PARTNER BRIEF

Unified Cyber Exposure Detection and Automated Remediation with Armis and Invicta

Overview

The Armis and Invicta Software partnership delivers a true closed-loop cyber exposure management solution, eliminating the long-standing disconnect between knowing where risk exists and actually fixing it at scale.

Armis provides authoritative, real-time asset intelligence across IT, IoT, OT, cloud, and medical devices thereby establishing the single source of truth for what exists, what's critical, and what's at risk. Invicta takes that intelligence and operationalizes it, enforcing SLAs, orchestrating workflows, and automating remediation actions across security and IT operations.

Together, Armis and Invicta move organizations beyond alerting and ticketing to measurable, outcome-driven risk reduction at machine speed, with comprehensive enterprise governance.

State of the Market

Enterprise attack surfaces are expanding faster than security teams can keep up. Cloud adoption, unmanaged devices, OT systems, medical devices, and ephemeral workloads have shattered traditional asset inventories and made static CMDBs obsolete. Meanwhile, security tools continue to operate in silos thus leaving remediation to slow, unprioritized manual processes.

At the same time, regulators and industry frameworks are raising the bar. Organizations are now expected to demonstrate:

- Continuous asset awareness
- Risk-based prioritization
- Defined remediation timelines (SLAs)
- Verifiable, auditable papertrails

Security teams are under pressure to do more with fewer people, yet remain trapped in workflows that rely on swivel-chair coordination between discovery tools, ticketing systems, and IT operators.

The Challenge

Most organizations suffer from a fundamental operational gap:

- **Visibility without action -** Security tools identify risks but lack the ability to enforce remediation in an efficient and comprehensive manner.
- **Action without context -** IT and SecOps teams are asked to remediate without understanding asset criticality, exposure, or business impact.
- **Manual coordination -** Analysts must triage alerts, open tickets, chase owners, track SLAs, and report compliance, all by hand.

This fragmentation drives up MTTR, increases human error, and leaves critical exposures unresolved longer than the business or regulators will tolerate.

The Joint Solution: Intelligence Meets Execution

Armis and Invicta jointly deliver a tightly integrated solution that unifies asset intelligence, exposure detection, and automated remediation into a single operational model.

What Armis Brings

Armis Centrix™ provides:

- **Continuous, real-time asset discovery** across IT, IoT, OT, and medical devices whether they are physical, virtual or a combination
- **Deep asset context**, including identity, ownership, location, criticality, and behavior
- **High-fidelity exposure detection**, spanning vulnerabilities, misconfigurations, and anomalous activity
- **Risk prioritization based on business impact**, not CVSS alone

Armis answers the most critical questions:

What do we have? | **What's exposed?** | **What actually matters right now?**

What Invicta Brings

Invicta SecOps provides:

- **Integrated SecOps and IT operations, bridging security, IT, and service desk teams**

Invicta answers the next question:

How do we fix it consistently, quickly, and at scale?

How It Works

The joint Armis and Invicta solution operates as a continuous, closed-loop security workflow that connects detection directly to execution. Armis continuously discovers and monitors all connected assets across IT, IoT, OT, and medical device environments using a combination of passive and safe smart active techniques. As assets are identified, Armis builds deep contextual awareness by capturing asset identity, ownership, criticality, behavior, and exposure so security teams understand not just what exists, but what matters most to the business.

When Armis detects vulnerabilities, misconfigurations, or anomalous behavior, it generates high-fidelity alerts enriched with this asset intelligence. These alerts are automatically ingested into the Invicta SecOps platform through real-time integrations or scheduled data feeds, eliminating the need for manual correlation or duplicate triage.

Invicta uses the incoming asset, risk context, and “finding to fix” recommendations to operationalize response. Each issue is evaluated against predefined SLA policies that account for asset criticality, exposure severity, and business impact. Based on this logic, Invicta initiates the appropriate remediation path by either executing automated actions such as patching, configuration changes, or software updates, or routing tasks through governed approval workflows where human oversight is required.

Throughout the process, the joint solution tracks progress from detection through resolution, ensuring remediation is completed within defined timelines and fully auditable. The result is a unified operational flow where insight, prioritization, execution, and validation occur continuously, enabling organizations to move from identifying risk to demonstrably reducing it at scale and with confidence.

Core Use Cases

- Automated incident and ticket creation from Armis alerts
- Exposure-based remediation prioritization across hybrid environments
- Asset-driven patching and software lifecycle management
- Unified SecOps and IT service operations
- Continuous compliance monitoring and SLA enforcement (with auditing drill down)

Joint Value Proposition

Together, Armis and Invicta deliver:

- **From insight to impact -** Detection is directly tied to the business
- **From alerts to outcomes -** Reduced risk, not just reduced noise
- **From manual effort to automation -** Security at enterprise scale
- **From fragmented tools to a unified operating model**

This partnership transforms security operations from reactive firefighting into proactive, governed, and measurable cyber exposure management.

Key Business Outcomes

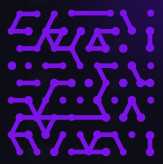
Organizations gain:

- Dramatically reduced mean time to detect and respond (MTTD/MTTR)
- Lower operational overhead through automation, prioritization and orchestration
- Clear asset ownership and accountability
- Continuous, real-time compliance visibility
- A unified system of record for security and IT operations
- Auditable, SLA-backed remediation and reporting

Conclusion

Armis Centrix™ establishes the foundation of trust, a real-time, authoritative view of every asset and exposure. Invicta SecOps ensures that intelligence drives decisive, automated action.

Together, Armis and Invicta deliver a unified, closed-loop operating model that bridges the gap between knowing risk exists and proving it has been eliminated.



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