DEFECTDOJO

BUYER'S GUIDE · 2026 EDITION
FOR SECURITY LEADERS

UNIFIED VULNERABILITY MANAGEMENT

THE UVM BUYER'S GUIDE

A security leader's framework for evaluating unified vulnerability management in 2026 across the full lifecycle: the six stages, the ten capabilities, the architectures on offer, a weighted scorecard, the pitfalls, and a 30-day plan to decide with proof.

500+	50M+	10,000+	IDC
OFFICIAL INTEGRATIONS	DOWNLOADS	ORGANIZATIONS	MAJOR PLAYER IN ASPM

Contents

01 Executive summary PAGE 03

02 What unified vulnerability management is PAGE 04

03 The vulnerability lifecycle: six stages that matter PAGE 05

04 The ten capabilities every UVM platform must have PAGE 06

05 Architecture comparison PAGE 07

06 Evaluation scorecard PAGE 08

07 Common pitfalls PAGE 09

08 Why DefectDojo PAGE 10

09 Next steps: your 30-day evaluation plan PAGE 11

How to use this guide

Read sections 01 and 02 for the case you will make to leadership. Use sections 03 and 04 to write requirements that cover the whole lifecycle, section 06 to score vendors on equal terms, and section 09 to run the evaluation in 30 days.

Each lifecycle stage and capability ends with how DefectDojo Pro handles it, so you can check the claim against a live instance.

WHO THIS IS FOR

CISOs, vulnerability management leads and the engineers who keep application, infrastructure and cloud findings in order.

If your findings live in more than one console, this guide applies to you, whatever you call the program today.

KEY TAKEAWAY

The best UVM platforms cover the full lifecycle on one tool-agnostic platform, from discovery to compliance evidence, and never charge you more for covering more.

01

Executive summary

Organizations now generate vulnerabilities faster than they can fix them. Unified vulnerability management is how mature programs close that gap.

The vulnerability management market is worth about $17.6 billion in 2025 and growing 6% to 9% a year. That growth reflects a hard reality. The average enterprise runs dozens of scanners across application code, containers, cloud infrastructure, endpoints and networks, each with its own format, severity scale and dashboard.

Unified Vulnerability Management (UVM) addresses that fragmentation. Forrester describes UVM as the primary record of an organization's vulnerabilities and the place remediation work runs from. In practice it is one platform that ingests every scanner, normalizes and deduplicates the results, enriches them with real-world risk, enforces remediation SLAs and produces the reporting leadership and auditors ask for.

This guide gives you a framework for evaluating UVM platforms across the full lifecycle: six stages, ten capabilities, a weighted scorecard and the pitfalls that derail programs. Throughout, we show how DefectDojo Pro meets each requirement, drawing on the most widely deployed open source vulnerability management platform, with 50M+ downloads across 10,000+ organizations.

FIVE THINGS TO INSIST ON

1. Every scanner, application to network, in one normalized model.

2. Deduplication across tools, not only within one.

3. Ranking on real risk, refreshed as the threat changes.

4. SLAs, tickets and verification that close the loop.

5. Unlimited users and assets, so coverage is never taxed.

THE ONE-LINE TEST

Give every vendor real scan data from three scanners pointed at the same application. Ask how many unique issues it found, which one to fix first and why. Then ask to see that fix close itself on the next scan.

THE 2026 SHIFT

Attacks now move at AI speed, and AI-generated code ships faster than any team can review it. A platform that only stores and reports findings is a rear-view mirror. It has to rank each finding the moment it lands, route it to an owner, and put a fix in front of an engineer.

02

What unified vulnerability management is

UVM aggregates, normalizes, prioritizes and tracks vulnerabilities across the whole technology stack (applications, infrastructure, cloud, containers, endpoints and networks) in one platform, from discovery through verified remediation and compliance.

How UVM differs from traditional VM

DIMENSION	TRADITIONAL VM	UNIFIED VM
Scope	Network and infrastructure scanners	AppSec, infrastructure, cloud, containers, endpoints and SOC
Data model	Siloed per scanner	Normalized, deduplicated and enriched across all sources
Prioritization	CVSS severity alone	KEV, EPSS, business context, exploitability and reachability
Remediation	Manual tickets and spreadsheets	SLA enforcement, native ticketing, rules-driven triage
Reporting	Per-tool dashboards	One executive view, compliance evidence, audit trails
AI readiness	None	MCP support, AI-assisted triage, fixes shipped as pull requests

THE TEST OF UNIFIED

If an infrastructure finding and an application finding for the same CVE land in different queues, with different owners and different SLAs, the program is not unified yet. One model, one queue and one clock is the bar.

