DEFECTDOJO

EBOOK · 2026 EDITION
FOR SECURITY LEADERS

ENTERPRISE VULNERABILITY MANAGEMENT

TAKING CONTROL OF ENTERPRISE VULNERABILITY MANAGEMENT

How centralized, automated vulnerability management lets security teams import, analyze and report on risk across the SDLC: three states of a program, what changes at each step, and how to get started.

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

Contents

01 Executive summary PAGE 02

02 Operating without a centralized platform PAGE 03

03 Centralizing with Community Edition PAGE 04

04 Automating with DefectDojo Pro PAGE 05

05 Enterprise-grade visibility PAGE 06

06 Prioritization with environmental context PAGE 07

07 Why DefectDojo PAGE 08

08 Getting started PAGE 09

01

Executive summary

Enterprise security teams rely on findings from a long list of siloed tools to assess risk. Yet in the SANS 2025 survey, 69% of security teams still report metrics with manual or mostly manual processes.

That cannot last. The time to exploit a vulnerability has fallen from 63 days in 2018 to about five days today. Teams need a centralized, automated platform so they spend their time on testing and remediation, not on collecting data.

This eBook walks through three states of enterprise vulnerability management:

- **Operating without a centralized platform.**
- **Centralizing with Community Edition**, for one view across your entire threat landscape.
- **Automating with DefectDojo Pro**, for remediation and reporting across the whole SDLC.

KEY TAKEAWAY

Centralize first, then automate. Each step takes work off your team and puts their attention back on real risk.

02

Operating without a centralized platform

Without one place for every finding, vulnerability management turns chaotic. Three failures define it.

69%
OF SECURITY TEAMS REPORT METRICS MANUALLY OR MOSTLY MANUALLY

5 days
AVERAGE TIME TO EXPLOIT, DOWN FROM 63 DAYS IN 2018

57%
OF TEAMS SPEND 25% TO 50% OF THEIR TIME ON VULNERABILITY MANAGEMENT OPERATIONS

1 Manual processes

WHAT HAPPENS

Analysts compile results and metrics by hand, scanner by scanner, for every report and every meeting.

WHAT IT COSTS

Red tape and manual review cap how many assessments a team can run, and limit how far the program can scale.

2 Data duplication

WHAT HAPPENS

SAST, SCA, DAST and other scanners overlap. A DAST scan finds a weakness an SCA scan already reported.

WHAT IT COSTS

Developers investigate the same issue more than once, and the backlog grows with findings that are not new.

3 Lost focus on strategic testing

WHAT HAPPENS

Teams buried in compiling results and administrative overhead never reach the high-priority, actionable vulnerabilities.

WHAT IT COSTS

Time that should go to testing goes to operations instead. 57% of teams already spend a quarter to half their week there.

THE WAY OUT

Centralize the data first. Once every finding lands in one place, deduplication, prioritization and reporting become things a platform does, not things people do.

Sources: SANS 2025 survey; Help Net Security.

03

Centralizing with Community Edition

Community Edition is a free, open source vulnerability management platform. It imports security data from across the SDLC and gives teams a strong foundation to manage, analyze and report on every security risk.

Standardized data ingestion

Add findings through the UI, the API or a CI pipeline, from 360+ built-in parsers covering SAST, DAST, SCA, container, cloud and infrastructure tools. Reimporting a newer scan closes what the scanner no longer reports.

Customizable API-driven automation

A full REST API with OpenAPI documentation lets teams build their own automation on top of the platform, from import to ticketing.

One finding format

Every parser converts its tool's report into the same Finding format, so you can filter, compare and report across tools at once. Repeats from the same tool are marked as duplicates.

Core reporting and visualization

A report builder, a main dashboard and metrics by Organization, Asset and engineer give you the essential numbers to manage a central vulnerability inventory.

Ticketing and SLAs

Jira with two-way status sync and GitHub Issues, SLAs per Asset, and risk acceptance with an owner and an expiry date.

A community behind it

An OWASP flagship project with 50M+ downloads, supported by the community on GitHub and the DefectDojo Community Slack.

IN PRACTICE: SAS

SAS uses the DefectDojo API to build automated Jira workflows.

Developers receive only verified, triaged findings, and tickets close automatically after remediation.

WHERE COMMUNITY EDITION FITS

Community Edition centralizes the data and gives you visibility across your threat landscape. When the program needs to run at scale, DefectDojo Pro builds on the same data model and the same parsers.

04

Automating with DefectDojo Pro

DefectDojo Pro is built on the same core for programs that need to run at scale. The shift is from centralizing data to automating the whole security lifecycle, so manual data entry and report merging leave your team's week.

