



The Complete ASPM Buyer's Guide

Certified by Roland Cloutier,
(fmr) Global CISO, TikTok, ADP & EMC



The Complete ASPM Buyer's Guide

In today's "everything-as-code" world, building software is a high-speed, high-stakes game. Development teams are under pressure to deliver quickly, and security teams are struggling to manage an increasingly complex attack surface. This creates a what we call "AppSec Chaos" - a landscape filled with fragmented point solutions, inconsistent policies, and strained relationships between security and development teams.

Sound familiar?

The good news is, there's a solution: Application Security Posture Management (ASPM). ASPM platforms bring order to the chaos by unifying your security efforts, giving you a clear view of your application risks, and automating remediation processes. It's no wonder that, [according to Gartner](#), **40% of organizations developing proprietary applications will adopt ASPM by 2026.**

But how do you choose the right solution?

This buyer's guide is your roadmap to navigating the ASPM market. By understanding the key features and differentiators of leading vendors, you can make an informed decision that ensures your organization's applications remain secure, compliant, and resilient against evolving threats.

Keep reading to learn:

- What ASPM is
- Use cases for ASPM
- How to measure the ROI of ASPM
- What questions to ask vendors
- How to get internal buy-in

Table of Contents

What is ASPM?	04
Use Cases for ASPM	04
Key Components of ASPM	08
Signs You Need an ASPM Solution	09
How To Measure the ROI of ASPM	10
Questions to Ask Vendors	12
How to Get Internal Buy-In	17
Learn More About Cyscale	18

What is ASPM?

Application Security Posture Management is an AppSec platform that provides complete visibility, risk prioritization, and remediation capabilities to improve organizations' overall cyber resiliency.

[Introduced by Gartner as a distinct category](#) to fill the gaps left by traditional point solutions, ASPM platforms provide visibility of vulnerabilities across the entire software development lifecycle (SDLC), prioritize vulnerabilities based on risk scoring, enforce controls, and provide robust remediation capabilities.

Unlike traditional security tools that focus on isolated aspects of application security, ASPM platforms take a holistic approach, integrating CI/CD pipeline security, application security testing, posture management, and compliance monitoring into a unified platform.

Use Cases for ASPM

Before we drive into the specific use cases, let's first take a closer look at the challenges security and development teams are facing. According to the first-ever [State of ASPM Report](#):

80%

of application security professionals say that managing multiple security point solutions is challenging

88%

of CISOs say alert fatigue is causing developers not to remediate critical vulnerabilities

The average AppSec team uses

49 tools

90%

of application security professionals say that the relationship between their security and development teams needs improvement

Still trying to understand the specific applications of ASPM? Here are some use cases that demonstrate the value of platforms:

Use Case	Description	Benefits
Visibility & Optionality	Data from multiple security tools (native or third-party) is brought together into a single interface	Reduces complexity, improves efficiency, reduces licensing costs
Prioritization and Risk Management	Prioritizes vulnerabilities based on business impact	Reduces false positives, enhances risk management, helps teams focus on the right things to address critical issues first without wasting time
Enhanced Collaboration	Integrates security checks into the development workflow so that teams don't need to leave their environment	Identifies and fixes vulnerabilities early, important context is provided automatically, speeds up secure software releases
Compliance and Reporting	Assists in meeting compliance requirements and generating audit reports	Ensures regulatory compliance, demonstrates security best practices
Incident Response and Remediation	Provides guidance on remediation and mitigation of vulnerabilities	Streamlines incident response, minimizes disruption

Visibility & Optionality

According to the [State of ASPM 2024 report](#), 80% of application security professionals say that managing multiple security point solutions is challenging. That's not a surprise when you realize that **the average AppSec team uses 49 tools**. This leads to fragmented visibility and management challenges.

ASPM platforms unify various security tools and data sources into a single interface, simplifying management and enhancing visibility across the CI/CD pipeline and SDLC. Importantly, ASPM solutions can integrate with or replace your existing third-party tools, with proprietary scanners like [SAST](#), [SCA](#), and more built in.

The result? Reduced complexity, improved efficiency, and cost savings.

Prioritization and Risk Management

81% security and development leaders say that [teams experience too much vulnerability noise](#) and alert fatigue. ASPM helps reduce alert fatigue by analyzing factors like potential business impact, exploitability, and severity, and assigning a risk score to each vulnerability.