Market momentum

$17.6B
MARKET SIZE IN 2025

6.5%+
ANNUAL GROWTH THROUGH 2030

$24B+
PROJECTED MARKET BY 2030

Sources: MarketsandMarkets, Security Vulnerability Management Market (2025); Mordor Intelligence, Vulnerability Management Solutions (2026 to 2031); Grand View Research (2025 to 2030).

What drives it

- **Bigger attack surfaces.** Cloud migration, AI-generated code and connected devices add findings faster than teams add people.
- **Regulation with teeth.** The EU Cyber Resilience Act, SEC disclosure rules and PCI DSS 4.0 expect proof that vulnerabilities were found, tracked and fixed within policy.
- **Headcount does not scale.** Automation and consolidation are the only way to close the gap.

03

The vulnerability lifecycle: six stages that matter

A UVM platform must support every stage, not only discovery. Evaluate vendors against all six, or you may buy a platform that ingests well and falls short on remediation or evidence.

1 Discovery and ingestion

WHAT THE STAGE NEEDS

Scanners generate findings and the platform takes them in from every tool you run, by native parser, API or standard formats like SARIF and CycloneDX.

HOW DEFECTDOJO PRO HANDLES IT

500+ integrations, the Universal Parser for any CSV, JSON or XML report, and 140+ Upstream Connectors that pull findings and assets on a schedule.

2 Normalization and deduplication

WHAT THE STAGE NEEDS

Different scanners use different severity scales, names and formats. The platform must map them to one model and collapse the same CVE reported four times into one finding.

HOW DEFECTDOJO PRO HANDLES IT

Every parser converts its tool's report into the same Finding format. Cross-tool deduplication is chosen per tool in the UI, and Vulnerability Explorer shows each CVE once with every Asset it affects.

3 Enrichment and prioritization

WHAT THE STAGE NEEDS

Scanner severity is not enough. Findings need KEV status, EPSS, asset criticality, exploitability and reachability to surface the small share that carries real risk.

HOW DEFECTDOJO PRO HANDLES IT

EPSS, KEV and exploit-maturity data are added to every finding with a CVE and refreshed every 24 hours, feeding a priority score and risk band for every finding.

4 Assignment and remediation

WHAT THE STAGE NEEDS

Ranked findings must reach engineering and operations automatically, with owners, SLAs and escalation, in Jira, ServiceNow, GitHub, GitLab or Azure DevOps.

HOW DEFECTDOJO PRO HANDLES IT

Triage Engine rules assign owners and open tickets. Downstream Connectors reach the tracker each team uses, and the Remediation Center turns findings into a short list of fixes with due dates.

5 Verification and closure

WHAT THE STAGE NEEDS

After a fix, the platform must confirm it worked, by rescan or attested evidence, then close the finding and reopen it automatically if the issue comes back.

HOW DEFECTDOJO PRO HANDLES IT

Reimporting a newer scan closes the findings the scanner no longer reports, and anything that comes back reopens, with no manual bookkeeping.

6 Reporting and compliance

WHAT THE STAGE NEEDS

Leaders need risk trends, SLA compliance and remediation velocity. Auditors need evidence that findings were handled within policy for PCI DSS, SOC 2, the EU CRA and more.

HOW DEFECTDOJO PRO HANDLES IT

The Command Center and its Posture Score, five Insights views, scheduled report templates, and findings mapped to nine bundled compliance frameworks with audit logs behind them.

04

The ten capabilities every UVM platform must have

Write your requirements from this list, then check each one against a live instance during the proof of concept.

1 Universal scanner integration

Native support across SAST, DAST, SCA, container, cloud, network and endpoint scanners, with an open parser architecture for anything new.

IN DEFECTDOJO PRO 500+ integrations, the Universal Parser, 140+ Upstream Connectors, and Smart Upload to split infrastructure scans by host.

