SOLUTION BRIEF

# Wiz + CyCognito: Holistic Exposure Management, with Integrated Context

CyCognito strengthens Wiz's cloud-native security with an outside-in perspective and active testing. Validated findings are seamlessly integrated into DevSecOps workflows to streamline remediation across the attack surface.

CYCOGNITO

## The Challenge

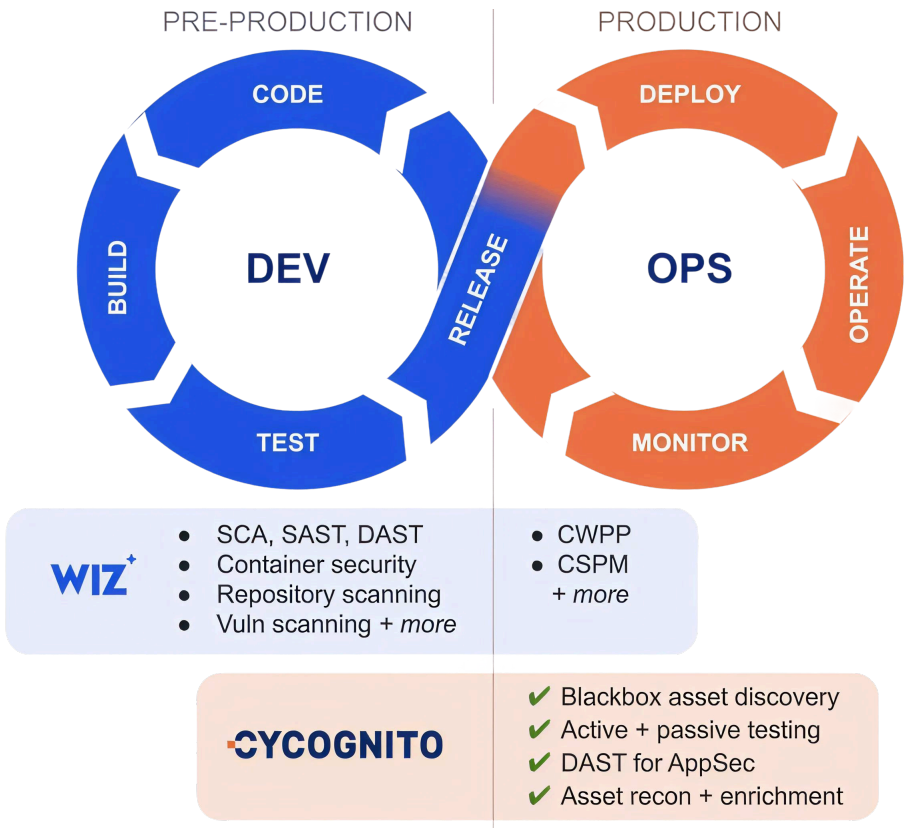
Security teams struggle with two critical gaps: the rapid adoption of low-code/no-code platforms and developer self-service capabilities often bypass security tools, leading to ungoverned application deployments that fall outside existing security coverage.

According to the Linux Foundation, 40% of organizations experience cloud infrastructure security incidents. Despite contextual insights from security solutions, the overwhelming volume of vulnerabilities (40,000 in 2024) makes prioritization nearly impossible, leaving teams unable to distinguish theoretical risks from genuine exploitable threats.

## The Solution

CyCognito and Wiz together enable cloud security teams to significantly increase cloud workload security coverage by combining the deep visibility of Wiz's CNAPP with CyCognito's continuous DAST and deployment gap discovery.

Wiz's CNAPP prioritizes the risks that matter most and detects real-time threats across your cloud environment. CyCognito complements this by operating independently of cloud provider APIs to discover externally exposed assets across sanctioned and unsanctioned environments—including shadow IT, forgotten instances, and third-party services—spanning public, private, and hybrid clouds..

