

SmartSuite

GRC & Resilience > Cyber & IT Risk · Datasheet

Cyber Threat Management

Identify and respond to cyber threats with real-time visibility, structured workflows, and integrated risk and incident management.

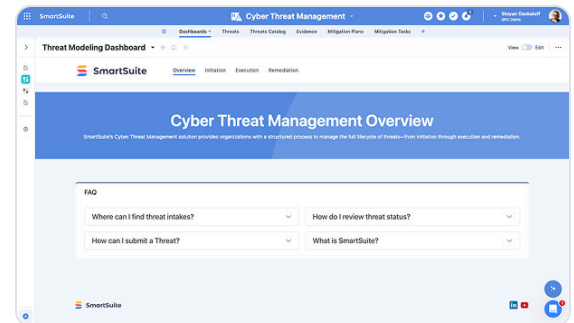
SKU	GRC-CYB-THR
Solution area	GRC & Resilience
Works with	Incident Management, Enterprise Risk Management (ERM), Compliance Assessments & Testing, Third Party Risk, Issues Management, Operational Resilience
Updated	Sep 26, 2026
Datasheet	v1.0

What it is

Cyber Threat Management is the process of identifying, analyzing, and responding to cybersecurity threats and vulnerabilities. It enables organizations to monitor threat activity, prioritize response efforts, and reduce risk exposure across systems and infrastructure.

Cyber Threat Management is the process of identifying, analyzing, and responding to cybersecurity threats that could impact an organization's systems, data, and operations. SmartSuite's Cyber Threat Management software provides a structured, scalable system to manage threats across your enterprise — enabling proactive risk reduction and coordinated response.

SmartSuite enables organizations to capture threat intelligence, assess threat severity, and manage response workflows across security and risk teams. With a centralized system of record, teams can track threat indicators, vulnerabilities, and response actions in a way that is repeatable, auditable, and defensible.



Cyber Threat Management in SmartSuite.

Core capabilities

Threat Intelligence Management

Capture and manage threat intelligence from internal and external sources to identify emerging risks.

Threat Classification & Prioritization

Assess threats based on severity, likelihood, and potential business impact to prioritize response efforts.

Vulnerability Tracking

Track vulnerabilities across systems, applications, and infrastructure with clear ownership and status.

Threat Response Workflows

Define and manage response processes, including investigation, containment, and mitigation actions.

Risk Integration & Scoring

Align threats with enterprise risk scoring and reporting for better visibility and prioritization.

Dashboards & Threat Analytics

Visualize threat trends, exposure, and response performance through real-time dashboards.

Automated Alerts & Notifications

Trigger alerts and notifications for high-priority threats and response activities.

Cross-Product Integration

Link threats to incidents, risks, issues, controls, and vendors for full lifecycle visibility.

Role-Based Access Control

Ensure secure access to threat data and workflows across security and risk teams.

The Threat Management Lifecycle

Step 1 Identify Threats Capture threat intelligence and identify potential vulnerabilities and risks.	Step 2 Assess & Prioritize Evaluate threat severity, likelihood, and potential impact on the organization.	Step 3 Respond & Mitigate Execute response workflows to contain and mitigate threats.	Step 4 Monitor & Track Track threat status, response progress, and evolving risk exposure.	Step 5 Analyze & Improve Perform post-event analysis to strengthen controls and reduce future risk.
---	--	---	--	---

Who it is for

Chief Information Security Officer (CISO)

Oversees cybersecurity strategy and threat management across the organization.

Security Operations Center (SOC) Manager

Monitors threats, investigates incidents, and executes response actions.

Compliance & Risk Manager

Aligns cyber threats with enterprise risk assessments and mitigation strategies.

Compliance Manager

Ensures cybersecurity practices align with regulatory requirements and standards.

IT Operations Lead

Manages system vulnerabilities and ensures infrastructure resilience.

Executive / Board Member

Monitors cyber risk exposure and security posture through dashboards.

Works with

Incident Management

Security incidents are tracked and resolved through structured incident response workflows.

Enterprise Risk Management (ERM)

Cyber threats impact enterprise risk exposure and reporting.

Compliance Assessments & Testing

Security controls are validated through compliance testing and audits.

Third Party Risk

Vendor vulnerabilities and threats are incorporated into third-party risk assessments.

Issues Management

Threat-related findings and vulnerabilities are tracked through remediation workflows.

Operational Resilience

Threat impacts inform resilience planning and continuity strategies.

Built differently. Cyber Threat Management 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 Cyber Threat Management configured for your organization, or read the full product entry at smartsuite.com/products/cyber-threat-management.

[Schedule a demo](#)