THE STATE OF ASPM 2025

PRESENTED BY cycode

The State of ASPM:
Navigating Gen AI, the Code Boom, ASPM, & Modern AppSec Challenges

The Cycode Manifesto: A 2025 Outlook

Written by Lior Levy, CEO of Cycode, and signed by Roland Cloutier, Former CSO at TikTok.

Over 93 billion lines of code were generated in the past year alone, driven by the transformative rise of generative AI (GenAI) and machine learning. This unprecedented "code boom" has not only reshaped the speed and scale of software development, but also created an unmanageable attack surface, leaving organizations struggling to keep up with the pace of innovation.

And things aren't slowing down. Gartner predicts that 80% of enterprises will embed AI deeply into their operations by 2026.

In an attempt to rise to these new challenges, many organizations are adding more and more tools to their security stack. Unfortunately, this tool sprawl has led to a new set of problems. Security teams are fatigued by alerts, false positives waste valuable time and resources, and critical threats can get lost amongst all the noise. These inefficiencies strain the relationship between security and development teams, eroding trust and hindering productivity. Developers are burdened with addressing non-critical vulnerabilities, while real threats slip through the cracks. This not only increases risk, but also drives up costs due to tool ownership and inefficiencies.

That's where Application Security Posture Management (ASPM) comes in.

By providing comprehensive visibility, prioritization, and remediation, ASPM platforms stop application risk before it starts. The result? A reduced developer productivity tax and a lower total cost of ownership and overhead.

Importantly, the evolution of ASPM has mirrored the changing needs of the industry.

The first wave of ASPM was largely focused on aggregation—tools that brought together security data but lacked context, leaving teams struggling to act on fragmented insights. The second wave emerged in response to crises like Log4J, which exposed the vulnerabilities of modern software supply chains.

These solutions tackled the critical need for supply chain security but often failed to address deeper, systemic issues.

Now, we've arrived at the third and most transformative wave: **Complete ASPM**.

Complete ASPM combines proprietary scanning tools with seamless third-party integrations and advanced capabilities like AI-powered risk prioritization. By unifying these elements, Complete ASPM helps teams overcome AppSec Chaos once and for all.

Of course, AppSec is just one piece of a much larger cybersecurity puzzle. Some vendors offer tools that attempt to solve several challenges - like code security and cloud security. While cloud and code security should certainly integrate, relying on a single solution to address both will result in inadequate protection and increased risks. That's why a "separation of duties" is essential: if businesses want to ensure that security is an enabler of innovation and not a bottleneck, leaders must look for best-in-class solutions with expertise in their respective domains. In the realm of code security, Cycode is that solution.

We don't believe organizations should have to choose between innovation and security. Our mission is to enable companies to deliver safe code, faster...and adding yet another tool to your tech stack won't help you unlock speed, agility, or resilience. **Businesses need a platform approach to help them embed security into every phase of development.**

Ready to step into the future of application security, where clarity replaces chaos and collaboration drives success?

Lior Levy, CEO of Cycode
Roland Cloutier, Former CSO at TikTok

THE STATE OF ASPM 2025

Table of Contents

The 2025 State of ASPM
Executive Summary

The 2025 State of ASPM Report marks the second annual study from Cycode, building on the industry's first ASPM report released last year.

This year's findings provide a deeper look into the critical challenges and opportunities shaping application security as organizations grapple with growing attack surfaces, tool sprawl, and the rapid adoption of generative AI.

One thing is clear: 2025 will be a turning point for application security practices.

Other key takeaways include:

GenAI is Exacerbating the Unmanageable Attack Surface: 59% of security professionals agree that today's attack surface is unmanageable, with GenAI and code security emerging as the top blindspots.

Budgets Are Growing, But Oversight is Lacking: Security budgets are expected to grow by an average of 50% in the next 12 months, but 77% of security professionals admit their organization lacks a full understanding of where their annual budget is being spent. This disconnect is largely driven by the proliferation of point solutions, which address narrow, niche problems but often add complexity and hidden costs.

