DEFECTDOJO

BUYER'S GUIDE · 2026 EDITION
FOR SECURITY LEADERS

DEVSECOPS

THE DEVSECOPS BUYER'S GUIDE

A security leader's framework for building security into the development lifecycle in 2026 without slowing engineering: the maturity spectrum, the ten capabilities to require, 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 DevSecOps is, and why now PAGE 04

03 The DevSecOps maturity spectrum PAGE 05

04 The ten capabilities every DevSecOps platform must have PAGE 06

05 Architecture comparison PAGE 08

06 Evaluation scorecard PAGE 09

07 Common pitfalls PAGE 10

08 Why DefectDojo PAGE 11

09 Next steps: your 30-day evaluation plan PAGE 12

How to use this guide

Read sections 01 to 03 for the case you will make to leadership and to place your program on the maturity spectrum. Use section 04 to write requirements, section 06 to score vendors on equal terms, and section 09 to run the evaluation in 30 days.

Every capability ends with how DefectDojo Pro meets it, so you can check the claim against a live instance during the proof of concept.

WHO THIS IS FOR

CISOs, AppSec leads, platform engineers and the developers who will live with the result.

If findings from more than one scanner land in your pipelines, this guide applies to you, however far along the DevSecOps path you are.

KEY TAKEAWAY

DevSecOps is an operating model, not a tool. It needs an orchestration layer that takes every scanner in, removes the noise, ranks on risk and puts the work where developers already are.

01

Executive summary

Most organizations agree on DevSecOps. Far fewer run it. The gap is tool sprawl, noise, and findings that never reach the developer who can fix them.

The DevSecOps market is projected to pass $20 billion by 2030, growing above 13% a year. Regulation is one driver: Executive Order 14028 and the EU Cyber Resilience Act both expect evidence of secure development. Breaches that start in the application layer are the other.

Execution lags. Security teams manage three to six tools on average, 71% say their alerts carry heavy noise from false positives and duplicates, and the mean time to remediate a critical vulnerability is still 65 days. While 47% of organizations say they follow DevSecOps practices, only 36% have adopted DevSecOps workflows.

This guide gives you a structured way to evaluate DevSecOps platforms: a maturity spectrum to place your program, the ten capabilities that matter, the architectural trade-offs, a weighted scorecard and a four-week plan. Throughout, we show how DefectDojo Pro meets each requirement as a vendor-neutral orchestration layer.

FIVE THINGS TO INSIST ON

1. Every scanner in the pipeline, in one queue.

2. Deduplication across tools before a developer sees anything.

3. Prioritization on real risk, not scanner severity.

4. Findings delivered in the tools developers use, with two-way sync.

5. An API for everything, and no lock-in to one vendor.

THE ONE-LINE TEST

Send one week of pipeline scans from three of your tools through each platform, then count the tickets that reach developers. If the number is bigger than the number of real fixes, the platform is adding noise, not removing it.

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 DevSecOps is, and why now

Gartner describes DevSecOps as building security into agile and DevOps development as smoothly as possible, without slowing developers or pulling them out of their toolchain. In practice that means security testing, vulnerability management and compliance checks run automatically at every stage, from commit to production.

$20B+
DEVSECOPS MARKET PROJECTED BY 2030

93%
OF SECURITY LEADERS MANAGE 3+ SECURITY TOOLS

65 days
AVERAGE MTTR FOR CRITICAL VULNERABILITIES

Three forces behind the shift

- **Velocity has outpaced security.** Teams ship many times a day. Quarterly scans, manual pen tests and release-blocking reviews cannot keep up, so security becomes a gate people route around.
- **Tool sprawl creates noise.** 57% of DevSecOps teams run five or more tools, each with its own format. Without normalization and deduplication, teams drown in duplicates and conflicting priorities.
- **Regulation wants evidence.** Executive Order 14028, the EU Cyber Resilience Act, NIS2 and PCI DSS 4.0 all expect proof of secure development, with an audit trail behind it.

