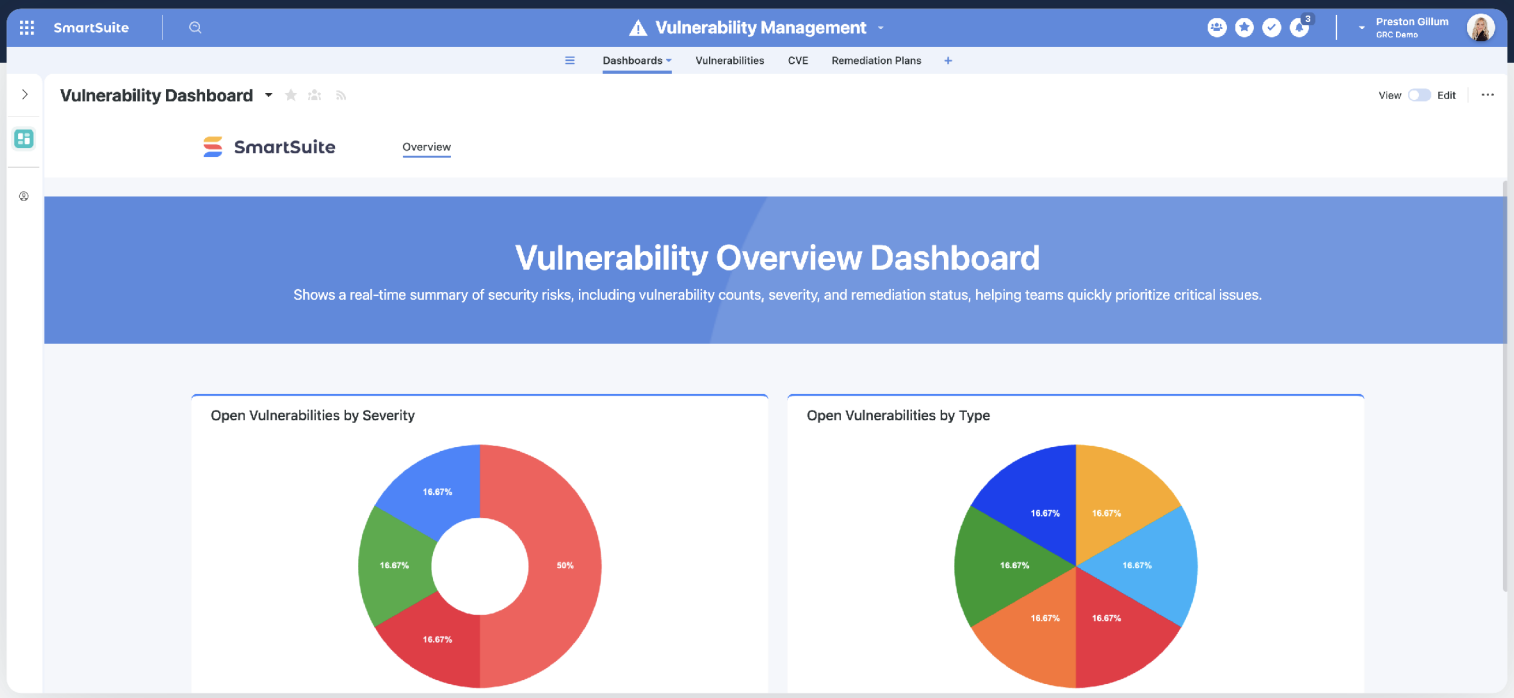
DATASHEET

Vulnerability Management

Centralize CVE intake, prioritize with CVSS and EPSS, track remediation SLAs, and connect every finding to the assets, vendors, and risks it affects — on one platform built for security teams that need to fix what matters first.



From scattered scan output to risk-prioritized remediation

Most security teams drown in scanner output — thousands of findings, no agreed prioritization, and remediation that lags scanning by months. SmartSuite operationalizes vulnerability management as a connected program: every CVE, every affected asset, every remediation plan, and every SLA lives in one governed system, with risk-based prioritization layered on top of raw severity. **Every vulnerability is scored. Every remediation has an owner. Every SLA breach is visible.** The result is a vulnerability program defensible for auditors, operational for the security team, and trusted by the CISO — fewer findings sitting open past their remediation target, and a clear story for board reporting.

