Forgepoint

2025 Q1 Report

/ Forgepoint Forward /

What's Ahead in Application Security Posture Management (ASPM)

Table of Contents

2 Introducing Forgepoint Forward

3 The State of Application Security

4 Challenges

6 The Opportunity for ASPM Startups

9 Trends

12 What CISOs Want

15 Final Thoughts on the Future of ASPM

16 Acknowledgements

18 Endnotes

> “*They [developers] don’t care about dashboards, pretty pictures. Tell us what I need to fix, make sure that it is validated, so that I can add it to the next sprint and be done with it…Tie in the developer community – create an ecosystem where developers can know who is fixing vulnerabilities, so that it is a little bit faster.”*

Jerry Kowalski

CISO, Jefferies

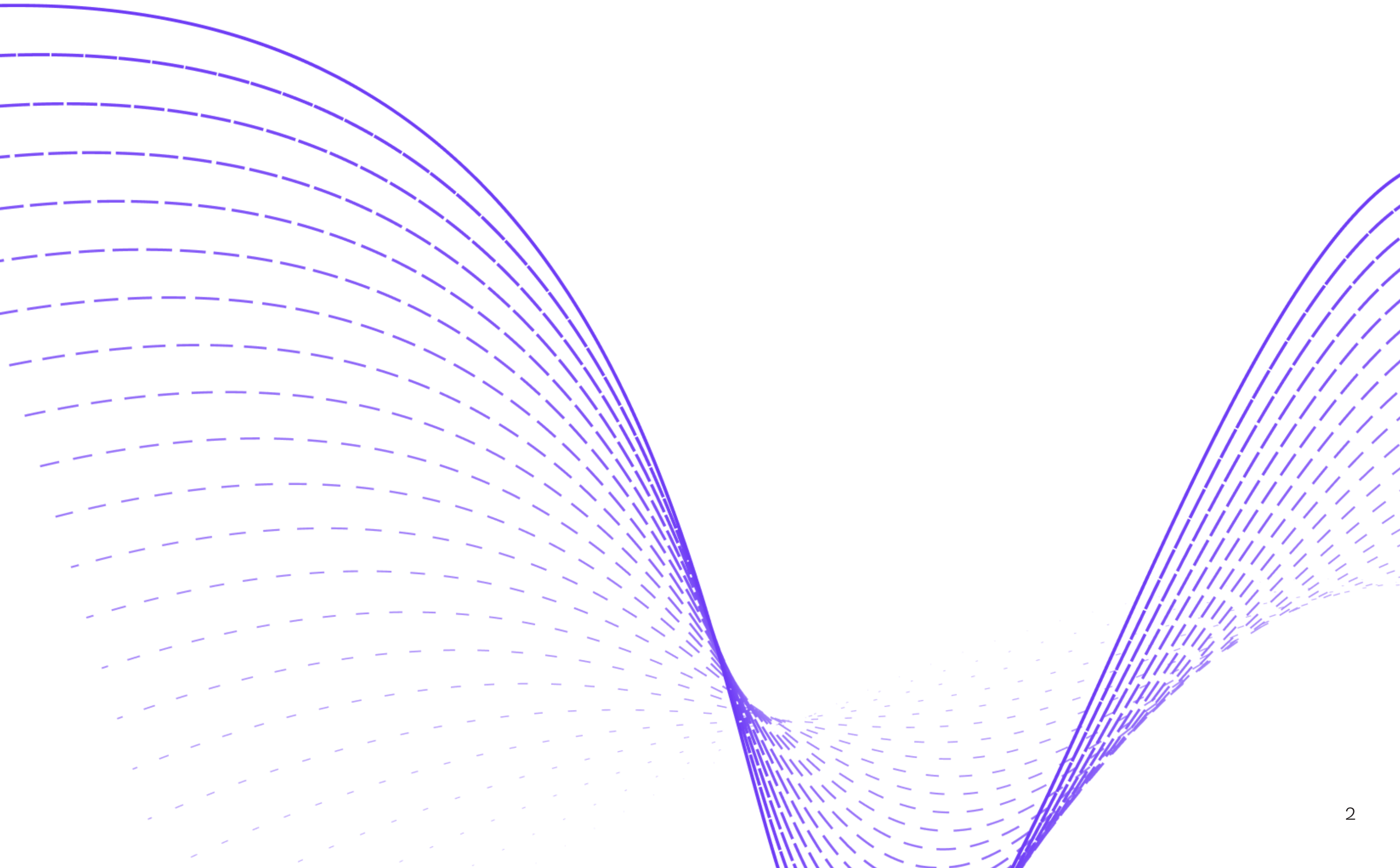
Introducing Forgepoint Forward

In today's rapidly evolving digital landscape, the role of cybersecurity has never been more critical. Modern organizations navigate a complex threat environment, often relying upon big tech partners and legacy solutions, but still face critical security gaps. These gaps represent risks and opportunities – the linchpins of cybersecurity innovation, software development, and economic progress.

As longtime investors, operators, and company-builders with decades of experience in cybersecurity, the Forgepoint Capital team has the privilege of collaborating with a deep network of CISOs, CIOs, CEOs, industry experts, and national security leaders. These individuals are at the forefront of defending against cyber threats, implementing robust security postures, and fostering organizational and industry resilience.

What follows is the second edition of Forgepoint Forward, a series of quarterly reports on the most critical emerging spaces in cybersecurity, artificial intelligence, and infrastructure software. Forgepoint Forward presents our findings from extensive research and interviews with experts across our network- including our Global Advisory Council. Our goal is to highlight investment trends and market projections, as well as startups involved in promising areas, to identify key opportunities for entrepreneurs and the cybersecurity community.

We would like to extend our thanks to everyone in our community who shared their insights and contributed to this report. A full list of contributors can be found at the end of this report under Acknowledgements.



The State of Application Security

For many enterprises, shift left has become an integral part of securing the software development life cycle (SDLC). Security testing is happening earlier and more frequently throughout the development process, aligning with a growing demand for vulnerabilities to be discovered before they can be exploited in production runtime environments[1]. DevSecOps, the integration of security in development, is maturing as a discipline: half of organizations currently implement DevSecOps and an additional 31% are working towards implementation, according to a 2023 Gartner survey[2].

