

THE STATE OF
ASPM
2024



INTRODUCTION:

Digital Transformation Alters the Security Landscape

The unstoppable pace of digital transformation has businesses shipping code at an unprecedented rate. At the same time, the cybersecurity threat level for applications is at an all-time high. In 2023 alone, the likes of [JumpCloud](#), AT&T, Tesla, and T-Mobile have all experienced high-profile data breaches that have impacted both customers and employees.

Application security teams are finding themselves under increasing pressure to protect their software applications from threats and vulnerabilities.

With the rise of cloud computing, modern applications now run on highly dynamic infrastructure. This has shifted the responsibility for infrastructure from IT Ops to development teams. At the same time, the DevOps revolution changed the way applications are built and delivered. Development teams must innovate at blistering speed, releasing new software weekly, daily, and even hourly, for the business to remain competitive. AppSec teams are now dealing with more lines of code than ever before. And new ways of creating code – like using open source components or GenAI – mean that organizations are responsible for the security of code they don't actually write in house.

The impact of digital transformation has caused application security teams to struggle to keep up with development. AppSec wants to be seen as a business enabler but all too often it has become a bottleneck. Though security needs to be a team sport, AppSec teams still struggle to collaborate with development. AppSec teams lack the visibility to identify critical alerts and are often unable to get alerts to the right developers at the right time. The business, and ultimately its customers, are the ones who pay the price for these inefficiencies.

Application Security Posture Management (ASPM) is a promising new application

RESEARCH METHODOLOGY

Cycode commissioned an independent, vendor-agnostic survey of 500 US security professionals:



security platform designed to address the many shortcomings of traditional AppSec point solutions. Among its many features, ASPM promises full visibility from code to cloud, enhanced risk scoring and prioritization, and automated remediation. ASPM intends to break down the silos between security and development, promoting instead a culture of collaboration where security is seen as a team sport.

A number of vendors have rushed to market claiming that their solution fits into this category. This report cuts through the noise to truly define what ASPM is, the key components every ASPM solution should have, and the difference between a complete and incomplete ASPM solution.

In The State of Application Security Posture Management (ASPM) 2024, we explore how digital transformation and AppSec chaos are affecting both AppSec and development teams. We draw on our own research among 500 CISOs, AppSec Directors, and DevSecOps Directors in US companies with 1,000+ employees to uncover and understand key insights about ASPM with the goal of making application security programs more effective and efficient.

TABLE OF CONTENTS

Introduction: Digital Transformation Alters the Security Landscape	02
AppSec Chaos Is the Norm	04
Application Security Posture Management Defined	06
Key Components of Application Security Posture Management	07
Complete vs. Incomplete Application Security Posture Management	08
Key Insights:	09
Insight 1 - AppSec Chaos Reigns over Today's Attack Surface	10
Insight 2 - Crowded Tool Stacks Are Doing More Harm Than Good	11
Insight 3 - Tool Sprawl Is Creating Visibility Issues and Blind Spots	12
Insight 4 - Alert Fatigue from Noisy Tools Are Putting Strain on Security and Development Teams	13
Insight 5 - Overwhelmed Security and Dev Teams Aren't Working Well Together	14
Insight 6 - Regulatory and Compliance Requirements Are Creating Urgency to Improve Security Hygiene	15
Insight 7 - Shifting Security Left Is Slowing Development	16
Insight 8 - More Clarity Is Needed About Who Is Responsible for Application Security	17
Insight 9 - More Needs to Be Done to Encourage a Culture of Collaboration Between Security and Development Teams	18
Insight 10 - A Single ASPM Platform Creates Order from Chaos	19
Conclusion: Complete ASPM Is the Complete Solution to AppSec Chaos	20

AppSec Chaos Is the Norm

Security practitioners are under a tremendous amount of pressure to secure today's applications. On a daily basis, they face an ever-expanding threat landscape, budgetary and personnel constraints, and increasing regulatory pressures to name just a few challenges. Liability for breaches has even begun to shift personal responsibility to security executives, as shown in cases like Uber and SolarWinds.

As applications and development ecosystems grow more complex, securing them becomes more challenging. The following are some of the major obstacles we see in application security today:



Unmanageable Attack Surfaces: Attack surfaces – which include both applications and the pipelines used to build and deploy them – have grown to unmanageable proportions.



Tool Sprawl: In an attempt to shrink attack surfaces, security teams have adopted numerous point solutions. Instead of solving the problem, security teams are now overloaded with tools, and have gaps in visibility between tools.



Security and Development Working in Silos: More tools have resulted in more silos and an ever-widening rift between security and development teams.



Alert Fatigue Resulting in Missed Critical Risks: With the proliferation of tools comes a spike in the number of alerts, including duplicates. Both security and dev teams are inundated and struggle with alert fatigue. The sheer volume of alerts impedes visibility and can even cause critical alerts to be missed.