Traditional AppSec vs. DevSecOps

DIMENSION	TRADITIONAL APPSEC	DEVSECOPS
When security runs	At the release gate	At commit, build, deploy and runtime
Who owns findings	Security triages and assigns	Developers, in GitHub, GitLab or Jira
Tool integration	CSV exports and spreadsheets	API-first, automated in CI/CD
Finding volume	Raw scanner output, heavy duplication	Deduplicated, normalized, ranked by risk
Remediation speed	65+ days average MTTR	Up to 11.5x faster with mature practices
Compliance evidence	Written by hand	Audit trails and reports generated automatically

Sources: Grand View Research; Mordor Intelligence; Fortune Business Insights; StrongDM DevSecOps Statistics 2025; Seemplicity 2025 Remediation Operations Report.

03

The DevSecOps maturity spectrum

Gartner's DevSecOps maturity model looks at skills, developer enablement, secure design, testing and vulnerability management. Most organizations sit somewhere on this four-level spectrum.

LEVEL	WHAT IT LOOKS LIKE	CHARACTERISTICS	KEY GAP
Level 1: Ad hoc	Testing happens sporadically, driven by audits or incidents.	Manual pen tests, spreadsheet tracking, no CI/CD integration, findings scattered across tools.	No central place to manage or deduplicate findings.
Level 2: Foundational	Some tools are in place but run separately with little automation.	SAST and DAST deployed outside CI/CD, basic ticketing, findings reviewed by hand.	No normalization across tools; developers switch context constantly.
Level 3: Integrated	Security runs in CI/CD with findings managed in one place.	Pipeline scanning, central platform, deduplication, SLA tracking, developer workflows.	Often no risk-based ranking, and AppSec, infrastructure and SOC still split.
Level 4: Optimized	Risk-based orchestration across every security domain.	Risk-based prioritization, rules-driven triage, AI assistance, fixes shipped as pull requests, compliance automation.	Continuous improvement, measured with real metrics.

WHERE DEFECTDOJO FITS

DefectDojo Pro is built to move a program from Level 2 to Level 4. It provides the central orchestration of Level 3, and the risk-based prioritization, Triage Engine, unified AppSec and SOC coverage and AI assistance that define Level 4.

Questions that place you on the spectrum

- Does every pipeline send its scan results somewhere central without a person involved?
- Does a developer get one ticket when three scanners find the same issue?
- Is your backlog ranked by exploitability and business impact, or by scanner severity?
- Could you hand an auditor evidence of what was found and fixed, without a spreadsheet?
- Does anything ship a fix, or only open a ticket?

PLACE YOURSELF HONESTLY

Most teams that call themselves Level 3 are Level 2 with a dashboard. If a developer still gets the same vulnerability from two scanners as two tickets, you are not integrated yet.

04

The ten capabilities every DevSecOps platform must have

Write your requirements from this list. Each capability states what to look for, then how DefectDojo Pro meets it, so you can verify the claim during the proof of concept.

1 Broad security tool integration

WHAT TO LOOK FOR

Ingest findings from every scanner in your stack (SAST, DAST, SCA, container, infrastructure, cloud and custom tools) through native parsers, API connectors or formats like SARIF and CycloneDX.

HOW DEFECTDOJO PRO DOES IT

500+ integrations: every Community Edition parser, the Universal Parser for any CSV, JSON or XML report without one, and 140+ Upstream Connectors that pull results on a schedule.

2 CI/CD pipeline integration

WHAT TO LOOK FOR

Scans must land automatically on every build, not in a separate process. Look for API hooks any pipeline can call, build metadata on each scan, and a way to gate a deployment on a threshold.

HOW DEFECTDOJO PRO DOES IT

Pipelines send scans through the API, the Universal Importer or the DefectDojo CLI, with imports running in the background. Each scan records build, commit, branch and repository, and the API can gate a release.

3 Intelligent deduplication

WHAT TO LOOK FOR

When five scanners report the same vulnerability, you need one finding, not five. Deduplication must work across tools, with matching you can tune.

HOW DEFECTDOJO PRO DOES IT

Cross-tool deduplication with several matching algorithms, chosen per tool in the UI. Dedupe Pools let a group of Assets deduplicate against each other.

4 Risk-based prioritization

WHAT TO LOOK FOR

Combine CVSS, KEV, EPSS, asset criticality, exploitability and business context so developers fix the most dangerous findings first, not the loudest.

HOW DEFECTDOJO PRO DOES IT

A priority score and risk band (Urgent, Needs Action, Medium, Low) for every finding, weighing EPSS, KEV, threat intelligence, reachability, root-cause reach and business attributes.