At the same time, application security faces headwinds. Modern software development necessitates speed and innovation, and application security management- including secure-by-design principles advocated by the Cybersecurity and Infrastructure Security Agency (CISA) and DevSecOps practices- must keep up with the pace of business. Meanwhile, a proliferating number of applications is also expanding the attack surface.

What concerns do CISOs have regarding their Application Security Posture?

CISOs, CEOs, and other experts in the Forgepoint community identified several persistent challenges in securing applications and the software development process:

- An imperfect dynamic between security and developer teams
- Vast amounts of false positives necessitate the manual validation of alerts and findings
- Tool sprawl creates an overwhelming number of vulnerability alerts, making it more difficult to interpret findings

“

Software developers have long been the first line of defense against threat actors, but they are sent to battle with little knowledge, inadequate tools, and KPIs that are at odds with AppSec goals and outcomes. The contemporary CISO needs to focus on the strategic elimination of core categories of vulnerabilities rather than a continuous loop of putting out spotfires.

This requires a preventative, positive security culture, data-driven assessment of problem areas, and security-skilled developers that are aligned with top-down enterprise security goals.”

Pieter Danhieux

CEO, SecureCodeWarrior

Challenges

1) Legacy Application Security Testing (AST) methods slow down production.

Legacy secure coding practices include reviewing source code, documenting and reporting identified vulnerabilities, and remediating issues. Each of these steps can slow down production - a phenomenon referred to as the productivity tax. Manual application security testing at the end of the SDLC leads to delays and frustrations for software engineers, who prioritize reducing mean time to remediation (MTTR)[3] and quickly push and deploy code.

Without secure coding policies at scale, software engineers may then cut back on security measures to meet deadlines. Achieving speed at the expense of security, however, can leave enterprise applications vulnerable to threats and create friction between security and development teams.

> “
>
> *At the core of the AppSec problem is the mindset of the engineer. The business drives them to produce at a certain pace, so they do not make security matters a focal point within the development journey.”*

Andres Andreu

Deputy CISO, Hearst

> “
>
> *There has to be trust between security and developer teams... nobody wants to waste time.”*

Jerry Kowalski

CISO, Jefferies

2) The problem of vulnerability alerts is overwhelming.

Organizations rely on more software than ever to facilitate and expedite internal and customer-facing processes. Security teams tackle an ever-expanding[4] attack surface and, subsequently, a rapidly growing number of vulnerability alerts from application security tools. False positives are rampant, contributing to alert fatigue, especially within large enterprises. Security teams must manually validate vulnerabilities and determine which issues they are equipped to resolve—a time-consuming process.

There is a need for security methods that identify a more manageable number of true positive vulnerabilities. At the same time, there needs to be greater trust that software engineers will remediate issues properly.

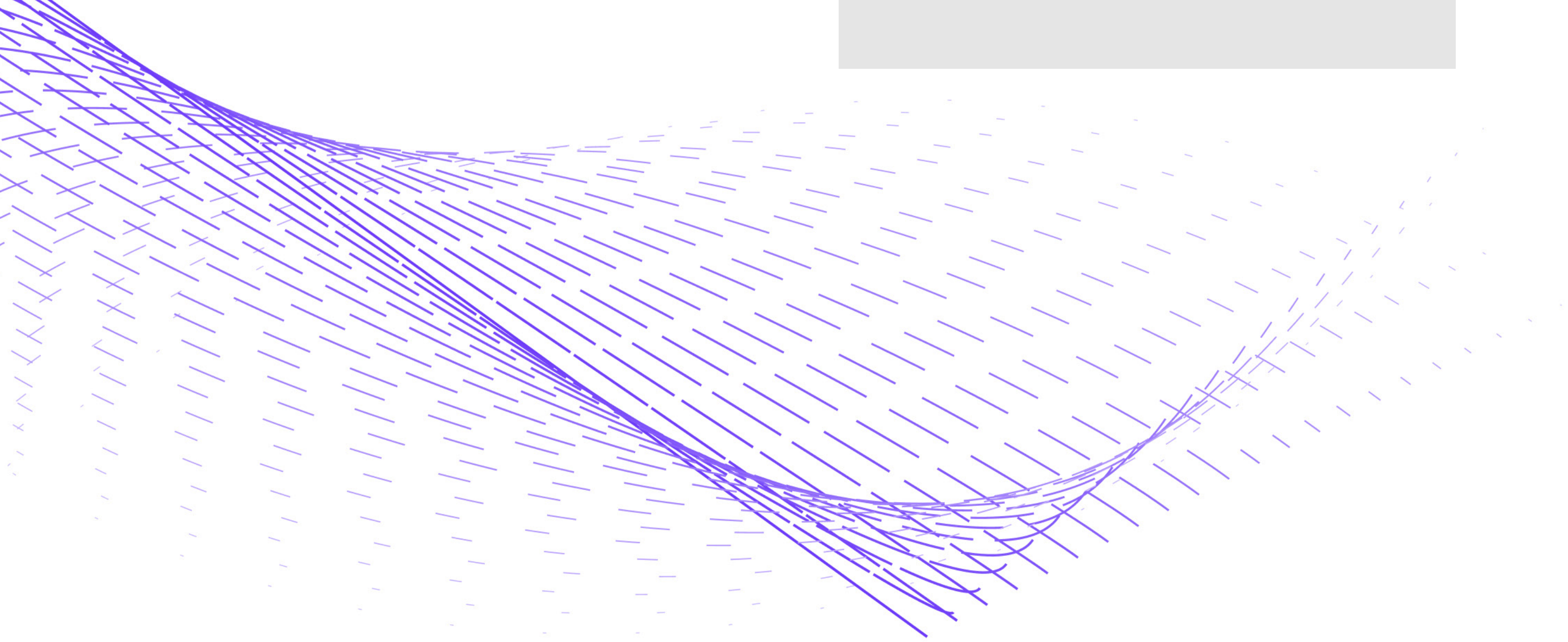
3) There is a lack of unified visibility and oversight.

According to Gartner, 37% of organizations use AppSec products from 10-20 different security vendors[5]. Teams within the same company may inconsistently utilize AppSec testing tools, creating a widespread lack of oversight. These tools must be comprehensively managed and implemented to enable real-time vulnerability detection and visibility. Modern organizations benefit from process automations which correlate and deduplicate data from various sources, rationalize findings, generate reports, and provide consolidated data oversight.