Tool Sprawl is Crippling AppSec Teams: Organizations use an average of 50 security tools, with 67% of respondents saying managing them is a significant hurdle. Across the board, tool sprawl is reducing visibility, creating blindspots, and limiting collaboration between security and developer teams.

2025 Will Be the Year of Code Security: 73% of security leaders believe "code is everywhere", but 63% say CISOs aren't investing enough in code security. At the same time security leaders are pushing for a separation of duties, with 86% agreeing that ASPMs and CNAPPs are complementary solutions that shouldn't come together as one platform.

ASPM is the Answer to AppSec Chaos: Security professionals are fighting back: 61% have already started consolidating their tool stacks, and 88% say they would consolidate further in the next 12 months if given the chance.

RESEARCH METHODOLOGY

Cycode commissioned an independent, vendor-agnostic survey of 701 CISOs, AppSec Directors, and DevSecOps managers across the UK, US, and Germany, with 50% of respondents working within companies with 5,000+ employees.

Survey conducted in
November 2024

700
Respondents

CISO | AppSec Team | DevSecOps Team

US, UK, Germany
Market

US | UK | Germany

1K-5K Employees
50%

5K+ Employees
50%

Key Insights

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

Insight 1 - GenAI is Exacerbating the Unmanageable Attack Surface | **Insight 2 -** Tool Sprawl Continues to Fuel AppSec Chaos | **Insight 3 -** Blindspots are Growing as Code Volume Surges | **Insight 4 -** Security Leaders are Losing Track of Their Budgets | **Insight 5 -** Securing Code Must be a Priority in 2025 | **Insight 6 -** AppSec Tool Sprawl is Stretching the Talent Gap | **Insight 7 -** Compliance is Forcing Change in AppSec | **Insight 8 -** The relationship Between Security and Developer Teams Remains Strained | **Insight 9 -** Security Teams are Already Taking Steps to Combat Tool Sprawl | **Insight 10 -** ASPM Platforms are Helping Teams Collaborate, Combat Alert Fatigue, and Focus on the Risks that Matter Most

INSIGHT #01

GenAI is Exacerbating the Unmanageable Attack Surface

The growing complexity of today's attack surface has left security professionals struggling to maintain control, with over half (59%) of respondents agreeing that today's attack surface is completely unmanageable.

This highlights the urgent need for organizations to rethink how they manage and secure their applications.

59%

of security professionals agree that today's attack surface is unmanageable

GenAI is partly to blame, with 70% of respondents saying GenAI has exacerbated existing visibility challenges.

70%

"GenAI has exacerbated existing visibility challenges."

That's because GenAI has enabled an unprecedented increase in code volume, much of it written by individuals without a deep understanding of secure architecture.

At the same time, bad actors are leveraging the same technology to deploy more sophisticated and large-scale attacks at unprecedented speed.

It's no wonder 72% of security leaders agree that the age of AI necessitates a complete overhaul in how organizations approach application security.

72%

"The age of AI necessitates a complete overhaul in how organizations approach application security."

INSIGHT #02

Tool Sprawl Continues to Fuel AppSec Chaos

AppSec Chaos continues to prevent organizations from managing risks, fostering collaboration, and delivering secure software at scale.

To address this challenge, 35% of organizations are allocating the lion's share of their security budget to the evaluation of security tools and technology.

35%

of organizations are allocating the lion's share of their security budget to the evaluation of security tools and technology.

But this approach has created unintended consequences. The average organization now uses 50 security tools across their security and development teams, an increase compared to last year.

Paradoxically, the research shows that the more tools a company has, and the larger its AppSec team, the more unmanageable its attack surface becomes.

The challenge doesn't end there. Over two thirds (67%) of security professionals surveyed say that managing all of these tools is a significant hurdle, and 33% rank tool sprawl as their top application security concern.

This highlights a critical disconnect: teams often assume that adding more tools will help them gain control over their attack surface, but in reality, tool proliferation is the root of many application security teams' problems.

