

Data Attack Surface Manager

Continuous Data Risk Evaluation & Remediation Solution

Product Description

Superna's Data Attack Surface Manager (DASM) solution integrates AI-powered analytics, dynamic access enforcement, and real-time data exposure intelligence. It is purpose-built to extend traditional vulnerability scanning tools by managing the full lifecycle of vulnerability detection, prioritization, and remediation — with a strong focus on securing unstructured data and the data attack surface.

Business Challenges

Organizations struggle with traditional vulnerability management solutions that fail to prioritize data risks effectively, including:

- Inaccurate vulnerability scoring, ignoring user access patterns, data classification and data protection
- 50% of the attack surface missed by not considering user identities
- Reactive response over proactive risk management
- Blind spots due to lack of real-time attack surface discovery
- Inability to actively enforce real-time mitigation strategies or apply compensating controls to limit exposure
- Lack of Zero Day vulnerability protection
- Missing a data-centric view of assets and risks

Solution Overview

Superna Data Attack Surface Management transforms traditional vulnerability management by layering data-centric AI prioritization on top of your existing VM scanning tools. This integrated approach turns standard vulnerability scans into a complete Exposure Assessment platform—one that prioritizes remediation based on the actual data risk, not just device-centric device-centric CVSS scores.

By correlating data access behaviors, user identities, host-level risk scores, and sensitive data classification, organizations gain up to 4x improvement in remediation accuracy and precision. Security teams can confidently prioritize and automate the mitigation of high-risk assets and users, ensuring that the most critical exposures—those affecting sensitive or regulated data—are addressed first.

This solution enables a proactive, data-aware defense posture that aligns remediation efforts with business impact and regulatory risk.

Value

- ✓ Prioritize remediation based on actual data risk rather than device risk scores, reducing time and resources spent
- ✓ Identify high-risk hosts and users in real-time to gain an advantage over adversaries
- ✓ Implement automated compensating controls to block data access from vulnerable assets
- ✓ Measure risk with deep understanding of the classification risk within the data itself
- ✓ Improve mean time to detect (MTTD) and mean time to respond (MTTR) for critical vulnerabilities
- ✓ Enable Active Defense to protect data from zero-day vulnerabilities
- ✓ Gain asset visibility to regulatory data risk and exposure

Key Features

- **Data Attack Surface Visibility:** Identifies high-risk users and hosts with privileged access to sensitive data. Provides real-time insight into which users and devices pose the greatest threat based on behavior and access to sensitive files.
- **Data-Centric Risk-Based Prioritization:** Uses AI to score hosts and users based on data exposure risk:
 - User access behavior patterns and permissions
 - Host risk assessment based on data exposure
 - PII, PHI & Financial Data Classification of hosts and users accessing high risk data
- **Automated Remediation:** Blocks data access from high-risk assets until vulnerabilities are mitigated.
- **Dynamic Data Shield (DDS):** Enforces security policies to prevent untrusted hosts from accessing data.
- **Integration with ITSM & SIEM:** Automates security incident creation and remediation tracking.
- **Risk Reduction Reporting for Data-Linked Hosts:** Generates reports that track vulnerability reduction over time specifically for hosts that previously accessed sensitive data — enabling measurable improvement tracking.
- **Visibility into the Data Attack Surface in InsightVM:** Enables native visualization of data-centric risk exposure directly within Rapid7 InsightVM via Live Dashboards and Dynamic Asset Groups.

Technology Components

- Rapid7 InsightVM
- Superna Data Attack Surface Management (DASM) & Data Security Edition
- Endpoint protection integrations (Optional)
- ITSM integrations (Optional)

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.

Content Integrity Assurance - Beyond Classification

- **Detect Stealthy Tampering:** Identify encryption edits in documents, logs, designed to evade traditional detection.
- **Uncover Obfuscated Payloads:** Expose malicious content that's encrypted or disguised to appear legitimate.
- **Catch Semantic Drift:** Reveal subtle meaning changes in critical files that classification tools overlook.
- **Validate Integrity at Scale:** Confirm content coherence and detect malicious or suspicious edits to business data.
- **Stop AI-Era Threats:** Detect GenAI malicious content manipulations that change your contents meaning.
- **Protect Critical Data:** Ensure business-essential information remains trustworthy, safeguarding customers and compliance.
- **AI training data integrity:** AI data pipelines need high quality data, this capability identifies low quality training for models or RAG use cases.

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 and synced into a Dynamic Asset Group in InsightVM.
- **Rapid7 InsightVM integration:** Creates a Dynamic Asset Group listing all the IP addresses of Data Attack Surface hosts.
- **Compensating Controls Activation (Optional):** Blocks access to sensitive data for high-risk users until remediation.
- **Automated Remediation & Reporting (Optional):** ITSM integration creates remediation tickets automatically.
- **Continuous Monitoring & Policy Enforcement:** Security teams receive updates on mitigation progress.

Key Capabilities

- Integration with InsightVM resolving prioritized vulnerabilities.
- Custom Live Dashboards for data-linked host monitoring.
- Real Risk score integration with data-layer inputs.
- Real-time asset updates using Dynamic Sites.
- AI-powered data-centric risk scoring for hosts and users.
- Real-time asset and user risk profiling.
- Enforcement of automated compensating controls.
- PII/PHI/financial data classification for enhanced context.
- Continuous monitoring and policy enforcement lifecycle.

Get Started with Superna



Schedule a Demo |  Speak with an Expert