Shift Left Slowing Innovation: Instead of reducing security logjams, shifting security left simply threw alerts over the fence to developers with little or no guidance on how to fix them. Despite lacking security expertise and training, developers were suddenly expected to remediate vulnerabilities on the side in addition to their full-time job of developing new features.



Growing Distrust Between Security and Development: Security is not a developer-first problem, yet shift left and noisy security scanners have slowed developers' ability to innovate. In the race to release new features, security has become a bottleneck to innovation, which has increased distrust and reduced collaboration between security and development teams.



Regulatory and Compliance Mandates: Increased regulatory and compliance initiatives have placed additional burden on security and developer teams. SOC 2, ISO 27001, SSDF, SLSA, and more have added an additional layer of reporting on already overloaded teams.



All these factors combined have created a perfect storm that we call [AppSec Chaos](#).

AppSec chaos is hampering the ability to innovate securely. To reverse the effects of AppSec chaos, security practitioners need to change the way in which they approach application security. As we have seen, point solutions are no longer the answer. To deliver secure software fast, organizations must adopt a holistic approach to AppSec. That approach needs to pull all security signals from code to cloud into one unified platform then correlate, prioritize, and remediate any risk. Application Security Posture Management is that platform.

Application Security Posture Management Defined

Application Security Posture Management is an AppSec platform that continuously manages the security of modern applications to improve overall risk posture. ASPM delivers visibility, detection, correlation, prioritization, and remediation of security vulnerabilities and defects across the entire software development lifecycle (SDLC).

The platform delivers code to cloud coverage by ingesting data from multiple sources – like application security testing (AST) tools, repo data, and more. This data is then analyzed to identify the most critical risks to the business.

ASPM platforms act as a management and orchestration layer for security tooling, so that you can enable controls and enforce security policies. By providing consolidated application security findings on one platform, ASPM delivers a comprehensive view of security and risk across an entire organization while also facilitating the management and remediation of individual findings.



ASPM traces its roots back to 2016 when Gartner first defined Application Vulnerability Correlation (AVC) as a market segment. AVC was an application security workflow and process management tool that streamlined SDLC vulnerability remediation. Within a year, AVC evolved into Application Security Testing Orchestration (ASTO), which provided a management layer between development, operations, and security systems. In 2019, ASTO technology was replaced by Application Security Orchestration and Correlation (ASOC) platforms. The goal of ASOC was to ease software vulnerability testing by automating workflows and remediation. In 2023, ASPM platforms that manage and automate the entire application security ecosystem came to market.

2016

Application Vulnerability Correlation (AVC)

2017

Application Security Testing Orchestration (ASTO)

2019

Application Security Orchestration and Correlation (ASOC)

2023

Application Security Posture Management (ASPM)

Key Components of Application Security Posture Management

Though many companies claim to have an ASPM platform, they don't deliver many of the required core functionalities. This includes tool consolidation via native scanners, prioritization that identifies the top 1% of risk, and the facilitation of security-developer collaboration. To truly deliver ASPM, the solution needs to organize the chaos of information by providing a number of key functionalities, including the following:



Code to Cloud Visibility: Continuous monitoring of code, tooling, processes, and data from operational environments such as cloud platforms, containers, and physical infrastructure..



Vulnerability Scanning: Scanning for known vulnerabilities using both native and third-party tools, such as secrets scanning, SCA, and SAST.



Prioritization and Risk Management: Prioritizing issues based on severity and risk score.



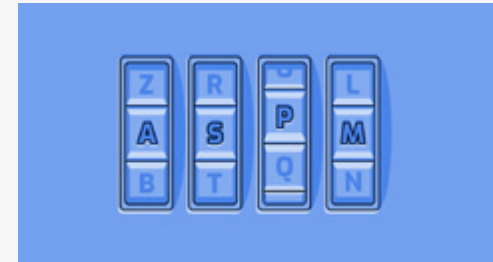
Remediation and Mitigation: Suggesting code changes, configuration adjustments, or the application of security patches.



Compliance: Delivering evidence to comply with various security standards and regulations such as SSDF, SOC 2, and ISO 27001.



Reporting and Analytics: Generating reports and analytics to show the security posture of applications over time.



TO LEARN MORE, READ:

[Application Security Posture Management \(ASPM\): Key Components for Complete Coverage.](#)

Complete vs. Incomplete Application Security Posture Management

When evaluating ASPM platforms, it is important to understand the difference between complete and incomplete solutions. A complete ASPM platform is one that has a comprehensive suite of native AST tools. This includes such tools as Software Composition Analysis (SCA), Static Application Security Testing (SAST), Secrets Scanning, Containers, and Infrastructure as Code (IaC) scanning.

Furthermore, complete ASPM platforms are able to ingest security data from third-party AST tools, bringing all your alerts to one platform. The flexibility of a complete platform allows organizations to easily select and connect the scanners that are right for their ecosystem.

