

Publication date:

29 Feb 2024

Author(s):

Rik Turner, Senior Principal Analyst

On the Radar: Cyscale offers ASPM, from scanning to prioritization and remediation

Summary

Catalyst

Cyscale is a developer of application security posture management (ASPM) technology. This is proactive AppSec technology that ingests data from multiple code scanning platforms, dedupes, normalizes, and correlates it, then applies analytics to prioritize issues based on their criticality and suggests remedial action.

Omdia view

Posture management is a proactive approach to security that is applied to an expanding range of areas within enterprise infrastructures, applications being among the latest. The term ASPM, coined by a leading analyst firm, succeeds a previous one, namely application security orchestration and correlation (ASOC). The move to the newer name has the advantage that it implies the inclusion of prioritization into the mix in addition to associating this technology with the broader SPM trend.

That application security can benefit from the more proactive approach of identifying issues before they are exploited by attackers, thereby reducing the app's attack surface, is beyond question. How to go about it, on the other hand, is a debate that is still playing out in the market. On the one hand, we have the vendors that propose an aggregation, correlation, and prioritization platform without any scanning capability, instead relying on ingesting third-party scanners' output. On the other hand are companies such as Cyscale, which offer all the building blocks to scan the disparate parts of an app as well as the downstream prerequisites of an ASPM platform. This "complete ASPM" approach definitely appeals to a variety of

customer types, sizes, and industries, and the fact that Cymode can also ingest data from other sources via its ConnectorX third-party security tool connector makes it even more attractive.

Why put Cymode on your radar?

Cymode offers what it calls a “complete” ASPM platform, in that it can deliver both the multiple scanning capabilities and the prioritization and remediation required for such an offering. This also enables it to talk of enabling application security “from code to cloud.”

However, aware that many prospective customers, particularly in high-end enterprises, will already be running other application security testing tools, it offers its ConnectorX tool to facilitate the ingestion of their output into its platform. It is already well advanced in its goal of covering the majority of the third-party tools it needs to work with in this way.

Market context

The challenge of securing applications remains high despite, or perhaps because of, the large number of available tools. The speed of software development and deployment, combined with the availability of more scanning and AppSec tools, means more issues are being identified. Security teams are overwhelmed by a cacophony of vulnerabilities, leading to longer remediation timelines and increased risk. The problem can overwhelm development and security processes, but there is often little to explain its importance and impact at the business level.

ASPM is one of the more recent entrants into the family of technologies whose initialisms end in SPM. Starting out in the 2010s with workloads in the cloud-native environments of infrastructure- and platform as a service (IaaS and PaaS), where it bears the name cloud security posture management (CSPM), the spectrum has expanded over the years to encompass the software-as-a-service (SaaS) world (SSPM) and, even more recently, data (DSPM). That it now also extends to applications with ASPM is no surprise, but it does present more of a challenge when it comes to defining this new capability.

In all the other cases, the SPM flavor in question emerged where there had not previously been an established technology:

- CSPM arose to address the need to find issues in cloud-native workloads before they were discovered and exploited by threat actors.
- SSPM did the same thing for SaaS apps, where of course the security requirements are more restricted (basically relating to the data residing in the app and the access rights that have been granted to it).
- DSPM applies the same logic to data stores, primarily ones held in the cloud, though some vendors extend that to the on-premises environment as well.

In all three cases, the *modus operandi* is to start with discovery of the assets in question, whether cloud workloads, SaaS apps in use within the organization, or the data stores that its employees have set up (which in the cloud can be spun up and populated at a moment’s notice). From there, a complete inventory of the assets is put together, after which it is analyzed for issues, which may be vulnerabilities, misconfigurations, or excessive permissions.

The SPM vendor then brings to bear a mixture of rules and artificial intelligence / machine learning (AI/ML) to prioritize those issues, with a view to helping security teams know where to start on what may be an extensive list, based on the criticality of the problems that have been identified. The platform then also proceeds to suggest remedial action for those most critical issues.

Inventory, analysis, prioritization, and recommendations

In other words, SPM posits a proactive approach to security, identifying issues before they have become a problem. All its various flavors have in common this workflow of inventory, then analysis, prioritization, and recommendations.

In the case of ASPM, on the other hand, there were already multiple AppSec technologies in existence before its emergence, all of them dedicated to finding and alerting on issues in application code.