> “
>
> *Developers and security teams would be well served to establish detailed security standards regarding what is required to promote an app to production. That makes it easier for everyone to know what needs to be fixed now vs backlog vs acceptable risk which means the process moves faster and automatically provides proof of reasonable care. It also makes it possible to hold vendors accountable to delivering quality products with low false positive rates.”*

Alan Snyder

CEO, NowSecure



The Opportunity for ASPM Startups

Innovative Application Security Posture Management (ASPM) startups have emerged to solve these pain points by correlating AppSec vulnerability alerts to visualize the entire secure software development life cycle (SSDLC)[6]. These ASPM tools present a powerful way for enterprises to better inform and implement their AppSec strategies. Gartner predicts that ASPM will become transformational and will reach mainstream adoption in the next 2-5 years[7]. ASPM startups have an opportunity to fill the existing gaps in observability, streamline alert management, and promote stronger security-developer collaboration.

ASPM Market

A number of ASPM startups have entered the market landscape. Many of these startups- categorized by their initial commercial strategies in the map on page 7- now operate in numerous areas within ASPM, offering vulnerability management, alert prioritization, code remediation and workflow enhancement capabilities. While most ASPM tools aggregate alerts, some focus on specific segments such as remediation and prioritization.

> “
>
> *What ASPM tools are doing is starting to bridge the gap between security and software engineering in a way that facilitates safer coding...They are providing a more seamless experience for a software engineer to introduce safer mechanisms in their code. This is about creating a safe set of business practices as opposed to just a set of business practices.”*

Andres Andreu

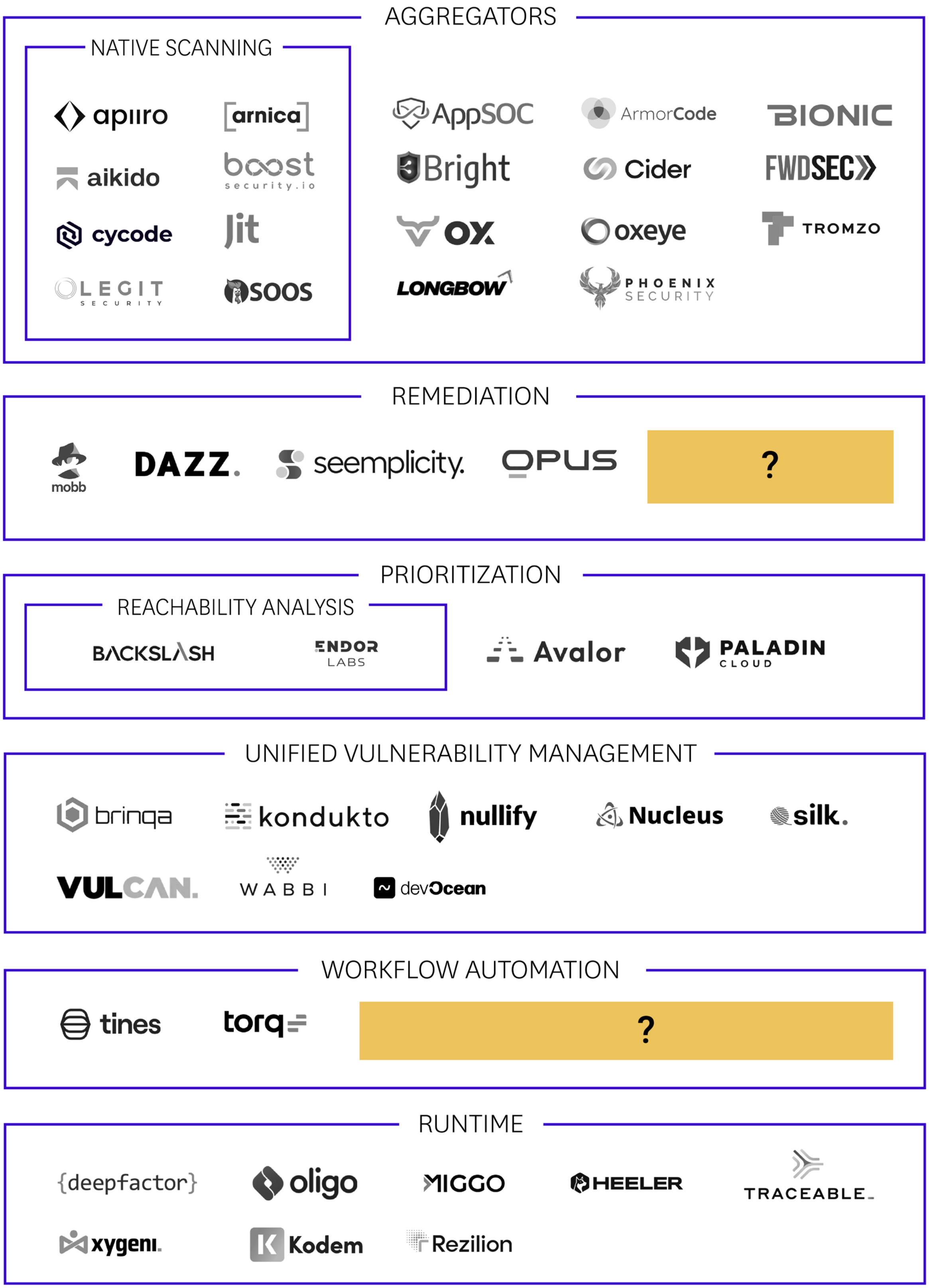
Deputy CISO, Hearst

What does a successful ASPM tool offer?

Our community of experts identified several key traits that define a successful ASPM tool:

- Reduces the volume of security incident alerts and tickets agents to facilitate clearer threat environments.
- Offers customized remediation and prioritization processes.
- Utilized and liked by developers.

ASPM Market Map



AGGREGATORS

NATIVE SCANNING

apiiro

arnica

aikido

boost security.io

cycode

Jit

LEGIT SECURITY

SOOS

AppSOC

ArmorCode

BIONIC

Bright

Cider

FWDSEC

OX

oxeye

TROMZO

LONGBOW

PHOENIX SECURITY

REMEDIATION

mobb

DAZZ.

seemplicity.

OPUS

?

