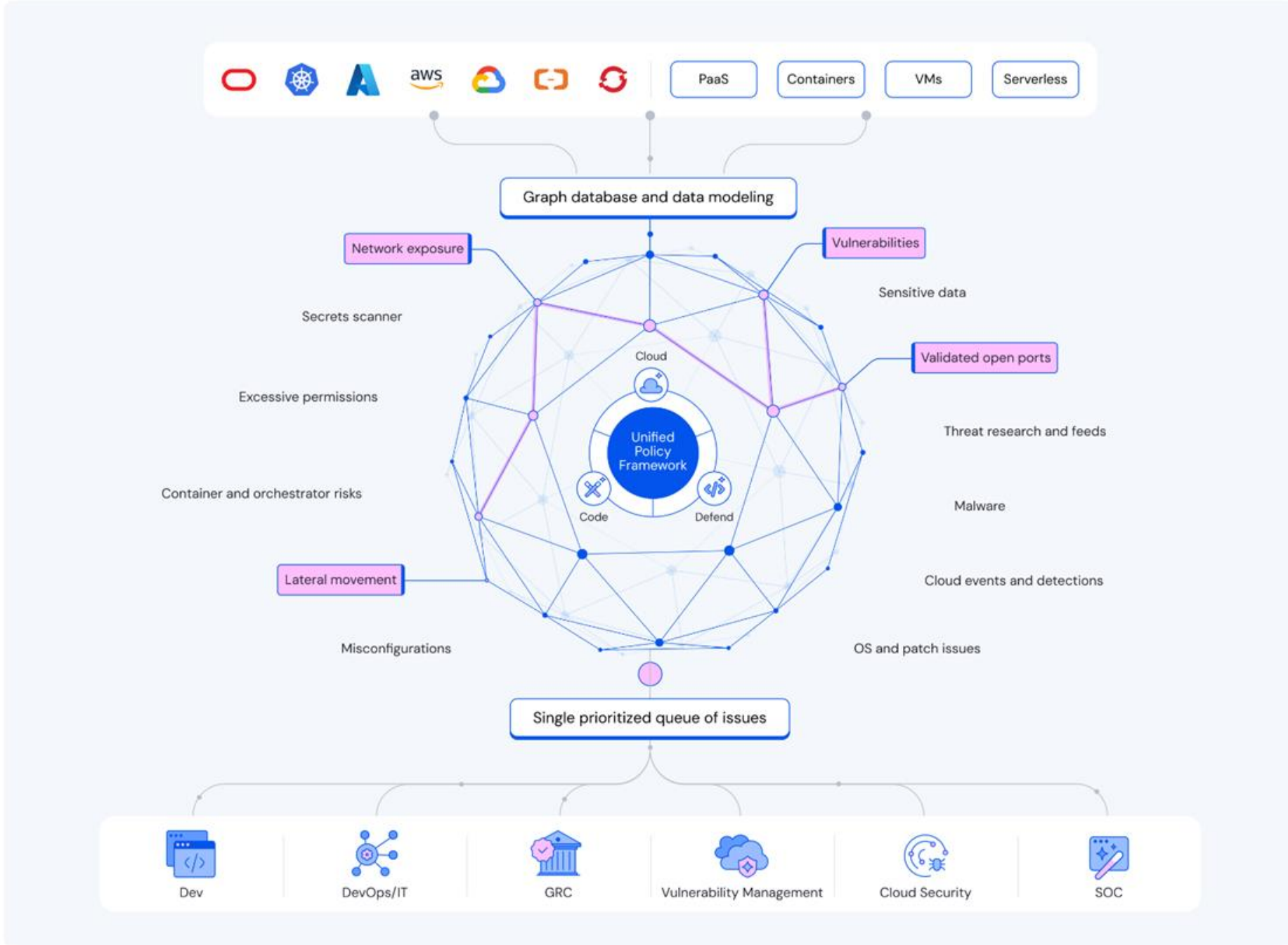
The cloud security operating platform

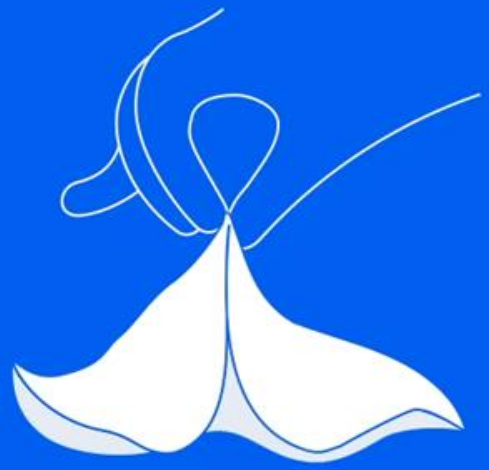
Use cloud to runtime context for greater prioritization



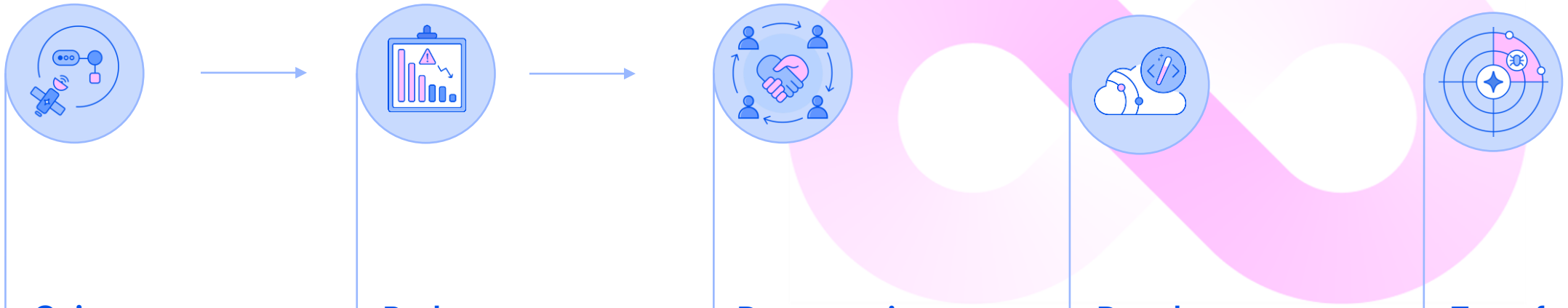
The cloud security operating platform

Born for the cloud, Wiz CNAPP is the platform to secure your cloud from code to runtime





Cloud Security Maturity Framework



Gain Visibility

100% code-to-cloud visibility into any repo, pipeline, and cloud

Normalize across clouds and architectures to simplify security

Map app and infrastructure ownership and business context

Reduce Critical Risk

360° understanding of workload, cloud, data, SDLC & compliance risks

Prioritize attack paths that are validated with runtime context

Clear context, guidance, 1-click PR fixes, and swap opportunities for secured container images to reach 0 critical risks fast

Democratize Security

Automate high-fidelity alerts to the right owners for proactive remediation

Ingrain security into the development process through self-service

Monitor and report on security KPIs and trends by business unit

Develop Securely

Give devs cloud context directly in IDEs and code for secure by design

Enforce code-to-cloud guardrails to prevent issues from ever being deployed

Start secure with zero-CVE container images

Protect the software supply chain with SBOM and risk assessment of OSS and 3rd party components

Transform Cloud SecOps

Comprehensive coverage and monitoring for cloud-native threats

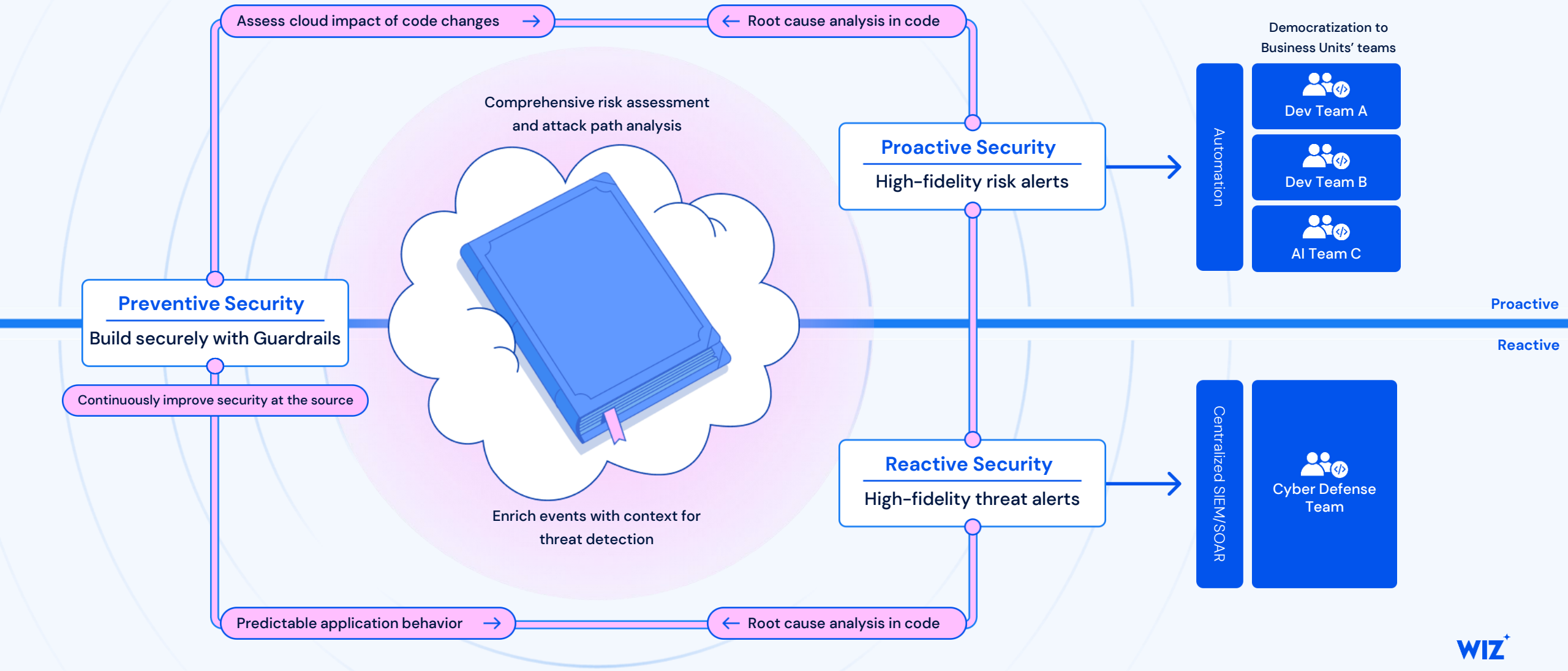
Rapid investigation and AI assistance that speeds analysis and upskills analysts

Runtime blocking and one-click containment playbooks to speed MTTR

WIZ

The Cloud Operating Model

Breaks the siloes between your engineering and security teams
to achieve defense-in-depth and continuous security improvement



Driving outcomes

Effectiveness

50% Of customers achieve 0 criticals

- Attack path analysis
- Prioritization
- Automated workflows

Efficiency

50% Of active users are Dev/DevOps

- Democratization
- Tool consolidation
- Triage to code

Acceleration

<24hr Immediate visibility to emerging threats

- Complete visibility
- Cloud & AI adoption
- Technology inventor

Impact.
We are impact obsessed.

