

Vulnerability Management (GRC)

Manage vulnerabilities based on business risk with asset context, real-time visibility, and structured remediation workflows across systems and applications.

SKU	GRC - CYB - VUL
Solution area	GRC & Resilience
Works with	Enterprise Assets & Structure, Cyber Threat Management, Enterprise Risk Management (ERM), Compliance Assessments & Testing, Issues Management, Incident Management
Updated	Sep 26, 2026
Datasheet	v1.0

What it is

Vulnerability Management is the process of identifying, assessing, prioritizing, and remediating security weaknesses across systems and applications. A risk-based approach enables organizations to focus on vulnerabilities that pose the greatest threat to business operations, rather than treating all findings equally.

SmartSuite’s Vulnerability Management software provides a structured, risk-based approach to identifying, prioritizing, and managing vulnerabilities across your organization. Instead of treating vulnerabilities as isolated technical findings, SmartSuite connects them to assets, systems, and business context—enabling organizations to focus on what matters most.

Teams can ingest vulnerability data from scanners and security tools, enrich it with asset and ownership data, and prioritize remediation based on risk, exposure, and business impact. This ensures that critical vulnerabilities are addressed first, while reducing noise from low-impact findings.

Core capabilities

Vulnerability Data Ingestion

Import vulnerability data from scanners and security tools into a centralized system of record.

Risk-Based Prioritization

Prioritize vulnerabilities based on asset criticality, exposure, and business impact.

Asset & System Context Integration

Link vulnerabilities to assets, applications, and business units for full visibility.

Remediation Workflow Management

Assign ownership, track remediation progress, and enforce accountability across teams.

Exposure & Risk Dashboards

Visualize vulnerability trends, high-risk assets, and remediation performance in real time.

Threat Correlation

Align vulnerabilities with active threats to identify and prioritize critical risks.

Compliance & Control Alignment

Map vulnerabilities to control requirements and compliance frameworks.

Issues & Remediation Tracking

Track unresolved vulnerabilities as issues with full lifecycle management.

Role-Based Access Control

Ensure secure access to vulnerability data across security, risk, and IT teams.

The Vulnerability Management Lifecycle

Step 1 Identify Vulnerabilities Ingest vulnerability data from scanners and external sources.	Step 2 Enrich with Asset Context Link vulnerabilities to systems, applications, and ownership.	Step 3 Assess & Prioritize Risk Evaluate severity based on business impact and exposure.	Step 4 Assign & Remediate Track remediation activities and enforce accountability.	Step 5 Monitor & Report Continuously monitor exposure and report on risk reduction.
---	--	--	--	---

Who it is for

Chief Information Security Officer (CISO) Oversees vulnerability exposure and aligns remediation with security strategy.	Risk Manager Integrates vulnerabilities into enterprise risk assessments and reporting.	Security Operations Lead Monitors vulnerabilities and coordinates remediation activities.
IT Operations Lead Executes remediation and manages system-level vulnerabilities.	Compliance Manager Ensures vulnerabilities are addressed in alignment with regulatory requirements.	Executive / Board Member Monitors overall vulnerability exposure and risk trends.

Works with

Enterprise Assets & Structure Provides asset context, ownership, and system relationships for accurate prioritization.	Cyber Threat Management Aligns vulnerabilities with threat intelligence and active risk indicators.
Enterprise Risk Management (ERM) Incorporates vulnerability exposure into enterprise risk reporting.	Compliance Assessments & Testing Links vulnerabilities to security incidents and response activities.
Issues Management Tracks vulnerabilities as actionable remediation items.	Incident Management Links vulnerabilities to security incidents and response activities.

Built differently. Vulnerability Management (GRC) runs on the same relational platform as every other SmartSuite product, so its records link to the risks, controls, issues and evidence they affect, and every report reflects the current state rather than a copy.

See it working with your data

Ask your SmartSuite account team for a demo of Vulnerability Management (GRC) configured for your organization, or read the full product entry at smartsuite.com/products/vulnerability-management-grc.

Schedule a demo