DARKReading

WHITE PAPER

Managing Risk at Scale: How to Gain Visibility, Quiet the Noise, and Secure Applications Across the Enterprise

Sponsored by

BLACKDUCK®

Today, software has become the backbone of business across all sectors, with development growing exponentially in the last decade. More applications than ever need to be secured, with complex AI-fueled environments and supply chains only increasing the complexity for overworked security teams. These teams must ensure application security at scale while facing the pressure of growing regulations and managing around the restraints of limited budgets and headcounts.

Effectively managing software application risk for the enterprise requires teams to scale application security across the SDLC, all business units, organizational silos, and thousands of applications growing in volume and sophistication. Many organizations try throwing security tools at the problem, but this often only increases the complexity and operational inefficiency of the security program and the frustration of developers and security teams.

Today's organizations must embrace a "shift everywhere" approach, driven by tight integrations throughout the SDLC, intelligent automation, a consistent implementation of security policies and access to the correct tools and resources to secure software applications at scale. Fortunately, the growing adoption of application security posture management (ASPM) can provide a helpful foundation. This whitepaper will examine the challenges of modern software developers, the necessary components of securing software at scale, and examine why ASPM is the best option to manage software risk and secure applications across the enterprise.

Challenges facing today's application security teams

As businesses compete to provide the fastest, most seamless experience to a dispersed, on-the-go customer base, the need for software applications grows exponentially. Software is now the backbone of all business sectors, and regardless of industry, modern companies find themselves in the de facto software development business. Developers face increasing pressure to produce more sophisticated applications and get them to market with increasingly faster release cycles. Unfortunately, this intense focus on acceleration in development often results in security taking a back seat to speed.

Further complicating matters, today's risk landscape is more perilous than ever. More applications mean more attack surfaces for a growing population of threat actors who employ increasingly sophisticated tools and practices. Modern environments and supply chains grow increasingly complex with digitalization, cloud and GenAI. These rapidly advancing technologies help developers create code faster but can significantly increase security risks for their organizations.

MORE TOOLS MEAN MORE COMPLEXITY

Many organizations respond by throwing security tools at the problem—a recent paper by the Enterprise Strategy Group, "Cracking the Code of DevSecOps," discovered that over 70% of enterprises use more than 10 AST solutions. Collecting tools isn't the answer, as the proliferation of security tool solutions only creates more noise and complexity. Complexity adds friction, bogging down development teams and increasing the chances of frustrated developers skipping over security steps to prevent a workflow from slowing down. In addition to introducing security risks, skipped steps and practices can result in paying for tools that aren't used properly or effectively, decreasing their ROI.

When teams juggle multiple tooling solutions, risk visibility can become more complex and time-consuming. When risk data spreads across numerous tools, teams must burn valuable time aggregating dashboard data and reports to formulate an accurate view of risk. The use of disparate tools also slows developer's time to triage and remediate due to potential duplicate issues, no prioritization across tools and often a lack of actionable context or guidance surrounding issues.

REGULATORY DEMANDS AND LIMITED RESOURCES BRING ADDED PRESSURE

Today's application security teams also face significant pressure to comply with a rapidly increasing number of regulatory laws. Protecting sensitive personal data is a serious matter today—hefty fines, possible criminal prosecution, and severe reputational damage can await companies that slack on security and experience breaches compromising customer data. General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Healthcare Insurance Portability and Accountability Act (HIPPA) garner most of the headlines. Still, many other lesser-known data privacy regulations exist in states like Florida, Iowa, Indiana, Texas, Montana, and Tennessee, which all enacted strict, comprehensive privacy laws in 2023.

A lack of internal resources often makes matters more challenging for many security teams today. Organizations expect their application security teams to secure more surfaces across increasingly complex supply chains with no increase in budget or headcount. They often must succeed despite significant cutbacks in these resources.

Solutions for scaling application security across the enterprise

CREATE A UNIFORM METHOD TO IMPLEMENT POLICIES

Successfully scaling application security (AppSec) starts with uniformly implementing policies for testing and enforcing SLA's for prioritizing and remediating issues. Without consistent implementation across the enterprise, different teams use different policies within different tools, and problematic inconsistencies develop in how each team manages SLAs, prioritization, remediation, and as a result, how teams measure risk.

A consistent, centralized approach to implementing and enforcing policies helps ensure uniform risk reporting and provides insight into risk across roles, departments, and business functions. It also allows the threat visibility needed for compliance and management reporting while helping successfully implement and manage an application security program across an enterprise with less operational effort and more time for strategic imperatives.

INTEGRATE AND AUTOMATE

Shift everywhere has become the mantra for today's successful AppSec programs. Because shift everywhere means AST everywhere, AST must become a part of the entire development framework. Testing must be integrated and performed automatically as soon as an artifact is available, no matter where it falls in the SDLC.

In most organizations today, teams will prioritize and classify discovered defects by the risk presented to the company's unique application or business case. Teams then create priority lists with low, medium, high and critical ratings to be enforced by automated policy management in the SDLC. Typically, most organizations will assign time frames based on defect severity–critical warranting fix now, and a high priority defect fix within two weeks.

For stricter DevOps organizations AST results must be curated and presented to development teams when and only when prioritization indicates issues must be addressed **now**. Doing this relies on policies that are centrally implemented and applied across all testing types. In Black Duck's most recent Building Security in Maturity Model Report (BSIMM14), a report that is the result of studying real-world software security initiatives (SSI's) or also commonly known as software security programs (SSP's), it stresses the importance of a shift everywhere approach. "Today, firms that have embraced the culture of shift everywhere in the pipeline are updating policy and strategy to integrate security touchpoints as-code throughout the SDLC," the report states.