Beyond offering unparalleled code-to-cloud visibility, [Cycode's Risk Score](#) seamlessly integrates into existing workflows. The parameters of the risk scoring formula can be tailored to align with specific business needs and risk tolerance levels, providing a customized approach to risk management.

Interconnecting risk data across various security tools and platforms is absolutely critical in this process. By aggregating and correlating data from diverse sources, security teams gain a holistic view of potential threats, enabling them to accurately assess risk in context. This interconnected approach ensures that all relevant information is considered when evaluating vulnerabilities, leading to more informed decision-making.

This comprehensive, data-driven strategy not only streamlines the prioritization process but also enhances the accuracy of risk assessments. It empowers security teams to concentrate their resources on addressing the vulnerabilities that pose the greatest threat to the organization, thereby improving the overall security posture and significantly reducing the potential damage from a cyberattack.

Enhanced Collaboration Between Security and Development Teams

ASPM platforms bridge the gap between security and development teams by seamlessly integrating security checks into the SDLC. This early integration provides developers with a ubiquitous view across the entire pipeline, allowing them to identify and fix vulnerabilities much sooner in the development process.

This holistic approach leads to several **key benefits**:

- **Reduced rework:** By catching vulnerabilities early in the development pipeline, developers can address issues before the code is integrated into the larger codebase. This reduces the need for extensive rework and costly fixes later in the development cycle, ensuring smoother project progression.
- **Faster development cycles:** Early identification and remediation of vulnerabilities streamline the development process, minimizing delays that could arise from security reviews or bug fixes closer to release. This integration allows for faster development cycles and quicker time-to-market for new features, as security is no longer a bottleneck.
- **Empowered developers:** ASPM [integration within developer workflows](#) provides developers with the tools and real-time context they need to write secure code from the outset. This fosters a culture of security ownership within development teams, where developers are empowered to proactively address security concerns as they code, rather than waiting for security audits later in the process.
- **Enhanced security posture:** By proactively addressing vulnerabilities early and maintaining visibility across the entire development pipeline, organizations can significantly improve their overall application security posture. This approach reduces the attack surface for potential threats, ensuring that security is built into the fabric of the development process from start to finish.

Compliance and Reporting

ASPM platforms take the complexity out of compliance management, transforming it into a streamlined and efficient process. By automating report generation for security standards like [NIST SSDF and Self-Attestation](#), they eliminate the manual work that used to burden security teams, freeing up critical time and resources.

ASPM's robust reporting capabilities provide auditors with a clear, comprehensive view of your organization's security posture, making audits smoother and quicker. Ultimately, ASPM ensures your applications adhere to relevant security policies and regulations, reducing the risk of non-compliance and avoiding potential financial penalties.

Incident Response and Remediation

A relentless stream of vulnerabilities can overwhelm security teams, while sluggish remediation times expose organizations to potential data breaches and financial losses.

ASPM platforms directly address these challenges by empowering both security and development teams. They don't just identify vulnerabilities; they offer clear, step-by-step instructions for developers to fix or mitigate threats and offer tools like [bulk remediation](#) that enable developers to address vulnerabilities within their familiar workflows to minimize disruption to development cycles.

This collaborative approach leads to a significant reduction in Mean Time to Remediate (MTTR), ensuring vulnerabilities are addressed swiftly and effectively.



Key Components of ASPM

- **CI/CD Pipeline Security**

Because CI/CD pipelines are an attractive target for malicious actors, a complete ASPM platform must be equipped with [CI/CD pipeline security](#) capabilities that align with [DevOps practices](#) and support a [shift-left approach](#). This includes auditing privileges, [scanning and detecting secrets](#), [source code leakage detection](#) and continuous monitoring and logging to identify and mitigate threats swiftly.

Integrating these security measures within CI/CD pipelines ensures early detection and resolution of vulnerabilities, maintaining the speed and scalability of development while enforcing security policies and compliance requirements.

- **Next-Gen Application Security Testing (AST) Capabilities**

A complete ASPM platform must also include advanced [Application Security Testing \(AST\)](#) capabilities, including developer-friendly [Static Application Security Testing \(SAST\)](#) and [Software Composition Analysis \(SCA\)](#) that help teams identify, prioritize, and remediate risks.