2 Cross-tool deduplication

Matching that collapses duplicates across every scanner, tunable per tool, per product and per environment.

IN DEFECTDOJO PRO Matching algorithms chosen per tool, Dedupe Pools across Assets, and Root Causes that group what one fix clears.

3 Risk-based prioritization

KEV, EPSS, asset criticality, business impact, exploitability and reachability, combined to surface the findings that carry real risk.

IN DEFECTDOJO PRO A priority score and risk band for every finding, with weights you set per Asset.

4 SLA-driven remediation tracking

SLAs by severity or risk (for example, Critical in 7 days, High in 30), warnings before breach, escalation, compliance reporting.

IN DEFECTDOJO PRO SLAs by severity or risk, never past the CISA KEV due date, assigned by business criticality.

5 Native ticketing and workflow automation

Two-way integrations with the trackers your teams use, and a rules engine for assignment, escalation and enrichment.

IN DEFECTDOJO PRO Jira two-way sync, Downstream Connectors for Azure DevOps, GitHub, GitLab, ServiceNow and more, and the Triage Engine.

6 AppSec, infrastructure and SOC in one place

One platform for application findings, infrastructure vulnerabilities, cloud misconfigurations and SOC alerts, with no separate dashboards.

IN DEFECTDOJO PRO Application, infrastructure, cloud and SOC findings share one normalized model and one queue.

7 CI/CD pipeline integration

API-first ingestion from the SDLC, with build metadata on every scan and deployment gating on thresholds.

IN DEFECTDOJO PRO API, Universal Importer and DefectDojo CLI for pipelines, with build, commit and branch on every scan.

8 Executive reporting and compliance

Views for executives, practitioners and auditors, exportable for board decks and regulators (PCI DSS, SOC 2, EU CRA, SEC disclosure).

IN DEFECTDOJO PRO Command Center, Posture Score, scheduled executive PDFs, FedRAMP POA&M and OSCAL output.

9 AI-ready architecture

Open standards such as the Model Context Protocol, so AI can work with your vulnerability data, plus AI that takes work off the queue.

IN DEFECTDOJO PRO A built-in MCP server, AI-assisted triage proposals, and Sensei (add-on) opening pull requests that fix the finding.

10 Scale and flexible deployment

Millions of findings across thousands of assets without slowing down, on SaaS, self-hosted or hybrid deployments that meet data residency rules.

IN DEFECTDOJO PRO Cloud-hosted, self-hosted or air-gapped, with a FIPS 140-3 mode for regulated environments.

05

Architecture comparison

UVM vendors take very different approaches. The architecture decides who controls your data, how far the platform can see, and what it costs to change your mind later.

CATEGORY	WHAT IT IS	STRENGTHS	LIMITATIONS
Open source foundations	Community-built platforms with a commercial edition on top. Transparent, auditable code.	No lock-in, code inspected by a global community, flexible deployment, visible roadmap.	The free edition needs internal resources to host and tune.
Scanner-native platforms	UVM from vendors who also sell scanners, bundled with their scanner suite.	Deep integration with the vendor's scanners, one contract.	Bias toward the vendor's tools, thin third-party support, lock-in risk.
Exposure management	Platforms that extend UVM into attack surface management and risk quantification.	Broader risk context, attack path analysis, asset discovery.	Higher complexity and cost; may exceed current program maturity.
GRC and ITSM add-ons	Vulnerability features added to governance, risk, compliance or IT service platforms.	One platform for GRC and security, existing enterprise contracts.	Vulnerability management is not the focus; deduplication and triage stay shallow.

WHERE DEFECTDOJO FITS

DefectDojo combines an open source foundation, an OWASP flagship with 50M+ downloads, with the commercial depth of DefectDojo Pro: risk-based prioritization, the Triage Engine, cross-tool deduplication, AppSec and SOC in one queue, MCP support and native ticketing, all tool-agnostic and available cloud-hosted, self-hosted or air-gapped.

Questions to ask about architecture

- Does it cover application and infrastructure findings in the same model?
- If I replace a scanner next year, what breaks?
- Can I export every finding, with its history, without a services engagement?
- Is the core inspected by anyone outside the vendor?
- Is there a written data residency answer for every region I operate in?