Enabling security teams to win at risk reduction.

Bringing Sec, Dev, and Ops together in a cloud security program.

Enabling teams to build faster in the cloud.

WIZ

Wiz is a Leader with the Highest Score in the Current Offering Category

Forrester Wave™ for Cloud Native Application Protection Solutions, Q1 2026

Wiz received the highest possible score in these criteria:

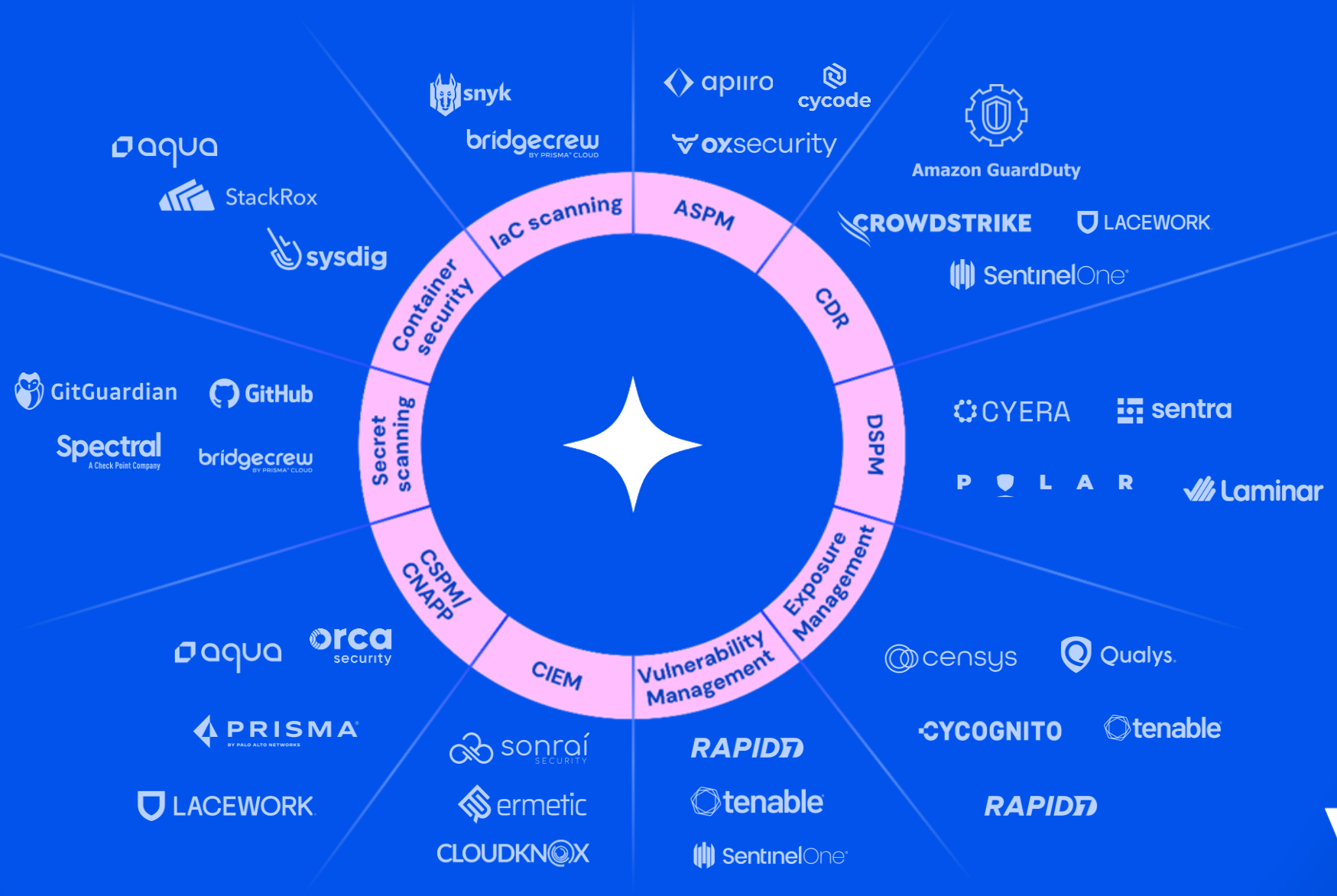
Innovation	CSPM Capabilities	Agentless CWP
Roadmap	CIEM	Agent-based CWP
Container Runtime Protection	Agentic AI and Copilots	CSPM Cloud Coverage
Supporting services and offerings	Infrastructure as Code (IAC) Security Reporting	CNAPP Administration Management

Source: The Forrester Wave ™ for Cloud Native Application Protection Solutions, Q1 2026 by Andras Cser at al, Forrester, February 17,2026.

Forrester does not endorse any company, product, brand, or service included in its research publications and does not advise any person to select the products or services of any company or brand based on the ratings included in such publications. Information is based on the best available resources. Opinions reflect judgment at the time and are subject to change. For more information, read about Forrester's objectivity here

The Wiz Platform: Consolidation to drive impact

Our single platform displaces point products and enables dev-security collaboration



WIZ

The Way Forward

Understanding Your Goals

Define goals & needs:
- Current state
- Desired changes
- Critical capabilities

Use case exploration

Requirements Building

- Demos by use case
- Define POV goals & test plan
- Executive validation of the value proposition

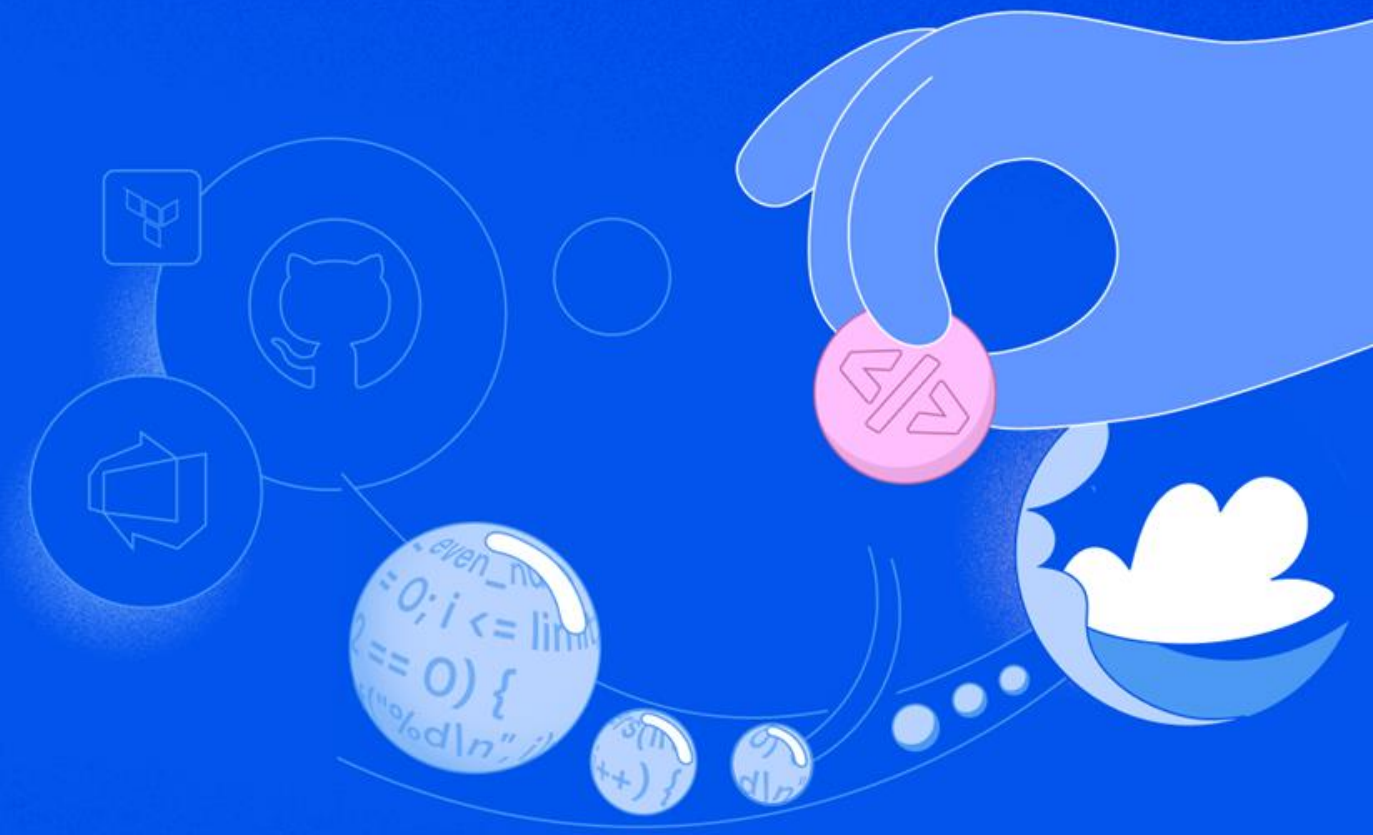
Proof of Value

- Kick off and integration
- Game-ified platform exploration & criteria testing
- Finalize the business case
- Findings review