Capabilities built for risk-based vulnerability management

Central CVE & vulnerability repository

Every vulnerability lives as a structured record with Vuln ID, multi-CVE references, CVSS score, type (SQL Injection, XSS, RCE, DoS, Broken Auth, MitM), severity, discovery date, and remediation plan. Findings from scanners, manual review, and external intel all flow into one governed inventory.

Multi-factor risk prioritization

The Vulnerability Prioritization Matrix combines Severity × Exploitability × Exposure × Asset Criticality into a defensible Risk Score and Priority tier. SLAs follow tier: Critical 7d, High 15d, Medium 30d, Low 60d — with SLA Breach flags and Trend indicators.

NVD, CISA KEV & EPSS enrichment

Every CVE enriches automatically against three authoritative sources: NVD (CVSS v3.1 base score, attack vector, CWE), CISA Known Exploited Vulnerabilities (required action and federal due date), and EPSS (30-day exploit probability). Known-exploited findings surface before CVSS-only triage would catch them.

Remediation plans & closed-loop tracking

Each vulnerability links to a Remediation Plan with owner, due date, patch reference, and evidence upload. Status moves through Open → In Progress → Closed with exception handling for risk-accepted items. Severity and Type dashboards refresh continuously.

Vulnerability visibility at every level

Security analyst

A personalized queue surfaces only the findings assigned to them — CVE, CVSS, EPSS probability, affected assets, and SLA countdown. Drill from a finding into the linked asset, remediation plan, and prior history in two clicks.

IT operations & remediation owner

An action-focused view shows only findings requiring their patch or configuration work, with context already pulled in: required action from CISA KEV, vendor patch references, and evidence requirements. Status updates flow back to the security team automatically.

CISO & security leadership

The Vulnerability Overview Dashboard rolls up Open Vulnerabilities by Severity, by Type, SLA breach counts, and trend over time. Board reports refresh continuously against CISA KEV alignment and remediation SLA performance — no manual rebuilds.

Built differently. SmartSuite is the vulnerability platform where CVEs, affected applications, IT assets, vendors, remediation plans, controls, and the enterprise risk register live on the same governed graph — so every finding ties to the asset that's exposed, every remediation has an owner with a deadline, and every dashboard reflects current posture, not last week's scan dump.

Connected to the rest of your GRC program

- **Business Structure & Hierarchy**
  Vulnerabilities link to Applications, IT Assets, and Business Units so exposure reflects the actual operating model and asset criticality
- **Cyber Threat Management**
  Active threats and known exploited CVEs trigger reassessment of related vulnerabilities and accelerate remediation priority
- **Issues Management**
  Overdue remediation, accepted exceptions, and SLA breaches flow into closed-loop issues with owners and review cadence
- **Enterprise Risk Management**
  Aggregate vulnerability exposure rolls up to the enterprise risk register; control deficiencies feed cyber risk reporting
- **Third-Party Risk Management**
  Vendor-introduced vulnerabilities tie to the vendor record; supply-chain CVEs surface as part of vendor risk reviews
- **Compliance Assessments & Testing**
  Vulnerability evidence and remediation history feed audit and control assessments without duplicate collection

Built for everyone with a stake in vulnerability management

Chief Information Security Officer
Oversee enterprise vulnerability posture, SLA performance, and CISA KEV alignment — board-ready dashboards in one click.

Security Lead & Program Manager
Coordinate triage, prioritization, scanning integrations, and remediation cycles across security and IT teams.

Security Analyst
Log vulnerabilities, perform triage, assign actions, validate CVE enrichment, and drive findings to closure.

IT Operations & Patch Owners
Apply patches, configuration changes, and compensating controls; upload evidence and update remediation status.

Application & Asset Owners
Validate findings on their systems, approve remediation windows, and document exceptions when patches aren't feasible.

Risk & Compliance Teams
Pull vulnerability evidence for audit and regulator response; track risk acceptance decisions and exception expirations.

Fix what matters first — with the data to prove it

A complete GRC suite that connects vulnerability management with risk, threats, vendors, and audit — on one AI-native Work OS, enriched by NVD, CISA KEV, and EPSS.

NVD · CISA KEV · EPSS · CVSS v3.1 · CWE

Learn more at **smartsuite.com/products/vulnerability-management** · Contact your SmartSuite representative to schedule a demo