The Risk-Based Vulnerability Management Buyers Guide

How Security Leaders Can Move Beyond CVSS Scores to Prioritize What Actually Matters

3%

Of vulnerabilities pose real exploitable risk

5 days

Average time-to-exploit for new vulnerabilities

18%

Of organizations use EPSS for prioritization

DEFECTDOJO

Unify
Connect
Secure

Contents

01 Executive Summary

The average enterprise security team faces a staggering volume of vulnerability findings. CVE issuance increased 20% year-over-year in 2025, and the average time-to-exploit for a new vulnerability has dropped to just five days. Yet research consistently shows that only about 3% of vulnerabilities represent real exploitable risk in any given environment. The challenge is no longer finding vulnerabilities—it is knowing which ones to fix first.

Traditional vulnerability management relies on CVSS severity scores to prioritize remediation. But CVSS measures theoretical severity, not real-world exploitability or business impact. The result: security teams waste cycles chasing “Critical” findings that pose no actual risk while genuinely dangerous vulnerabilities languish in the backlog.

Risk-Based Vulnerability Management (RBVM) solves this by combining vulnerability data with threat intelligence (KEV, EPSS), asset context (business criticality, internet exposure), and environmental factors (exploitability, reachability) to produce a prioritized remediation backlog ordered by actual risk to the organization. Gartner’s Continuous Threat Exposure Management (CTEM) framework positions RBVM as the prioritization and mobilization engine at the center of modern exposure management.

This guide gives security leaders a structured framework for evaluating RBVM solutions. It explains why CVSS alone fails, details the risk inputs that matter, covers the eight capabilities every RBVM platform must have, and provides a weighted evaluation scorecard. Throughout, we show how DefectDojo Pro’s risk-based prioritization engine—launched May 2025—addresses each requirement.

Key takeaway: Only 3% of vulnerabilities pose real risk, but most organizations lack the tooling to identify which 3%. DefectDojo Pro’s risk-based prioritization engine combines KEV, EPSS, exploitability, reachability, business impact, and compliance exposure to surface exactly those findings—so your team remediates what matters, not what’s loudest.

02 Why CVSS Alone Fails

CVSS (Common Vulnerability Scoring System) has been the industry standard for rating vulnerability severity since 2005. It provides a useful baseline, but it was never designed to be a prioritization tool. Here is why relying solely on CVSS leads to poor remediation outcomes:

CVSS measures theoretical severity, not actual risk

A CVSS 9.8 vulnerability in an air-gapped internal system with no sensitive data poses far less risk than a CVSS 7.2 vulnerability in an internet-facing payment service. CVSS cannot capture this difference because it does not consider your specific environment.

CVSS does not account for active exploitation

CVSS scores are static—they do not change when a vulnerability is actively exploited in the wild. A CVSS 6.5 vulnerability with a public exploit being used by ransomware groups is far more urgent than a CVSS 9.0 vulnerability with no known exploit. RBVM incorporates KEV and EPSS data to capture this dynamic.

CVSS creates an overwhelming volume of "Critical" findings

When every scanner flags thousands of Critical and High findings, everything becomes a priority—which means nothing is. Security teams suffer alert fatigue and resort to arbitrary selection or first-come-first-served remediation, which research shows is the least effective approach.

CVSS ignores business context entirely

A vulnerability in a revenue-generating production application has fundamentally different risk implications than the same vulnerability in a development sandbox. RBVM factors in asset criticality, data sensitivity, regulatory exposure, and revenue impact to produce a prioritization that reflects your organization's actual risk posture.

Factor	CVSS-Only Approach	Risk-Based (RBVM) Approach
Severity source	Static CVSS score	CVSS + KEV + EPSS + business context
Exploit awareness	None	Active exploitation (KEV), predicted exploitation (EPSS)
Asset context	None	Business criticality, internet exposure, data sensitivity
Prioritization output	Static severity list	Dynamic, ranked remediation backlog
Remediation efficiency	Low—teams chase volume	High—teams focus on the 3% that matter

03 The RBVM Framework: Inputs That Drive Real Prioritization

Risk-based prioritization is only as good as the data inputs feeding it. A mature RBVM platform combines multiple risk signals to produce a composite priority score for each finding. Here are the six categories of input that matter:

1. Known Exploited Vulnerabilities (KEV)

CISA's KEV catalog identifies CVEs that are confirmed actively exploited in the wild. If a vulnerability is on the KEV list, it should be treated as urgent regardless of its CVSS score. Research shows that 40% of KEV-listed vulnerabilities are exploited within 48 hours of listing.

