PARTNER BRIEF

# The Armis and ServiceNow Partnership

This collaboration is poised to elevate the security standards of organizations across multiple industries, orchestrating a transformation in their overall security posture.

The strategic alliance between the Armis Centrix™ Platform and ServiceNow is dedicated to empowering customers with full-scale visibility, security, and management capabilities across diverse device ecosystems, encompassing IT, IoT, OT, and IoMT realms.

# Challenges

IT & security teams do not have enough resources to keep up with threats, gain visibility into vulnerable applications and prioritize alerts fast enough.

The number of targeted attacks continues to rise and security teams have become overwhelmed with alerts.

Ineffective use of data from insightful but disparate sources to effectively prioritize incident response efforts.

# At a Glance:

Armis Centrix™ and ServiceNow provide a unified asset management platform for managed, unmanaged, IoT, and manufacturing/OT devices in addition to IT.

The Armis Centrix™ platform ensures that ServiceNow remains consistently informed about the status of every device within your environment.

Armis Centrix™ continuously monitors devices for additional information it can use to true-up details in your ServiceNow CMDB, giving you a complete and up-to-date asset inventory whenever you need it.

# The Partnership

Armis and ServiceNow have forged a strategic partnership aimed at empowering your organization with unparalleled insights into your asset inventory. This collaboration is enabling IT teams to achieve deep insights into their asset landscape, facilitating informed decision-making and strategic planning. In leveraging this partnership, you can optimize your investments in ServiceNow as CMDB, ensuring that resources are maximized and utilized efficiently.

Our joint efforts enable the seamless bridging of coverage gaps, unifying all assets under a single, cohesive framework. This unified approach not only enhances your business operations but also fortifies your security posture, providing comprehensive protection across your entire asset ecosystem.

# Partnership Feature Highlights:

- Complete non-intrusive discovery which works with all devices, managed and unmanaged, IT, OT/IoT, or IoMT.
- Aggregate and share relevant, contextual asset insights with full context.
- Armis ServiceGraph connector to create an up-to-date and accurate inventory of assets in ServiceNow CMDB.
- Prioritize vulnerability remediation based on business impact and ServiceNow Vulnerability Response.
- Full vulnerability life cycle management with automatic or manual ticket creation in ServiceNow.
- KPIs in ServiceNow with real-time, prioritized asset context powered by the Armis AI-driven Asset Intelligence Engine.
- Security Response to reduce mean-time-to-resolution (MTTR).
- Assist your zero trust validation. This framework ensures that all assets are continuously monitored.
- Automatically create ServiceNow incident response tickets based on abnormal and/or threat activity.
- Track and visualize progress with curated dashboards, reports, and ticket progress.

# How It Works

## Service Graph Connector for Armis

With Service Graph Connector you can identify and classify managed, unmanaged, OT, and IoT (in addition to IT) devices in real-time- in fact, Armis maps to many ServiceNow CI tables automatically. Continuous traffic inspection enables effortless tracking of device activity, keeping the CMDB current. Additionally, it reduces duplicate or outdated CMDB entries, optimizing asset management and operational efficiency.

## Vulnerability Response Integration with Armis

Certified for ServiceNow Operational Technology Vulnerability Response (OT VR) compatibility, the Armis Centrix™ platform enables real-time discovery across all device types, including OT, IoT, and unmanaged devices. It prioritizes vulnerabilities using the Vulnerability Prioritization and Remediation Risk Score and streamlines remediation efforts. Automated closure of vulnerabilities that are based on outdated threat intelligence or old logs. This integration is fully compatible with the Service Graph Connector for Armis, it supports both IT, medical and OT workflows.

## Armis Security Incident Identification & Response

Automatically identify and mitigate risks across all device types, including unmanaged, IT, IoT, OT/ Industrial Control Systems (ICS), and medical devices as they connect to your network. Armis provides additional contextual information about devices and events, enabling efficient threat remediation and incident updates through policy-based actions. Import Armis Alerts directly into ServiceNow as Security Incidents, streamlining incident management. Benefit from guided setup and integration dashboards for intuitive use and prioritization of security alerts.

## Armis Incident Integration

Effortlessly identify and address risks across all device types upon network connection, including unmanaged, IoT, OT/ICS, and medical devices. Armis enriches this process via its 4 billion strong asset intelligence engine. It provides comprehensive contextual information about devices and events, facilitating streamlined and informed decision-making. Harness the power of policy-based actions within Armis to efficiently remediate threats and update incidents, ensuring precision and operational efficiency.

