ARMIS® IONIX

PARTNER BRIEF

IONIX + Armis

© Copyright Armis 2025

Overview

Enterprises today face an unprecedented challenge: their digital environments are expanding faster than security teams can keep pace. Cloud adoption, mergers and acquisitions, remote work, and third-party dependencies have created an attack surface that is vast, constantly changing, and difficult to secure. Traditional tools either focus externally on what attackers can see or internally on what organizations own, but rarely both.

The integration of IONIX External Exposure Management with the Armis Centrix™ closes this gap. Together, they deliver an end-to-end cyber exposure management solution that connects external attack surface visibility and exploit validation with unmatched internal asset intelligence, ownership mapping, and business risk context.

The Market Today & the Challenge

IT, Security, and Risk leaders are tasked with solving for:

- **Dynamic and borderless attack surfaces** – Shadow IT, subsidiaries, and cloud sprawl create exposures that are often invisible to internal teams.
- **Noise and false positives** – Thousands of alerts, most unvalidated, overwhelm teams and waste precious remediation cycles.
- **Lack of linkage** – External exposures rarely map cleanly to the internal assets, owners, and business functions they threaten.
- **Prolonged exposure windows** – Unclear accountability and context leave vulnerabilities unaddressed, giving attackers the advantage.

For these executives, the issue is no longer about finding vulnerabilities, it's about knowing which ones matter, who owns them, and how to focus the right resources on what matters most to the specific organization.

© Copyright Armis 2025

The Joint Solution

IONIX + Armis = Full-Spectrum Cyber Exposure Management

IONIX brings continuous external asset discovery, exposure validation, and false-positive elimination. It ensures that only exploitable vulnerabilities make it to the remediation pipeline.

ARMIS brings deep internal visibility across IT, OT, IoT, and medical environments whether the assets are physical, virtual or a combination. It enriches exposure data with asset relevant information in addition to ownership, dependencies, and operational risk context.

When combined, the two platforms enable organizations to:

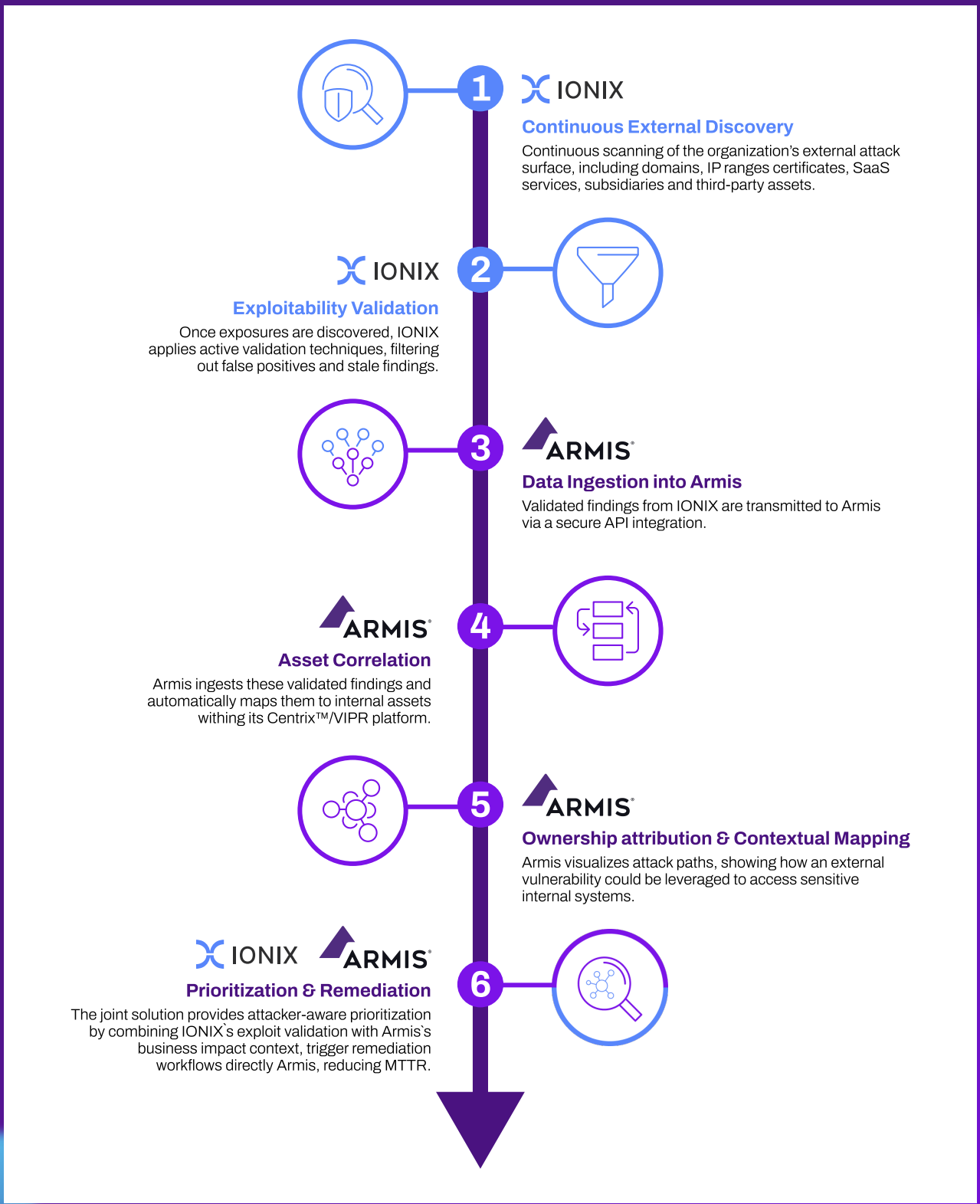
See everything across external and internal attack surfaces.