Importantly, both SAST and SCA capabilities should be based on proprietary scanners and not on [open source](#) to ensure better, more accurate risk prioritization and fewer false positives.

- **Posture Management**

Seamless integration with existing security infrastructure, including [third-party security tools](#), ensures a unified approach to posture management. By ingesting findings, prioritizing vulnerabilities for fixing, and offering built-in remediation, a complete ASPM platform identifies root causes, traces the entire risk path, and helps teams visualize threats through a single pane of glass.

The result? Enhanced [cyber and business resilience](#).

Signs You Need an ASPM Solution

Without an ASPM solution in place, organizations and teams (both development and security) are likely experiencing a number of pain points. Do any of these sound familiar?

If so, it's time to evaluate vendors. Skip to [this section](#) for 30+ questions to help you choose the right solution.



Fragmented Tools and Processes

You're using several security tools that don't integrate well, making it difficult to manage and correlate data from disparate sources.



Inefficient Vulnerability Management

Security teams are overwhelmed by the volume of security alerts and face challenges in prioritizing and addressing critical vulnerabilities.



Strained Communication

Poor collaboration between security and development teams and a lack of clarity around who owns what is affecting how quickly and effectively security risks are being remediated.



Lack of Comprehensive Visibility

You have blind spots in the development and deployment processes, and can't see your entire application security posture.



Slow Remediation Times

Manual and cumbersome remediation workflows are causing high mean-time-to-remediation (MTTR) and prolonged exposure.



Inadequate Continuous Monitoring

Reliance on periodic security assessments leaves gaps in security coverage between scans.



Difficulty in Aligning with Modern Development Practices

Security struggles to integrate into fast-paced DevOps and CI/CD pipelines, leading to late discovery of vulnerabilities.



Expanding Attack Surfaces in the Software Supply Chain

The increased complexity of cloud computing, APIs, microservices, and third-party components makes it challenging to secure the entire software supply chain.



Security Expertise Gap

A shortage of skilled cybersecurity professionals necessitates automation to handle routine security tasks and optimize resource allocation.

How To Measure the ROI of ASPM

So, how can you tell if your ASPM solution is really cutting the mustard? Let's break it down.

First off, is your ASPM tool actually helping you prioritize what matters? Is it cutting through the noise and highlighting the real risks? If it's not saving your team time by focusing on the critical issues, it's not doing its job.

Next, are you seeing a difference in how quickly you're fixing problems? If your ASPM tool is streamlining your processes and improving teamwork between security and development, you should notice a speedier response time.

It's also essential to consider how well the tool fits into your everyday workflow. Does it integrate smoothly with your existing tools and processes? And is it helping you stay on top of compliance requirements?

To get a clearer picture of your ASPM solution's performance, keep an eye on these key indicators:



Breaches prevented



Vulnerability detection rate



False positive rate



Mean time to remediate



Coverage of application portfolio



Compliance adherence



Number of high-risk vulnerabilities



Incident response time



Cost of remediation



Developer feedback on tool usability



Incident response collaboration

CUSTOMER SUCCESS STORY

Rapyd

About Rapyd

Rapyd powers local payments globally, enabling quick market access for companies. Its platform unifies over 900 payment methods in more than 100 countries. Investors include Stripe, General Catalyst, and Tiger Global.

Problem

- Concern over developers hardcoding secrets in source code
- Need to secure the software supply chain amid rising attacks
- Required robust integration capabilities, proprietary scanners, and tool that would support compliance requirements in the highly regulated FinTech industry

Solution

- Rapyd uses Cyscale for hardcoded secrets scanning, leak detection, CI/CD security, and Software Composition Analysis (SCA)
- High-quality, proprietary scanners, developed in-house
- Seamless integration into Rapyd's SDLC



We evaluated several vendors that either didn't have their own scanners, or their scanners created a lot of noise. Cyscale really has developed a lot of in-house scanners that are built in a better way than the market standard.

- Erez Mor, Director of Security Engineering at Rapyd

Results

- Complete visibility of different systems across the different software development pipelines
- Improved code-writing practices
- Reduced risk
- Fewer false positives
- Enhanced collaboration and productivity between security and R&D teams
- Tool consolidation and cost savings
- Faster MTTR

Complete vs. Standalone ASPM

While many companies claim to have an ASPM platform, they don't deliver many of the required core functionalities. So what's the difference between complete ASPM solutions and incomplete solutions?