5 Developer workflow integration

WHAT TO LOOK FOR

Developers will not adopt a platform that makes them leave their tools. Findings must reach GitHub, GitLab, Jira, Azure DevOps or ServiceNow with context, fix guidance and a link back.

HOW DEFECTDOJO PRO DOES IT

Jira with two-way status sync, plus Downstream Connectors for Azure DevOps, GitHub, GitLab Boards, Bitbucket, Linear, ServiceNow and more. Status flows back without double entry.

6 API-first architecture

WHAT TO LOOK FOR

Everything must be automatable: import findings, create engagements, query metrics, export reports. If a workflow needs clicks, it will not keep pace with engineering.

HOW DEFECTDOJO PRO DOES IT

A full REST API with OpenAPI documentation, plus endpoints for every Pro feature. The MCP server lets AI assistants do the same work, with each user's own permissions.

7 Triage automation

WHAT TO LOOK FOR

Routine finding management should not need a person: escalate, assign by ownership, tag compliance scope, close on a verified fix.

HOW DEFECTDOJO PRO DOES IT

The Triage Engine runs no-code rules when a scan lands or a finding changes. New rules start in Simulate mode, and every change traces back to the rule that made it.

8 SLA enforcement and remediation tracking

WHAT TO LOOK FOR

Set SLAs by risk, notify owners before a breach, escalate overdue findings, and track compliance across products and teams.

HOW DEFECTDOJO PRO DOES IT

SLAs by severity or by risk, assigned automatically by business criticality. Scan Cadence flags Assets whose expected scans have stopped arriving.

9 Compliance reporting and audit evidence

WHAT TO LOOK FOR

Produce evidence auditors accept: what was scanned, found, ranked, fixed and still open, mapped to PCI DSS, SOC 2, NIST and the EU Cyber Resilience Act.

HOW DEFECTDOJO PRO DOES IT

Findings map to nine bundled frameworks. Saved report templates run on a schedule or by rule in PDF, HTML, CSV, Excel or JSON, and SBOM and VEX documents export in standard formats.

10 Vendor-neutral, no lock-in

WHAT TO LOOK FOR

The platform should work with any scanner, CI system and ticketing tool, so you can adopt the best tool for each job as the program grows.

HOW DEFECTDOJO PRO DOES IT

Born as an OWASP flagship open source project and tool-agnostic by design. Replace a scanner and the history of its findings stays in DefectDojo.

WHY THE LAST ONE MATTERS

Every scanner vendor will tell you it does DevSecOps. The orchestration layer is the one place that has to stay neutral, because it outlives every tool you plug into it.

05

Architecture comparison

DevSecOps capabilities ship in very different architectures. The architecture decides how far the platform can see and how hard it is to change course later.

CATEGORY	WHAT IT IS	STRENGTHS	LIMITATIONS
Open source foundations	A community-built platform with a commercial tier that adds enterprise DevSecOps capabilities.	Transparent, vendor-neutral, no scanner lock-in, large community and integration ecosystem.	The free edition needs internal resources to host and tune; automation and risk ranking come with the commercial tier.
Scanner-native platforms	DevSecOps built into a scanning vendor's platform and tied to its own SAST, DAST and SCA tools.	Deep integration with the vendor's scanners, one contract.	Lock-in to the vendor's scanners, thin third-party support, biased prioritization.
CI/CD security add-ons	Security features that bolt onto one CI/CD platform.	Low friction for developers, native to the pipeline, fast to deploy.	Limited to one CI/CD platform, shallow lifecycle, no cross-tool deduplication.
Developer security platforms	Developer-first tools that put scanning in the IDE, pull request and CLI.	Fast feedback, strong developer adoption.	Usually SAST and SCA only, no cross-tool deduplication, little SLA or compliance support.

WHERE DEFECTDOJO FITS

DefectDojo starts from an open source foundation: an OWASP flagship project with 50M+ downloads and 500+ integrations. DefectDojo Pro adds the orchestration: pipeline imports, cross-tool deduplication, risk-based ranking, the Triage Engine, delivery to developer tools and compliance reporting, without tying you to any scanner vendor.

Questions to ask about architecture

- Does it treat a competitor's scanner as well as its own?
- If we change CI systems next year, what breaks?
- Does it deduplicate across tools, or only within one?
- Can I run it in my own environment, including air-gapped?
- Can I export every finding with its history, without a services engagement?

