seemplicity

CHECKLIST

Is Your Application Security Falling Behind?

Application Security Posture Management (ASPM) provides organizations with the tools to gain comprehensive visibility, streamline prioritization, and address vulnerabilities proactively.

Determining whether your organization needs an ASPM solution begins by analyzing your current application security challenges. Are you struggling to gain full visibility into your application landscape? Do you find it difficult to prioritize risks effectively or manage remediation efforts in a timely manner?

This comprehensive checklist is designed to help you evaluate your readiness, pinpoint gaps in your remediation processes, and decide if implementing an ASPM solution is a strategic fit for your organization's needs.

ASPM Checklist for Effective Application Security

Review each statement below and mark the items that reflect your current environment or challenges. The more boxes you check, the stronger the case for integrating an ASPM solution to enhance visibility, workflow efficiency, and risk reduction.

Each statement is accompanied by examples to highlight the challenges, serving as context rather than individual options to choose from.

LIMITED VISIBILITY ACROSS APPLICATIONS AND ENVIRONMENTS

- You lack a unified dashboard and struggle to gain complete visibility over your full application landscape.
- Managing software vulnerabilities is challenging due to fragmented tools and siloed data.
- It is difficult to identify vulnerabilities, risks, and blind spots across environments.

Without centralized oversight, it becomes difficult to identify vulnerabilities, risks, and blind spots across applications and environments, making proactive security nearly impossible.

GAPS IN FULL SDLC MONITORING

- Application security controls are applied only at certain stages of the Software Development Lifecycle (SDLC).
- Risks from code changes, third-party libraries, or supply chain components are not systematically managed.
- Security efforts tend to be reactive rather than integrated across all development phases.

Securing applications effectively requires integration across all stages of the SDLC. Without a comprehensive approach, risks can slip through unnoticed, leaving critical vulnerabilities unaddressed.

DIFFICULTY PRIORITIZING VULNERABILITIES

- The volume of vulnerability findings makes it challenging to identify and address business-critical risks promptly.
- Differences in risk metrics across different data sources result in inconsistent risk assessments.
- Limited context around vulnerabilities makes it difficult to determine which issues should be prioritized.

Managing vulnerabilities is challenging when critical issues are overlooked, and less urgent risks consume resources. Without clear prioritization, remediation becomes inefficient and business-critical risks go unaddressed.

MANUAL, SLOW, AND FRAGMENTED REMEDIATION WORKFLOWS

- Remediation is managed through emails, spreadsheets, or other manual processes.
- High mean-time-to-remediate (MTTR) persists due to workflow inefficiencies.
- Vulnerabilities remain unaddressed for extended periods, increasing exposure to risk.

Inefficient and manual workflows slow down remediation efforts, leaving vulnerabilities unaddressed longer and increasing your organization's exposure to unnecessary risks.

NOISE OVERLOAD FROM SECURITY TOOLS

- Your team is overwhelmed by false positives and redundant findings from various security scanners.
- Excessive noise delays response times and makes it harder to focus on real threats.
- Resource constraints are exacerbated by constant triage of irrelevant alerts.

Dealing with excessive noise makes it harder to focus on real threats, leaving your applications vulnerable and your team stretched thin.

COLLABORATION SILOS BETWEEN SECURITY, DEVELOPMENT, AND OPERATIONS

- Communication gaps exist among Security, Development, and Operations teams.
- Misaligned priorities and lack of shared context delay remediation efforts.
- Teams face friction and collaboration challenges due to using different tools and unfamiliar platforms.

When teams lack a shared understanding of what needs to be fixed and why, response times suffer and remediation efforts become inconsistent.

NO CONTINUOUS PROGRESS TRACKING AND SLA MANAGEMENT

- There is limited or no insight into the status of ongoing remediation tasks.
- Tracking adherence to remediation Service-Level Agreements (SLAs) is difficult.
- Accountability for security outcomes is hard to assign due to a lack of transparency.

Limited visibility into remediation efforts and SLA adherence can make it challenging to ensure accountability and maintain efficient workflows, leaving gaps in your security posture.

LACK OF ROI FROM EXISTING SECURITY TOOLS

- Existing application security tools produce large volumes of data but lack actionable insights.
- Automation is limited or non-existent, making it hard to optimize workflows.
- Integration with other security tools is challenging, hindering the implementation of a comprehensive security strategy.

Security tools that produce excessive data without clear insights or automation can make managing security overwhelming, often creating more problems than they solve.

What Do Your Results Reveal?

If you checked several boxes on this checklist, it's a clear sign that your organization is dealing with operational friction, blind spots, and inefficiencies that can hinder performance and increase risks. These challenges are exactly what ASPM is designed to address.

By providing a unified approach to managing and improving your application security posture, ASPM helps close gaps, streamline processes, and enhance overall efficiency.

The more pain points you identify, the greater the opportunity to unlock significant improvements and ensure your systems are secure, effective, and aligned with your organizational goals.