Incomplete ASPM solutions, on the other hand, are only able to ingest vulnerability data from third-party scanners. If an incomplete ASPM does have scanning capabilities, they are extremely limited, lacking one or more core AST tools. For example, they may cover open source libraries with SCA but can't scan proprietary code, find hardcoded secrets, or detect CI/CD tool configurations. With an incomplete ASPM, organizations are dependent on the vendor to provide the correct integrations.

An incomplete ASPM solution is like a point solution. It does not solve for tool sprawl, and organizations still have to manage, on average, more than 50 existing AppSec tools.

Key Insights

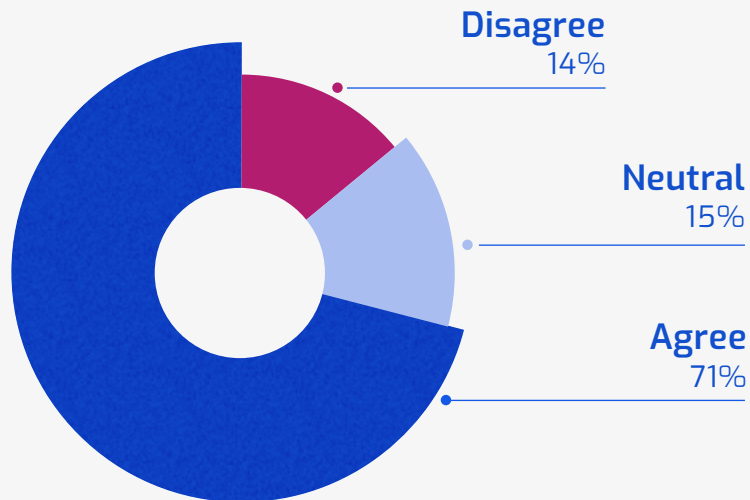
The following are the top 10 ASPM insights that we have uncovered through our extensive primary research.

Insight 1 - AppSec Chaos Reigns over Today's Attack Surface | **Insight 2** - Crowded Tool Stacks Are Doing More Harm Than Good | **Insight 3** - Tool Sprawl Is Creating Visibility Issues and Blind Spots | **Insight 4** - Alert Fatigue from Noisy Tools Are Putting Strain on Security and Development Teams | **Insight 5** - Overwhelmed Security and Dev Teams Aren't Working Well Together | **Insight 6** - Regulatory and Compliance Requirements Are Creating Urgency to Improve Security Hygiene | **Insight 7** - Shifting Security Left Is Slowing Development | **Insight 8** - More Clarity Is Needed About Who Is Responsible for Application Security | **Insight 9** - More Needs to Be Done to Encourage a Culture of Collaboration Between Security and Development Teams | **Insight 10** - A Single ASPM Platform Creates Order from Chaos

AppSec Chaos Reigns Over Today's Attack Surface

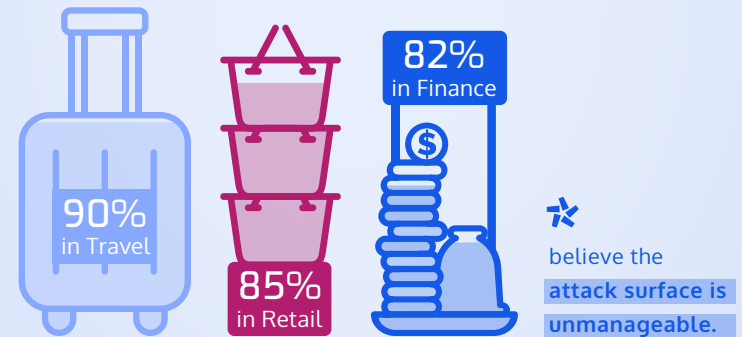
Our data shows a general feeling of unease among Application Security teams when it comes to attack surfaces. The majority of AppSec teams (71%) feel that today's attack surface is unmanageable. Only 14% of those surveyed felt that modern attack surfaces were manageable. This indicates that many security teams feel unable to effectively manage current threats.

Today's Attack Surface Is Completely Unmanageable



CISOs in particular are feeling this way. Almost 4 in 5 (78%) CISOs surveyed agreed that today's attack surface is unmanageable. Just over 3 in 5 (61%) DevSecOps Directors surveyed feel the same.

Segmented by industry, 90% of those surveyed in Travel, 85% in Retail, and 82% of Finance believe the attack surface is unmanageable.