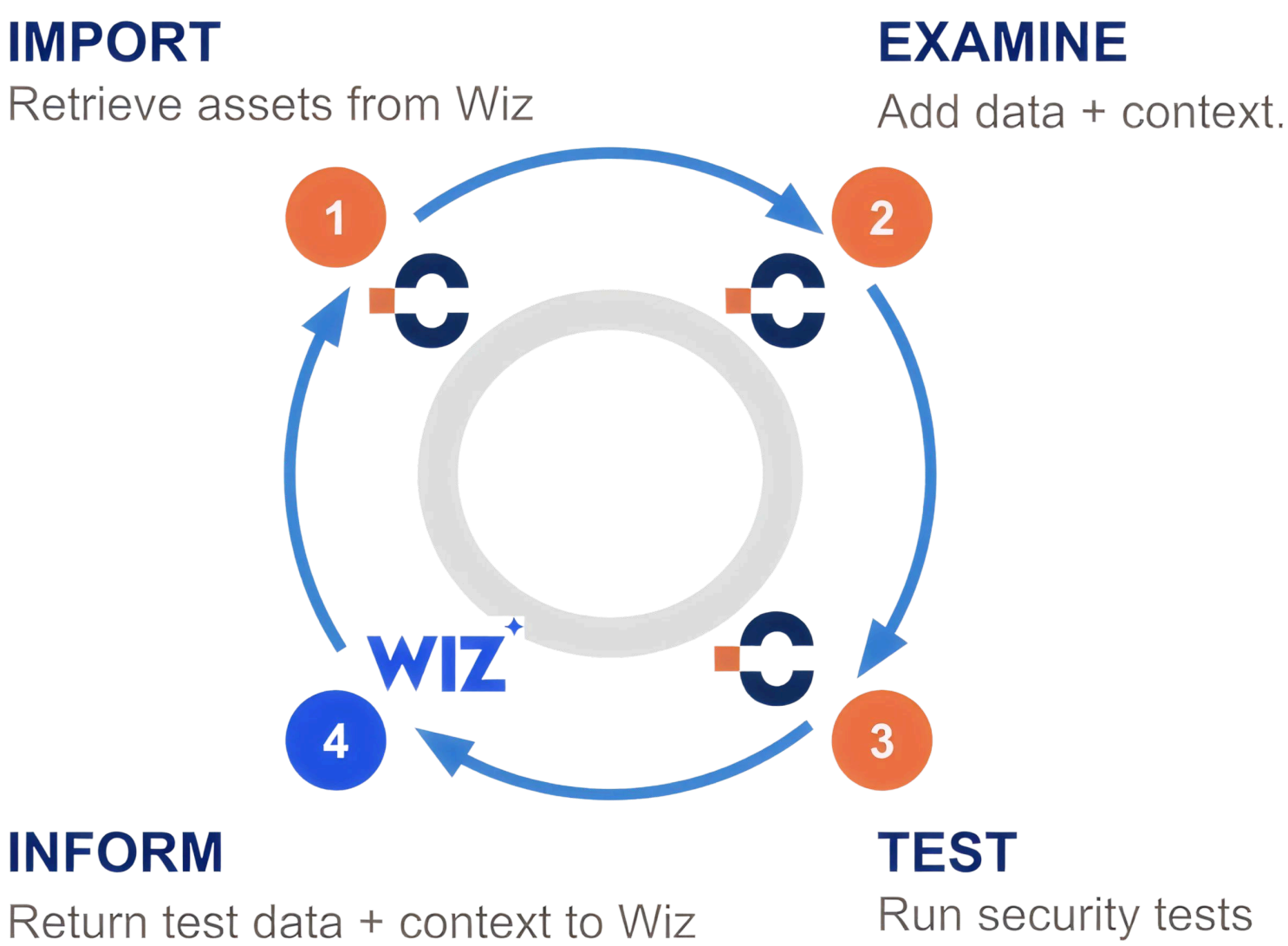



With over 90,000 non-intrusive active tests, including DAST for web apps, CyCognito validates real-world risks such as OWASP Top 10 issues, sensitive data exposures, and insecure configurations.