This is due to a huge variety of programming languages, models, and increasingly sophisticated and distributed environments. The growing need for systematic testing through the development pipeline and into operations has led to the availability of many tools for security testing and exercising of code elements across the entire software supply chain, as outlined in the Omdia report *Omdia Market Radar for Next-Generation Application Security: Pipeline (Pipeline NGAS)*. There was a veritable alphabet soup in the market even before this latest addition. It includes such platforms as

- The application security testing (AST) tool spectrum, of which the static (SAST), dynamic (DAST), and interactive (IAST) are the most well-known, which analyze the code itself for potential vulnerabilities
- Software composition analysis (SCA), an outcrop of SAST designed specifically to address issues in open source software and the requirement for software bills of materials, which both investigate the supply chain and assembly of software elements
- API security tools, which identify all APIs used in the development pipeline, assess how they will work when software is deployed, and monitor them during production
- Infrastructure-as-code (IaC) checking, which inspects how the infrastructure to be used by an application (for example configurations, templates, variables, files, and modules), fits with security policies

The upshot of this situation is that there is no shortage of tools for finding security-related problems in application code, so software development and operational teams can be overwhelmed by potential vulnerability issues needing attention.

Context to gauge criticality

Paring this down to a manageable challenge requires further contextual analysis based on business impact, likelihood of occurrence, risk appetite, and the resources required to fix a problem. This contextual analysis combines information from both the development pipeline and operational runtime with business and organizational criteria.

Some ASPM tools are designed to rely on the output from other AppSec platforms, ingesting it for analysis and prioritization based on the riskiness of the issues raised. Their vendors tend to stress their abilities in gauging risk as the key value they add to the equation, not to mention the fact that they enable customers to continue using their existing AppSec tools. Others offer a broad suite comprising elements including

testing, analysis, visualization, and prioritization. In all cases the key ASPM capabilities are seen as reducing overload and focusing on the most important and worthwhile AppSec issues to address.

Reachability

Risk, of course, relies on an awareness of the overall context in which the issue detected exists (i.e., whether the application in question handles sensitive information, whether a vulnerability is exploitable, and critically, how reachable it is from the outside world). If it meets these criteria, clearly any issue with that app should be prioritized.

An analogy here is with the vulnerability management sector, long dominated by the big three vulnerability scanner vendors: Qualys, Tenable, and Rapid7. In the middle of the last decade, however, new names such as Kenna Security and RiskSense (acquired in 2021 by Cisco and Ivanti respectively) emerged to offer prioritization of the lists of vulnerabilities found by any of the scanners.

Posture management equals proactive security

The end goal of using ASPM, like any other SPM tool, is to make proactive changes that improve the security posture. ASPM offers the potential for clearer visualization of security issues that can be understood by developers, operational teams, and business management alike. This broader context allows prioritization based not only on the software assets and vulnerabilities involved but also on the resources required to remediate.

An additional concept worth highlighting in ASPM is the notion of attribution. This term is widely used in cybersecurity, but it normally refers to the ability to pin the blame for a piece of malware on a particular threat actor, such as a specific ransomware group or hacker collective. In the context of ASPM, on the other hand, it is used to mean the identification of individuals or development team responsible. This is an important capability, particularly in large organizations where development teams can run into the hundreds and even, in some cases, thousands and span right across the entire software supply chain.

Product/service overview

Cyscale was using the ASOC denomination for its overall platform before the ASPM category came along. As things stand today, the platform is known as Cyscale Complete ASPM, the constituent elements of which are

- **Application Security Testing**
 - **Static application security testing:** the doyen of application security testing, dating back to the 1990s as an approach to securing code after SQL injection became an established attack technique, SAST analyzes an application from the inside, examining source code, byte code, and binaries for coding and design flaws while the app is inactive.
 - **Software composition analysis:** emerging in the 2000s as an offshoot of SAST for a specific subset of code application code, SCA focuses on finding vulnerable open source dependencies and alerting security teams so that they can be remediated.
 - **Infrastructure-as-code security:** with ever more development teams relying on the ability to define the infrastructure within which the apps they write will run, this is technology that finds misconfigurations in the IaC code they write using tools such as Terraform, CloudFormation, and Kubernetes. It also compares IaC configurations with

those in production to identify drift, finding situations where configurations are no longer aligned and are operating in an insecure way. It then alerts the right teams so these environments can be fixed.

