Joint Solution Brief Form

We're excited to collaborate with you on a joint solution brief that highlights the value of our integration for customers, prospects, and our sales teams alike.

🤝 Product Information

Product Name to Integrate with Wiz
(Max 100 characters)

HackerOne

Executive Summary of the Integration
Brief overview of what the integration does and why it matters.

The Wiz and HackerOne integration brings proven, exploitable findings from penetration tests, bug bounty, vulnerability disclosure, and AI red teaming programs directly into Wiz as Attack Surface findings, each carrying severity, proof of concept, and remediation guidance. Findings are automatically mapped on the Security Graph to the underlying cloud infrastructure, identities, and data flows, revealing the full blast radius. As a result, security teams have an extended view into the impact of risks, helping them better prioritize and remediate.

🤝 Market Context

Market Challenge
Describe the problem or gap in the market that this integration addresses.
(Max 440 characters)

Penetration test and bug bounty findings often live in isolation, disconnected from the cloud environments they impact. Without visibility into the underlying

infrastructure, identities, and data flows behind an exploitable finding, security teams struggle to assess its true blast radius and prioritize accordingly. Findings get handed off to development teams and quickly buried in backlogs as feature work takes priority, leaving proven, exploitable risk exposed and remediation stalled.

Key Benefits of the Integration

List 3–5 clear and compelling benefits. Use bullet points.

- **Full Blast Radius Visibility:** HackerOne findings, including severity, proof of concept, and remediation guidance, flow into Wiz and are automatically mapped on the Security Graph to the underlying infrastructure, identities, and data flows, revealing the true impact of each exploitable finding.
- **Accelerated Remediation:** Security teams can prioritize risk based on cloud context and route findings to the right owners within Wiz, closing the gap between discovery and fix.
- **Seamless Workflow Integration:** Researchers and program managers continue working in HackerOne while the broader security organization drives remediation in Wiz, no context switching or duplicate effort.

 Storytelling & Use Case

The “Better Together” Story

Explain why this partnership makes sense and how it adds value.
(Max 1000 characters)

HackerOne delivers proven exploitability from skilled security researchers who test like real attackers. Wiz delivers deep visibility into the cloud environments that those findings impact. Together, they connect what's exploitable with what's at risk, giving security teams the context to act decisively. Findings are no longer isolated reports—they're mapped to the infrastructure, identities, and data that reveal the full blast radius, so teams prioritize based on real impact, not guesswork.

Use Case Overview

Detail the challenge, how the integration solves it, and the resulting impact.
(Max 1400 characters)

Use Case: Tracing a Critical Finding from Bug Bounty Report to Cloud Blast Radius

A security researcher participating in a bug bounty program discovers unauthenticated access to an admin password reset endpoint in a customer-facing web application. The finding is validated in HackerOne with a proof of concept showing the attacker can reset admin credentials without authentication and gain full administrative access.

Challenge: The security team knows the vulnerability is exploitable—but the web application runs across multiple cloud environments. Which cloud accounts host the affected infrastructure? What data stores does the application connect to? What could an attacker with admin access reach beyond the application itself? The pen test report alone doesn't answer these questions, and manually tracing the path across cloud environments takes days.

Solution:
The finding flows from HackerOne into Wiz as an Attack Surface finding. The associated host is automatically mapped on the Security Graph, immediately showing the security team that the vulnerable application runs on an EC2 instance connected to an RDS database containing customer records, with an attached IAM role that can access secrets in AWS Secrets Manager.

With the full picture quickly visible in Wiz, the security team can prioritize based on real impact and drive remediation with the right context: the exploitable entry point, the level of access gained, and the sensitive data at risk. What started as a single bug bounty report becomes a prioritized, contextualized remediation effort rather than another item lost in a backlog.

Company & Contact Details

Company Description

Briefly describe your company, including your focus and mission.
(Max 420 characters)

HackerOne is a global leader in Continuous Threat Exposure Management (CTEM). The HackerOne Platform unites agentic AI solutions with the ingenuity of the world's largest community of security researchers to continuously discover, validate, prioritize, and remediate exposures across code, cloud, and AI systems. Through solutions like bug bounty, vulnerability disclosure, agentic pentesting, AI red teaming, and code security, HackerOne delivers measurable, continuous reduction of cyber risk for enterprises. Industry leaders, including Anthropic, Crypto.com, General Motors, Goldman Sachs, Lufthansa, Uber, UK Ministry of Defence, and the U.S. Department of Defense, trust HackerOne to safeguard their digital ecosystems. HackerOne was recognized in Gartner's Emerging Tech Impact Radar: AI Cybersecurity Ecosystem report for its leadership in AI Security Testing and has been named a Most Loved Workplace for Young Professionals (2024).

File Uploads

Company Logo

Format: SVG

Integration Screenshots (x2)

Format: PNG

Max Size: 1 MB each

Integration Architecture Diagram

Format: PNG

Max Size: 1 MB