PRIORITIZATION

REACHABILITY ANALYSIS

BACKSLASH

ENDOR LABS

Avalor

PALADIN CLOUD

UNIFIED VULNERABILITY MANAGEMENT

brinqa

kondukto

nullify

Nucleus

silk.

VULCAN.

WABBI

devOcean

WORKFLOW AUTOMATION

tines

torq

?

RUNTIME

{deepfactor}

oligo

MIGGO

HEELER

TRACEABLE

xygeni.

Kodem

Rezilion

Forgepoint

ASPM Market

Here is how we define each of these categories:

1) Aggregators provide an overview of an enterprise's applications and critical AppSec risks. They typically integrate with legacy code-scanning or open-source scanning testing tools (Tromzo, Armorcode), though some platforms can alternatively replace them with native security tooling (Arnica, Cycode). Startups in this space promise real-time application observability and offer integrations into developer workspaces.

Though once distinct from cloud-native application protection platform (CNAPP) platforms, many ASPM aggregators have started to offer cloud infrastructure, container, and physical infrastructure risk management capabilities. This consolidation of cybersecurity platform offerings is blurring the lines between CNAPP and ASPM as legacy vendors and startups that were initially aggregation tools now promote all-in-one "code-to-cloud" products.

2) Remediation tools accelerate the process of risk remediation by providing guidance and possible fixes in a unified platform (Seemplicity, Dazz). These tools may offer AI-powered automated remediation (Mobb.ai). Many remediation-centric startups self-define as vulnerability management tools rather than ASPM.

3) Prioritization and Triage providers prioritize vulnerabilities and inform remediation strategies in a variety of ways, including with agentless tools and AI-based capabilities. Certain vendors utilize reachability analysis to identify exploitable risks by investigating the context behind how the vulnerable function is used[8]. Risk scores- which may be coded into the product or customized for each customer (Avalor)- are generated according to the impact of a vulnerability to an industry or a business.

4) Unified Vulnerability Management platforms provide a dashboard for customers to view correlated findings in one place. They often integrate threat intelligence and contextual analysis to generate customizable reports that communicate risk and ensure compliance. Certain vendors also identify code owners and assign remediation tickets from tools like Jira or ServiceNow (Vulcan Cyber).

The following categories can be considered ASPM-adjacent:

5) Workflow Automation tools help companies build and implement secure, consolidated workflows. They focus on promoting speed and efficiency for security and engineering teams. These tools unify workflows and processes across an organization and integrate security tools throughout the SDLC based on company policies. Automation/orchestration tools can also be considered a part of Security Orchestration, Automation, and Response (SOAR), and may be no-code, plug-and-play style solutions.

6) Runtime Solutions prioritize vulnerabilities by determining which are exploitable in runtime depending on the user's environment. These tools build on application contextualization by analyzing what components are being used – specific code blocks, functions, methods, and symbols -- and how data flows within them[9]. Some providers offer agentless products (Rezilion) while others user agents.

Trends

1) Converging solutions

While many ASPM startups initially focus on a specific area (prioritization, remediation, automation and orchestration, etc.), platform expansions are becoming more common as ASPM tools begin to cover various functional categories and tap into adjacent markets.

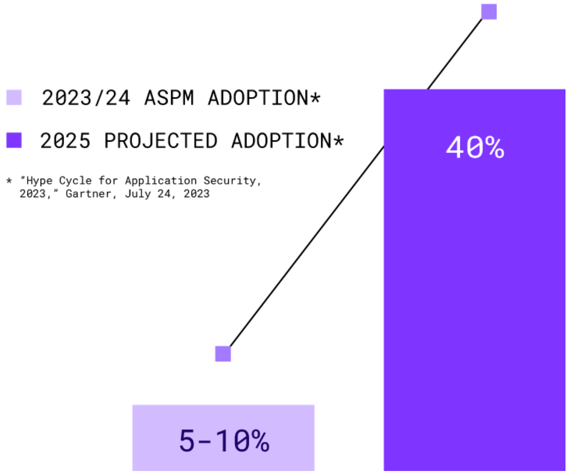
This platform expansion is being driven by customer-focused product development, as customers with good working relationships ask their current providers for solutions to additional pain points. For example, more startups are beginning to develop the ability to send customized reports to team leads or create customized risk score assessments. ASPM platforms are also starting to generate Software Bill of Materials (SBOMs) or do Software Composition Analysis (SCA). While Application Security Posture Management (ASPM) vendors are starting to offer basic capabilities in software supply chain security, companies like ReversingLabs provide advanced solutions that specialize in comprehensive binary analysis, enabling full decomposition of complex binaries of any size, file type, complexity, or extension. Uniquely capable of handling both open-source and commercial binaries, ReversingLabs delivers accurate SBOMs and unparalleled insights into software security, a space which ASPM vendors are now working to close the gap and participate in as well.

2) An increasingly crowded market

In our view, the ASPM market's growth potential is undermined by the sheer volume of startups in the space. New entrants are enticed by accelerated market adoption of the novel 'ASPM' term (once referred to as ASOC- Application Security Orchestration and Correlation). To ride this momentum, they have stitched together point solutions and market themselves as a platform under the ASPM umbrella. In addition to creating a noisy market, this has made product differentiation more difficult in the eyes of both customers and investors.

3) Slow but growing adoption rate

ASPM's current market adoption rate stands between 5-10%. This less-than-expected number shows that it is still an adolescent space, especially compared to SCA's maturity and 50%+ market penetration. However, the pace of ASPM adoption is likely to accelerate. Gartner predicts over 40% of organizations will adopt ASPM by 2025[10].



* "Hype Cycle for Application Security, 2023," Gartner, July 24, 2023

While some organizations are looking to third party ASPM providers, certain organizations have been working to build risk dashboards to solve similar pain points. Those building these capabilities in-house to fill gaps in their AppSec programs will now choose between using these in-house dashboards to view things on top of an ASPM solution or integrate the two somehow.

The portion of a company's security budget dedicated to AppSec varies depending on the number of customer or internet-facing applications they deploy. However, the CISOs we spoke with forecasted increases in their AppSec budget spend to onboard management tools like ASPM.

Decision-makers tend to measure return on investment by the average number of vulnerabilities per device and the sum and/or severity of resolved vulnerabilities prior to production. Thus, enterprise customers will likely pick ASPM tools with proven track records that demonstrate high accuracy, minimal time to validate issues, and a reduction in application-related incidents.

