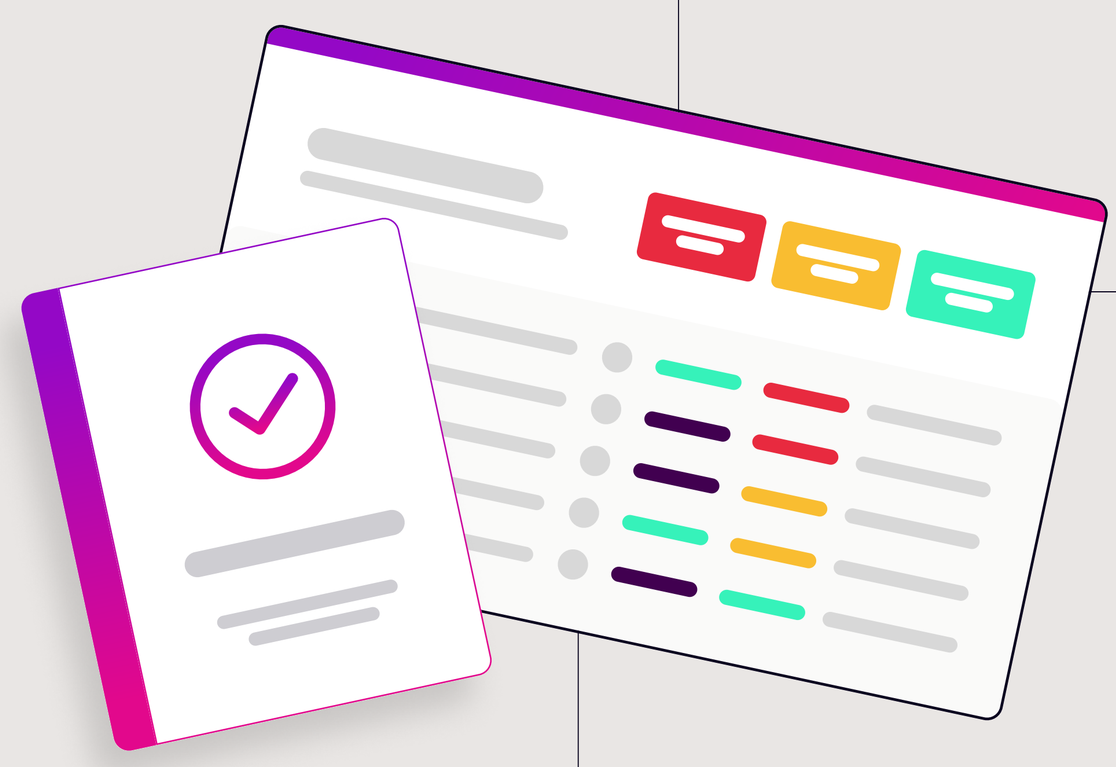
seemplicity

A Security Leader's Guide to ASPM



GUIDE

Applications are the foundation of modern organizations, but their complexity has outpaced traditional security measures. With every release cycle, security leaders face the challenge of enabling innovation while safeguarding a dynamic attack surface. The rise of cloud-native architectures, Continuous Integration/Continuous Deployment (CI/CD) pipelines, and microservices has introduced unprecedented agility – but also significant risks.

Application Security Posture Management (ASPM) represents a paradigm shift, designed to address these modern challenges. By integrating seamlessly into DevSecOps practices, ASPM consolidates data, streamlines workflows, and prioritizes vulnerabilities, enabling organizations to embed security throughout fast-moving development cycles without slowing innovation. It bridges the gap between security and development, ensuring risks are addressed early while maintaining control and visibility.

This guide is tailored to help security leaders overcome their most pressing challenges, whether it is accelerating remediation, improving cross-team collaboration, or scaling security efforts in alignment with business goals. By adopting ASPM, organizations can not only reduce risk but also strengthen their DevSecOps practices to support long-term resilience and growth.

Adapting Security Strategies to Modern Challenges

Security leaders must navigate increasingly diverse technology environments, accelerated development cycles, and sophisticated attack vectors while ensuring vulnerabilities are addressed quickly and efficiently. To meet these challenges, adapting security strategies is not optional; it is essential for safeguarding applications without hindering innovation. These demands require a rethinking of traditional approaches, as security leaders grapple with challenges such as:

COMPLEXITY OF MODERN ENVIRONMENTS

Cloud-native architectures, hybrid cloud strategies, and microservices have revolutionized how applications are developed and deployed, allowing organizations to innovate and scale rapidly. However, these advancements also create sprawling attack surfaces that are challenging to monitor and secure consistently. Each environment introduces unique vulnerabilities that require tailored remediation plans. Security leaders must navigate this complexity while ensuring they do not disrupt business-critical application development – a balancing act that calls for more integrated and adaptive strategies.

