EBOOK

brinqa

The No BS Guide to ASPM

What you need to know about Application Security Posture Management

THE PROBLEM WITH APPSEC TODAY

The business landscape has evolved due to pandemic changes, digital transformation pressures, and shifting consumer behaviors driving organizations to lean heavily into software.

Organizations are building more software than ever, with development now outpacing traditional security processes. Understanding your application security at any moment has become harder than ever. The rapid scaling of cloud environments has inadvertently expanded the attack surface, leading to numerous vulnerabilities ripe for exploitation. Merely identifying these security flaws is not enough; organizations become liable for potential breaches without fixing them.

To counter this, a comprehensive and dynamic approach involving Application Security Posture Management (ASPM) is required, a method that evolves application security. ASPM integrates various technologies and automation strategies, enabling organizations to identify, assess, prioritize, and address vulnerabilities, ensuring they don't fall behind in the ever-evolving cybersecurity landscape.

ASPM, by unifying all application security findings, fills a critical - and previously missing - piece of the AppSec puzzle and aligns remediation priorities with business priorities. ASPM abstracts out your toolset to create a bird's eye view of your application security posture, ensuring that potential vulnerabilities are identified, prioritized, and mitigated across the software development life cycle, enabling organizations to gain improved visibility, control, and strategic planning in their security framework, fostering collaboration, efficiency, and adaptability. Blending integrated risk assessment, real-time monitoring, and the ability to scale, ASPM is emerging as a vital element in contemporary software development, presenting a new frontier in securing today's complex and fast-paced, digitally interconnected world.

WHAT IS APPLICATION SECURITY POSTURE MANAGEMENT (ASPM)?

ASPM is an approach that evolves how organizations handle application security. It provides a dynamic solution to manage and enhance the security stance of an organization's diverse set of applications. Instead of a disjointed view of security findings, which leads to inefficiencies and security gaps, ASPM unifies and contextualizes these findings.

This is critical to properly prioritize exposures and identify which findings are related to which applications, which also assists in identifying systemic problems across application portfolios. Once identified, ASPM helps orchestrate the remediation ticketing and tracking process.

How Does ASPM Work?

As organizations "shifted left" they accumulate various technologies and approaches to Application Security (AppSec), creating silos that ASPM unifies. It seamlessly integrates into existing workflows and processes, decreasing dependence on manual interventions and optimizing assessment and remediation procedures.

Integrating and utilizing specialized application security tooling is an integral part of ASPM. These tools can include everything from Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) tools to Interactive Application Security Testing (IAST) tools and Software Composition Analysis (SCA) tools. This comprehensive tooling helps identify and mitigate potential vulnerabilities throughout the different stages of the software development life cycle.

ASPM also involves correlating security data gathered from multiple sources, which is then analyzed, interpreted, and triaged to provide meaningful insights. This process helps identify the immediate security threats but also aids in understanding the underlying patterns and recurring vulnerabilities. Consequently, based on these insights, organizations can create and enforce effective application security policies tailored to their unique needs.

The holistic approach of ASPM grants improved visibility over the organization's security posture, enabling them to comprehensively view their application security landscape.

This, in turn, facilitates informed decision-making and strategic planning to bolster their overall security framework.

Why Does ASPM Matter?

ASPM is emerging as a vital element in contemporary software development and is especially crucial in enhancing the maturity of your DevSecOps program. This surge in recognition is not sudden but is an evolution of existing techniques and technologies, including CI/CD pipelines, integrated with a rising focus on security in today's fast-paced, digitally interconnected DevOps world. In fact, Gartner predicts that by 2026, over 40% of organizations developing proprietary applications will adopt ASPM to more rapidly identify and resolve application security issues.*

OF ORGANIZATIONS DEVELOPING APPLICATIONS WILL ADOPT ASPM IN THE NEXT 3 YEARS

*Source: Gartner Innovation Insight for Application Security Posture Management, May 2023

Pioneering companies have been incorporating aspects of what we now label ASPM into their AppSec and DevSecOps practices for some time. Still, these methods and techniques have only recently been formalized and identified as a distinct part of the application security playbook. They often refer to it as their AppSec team doing vulnerability management or their vulnerability management team overseeing AppSec findings. None of which showed a clear delineation of ownership or operations.