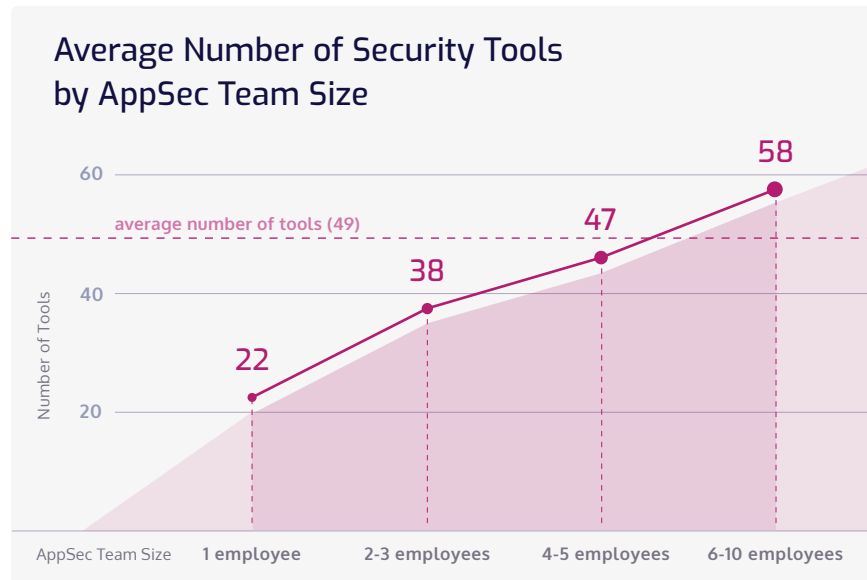


Tool Sprawl Is Causing Harm

With attack surfaces becoming more unmanageable by the minute and malicious actors lurking around every corner, organizations have been turning to a wide variety of AppSec tools to protect themselves.

Our data shows that 95% of security professionals surveyed are currently using 20 or more security tools across their developer and security teams within their organization.

Not surprisingly, the larger the AppSec department, the more tools they are likely to use. However, there was no statistically significant difference between companies with 1,000-4,999 employees and companies with 5,000 or more employees.



Our data shows that, rather than improving matters, the proliferation of AppSec tools currently in use across organizations is only contributing to the feeling of being overwhelmed. Almost 4 in 5 (78%) security professionals surveyed say they find managing multiple different security tools challenging.



4 out of 5

Security Professionals Surveyed

Find Managing Multiple Security Tools Challenging.

Data Silos Are Creating Visibility Issues and Blind Spots

One of the major challenges arising from the use of so many application security tools is the formation of data silos. Data silos make it extremely difficult for developer and security teams to have complete visibility over their development pipelines.

In fact, when security professionals were asked to name their top AppSec concerns, gaps in visibility due to multiple tools (29%) was the second most common response.

Security professionals are also concerned that limited visibility into their development pipelines are creating troubling blind spots that impact their security posture and attack surface.

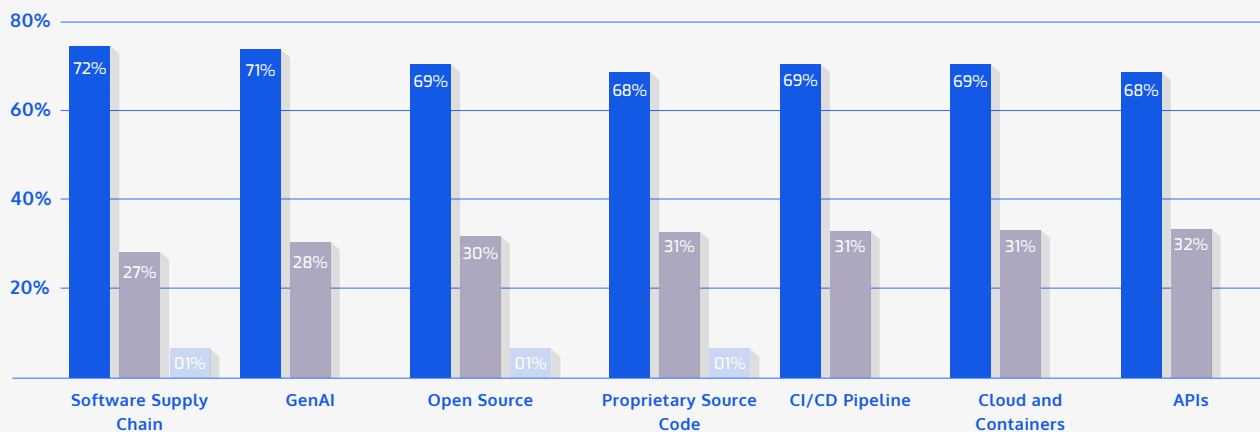


Gaps in Visibility Because of Multiple Tools Is the Second Most Common Application Security Concern.

Unsurprisingly, the more tools an organization uses, the more likely they are to be concerned about visibility. Security professionals surveyed who are using the highest number of AppSec tools are most likely to be concerned about various blind spots in their security posture and attack surface. This further highlights the fact that tool sprawl is a significant contributing factor to AppSec chaos.

To what extent, if at all, are you concerned that:

The Following Are Blindspots in Your Security Posture & Attack Surface?



Security Professionals Surveyed Are Concerned That:



72%

Their **Software Supply Chain** is a blind spot



71%

GenAI is a blind spot



69%

Open Source components are a blind spot

Alert Fatigue from Noisy Tools Is Putting Strain on Security and Development Teams

Another issue plaguing security professionals is the constant influx of alerts generated by their numerous application security tools. The constant noise causes alert fatigue, which can cause a delay in response or sometimes even missing critical alerts.