ACCELERATED DEVELOPMENT PIPELINES

The speed of modern development cycles is another major challenge for security leaders. Agile methodologies and DevSecOps practices have enabled rapid innovation, with 71% of businesses reporting that they deploy application updates at least once a week (2024 State of Application Security Report, CrowdStrike).

While this pace allows businesses to stay competitive, it also increases the likelihood of vulnerabilities being introduced during development. CI/CD pipelines, which drive these accelerated workflows, are highly effective but leave little time for traditional security reviews. Alarmingly, only 54% of major code changes undergo a full security review before being deployed to production (2024 State of Application Security Report, CrowdStrike), leaving significant gaps that attackers can exploit. Security leaders are faced with the near-impossible task of ensuring that vulnerabilities are addressed without slowing down these high-velocity pipelines.

71% of businesses deploy application updates at least once a week.

54% of major code changes undergo a full security review

Source: CrowdStrike 2024 State of Application Security Report

EVOLVING ATTACK VECTORS

As development practices evolve, so do attack methods. Applications have become primary targets for cyber threats, with 50% of organizations reporting that their applications were compromised in the past year (2024 Application Security Report, Fortinet). Attackers increasingly exploit vulnerabilities in both pre-production and production environments, targeting not only internal code but also third-party libraries and dependencies. Software supply chain attacks, such as those exploiting compromised packages or open-source vulnerabilities, have added another layer of complexity for security leaders. Protecting applications now requires a comprehensive approach that secures every aspect of the software development lifecycle (SDLC), from internal development processes to external integrations.

50%

of organizations reported that their applications were compromised in the past year

Source: 2024 Application Security Report, Fortinet

DEMAND FOR HOLISTIC VISIBILITY

Fragmented tools and siloed data further exacerbate the challenges faced by security leaders. Without a unified view of vulnerabilities across the SDLC, it is a struggle to assess risk comprehensively or prioritize efforts effectively. This lack of visibility can lead to blind spots, where vulnerabilities go undetected or unresolved, compounding the risk of exploitation. For organizations managing complex environments, the inability to achieve holistic visibility creates a significant barrier to effective security operations.

SLOW REMEDIATION AS A BOTTLENECK

Security scanning tools are essential for detecting and identifying vulnerabilities, but the sheer volume of findings they generate often overwhelms security teams. Instead of streamlining remediation efforts, this excessive noise creates additional challenges, ironically slowing down time to resolution. According to Seemplicity's 2024 Remediation Operations Report, 51% of organizations report that the noise generated by their security scanning tools is high, resulting in slow or delayed remediation. In fact, 70% of critical incidents take longer than 12 hours to resolve (2024 State of Application Security Report, CrowdStrike), leaving organizations exposed to potential exploitation for extended periods.

For modern development cycles, which leave little room for slow remediation processes, this disconnect between the speed of development and the inefficiency of remediation not only heightens risk but also disrupts collaboration between security and development and operations teams. The inability to resolve vulnerabilities quickly undermines the agility of the entire development process, creating frustration and friction across departments.

51%

of organizations say the level of noise generated by scanning tools is high

70%

of critical incidents take longer than 12 hours to resolve

Source: 2024 Remediation Operations Report, Seemplicity | 2024 State of Application Security Report, CrowdStrike

Strategic Benefits of ASPM for Security Leaders

With increasing complexity in application development and a growing volume of vulnerabilities to manage, traditional approaches often leave critical gaps. ASPM addresses these challenges by delivering strategic advantages that align security efforts with organizational goals.

CENTRALIZED OVERSIGHT

One of the key benefits of ASPM is its ability to consolidate data from fragmented tools and environments into a single, unified platform. This centralized oversight provides visibility into vulnerabilities across applications and environments, enabling security leaders to maintain situational awareness and make informed, organization-wide decisions. By eliminating blind spots and delivering actionable intelligence, ASPM allows security leaders to manage risks and maintain control over their organization's security posture.

PROACTIVE RISK MANAGEMENT

Traditional security practices often rely on reactive approaches, addressing vulnerabilities only after they are identified through periodic scans or external threats. ASPM shifts this paradigm by embedding security into the entire SDLC, enabling a proactive stance. Continuous monitoring of applications ensures that vulnerabilities are constantly detected and assessed, reducing the risk of exploitation. This proactive approach helps security leaders anticipate risks before they escalate, allowing for innovation without compromising security.