These findings flow into Wiz platform, where they are visualized in the Security Graph and correlated with internal cloud context. The result is improved risk prioritization, new visibility into attack paths, and faster, more informed remediation.

## How It Works

The Wiz-CyCognito integration creates a seamless security workflow. This begins with your existing Wiz asset inventory and extends protection across your complete external attack surface. Then, through automated data exchange and unified reporting, security teams gain comprehensive visibility and validated findings without switching between platforms.



Together, Wiz and CyCognito provide unified, attacker-aware visibility that helps teams detect, validate, and remediate exposures faster.

Here's a more detailed breakdown of how it works:

## (1) Import

CyCognito automatically retrieves Wiz's complete asset inventory, providing a foundation of known cloud resources and applications for comprehensive security testing.

## (2) Examine

CyCognito performs autonomous external discovery to identify additional exposed assets (including shadow IT and ungoverned applications), then gathers over 200 data points for every asset including attribution information, port status, and business purpose.

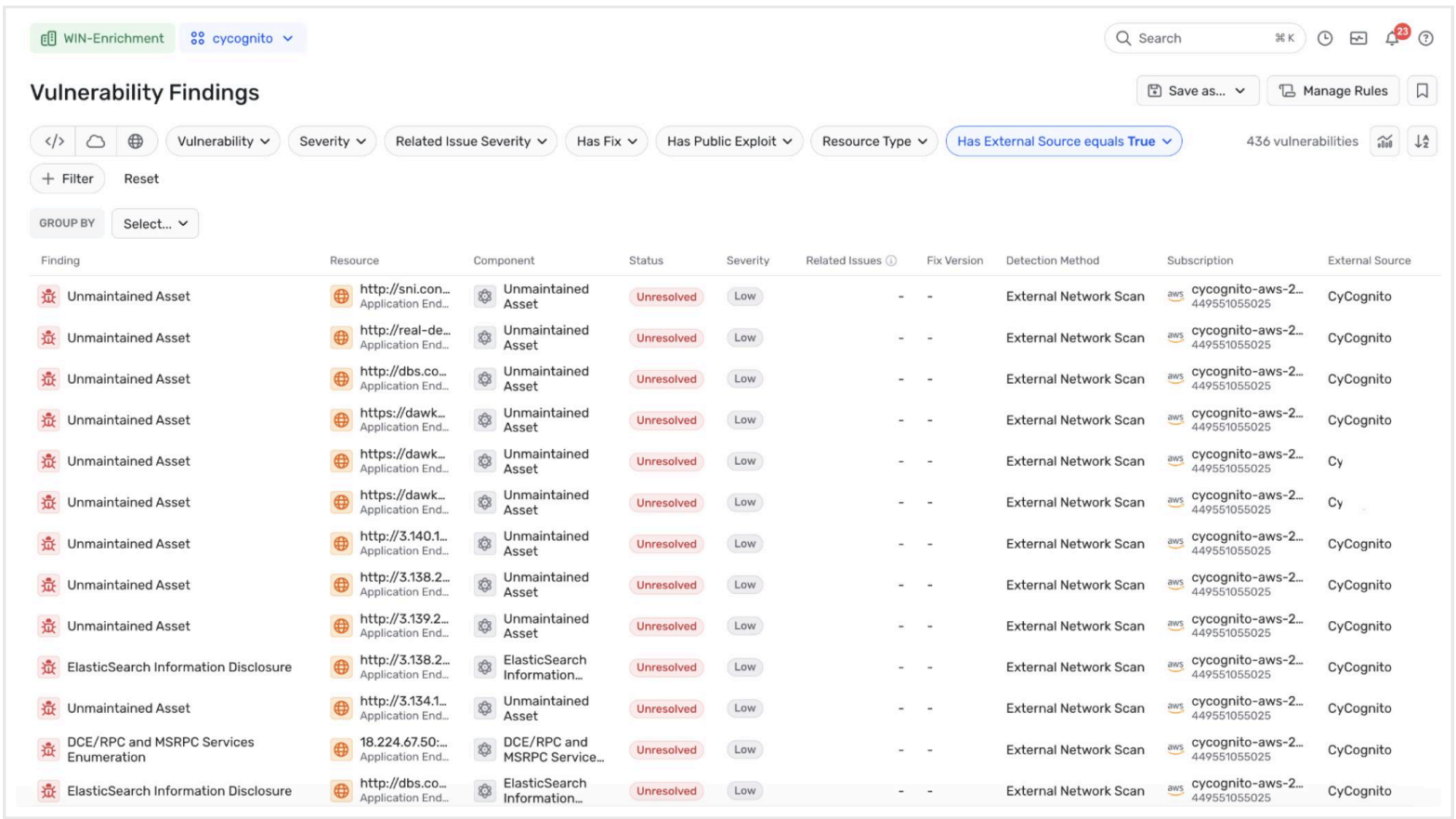



Figure 1: New high-risk issues or from CyCognito integration

## (3) Test

CyCognito executes over 90,000 passive and active security tests, including DAST for web applications, to identify exploitable vulnerabilities such as OWASP Top 10 risks, sensitive data exposure, and security misconfigurations in live production environments.