## ServiceNow Asset Pull Integration

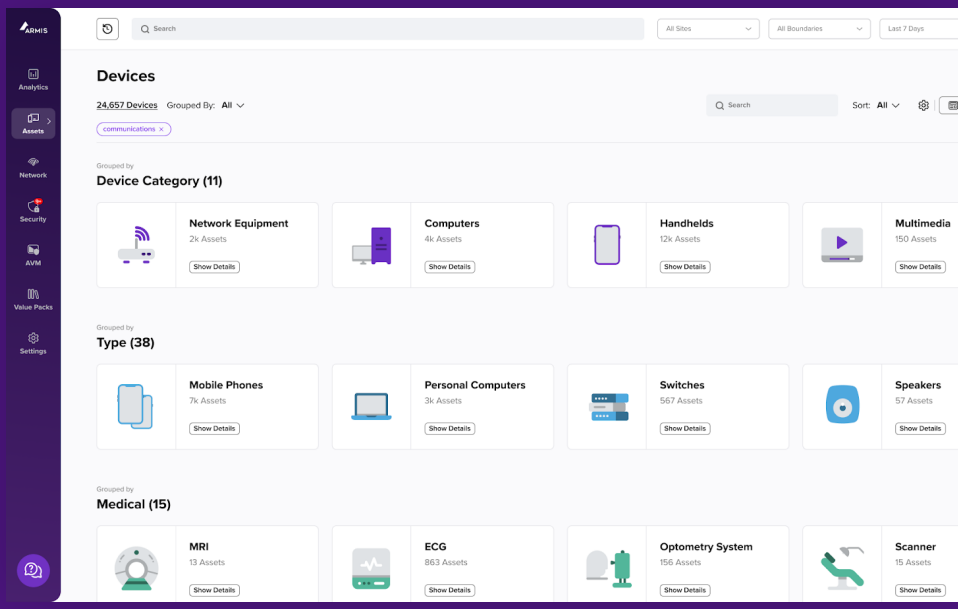
Pulls in assets from ServiceNow to correlate and aggregate assets for improved accuracy in both environments. Having a new data source using the ServiceNow CMDB as the source of the asset information also feeds the Armis Intelligence engine- growing that data set for improved contextual knowledge. This, in conjunction with our existing Service Graph Connector, gives Armis tremendous flexibility with how assets are managed and contextualized between both platforms.

## Business Application Dependency Mapping

This maps how business applications communicate and map to each other. This is relevant for understanding criticality and function to the business for Vulnerability Prioritization and Remediation.