Upstream Connectors

140+ connectors reach the APIs of scanners, cloud platforms and code hosts and pull in findings and assets on a schedule. New assets in a connected tool show up without anyone creating them.

The Universal Parser

Map any CSV, JSON or XML report that has no built-in parser, so the platform keeps working even when a vendor changes its export format.

Smart Upload

One infrastructure scan covering hundreds of hosts lands on the right Asset for each host, with no manual splitting.

Deduplication tuning

Choose matching algorithms per tool in the UI, including cross-tool deduplication, so the same issue from different scanners is worked once.

The Triage Engine

A no-code rules engine. Rules run when a scan lands or a finding changes, then assign reviewers, escalate high-risk findings, accept risk, open tickets or send messages. New rules start in Simulate mode.

Root Causes and the Remediation Center

Group the findings one fix would clear across every Asset, and turn open findings into a short list of fixes, each with a due date.

WHAT CHANGES FOR THE TEAM

Results arrive on their own, duplicates disappear before anyone reads them, and routine decisions are made the same way every time. Analysts spend the hours they get back on testing and remediation.

05

Enterprise-grade visibility

Pro is built to show program metrics the way enterprise leadership asks for them, with every number linked to the findings behind it.

The Command Center

Where findings come from, how many survive deduplication and triage, and what is waiting for action, with a short daily brief at the top that links straight to the evidence.

Posture Score

One number from 0 to 1000 that leaders can follow over time, and click through to the findings that lower it.

Dashboards and reports that run themselves

Start from templates such as executive brief, priority, triage and tool coverage. Share them, set team defaults, and send a scheduled executive pack as a PDF. Saved report templates run on a schedule or by rule, in PDF, HTML, CSV, Excel or JSON.

Five Insights views

Executive Insights

High-level metrics for management visibility and last-minute reporting.

Priority Insights

What to fix first, by priority score and risk band.

Program Insights

Whether the program is working, including time and cost saved through automation.

Remediation Insights

SLA tracking and mitigation speed across products.

Tool Insights

Which scanners earn their keep and which are the noisiest, to manage tool sprawl.

06

Prioritization with environmental context

Pro moves beyond scanner severity to help teams fix what matters most, and backs the platform with enterprise support and security.

Exploit intelligence on every finding

EPSS scores, the CISA KEV catalog (including known ransomware use) and exploit-maturity data are added to every finding with a CVE and updated every 24 hours, whichever tool found it.

A priority you can tune

A priority score and risk band (Urgent, Needs Action, Medium, Low) weigh severity, EPSS, KEV, threat intelligence and reachability with business attributes: criticality, internet exposure, revenue and user records.

Different rules for different assets

Each Asset can run its own Prioritization Engine, so a customer-facing app and an internal test system are ranked differently.

Reachability and exposure

See whether vulnerable code is actually called and whether a host can be reached from the internet, so findings nobody can reach stop crowding out the ones that matter.

Enterprise support and security

- Commercial support for cloud-hosted, self-hosted and air-gapped deployments, with a dedicated customer success manager.
- Unlimited users, and feature requests that are prioritized and guaranteed a review.
- On DefectDojo Cloud, monitoring, maintenance and backups are handled for you.
- Single sign-on through SAML, OpenID Connect, Microsoft Entra ID, Okta, GitHub Enterprise, GitLab and more, with MFA and SCIM provisioning.

07

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.

08

Getting started

Organizations can no longer rely on phased, manual testing cycles. Enterprise security needs continuous, pipeline-integrated scanning and one view of the organization's security posture.

01 **Start with Community Edition**
Install the free open source platform with Docker Compose or Helm and bring your scanners into one place.

02 **See DefectDojo Pro on your data**
Book a live session with your own scanners and findings at defectdojo.com/book-a-demo.

03 **Move your data**
Migrate your Community Edition data to DefectDojo Cloud, or to a self-hosted or air-gapped Pro deployment.

04 **Automate**
Turn on Upstream Connectors, risk-based prioritization and Triage Engine rules, then measure the hours your team gets back.

Conclusion

Community Edition gives thousands of organizations centralized vulnerability management across their enterprise security landscape, and DefectDojo has been downloaded more than 50 million times.

DefectDojo Pro automates remediation across the SDLC. Using business criticality and exploit probability, it makes sure teams fix the most dangerous risks first instead of drowning in noise from tool sprawl.

Pro lets an organization run security like a command center, where security speeds development up instead of slowing it down, with the support, intelligence and automation to protect an enterprise at scale.

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. Sources: SANS 2025 survey; Help Net Security. IDC MarketScape: Worldwide Application Security Posture Management 2025. 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.