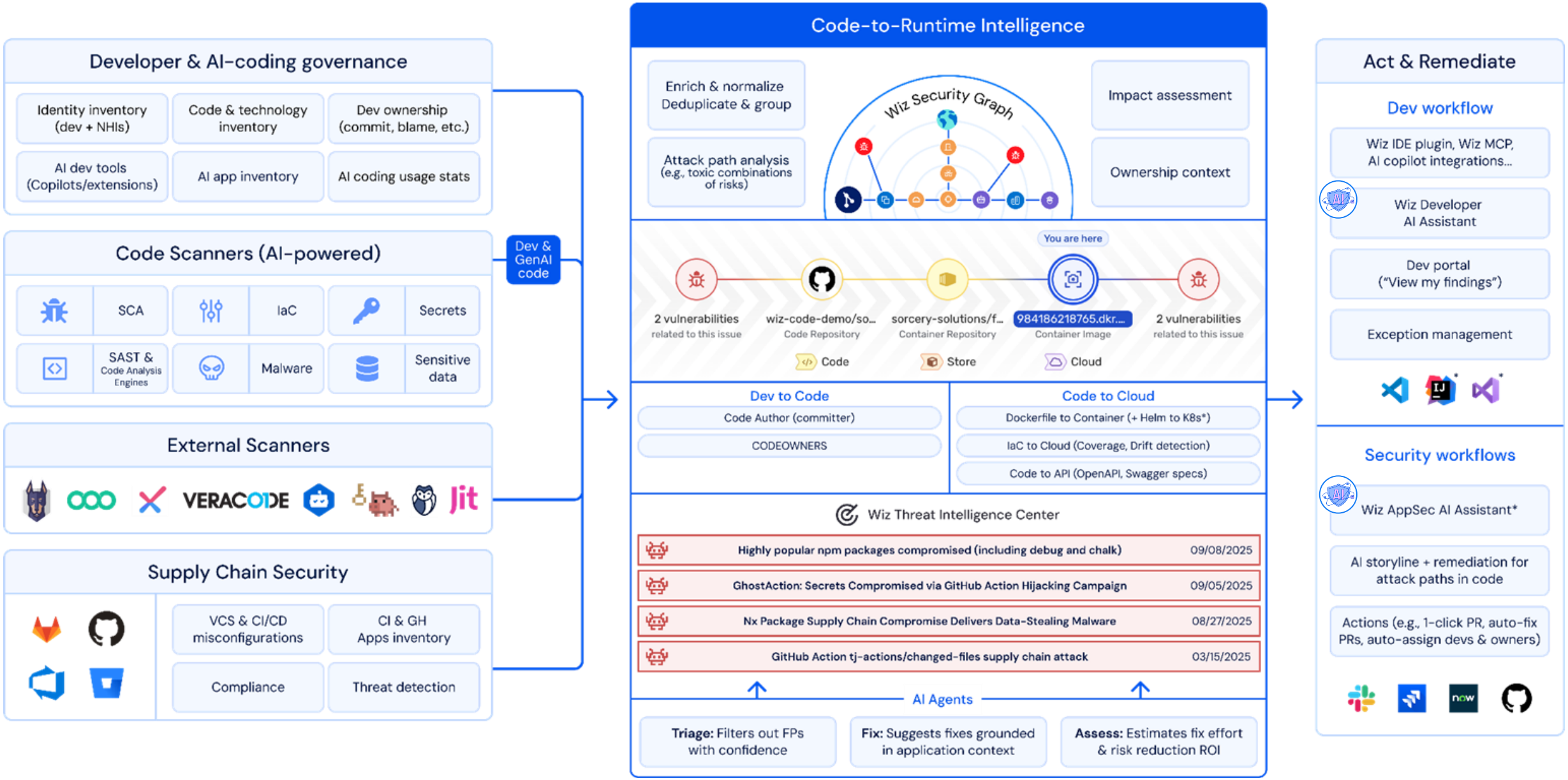
Transform to Production

- Reference conversations with customers
- Co-create launch plan
- Procurement & deployment

Wiz Code



Wiz Code: AI-powered ASPM for Unified Cloud & App Security



Accelerate Your Transformation Toward Cloud & AI-Native AppSec

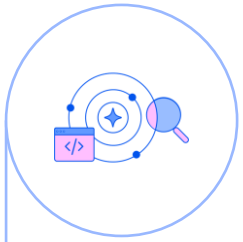
Remediation

Hardening

1. DISCOVER & MODEL APPS

- **Automatically discover all application components**: repositories, CI workflows, developers, services & tech stacks.
- Map ownership to code authors and teams, creating projects and services that reflect your internal organization

Goal: 100% visibility into existing and new apps



2. PROFILE CODE RISKS WITH CLOUD CONTEXT

- **Activate code scanning:** SCA, SAST, IaC, and secrets. Weekly or daily scanning.
  - **Bonus:** Ingest all third-party security findings.
- **Assess SDLC Posture:** Evaluate VCS and CI/CD for insecure defaults.
- **Correlate code findings with runtime signals** to normalize, deduplicate, and prioritize real risks

Goal: Prioritize real risks across your code and cloud

3. ONBOARD DEVELOPERS

- **Accelerate remediation with integrated workflows;** auto-assign findings to code owners and create tickets with SLAs.
- **Enable PR and CI/CD scans for all new code.** Developers review Wiz findings directly in their VCS security tab.
- **Deliver built-in AI-powered,** one-click fix suggestions tailored to

Goal: Achieve "Zero Critical" risks in Code & CI/CD.

4. ESTABLISH GUARDRAILS & ENFORCE PRE-DEPLOYMENT GATES

Level up developer workflows to "stop the bleeding"

- Configure policies to block PRs or fail CI/CD builds on policy violations, proactively "stopping the bleeding".
- Promote client-side prevention with pre-commit checks and the Wiz IDE plugin to prevent known issues before deployment.

Goal: Aim for 100% dev adoption & policy coverage

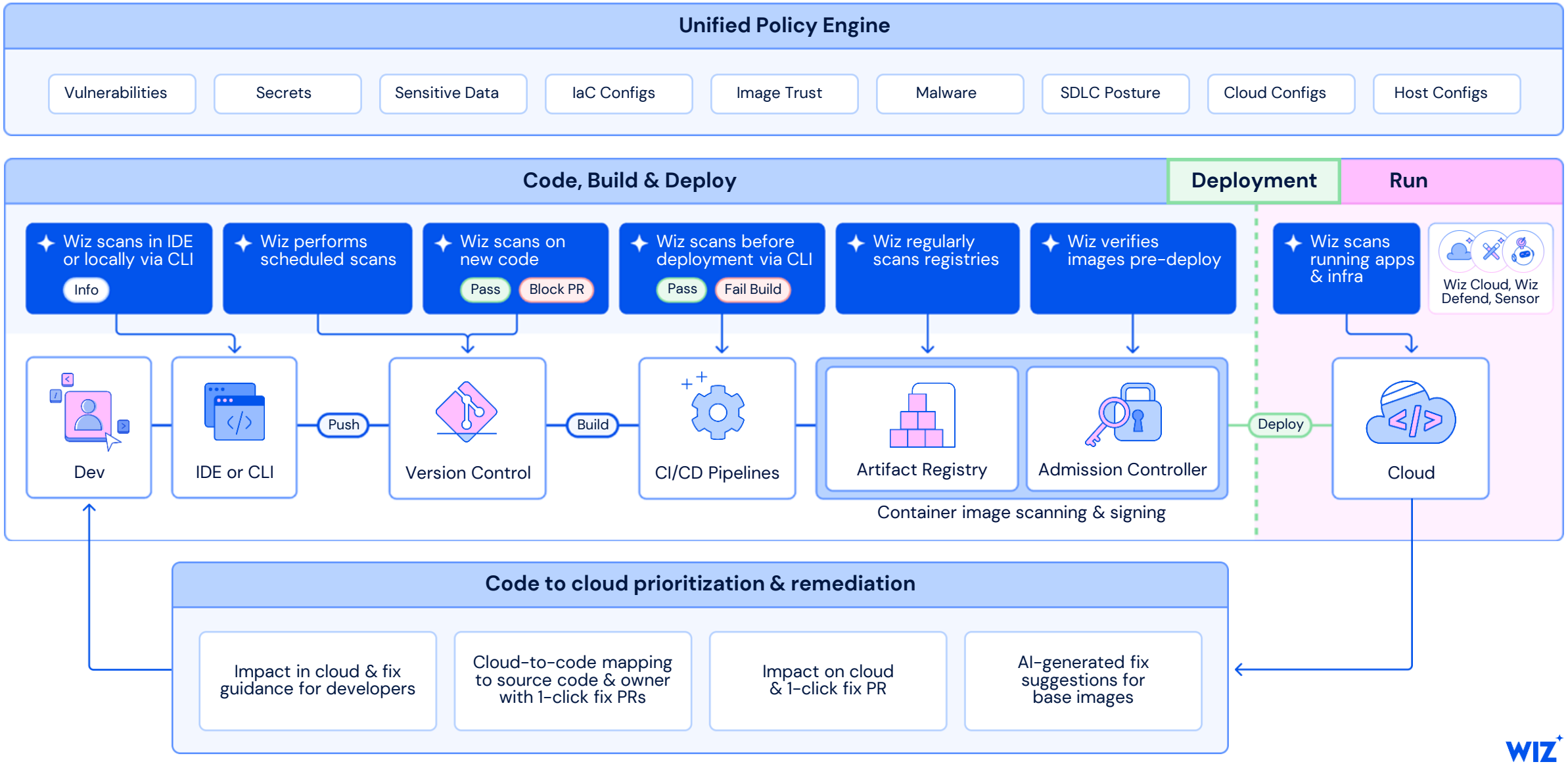
5. TRANSFORM APPSEC / TRANSFORM APPLICATION DEVELOPMENT

- Integrate application and business context earlier for risk-based decisions (CMDB, service catalogs).
- Achieve full compliance with OWASP TOP 10 CI/CD, CIS benchmarks for SDLC.
- Invest in strategic initiatives to shift to secure-by-default
  - **Integrity/provenance:** Implement artifact signing in CI/CD.
  - **Start Secure:** Migrate images to WizOS for near-zero CVEs.