Validate what matters with deduplication, risk contextualization, and prioritization.

Act fast with precise mapping to owners and remediation workflows.

© Copyright Armis 2025

How it works



© Copyright Armis 2025

The integration establishes a closed-loop exposure management workflow:

1. **Continuous External Discovery (IONIX)**
   Finds internet-facing assets across domains, IP ranges, subsidiaries, SaaS, and third parties.
2. **Exploitability Validation (IONIX)**
   Confirms which vulnerabilities are actively exploitable, eliminating noise and stale alerts.
3. **Data Flow into Armis**
   Validated findings flow securely via API into Armis with full metadata.
4. **Asset Correlation (Armis)**
   Maps exposures to affected IT, OT, IoT, and IoMT devices inside the enterprise.
5. **Ownership & Contextual Mapping (Armis)**
   Assigns exposures to business units, device owners, and dependencies, visualizing attack paths.
6. **Prioritization & Remediation (Joint)**
   Teams can immediately prioritize based on exploitability and business impact, cutting Mean Time to Remediation (MTTR) from months to days.

Key Use Cases

The true strength of the IONIX and Armis integration lies in how it translates complex challenges into practical, high-value outcomes for the organization. By combining continuous external discovery and exploit validation with deep internal asset intelligence and business context, the joint solution empowers organizations to eliminate blind spots, cut through noise, and focus resources where they matter most. The following use cases highlight how enterprises benefit from this unified approach.

- **Comprehensive Attack Surface Visibility**
  Unified external and internal inventories eliminate blind spots.
- **Validated Risk Identification**
  Only exploitable vulnerabilities flow into pipelines, saving time and reducing wasted effort.
- **External-to-Internal Risk Correlation**
  Maps external exposures to internal assets, owners, and business processes.
- **Accelerated Remediation**
  Automates ownership attribution and remediation workflows, drastically reducing MTTR.
- **Compliance & Posture Assurance**
  Demonstrates measurable risk reduction and supports frameworks such as HIPAA, NIST, and IEC.

© Copyright Armis 2025

Benefits & Key Outcomes

FEATURES	BENEFITS
Continuous External Asset Discovery	Eliminates blind spots across cloud, subsidiaries, and internet-facing assets.
Exploitability Validation	Ensures teams focus on high-fidelity risks, not false positives.
Unified Asset Intelligence	Correlates external exposures with internal IT, OT, IoT, and IoMT assets in one view.
External-to-Internal Risk Correlation	Enables accurate impact assessment and prioritization.
Automated Ownership Attribution	Speeds accountability and streamlines workflows.
Prioritized Remediation Workflow	Cuts MTTR from months to days, boosting resilience.

Key Outcomes:

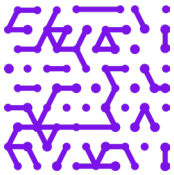
- Blind spots eliminated across the entire digital estate.
- Focus on exploitable, business-relevant risks.
- Faster remediation with clear accountability.
- Measurable improvement in security posture.

© Copyright Armis 2025

Summary

The IONIX and Armis integration bridges a critical gap in cybersecurity. IONIX ensures organizations know exactly which external exposures are exploitable, while Armis maps those risks to the internal assets, owners, and business functions they could disrupt. The result is a holistic, actionable view of enterprise risk that addresses the full portfolio of internal as well as external assets as well as a closed loop process in terms of the prioritization, methodology and assignments to address unacceptable organizational risk.

Together, IONIX and Armis enable security teams to move beyond reactive vulnerability management toward a proactive, risk-based defense strategy that aligns with how attackers operate and the most effective course of response actions.



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

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial

© Copyright Armis 2025