With the current state of software development, characterized by rapidly increasing development speeds and complexity, ownership and defined processes are necessary for security. Doing this requires robust and integrated CI/CD pipeline security processes. Without these security measures embedded in the development pipeline, the risk to an organization escalates dramatically.

What Are the Benefits of ASPM?

ASPM presents numerous benefits that significantly advance the security posture of an organization. One of the key advantages is the elimination of application security silos. By fostering an environment of collaboration and transparency, ASPM integrates various aspects of application security into a coherent whole.

This integrated approach:

1. Breaks down the barriers between different teams and their respective responsibilities
2. Ensures a consistent and cohesive approach to application security
3. Provides clearer directives for what to fix now
4. Focuses development resources on fixing what matters
5. Fosters trust between security and engineering teams

Using ASPM also leads to improved visibility of application security controls, allowing organizations to gain a comprehensive overview of their security posture. With this enhanced perspective, vulnerabilities can be prioritized and triaged more effectively, leading to a more efficient use of resources in addressing exposures. In addition to this, ASPM facilitates streamlined remediation and mitigation processes, enabling organizations to respond quickly and decisively to identified vulnerabilities. SANs research has shown that attackers discover and pursue vulnerabilities in less than 7 days after release, but most organizations take almost 30 days to resolve them.

What's more, ASPM yields trustworthy and actionable reports that can be utilized by security teams, developers, and leadership alike. These reports provide valuable insights into the state of application security, informing strategic decision-making and facilitating ongoing improvement efforts.

Unlike conventional security measures that often provide only a snapshot of an organization's security posture, ASPM offers a continuous view, enabling real-time monitoring and adjustment of security controls.

This constant approach enables organizations to stay ahead of evolving threats and vulnerabilities, ensuring the ongoing maturity of their security posture.

ARE YOU READY FOR ASPM?

Before diving headfirst into ASPM, organizations must evaluate their preparedness. This assessment should not be overlooked, as it is the foundation for effective and efficient ASPM implementation.

Organizations should thoroughly review their existing AppSec tools and other relevant data sources such as pen tests, audits, or bug bounty programs to get started.

- What scanners are in place?
- How much data is being generated by these tools?
- How is the organization managing this plethora of information?
- How is the organization prioritizing these findings?
- Are they exporting snapshots to CSV files or working within the user interfaces of each respective tool?

The answers to these questions give an organization a clear picture of its current state, aiding in the decision-making process for ASPM adoption. Moreover, organizations should also scrutinize their current methods of prioritizing findings for remediation. Are these processes effective and efficient? Or do they leave room for potential threats to slip through the cracks?

In the context of fast and large-scale development, this readiness assessment can empower developers to embrace ASPM, even if there are gaps in their existing tooling and processes. Implementing ASPM can help identify these gaps and prioritize the organization's approach to application security risk. The transformation that ASPM brings to an organization is not just about introducing a new tool; it's about refining and enhancing existing processes, prioritizing areas for improvement, and ultimately creating a more secure application development environment. No matter the readiness level, starting with an informed view of your current position will help guide your journey toward a robust and mature application security posture.

HOW TO GET STARTED WITH ASPM

The first step in implementing ASPM within an organization is identifying and engaging key stakeholders in the process. This collective involvement ensures a holistic understanding of the organization's security posture, setting the stage for informed decision-making.

Next, you must evaluate different ASPM tools with your specific use cases. Look for compatibility across all your applications – from legacy to new and everything in between. Finding an ASPM solution that seamlessly integrates with your existing development process and ticketing systems like Jira is crucial. This way, developers won't have to adopt an entirely new toolset, but instead, the security measures will work within systems and processes they're already familiar with. This smooth integration improves the developer experience, unifies the workflow, and streamlines security operations.

Another vital aspect to consider during ASPM implementation is risk assessment and threat modeling. An in-depth understanding of your applications' potential risks and threats will provide a roadmap for prioritizing security measures. Similarly, ensuring your chosen ASPM solution can scale with your organization and effectively monitor its performance is pivotal for maintaining a solid security posture.