Goal: Maintain "Zero Critical" and harden the SDLC

Wiz Code Reference Architecture

A layered approach to secure by design with guardrails in the IDE, VCS, and CI/CD pipelines



Wiz Code customers improve application & cloud security posture while enhancing developer productivity

> Now, people can look up and say, "This is the attack path, and this is what I should do." [Wiz Code] has **brought us closer to developers** and shown that we make remediation easy for them, not hard.

Roland Lechner,
Director of Cloud Security, BMW Worldwide

- Reduced critical issues by **95%** in multi-cloud environments
- Unified toolchain with all-in-one scanners and code-to-cloud view
- Embedded guardrails into developer workflows (CI/CD)
- **Protecting critical IP** with software supply chain security

- 1,250+ developers
- GitHub integration, WizCLI and Wiz IDE
- AWS
  Azure
  Kubernetes
  GitHub

> Being able to see and understand all of our infrastructure and how it works **has made our security and development teams more efficient.** We use Wiz like Google to [see] and query our resources.

Nick Waringa
Head of Secure Product and Infrastructure

- Consolidated 7 OS & Commercial AST tools
- Reduced TCO by **50%,** will increase as contracts expire
- Reduced container vulnerabilities by **51%**
- Consistent process for scanning and developer-led fixes

- WizCLI in CI/CD, K8s Admission Controller
- AWS
  Azure
  Kubernetes
  GitHub

Wiz Defend

SecOps teams need a unified approach that is purpose-built for cloud, with cloud context

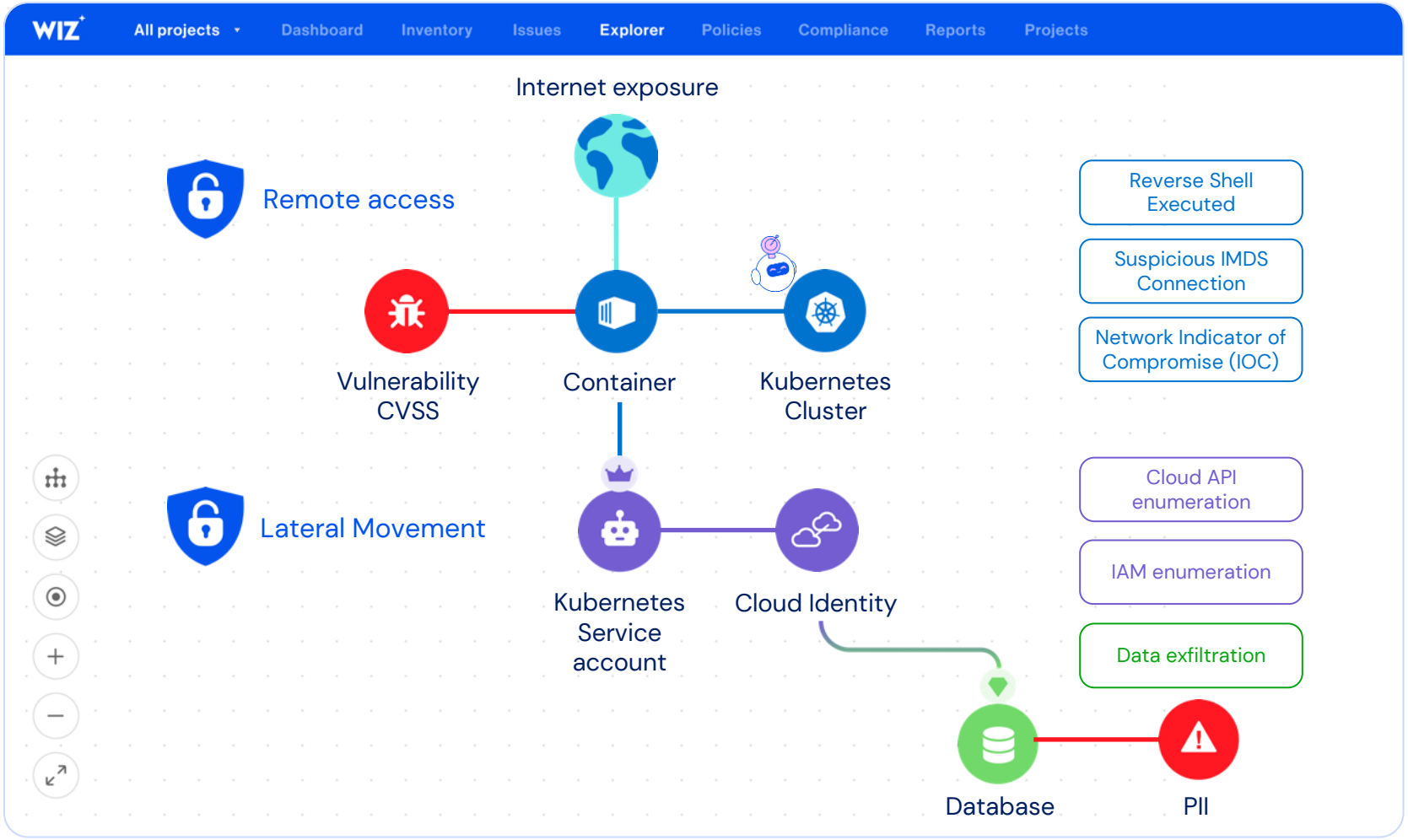
01 Runtime, cloud, and SaaS signals

02 Behavioral analytics

03 Cloud and code context

04 Cloud threat intelligence

1 precise threat alert



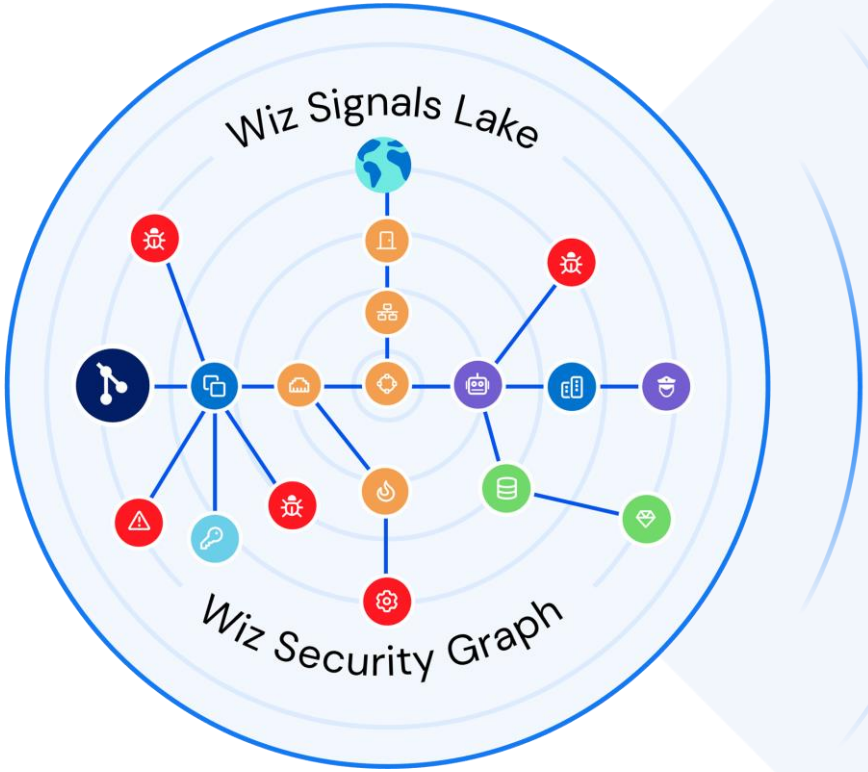
Wiz Defend: Detection and Response Built for the cloud

Cloud Threat Intel

Runtime Sensor

Cloud Telemetry

Code to Cloud Risk Context



Prepare

IR readiness with log & runtime visibility mapping against MITRE ATT&CK

Detect

High-fidelity, cross-layer coverage with heuristics & Wiz cloud threat intel

Investigate

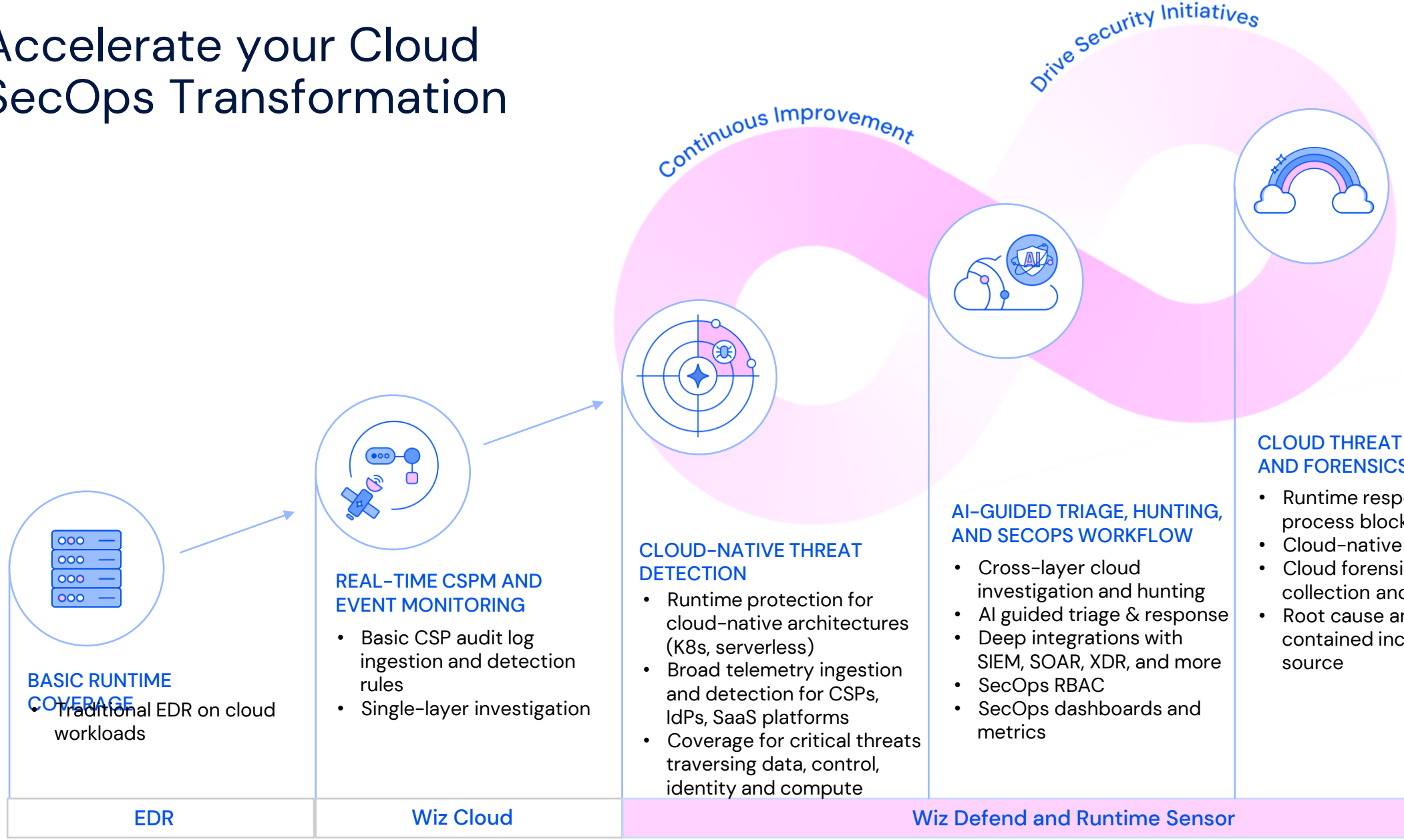
Automated attack timeline and immediate context for alert triage and threat hunting

