Data Attack Surface Manager

Continuous Data Risk Evaluation & Remediation Solution

Solution Brief

- Bi-directional integration of data risk context into Armis platform and Device Risk Scores influence the Data Attack surface risk scoring
- Real-time discovery of data access risk across managed and unmanaged assets
- Policy-based data isolation of high-risk access attempts
- Supports discovery of data access attempts from IoT and OT devices
- Unified view of asset risk based on user behavior and data access context
- Complete attack surface assessment exposure of assets and users

Solution Overview

Superna's Data Attack Surface Manager (DASM) integrates with Armis Centrix to provide real-time visibility, risk scoring, and policy-based enforcement for user and host interactions with sensitive data. Unlike traditional device-centric approaches, this integration focuses on the data itself as the core asset, monitoring which devices users are leveraging to access it, and applying policy-based isolation when risky access patterns are detected.

In the modern enterprise, risk management is not about device risk scores. It's about understanding how devices are used by users to access centralized data repositories. With data no longer stored locally but aggregated into high-value storage environments, the focus must shift to data protection as the primary objective of cyber risk programs.

Enterprise risk and remediation strategies must evolve to prioritize actions based on data risk, not just device vulnerability scores. True business risk visibility begins at the data layer, where sensitive information is accessed, classified, and potentially exposed. The integration ensures that asset remediation is aligned with data sensitivity and usage context, delivering a smarter, business-aligned approach to security.

Superna DASM further enhances this capability by incorporating Armis-provided asset risk scores directly into its data risk AI model. Armis computes these scores using comprehensive context derived from network activity, endpoint telemetry, and assetto-asset data flows, enriching DASM's risk analysis. This allows organizations to enforce data protection policies grounded in multidimensional risk intelligence, prioritizing enforcement based on a full-spectrum view of user behavior, data interaction, and enterprise risk posture. This integration enables continuous detection and control of the data attack surface, using Armis to enrich asset intelligence and Superna to act on risky behaviors with immediate policy enforcement.

Business Challenges

Organizations face increasing difficulty securing unstructured data environments due to:

- No Data context applied to risk or exposure assessments of assets, leading to poor security decisions
- Blind spots from managed, unmanaged, or IoT/OT devices accessing sensitive data
- Inability to correlate data access with user identity and behavior
- All data is treated as the same risk, but Superna classifies data and shows where your highest data risk lies
- Lack of visibility into the data attack surface
- No real-time compensating control to isolate or block risky data access attempts
- Gaps in understanding the devices used to access centralized data
- Incomplete risk analysis due to overreliance on devicecentric security models without data context
- Difficulty prioritizing remediation across enterprise assets due to lack of data-layer visibility

Key Features

- **Asset Discovery and Visibility**: Superna DASM continuously discovers and maps all users and devices interacting with enterprise data, including managed, unmanaged, and shadow IT assets. It provides a unified view of the data access landscape and uncovers previously invisible assets that pose risk at the data layer.
- **Cyber Threat Detection and Response**: Superna DASM uses AI to detect abnormal access patterns and behaviors in real time, identifying high-risk users and hosts interacting with sensitive data. This enables rapid response through policy-based isolation and alerting mechanisms that address data-layer threats.
- **Vulnerability Management**: By scoring access patterns and enforcing isolation policies, DASM prioritizes remediation efforts for users and assets based on their interaction with critical data. This enables organizations to proactively reduce risk exposure tied to data access behaviors.
- **Zero Trust Security**: DASM enforces a zero trust model at the data layer by validating and monitoring every user and device attempting to access sensitive data. It ensures least privilege access is factored into risk assessments and enforces policy controls to dynamically protect data based on risk and content classification.
- **Operational Technology (OT) Security**: While Armis specializes in OT environments, DASM complements this by detecting and monitoring data access attempts from OT and IoT devices. It brings data visibility into environments where traditional endpoint monitoring is not possible.
- **Cyber Exposure Management**: DASM provides real-time insight into the true exposure of business-critical data by correlating access with user identity, asset risk, and data classification. It enables organizations to quantify and reduce their data-centric risk posture continuously.
- **Integration and Automation**: Superna DASM integrates with Armis and other ITSM/SIEM platforms to automate threat response and enforcement actions. It ensures that insights from data-layer monitoring can trigger policy controls, ticket creation, and real-time isolation workflows.