> ***DefectDojo Pro:*** *DefectDojo Pro automatically enriches every CVE-linked finding with KEV status and can auto-escalate KEV-listed findings via the Rules Engine.*

2. Exploit Prediction Scoring System (EPSS)

EPSS provides a probability score (0–1.0) estimating the likelihood that a vulnerability will be exploited in the next 30 days. EPSS v4 (released March 2025) significantly improved prediction accuracy. While only 18% of organizations currently use EPSS, those that do report it as 95%+ effective for prioritization.

> ***DefectDojo Pro:*** *DefectDojo Pro syncs EPSS scores for every finding automatically, and the risk-based prioritization engine incorporates EPSS as a core input alongside KEV and business context.*

3. Asset Criticality & Business Context

Not all assets are equal. A vulnerability in a revenue-generating, customer-facing production system carries fundamentally different risk than the same vulnerability in an internal dev sandbox. RBVM platforms must let you define business criticality, data classification, regulatory scope, and revenue attribution at the asset or product level.

> ***DefectDojo Pro:*** *DefectDojo's Product-level metadata supports business criticality, external audience classification, and regulatory tagging—all of which feed into the risk-based prioritization engine.*

4. Exploitability & Reachability

Can the vulnerability actually be reached by an attacker in your environment? Is there a public exploit? Is the vulnerable component exposed to the internet or isolated behind multiple network layers? These factors dramatically change the real risk of a finding.

> ***DefectDojo Pro:*** *DefectDojo Pro's prioritization engine factors in exploitability and reachability data to distinguish between theoretically severe and practically dangerous findings.*

5. Compliance & Regulatory Exposure

A vulnerability in a system that processes cardholder data (PCI-DSS scope), health records (HIPAA), or EU personal data (GDPR/CRA) carries additional regulatory risk—potential fines, audit failures, and mandatory disclosure. RBVM must account for compliance exposure.

> ***DefectDojo Pro:*** *DefectDojo Pro factors compliance penalties, user record exposure, and regulatory scope into its prioritization scoring, supporting PCI-DSS, NIST SP 800-40, and EU CRA frameworks.*

6. Temporal Intelligence & Trend Data

Has the vulnerability's risk profile changed? Is exploit activity increasing? Has a new proof of concept been published? RBVM platforms should dynamically update priorities as the threat landscape evolves, not just at scan time.

> ***DefectDojo Pro:*** *DefectDojo Pro's continuous EPSS sync and KEV monitoring ensure that finding priorities update dynamically as threat intelligence changes.*

---

04 8 Capabilities Every RBVM Solution Must Have

1. Automated KEV & EPSS Enrichment

Every CVE-linked finding must be automatically enriched with current KEV status and EPSS probability scores—without manual lookup or CSV imports. Data should refresh continuously.

2. Configurable Risk Scoring Engine

A black-box risk score is insufficient. You must be able to configure how inputs (KEV, EPSS, asset criticality, exploitability, compliance scope) are weighted in the composite priority score to reflect your organization's risk appetite.

3. Business Context Integration

The platform must let you define business criticality, data classification, regulatory scope, and revenue attribution at the product or asset level, and automatically factor these into finding prioritization.

4. Cross-Tool Deduplication

When multiple scanners report the same vulnerability, the platform must collapse duplicates into a single finding with the highest-fidelity risk score—not create separate entries that inflate the remediation backlog.

5. SLA-Driven Remediation

Define remediation timelines by risk level (not just CVSS severity), auto-notify before SLA breach, auto-escalate overdue findings, and report on SLA compliance rates.

6. Rules Engine & Automation

Automate finding management: auto-escalate KEV-listed findings, auto-assign based on product ownership, auto-tag based on compliance scope, auto-close based on rescan results. No human effort for routine decisions.

7. Dynamic Prioritization Updates

Finding priorities must update when threat intelligence changes—new KEV listing, EPSS score shift, new public exploit—not just at the next scheduled scan.