06

Evaluation scorecard

Score each vendor from 1 to 5 on every criterion, multiply by the weight, and compare totals. Adjust the weights to your program before the first demo, not after.

CAPABILITY	WEIGHT	WHAT TO EVALUATE	VENDOR A	VENDOR B	VENDOR C
Tool integration breadth	15%	Native parsers, scheduled connectors, API import, SARIF and CycloneDX			
CI/CD pipeline integration	10%	Pipeline import tools, build metadata, release gating			
Intelligent deduplication	15%	Cross-tool accuracy, tunable matching, measured noise reduction			
Risk-based prioritization	15%	KEV, EPSS and asset context in one score; configurable and transparent			
Developer workflow push	10%	GitHub, GitLab, Jira, Azure DevOps, ServiceNow, with context and two-way sync			
API-first architecture	5%	Full REST API, documented, covers every feature			
Triage automation	10%	Escalate, assign, tag and close by rule, with a safe way to test rules			
SLA enforcement	5%	Risk-based SLAs, notification and escalation, compliance reporting			
Compliance reporting	10%	PCI DSS, SOC 2, NIST and CRA mapping; exportable audit evidence			
Pricing and vendor neutrality	5%	Transparent model, unlimited users and assets, scanner independence			
Total weighted score	100%				

RUN IT ON YOUR DATA

Import the same multi-scanner dataset into every vendor during the POC. Count how many duplicates each platform collapsed, and check whether the top ten priorities match what your team would choose by hand.

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 DevSecOps programs that stall picked a tool when they needed an orchestration layer, or forgot that developers have to want to use it. Six ways that happens.

1 Buying a scanner, not a platform

A SAST or DAST tool finds vulnerabilities. A platform manages them from discovery through remediation and compliance. Buy a scanner expecting DevSecOps and you will build the orchestration layer yourself, or add yet another tool.

2 Ignoring developer experience

Findings that land in a portal developers never visit do not get fixed. 45% of teams report misaligned workflows. Meet developers in GitHub, GitLab, Jira and Azure DevOps.

3 Underestimating deduplication

Several scanners finding the same issue should not create several work items. Without deduplication the backlog inflates three to five times and your metrics stop meaning anything.

4 Locking into a single-vendor stack

"Built-in DevSecOps" from a scanner vendor favors its own tools. As the program matures you will want the best tool for each job. A neutral platform keeps that option open.

5 Treating DevSecOps as a purchase

The platform enables the operating model; it does not replace it. Plan for process change, developer training and executive sponsorship alongside the technology.

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

These models penalize the behavior you want: more coverage, more people looking, more tools. Insist on unlimited users and assets so broader adoption is rewarded, not taxed.

A SEVENTH, 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 every vendor what their agent changes in your repositories 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	Inventory your security tools, CI/CD pipelines and ticketing systems. Decide which integrations are critical and what deduplication and prioritization you need. Prepare multi-scanner test data.	Requirements document, tool inventory and the scorecard from section 06 with your weights
Week 2	Run vendor demos on the same dataset. Compare deduplication rates, ranked output, delivery to developer tools and pipeline setup.	Completed scorecards and a shortlist of two or three
Week 3	Run the POC. Import production scan data, tune deduplication, set up prioritization, connect a pipeline, push findings to Jira, GitHub or GitLab, and let a developer close one end to end.	POC results: deduplication rate, ranking accuracy, developer feedback, SLA setup effort
Week 4	Evaluate pricing and confirm the deployment model, data residency and support commitments. Build the business case around noise removed and MTTR improved.	Vendor recommendation with business case and projected MTTR improvement

What a good POC proves

- Three of your tools, one queue, no duplicates.
- A pipeline that imports on every build without anyone touching it.
- A developer who received a finding in their own tool and closed it.
- A fix that closed the finding on the next scan.

START WITH THE FREE ONE

Community Edition is the free open source platform. Prove the integrations and your pipeline imports this week, then move the same data to DefectDojo Pro for cross-tool deduplication, risk-based ranking, the Triage Engine 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 Grand View Research, Mordor Intelligence, Fortune Business Insights, the Gartner DevSecOps Maturity Model, StrongDM DevSecOps Statistics 2025, the Seemplicity 2025 Remediation Operations Report and publicly available vendor documentation. 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.