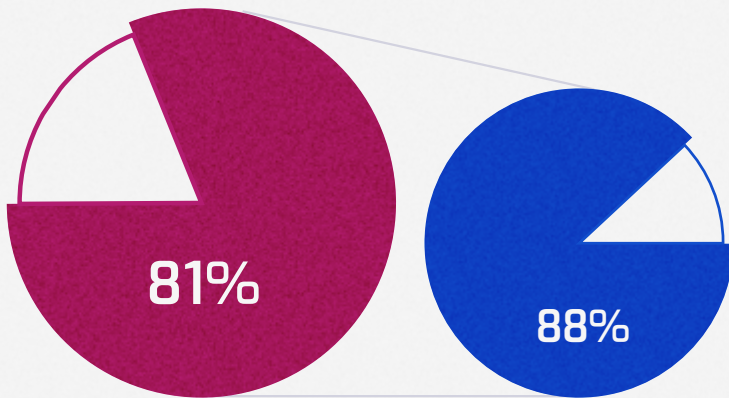
A sizable 76% of the security professionals surveyed find that managing all of these alerts is challenging. More than 4 in 5 (81%) respondents say they feel that their developer teams are experiencing too much vulnerability noise and alert fatigue.

With so much noise to cut through, it's no wonder that almost three quarters (74%) of security professionals surveyed find it challenging to know which vulnerabilities to fix first. Furthermore, 83% of respondents are not always able to scale the process of getting vulnerabilities to the right developers at the right time.

In addition, 80% of respondents whose developer teams are experiencing too much noise and alert fatigue also think that their developer teams aren't remediating all vulnerabilities due to this.

What is abundantly clear is that alert fatigue is putting security and development teams under serious strain. The result: Organization's applications and the data they contain are at risk.

Alert fatigue is a symptom of another major issue being faced within organizations. Security and development teams are struggling to work well together.



81%

Believe Developer Teams Experience Too Much Vulnerability Noise and Alert Fatigue



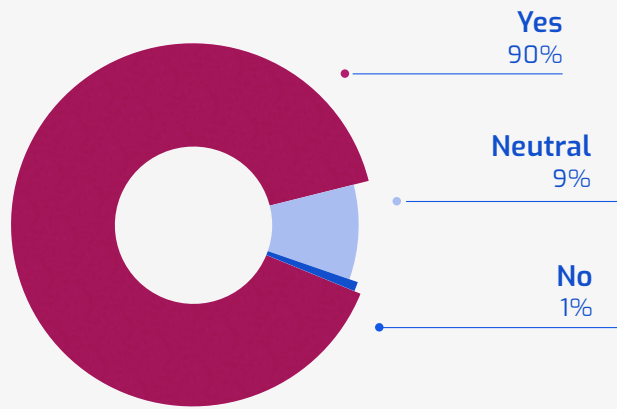
88%

CISOs Who Also Think Developer Teams Aren't Remediating All Vulnerabilities

Overwhelmed Security and Dev Teams Aren't Working Well Together

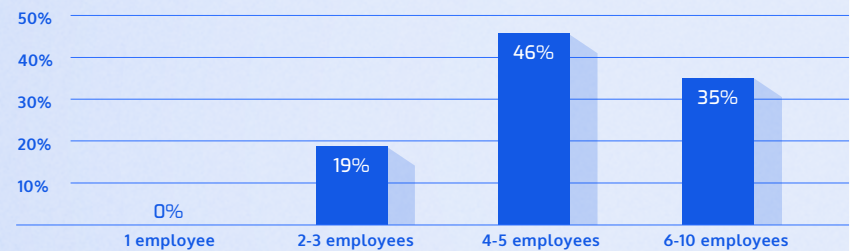
Developers are under pressure to deliver innovative solutions. Fixing security issues is not their primary job. When security hands alerts to developers with little or no context, it stresses an already strained relationship. In fact, 90% of respondents said the relationship between security and developers needs to improve.

Does the Relationship Between Security and Developers Need to Improve?



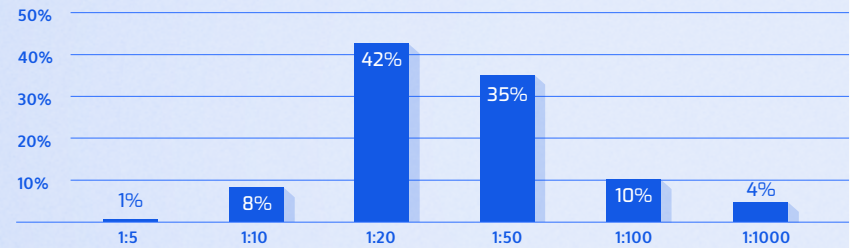
Adding to this friction, AppSec teams tend to be small despite the outsized expectations to secure applications, software supply chains, and CI/CD pipelines. Half of all AppSec departments in organizations with 1,000-4,999 employees have only 4-5 security staff. For companies with 5,000+ employees, 41% had 4-5 AppSec staff, while only 42% had 6-10 staff. None of the companies surveyed reported having AppSec teams larger than 10.

