PARTNER BRIEF

Armis + HackerOne

Effectively bridge the gap between asset discovery and risk remediation.

From Visibility to Validation

Security teams are overwhelmed by thousands of potential exposures across an ever-expanding attack surface, yet they lack the research depth to know which ones truly matter from an adversarial technical research perspective. While Armis provides critical visibility and identifies exploitability in the wild, this capability is now augmented by HackerOne's security researcher community testing to confirm how these global threats specifically impact a customer's unique environment. Without this direct link between asset criticality and proven exploitability, organizations risk wasting effort on theoretical issues while critical, manually-verifiable exposures remain unaddressed.

Transforming Asset Discovery into Actionable Defense

This integration combines Armis's comprehensive real-time visibility into all connected assets with HackerOne's elite security researcher community to transform theoretical risks into validated, actionable intelligence. Armis identifies every asset in the enterprise, from IT, OT, IoT to IoMT, and HackerOne's researchers then target those specific assets to prove exploitability, ensuring remediation is focused on real-world impact.

Precision Prioritization

The integration replaces guesswork with evidence by mapping adversarial research findings directly to the authoritative asset records maintained by Armis. This allows teams to see not just that a vulnerability exists, but that a researcher has successfully bypassed the specific defenses of a business-critical asset.

Adversarial researcher Context for Inventory: Use Armis asset data to guide HackerOne researchers toward your most critical or exposed business surfaces.

Validated Prioritization: Shift from "CVSS-based" luck to "exploit-based" certainty by combining Armis risk scores with proven findings from the HackerOne community.

Dynamic Exposure Tracking: Automatically update the risk posture in Armis as soon as a researcher validates a fix or identifies a new bypass.

Use Case

Validated Exploit on a Critical Medical IoT Device

1. Armis continuously discovers and classifies a connected medical imaging device in a hospital network. It identifies firmware version, exposure, segmentation posture, and clinical criticality.
2. HackerOne's offensive testing identified a remote code execution vulnerability affecting that device model.
3. The integration automatically:
   - Maps the finding to Armis' authoritative device record
   - Enriches the vulnerability with asset criticality and operational risk
   - Flags regulatory impact (e.g., healthcare compliance exposure)
   - Routes the issue to the appropriate IT/biomedical engineering team
4. Prioritization reflects:
   - Confirmed exploitability (HackerOne)
   - Business/clinical impact (Armis asset context)
   - Network exposure level
5. Remediation is tracked through integrated workflows, and exposure status is continuously monitored by Armis post-fix.

> **Outcome:** The organization eliminates a validated, high-impact exposure on a critical operational asset with clear auditability and measurable risk reduction.

Why This Integration Matters

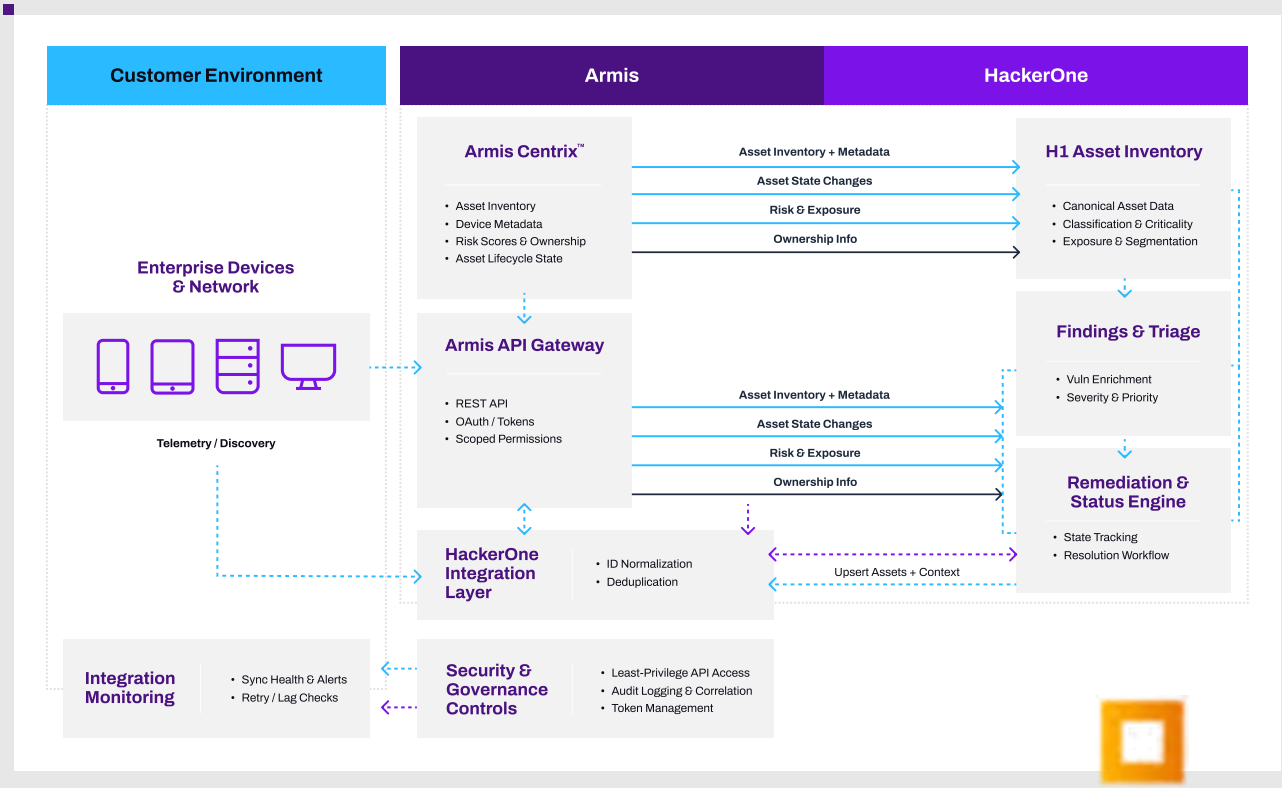
Security: Identify and validate exploitable vulnerabilities, reduce false positives, and prioritize remediation based on proven impact.

End-to-end Platform: Gain continuous visibility into validated adversarial research and exposures through a unified platform that connects discovery, prioritization, and remediation workflows.

Operational: Decrease triage time, eliminate duplicate analysis, and accelerate fix cycles with findings that are already validated and contextualized.

Financial: Maximize security ROI by focusing resources on exposures that materially reduce breach risk and lower overall time at risk.

Technical Overview



Asset Sync

- Armis exposes asset inventory, device metadata, risk scores, and ownership via API.
- HackerOne ingests asset identifiers and contextual metadata.

Vulnerability Mapping

- HackerOne findings are enriched with:
  - Device classification
  - Business criticality
  - Exposure attributes
  - Network segmentation context

Bi-directional Updates

- Remediation status updates from HackerOne reflect back into Armis for continuous exposure tracking.
- Armis updates and adjusts prioritization dynamically (asset state change, decommissioning, drift).

Policy Enforcement

- Access controls and data sharing follow least-privilege API scopes.
- All enrichment and data flows are auditable.

Executive Summary

While Armis tells you **what** you have and its potential risk, HackerOne provides **how** an attacker could exploit it. Together, they provide a continuous loop of discovery and adversarial validation that ensures your most critical assets are resilient against real-world attacks.

hackerone

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.

ARMIS®

Understand the Armis difference:

- Comprehensive visibility
- Intelligent insights
- Proven outcomes

Try Armis Centrix™ Today

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

+1 888 452 4011

armis.com