Respond

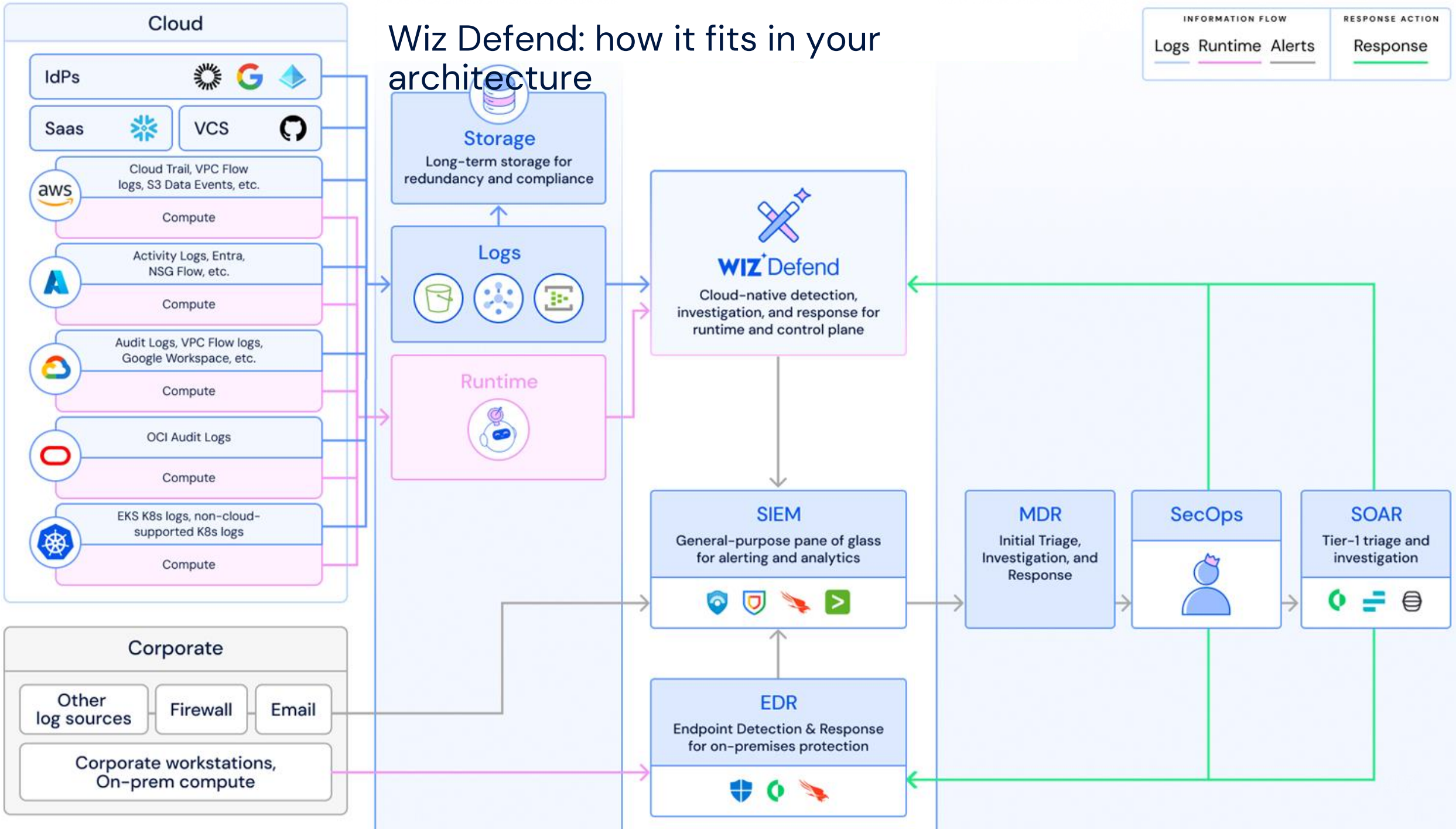
Runtime blocking, cloud-native containment, and automated forensic data capture

- SOC
- Detection Engineering
- Incident Response & Hunting
- Digital Forensics
- App Owners

Accelerate your Cloud SecOps Transformation



Wiz Defend: how it fits in your architecture



Improve the business value of your cloud SecOps program

Tool consolidation and effectiveness

> Wiz has transformed our approach to cloud detection & response by providing accurate detections, and the context we needed but never thought possible.

5x better

Improved visibility and coverage

Reduced MTTR

> It used to take us hours to determine which issues were urgent threats. Now, it takes five minutes, and we're finding and addressing the right problems.

10x Faster

Time to detect and respond to threats

Susanne Senoff
CISO

PROS

Security team productivity

> We typically find all alerts generated by Wiz Defend valuable to review. The alerts are high-fidelity, and we never need to question why something's firing

<24hr

Immediate visibility to emerging threats

Reduced MTTI and escalations

> I [can] open an issue and quickly see which user accessed which bucket, what files they interacted with, and determine if that activity matched their job responsibilities.

10x Lower

Effort to find and remediate issues

Chris Long
Sr. Director of Security

Material

Unprecedented
time to value

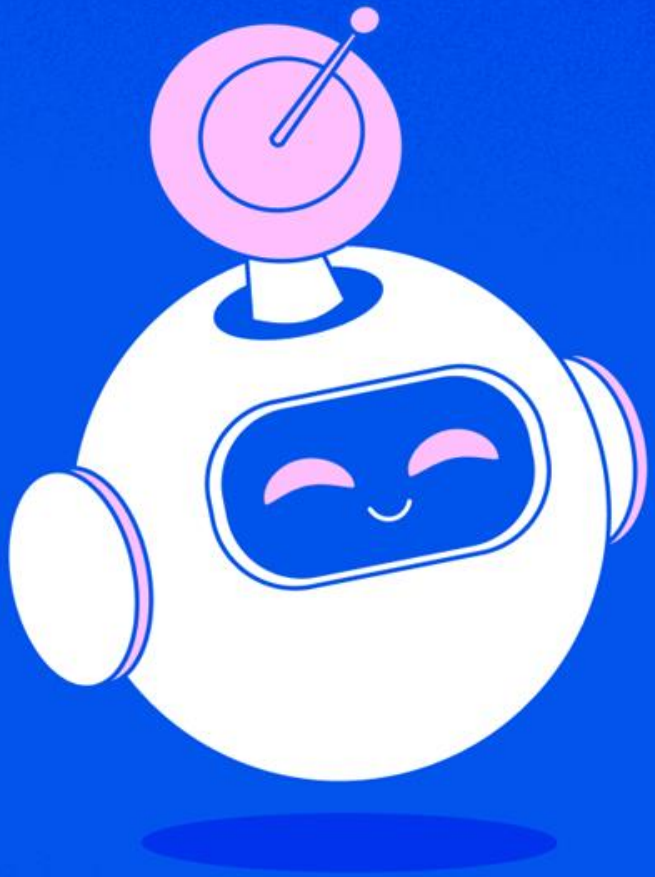
> Wiz Defend has brought data across our event sources together to help investigate detections from start to finish. From our identity provider logs pinpointing the actor to Wiz's runtime events illustrating the individual process execution and network activity. From Wiz Defend, we have confidence in our detection and investigation capabilities.