Success starts with direct integration into developer tools and workflows. Instead of forcing developers to log into separate security tools to perform tests, they can see issues right in their IDE as they code, and leverage remediation guidance and developer training to fix it in real time. Integrating into tools like Jira prioritizes issues for developers—so they know what to fix, how to fix it, and in what order without ever needing to leave Jira.

ACCESS THE RIGHT TOOLS AND RESOURCES

Teams must identify and implement critical testing across the SDLC efficiently and cost-effectively by identifying gaps within teams and augmenting as necessary with external resources and expertise. Connecting and enabling the right internal and external resources gives teams the skills, tools, discipline and capability to analyze any app cost-effectively and at any depth or time. Accessing the necessary resources continuously becomes more challenging as the constant proliferation of software brings more and larger applications with increased volume and variety of testing which requires security expertise across many testing types. Finding this expertise can prove difficult for many organizations with the growing demand for skilled security engineers.

Testing must scale up and down as needed, requiring access to the right tools capable of handling larger applications and increased volume. It's critical to find a vendor providing access to multiple core testing types that can integrate across the security tool stack, the developer tool stack and the SDLC. Also, engaging third-party experts can help bridge any gaps with in-house skillsets or integrations. Many organizations in heavily regulated industries like finance must arrange a minimum of yearly third-party testing on their applications to remain compliant.

ASPM's role in securing the future

A secure future for any organization depends on managing risk and scaling application security across the enterprise. The answer lies not in the proliferation of disparate tools but rather in adopting a uniform methodology that centralizes control, orchestrates testing, enforces policies, prioritizes issues and oversees the collection of the best tools and resources necessary to safeguard applications at scale.

As applications and environments expand in number and complexity, ASPM provides a valued guide for organizations facing today's numerous software security challenges. And the trend toward ASPM adoption is growing. The recent Gartner report "Innovation Insight for Application Security Posture Management" predicted that by 2026, over 40% of organizations building proprietary applications will adopt ASPM to identify and resolve their application security issues more rapidly.

ASPM delivers the foundation for this centralized approach. With the correct tools to support continuous testing throughout the SDLC, fueled by robust policies that automate critical testing and enforce the proper SLA's, it can give teams a way to scale application security in a time when budgets and resources are constricted. The Gartner report explained

the critical role of ASPM for today's organizations, saying: "Application security posture management analyzes security signals across software development, deployment and operation to improve visibility, better manage vulnerabilities and enforce controls. Security leaders can use ASPM to improve application security efficacy and better manage risk."

Rajesh Subramani, an application security engineer at CGI, discovered firsthand how an ASPM tooling solution—Software Risk Manager from Black Duck—could help his team improve visibility and quickly address critical security issues. The team at CGI found themselves overwhelmed with tools but lacking a centralized view of risks and solutions. "Within our U.S. application security testing scope, we have well over 100 software projects underway," explains Subramani. "With that many projects in development through deployment, all being examined by a spectrum of security testing tools, it was important that we start getting consolidated reports with results in one place."

The CGI team chose Black Duck' Software Risk Manager. This unified ASPM solution combines policy, orchestration, correlation, and built-in static application security testing (SAST) and software composition analysis (SCA) engines to integrate security activities intelligently and consistently across the software development life cycle.

Software Risk Manager checked all the boxes for CGI. They gained a complete picture of security risks, a thorough understanding of their AST fleet's process and performance, and the ability to make quick, informed security decisions from a single source of truth. "Black Duck and Software Risk Manager have provided the results we're looking for," Subramani continued. "We can get results from all the tools we use consolidated into one place and get the results filtered down to only the information we need."

While ASPM should be a key piece of a centralized, automated, orchestrated solution, it isn't the only piece necessary for an effective AppSec management program. Scaling security testing up and down the SDLC requires partnering with vendors who can provide the right tools capable of scaling to handle large application volumes. Organizations must select vendors who can provide multiple-core testing types and third-party consultants to assist filling in any gaps with in-house expertise. Every team must access the right tools to perform the right tests at the right time across the entire SDLC while relying on a centralized ASPM management model to pull it all together.

How Black Duck can help

Black Duck is the only vendor with a comprehensive portfolio of best-of-breed solutions that cover every stage of the SLDC. Black Duck AST solutions provide an open ecosystem, enabling organizations to leverage their existing AST tools while improving their risk posture and development productivity. Because Black Duck can aggregate and prioritize findings from 155+ Black Duck, third-party, open source, and other testing types like threat modeling and penetration testing, your organization can gain a consolidated, clear view of your software risk at any point in time.

Black Duck AST solutions empower organizations to run the right test, at the right time, at the right depth of analysis, with best-in-class solutions for the "essential three" AST testing types: SAST, SCA, and DAST. Black Duck also offers both on-premises security management solutions in Software Risk Manager, and SaaS security management solutions via the Polaris Software Integrity Platform® and WhiteHat® Dynamic. And for those who need to outsource expertise, the Black Duck services team has over 500 security professionals ready to bridge the gap in your existing AST solutions. The Black Duck Software Integrity Group is an industry leader you can trust, one that has been named the Leader in the Gartner® Magic Quadrant™ for Application Security Testing for the past seven consecutive years.

Learn more about how Black Duck can help your team effectively manage enterprise risk and scale application security across the SDLC.