Size of Application Security Departments



When asked about the ideal ratio of security to developers, 42% of respondents stated the ratio should be 1:20. In companies with 5,000 or more employees, 47% felt 1:20 was the ideal ratio, while 36% felt a ratio of 1:50 was better. In companies with 1,000-4,999 employees, 37% cited 1:20, whereas 33% said 1:50 was a better ratio.

Ideal Ratio of Security Personnel to Developers



From our own experience, the ratio for most organizations is one security person per 100 developers. Small AppSec teams are overloaded managing multiple tools, and hiring additional personnel is difficult in budget-constrained departments.

With a complete ASPM solution, security teams are more efficient. With the context provided by ASPM, security can manage, prioritize, and remediate alerts from one platform, making them feel like a team with a lower 1:20 ratio.

Regulatory and Compliance Requirements Are Creating Urgency to Improve Security Hygiene

The already strained relationship between security and development is made worse by ever-tightening regulations around data privacy and compliance. Many new security frameworks and compliance standards like SSDF, SLSA, and SBOMs are designed to provide greater transparency into the security of an organization's software development and delivery processes. While these standards are useful in understanding an organization's security posture, they place additional burden on already stressed teams.

According to our data, 85% respondents say it's urgent that they implement good security practices and hygiene in their organization due to the exponential increase in security regulations and compliance.

This is especially true for security teams, with 88% of CISOs and 86% of AppSec Directors surveyed saying they feel a sense of urgency. Interestingly DevSecOps Directors are only slightly less concerned with 78% of those surveyed saying the same.

It is interesting to note that the majority of those surveyed said that improving security hygiene must also be balanced with budget cuts. Despite being very concerned about meeting current regulations and compliance standards, 75% of security professionals say they must weigh these demands against budget constraints.



**75% of Security
Professionals say
They Must Weigh
Compliance Against
Budget Constraints.**

Shifting Security Left Is Slowing Development

The constant pressure to deliver new technology has organizations shipping code at an unprecedented rate. To reduce security bottlenecks and costs, organizations have shifted security left. Developers now carry out security testing and fix vulnerabilities earlier in the software development life cycle where issues are less costly to remediate.

Our data shows that shift left is a widespread practice. In fact, 91% of security professionals surveyed say that when developers are resolving security issues, they are resolving them within their developer workflows (e.g., IDEs, CLIs, SCMs).

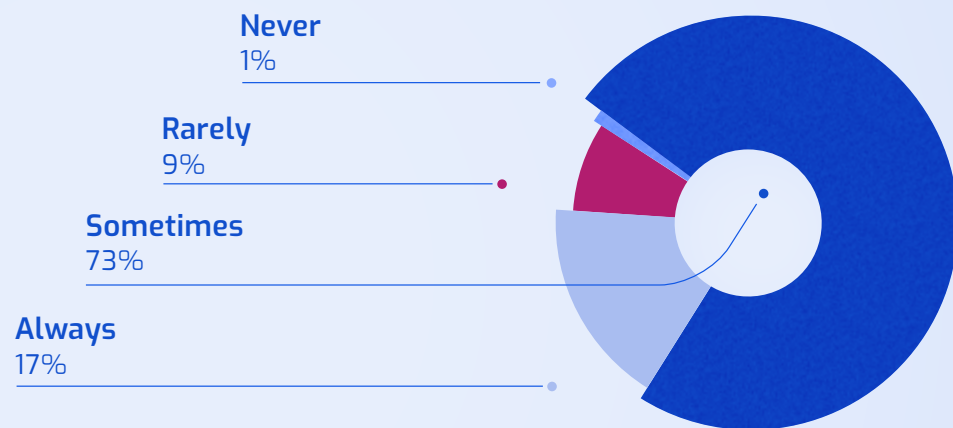
Unfortunately, 83% of respondents said that they have trouble getting the right vulnerabilities to the right developers at the right time. This shows that shifting left is often an imperfect process.

There is a better way to shift left and do so successfully. Read our blog [Controlled Shift Left: A Strategic Blueprint for Modern Software Security with Cyscale](#) to learn more.

Our data also shows that security concerns are putting speed bumps on the road to new software development.

A significant majority (70%) of security professionals surveyed who are concerned that the likes of open source components, third-party code, Gen AI, and APIs represent blind spots in their security posture and attack surface say that the cadence of software development or deployment has slowed because of security processes.

How Often Are You Able
to Get the Right Vulnerabilities to the
Right Developers at the Right Time?



More Clarity Is Needed About Who Is Responsible for Application Security

Our data uncovered that a major disconnect exists between security and development teams.

