



Secure everything
you build and run



INTRODUCING THE

The Wiz AI and Cloud Security Platform

Code

Pipeline

Cloud

Runtime

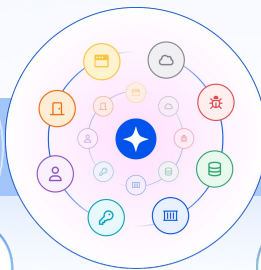
RUNTIME TO CODE

Fix exploitable risk at the source automatically

CODE TO RUNTIME

Proactively test reachable vulnerabilities with context

AI Agents



Mika

WIZ⁺Code

SECURE DEVELOPMENT

Start AI and app development
secure from the AI-DLC

WIZ⁺Cloud

MANAGE POSTURE

Reduce cloud, hybrid, and AI
risks proactively

WIZ⁺Defend

STOP THREATS

Detect and contain malicious
cloud and AI attacks

Vulnerabilities

Identity

Configuration

Data and AI

Public Exposure

Secrets

Attack Surface Validation

Secure and govern multi-cloud
and AI environments

Proactively mitigate
exposures anywhere

Ship secure AI apps
and code

Readiness for cloud
and AI threats

Reduce
Risk

Decrease
Cost

Drive Consolidation &
Efficiency

Adopt AI Securely
& Fast

Accelerate
Revenue

The New Mandate: AI Threat Readiness

The risks and exploits are changing.

AI-powered attackers increasingly target the application layer, using models to understand application logic and identify exploitable paths.

THE NEW MANDATE

Eliminate critical risk and scan any exposure with AI

The speed of exploitability is changing.

AI compresses the time from vulnerability disclosure to exploitation, requiring faster prioritization, ownership, patching, and zero-day response.

THE NEW MANDATE

Accelerate patching and zero-day response

The way software is built is changing.

AI changes both what must be scanned, requiring model-driven analysis of existing code to uncover complex risks, alongside stronger guardrails for AI-assisted development.

THE NEW MANDATE

AI native SDLC and deep AI code scanning

The speed of attacks and perimeter is changing.

AI expands the security perimeter to developer workstations and the SDLC, as coding agents gain broader access, turning a single compromise into a path across the entire environment.

THE NEW MANDATE

Detect and contain threats in real time, extend protection to supply chain risks

The entire environment is changing.

IN THE AI ERA, AGENTS CONNECT SAAS, CODE, DATA, AND INFRASTRUCTURE, WHILE INTRODUCING ENTIRELY NEW AI INFRASTRUCTURE LAYERS TO PROTECT

THE NEW MANDATE

Breadth of visibility: Continuously discover, assess, and protect the full environment

Cloud

On-prem & private cloud

SaaS

AI Applications

Identity

Data

Speed of action: Implement machine speed automation and build towards self-healing

Human-led

Human-in-the-loop

AI-led

Using Wiz to Prepare – What Teams Should Do Now

1. Eliminate critical risk and scan for exposure with AI

- Address open **critical Wiz issues**
- Define remediation workflows to route and fix new criticals fast
- Reduce unnecessary exposure with **ASM**
- Scan all exposure with AI
Continuously scan exposed code with the **Red Agent**



2. Accelerate patching and zero-day response

- Review high-exposure technologies, map ownership to speed remediation
- Leverage **Green Agent** & code-to-cloud mapping
- Build **Threat Center workflow** for zero-day response
- **Start Secure:** Enforce guardrails in code (block vulns from being deployed) and use hardened infra (WizOS)



3. AI native SDLC and deep AI code scanning

- **Prioritize** critical code for advanced AI analysis based on exposure and business impact
- Use advanced models to scan complex, customer-facing code
- Build a **continuous lifecycle** for detection, validation, and remediation of deep AI scans findings
- Use AI and workflows to **automate triage and validation** of findings according to organizational processes



4. Detect and contain threats in real time, protect against supply chain risks

- Move from manual alert triage to **Blue agent** investigation
- Use **automated response playbooks** to enable fast containment, with humans approving sensitive actions when needed
- Protect against **supply chain attacks** and harden the **developer workstation**



Breadth of visibility: Continuously discover, assess, and protect the full environment