- **Container image security:** Cymode’s container image security focuses on safeguarding containerized applications by scanning container images for vulnerabilities, misconfigurations, and compliance issues.

- **Pipeline Security**

- **Secrets scanning:** developers rely on secrets to access code, repositories, and so on, and this AI-backed tool detects secrets residing anywhere in the software development lifecycle (SDLC), including ticketing, documentation, and messaging tools. This enables an organization to remove such secrets to reduce its attack surface before pushing the code into production.
- **Source control and CI/CD security:** the idea here is to provide a single place from which the organization can manage both governance and security policies across the entire SDLC, which in large organizations can often entail several teams using a wide variety of tools. To this end, Cymode deploys its CI/MON (pronounced “simon”) technology, a lightweight eBPF runtime security sensor for detecting and preventing real-time threats against a customer’s CI/CD pipeline.
- **Source code leakage detection:** this is the reactive dimension of the platform, designed to detect suspicious behavior and identify when proprietary code is exposed to attack.
- **CI/MON:** a runtime security agent leverages eBPF technology to monitor activities within the kernel in order to prevent unauthorized access and mitigate sophisticated attacks in real time.

- **Posture Management**

- **ConnectorX:** the tool offers the ability to connect to third-party sources of data so that it can be ingested by Cymode.

- **Risk Intelligence Graph (RIG)**

- Cymode Risk Intelligence Graph is a discovery graph that connects and correlates a customer’s environments and alerts across the SDLC. It provides prioritization, designed to filter out noise and enable security teams to focus on the most urgent vulnerabilities.

The Cymode Complete ASPM platform takes the output of all these individual tools, correlates it, and applies analytics to determine which issues should be prioritized, providing security teams with the context necessary to understand its decision. It also recommends what the remedial action should look like, with that feedback in ticketing systems and/or in the integrated development environment that the developer in question is using. In the case of an open source software vulnerability detected by the SCA component, the platform can open a pull request for the purpose of remediation.

ConnectorX for third-party integrations

Of course, Cymode does not expect its technology to exist entirely in homogeneous environments. For this reason, the vendor has multiple integrations with other tools in each of the categories included within its portfolio and in some additional ones that it does not cover, such as dynamic application security testing (DAST).

To ease such third-party integrations, in November 2023 Cymode launched a tool called ConnectorX, which it describes as a “click-and-connect” facility. Among the vendors to whose platform it enables a connection, Cymode lists the likes of JFrog, Snyk, Orca, Wiz, SonarQube, and BlackDuck (part of Synopsys though currently up for sale as that vendor exits the software security market).

Company information

Background

Cymode was founded in 2019 by CEO Lior Levy, CTO Ronen Slavin, and VP of R&D Dor Atias. Levy’s prior career includes time as a solutions architect at Symantec and, before that, as head of mobile and presales engineer at Merlinx, a provider of cyber-intelligence solutions for law enforcement, intelligence agencies and national security organizations. He was also cofounder and CTO at Babel5, a mobile entertainment platform developer.

Slavin previously held leadership roles at Reason Cybersecurity, which develops technology for the consumer market, and before that was cofounder and CTO at FileLock, a security vendor acquired by Reason. Atias held R&D management roles at CA Technologies and then at Broadcom after it acquired CA in 2018. All three men also have Insider status at Israeli venture capital firm YL Ventures.

Cymode has raised a total of \$81m, most recently announcing a \$56m Series B round in November 2021, led by Insight Partners with YL also taking part.

Current position

Cymode delivers its platform in SaaS mode by default. However, it also offers an air-gapped version for on-premises installations, designed to meet the requirements of customers that cannot embrace cloud services. This ability to deploy on-premises further enables the vendor to address hybrid environments such as organizations whose source code management platform resides on their premises or, at least, behind their corporate firewall.

Cymode targets the enterprise and midsize segments of the market, boasting a customer base that today includes Ford, UBS, Paypal, Cisco, and Equinix. It has customers around the world with a particular strength in North America and Europe. Its go-to-market is still primarily direct.

The charging mechanism for Cymode’s technology is a subscription-based model; the size of the subscription is calculated based on the number of developers using the platform within an organization and on the number of Cymode capabilities the customer is using (i.e., whether Cymode is doing all the scanning or ingesting from third-party tools).

