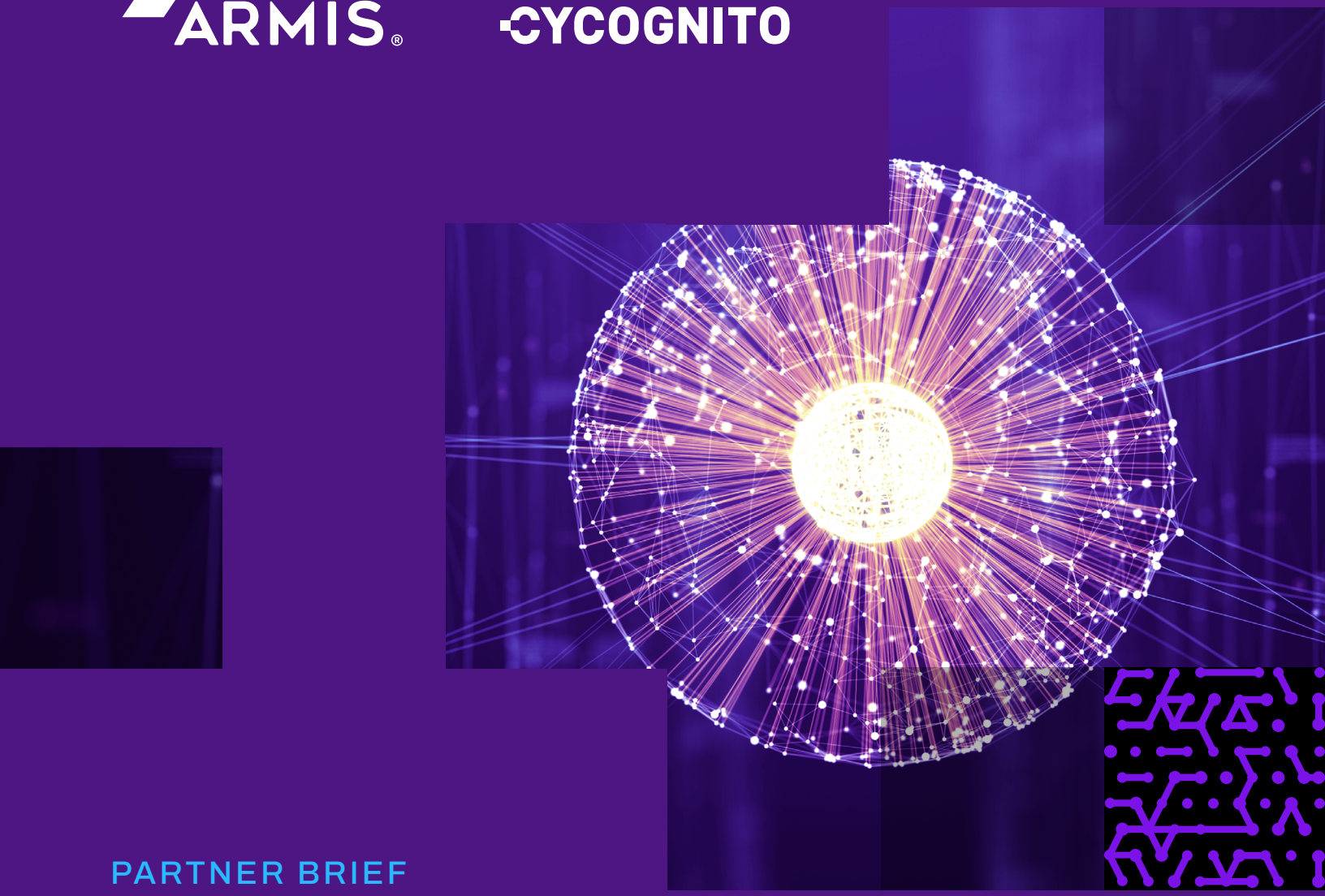
ARMIS®

CYCOGNITO



PARTNER BRIEF

Holistic Exposure Management – Actionable Insight Into Your Attack Surface Risks

CyCognito and Armis help Security and IT Operations teams gain complete asset visibility, map critical attack paths, and accelerate remediation.