4) Frequent acquisitions and looming legacy vendor presence

Prominent legacy vendors offer a wide array of products in the Application Security space. Static Application Security Testing (SAST) and Source Code Analysis (SCA) are mature market segments, and large enterprises tend to utilize one or more vendors from these areas.

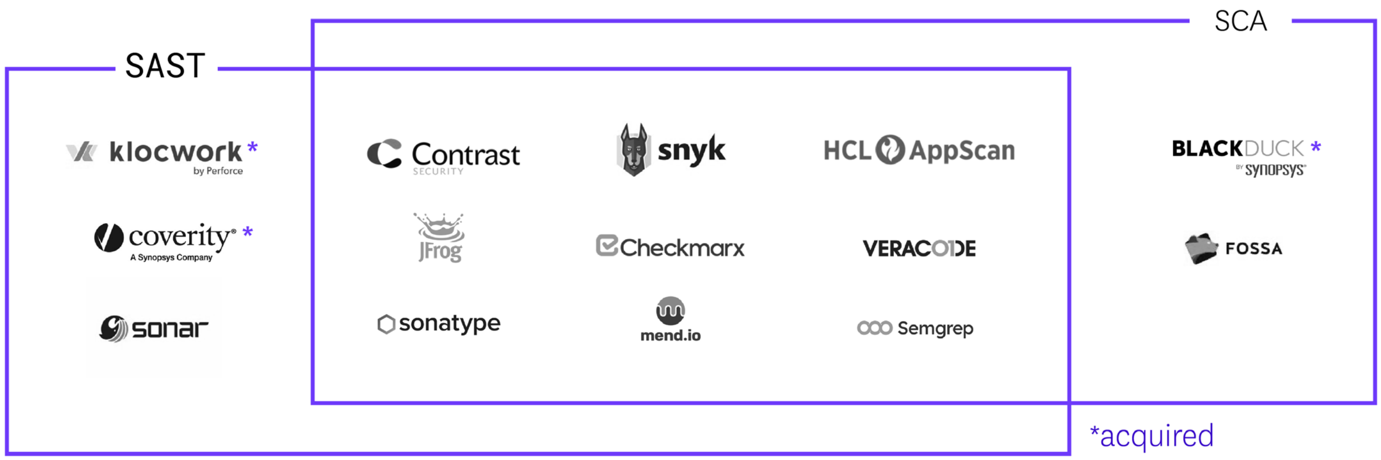
Legacy vendors such as Checkmarx and Veracode already examine code in the development process, but their end users are largely underutilizing their tools and customers have little attachment.

> “
>
> *Security scanning is not just for bugs; it is also about importance. You must start measuring the number of application incidents going down.”*

Jerry Kowalski

CISO, Jefferies

Legacy Vendors



> “
>
> *Adoption of security tools is not where it needs to be – developers choose not to use them. The tools that you have, if adoption is just 10%, it does not matter.”*

Jerry Kowalski

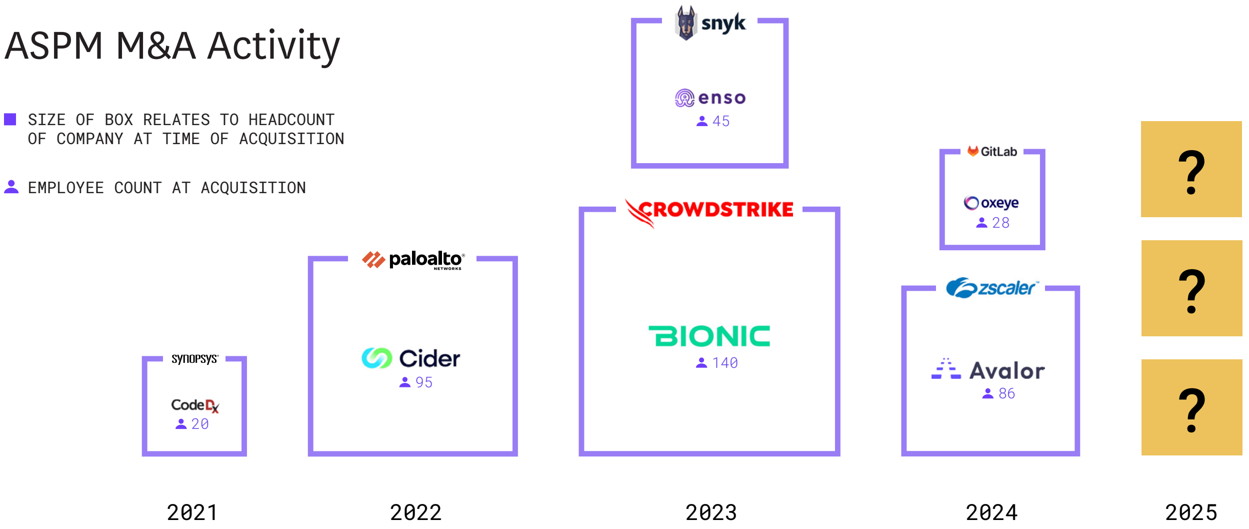
CISO, Jefferies

As a result, large vendors have begun entering an already crowded ASPM space. Traditional AST vendors have acquired startups with ASPM solutions to fill the gaps in their product portfolios.

Synopsys was one of the first legacy players to incorporate ASPM into their portfolio with the acquisition of Code Dx[11] in 2021 to provide a consolidated view of correlated vulnerability data and risk reporting. Other large vendors also foresaw the need for ASPM before the commercial market was established and developed their own solutions; for example, Checkmarx announced Fusion, an automated remediation product, in June 2022[12].

