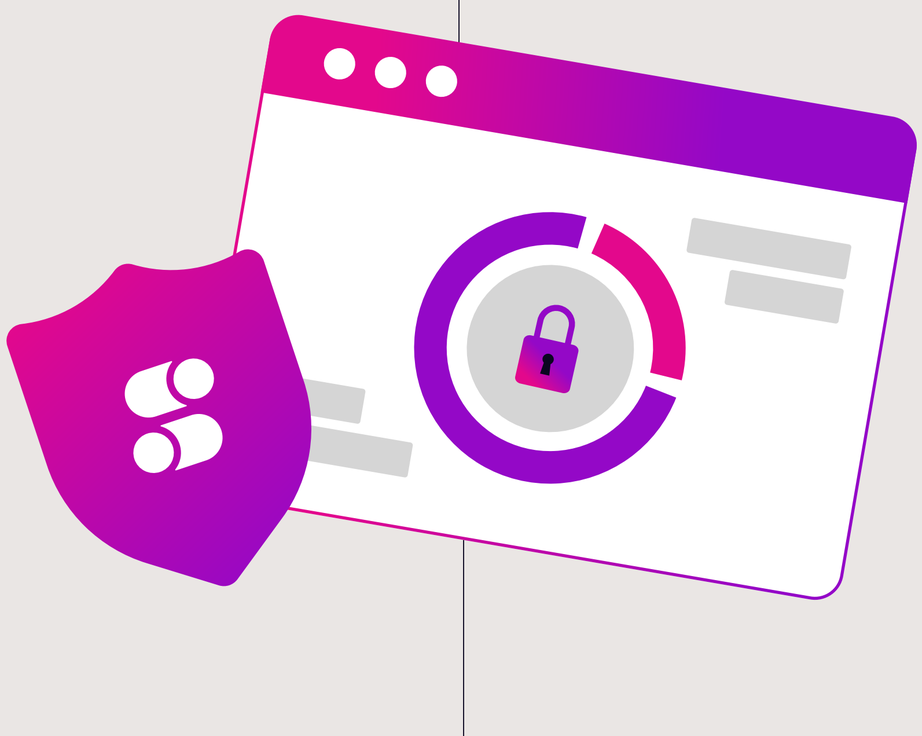
seemplicity

GUIDE

AppSec is Dead: A Buyer's Guide to Next Gen ASPM Platforms

How to Select the Right ASPM Solution to Accelerate Fixes, Improve SLA Compliance, and Reduce Risk



Product Security, DevSecOps and Development teams are overwhelmed with findings generated by siloed application security testing tools, leaving these teams with fragmented data, delayed remediation, and rising security risk.

With the advent of Application Security Posture Management (ASPM), there's a new way forward. ASPM platforms streamline application security by integrating testing tools, automating remediation workflows, and aligning with modern DevSecOps practices. This guide cuts through the noise to help you choose an ASPM solution that unifies your security testing results, prioritizes what really matters, and gets fixes into production – fast.

By the end of this guide, you'll have a clear framework to evaluate ASPM vendors, understand key selection criteria, and access a checklist designed to help you move from findings to fixes without friction.

Table of Contents

What Is an ASPM Platform?

An ASPM Platform is a modern, unified approach to application security that consolidates and prioritizes findings from a variety of security testing tools –ranging from static and dynamic analysis to software composition analysis. Rather than simply scoring vulnerabilities, ASPM platforms focus on accelerating remediation by integrating seamlessly into CI/CD pipelines and development workflows.

Key Characteristics of an ASPM Platform

Unified Data	Consolidates alerts from multiple testing tools (SAST, DAST, SCA, etc.) into a single, actionable view.
Risk-Based Prioritization	Uses contextual factors—like exploitability, application criticality, and business impact—to rank vulnerabilities so teams know what to fix first.
Automated Workflows	Integrates with ticketing and development tools (e.g., Jira, email, Slack) to assign tasks directly to the right teams.
Continuous Monitoring	Delivers real-time updates as applications evolve, ensuring vulnerabilities are caught early and fixed fast.

By addressing the “security vs. speed” dilemma, an ASPM Platform helps organizations shift from a reactive patching mentality to proactive, continuous risk management.

Gartner

Recommendations

- Prioritize ASPM implementation in organizations with diverse development teams, especially those using various development and security tools to facilitate tedious application security (AppSec) efforts.
- Determine the organization's requirements, such as improving the visibility of various components that make up an application or system, the need for increased productivity, improved security effectiveness or risk management. This assessment will increase the effectiveness of ASPM tool selection and implementation.

Gartner

Recommendations

- Ensure the ASPM approach can support any legacy applications in your organization's portfolio, as certain tools are tailored for cloud-native applications.
- Evaluate the ASPM market to ensure you can support and integrate with existing development and security tools in your DevSecOps pipeline.

Understanding the ASPM Buying Journey

Selecting an ASPM Platform begins with a clear assessment of your current challenges and ends with a well-planned rollout that integrates with your existing DevSecOps workflows. Below is a step-by-step framework to guide you through the evaluation process and ensure you choose a platform that delivers lasting impact - not just another tool.