Executive Summary

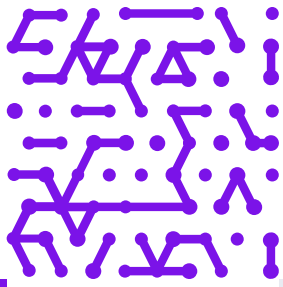
The integration of CyCognito's external attack surface management with Armis Centrix™ delivers the industry's first truly comprehensive internal and external exposure management solution. CyCognito provides visibility into externally exposved assets such as domains, IP addresses, URLs, and certificates, while Armis provides continuous, real-time insight into all internal IT, OT, IoT, and IoMT assets. Together, they enable organizations to map critical attack paths, prioritize based on real-world exploitability, and accelerate risk remediation, thereby reducing mean time to resolution (MTTR) from months to days and significantly strengthening security posture.

Before

- Blind spots and shadow IT/OT/IoT create risk
- Manual effort to identify asset owners
- No visibility into how external risks affect internal assets
- Thousands of unprioritized alerts and vulnerabilities

After

- Continuous discovery of external and internal assets
- Automated ownership attribution across environments
- External-to-internal risk correlation and impact assessment
- Risk prioritization based on exploitability and proximity to critical assets

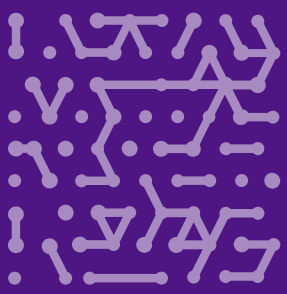


The Challenge

Organizations face complex, expanding attack surfaces that include both visible external assets and hidden internal systems. M&A activity, shadow IT, unmanaged IoT, and cloud sprawl add further complexity. Even with strong internal visibility, security teams often lack insight into how externally exposed assets relate to internally critical systems, making it difficult to prioritize and remediate risks that matter most.

The Solution

The Armis + CyCognito integration bridges the gap between **external discovery** and **internal security**. CyCognito continuously maps an organization's externally exposed assets and tests for vulnerabilities, while Armis Centrix™ identifies and monitors internal assets, including IT, OT, IoT, and IoMT, at scale. The integration correlates external risk data with internal context, enabling teams to quickly understand the full scope and impact of threats, assign ownership, and remediate efficiently.



Joint Value Proposition

- CyCognito brings industry-leading external asset discovery and risk validation, helping security teams identify unknown or misconfigured internet-facing assets such as domains, certificates, IPs, and exposed cloud infrastructure, and assess their exploitability using automated testing (DAST, vulnerability assessment, and pen testing).
- Armis brings unparalleled internal asset intelligence across IT, OT, IoT, and IoMT, while also identifying how external threats could reach internal “crown jewel” systems through attack paths, assigning ownership, and enabling precise, prioritized remediation based on exposure impact.

Together, Armis and CyCognito provide end-to-end exposure management, helping organizations:

- See everything (inside and out)
- Fix what matters most
- Prove security posture improvements

Better Together: Key Benefits

Unified Internal + External Asset Discovery
Gain a complete, continuously updated inventory of all assets, from public-facing domains to unmanaged devices in remote facilities.

Continuous External Risk Validation
CyCognito automatically discovers, tests, and ranks exposed assets based on exploitability and attacker interest.

Internal Impact Correlation and Attack Path Modeling
Armis Centrix™ maps how vulnerabilities and threats could be leveraged to reach sensitive internal systems, including medical devices, industrial controllers, and core IT infrastructure.

Automated Ownership Attribution
Armis links vulnerabilities to specific business owners across all environments, IT, OT, IoT, cloud, and medical systems, accelerating resolution.

Attacker-Aware Prioritization
CyCognito brings an external attacker perspective, while Armis provides an early warning of threats by leveraging AI, human threat intelligence (HUMINT), honeypots, and dark web monitoring.

Security Control Validation
Identify security gaps across CAASM, CPS, or SASE initiatives by comparing internal defenses with real-world external exposures.