Nate Stevens
Security Engineer
matillion

Agentless context & automatic **investigation** rapidly reduces MTTR

WIZ

Wiz Sensor



The best of both worlds:

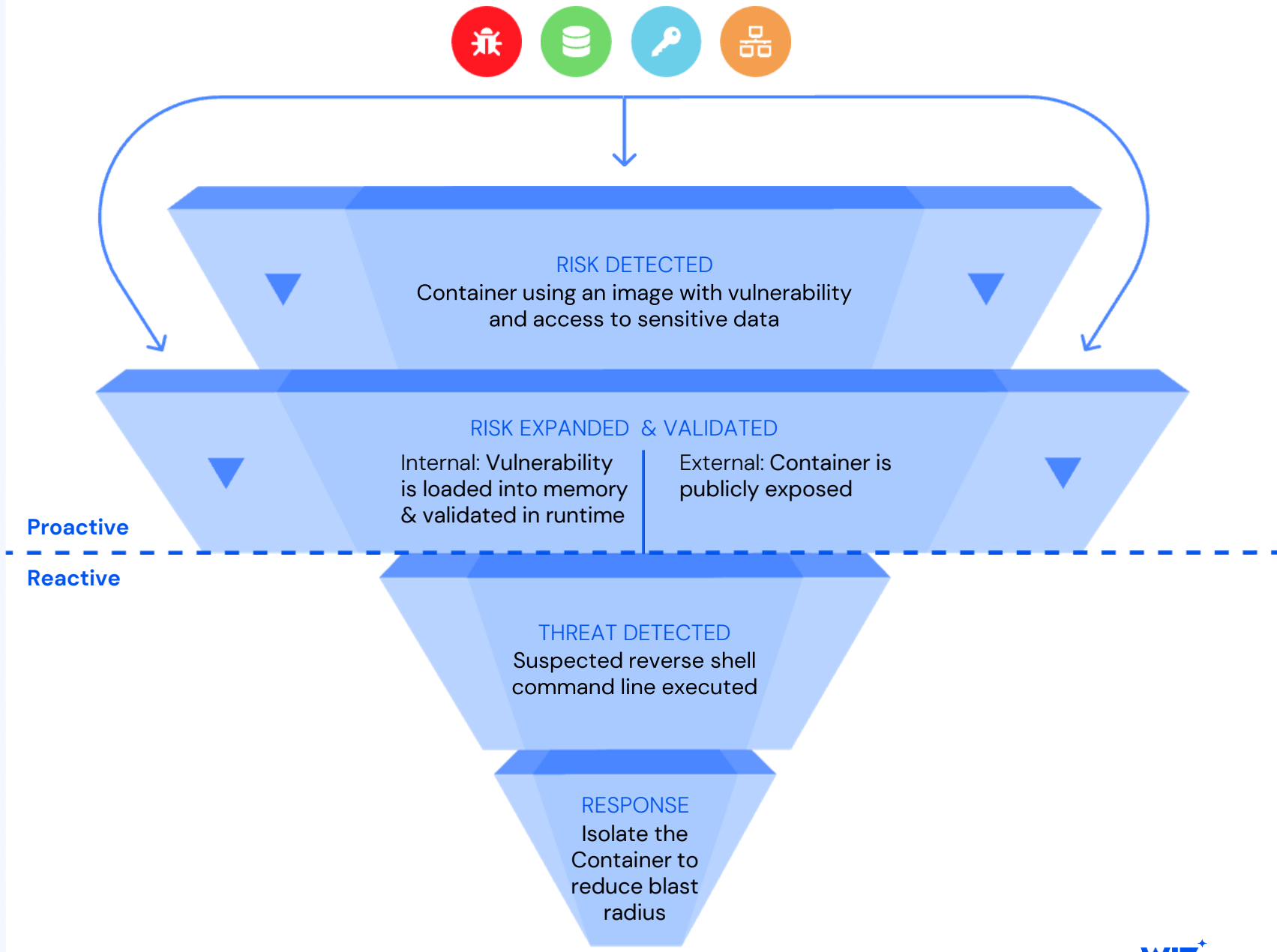
Start Agentless, Layer Runtime On-top

From **Vulnerability** Findings to Process **Termination**

From **Data** Findings to VM **Containment**

From **In-Memory Secret** Findings to immediate **Rotation**

From **Network Exposure** to VM **Isolation**



Wiz Sensor: Runtime protection and risk assessment built for the cloud

Information Security | Vulnerability Management | Cloud Security | Container Security | SOC | IR

WIZ Cloud
WIZ Code

Reduce noise and prioritize risks with runtime context

Reduce MTTD and MTTR

WIZ Defend

Runtime Risk Assessment & Hardening

- Container Security
- CWPP
- API Security
- Vulnerability Runtime Validation
- SBOM Runtime Validation
- Real-time Network Analysis

- Lightweight
- eBPF based
- Easy to deploy

Threat Detection & Response

- Real-time Detection
- Runtime Response
- File Integrity Monitoring
- Runtime Hunting & Intelligence
- Behavioral and IOC Threat Detection
- Runtime Forensics

Clouds | aws

Platforms |

Wiz For Container Security Reference Architecture

Agentless
Sensor

Remediate in code

Developers

Enforce policies code to cloud

Security

Secure by Design

Secure at Runtime

Code

CI/CD Tools

Dev Laptop

Code and IaC

IDE

IDE Plugin & Hook

VCS

Event-Triggered scans

Pass

Periodic scans

Fail

Policies
HCR
Sensitive Data

Policies
HCR
Sensitive Data
D & R Rules

Build

CI/CD Tools

Build Job

Scan IaC

Pass

Scan Container Image

Fail

Image Signing

Add digital fingerprint using Cosign/notary or native solution

Image Registries

Periodically scans container images for vulnerabilities

Admission Controller

Verify potential misconfiguration and images are trusted

Fail

Pass

Run

Cloud Platform

Config.
Network
Identity

Events

Container Platform

KSPM

Cluster Hardening (CIS)

Attack Path & Lateral Mov.

Vulnerability (Validated at runtime)

Secret Scanning

FIM (Agentless + Sensor)

Audit Logs

Real-Time Detection & Blocking

Threat Hunting (Runtime Execution Data)

Wiz Cloud

Wiz for CSPM Reference Architecture

How do I shift left?

Scan IaC templates in VCS, IDE, and CLI and container and VM images in CI/CD pipelines to block risky deployments

What is in my cloud?

Wiz Inventory
Full stack visibility & real-time scanning

Cloud Configuration Scanner

Resources, Networks, Identities, AI pipelines, SaaS

Agentless Workload Scanner

VMs, Containers, Serverless

What are my misconfigurations?

- Misconfiguration rules
- Findings generated with severity

How do I prioritize risk?

Controls based on deep risk assessment

- Misconfigurations
- Vulnerabilities
- Networks
- Identities
- Data
- Malware
- Secrets

Issues generated with severity

How do I prioritize?

Wiz Security Graph

Graph-based context
Single prioritized queue of issues

Who owns this risk?

RBAC project segmentation

How do I remediate?

- Ticketing & messaging integrations
- Automatic remediation workflows

Improved security and compliance posture

0 critical risks

Focus on best practices

Democratize security

What is my compliance status?

Compliance Frameworks

Compliance Heatmap

How do I demonstrate compliance?

Compliance Reports

Granular and Executive Reports

How do I meet unique requirements?

Customization

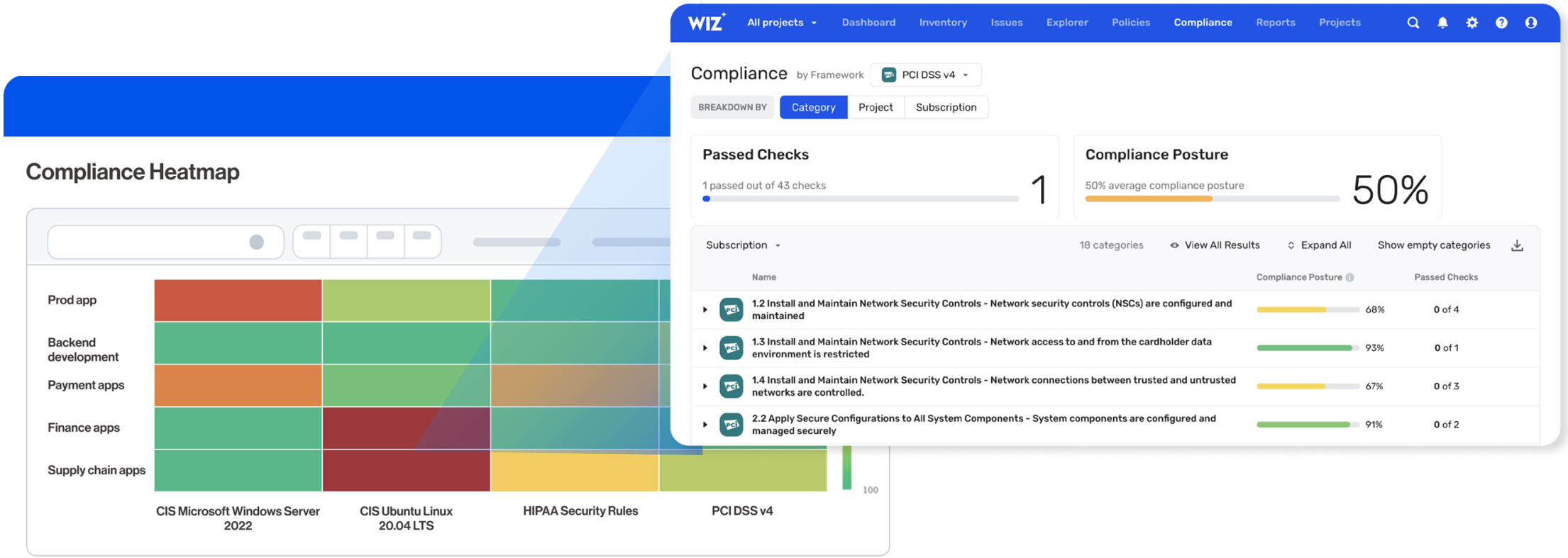
Controls Frameworks

Wiz for Compliance

- **Automatic** compliance assessment
- **295** built-in standards and **frameworks**
- Compliance heatmap across your organization
- **Extend cybersecurity across teams**, tools and departments
- Granular and exec reports at the click of a button

295

Mapped compliance standards



From Silos to Unified Vulnerability Management

Unified visibility enriched with context, driving actionable remediation

Wiz Native Scanners

- Cloud Scanner
- Code Scanner

External Scanners

- Vuln. Scans
- Pentests
- Secrets
- SAST
- EASM
- DAST
- SCA
- AppSec

Asset Inventory & Ownership

- CMDB
- Service Catalog
- Asset deduplication
- Asset Repositories
- Network & DNS addresses
- Cloud to code change history

Build Context

- Data enrichment & normalization
- Vulnerability deduplication

Wiz Code-to-Cloud

Wiz Security Graph

Prioritize

- Projects Based Business Context
- External Exposure Validation
- Threat Intel
- Source Mapping (code-to-cloud)
- Attack Path Analysis
- Risk Issues
- Posture Issues
- AI Remediation Recommendation Agent

Act & Remediate

- Ticketing & notifications & Automations
- Cloud remediation
- Remediation Integrations
- Code remediation
- 200+ integrations
- AI Remediation Action Agent

Cloud, Code, Runtime Context

Key Benefits

- MTTR Reduction
- Manual Overhead Reduction
- Time Saved per Developer per Vulnerability
- SLA Adherence Increase

Holistic Exposure Management

Continuously fix critical exposures from code to cloud to ground

Code (ASPM)

50% Fixed at the IDE

20% Fixed at the PR

10% Blocked at CI/CD

WIZ Code — SCA, IaC, Malware, SBOM, Secrets, Data, SAST*

WIZ UVM — Semgrep, Checkmarx, VERACODE

Cloud — WIZ Cloud

aws

160K Critical and High With Public Exploit

14K Exposed Resources

149 Critical Attack Paths

23 Validated in Runtime + External Attack Surface

On-prem

100K Critical and High With Public Exploit

8K Exposed Resources

89 Critical exposure on critical resources

10 Validated in Runtime + External Attack Surface

WIZ — WIZ UVM

Remediation & Response

Remove toxic combinations in cloud and code

Posture issues to drive long-term hygiene

Remediation playbooks and AI assistance

Complete asset inventory and business ownership

Wiz CIEM: Effective Identity and Permissions Analysis

Identity Sources

Identity Engine

- Humans & Non-Humans
- Effective Access
- Lateral Movement
- Unused Permissions

Risk Context

- Sensitive Data
- Public Exposure
- Identity Configs
- Key Rotation
- Exposed Secrets
- Org Level Policies

Log Collection

Discover

Auto-discover identities, admins, 3rd party identities and all cloud keys.