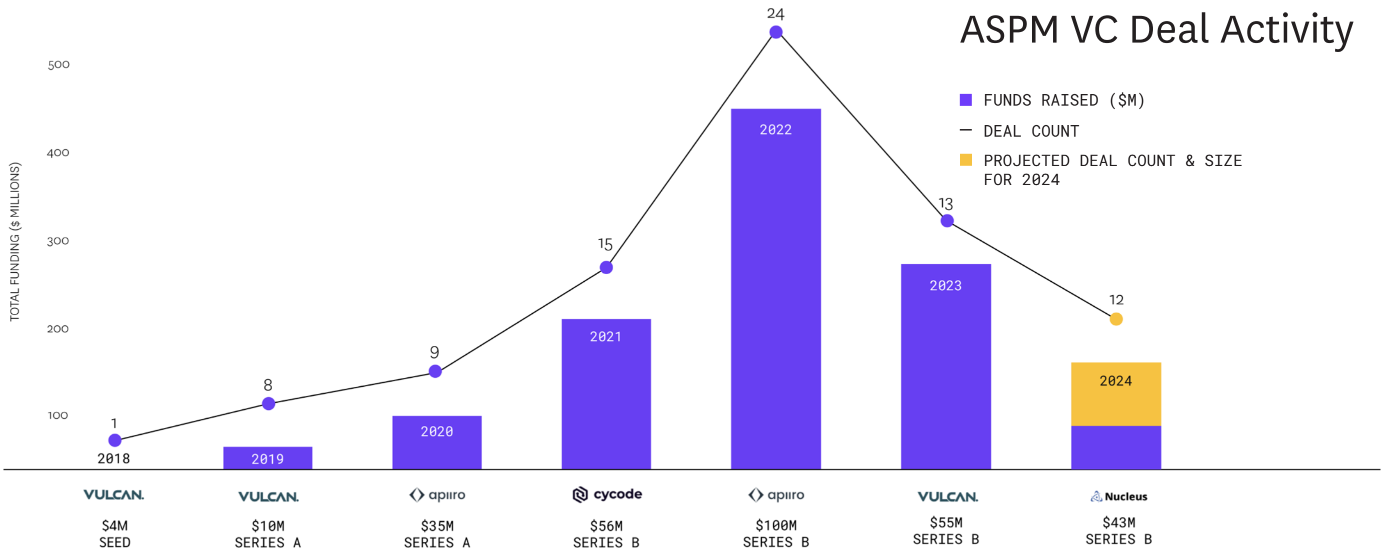
Other notable market movements have occurred in just the past year. In June 2023, developer security provider Snyk acquired Enso Security to help security teams scale AppSec programs[13] and a few months later launched ASPM product Snyk AppRisk[14].

ASPM M&A Activity



We predict significant market consolidation as more legacy vendors acquire early-stage ASPM startups, a trend most recently shown by CrowdStrike's acquisition of Bionic in 2023[15] along with Armis's acquisition of Silk Security's[16] and Zscaler's acquisition of Avalor in 2024[17]. Vulnerability management vendors such as Qualys and Tenable and cloud security providers like Wiz and Palo Alto are likely to enter the ASPM space via acquisitions.

Enterprises tend to prioritize AST/code scanning vendors over management tool providers, giving legacy vendors with more comprehensive offerings an edge over ASPM startups and making acquisition the most likely startup exit strategy. ASPM startups vastly outnumber potential acquirers, so we expect competition for acquisitions to be intense: a fight to differentiate while battling over leftover market share. Investors have taken note. 2022 was a record year for ASPM VC funding, with 24 deals totaling around $383 million. In the two years since, funding to ASPM startups has dwindled as legacy vendors ventured into the market.

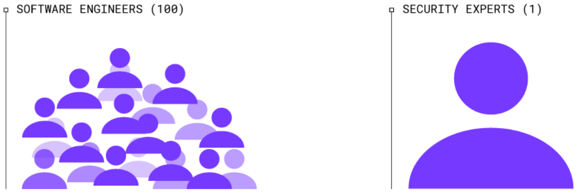


What CISOs Want

1) Developer-oriented tools can improve ASPM adoption

As more AppSec responsibility is shared between security and software engineering teams (54% of software engineering leaders surveyed by Gartner are directly responsible for application security)[18] developers are increasingly part of product security decisions. The number of software engineers in a company often vastly outnumbers security experts – according to a survey conducted by Software Development Times, this ratio is around 100:1. Startups are not just selling products to a security audience: they're selling to engineers[19].

Enterprises want to significantly improve adoption amongst their developers to get the most out of their AppSec tools. We perceive a growing demand for tools that not only incorporate but further expedite agile development methods. Enterprise customers are looking for ASPM that facilitates an ecosystem of visibility. This includes capabilities such as assigning validated vulnerabilities to the right person for remediation and enabling developers to see who has resolved an alert, when, and how, to avoid rediscovery.



100:1 RATIO OF SOFTWARE ENGINEERS TO SECURITY EXPERTS IN LARGE COMPANIES

ASPM platforms do not need to have flashy GUI (Graphical User Interface) or feature-rich dashboards. They should minimally disrupt an engineer's workflow and streamline the AppSec tool onboarding and training processes for software engineers and developers. Enterprise customers are also seeking vulnerability management which is seamlessly interwoven with integrated development environment (IDE) plugins or configuration management databases (CMDB)[20] (Bionic (acquired), Armorcode) to bring the AppSec environment closer to where developers work day-to-day.

In particular, demand for automated and streamlined remediation products is likely to grow. Early adopters of ASPM technology tend to be groups with mature DevSecOps programs and highly involved engineering teams; startups have an opportunity to tailor their messaging to appeal to interested non-cybersecurity audiences such as these. For example, Tines has been particularly successful in positioning its solution as a kitschy product which appeals to the developer crowd compared to its workflow automation competitor Torq, which appeals more to a CISO and executive audience given its greater focus on security analytics and lower technical requirements.

Gearing ASPM tools to a developer audience will help newcomers and established vendors alike achieve greater product-market fit and improve adoption. The bottom line: companies should not have to re-market their tools to developers. ASPM providers that appeal to developers will be on enterprise buyer wishlists.

> *"The point of AppSec is to make secure code. Who makes that secure code? Developers. The tools have to be for developers, not security teams."*

Jerry Kowalski

CISO, Jefferies

Higher adoption rates will enable security leaders to better prove the business value of their security programs, retaining and increasing cybersecurity budgets going forward. The bottom line: companies should not have to re-market their tools to developers. ASPM providers that appeal to developers will be on enterprise buyer wishlists.