[A complete ASPM platform](#) is one that has a comprehensive suite of **proprietary application security scanning tools**.

This includes:

- [CI/CD Security \(Pipeline Security\)](#)
- [Secrets scanning & detection, Code leak detection](#)
- [Software Composition Analysis \(SCA\)](#)
- [Static Application Security Testing \(SAST\)](#)
- [Infrastructure as Code \(IaC\) scanning](#)

Complete ASPM platforms also offer flexibility, allowing organizations to easily select and connect the third-party tools that are right for their unique ecosystem and requirements.

Unlike complete solutions, Standalone ASPM solutions don't have native scanning capabilities. Instead, they're only able to ingest data from third-party security tools.

If they do have scanning capabilities, they're extremely limited in providing complete visibility. As a result, they're **not** able to prioritize vulnerabilities based on a complete picture of risk, and aren't able to provide effective remediation capabilities.

All of this means that organizations that rely on standalone ASPM solutions are dependent on the vendor to provide the correct integrations, as is the case with point solutions.

Questions to Ask Vendors

When evaluating ASPM solutions, it's crucial to ask vendors targeted questions to ensure their offerings align with your organization's needs.

We've outlined key questions to help you assess various aspects such as integration capabilities, scanner types, policy enforcement, and more. By addressing these critical areas, you can make an informed decision and select an ASPM solution that effectively enhances your security posture and supports your development workflows.



Pipeline Visibility

Gaining deep visibility into your CI/CD pipelines is critical for understanding your application security posture. An ASPM solution should provide real-time insights into security risks at every stage of the development process, enabling proactive mitigation.

- Questions to ask:**
1. How does the ASPM solution provide visibility into our CI/CD pipelines?
 2. Can we track and monitor security issues across different stages of the pipeline?
 3. How does the platform alert us to security issues in real-time during the development process?



Coverage of the SDLC

Coverage of the SDLC ensures that security measures are applied at every stage of development, from coding to deployment. This holistic approach helps in early detection and remediation of vulnerabilities, reducing the risk of security breaches and compliance issues.

- Questions to ask:**
1. How does your ASPM solution support security across the entire software development lifecycle (SDLC)?
 2. Are there specific features for early-stage development versus post-deployment monitoring?
 3. How does the solution facilitate secure coding practices from development to deployment?



Scanners

Scanners are tools within the ASPM solution that identify security vulnerabilities in your applications. Understanding whether the scanners are proprietary or open-source, is important because it affects the accuracy, reliability, and frequency of updates.

- Questions to ask:**
1. What types of scanners are included in your ASPM solution?
 2. Are the scanners proprietary or based on open-source technology?
 3. How effectively do your scanners handle proprietary, open-source, and AI-generated code and are you able to prioritize risk?



Integration Coverage

Integration coverage refers to how well the ASPM solution can integrate with your existing development tools, CI/CD pipelines, and other third-party applications. Seamless integration ensures that security practices are embedded into your current workflows without causing disruptions.

- Questions to ask:**
1. How does the ASPM solution integrate with our existing development tools and CI/CD pipelines?
 2. Can the platform integrate with our current security information and event management (SIEM) systems?
 3. What APIs or connectors are available for seamless integration with other third-party tools?



Policy Enforcement

Enforcing consistent security policies across all stages of the development process is fundamental to reducing risk. Your ASPM solution should offer flexible policy definition and enforcement capabilities to align with your organization's specific security requirements.

- Questions to ask:**
1. How are security policies defined and enforced within the ASPM platform?
 2. Can we customize policies to align with our organizational security standards?
 3. What mechanisms are in place to ensure compliance with these policies?



Prioritization and Triage

Efficiently managing vulnerabilities requires intelligent prioritization. Look for an ASPM solution that effectively ranks vulnerabilities based on risk, providing actionable insights to focus remediation efforts and ensure that the most significant risks are mitigated promptly.

- Questions to ask:**
1. How does the ASPM solution prioritize security vulnerabilities?
 2. What criteria are used to determine the criticality of vulnerabilities?
 3. Does the platform offer automated triage to streamline the remediation process?