06

Evaluation scorecard

Score each vendor from 1 to 5 on every criterion, multiply by the weight, and compare totals. The weights reflect what matters most to leaders running programs at scale; adjust them before the first demo, not after.

CAPABILITY	WEIGHT	WHAT TO EVALUATE	VENDOR A	VENDOR B	VENDOR C
Scanner integration breadth	15%	Native parsers, open parser framework, scheduled connectors, SARIF and CycloneDX			
Deduplication accuracy	15%	Cross-tool deduplication, tunable matching, false-positive rate			
Risk-based prioritization	15%	KEV and EPSS enrichment, business context, exploitability, reachability			
SLA management	10%	Policy definition, notifications, escalation, compliance reporting			
Workflow automation	10%	Native ticketing, rules engine, automatic assignment			
Lifecycle coverage	10%	Discovery through verification and closure, with reopen on regression			
Reporting and compliance	10%	Executive views, audit evidence, regulatory framework mapping			
Unified scope	5%	AppSec, infrastructure, cloud and SOC findings in one platform			
AI readiness	5%	MCP support, AI-assisted triage, fixes shipped as pull requests			
Pricing and licensing	5%	Transparent model, unlimited users and assets, no per-scanner penalty			
Total weighted score	100%				

RUN IT ON YOUR DATA

Run the POC with your top two or three vendors using real scan data from at least three scanners pointed at the same application. Measure deduplication accuracy, integration setup time and SLA configuration effort.

WEIGHT THE LAST ROW HONESTLY

Pricing is 5% of the score and 100% of the renewal conversation. Get the pricing model in writing before the POC, and check whether adding users, assets or scanners changes the number.

07

Common pitfalls

Most UVM programs that disappoint bought something that does one stage of the lifecycle well and calls it unified. Seven ways that happens.

1 Confusing scanning with management

Scanning is stage one. If a "UVM" vendor only discovers and reports, you still need separate tools for deduplication, prioritization, SLAs, ticketing and evidence. Insist on the full lifecycle.

2 Choosing a scanner vendor's UVM

When the UVM comes from a scanning vendor, everyone else's scanners become second-class. Swapping or adding tools later means fighting your own platform.

3 Ignoring deduplication quality

Exact-match deduplication misses the same issue reported two ways. Ask vendors to demonstrate with your multi-scanner data. The gap between 60% and 95% accuracy is measured in engineer hours.

4 Per-user, per-asset or per-scanner pricing

These models penalize growth. As coverage expands, costs balloon, sometimes forcing teams to cut scanner coverage, the opposite of the outcome you need.

5 Overlooking the AppSec and infrastructure divide

Separate platforms for application and infrastructure vulnerabilities mean duplicate workflows and two pictures of risk. Check that one platform covers both.

6 Underestimating migration

Moving historical data is real work. Evaluate import coverage, API quality and services. 500+ native integrations remove most custom parser work from the plan.

7 Neglecting the developer experience

If developers hate the tool, adoption stalls. Check how findings reach them: tickets with clear fix guidance, and false positives they can dismiss without leaving their tools.

ONE MORE, FOR 2026

Mistaking an AI that describes findings for one that fixes them. Summaries and chat over a backlog are useful. They are not remediation. Ask what the agent changes in your repositories and cloud accounts, and who approves it.

08

Why the world runs on DefectDojo

Open source since 2014, born inside a real application security program, built with the OWASP community for the people who refuse to accept the status quo. No platform in security has been deployed, inspected and stress-tested more.

500+
OFFICIAL INTEGRATIONS

50M+
DOWNLOADS

10,000+
ORGANIZATIONS · OWASP FLAGSHIP

IDC
MAJOR PLAYER IN ASPM

One queue for every scanner

500+ integrations by file, API or scheduled Connector, all in one normalized model. **Most tools dedupe inside one scanner. DefectDojo Pro dedupes across every tool.**

Risk ranking you can defend to an auditor

EPSS, CISA KEV, threat intelligence, reachability and business context in one priority score, with weights you set per Asset. **Severity is not risk.**

Sensei ships the fix

Available as an add-on to DefectDojo Pro, Sensei opens pull requests that fix code findings and cloud misconfigurations. **You set the autonomy. Control stays yours.**

Evidence, not spreadsheets

Findings mapped to nine bundled compliance frameworks, with **FedRAMP POA&M and OSCAL output, CMMC scoring and EU CRA Article 14 reporting** built in.