67%

of security professionals say managing multiple different security tools is challenging

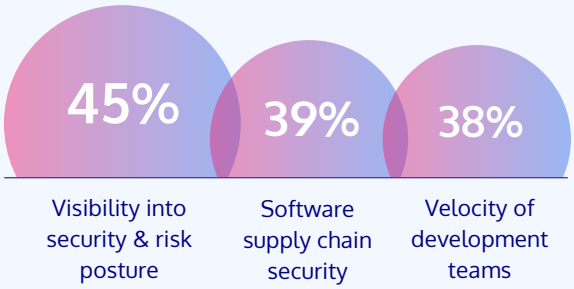
To move forward, organizations must rethink their reliance on point solutions and prioritize strategies that reduce complexity rather than adding to it.

INSIGHT #03

Blindspots are Growing as Code Volume Surges

According to the data, visibility into security and risk posture is the top application security concern among security professionals.

Top 3 Biggest Application Security Concerns



And when it comes to their biggest blindspots, GenAI has emerged as the #1 blindspot reported by security professionals, followed by the exponential growth in code. These two challenges are deeply intertwined: as generative AI accelerates development, the attack surface expands, making it harder for teams to maintain visibility and respond effectively.

Top 5 Application Security Blindspots:

GenAI	71%
Exponential Increase in ode	70%
Secret Detection	68%
Software Supply Chain	68%
Cloud Security	67%

The research also reveals a concerning link between tool sprawl and blindspots.

For example, half (50%) of security professionals surveyed who currently use under 20 security tools across their security and developer teams say they are concerned about the exponential increase in code. This figure climbs to almost three quarters (73%) of respondents with 81-100 security tools in use.

Concerned About the Exponential Increase in Code

50%

under 20 security tools in use across their security and developer teams

73%

81-100 security tools in use across their security and developer teams

This once again highlights the negative impact of tool sprawl, as outlined in Insight #02. Instead of improving visibility, an overload of tools often introduces additional complexity and chaos, making it harder for teams to gain a clear understanding of their risk posture.

These findings confirm that it's time for organizations to rethink their approach to AppSec by consolidating all their point solutions into a single Complete ASPM platform.

INSIGHT #04

Security Leaders are Losing Track of Their Budgets

Security teams are pouring significant resources into tools and technology evaluation, with this area consistently topping the list of priorities for security budgets.

Security Budget Priorities Ranked

1. Security tools and technology evaluation
2. Incident response and investigation
3. Security awareness and training
4. Reporting and compliance
5. Cloud security
6. Code security
7. Patching

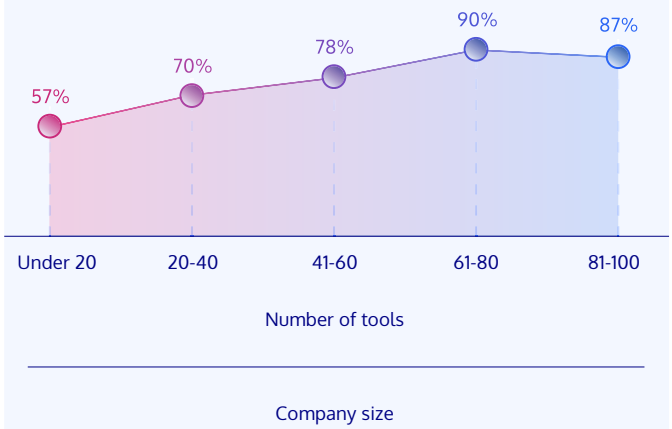
However, despite this heavy spending, 77% of security professionals admit their organization lacks a full understanding of where their annual budget is being spent.

77%

of security professionals Admit their organization lacks a full understanding of where their annual budget is being spent.

This disconnect becomes even more pronounced in organizations with large tool stacks. Among respondents with fewer than 20 tools in use, 57% report budget visibility challenges. However, this figure skyrockets to 90% among those with 61-80 tools and 87% among those with 81-100 tools. This highlights a troubling trend: the more tools an organization uses, the harder it becomes to track and justify spending.

"My organization lacks a full understanding of where the annual budget is being spent."



71%

in organizations with under 1k employees

84%

in organizations with over 1k employees

Point solutions are likely to blame. By addressing narrow, niche problems, these tools create overlap, inefficiencies, and hidden costs that make it difficult for security leaders to gain a clear view of how resources are being allocated.