On the one hand, application security teams are now responsible for more threats than ever before, including the application itself, software supply chain security, and pipeline security. They are also responsible for cutting through the noise and assigning remediation tickets to keep security workflows moving efficiently. Meanwhile, developers are getting bogged down in security issues thanks to the widespread practice of shifting left.

Essentially, security has become so all-consuming that there is now major confusion over whether security or development is truly responsible for resolving security vulnerabilities.

This uncertainty is reflected in our data. Almost 9 in 10 (88%) security professionals surveyed said that the responsibility for the security of applications within their organization is spread across multiple groups, each with their own tools.

With so many tools and siloed teams in play, it is no wonder that more than three quarters (77%) of security professionals surveyed find understanding who 'owns' security to be a challenge.



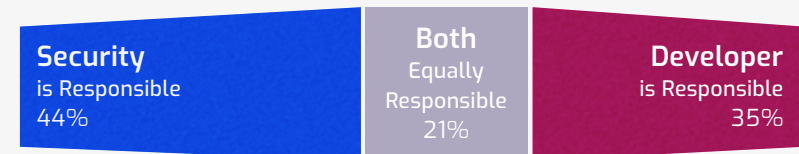
88% Say Responsibility for Security Applications Is Spread Across Multiple Groups with Their Own Tools



77% Say Understanding Who Owns Security Is Challenging

This is also supported by further findings that nearly half of (44%) security professionals surveyed think security teams are responsible, while over a third (35%) think that developers are responsible, and just over a fifth (21%) think that both teams are equally responsible. (Q5)

Who Should Be Responsible for Resolving Security Vulnerabilities?



This data shows a general lack of consensus on who should be responsible for fixing security flaws. Very few respondents (21%) see both security and development equally responsible, which indicates that most do not see security as a team sport. Certainly security works best when it's a collaboration between security and development teams, yet greater clarity of this relationship is still necessary to gain operational success.

More Needs to Be Done to Encourage a Culture of Collaboration Between Security and Development Teams

The confusion over who owns security also indicates a breakdown in collaboration between security and development teams. In fact, three quarters (76%) of security professionals surveyed say they find implementing a culture of collaboration between security and developer teams to be challenging.

Once again, CISOs are especially likely to find this challenging. Over 4 in 5 (83%) CISOs surveyed said they find implementing a culture of collaboration between security and developer teams to be challenging. Just less than three quarters (74%) of DevSecOps Directors surveyed and 7 in 10 (70%) AppSec Directors surveyed said the same.



76% Find Implementing a Culture of Collaboration Between Security and Developer Teams Challenging

Meanwhile, 90% of security professionals surveyed said the relationship between security and developers needs to improve.

This rift between security and development teams is one of the main obstacles standing in the way of teams adopting new solutions that could help to combat AppSec chaos.

Despite the very pressing need to overcome the challenges we've outlined in previous sections, a number of factors may end up preventing security professionals from adopting new Application Security solutions.

Main Blockers/Barriers to Adopting New Application Security Solutions

01

Creating cross-functional teams (breaking down silos between security, engineering, and DevOps)

02

Training developers in secure coding best practices

03

Time to value is too long

04

Gaining developer buy-in

05

Budget constraints

Bridging the gap between teams is a challenge that organizations are going to have to face head on if they ever want to fully get to grips with their application security programs.

A Single ASPM Platform Creates Order from Chaos

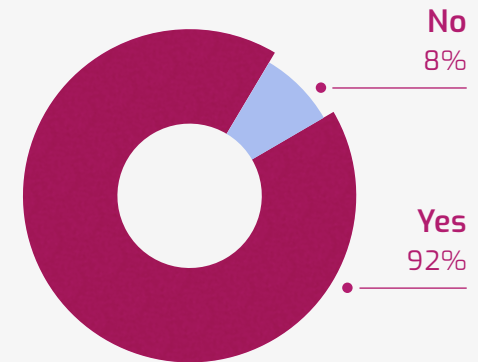
While the odds seem stacked against security and development teams in the battle against AppSec chaos, our data shows signs that positive change is on the horizon.

In fact, 92% of security professionals surveyed have plans to consolidate their security tool stack over the next 12 months. Meanwhile, 90% would consider consolidating all of their AppSec tools into a single platform over the next 12 months if they had the opportunity.

Tool consolidation has several drivers. First, by centralizing on one platform, organizations eliminate tool silos, remove blind spots between tools, and gain context into risk across the SDLC. This both delivers better visibility and helps security teams reduce the noise generated by scanners and duplicate alerts. Second, tool consolidation lowers costs both in the form of licensing fees and in the personnel required to manage numerous tools. Standardizing on one platform makes AppSec programs easier and less costly to monitor and manage.

Having too many application security tools has created distrust across organizations. As shown by our data, we expect the next 12 months to be marked by significant tool consolidation as many organizations move to one platform to achieve both better visibility and collaboration among teams. Consolidation onto an ASPM platform will deliver better security outcomes and free up personnel from managing point solutions to performing higher order security tasks.