# Use Cases:

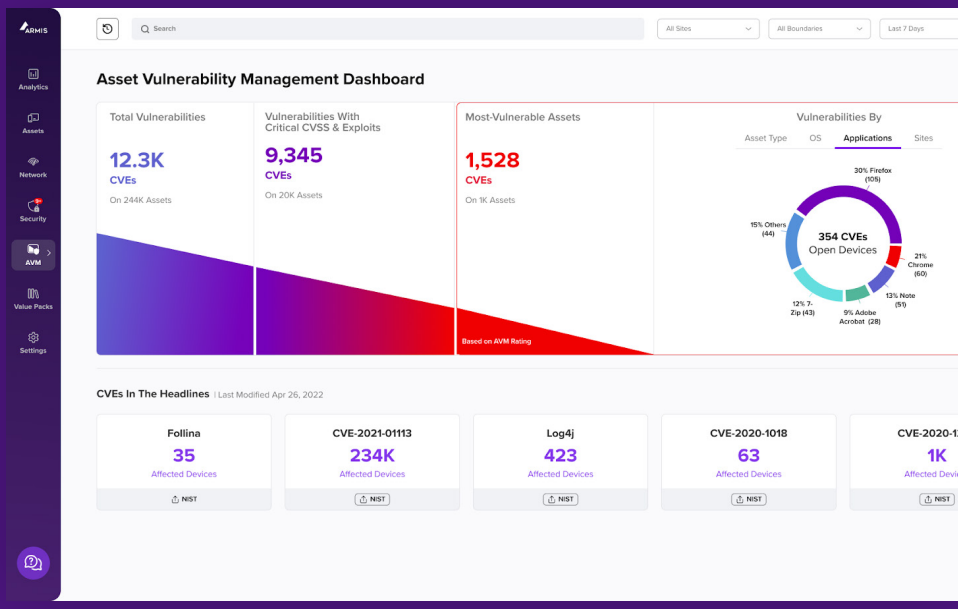
## Complete Visibility into all Assets




Armis Centrix™ delivers an extensive array of contextual intelligence, serving as the cornerstone for maintaining an up-to-date, precise, and all-encompassing asset inventory within the ServiceNow Configuration Management Database (CMDB). Through seamless integration, Armis Centrix™ continually enriches ServiceNow's CMDB with real-time insights, ensuring that every asset is meticulously documented and accurately represented. The ServiceNow Asset Pull Integration to bring ServiceNow assets in is important for bi-directional enrichment to ensure every asset is represented in both platforms. This dynamic synergy guarantees that organizations have a holistic understanding of their asset landscape, enabling informed decision-making, efficient resource allocation, and robust security governance. With Armis Centrix™, organizations can trust that their ServiceNow CMDB remains current, comprehensive, and primed for effective asset management and security operations.

## Prioritize Vulnerability Remediation and Improve MTTR

The integration of Armis Centrix™ and ServiceNow's Vulnerability Response Module streamlines remediation efforts by aligning asset criticality with vulnerability severity. Leveraging Armis Centrix™'s contextual intelligence, organizations can assess asset importance and potential security impact, while ServiceNow's platform offers centralized vulnerability lifecycle management.




This allows security teams to prioritize remediation based on critical assets and severity of vulnerabilities, ensuring efficient allocation of resources. With visibility into remediation progress, organizations can proactively address security risks, fortify resilience, and protect digital assets effectively.

## Data-driven Security Response

Maximize efficiency in incident response operations with the integration of ServiceNow Incident Response and the Armis AI-driven Asset Intelligence Engine. This joint solution enables organizations to expedite triage efforts by prioritizing critical alerts and enhancing investigations with contextual insights. Leveraging the comprehensive asset intelligence provided by Armis, security teams gain valuable context surrounding alerts, empowering them to make informed decisions swiftly. By focusing on critical alerts and leveraging contextual insights, organizations can accelerate incident investigations, minimize response times, and effectively mitigate security risks based on business impact.

# Centralize Visibility and Business Application Dependencies

The integration of ServiceNow's sophisticated business applications mapping capabilities with Armis Centrix™ enhances risk management and remediation prioritization processes. By leveraging ServiceNow's comprehensive understanding of business applications, Armis Centrix™ gains valuable insights into the criticality and dependencies of all assets within the organizational infrastructure. This enriched data enables more precise risk assessment and facilitates the prioritization of remediation efforts based on business impact. By aligning risk and remediation priorities with the strategic objectives of the organization, this integration empowers security teams to focus resources where they are most needed, effectively strengthening the overall security posture. With ServiceNow's deep business applications mapping capabilities complementing Armis Centrix™, organizations can proactively mitigate risks, optimize remediation strategies, and safeguard their digital assets with confidence.

# Bringing the Armis Difference to ServiceNow

## Comprehensive

Leverage a complete, unified inventory of every asset in the environment, including those that are outside your corporate network that go beyond IT such as OT and IoMT devices, to ensure awareness across the full asset attack surface.

## Complete

Only Armis knows the risk of every asset in your OT environment, allowing you to prioritize your mitigation efforts and focus on high stakes remediation tasks.

## Contextualized

Only Armis has a global Asset Intelligence Engine of over 4 billion devices and growing. The behavior of this unparalleled data set allows us to accurately define normal baseline behavior for assets in your ecosystem.

## Case Study:

"We have more centralized and consistent control in an environment that had no standardization whatsoever prior to Armis. Now we have a single asset repository and a single asset management solution for our entire manufacturing network, which before was duplicated 50 times," says Towers.

"We've been so successful in the plant environment that we will be implementing Armis on the enterprise side as well."

**Mike Towers**
Chief Security and Trust Officer
Takeda Pharmaceuticals

servicenow

## ServiceNow (NYSE: NOW) is improving enterprise operations across the globe.

Its cloud-based platform and solutions deliver digital workflows that create great experiences and unlock productivity for employees and the enterprise. Within ServiceNow Security Operations, ServiceNow offers two solutions: Security Incident Response and Vulnerability Response, designed to help security and IT teams to respond faster and more efficiently to incidents and vulnerabilities.

For more information, visit: www.servicenow.com

ARMIS

## Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

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 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