PRODUCT SOLUTION

DEFENSESTORM
THE BEST OFFENSE

Vulnerability Management Integrated with GRID Active

Platform-integrated vulnerability scanning that turns findings into governance evidence, risk scores, and examiner-ready proof, all inside GRID Active.

POWERED BY CODA INTELLIGENCE (A PDQ COMPANY)

THE CHALLENGE

Vulnerability Data That Lives in a Silo Helps No One at Exam Time

Every financial institution runs vulnerability scans. The question is what happens next. For most FIs, scan results sit in a standalone tool, disconnected from governance workflows, risk assessments, and the evidence trail examiners expect. When exam season arrives, someone exports a CSV, reformats it in a spreadsheet, and manually maps findings to controls.

The real gap is not scanning. It is connecting scan data to action, remediation tracking, and proof. Without that connection, vulnerabilities pile up, exceptions go untracked, and examiners see gaps between what your program claims and what the evidence shows.

THE SOLUTION

Vulnerability Management That Lives Inside Your Cyber Risk Platform

DefenseStorm Vulnerability Management, powered by CODA Intelligence, brings scanning data directly into GRID Active, the same platform where your institution manages detection, governance, risk, and compliance. Vulnerabilities are not just discovered. They are tracked as tasks, mapped to controls, scored against NIST 800-53, and documented as evidence for examiners.

With flexible deployment and collaborative management by DefenseStorm, your team gets expert configuration, tuning, and ongoing support, not just a login.

FROM SCAN TO EVIDENCE

How It Works Inside GRID Active

Vulnerability data flows directly into GRID Active, connecting scanning activity to governance, risk, and compliance workflows in four steps.

Deploy & Scan

DefenseStorm configures internal scanners, external cloud scanners, and endpoint agents across Windows, Mac, and Linux. Coda scans continuously and scores devices against NIST 800-53.

Track & Remediate

Findings flow into GRID Active as tasks, mapped to controls and governance frameworks. Your team tracks remediation, manages exceptions, and documents progress inside the platform.

Report & Prove

Governance reviews pull directly from scan data. Visualizations, dashboards, and reports are generated inside GRID Active, giving examiners the continuous evidence they expect.

WHAT YOU GET

Scanning, Scoring, and Evidence in One Platform

Full-Environment Scanning & Compliance Scoring

Deploy internal scanners for private networks, external cloud scanners for public-facing assets, and agents for endpoint coverage across Windows, Mac, and Linux. Every device is scored against NIST 800-53 controls with a SCAP score, giving your team a defensible, framework-aligned view of security posture.

Key outcome: Complete coverage with compliance scoring on every device scanned.

Closed-Loop Remediation & Task Tracking

Vulnerabilities become tasks inside GRID Active, mapped to your controls and governance frameworks. Remediation is documented, exceptions are tracked, and the loop closes with evidence, not assumptions. Contextual risk scoring prioritizes what matters most to your institution.

Key outcome: Every finding tracked from discovery through remediation with full evidence trail.

Network Edge Testing & Endpoint Verification

Go beyond patch-level checks with network edge scanning that validates firewall controls and static analysis that identifies configuration weaknesses. Automatically verify that endpoint protection is installed and up to date, closing a common examiner question before it is asked.

Key outcome: Deeper security validation that satisfies examiner scrutiny.

VM Data That Strengthens Every Part of Your Program

Because Coda VM data lives inside GRID Active, it strengthens capabilities you already use:

Governance & Monitoring
Schedule reviews of vulnerability data as evidence mapped to FFIEC, NIST, and CIS controls.

Cyber Risk & Compliance
Scan results feed directly into risk assessments with quantitative data for risk scoring.

MDR
Vulnerability context enriches threat detection; analysts see known vulnerabilities during triage.

Advanced Reporting
Build custom dashboards showing vulnerability trends, remediation progress, and posture over time.

Why VM Belongs Inside Your Cyber Risk Platform

Unified Data, Unified Evidence
Vulnerability data lives alongside threat detection, governance, and risk assessment data in GRID Active. No more exporting CSVs and manually mapping findings to controls.

Framework-Aligned from Day One
SCAP scoring against NIST 800-53 gives your institution a defensible compliance baseline. Mapped controls connect scanning activity to the frameworks examiners care about.

Collaboratively Managed by DefenseStorm
This is not a software license with a knowledge base. DefenseStorm manages configuration, tuning, scanner deployment, and ongoing support alongside your team.

Closed-Loop Remediation
Vulnerabilities become tasks. Tasks map to controls. Remediation is documented. Exceptions are tracked. The loop closes with evidence, not assumptions.

Full Environment Coverage
Agents for endpoints (Windows, Mac, Linux), internal scanners for private networks, external scanners for public-facing assets. One solution, complete visibility.

Built for How FIs Work

800-53 NIST compliance scoring on every device	**SCAP** Framework-aligned posture benchmarking	**10,000+** Banking-specific controls mapped (platform-wide)
200+ Banks and credit unions protected by DefenseStorm	**1** Platform for MDR + Governance + Risk + Compliance + VM	**3** Deployment options: agents, internal, and external scanners

Platform-wide stats reflect the full DefenseStorm customer base.

Turn vulnerability data into examiner-ready evidence. **DefenseStorm is the best offense.**
Connect vulnerability scanning to your governance program, risk assessments, and compliance reporting, all inside the platform you already use.

470-519-0020
info@defensestorm.com