Contextual Risk

Stale admins, cleartext keys allowing lateral movement, unused access to sensitive data.

Investigate

Investigate granted permissions vs permissions used. Review cross-cloud or cross environment access.

Resolve

Auto-remediate or provided remediation steps, with action driver integrations.

- Identity Security
- Cloud Security
- DevOps/IAM Engineering
- IT

Identity Security

Ticketing & Messaging

Wiz DSPM: Democratizing Data Security

Cloud Storage

Buckets, Databases, Data Warehouses, Serverless, VMs, Code Repositories

Data & AI Platforms

SaaS Platforms

Y25

On Prem

Y25

Databases

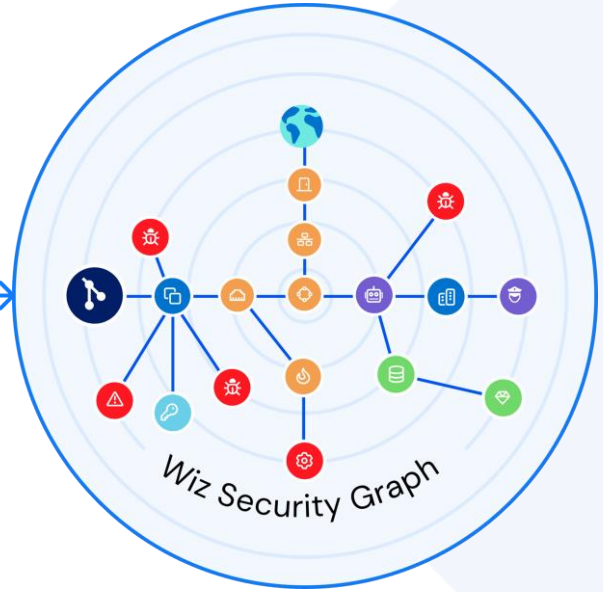
File shares

Servers

Data Catalog

Data Classification

Pattern matching
Local Context
Learnt Data
AI/ML classification



Cloud Risk & Threat Context

Reduce

Stop data sprawl by finding and deleting Shadow data

Restrict

Map and remove any over privileged access

Relabel

Label cloud assets with their data sensitivity

Relocate

Ensure data jurisdiction complies with your needs

Reconfigure

Ensure configurations such as encryption & retention are set

GRC Team

Cloud Security & Cyber Defense

Data Security

Dev & DevOps

WizOS: Operationalize secured images at scale

Mitigate Risk

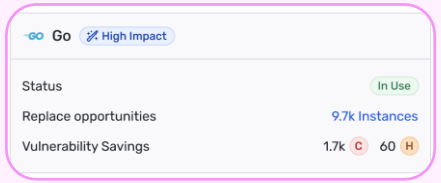
Assess your current image landscape and risk posture

Prioritize migration to address the most urgent risks

Complete container image inventory and risk assessment

Identify all WizOS eligible replacement opportunities

Replacement and vulnerability savings with Image Catalog



Gain Visibility

Start Secure

Enforce guardrails in CI/CD and with Admissions Controller

Empower developers with 1-click image swaps in IDE & pull requests

Enforce Guardrails

WIZOS IMAGES

.NET GO OpenJDK NGINX node

& more...

WizOS Package Repository

Built from source by Wiz

SBOMS & provenance with every release

SLAs for CVE remediation

FIPS and STIG-hardened image variants

Cloud Security

Product Security

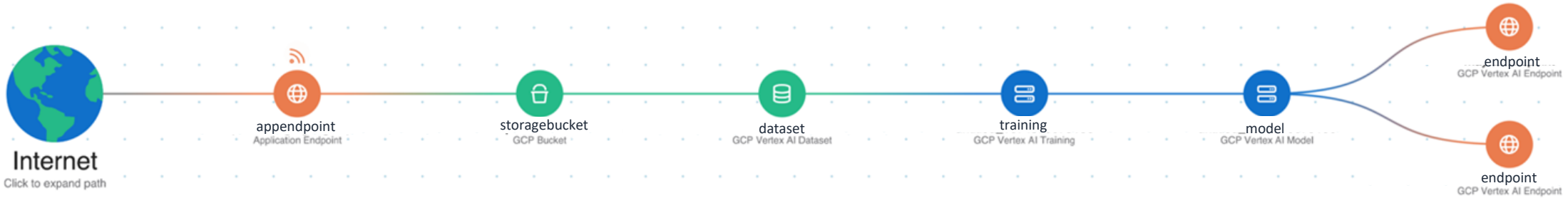
DevOps & Platform Engineering

Developers

WIZ

Wiz AI-SPM

Detecting attack paths in AI pipelines require context



Business context

- Data sensitivity
- Environment
- Business team

Cloud context

- Resource configuration
- Networking
- Identities

Workload context

- Vulnerabilities
- Inventory
- Exposed secrets

AI context

- E2E pipeline risks
- Model exposure of sensitive data
- Dynamic scanner of model vulnerabilities
- Model runtime alerts

Industry logo slides under NDA

The Largest Private Cybersecurity Company

$1.9B raised

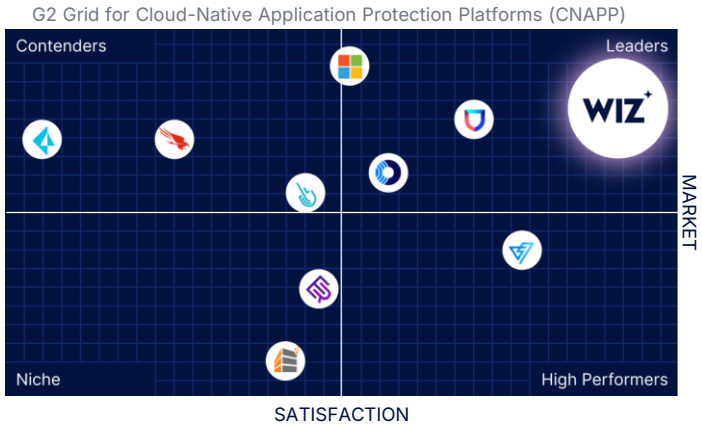
Index Ventures · THRIVE CAPITAL · INSIGHT PARTNERS · SEQUOIA · Lightspeed · andreessen horowitz

Enabling Security Impact

50% Of Customers achieve 0 Criticals

>50% Of Active Users are Devs/DevOps

The Leader in Cloud Security



Industry leading global tech companies secure their cloud with Wiz

BLOCK · snowflake · PLAID · LinkedIn · tide · Robinhood · Veeva
slack · UiPath · salesforce · GitLab · grammarly · Adobe · redis
Wolt · zendesk · CISCO · Hewlett Packard Enterprise · Amplitude · Five9 · freshworks
GitHub · DocuSign · MINDBODY · rubrik · fiverr. · paylocity · deliveroo

The Largest Private Cybersecurity Company

$1.9B raised

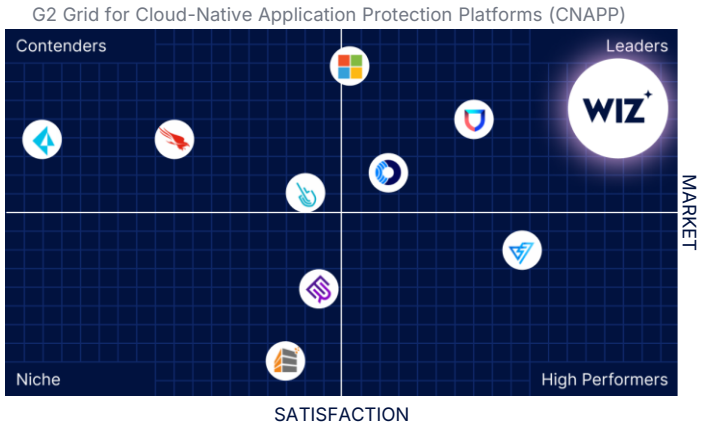
Index Ventures · THRIVE CAPITAL · INSIGHT PARTNERS · SEQUOIA · Lightspeed · andreessen horowitz

Enabling Security Impact

50% Of Customers achieve 0 Criticals

>50% Of Active Users are Devs/DevOps

The Leader in Cloud Security



Industry leading global healthcare companies secure their cloud with Wiz

Bristol Myers Squibb · Takeda · Pfizer · lyra · HCA Healthcare · CENTENE Corporation
KAISER PERMANENTE · BAUSCH Health · Quest Diagnostics · Phreesia · PerkinElmer · DaVita
CEDARS-SINAI MEDICAL CENTER · HENRY SCHEIN ONE · THIRTY MADISON · GENOMONCOLOGY · iz.ai · Elevance Health
dexcom · DaVita Kidney Care · BLINK HEALTH · MOLINA HEALTHCARE · abbvie · PRECISION MEDICINE GROUP