STRATEGIC PRIORITIZATION

61% of organizations identified prioritization as one of their top three challenges (2024 State of Application Security Report, CrowdStrike). Without effective prioritization, teams often waste time deciding what to focus on or, worse, allocate resources to low-priority tasks that do little to reduce overall risk. ASPM ensures vulnerabilities are addressed in alignment with organizational objectives by factoring in aspects such as exploitability, application criticality, and business impact.
By doing so, ASPM reduces the noise created by low-priority findings and ensures resources are allocated where they are needed most, streamlining remediation efforts and reducing the risk of high-impact exploits.

61%

of organizations identified prioritization as one of their top three challenges

Source: 2024 State of Application Security Report, CrowdStriket

ENHANCED CROSS-TEAM COLLABORATION

Collaboration between security, development, and operations teams is essential for addressing vulnerabilities effectively, yet organizational silos often stand in the way. Development and operations teams are driven by speed and delivery, while security teams focus on mitigating risk, leading to misaligned priorities, communication gaps, and unclear ownership of vulnerabilities. ASPM breaks down these silos by providing unified visibility and actionable context for all teams. This alignment reduces friction, improves accountability, and ensures that vulnerabilities are addressed consistently and efficiently across teams, without slowing down development timelines.

COST OPTIMIZATION

Managing application security efficiently is not just about mitigating risk but also about maximizing the return on security investments. ASPM enhances the ROI of existing tools by effectively managing the constant flow of findings from said tools and minimizing redundant processes, enabling teams to resolve vulnerabilities faster with fewer resources. It reduces operational inefficiencies, such as manual tasks or duplicated efforts, while providing measurable metrics like reduced Mean Time to Remediate (MTTR). For security leaders, this efficiency translates into tangible cost savings and provides data-backed evidence of value to executive stakeholders.

PROGRESS TRACKING

Without clear visibility into remediation workflows, vulnerabilities can linger unresolved, bottlenecks go unnoticed, and critical timelines slip, increasing exposure to risk. ASPM solves this challenge by offering real-time tracking of remediation progress, enabling security leaders to monitor timelines, identify delays, and ensure service level agreement (SLA) adherence. This level of visibility not only allows security leaders to showcase measurable progress but also helps identify and eliminate workflow inefficiencies. With ASPM, remediation outcomes are no longer left to chance – teams can demonstrate clear impact and accountability, aligning security efforts with business goals.

Getting Started with ASPM

Implementing an ASPM solution requires careful planning to ensure alignment with organizational goals and operational efficiency. Security leaders play a key role in managing the practical aspects of ASPM adoption, from identifying use cases to demonstrating its impact within your teams. The following steps provide a practical framework for getting started with ASPM.

CONDUCT A GAP ANALYSIS

Evaluate the effectiveness of your current tools and workflows to identify inefficiencies or blind spots that ASPM can address. Focus on areas where your teams struggle, such as noise from scanning tools or bottlenecks in remediation workflows. A thorough gap analysis helps pinpoint specific problems that ASPM can solve, ensuring a smoother implementation process.

INITIATE A TARGETED PILOT

Start small to demonstrate ASPM's value quickly. Choose a manageable scope, such as high-risk applications or critical workflows, for your ASPM pilot. A targeted pilot is an opportunity to validate the tool's capabilities, gather feedback from your teams, and refine workflows. A successful pilot will highlight ASPM's ability to improve day-to-day operations and pave the way for broader adoption.

DEFINE TEAM-LEVEL METRICS FOR SUCCESS

Identify measurable goals that matter to your teams, such as improving SLA compliance, reducing remediation delays, or streamlining cross-team collaboration. These metrics will help evaluate the operational impact of ASPM and provide the data needed to communicate its value to senior leadership.

COLLABORATE WITH STAKEHOLDERS TO BUILD SUPPORT

Work closely with your teams and other departments, such as development and IT, to ensure alignment during the ASPM rollout. Share pilot results and use real-world examples to demonstrate ASPM's value. Effective collaboration will help secure buy-in from senior leadership and other key stakeholders, ensuring a smooth transition to full implementation.

ASPM as an Operational Enabler for Security Leaders

ASPM represents far more than just a technical solution – it is a transformation that enables security leaders to align their teams, processes, and tools with broader organizational objectives. ASPM equips security leaders with the tools to streamline workflows, prioritize effectively, and scale operations efficiently. By centralizing fragmented data and automating critical processes, it fosters collaboration and ensures vulnerabilities are addressed quickly and consistently.

Beyond operational improvements, ASPM enables security leaders to align their efforts with overarching business priorities, improving metrics such as SLA adherence and Mean Time to Remediate (MTTR). By driving measurable results and reducing inefficiencies, ASPM positions security leaders as key enablers of innovation and resilience, ensuring their teams deliver both security and value at scale.