Pricing that never punishes coverage

Unlimited users and assets. **Cloud-hosted, self-hosted or air-gapped, and your data belongs to you.**

Prove it before you buy it

Community Edition is the free open source platform, built on the same data model and parsers as Pro. **Run it in your stack, then bring your data to Pro when the program scales.**

CAPABILITY	COMMUNITY EDITION · WHERE PROGRAMS START	DEFECTDOJO PRO · WHERE PROGRAMS SCALE
Ingestion	360+ built-in parsers, by file upload, API or CI pipeline	Every Community Edition parser, plus the Universal Parser and 140+ Upstream Connectors that pull findings on a schedule
Deduplication	Same-tool deduplication, set in configuration	Cross-tool deduplication chosen per tool in the UI, plus Root Causes that group findings one fix will clear
Prioritization	Ordered by severity and CVSS, with business attributes recorded on each Asset	A priority score and risk band for every finding, weighing EPSS, KEV, threat intelligence, reachability and business context
Triage and SLAs	SLAs per Asset, risk acceptance with an owner and expiry date	Triage Engine rules, SLAs by severity or risk, approval workflow for accepted risk
Remediation	Jira with two-way sync, and GitHub Issues	Downstream Connectors for Azure DevOps, GitHub, GitLab, ServiceNow and more, plus the Remediation Center
Access and support	Local accounts and RBAC, community support on GitHub and the DefectDojo Community Slack	SSO, MFA, custom roles, instance-wide audit logs and commercial support with a dedicated customer success manager

SEE IT ON YOUR DATA

defectdojo.com/book-a-demo

A live session with your scanners, your findings and your questions. No canned deck.

COMPARE EDITIONS

defectdojo.com/pricing

See what each edition includes and get a quote sized to the findings volume you actually run.

09

Next steps: your 30-day evaluation plan

A structured evaluation prevents analysis paralysis and compares vendors on equal footing. Adapt the four weeks to your procurement calendar; keep the order.

WEEK	ACTIVITY	DELIVERABLE
Week 1	Define requirements and success criteria. Inventory scanners, ticketing systems and CI/CD pipelines. Pick two or three representative applications and real scan data from at least three scanners.	Requirements document and the scorecard from section 06 with your weights
Week 2	Run vendor demos with your requirements as the agenda and your data on screen. Evaluate deduplication quality, integration setup time, SLA configuration and dashboard usability.	Completed scorecards and a shortlist of two or three
Week 3	Run the POC. Import real data from several scanners and test the full lifecycle: ingestion, deduplication, prioritization, SLAs, ticketing, verification and reporting.	POC results: deduplication accuracy, integration time, SLA compliance
Week 4	Evaluate pricing and select your vendor. Confirm the deployment model, data residency and support commitments, then build the business case for leadership.	Vendor recommendation with business case and ROI projection

What a good POC proves

- Three scanners, one application, one deduplicated list.
- A ranked queue your team agrees with, and can explain.
- An SLA breach warning that reached the right person.
- A fix that closed its finding on the next scan.

START WITH THE FREE ONE

Community Edition is the free open source platform. Prove the integrations in your own stack this week, then move the same data to DefectDojo Pro for risk-based prioritization, the Triage Engine, cross-tool deduplication and enterprise support.

Join the underground.
Get your backlog to zero.

Security does not have to be a struggle, and your tools should not hold your data hostage. Bring your scanners and your backlog. defectdojo.com/book-a-demo

Produced by DefectDojo Inc. Questions: info@defectdojo.com or defectdojo.com. Market data from MarketsandMarkets (2025), Mordor Intelligence (2026 to 2031), Grand View Research (2025 to 2030) and The Forrester Wave: Unified Vulnerability Management Solutions, Q3 2025. IDC MarketScape vendor assessment for Application Security Posture Management. Product facts describe DefectDojo Pro as of October 2026; Sensei is available as an add-on to DefectDojo Pro. All trademarks are the property of their respective owners. © 2026 DefectDojo Inc. All Rights Reserved.