The Largest Private Cybersecurity Company

$1.9B raised

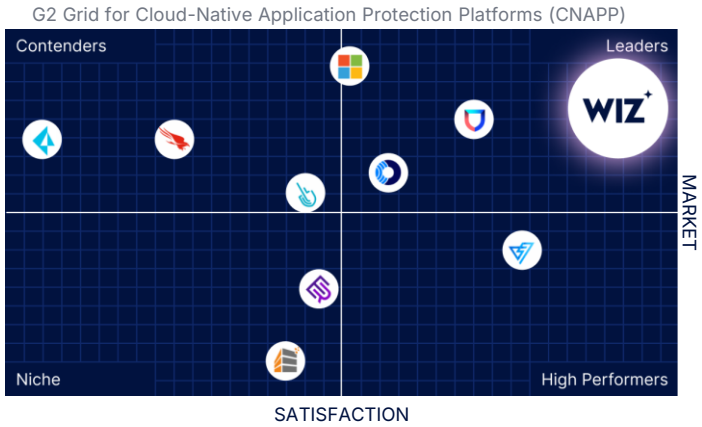
Index Ventures · THRIVE CAPITAL · INSIGHT PARTNERS · SEQUOIA · Lightspeed · andreessen horowitz

Enabling Security Impact

50% Of Customers achieve 0 Criticals

>50% Of Active Users are Devs/DevOps

The Leader in Cloud Security



Industry leading global financial services companies secure their cloud with Wiz

BARCLAYS · BRIDGEWATER · JPMORGAN CHASE & CO. · experian. · MONUMENT · AON · PayPal
Brex · BlackRock. · BLOCK · Fannie Mae · MSCI · globalpayments · ASSURANT
fiserv. · New American Funding · Vanguard · Morgan Stanley · Revolut · NAVY FEDERAL Credit Union · IG
Blackstone · BOK FINANCIAL · lili · CITY NATIONAL BANK The way up. · London Stock Exchange · PLAID · CapitalOne

The Largest Private Cybersecurity Company

$1.9B raised

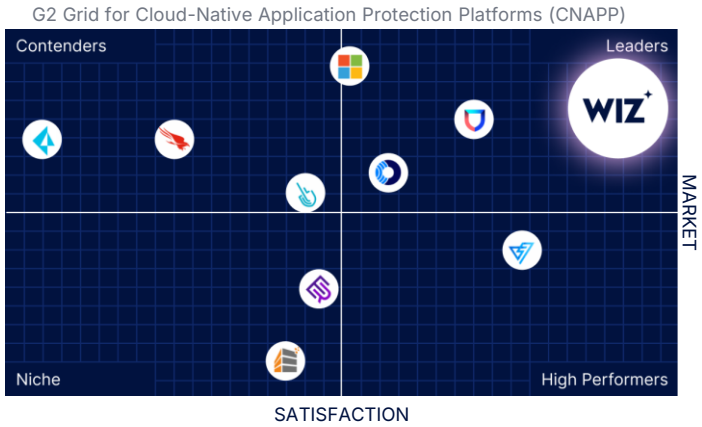
Index Ventures · THRIVE CAPITAL · INSIGHT PARTNERS · SEQUOIA · Lightspeed · andreessen horowitz

Enabling Security Impact

50% Of Customers achieve 0 Criticals

>50% Of Active Users are Devs/DevOps

The Leader in Cloud Security



Industry leading global retail companies secure their cloud with Wiz

The Home Depot · NIKE · REI co-op · wayfair · macy's · lululemon · LTK · carter's · asos · BURBERRY LONDON · COSTCO WHOLESALE · LVMH · overstock · Columbia Sportswear Company · Carrefour

The Largest Private Cybersecurity Company

$1.9B raised

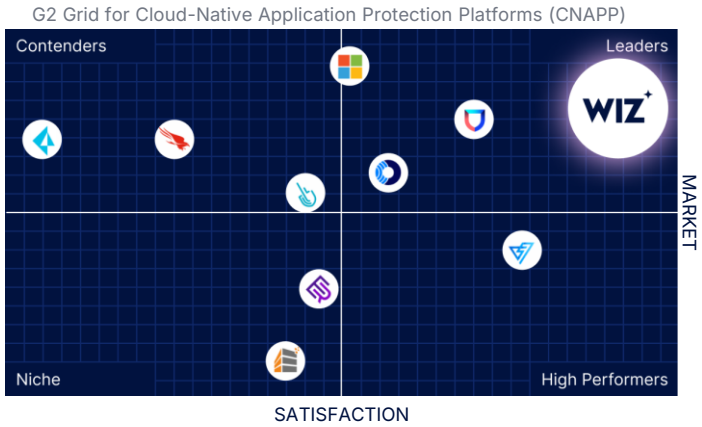
Index Ventures · THRIVE CAPITAL · INSIGHT PARTNERS · SEQUOIA · Lightspeed · andreessen horowitz

Enabling Security Impact

50% Of Customers achieve 0 Criticals

>50% Of Active Users are Devs/DevOps

The Leader in Cloud Security



Industry leading global manufacturing companies secure their cloud with Wiz

Chevron · COLGATE-PALMOLIVE · GARMIN · DIAGEO · Unilever · BMW · RIVIAN · Audi · Henkel · MATTEL · Honeywell · AVERY DENNISON · TESLA · kenvue · MARS · SIEMENS · KraftHeinz · MAXAR TECHNOLOGIES · Shell · Mondelēz International · General Mills · OTIS · MHolland · Linde

The Largest Private Cybersecurity Company

$1.9B raised

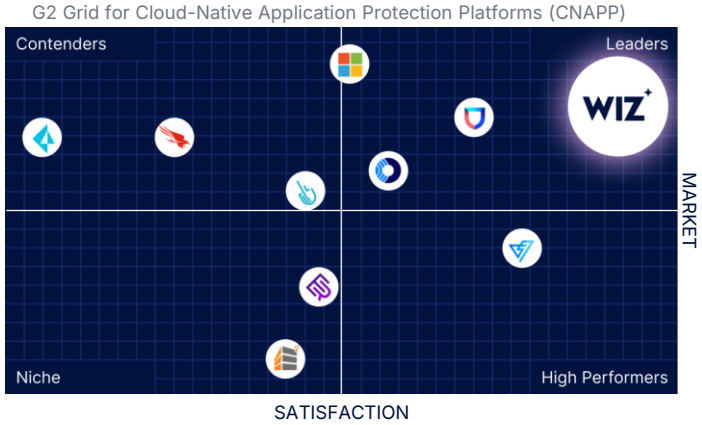
Index Ventures · THRIVE CAPITAL · INSIGHT PARTNERS · SEQUOIA · Lightspeed · andreessen horowitz

Enabling Security Impact

50% Of Customers achieve 0 Criticals

>50% Of Active Users are Devs/DevOps

The Leader in Cloud Security



Industry leading global media & entertainment companies secure their cloud with Wiz

Spotify · Paramount · Hard Rock DIGITAL · FOX · MGM · Schibsted · SiriusXM · Electronic Arts · The New York Times · HEARST

The Largest Private Cybersecurity Company

$1.9B raised

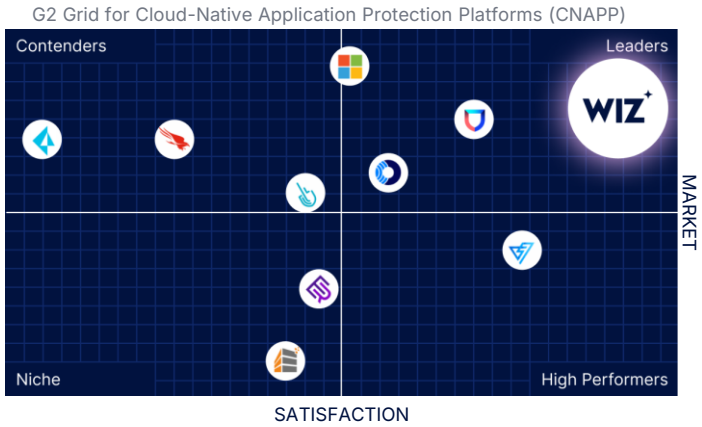
Index Ventures · THRIVE CAPITAL · INSIGHT PARTNERS · SEQUOIA · Lightspeed · andreessen horowitz

Enabling Security Impact

50% Of Customers achieve 0 Criticals

>50% Of Active Users are Devs/DevOps

The Leader in Cloud Security



Industry leading global companies secure their cloud with Wiz

redis · rubrik · BigID · tide · Wolt · Artlist

PRISMHR · Assent · contentful · 3D SYSTEMS · AON · Blue Apron

Kaseya · MX · via · UiPath · snappy · BLINK·HEALTH

atlan · Lusha · Salesloft. · deliveroo · Barracuda · VALIUZ

ServiceTitan · illuminate education · MONUMENT · yotpo. · lyra

The Largest Private Cybersecurity Company

$1.9B raised

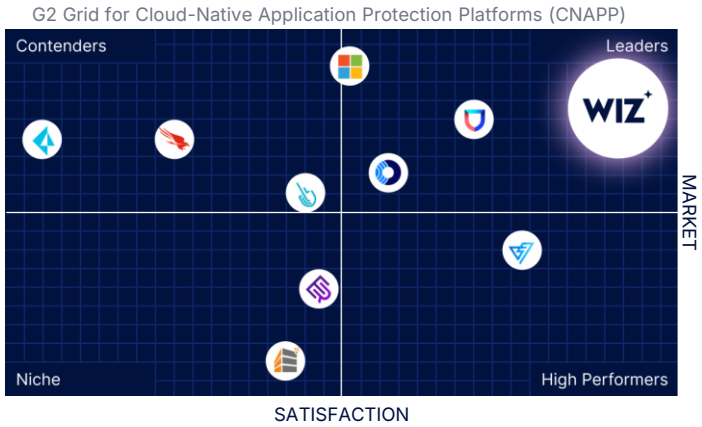
Index Ventures · THRIVE CAPITAL · INSIGHT PARTNERS · SEQUOIA · Lightspeed · andreessen horowitz

Enabling Security Impact

50% Of Customers achieve 0 Criticals

>50% Of Active Users are Devs/DevOps

The Leader in Cloud Security



Industry leading global AI companies secure their cloud with Wiz

perplexity · OpenAI · snowflake · Weights & Biases · Jasper · glean