> “*Instead of having to go research a library that will give me input validation capabilities, I, as a software engineer, just have to make a function call to a library that is now readily at my fingertips. That’s how you start to introduce security mechanisms into software engineering, because now you’re not adding a burden to that person’s day to day.*”

Andres Andreu

Deputy CISO, Hearst

2) Seamless and Comprehensive Integrations

Larger enterprises, especially organizations with mature AppSec teams and diverse development teams that utilize a variety of development tools, highly prioritize an ASPM product’s ability to support legacy applications. Current startup products vary widely in the scope of integrations and levels of functionality.

The expansion of product integrations is a low-effort, high-reward route to attract a larger customer base. Some startups have pursued this strategy already. For example, Armorcode has become known for its broad array of integration capabilities—over 200+-compared to the standard range of 100-150.

The ability to integrate an ASPM product into existing workflows minimizes disruptions and thus apprehension among developer teams. ASPM providers should pursue greater workflow integrations with Integrated Development Environments (IDEs), Command-Line Interfaces (CLIs), and ticketing systems such as Jira to bring their product to end users accustomed to these production environments. Played right, and workflow integrations may serve as an important differentiator.

3) Automated and AI-Assisted Remediation

42% of developers spend between 2 and 12 hours a month on remediation, and an additional 33% said that they spend 12 to 36 hours. However, only a fraction of that time is spent remediating; most of it is dedicated to slow research or consulting needed to understand how to begin[21].

In our view, AI has enormous potential in the realm of remediation. As AI discourse has taken center stage since late 2022, some ASPM startups have introduced or elevated AI Assistants or Security Agents which automate processes to support developers remediate. For example, Mobb.ai uses ‘patent-pending hybrid AI technology’[22]. According to Gartner, 40% of development organizations will use the AI-based auto-remediation of insecure code as a default in 2026, an enormous increase from less than 5% in 2023[23].

> “
>
> *By capturing real-time application behavior and contextual nuances, AI can make smarter, more accurate recommendations. When AI is integrated with deep tracing, it gains the ability to dynamically consider application security risks while offering suggestions or reviewing code. This ensures that AI not only helps developers write efficient code but also proactively addresses potential security vulnerabilities, making the development process more resilient and secure.”*

Elizabeth Lawler

CEO, AppMap

Remediation has been a consistent focus area for CISOs and AppSec budgets. Customers seek solutions that facilitate vulnerability alert prioritization and offer starting points for remediation. In other words, they are looking for tools that identify what should be fixed first given limited time and resources. Additionally, customers are interested in customizable tools that address their unique security needs. AI-enabled remediation solutions can provide these capabilities. That being said, our community of C-suite and security leaders have expressed mixed feelings about automated remediation and processes that enable a developer to simply click and approve a security fix. Despite a tepid initial reception, ASPM providers have stepped up to provide such solutions. Dazz recently garnered attention for their ability to identify code owners and autogenerate suggested code fixes within developer workflows by integrating with ticket management systems like Jira and Github. There has also been a rise in ‘AI copilots’ across the market, which help developers code and remediate issues while providing feedback. However, such ‘secure coding assistants’ have yet to prove adequate accuracy rates, and due to the nature of the technology, remediation will always require security-skilled developers to govern proposed fixes. Tools that support these people amid a talent shortage are a promising area for growth

Overall, the role of AI in Application Security is promising across use cases including prioritization, remediation, workflow automation, and code assistance. In the end, efficient execution will be the true differentiator for ASPM startups- not the mere inclusion of AI.

> “
>
> *It won’t be ‘wow, we invented this new technique called machine learning, or deep learning, or even neural networks. Everyone’s doing that. It’ll be,‘We found a way to use deep learning that works efficiently, and sustainably. The differentiator probably won’t be that they’re doing something different than others. It’s that they’re doing it right.”*

Edward Amoroso

CEO & Founder, TAG Infosphere

Final Thoughts on the Future of ASPM

The broad shift from ASOC (Application Security Orchestration and Correlation) to the more comprehensive ASPM approach to manage application security posture across the entire software development life cycle caused waves throughout the market. Legacy vendors began rebranding and next-gen startups cropped up. Every provider started to promise that their product or platform enabled a stronger Application Security posture. As a result, there is now a large market of ASPM platforms which offer a wide array of AppSec capabilities and attempt to solve mounting needs around AppSec tool sprawl.

Our take on the market: Bearish

We are wary of the sheer number of startups in the ASPM market and short roster of enterprise acquirers. Over the next 2-3 years, we forecast greater consolidation across the board as legacy vendors acquire startups at relatively lower valuations. Startups that manage to avoid early acquisitions may find themselves fighting tooth-and-nail for a small share of a relatively small market. Strong exits may be rare given the convergence of Application Security spaces and decreasing product differentiation.

Here’s what might change our minds:

1) If convergence causes ASPM providers to absorb market share from adjacent AppSec spaces such as AST or SCA.

2) If market penetration can drastically improve from the current 5-10%.

3) If new entrants with less financial backing can still innovate to solve enterprise pain points in Application Security- such as by providing developer-oriented user experience or flexible selections of open source, proprietary, and third-party scanners- and achieve strong exits. Given the increasing AppSec and software supply chain security responsibilities shared between security and engineering teams, we hope to see startups disrupt the ASPM space by capturing the expanding developer mindshare.

CISOs, security teams, and developers alike have unmet needs which thoughtful and innovative ASPM providers can address. We are eager to see how the ASPM market continues to play out.

Acknowledgements

Special thanks to the following cybersecurity leaders and pioneers for their insights and contributions. If you are a startup interested in meeting with Forgepoint, or would like to be interviewed for future editions of Forgepoint Forward, please contact Rey Kirton at rkirton@forgepointcap.com.

Dr. Edward Amoroso
CEO & Founder, TAG InfoSphere

Andres Andreu
Deputy CISO, Hearst

Pieter Danhieux
CEO & Co-Founder, SecureCodeWarrior

Jerry Kowalski
CISO, Jefferies

Elizabeth Lawler
CEO & Co-Founder, AppMap

Alan Snyder
CEO, NowSecure

Mario Vuksan
CEO & Co-Founder, ReversingLabs

Preisha Agarwal
Analyst

Rey Kirton
Principal

Michael Cortez
Partner

Shane Shook, PhD
Venture Partner

With the help of Conor Higgins and Tanya Loh

About Forgepoint

Forgepoint Capital is a leading venture capital firm that invests in transformative cybersecurity, artificial intelligence, and infrastructure software companies protecting the digital future. With $1B+ AUM, the largest sector-focused investment team, and portfolio of over 30 companies, the firm brings over 100 years of proven company-building experience and its Global Advisory Council of nearly 100 leaders to support entrepreneurs advancing innovation globally. Founded in 2015 and headquartered in the San Francisco Bay Area and London, Forgepoint is proud to help category-defining companies reach their market potential. Learn more at www.forgepointcap.com and on LinkedIn.

