



PARTNER BRIEF

Armis + Superna Joint Solution Brief

General Overview

Enterprises today face an unprecedented challenge of securing the full spectrum of assets and access paths across IT, OT, IoT, and medical/critical infrastructure environments. Devices and users are no longer confined to traditional perimeters, and sensitive data is constantly accessed from a wide range of managed and unmanaged assets.

Armis Centrix™, the AI-powered Cyber Exposure Management Platform, provides real-time visibility and multidimensional risk intelligence across every connected asset in the enterprise. By integrating with Superna's Data Attack Surface Manager (DASM), organizations gain the ability to connect asset risk intelligence with data risk exposure, enabling policy-driven control of high-risk access attempts. Together, this joint solution transforms asset and data protection into a unified, business-aligned continuous threat exposure management (CTEM) strategy.

Key Challenges

- **Fragmented Visibility** - Traditional security tools often operate autonomously from one another without sharing insights. They focus on either devices or data, leaving critical blind spots in how assets are used to access high-value information.
- **Dynamic Threats** - Attackers exploit unmanaged devices, unpatched vulnerabilities, dormant permissions, and real-time data access paths to establish a foothold and then laterally progress through the digital landscape in order to exfiltrate valuable data.
- **Compliance Pressure** - Organizations must prove not just device compliance, but demonstrate governance risk and compliance across the entire landscape.
- **Reactive Security Models** - Device vulnerability scores alone don't capture the full picture of prioritized risk. What matters is how vulnerabilities, behaviors, and data sensitivity intersect and how organizations address unacceptable cyber exposure.

Enterprises need an approach that unifies device intelligence, user behavior, and data risk into a single exposure management framework. This is accomplished with the Armis - Superna joint solution that addresses both device and data risk together.

The Joint Solution

The integration of Armis Centrix™ and Superna DASM delivers end-to-end visibility and risk management by combining the industry's most comprehensive asset intelligence with advanced data attack surface management.

Armis Centrix™ discovers and classifies every connected asset, managed, unmanaged, across IT, OT, IoT, and medical devices, while continuously analyzing vulnerabilities, behaviors, and risk posture in real time.

Superna DASM ingests this intelligence to correlate device risk with live data access patterns, creating a Data Risk Score that reflects the true risk of specific users and hosts interacting with sensitive information.

Bi-directional integration ensures that DASM's data-centric insights flow back into Armis Centrix™, where organizations can apply custom risk factor policies, prioritize remediation of both the data as well as assets, and activate compensating controls through the Armis platform.

How It Works



Discovery & Classification - Armis Centrix™ continuously discovers every asset in the environment and enriches each with contextual intelligence, including vulnerabilities, behaviors, and communication patterns.



Data Access Monitoring - Superna DASM monitors how users and devices interact with SMB shares, NFS exports, and other centralized repositories, mapping real-world data usage against sensitive data locations.



Risk Correlation - Armis device risk scores are integrated into DASM's AI-driven data risk model. This creates a multidimensional risk picture that accounts for asset security posture, user activity, and data sensitivity.



Policy Enforcement - When risky access attempts are detected, DASM enforces isolation policies at the data layer. Armis Centrix™ updates risk posture and automates remediation workflows through integrations with ITSM, SIEM, and SOAR tools.



Continuous Feedback Loop - Data Risk Scores are synced back into Armis Centrix™, enabling recalculated device risk scoring and prioritized exposure management decisions across the enterprise.

Benefits and Outcomes

Unified Asset & Data Risk Management - Gain end-to-end visibility into how device security posture directly impacts data exposure.

Smarter Risk Prioritization - Focus remediation efforts on the assets and data access patterns that present the highest real-world risk to the business.

Preemptive Exposure Management - Detect and isolate risky access attempts before data exfiltration occurs, reducing dwell time and stopping breaches before damage is inflicted.

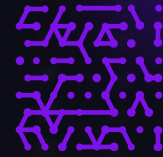
Operationalized Zero Trust - Enforce least-privilege access policies at the device, operational and file system layer based on real-world activity, not static permissions.

Compliance & Audit Readiness - Deliver auditable insights and drilldowns into data access and device behavior, satisfying regulatory requirements with contextual evidence.

Accelerated MTTR - Improve mean time to detect and respond by combining Armis's real-time asset intelligence with Superna's automated policy enforcement.

Business-Aligned Security - Align security operations with the protection of business-critical data while leveraging Armis Centrix™ to manage the broader attack surface across the digital landscape.

With Armis Centrix™ as the intelligence engine and Superna DASM as the enforcement layer for data risk, organizations can close the gap between asset risk and data exposure, creating a proactive, automated, and measurable cyber exposure management strategy.



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