INSIGHT #05

Securing Code Must Be a Priority in 2025

63% of respondents believe CISOs aren't investing enough in code security, even though it's a critical foundation for protecting applications. However, with the exponential increase in code creating more risk than ever, this will need to change in 2025.

63%

agree that **CISOs don't invest enough in code security**

According to nearly 3 in 4 (73%) of those surveyed, "code is everywhere," and securing it across applications is vital. Clearly, security professionals would welcome greater investment in code security.

3 out of 4 stated
"Code is everywhere, securing code is vital"

Encouragingly, security professionals surveyed expect their budgets to increase by an average of 50% over the next 12 months. This presents an opportunity to reprioritize investments and allocate more resources toward securing code.

Security professionals expect their **budgets to increase by an average of**

50%

over the next 12 months.

But code security demands expertise. While we advocate for a platform approach that reduces tool sprawl and complexity, it's essential not to consolidate tools to the point where organizations are left with sub-par solutions. Code security is too critical to be handled by generic platforms—it requires specialized expertise, and Cycode is the leader in this domain.

Security leaders seem to agree. Despite recent announcements from some vendors, 86% of respondents believe that ASPMs and CNAPPs are complementary solutions that shouldn't come together as one platform. This separation of duties ensures that teams can deploy best-in-class tools for each domain while maintaining the flexibility to integrate with other parts of their security ecosystem.

86%

of respondents believe that **ASPMs and CNAPPs** are complementary solutions that **shouldn't come together as one platform.**

INSIGHT #06

AppSec Tool Sprawl is Stretching the Talent Gap

It's no secret that security teams have, for a long time, faced a problem with a technical skills gap.

According to research carried out by the World Economic Forum, there is currently a shortage of around 4 million cyber professionals, with 71% of organizations stating that they have unfilled cybersecurity positions.

Unfortunately, this is hindering progress for many of the security professionals. In fact, 39% of respondents said that a shortage of staff to implement new solutions is one of the main things holding them back from adopting new AppSec solutions.

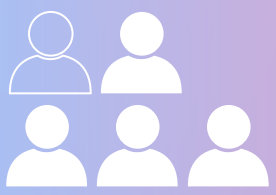
71%

of security leaders say they have unfilled cybersecurity positions.

39%

of security professionals say that a shortage of staff is holding them back from adopting new AppSec solutions.

Likewise, over 4 in 5 (83%) security professionals surveyed agree that having too many tools require specialist skills, and those skills that are increasingly difficult to find due to the ongoing cybersecurity talent gap.



4 in 5

agree that having too many tools require specialist skills, and those skills that are increasingly **difficult to find due to the ongoing cybersecurity talent gap.**

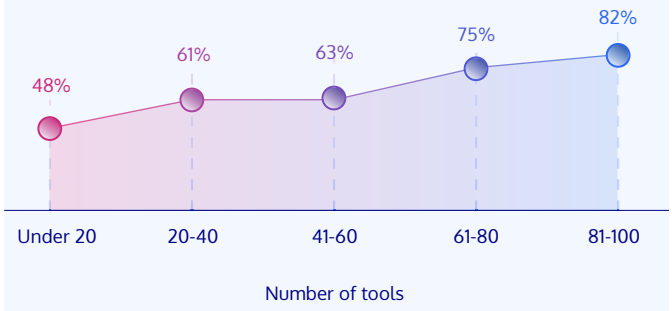
It's no wonder almost two thirds (65%) of security professionals surveyed say they find balancing the shortage of talent with AppSec challenging.

65%

of security professionals say they find balancing the shortage of talent with AppSec challenging.

The data also shows that the extent to which security professionals struggle with this is linked to the number of security tools their organization is currently using. Security professionals surveyed with 81-100 tools in play – 49% of whom are from large enterprises with 5,000+ employees – are significantly more likely than those with fewer tools to find this element of their role challenging.

"I find balancing the shortage of talent with AppSec needs challenging."



INSIGHT #07

Compliance is Forcing Change in AppSec

Compliance has become a driving force behind organizational security practices, with 59% of security professionals agreeing that regulations have brought a greater sense of urgency to their efforts. However, keeping up with the ever-evolving landscape of compliance requirements is becoming increasingly challenging.