STEP 1 | Identify Your Needs

Start by asking the hard questions:

1. **Fragmented Data?**
   Are you juggling multiple testing tools that produce isolated, uncorrelated findings?
2. **Overwhelming Noise?**
   Are your teams spending too much time sorting through low-priority alerts?
3. **Delayed Fixes?**
   Is the handoff from security to development slowing down your remediation?
4. **Process Bottlenecks?**
   Are manual workflows and spreadsheets stalling your pace of fixes?

If any of these pain points sound familiar, your organization is primed for an ASPM solution.

STEP 2 | Identify Your Needs

Before you evaluate vendors, clearly define what you need the platform to achieve. Focus on practical, day-to-day challenges:

Centralized Application Security Findings	Unify outputs from SAST, DAST, SCA, and more into a single cohesive view.
Real-Time, Risk-Based Prioritization	Automatically and dynamically adjust risk scores based on contextual data like business impact and exploitability.
Integrated, Automated Remediation Workflows	Route actionable tasks directly to developers' and operations teams' workflows - without manual intervention.
Seamless Collaboration	Use tools your teams already trust - like Jira, Slack and GitHub - to facilitate smooth remediation handoffs, eliminate friction and improve response times.

STEP 3 | Determine Key Stakeholders

Effective ASPM adoption hinges on getting alignment across the right teams. Each group brings different priorities to the table, and successful rollout accounts for them all:

STAKEHOLDERS	DESIRE	REQUIRE
CISO & Security Leadership	Visibility into exposure, SLA compliance, and measurable risk reduction.	A platform that provides executive-level dashboards, SLA tracking, and measurable remediation outcomes.
Product Security, Application Security & DevSecOps Leaders	A solution that meshes with agile development practices without slowing innovation	A platform that integrates into CI/CD workflows and automates remediation based on contextual risk.
Developers & Operations Teams	Actionable, prioritized remediation tasks that don't disrupt their workflow.	A solution that pushes fix-ready tickets into tools they already use.
IT & Cloud Security	Assurance that remediation won't disrupt business-critical systems or slow deployments.	A platform that supports secure fixes across cloud and infrastructure environments, without added complexity.

Keep these stakeholder needs front and center as you craft your ASPM strategy.

Core Features to Look for in an ASPM Platform

When evaluating an ASPM platform, security and DevSecOps leaders must look for a solution that not only aggregates security findings from various sources but also streamlines remediation across the entire application lifecycle. The ideal ASPM platform should provide continuous application security visibility, automated fix orchestration, and facilitate collaboration across development, security, cloud and IT teams. Below is a checklist of must-have capabilities to help guide vendor selection.

CENTRALIZED RISK VISIBILITY	Consolidates application security findings from multiple testing tools (SAST, DAST, SCA, etc.) into a single, actionable dashboard.
SMART FIX GROUPING	Aggregates similar vulnerabilities or misconfigurations that require the same remediation into one task to eliminate duplicate efforts.
CUSTOMIZABLE RISK SCORING	Enables dynamic adjustment of risk scores based on factors such as business context, application criticality, exploitability, and team priorities.
INTELLIGENT REMEDIATION ASSIGNMENTS	Supports nested organizational structures and team-based remediation, ensuring that tasks are directed to the appropriate development or security teams.
AUTOMATED FIX ORCHESTRATION	Auto-generates remediation tickets, assigns tasks, and tracks progress—integrating with ticketing systems like ServiceNow, Jira, or native integrations within CI/CD pipelines.
SEAMLESS INTEGRATION WITH DEVOPS	Works natively with your existing tools (e.g., CI/CD pipelines, issue tracking systems, collaboration platforms) without forcing you into a closed ecosystem.
EXCEPTION & RISK ACCEPTANCE MANAGEMENT	Provides workflows for documenting, tracking, and periodically re-evaluating accepted risks, false positives, or justified exceptions.
AUTOMATED SLA TRACKING & ESCALATION	Monitors remediation timelines, triggers alerts for overdue tasks, and escalates critical issues if SLA deadlines are at risk.
FIX VERIFICATION	Uses subsequent testing results to confirm that vulnerabilities marked as "fixed" no longer appear, avoiding false closures.
EASE OF DEPLOYMENT	Offers straightforward setup with intuitive, out-of-the-box automation that doesn't require extensive professional services.

Selecting The Right ASPM Platform

Some ASPM vendors bundle proprietary scanning tools with their platforms, suggesting an all-in-one solution. However, this approach can restrict flexibility and force organizations into a closed ecosystem—even if you already have best-in-class security testing tools. Organizations benefit most from an open, vendor-agnostic ASPM platform that allows them to:

Leverage Best-Of-Breed Security Tools	Utilize a mix of open-source and commercial scanners, cloud security tools, and code analysis platforms for optimal coverage.
Avoid Vendor Lock-In	Prevent reliance on a single vendor's proprietary tools, enabling you to switch or supplement tools without disruptive costs.
Maximize Existing Security Investments	Seamlessly integrate with the tools you've already deployed, ensuring that all security findings flow into a centralized remediation process without redundancy.
Enable Cross-Domain Collaboration	Integrate findings from application security, cloud security, and infrastructure security to foster a coordinated and unified remediation approach.