Do You Have Plans to Consolidate Your Security Tool Stack to 1 Platform Over the Next 12 Months?



90%

Would Consider Consolidating All of Their AppSec Tools Into a Single Platform Over the Next 12 Months

CONCLUSION:

Complete ASPM Is the Complete Solution to AppSec Chaos

Too many security programs have devolved into AppSec chaos. Modern-day attack surfaces have become unwieldy and unmanageable. Organizations have too many point solutions, which are costly, create gaps in visibility, and generate too much noise. The resulting alert fatigue is so great that teams miss critical alerts, which puts the business at risk. All too often, security and development teams are working in silos, and the data shows that collaboration is suffering and mistrust is growing. Finally regulatory and compliance demands further stress already overloaded security teams.

All these factors obstruct innovation and limit organizations' ability to differentiate to gain competitive advantage. Security is racing to keep up and yet still not meeting the demands to secure today's complex threat landscape. Ultimately security needs a better, more scalable solution to solve the pain points they face daily.

Complete ASPM

A complete ASPM approach is designed to remedy modern AppSec pain.

A complete ASPM platform allows organizations to consolidate tools onto one platform. Tool consolidation reduces costs by eliminating the license fees of the many point solutions it replaces and by freeing up personnel from managing those tools. It also provides superior visibility by erasing the huge gaps between tools. The efficiency gained by using a complete ASPM platform makes it feel as if the ratio of security to developers has decreased to 1:20 without needing to expand AppSec staff.

Also, a complete ASPM platform improves the management and remediation of alerts. It deduplicates alerts and provides context, drastically reducing alert fatigue. Ruthless prioritization helps organizations know that they are focusing on the most important risks first. Furthermore, remediation is shifted left in a controlled manner. Developers are given the right remediation advice in the right place at the right time so that they can fix and prevent defects in the first place.

Furthermore, a complete ASPM platform reduces security-developer friction and fosters collaboration between teams. By providing seamless developer workflows, a complete ASPM platform is able to make security a team sport. When security and development teams work together, they are able to continuously deliver secure software ahead of the market.

The bottom line is that, with a complete ASPM platform, organizations don't need to wait 12 months to realize value. ASPM implementations begin with just a few clicks, yet results start pouring in instantaneously, and value is immediate.

A complete ASPM is the right platform for organizations that want a high-efficiency, effective modern platform. When evaluating a new ASPM platform, however, not just any solution will do. It is essential to adopt a complete ASPM. A complete ASPM is one that has a comprehensive suite of native scanners but also allows you to connect your existing AST scanners. Incomplete ASPMs that don't allow for tool consolidation, and the associated savings on licensing fees, are no better than adding a new point solution to your tool stack.

Partnering with Cyscale

Partnering with Cyscale and our complete ASPM platform helps you solve today's AppSec challenges. Cyscale offers the only complete approach to ASPM on the market today.

With our complete [Application Security Posture Management \(ASPM\) platform](#), you can select and connect your existing security scanners or replace them altogether and use our own native scanners. Either way, Cyscale delivers total visibility of your application and your SDLC, providing the context you need to identify the most pressing threats to your business.

Cyscale's complete ASPM platform unites security and development teams with instant visibility and intelligent prioritization with our Risk Intelligence Graph (RIG). We help security and development teams work better together by allowing teams to prioritize and remediate the most critical vulnerabilities so developers can focus on what they do best: create innovative features that help differentiate your business.

AppSec Is a Team Sport

At Cyscale, we believe that AppSec is a team sport and that security is everyone's job. Cyscale's complete ASPM helps businesses achieve this by fostering intentional collaboration and controlled shift left. We know that developers do best when they are given the right tools to secure their code. Cyscale's complete ASPM platform delivers business-impact-driven alerts, code-to-cloud traceability, clear vulnerability ownership identity, and threat intelligence that automatically notifies you of zero-day attacks. Cyscale's complete ASPM is a solution that delivers scalability and speed, tool consolidation, enhanced visibility, and regulatory compliance support.

Cyscale truly delivers peace of mind from code to cloud with a complete ASPM.



ABOUT CYSCALE

Cyscale is the leading Application Security Posture Management (ASPM) providing Peace of Mind. Its complete ASPM platform scales and standardizes developer security without slowing down the business. With Cyscale's complete ASPM, security teams can eliminate context switching, amplify visibility, prioritize and eliminate risk to ensure end-to-end code to cloud coverage, leaving no room for attacks to go unnoticed. Cyscale's Risk Intelligence Graph (RIG) provides unmatched visualization, risk scoring, along with code to cloud traceability across the entire SDLC. Backed by tier-one investors Insight Partners and YL Ventures, the series-B company has raised \$80 million and boasts a number of the top global Fortune 100 customers in the world that are gaining immediate value. Book an online demo of [Cyscale's ASPM platform](#).

THE STATE OF
ASPM
2024



cyclope
Peace of Mind