Root Cause Analysis

Root cause analysis involves tracing security vulnerabilities back to their origin. This helps in understanding the underlying issues that lead to vulnerabilities, allowing for more effective remediation. Choose an ASPM solution that offers detailed root cause analysis reports that provide insights into specific code changes or configuration errors that need to be addressed.

- Questions to ask:**
1. How does the ASPM platform perform root cause analysis on identified vulnerabilities?
 2. Can it trace issues back to specific code changes or configuration errors?
 3. What level of detail is provided in the root cause analysis reports?



Remediation Orchestration

Streamlining the remediation process is essential for improving efficiency and reducing risk. An effective ASPM solution should automate repetitive tasks, integrate with ticketing systems, and provide guided remediation workflows.

- Questions to ask:**
1. How does the ASPM solution assist in automating remediation actions?
 2. Can it integrate with our ticketing systems to assign tasks to developers?
 3. Are there automated workflows for common remediation scenarios?



Source Code Security

Protecting your source code is paramount...just look at the [25+ biggest source code leaks](#) to better understand the consequences. Your ASPM solution should offer robust features for secure coding, static analysis, and code review to identify vulnerabilities early in the development process.

- Questions to ask:**
1. What capabilities does the ASPM platform offer for securing source code?
 2. How are code reviews and static analysis integrated into the development process?
 3. Can the platform detect and prevent common coding vulnerabilities?



Application Security Testing (AST) Capabilities

A comprehensive AST program is essential for identifying and mitigating vulnerabilities. Your ASPM solution should provide a range of testing capabilities, including SCAT and SAST, to address different types of vulnerabilities.

- Questions to ask:**
1. What types of application security testing are included in your ASPM solution?
 2. How are test results integrated and reported within the platform?
 3. Can the AST tools be customized to target specific application architectures or technologies?



Reporting & Dashboards

Effective communication of security risks is crucial for driving improvements. Your ASPM solution should provide customizable reporting and dashboards to meet the needs of different stakeholders, from developers to security executives.

- Questions to ask:**
1. What types of reports and dashboards are available in the ASPM solution?
 2. Can we customize reports to meet specific compliance or regulatory requirements?
 3. How are real-time security metrics presented to different stakeholders?



Security

Needless to say, ASPM platforms should effectively protect sensitive data via features like access controls and permissions. It should also adhere to industry best practices for data protection and privacy, including compliance with standards like SOC2.

- Questions to ask:**
1. What access controls and permissions are available to ensure secure use of the ASPM platform?
 2. Is your platform SOC2 compliant, and how do you maintain this compliance?
 3. How can we audit and manage user activities within the platform?



APIs

Extensibility is key for tailoring an ASPM solution to your specific needs. Robust APIs enable integration with custom tools and workflows, enhancing the solution's value.

- Questions to ask:**
1. What APIs are available for extending the functionality of your ASPM solution?
 2. How are these APIs documented, and what support is available for developers?
 3. Can the APIs be used to integrate custom security tools or workflows into the platform?



Pricing

Evaluate pricing models carefully to ensure they align with your budget and organizational structure. Consider factors such as the number of users, applications, and features when comparing pricing options.

- Questions to ask:**
1. What pricing models do you offer (subscription, pay-per-use, tiered pricing)?
 2. Are there additional costs for integrating with third-party tools or scaling up as our needs grow?
 3. Can you provide a detailed breakdown of what is included in each pricing tier?
-



Developer-Friendliness

Developers are key to successful security initiatives. An ASPM solution should be designed with developers in mind, offering intuitive interfaces, clear guidance, and integration with popular development tools.

- Questions to ask:**
1. How does your ASPM solution integrate with popular development tools and CI/CD pipelines?
 2. What features are available to help developers easily identify and remediate security issues?
 3. Do you offer training or resources to help developers effectively use your platform?
-



Vendor Support

Reliable vendor support is essential for the long-term success of your ASPM program. Evaluate the vendor's support offerings, including response times, availability, and knowledge base resources.

- Questions to ask:**
1. What levels of support do you offer?
 2. How quickly can we expect responses and resolutions to critical issues?
 3. Do you provide any onboarding assistance or ongoing training for our teams?