WIZ⁺ Code

Wiz Cloud

On-prem & private cloud

WIZ⁺ Cloud

Wiz for SaaS

Wiz AI App for AI Applications

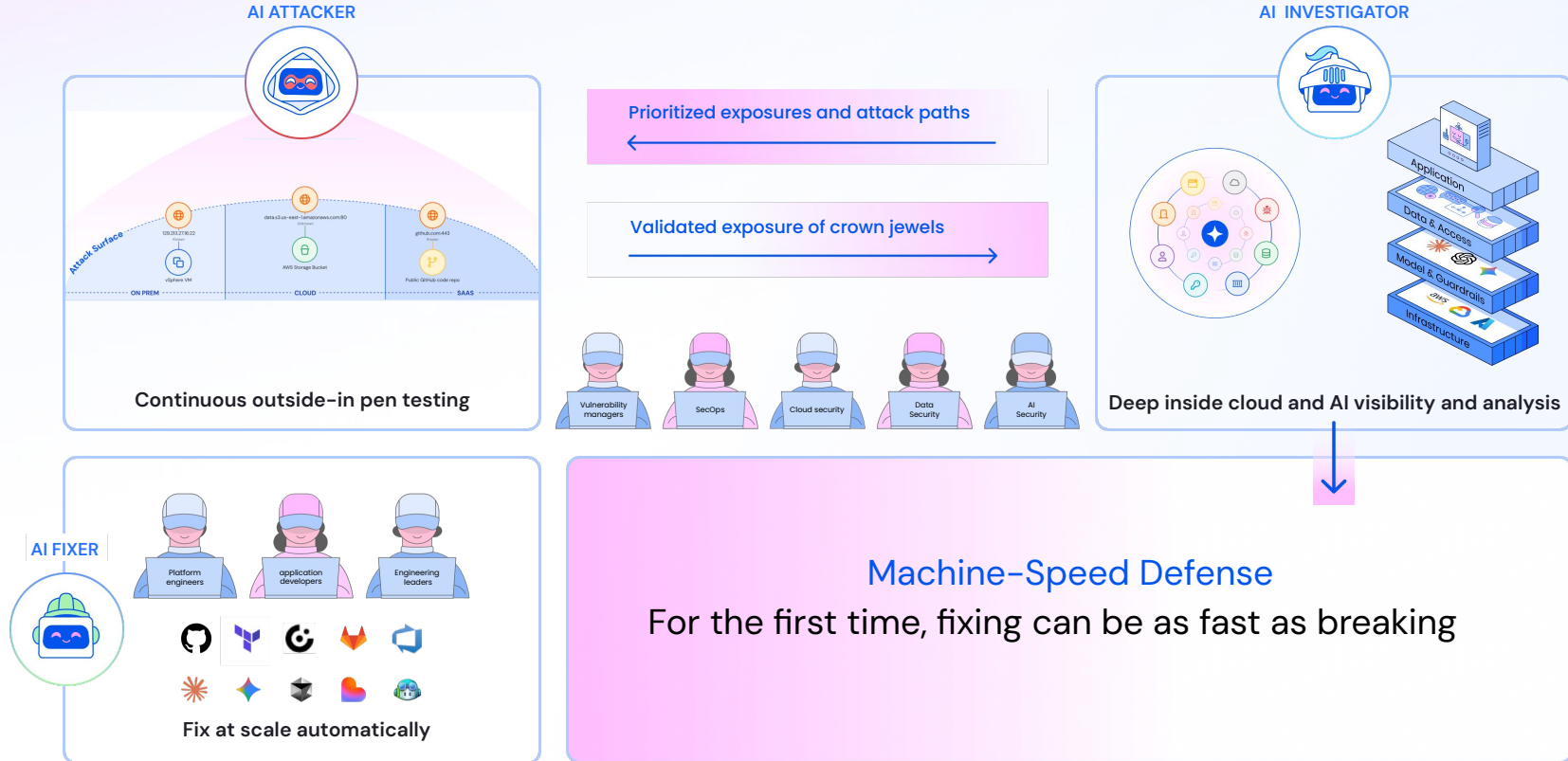
WIZ⁺ Defend

Wiz for Identity

Wiz for Data

OUR SOLUTION

Horizontal, agentic security – A model for the AI era



THE WIZ PLATFORM:

CONSOLIDATION TO DRIVE IMPACT

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