Finally, supporting user adoption and training is vital to successful ASPM implementation. Ensure that all team members, from developers to security analysts, are well-equipped to leverage the new tools and procedures. This training will increase user adoption rates and amplify your ASPM initiative's effectiveness, promoting your organization's robust, mature, and secure application development environment.

See the checklist ⟶

Getting Started Checklist

1

Engage Key Stakeholders

Identify and involve stakeholders for a comprehensive understanding of security posture and informed decision-making.

2

Evaluate ASPM Tools

Assess tool compatibility, seek integration with existing processes and systems, and prioritize familiarity for developers.

3

Prioritize Risk Assessment and Threat Modeling

Analyze risks, prioritize security actions, and ensure ASPM aligns with risk mitigation strategies.

4

Ensure Scalability and Performance Monitoring

Verify tool scalability, monitor security performance, and adapt measures as the organization grows.

5

Support User Adoption and Training

Train team members, boost user adoption, and highlight ASPM value for a mature and secure development environment.

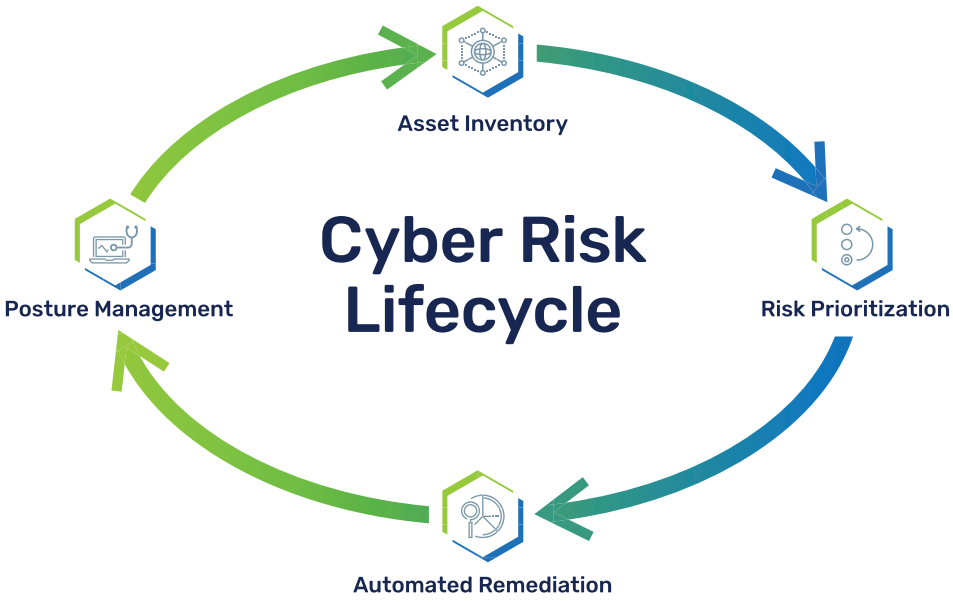
THE BRINQA APPROACH TO APPLICATION SECURITY POSTURE MANAGEMENT

Brinqa offers a powerful ASPM platform, providing an automated solution that spans every stage of the lifecycle - from unifying AppSec findings, prioritizing risks, and streamlining remediation, to producing insightful reports that motivate the business to act.

This automation not only bolsters efficiency and facilitates informed decision-making but also reduces human error and minimizes business disruptions, ultimately leading to a more secure application as a result of a stronger security posture.

The Brinqa Difference

The Brinqa platform sets itself apart through its distinctive approach to ASPM. One of its key differentiators is its comprehensive coverage of the entire cyber risk lifecycle. While other solutions might address only a segment of the lifecycle, Brinqa ensures seamless management from asset inventory through risk prioritization, automated remediation, and posture management, offering a holistic view of application security.



Moreover, Brinqa stands out because of its breadth of support for different data sources combined with a unified graph database, which correlates all your AppSec findings with your business context and threat intelligence. This comprehensive and cohesive view of your security landscape enables highly effective risk scoring and prioritization.