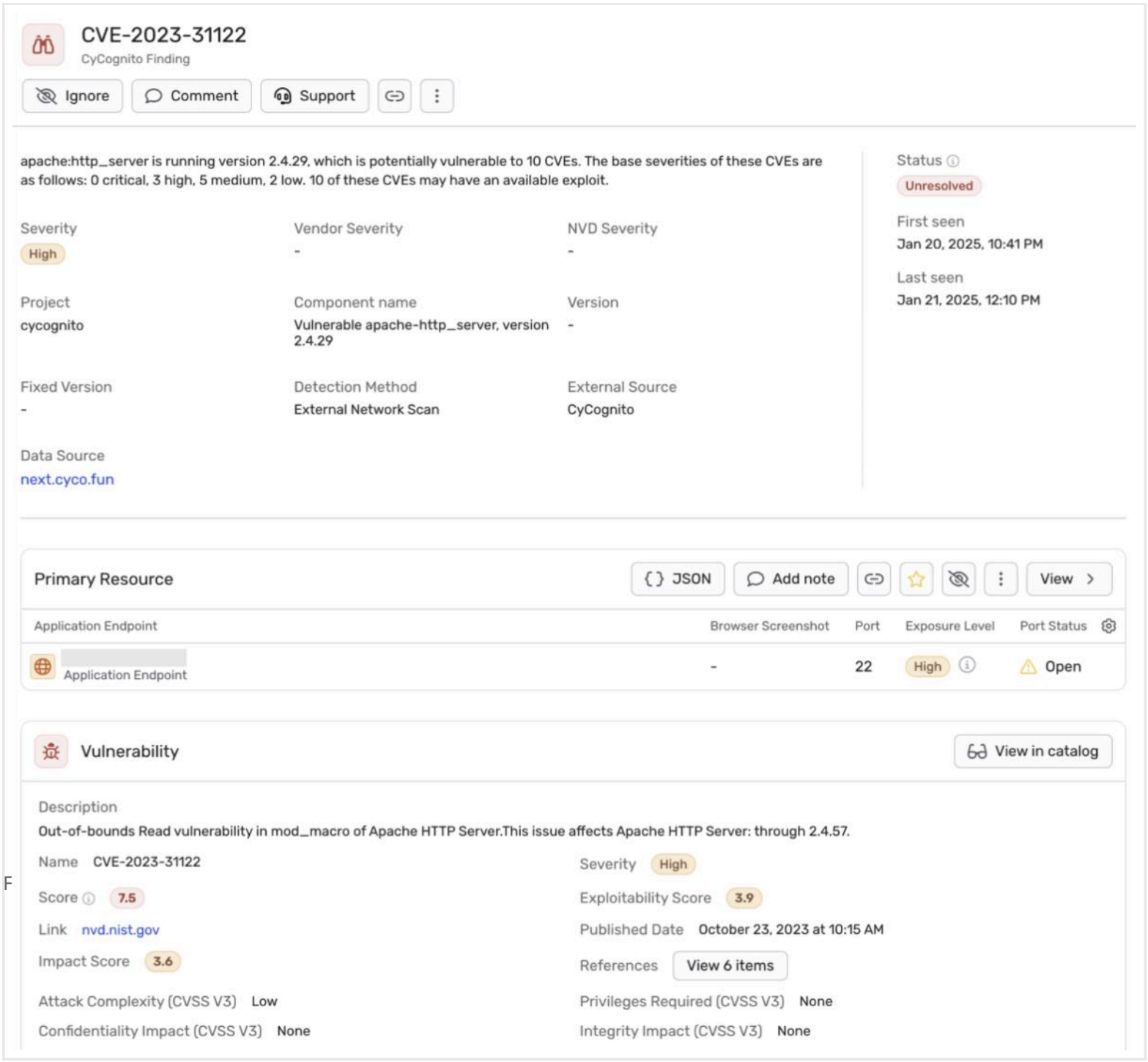



Figure 2: Detailed CyCognito test results in Wiz

## (4) Inform

CyCognito delivers validated test results, contextual data, and prioritized findings directly back to Wiz with detailed remediation guidance, enabling security teams to focus on genuinely exploitable threats rather than theoretical risks.