How to Get Internal Buy-In

Security is a team sport, which means you'll need to involve several key stakeholders to ensure the ASPM solution will meet your organization's comprehensive security needs. For example:

- **Security Team:** The backbone of your security posture, they'll evaluate the solution's ability to detect threats, prioritize vulnerabilities, and streamline incident response.
- **Development and DevOps Teams:** These teams will assess how well the ASPM solution integrates into their workflows, automates security checks, and accelerates development cycles.
- **Compliance and Risk Management:** They'll ensure the solution aligns with industry regulations and mitigates potential risks.
- **IT Operations:** Their focus is on the solution's infrastructure compatibility, performance impact, and integration with existing IT systems.
- **Procurement and Finance:** These teams will evaluate the solution's cost-effectiveness, ROI, and vendor relationships.
- **C-Suite:** Ultimately, executive buy-in is crucial for securing budget and resources. They need to understand the business value of ASPM in terms of risk reduction, cost savings, and competitive advantage.

To achieve internal alignment and secure buy-in, follow these **five steps**:

01

Identify Pain Points

Clearly articulate the challenges your organization currently faces related to application security. Use data and metrics to demonstrate the impact of these issues on the business.

02

Demonstrate Value

Highlight how ASPM can address these pain points by improving efficiency, reducing risks, and ensuring compliance. Quantify the potential benefits in terms of cost savings, revenue growth, and brand reputation.

03

Involve Stakeholders Early

Foster open communication and collaboration by involving key stakeholders from the beginning. Seek their input on requirements, priorities, and concerns.

04

Pilot and Iterate

Conduct a pilot program to test the ASPM solution in a controlled environment. Gather feedback from users and refine your implementation strategy based on the results.

05

Build a Strong Business Case

Develop a comprehensive business case that outlines the investment, expected return, and potential risks. Use clear and compelling language to communicate the value proposition to decision-makers.

Learn More About Cycode

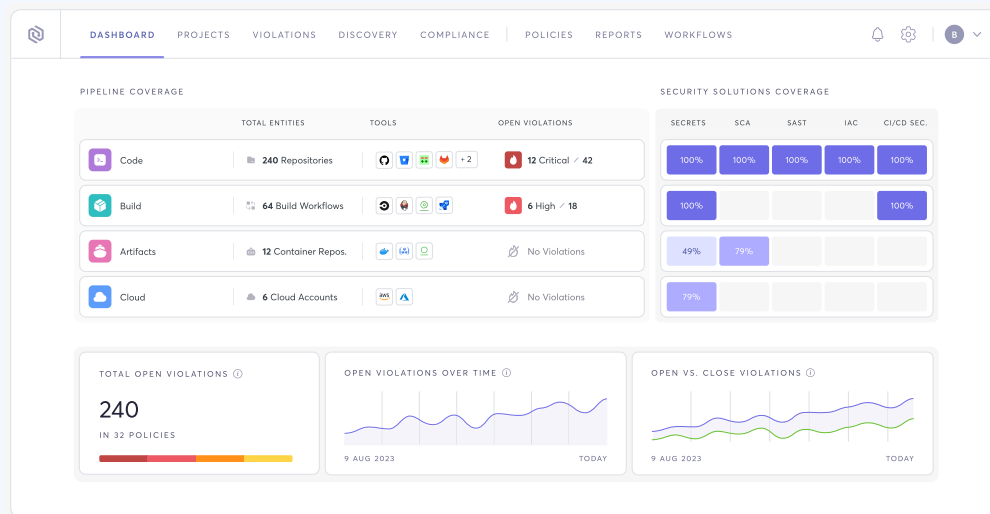
Cycode is the only Complete ASPM platform that scales and standardizes developer security without slowing down the business. The result? Teams can deliver safe code, faster.

Here's what sets us apart:

- Cycode lets you use our own proprietary scanners, or connects to your third-party scanner
- Our Risk Intelligence Graph (RIG) provides unmatched visibility, accuracy, prioritization, and traceability across the entire SDLC
- Cycode was founded by developers and is the only platform that brings together security and development teams
- Our world-class research team delivers security notifications on zero-day threats within the platform

Want to [learn more](#) about Cycode's complete ASPM platform?

[Book a demo](#) now to find out how we can help you reduce technical debt, prevent vulnerabilities, detect critical risks, and remediate them faster.



Peace of Mind
With a Complete ASPM