8. Actionable Remediation Guidance

Prioritized findings are useless if developers do not know how to fix them. The platform should surface remediation guidance, link to advisories, and push structured context into ticketing systems so developers can act immediately.

---

05 RBVM Architecture Comparison

RBVM capabilities are delivered through fundamentally different architectures. Understanding these trade-offs helps you select the right fit.

Category	Description	Strengths	Limitations
Open-Source + Commercial	Community-driven VM platform with an enterprise-grade commercial tier adding RBVM.	Transparent, tool-agnostic, no vendor lock-in, large integration ecosystem	Open-source tier may lack advanced prioritization; commercial tier required for full RBVM
Scanner-Native RBVM	RBVM built into a scanning vendor's platform, using their own scanner data as the primary input.	Deep integration with vendor's scanners, single platform for scan + prioritize	Biased toward vendor's own data, limited third-party tool support, lock-in risk

Category	Description	Strengths	Limitations
Standalone RBVM Platforms	Purpose-built RBVM tools that aggregate data from multiple scanners for risk-based prioritization.	Deep prioritization logic, strong threat intel integration	Yet another tool to integrate, may lack lifecycle management (ticketing, SLAs, compliance)
Exposure Management	Broader platforms that extend RBVM into attack surface management and risk quantification.	Holistic risk view, attack path analysis, asset discovery	Higher complexity and cost, may exceed current program maturity

> ***Where DefectDojo Pro fits:*** *DefectDojo combines the open-source foundation (OWASP Flagship, 43M+ downloads, 200+ integrations) with a commercial tier that delivers full RBVM—risk-based prioritization with KEV, EPSS, exploitability, reachability, and business context—plus the lifecycle management (SLAs, ticketing, rules engine, compliance reporting) that standalone RBVM tools typically lack. One platform from discovery through compliance.*

06 Evaluation Scorecard

Score each vendor 1–5 for each criterion, multiply by weight, and compare totals.

Capability	Weight	What to Evaluate	Vendor A	Vendor B	Vendor C
KEV & EPSS Enrichment	**15%**	Automated sync, refresh frequency, KEV auto-escalation			
Risk Scoring Configurability	**15%**	Adjustable weights, custom inputs, transparency of scoring logic			
Business Context Integration	**15%**	Product-level criticality, data classification, regulatory tagging			
Cross-Tool Deduplication	**10%**	Dedup accuracy across scanners, tunable matching algorithms			
SLA-Driven Remediation	**10%**	Risk-based SLA policies, auto-notify, auto-escalate, compliance dashboards			
Rules Engine & Automation	**10%**	Auto-escalate, auto-assign, auto-tag, auto-close capabilities			
Scanner Integration Breadth	**10%**	Native parsers, open framework, API ingestion, SARIF/CycloneDX			
Dynamic Priority Updates	**5%**	Continuous EPSS/KEV refresh, real-time priority recalculation			

Capability	Weight	What to Evaluate	Vendor A	Vendor B	Vendor C
Remediation Guidance	5%	Advisory links, fix recommendations pushed to tickets			
Pricing & Licensing	5%	Pricing transparency, no per-app or per-asset penalties			
TOTAL WEIGHTED SCORE	**100%**				

Tip: During your POC, import the same scan data into each vendor and compare the prioritized output. Ask: do the top 10 findings match what your senior security engineers would prioritize manually? That is the true test of a risk scoring engine.

07 Common Pitfalls to Avoid

Pitfall 1: Treating CVSS as "good enough"

CVSS measures theoretical severity, not real-world risk. Organizations that prioritize by CVSS alone spend 60%+ of remediation effort on findings that pose no practical threat. RBVM is not a nice-to-have—it is the difference between chasing volume and reducing risk.

Pitfall 2: Adopting EPSS without KEV

EPSS predicts future exploitation probability; KEV confirms current exploitation. If a vulnerability is on the KEV list, that information should supersede EPSS. The most effective approach uses both: KEV as a "definitely fix now" signal, EPSS as a "likely to be exploited soon" early warning.

Pitfall 3: Black-box risk scoring

If you cannot understand or configure how the vendor calculates risk priority, you cannot trust it. Insist on transparency: what inputs are used, how are they weighted, and can you adjust weights to reflect your organization's risk appetite?