Evaluating ASPM Vendors: A Step-by-Step Guide

Once you've defined your needs and core platform requirements , it's time to evaluate vendors. The goal isn't just to compare feature lists, it's to identify which platform will deliver real impact across your workflows, teams, and remediation timelines. Follow these steps for a systematic approach:

STEP 1 | **Define Must-Have Features**

Using the checklist on page 6, outline your organization's specific requirements.

STEP 2 | Request a Demo or Trial

Engage vendors in a proof-of-value (PoV) exercise, allowing them to demonstrate how their platform delivers value in practice – not just on paper:

Ask to see the following:

- How the platform consolidates, aggregates and prioritizes vulnerabilities.
- How remediation tasks are assigned to remediation owners.
- How SLAs are tracked.
- How exception handing and risk acceptance workflows are documented and managed.

STEP 3 | Assess Ease of Use and Setup

The platform should work for everyone – from security engineers to developers – without a steep learning curve or endless customization.

Consider the following:

- How long does it take to get up and running without significant custom development?
- Does the platform easily mesh with your existing CI/CD pipelines, ticketing systems, and collaboration tools?
- Is the interface intuitive for developers, security analysts, and operations teams alike?

STEP 4 | **Evaluate ROI**

Remediation speed is important, but so is long-term efficiency and cost-effectiveness.

Ask the following questions:

- How much manual effort does the solution eliminate?
- What is the expected reduction in Mean Time to Remediate (MTTR)?
- How will improved SLA compliance and operational efficiency translate into cost savings and measurable value for the business?

Identifying the Right Vendor

After evaluating vendors against your checklist, and going through a demo or run trials, the next step is to determine which one you want to move forward with - the one that aligns best with your security needs and operations goals. Use the following criteria to identify your winning vendor and ensure you select the best ASPM platform:

1 Prioritize a Smooth Proof of Value (PoV) Experience

A strong PoV can demonstrate measurable improvements in remediation and risk reduction within 30–60 days.

- How long does it take to go from set up to meaningful results?
- What onboarding resources or support are included in the trial period?
- Does the vendor require external support or custom development to demonstrate value?
- Can you measure early wins like automation, fix routing, or reduced triage time?

WINNING VENDOR INSIGHT

Top vendors deliver early momentum, demonstrating automation, faster ticketing, and frictionless integration during the first few weeks, without custom engineering.

2 Measure Real-Time Impact

You need more than anecdotal success. Confirm that the platform provides clear metrics on remediation speed and SLA performance by looking for real-time data and dashboards that track measurable criteria .

- Does the platform track MTTR, SLA compliance, and backlog reduction?
- Can it show improvements in remediation speed during the PoV?
- Are these metrics visible to both technical and executive stakeholders?
- How are risks escalated if SLAs are missed?

WINNING VENDOR INSIGHT

The right platform proves its worth with continuous insights that quantify value, turning vague process improvements into measurable outcomes.

3 Ensure Scalability

Verify that the ASPM solution can grow with your organization and support expanding application portfolios without added complexity.

- Can the platform support multiple business units and teams?
- Does it streamline day-to-day operations, or will it add new layers of maintenance and oversight?
- Will it accommodate future growth in application development, team size and tool acquisition?
- Does it require extensive customization to maintain over time?

WINNING VENDOR INSIGHT

Scalable platforms integrate easily, grow with your organization, and deliver long-term value without creating new bottlenecks.

Next Steps: From Evaluation to Implementation

Once you've selected an ASPM Platform, it's time to plan your rollout:

Secure Budget and Stakeholder Buy-In

Use business value assessments and pilot results to align internal teams and secure funding.

Plan for Implementation and Adoption

Develop a clear rollout plan that includes training, integration with existing workflows, and success metrics.

Monitor and Iterate

Launch a targeted pilot (e.g., with high-risk applications) and refine the process before a full-scale implementation.

Final Thoughts: Turning Findings into Fixes

Traditional vulnerability management isn't enough for today's rapid development cycles. An ASPM Platform isn't just another tool—it's a strategic enabler that transforms how organizations approach application security. By centralizing data, automating workflows, and delivering actionable insights, ASPM platforms help you move quickly from findings to fixes. In an environment where every minute counts, the right ASPM solution can mean the difference between reactive patching and proactive, continuous security.

With an ASPM Platform, you can break down silos, streamline remediation, and ultimately secure your applications at the speed of business.

seemplicity

Seemplicity's Remediation Operations Platform exemplifies this new approach by reducing mean time to respond, accelerating fixes, and ensuring compliance—all without the friction of traditional methods.

READ SOLUTION BRIEF