How it Works

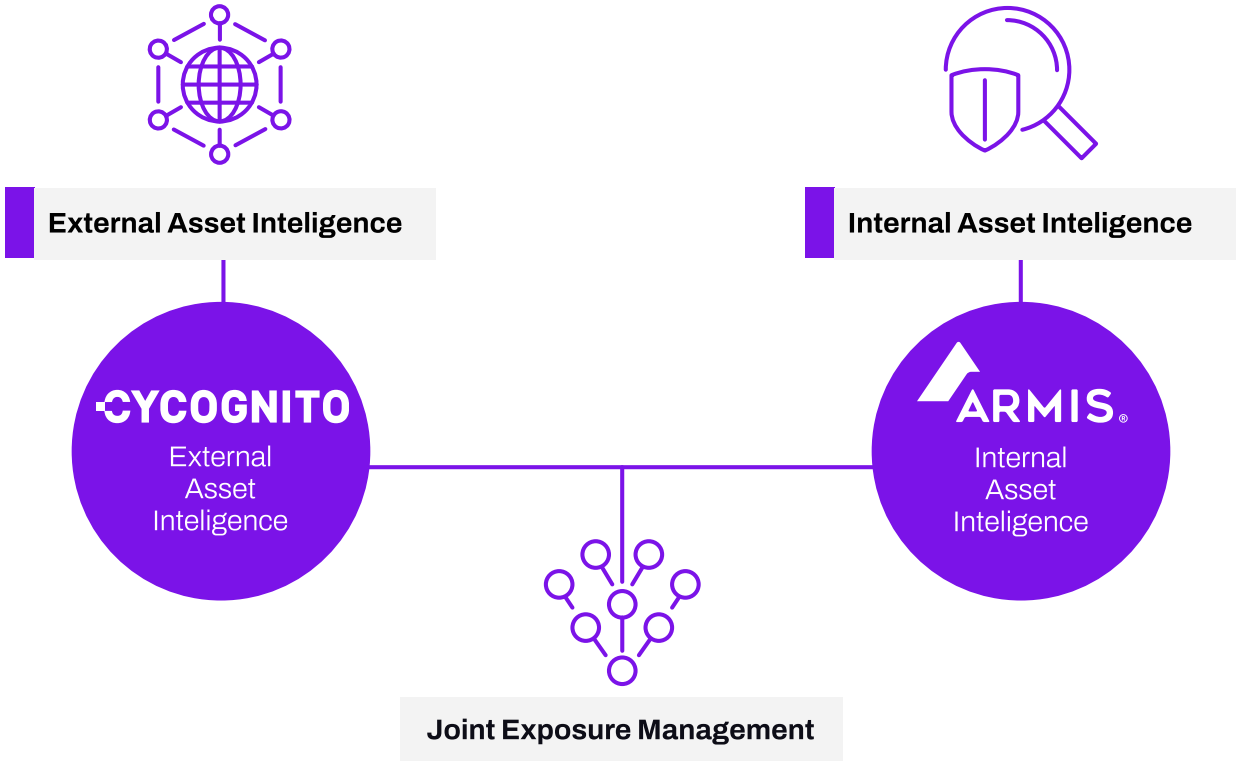
01 **Deploy the integration** to link CyCognito's external findings (e.g., exposed IPs, vulnerable domains) with Armis Centrix™ internal asset data and risk insights.

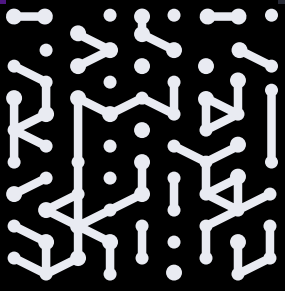
02 **Correlate data across all environments** including external, IT, OT, IoT, IoMT, cloud, and code repositories, for a unified risk picture.

03 **Prioritize based on real-world attacker behavior** and internal criticality, using dynamic context from both platforms.

04 **Remediate faster** with automatic attribution, intelligent grouping, and deduplication of issues, thus ensuring no effort is wasted and every risk is tracked to resolution.

Together, Armis and CyCognito offer complementary capabilities that unify external and internal attack surface management into a cohesive, risk-based workflow. By combining CyCognito's attacker-perspective discovery with Armis's deep internal visibility, organizations can go from reactive vulnerability management to proactive, prioritized remediation, before threats turn into a full blown attack.





CYCOGNITO

CyCognito is an external exposure management platform that discovers, tests, and prioritizes security risks. The platform provides the deepest, most accurate mapping of external attack surfaces without manual effort or seed inputs, and conducts 80,000+ security tests to identify critical vulnerabilities before attackers can exploit them.

Trusted by Fortune 500 companies and government agencies, CyCognito reduces remediation time from months to days. Learn more at cycognito.com

ARMIS

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