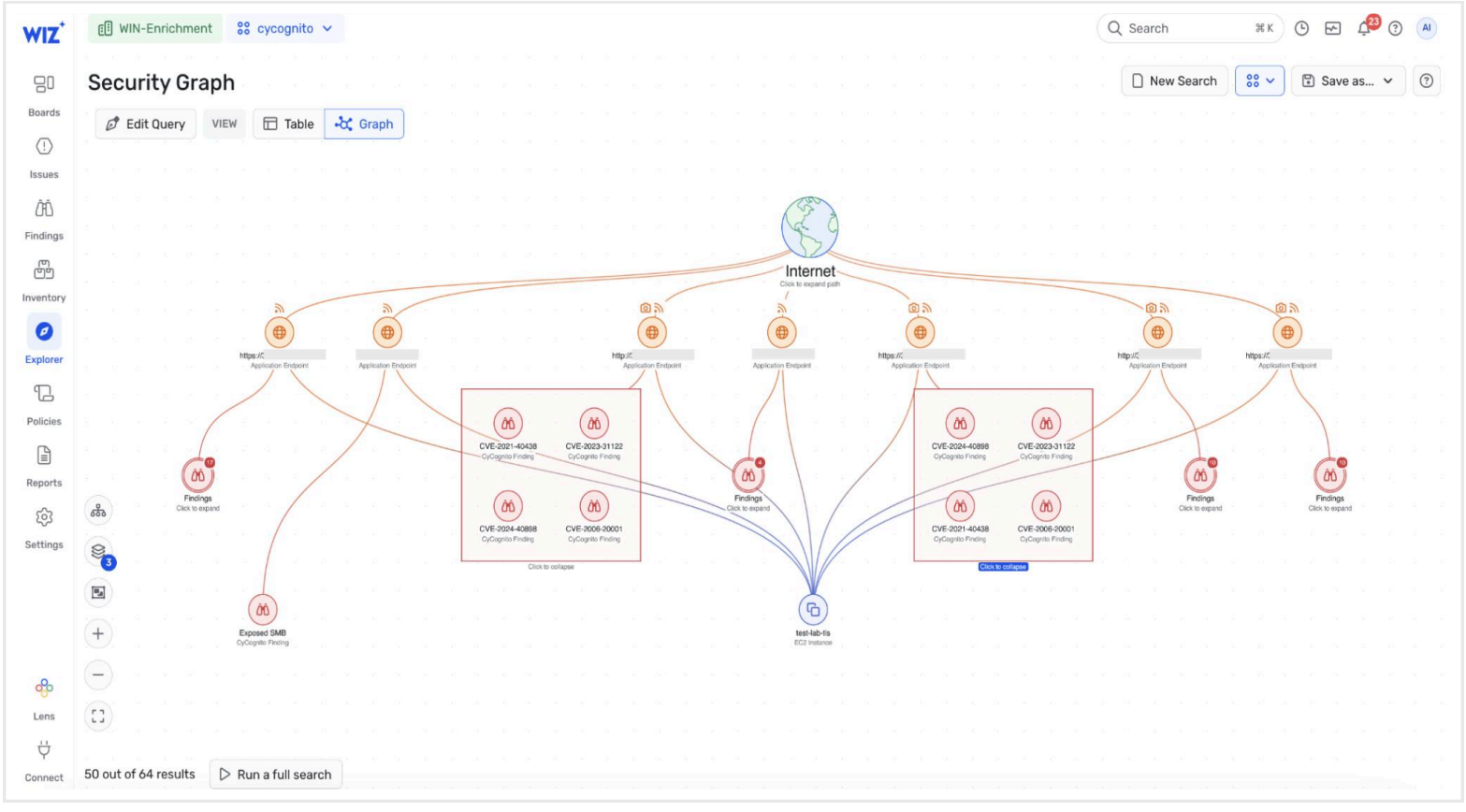



Figure 3. CyCognito test results visible in Wiz security graph

# Better Together

Wiz and CyCognito deliver a unified approach to cloud and external exposure management—combining internal visibility with the attacker's external perspective. Wiz provides deep context across cloud configurations, vulnerabilities, identities, and workloads, while CyCognito extends protection beyond the cloud perimeter to uncover and validate unmanaged, shadow, and third-party assets.

This joint solution enables organizations to:

- **Complete Security Coverage**
  Eliminate blind spots by combining Wiz's internal cloud inventory with CyCognito's external reconnaissance across all sanctioned and unsanctioned environments.

- **Verified Risk Prioritization**
  Focus on real threats through CyCognito's 90,000+ active security tests integrated with Wiz's contextual cloud intelligence.

- **Enhanced Attack Path Visibility**
  Understand complete attack chains from external exposure to internal cloud resources through unified security graph analysis.
- **Accelerated Remediation**
  Reduce mean time to remediation from months to days through automated workflows and security graph correlation.

By integrating CyCognito's continuous external discovery and attacker validation into Wiz's Security Graph, organizations gain an attacker-aware view of their entire digital footprint. This comprehensive visibility helps security teams focus on what matters most, accelerate remediation, and reduce business risk across hybrid and multi-cloud environments

## About Wiz

Wiz is a leading Cloud-Native Application Protection Platform (CNAPP) that secures AWS, Azure, GCP and hybrid environments. Its unified Security Graph correlates misconfigurations, vulnerabilities, identity risks and runtime threats. Wiz then automates risk prioritization and remediation within your DevSecOps toolchain.

## About CyCognito

CyCognito is an external exposure management platform that reduces risk by discovering, testing and prioritizing security issues. The platform scans billions of websites, cloud applications and APIs and uses advanced AI to identify the most critical risks and guide remediation. Emerging companies, government agencies and Fortune 500 organizations rely on CyCognito to secure and protect from growing threats.

To learn how the CyCognito platform uniquely helps you identify and prioritize the paths of least resistance into your IT ecosystem, so that you can eliminate them, visit CyCognito.com.