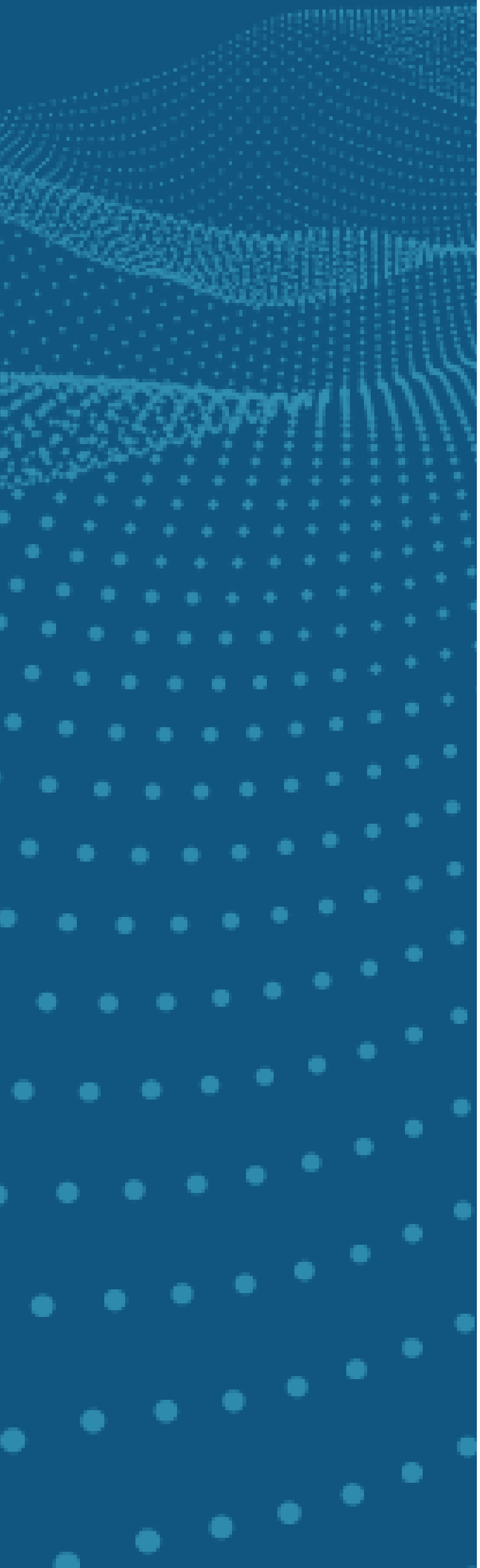

GUIDE

Increase Enterprise AppSec Risk Visibility with ASPM

Overview

Just as digital transformation has changed every business into a software business over the past few decades, so too has it made clear that software risk is business risk. Organizations in every industry sector are developing more and more software, which means that teams, tools, and processes have proliferated. This makes it increasingly difficult to see and understand AppSec risk across your whole enterprise. And without access to high-level risk information, you cannot provide an accurate snapshot of your risk posture to your executives, the board, partners, and customers.

Further, if you cannot see your risk posture, your organization is jeopardizing its ability to comply with industry and government compliance mandates. A fragmented view of risk means that your compliance audits will take much longer than necessary.

What organizations need is a risk management tool that provides identification, prioritization, and risk visibility across all stages of software development.

You Can't Fix What You Can't See

A comprehensive view of your risk posture allows you to assess risk from any point in your development cycle and gather insight across your entire organization. However, gaining this view can be complicated by several factors. A recent analyst report found that 42% of organizations cited gaining visibility into testing results as their top challenge.

Tool proliferation is a common roadblock to AppSec visibility. A recent survey by ESG found that 70% of organizations use 11 or more application security testing (AST) tools, and that doesn't even take into account vulnerability management platforms, custom BI dashboards, and manual testing tools. This tool proliferation adds increased complexity and cost, and as your software footprint grows, this patchwork of technologies and data sources impedes your development agility.

Development teams are forced to add time and resources to train, support, and maintain these tools. Moreover, when issues are stuck in point tools, remediation efforts become inefficient and you can't gain a clear picture of risk. Tool proliferation makes it nearly impossible to keep track of what was tested and what was fixed, and that makes prioritization difficult.

As software increases in volume it also is increasing in complexity. This complexity means more security tools, more tests, and more results—all of which impede, rather than improve visibility. It also drains resources and becomes unmanageable at scale. Too often, developers receive duplicate testing results and inefficient, noncontextual remediation guidance. This requires them to waste valuable time and resources triaging security issues before they can even hope to start fixing them. The effort required to manage tools, perform maintenance, and integrate tools into existing environments can result in releasing software that developers know is not secure or that has vulnerabilities.