The transparency of the process allows both security and development teams to understand the scoring methodology, fostering trust and enabling customization according to specific business needs.

Streamlining the remediation process is another critical differentiator for Brinqa. It aids security teams in quickly identifying the developers responsible for addressing specific vulnerabilities and accelerating remediation. Brinqa's solution features bi-directional sync with ticketing systems and provides mechanisms to validate whether fixes have been implemented.

reduction in dev time spent on security tools

reduction in time spent by security teams creating reports

Lastly, the Brinqa platform offers a powerful report builder, enabling businesses to tailor reports to their needs. Since Brinqa encompasses the entire cyber risk lifecycle, it provides reliable and trustworthy data that offers a comprehensive view of your security posture. The transparency and accuracy of these reports foster trust among stakeholders, positioning security teams as trusted advisors within the organization.

From Fragmented Tools to Cohesive Security:

A Fortune 500 Journey

A Fortune 500 financial services company was facing significant challenges securing its software development process. Attempting to produce vulnerability-free code with a staggering 500-1000 software builds a day, they utilized a broad set of AST tools, including Fortify (SAST), Burp Suite (pen test), Nexis (FOSS), and insider threat analysis. However, this tool-based security view was slowing down the development process. Developers had to log into 10 separate AST tools to understand app risk, leading to an inefficient workflow with no unified view of risk across all applications. Additionally, there was a lack of clarity regarding organizational app risk ownership and no method for comparing their risk management to other organizations.

The customer used the Brinqa Platform to develop consistent scoring and reporting methodology for application security risk. The goal was to harmonize various inputs, including pen test results, vulnerability management, static code analysis, and free and open-source software (FOSS) used in application development. Brinqa enabled the customer's IT risk and application security teams to operationalize this vision by providing a single cyber risk graph for collecting, analyzing, and scoring data. This facilitated the systematic assessment of risk factors, ensuring that crucial information could be accurately reported to executive management and business product line owners. With Brinqa, the customer created a cohesive and transparent process to gauge and manage application security risk.

With the integration of risk evaluation gates into their entire CI/CD pipeline, the company achieved a breakthrough in its application security posture. They managed to ship vulnerability-free code more efficiently, resulting in a 10x reduction in developer time spent on security tools and an 85% reduction in the security team's monthly time preparing risk reports. Decisions regarding business application risk shifted from a cumbersome monthly evaluation to real-time assessments. This change boosted development efficiency and security, instilling confidence in addressing accurate AST findings. Prioritization became tailored to their environment and business, fixing critical vulnerabilities promptly and aligning security with the company's risk profile.

Get Started with Brinqa

Don't let the onslaught of application security vulnerabilities overwhelm your organization with a flood of data from too many sources. With Brinqa, you benefit from a platform that orchestrates the entire cyber risk lifecycle across all your security tools, teams, and programs. Gain a live model of all assets, vulnerabilities, and relationships across the attack surface and enjoy context-rich risk scoring tailored to your unique business priorities. Brinqa enables you to report risk in terms that the rest of your business can understand and trust, bridging the gap between business applications, business units, and risk owners to foster a stronger security culture. Join industry leaders worldwide who are already securing their applications with Brinqa.

Book a demo today to discover how Brinqa can transform your organization's application security posture.

brinqa

Companies that use Brinqa remediate the vulnerabilities that matter to their business. Brinqa is the only solution that streamlines remediating the vulnerabilities that matter to the business across vulnerability, cloud, and application security programs in a single platform. CISOs, security program leaders, and their security teams rely on Brinqa to orchestrate the cyber risk lifecycle across millions of vulnerabilities and dozens of detection tools. The Brinqa Platform provides a unified view into all security tool findings, prioritizes vulnerabilities based on business context, and automates the remediation process so security teams can reduce more risk, communicate effectively and motivate business owners to act – all at enterprise scale. Brinqa is trusted by the world's leading brands, including Adidas, Nestle and Rolls Royce, and has been recognized as a leading vendor by Gartner, Forrester, IDC, GigaOm and G2. Based in Austin, Texas, Brinqa is backed by Insight Partners. Learn more at **www.brinqa.com.**