59%

agree that **the increase in regulation has brought a sense of urgency to their organization's security practices**

As just one example of new regulations, operational mandates from the Digital Operational Resilience Act (DORA), which applies to financial institutions in the EMEA region, come into effect in 2025, further complicating the regulatory landscape. Similarly, in the United States, FedRAMP compliance requirements continue to evolve, placing increasing pressure on organizations working with government agencies to meet stringent cloud security standards.

Unfortunately, over half of respondents (56%) report that maintaining compliance is becoming more and more difficult. One major reason is that compliance remains a manual and time-consuming process, as highlighted by another 56% of security professionals surveyed.

56%

report that maintaining compliance is becoming more and more difficult.

Surprisingly, organizations with larger tool stacks—61 or more tools—are even more likely to say compliance is a manual process than those with fewer tools. This suggests that their existing tools aren't fit for purpose when it comes to simplifying compliance workflows. Instead of reducing complexity, these bloated stacks often add to it.

INSIGHT #08

The Relationship Between Security and Developer Teams Remains Strained

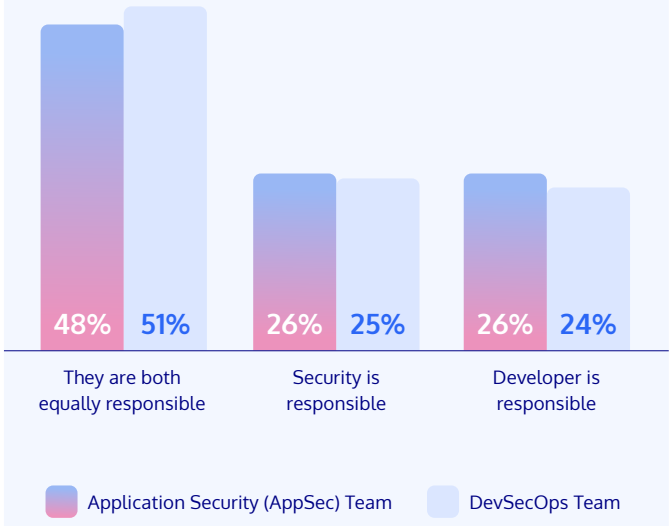
The relationship between security teams and developers remains under strain in 2025.

Almost three quarters (74%) of security professionals surveyed agree1 that the relationship between security and developers needs to improve.

74%
of security professionals agree that **the relationship between security and developers needs to improve**

Not only do almost 7 in 10 (68%) security professionals surveyed report that understanding who 'owns' security is challenging, but the data reveals that the division of responsibility isn't cut and dry.

Balance of Responsibility for Resolving Security Vulnerabilities: Security Teams vs. Developer Teams



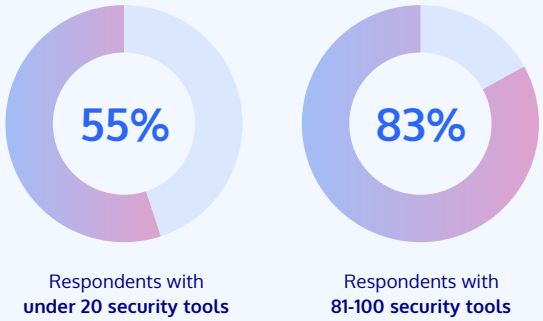
Clearly, more could be done to implement a culture of collaboration between these two teams.

Unfortunately, this is something almost 7 in 10 (68%) security professionals surveyed find challenging.

Worse still, the findings suggest that tool sprawl may be to blame for the rift between security and developer teams, and that the solution lies in consolidating crowded tool stacks into one, easy-to-manage ASPM platform.

While two thirds (66%) of security professionals surveyed who are currently using less than 20 security tools say they think the relationship between security and developers needs to improve, this figure rises to 4 in 5 (80%) using 81-100 tools. Similarly, just 55% of those with under 20 security tools find implementing a culture of collaboration between security and developer teams challenging, while over 4 in 5 (83%) of those with 81-100 tools say the same.