Compliance is a crucial responsibility for any enterprise development program, especially for organizations that manage payments, handle sensitive customer or patient data, or operate in a regulated market. Demonstrating compliance with specific standards is crucial to maintaining customer trust and avoiding legal or regulatory penalties, and highly regulated industries need to maintain tight controls on data and uphold system redundancy. When you lack visibility into your risk, you cannot meet your compliance obligations.

ASPM Allows You to See Your Risks, so You Can Fix Your Risks

Application security posture management (ASPM) solutions give teams a single place to manage their entire AppSec program. These tools align security and development teams by providing a consolidated view of what's been tested, what's been found, and what's being fixed.

ASPM solutions correlate and analyze data from a variety of sources to simplify issue interpretation, triage, and remediation. They also administer and orchestrate security tools to implement security policies. With ASPM, security teams can centrally manage application security findings via a consolidated view of security and risk status across the entire software development environment.

ASPM provides granular visibility into application security posture at every stage of the software development life cycle (SDLC). This allows you to establish policies and processes to address that risk in an organized manner, across your entire enterprise. You can consolidate your AppSec program, accelerate and automate your workflows, and centralize your risk visibility. ASPM does this by

- Providing a 360-degree view of risk scoring, findings, and key performance trends for all your projects and code sources
- Mapping findings to regulatory compliance standards (including NIST, PCI, HIPAA, DISA, OWASP Top 10) and providing audit reports for critical violations
- Delivering both UI- and API-based workflows to create, enforce, and monitor security policies across software assets and components
- Enabling security teams to specify risk thresholds for issue types, desired application security testing tooling, SLAs on remediation time for fixes, and required notifications to development stakeholders

Gaining visibility into your software and components is an enormous task that can require tracking thousands of distributed sources. Point solutions offer a limited view of software issues, and each has their own means for classifying risk. This results in an unclear and fragmented picture of compliance posture and no uniform way to implement AppSec across tools and teams.

ASPM solutions simplify your AppSec programs by bringing together testing, policy, and orchestration to integrate security activities intelligently and consistently across the SDLC. The visibility they enable allows your security and development teams to make informed decisions based on a single source of truth and deliver resilient applications at scale.

Prioritize Business Risk

After ASPM presents an overview of your AppSec risk, you can begin to use it to prioritize issue remediation. ASPM enables organizations to quickly and accurately understand their risk posture and then prioritize how to address those risks. It also provides a centralized way to connect security data, software resources, policies, and insights, so organizations can make quick, informed decisions to immediately bolster their security posture. ASPM allows you to

- Escalate critical defects based on risk and send them to developers
- Correlate and deduplicate issues, so teams can prioritize fixes without additional time spent triaging
- Prioritize issues based on business risk so developers can focus on fixing high-impact issues
- Simplify AST management with UI- and API-based workflows that create, enforce, and monitor security policies across your software assets and components

ASPM enables your security teams to specify risk thresholds for issue types, desired application security testing tooling, SLAs on remediation time for fixes, and required notifications to development stakeholders. All this allows you to streamline remediation to prioritize your highest business risk items, thereby consolidating your risks.

Map Compliance Violations

If your organization manages payments, handles sensitive customer or patient data, or operates in a regulated market, you may need to demonstrate compliance with specific standards to maintain customer trust and avoid legal or regulatory penalties. ASPM solutions can help you integrate software testing into your development workflows, focus analyses and remediation on compliance objectives, and report against the software standards that are most important to your business. An ASPM solution can help you keep up with compliance by

- Automating adherence to regulatory standards by leveraging policy workflows to codify conditions for testing and vulnerability management
- Embedding controls within pipelines through compliance-as-code
- Speeding up compliance reporting by mapping findings to regulatory compliance standards (including NIST, PCI, HIPAA, DISA, OWASP Top 10) and providing audit reports for critical violations

ASPM solutions enable your organization to make a uniform assessment of your software risk posture. This means that teams can trim their time to audit by leveraging ASPM compliance mapping and reporting, which traces individual findings to regulatory standards, down to the line of code.

How Black Duck Can Help

Black Duck Software Risk Manager™ is an on-premises ASPM solution that enables security and development teams to simplify their application security programs to improve risk posture.

It brings together policy, orchestration, issue correlation, and built-in static application security testing (SAST) and software composition analysis (SCA) engines to integrate security activities intelligently and consistently across the SDLC.

Software Risk Manager spans manual and automated AST, software resources, and development tools to provide a holistic context of risk. It allows you to implement automatic policies that prioritize issues based on business risk. And it aids in compliance by supporting more than 20 compliance standards including HIPPA, NIST, and OWASP Top 10, enabling you to map individual findings to regulatory violations.

With Software Risk Manager, security and development teams can make informed decisions from a single source of truth and deliver resilient applications at scale.

Learn more about Software Risk Manager

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.