Learn more at https://www.forgepointcap.com and https://www.linkedin.com/company/forgepoint-capital.

Company Highlights: Application Security & ASPM Portfolio

AppMap
Runtime code analysis for developers
appmap.io

NowSecure™
Mobile application security automation
nowsecure.com

REVERSINGLABS
Software supply chain security and threat intelligence
reversinglabs.com

SECURE CODE WARRIOR
Agile learning platform for secure code development
securecodewarrior.com

Portfolio

Forgepoint is proud to partner with these companies securing the way people live and work. For more information, see https://forgepointcap.com/companies/.

1KOSMOS | aka identity | ANITIAN | AppMap | BISHOPFOX

cinchy | Constella INTELLIGENCE | Converge | CyberCube | FORESCOUT

HUNTRESS | hyperproof | Instabug | interos | loginradius

LUMU | Lynx | NowSecure | nudge | RAD SECURITY

RAFAY | RAPIDFORT | REVERSINGLABS | SECURE CODE WARRIOR | SolCyber

SPHERE | STRATA | SUREFIRE CYBER | SYMMETRY | Synadia

uptycs | VERITUITY | whistic

Exits

CLOUDFLARE AREA 1 SECURITY | Attivo NETWORKS A SentinelOne Company | BehavioSec A LexisNexis Risk Solutions Company | SECUREAUTH | CLOUDENTITY | concourse LABS A FORTINET COMPANY

CYSIV A FORESCOUT COMPANY | ermetic a Tenable company | IDX A ZEROFOX COMPANY | Akamai | noname | Remediant NOW PART OF netwrix

snowflake | truera

Notes

1) "Application Security Guide for Software Engineering Leaders," Gartner, June 1 2023.

2) "DevSecOps: Strategies, Organizational Benefits and Challenges," Gartner Peer Community, Mar 3, 2023. www.gartner.com/peer-community/oneminuteinsights/devsecops-strategies-organizational-benefits-challenges-xrd

3) "Elevating Your AppSec Program with Metrics," KPMG, 2023. kpmg.com/us/en/articles/2023/elevating-appsec-program-metrics.html

4) "OWASP Top Ten Web Application Security Risks," OWASP, September 24, 2021. owasp.org/www-project-top-ten/

5) "Overview of Application Security Commercial Market," TAG Cyber, Feb 4, 2024.

6) "Overview of Application Security Commercial Market," TAG Cyber, Feb 4, 2024.

7) "Invest Implications: Innovation Insight for Application Security Posture Management," Gartner, May 17 2023.

8) "Five Types of Reachability Analysis (and Which is Right for You)." Endor Labs, Jan 2, 2024.

www.endorlabs.com/learn/5-types-of-reachability-analysis-and-which-is-right-for-you

9) "Runtime Intelligence, Meet AI." Kodem Security, Aug 30, 2023. www.kodemsecurity.com/resources/runtime-intelligence-meet-ai"Application Security Guide for Software Engineering Leaders," Gartner, June 1 2023.

10) "Hype Cycle for Application Security, 2023," Gartner, July 24, 2023

11) "Hype Cycle for Application Security, 2023," Gartner, July 24, 2023

12) "Runtime Intelligence, Meet AI." Kodem Security, Aug 30, 2023. www.kodemsecurity.com/resources/runtime-intelligence-meet-ai

13) "Closed Corporate Transaction Notification: Snyk, Application Security Testing," Gartner, April 30, 2024

14) "Snyk Announces Next Big Leap in DevSecOps With Ability of Enterprises to Now Secure Their Software Supply Chains at Scale," Snyk, June 7, 2023. snyk.io/news/snyklaunch-june-2023/

15) "CrowdStrike to Acquire Bionic to Extend Cloud Security Leadership with Industry's Most Complete Code to Runtime Cybersecurity Platform," CrowdStrike, Sep 19, 2023. www.crowdstrike.com/press-releases/crowdstrike-to-acquire-bionic-to-extend-cloud-security-leadership/

16) "Armis Acquires Silk Security to Incorporate Best in Class Security Prioritization and Remediation into Armis Centrix," Armis, Apr 17, 2024. www.armis.com/newsroom/press/armis-acquires-silk-security-to-incorporate-best-in-class-security-prioritization-and-remediation-into-armis-centrix/

17) "Hitting 'Ludicrous Speed' with Zscaler," Avalor, Mar 14, 2024. www.avalor.io/post/hitting-ludicrous-speed-with-zscaler

18) "Invest Implications: Innovation Insight for Application Security Posture Management," Gartner, May 17 2023.

19) "Companies are making up for lack of cybersecurity professionals by investing in their developers," Software Development Times, Aug 27, 2019. sdtimes.com/security/companies-are-making-up-for-lack-of-cybersecurity-professionals-by-investing-in-their-developers/

20) "Bionic Announces Integration with ServiceNow for Industry Leading Application Security Posture Management," PRNewswire, August 9 2023. https://www.prnewswire.com/news-releases/bionic-announces-integration-with-servicenow-for-industry-leading-application-security-posture-management-301896501.html

21) "Companies are making up for lack of cybersecurity professionals by investing in their developers," Software Development Times, Aug 27, 2019. sdtimes.com/security/companies-are-making-up-for-lack-of-cybersecurity-professionals-by-investing-in-their-developers/

22) "Mobb Releases Automatic Vulnerability Fixer for Code Repositories," Mobb.ai, Aug 1, 2024. content.mobb.ai/blog/automatic-vulnerability-fixer-appsec

23) "Hype Cycle for Application Security, 2023," Gartner, July 24, 2023

Forgepoint

/ Forgepoint Forward /

What’s Ahead in Application Security Posture Management (ASPM)

Backing builders of the
/digital future/

forgepointcap.com
650.289.4455
400 S. El Camino Real / Suite 1050
San Mateo, CA 94402

Website

LinkedIn