The vendor has three primary SKUs for its offering:

- AST only, which comprises all Cymode’s application security testing capabilities (i.e., all the scanners)
- ASPM Pro, which is just the pipeline security and posture management capabilities
- ASPM Ultimate, which combines all the tools together for the complete ASPM portfolio

As for its competitive landscape, though a lot of vendors are now using the ASPM initialism as part of their marketing, Cymode considers two companies in particular to be closest to its own approach, that is, offering

a complete set of scanning capabilities plus all the aggregation, correlation, and prioritization of their output. These are Apiiro and Legit.

Future plans

To guarantee the comprehensiveness of the platform's coverage, Cycode is adding more third-party integrations as one would expect. It reckons that, by the end of the first quarter of 2024, it will have 99% of the requirements for such integrations covered.

Beyond that, the vendor is looking at the addition of AI-based functionality to its platform, and to this end it is currently building the necessary data models. Part of this will be to strengthen its scanning capabilities, training ML models to identify anomalous patterns in code and so on. Another part will entail generative AI, which the company plans to harness to underpin developer workflows for remediation.

Key facts

Table 1: Data sheet: Cycode

Product/service name	Cycode ASPM	Product classification	Application security posture management (ASPM)
Version number	n/a	Release date	February 2022
Industries covered	All	Geographies covered	Global, with North America and Europe particularly strong
Relevant company sizes	Enterprise and midmarket	Licensing options	Subscription with per developer pricing
URL	https://cycode.com/	Routes to market	Mainly direct
Company headquarters	San Francisco, California, US and Tel Aviv, Israel	Number of employees	100+

Source: Omdia

Analyst comment

It was a logical step for the proactive security approach known as posture management to be extended beyond cloud-native workloads, SaaS, and data into applications. The rate at which new application code is being developed and pushed into production is such that AppSec is not just a key part of an organization's security tool kit but also an increasingly complex one. The AST spectrum of technologies continues to grow as the likes of IaC and API security become urgent requirements in their own right. Just as happened with other areas of enterprise infrastructure, the alerts are often so many and varied that security teams risk being overwhelmed and, as a result, missing the essential needles in a burgeoning haystack.

Thus, technology that can aggregate all the scanners' output, correlate it, prioritize critical alerts, then apportion responsibility for remediation with suggestions of what should be done will play an ever more critical role going forward. This is, in essence, the promise of ASPM.

There is currently something of a dichotomy in this market between those vendors that offer the aggregation, correlation, and prioritization capabilities without their own scanning, essentially proposing to work with any scanners and any outputs, and those that offer an entire soup-to-nuts ASPM platform, even though they too can ingest from third parties.

Cyscale is in the second group, but its ConnectorX capability means it can work with data from many of the most common scanning tools, not only in the development pipeline (JFrog, Snyk, and BlackDuck) but also in the production environment (e.g., CSPMs such as Orca and Wiz).

Omdia sees Cyscale as well positioned in this still emerging market. If anything, the risk to its business model may come from a market development such as the entry of a heavyweight security vendor into the ASPM space. Imagine, for instance, Palo Alto Networks entering the fray, bringing to bear all the might of its marketing muscle, not to mention the huge customer base to which it could upsell an ASPM offering.

For this reason, Cyscale should strive to raise its profile still further in this busy segment, educating the market about its expertise, particularly as it adds more AI-driven functionality to its platform.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

[*2024 Trends to Watch: Emerging Cybersecurity*](#) (December 2023)

[*Blockchain Technology and Adoption Trends*](#) (December 2019)

[*Fundamentals of Next-Generation Application Security for the Dev Pipeline \(Pipeline NGAS\)*](#) (June 2021)

[*Omdia Market Radar for Next-Generation Application Security: Pipeline \(Pipeline NGAS\)*](#) (July 2021)

[*On the Radar: Bionic reverse-engineers binaries for app visibility and security*](#) (March 2022)

[*On the Radar: Kodem offers runtime-informed software composition analysis*](#) (December 2023)

[*On the Radar: Phoenix pins impact, risk, cost, and ownership to app vulnerabilities*](#) (February 2024)

[*On the Radar: Tromzo applies intelligence to model and visualize AppSec criticality and responsibility*](#) (February 2024)

[*"CrowdStrike dives in proactive AppSec with \\$350m Bionic purchase"*](#) (September 2023)

Author

Rik Turner, Senior Principal Analyst, Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com