Pitfall 4: RBVM without lifecycle management

A prioritized list of findings is useless without the workflow to act on it. If your RBVM tool produces a ranked backlog but cannot push findings to Jira, enforce SLAs, or track remediation, you still need a separate platform to operationalize the output.

Pitfall 5: Ignoring business context

EPSS and KEV are powerful but insufficient without asset-level business context. A KEV-listed vulnerability in a decommissioned test server is less urgent than a non-KEV finding in a production payments system. Make sure your RBVM incorporates business criticality.

Pitfall 6: Per-asset or per-finding pricing

Some RBVM vendors price by the number of assets scanned or findings processed. As your vulnerability program scales, this creates unpredictable cost growth. Insist on pricing that does not penalize you for better security coverage.

---

08 Why DefectDojo Pro

DefectDojo Pro is the only platform that combines open-source transparency, 200+ tool integrations, intelligent deduplication, and a configurable risk-based prioritization engine—all within a full vulnerability lifecycle management platform that includes SLAs, ticketing, a rules engine, and compliance reporting.

What sets DefectDojo Pro apart for RBVM

- **Purpose-built risk-based prioritization.** Launched May 2025, DefectDojo Pro's prioritization engine combines KEV status, EPSS probability, exploitability, reachability, revenue impact, compliance penalties, and user record exposure into a composite Priority score (0–1150) and a Risk classification (Low → Urgent) for every finding.
- **Automated KEV and EPSS enrichment.** Every CVE-linked finding is automatically enriched with current KEV status and EPSS scores. No manual CSV imports, no stale data. Scores update continuously as threat intelligence evolves.
- **Business context at the Product level.** Define business criticality, external audience, data classification, and regulatory scope per Product. These inputs feed directly into the risk-based prioritization engine, ensuring findings are ranked by what matters to your organization.
- **Rules Engine for automated response.** Auto-escalate KEV-listed findings, auto-assign based on product ownership, auto-tag by compliance scope, and auto-close on rescan verification—all without human effort for routine decisions.
- **Full lifecycle, not just prioritization.** Unlike standalone RBVM tools, DefectDojo Pro covers the entire vulnerability lifecycle: ingestion from 200+ tools, deduplication, prioritization, SLA enforcement, native ticketing (Jira, ServiceNow, GitHub, GitLab, Azure DevOps), verification, and compliance reporting.
- **Unified AppSec + SOC.** The first platform to unify application security findings and SOC alerts under a single risk-based prioritization model, eliminating the need for separate tools.
- **AI-first with MCP.** The first RBVM-capable platform to support the Model Context Protocol, enabling AI models to access prioritized vulnerability data for intelligent triage.
- **Predictable pricing.** No per-application, per-asset, or per-finding penalties. Your cost does not spike as coverage expands.

Start Your Free 2-Week Trial of DefectDojo Pro

Import your real scan data, test risk-based prioritization against your environment, and see how DefectDojo Pro surfaces the findings that actually matter.

defectdojo.com/get-started-with-pro

09 Next Steps: Your 30-Day Evaluation Plan

Adapt this framework to your procurement timeline.

Week	Activity	Key Deliverable
Week 1	Define RBVM requirements: which risk inputs matter most to your organization? Inventory scanners, identify 2–3 test applications, and prepare multi-scanner data for POC.	Requirements doc, scorecard with custom weights, test data package
Week 2	Vendor demos with your data. Compare how each platform prioritizes the same set of findings. Evaluate: does the top-10 match what your senior engineers would prioritize manually?	Completed scorecards; shortlist of 2–3 candidates
Week 3	POC: import multi-scanner data, configure business context per product, test KEV/EPSS enrichment, set up SLA policies, and test ticketing integration.	POC results: prioritization accuracy, enrichment coverage, SLA config effort
Week 4	Evaluate pricing, negotiate terms, confirm deployment model and data residency. Build the business case quantifying remediation efficiency gains.	Vendor selection with business case and projected ROI

Ready to get started? DefectDojo Pro offers a free 2-week trial with full access to risk-based prioritization, KEV/EPSS enrichment, the rules engine, and all 200+ integrations. Visit defectdojo.com/get-started-with-pro to begin.

This guide was produced by DefectDojo. For questions, contact info@defectdojo.com or visit defectdojo.com.