Technology Components

- Superna Data Attack Surface Manager (DASM) & Data Security Edition
- Armis Centrix Platform
- Enterprise Storage Systems (Dell, NetApp, Vast Data, Qumulo, Hitachi, Microsoft, PureStorage)
- *Optional: ITSM and SIEM integrations for automated response*

Preemptive Automated Exposure Management

SMB/NFS PII Exposure Detection

- **Pinpoint Risk Hotspots**: Discover where sensitive data is most vulnerable by mapping actual user interactions with PII across SMB shares and NFS exports. Prioritize protection efforts based on real usage, not assumptions.
- **Quantify Exfiltration Risk in Real Terms**: Move beyond generic risk scoring by measuring the true threat: who accessed what, when, and how much sensitive data was involved. Turn unstructured data sprawl into a targeted risk profile.
- **Enable Targeted Remediation**: Focus remediation efforts on shares or exports with high PII concentration and high user interaction, reducing false positives and maximizing the impact of security operations.
- **Bridge Data Security with Compliance Monitoring**: Deliver auditable insights into how and where sensitive data is exposed—empowering compliance teams with contextual, actionable evidence tied to user behavior.

Permission vs. Usage Over-Exposure Analysis

- **Shrink the Data Attack Surface with Precision**: Identify users who have access to data they don't use. Reduce risk exposure from dormant or excessive permissions and enforce least-privilege access policies intelligently.
- **Operationalize Zero Trust at the File System Layer**: Go beyond static access control lists—use real-world activity to justify or revoke access. DASM aligns with Zero Trust principles by validating actual need-to-know.
- **Turn Audit Logs into Proactive Access Governance**: Convert audit trails into actionable access intelligence. Automate the detection of access drift and help teams surgically close privilege gaps before they're exploited.
- **Drive Access Reviews with Usage Context**: Equip IT and security teams with usage-based insights that make access reviews faster, smarter, and more defensible—especially in regulated environments.

How It Works

- **Data Access Discovery**: DASM continuously monitors data access and host-user interactions.
- **Risk Scoring**: AI-driven models analyze vulnerability data and access patterns.
- **Threat Detection & Prioritization**: High-risk users and hosts are identified in real-time by DASM. The Risk score of hosts in Armis Centrix are leveraged by DASM as input to the Data Risk Score. This integrates Centix multidimensional risk intelligence.
- **Armis Centrix Integration**: The Data Risk Score calculated by DASM is synced into Centrix using a custom asset property allowing the Risk score to be re-calculated within Armis using Custom Risk Factor Policies.
- **Compensating Controls Activation (Optional)**: If a host or user is deemed high-risk, access to sensitive data is blocked until remediation is complete. This applies a real-time data blocking permission to the underlying storage.
- **Automated Remediation & Reporting (Optional)**: ITSM integration creates tickets regarding offense compensating controls that have been actively applied. Webhooks allow easier integration into almost any SIEM/SOAR or ITSM platform. Leveraging Superna's 3rd party integration library.
- **Continuous Monitoring & Policy Enforcement**: Security teams receive updates on autonomous mitigation progress.

Why Superna DASM

- Enables data-driven risk prioritization focused on user/device access to sensitive information
- Improves MTTD and MTTR by monitoring live data interactions
- Reduces overall attack surface size by proactively isolating risky data access points
- Hardens critical user accounts and host assets to prevent data breaches before they occur
- Supports compliance mandates with full visibility into access to classified data
- Continuously assesses risk in real time as data is accessed, accelerating exposure detection and response
- Reveals the true attack surface to sensitive data, enabling security teams to respond with precision
- Maps data risk directly to the users and hosts responsible for that access, improving remediation accuracy
- Leverages Armis risk scoring across network, endpoint, and traffic telemetry to enhance data risk decisions
- Enables remediation and hardening actions across network, compute, and application layers, all prioritized by their relationship to business-critical data

Get Started with Superna

Schedule a Demo | Speak with an Expert