"It's challenging implementing collaboration between security and developer teams."



INSIGHT #09

Security Teams are Already Taking Steps to Combat Tool Sprawl

The good news is, security professionals have wised up to the perils of tool sprawl.

Almost 9 in 10 (88%) stated that, if given the opportunity, they would consolidate all their AppSec tools into a single platform in the next 12 months.

88%

of security leaders have **consolidated all of their AppSec tools into a single platform in the next 12 months if given the opportunity.**

Even more encouragingly, over half (61%) of security professionals surveyed have already started consolidating their tool stack. If you narrow the scope to AppSec tools specifically, over 2 in 5 (43%) have already consolidated all of their tools into a single solution.

43%

Say they have consolidated all of their AppSec tools into a single solution

Those who haven't are also keen to take this step, with The findings also suggest that budgets for 2025 will allow for this. See Insight #05.

INSIGHT #10

ASPM Platforms are Helping Teams Collaborate, Combat Alert Fatigue, and Focus on The Risks that Matter Most

If we've learned one thing, it's that more AppSec tools cause more problems for both security professionals and developers.

Two-thirds (66%) of security professionals surveyed say it's challenging to manage too many alerts. It's no surprise, then, that 65% struggle to know what vulnerabilities to fix. Likewise, 81% of security professionals report that they feel their developer teams are experiencing too many false positives and alert fatigue.

66%

of security professionals say it's challenging to manage too many alerts.

Across the board, these problems are made worse as organizations adopt more tools.

But it's not all bad news: the findings clearly demonstrate that teams can solve these problems with the right ASPM platform.

9 in 10 (90%) security professionals surveyed who are already using a commercial ASPM platform feel that their organization has a systematic way of understanding overall risk, and are always working on the most important vulnerabilities. On the other hand, just 55% of those without an ASPM platform say the same.

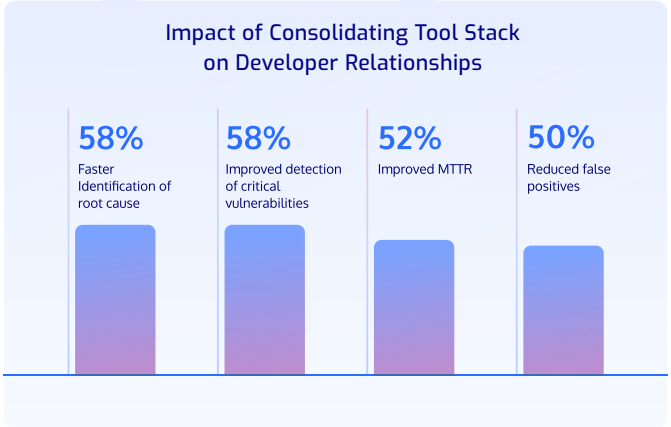
90% **of security professionals** with a commercial ASPM platform say their organization has a systematic way of understanding overall risk and are always working on the most important vulnerabilities.

Likewise, almost all (97%) security professionals surveyed who have consolidated their security tool stack to some degree say that doing so has improved their relationship with developers in a number of ways.

97%

who have consolidated their security tool stack have seen an improvement in their relationship with developers.

This includes faster identification of root cause, improved detection of critical vulnerabilities, improved MTTR, and reduced false positives.



How Can Cycode Help?

5 Minutes

Time to value and enhanced visibility

99%

Reduction in the number of critical vulnerabilities

200%

Increase in remediated vulnerabilities month over month

About Cycode

Cycode is the leading Application Security Posture Management (ASPM) providing Peace of Mind to its customers. Its Complete ASPM platform delivers safe code, faster. That means stopping application risk before it starts, reducing developer productivity tax, and lowering the total cost of ownership.

The platform can replace existing application security testing tools or integrate with them while providing cyber resiliency through unmatched visibility, risk driven prioritization and just in-time remediation of code vulnerabilities as scale. Cycode's Risk Intelligence Graph (RIG), the 'brain' behind the platform, provides traceability across the entire SDLC through natural language.

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 A DEMO

THE STATE OF

ASPM

2025

PRESENTED BY cycode