BLACKDUCK®

How to Scale Application Security Across the Enterprise

Overview

Enterprise organizations have hundreds of developers on numerous teams in dozens of business units. They are all working on thousands of applications, releasing software in very rapid iteration cycles. The challenges of development across all these software development life cycles (SDLCs), business units, and organizational silos are well known, and the sheer scale of enterprise development multiplies these challenges.

Managing software application risk at enterprise scale means shifting security everywhere—using application security testing (AST) tools to standardize security policies, and integrating and automating testing throughout the SDLC. It also means ensuring that your people are trained on, and can access, the correct tools and resources to secure software applications at scale.

Building trust in your software means ensuring that your people, processes, and technology are aligned to address security risks at all stages of the application life cycle.

The Challenges of Managing Security at Enterprise Scale

The acceleration of software development both for internal and external purposes means that organizations need to secure a growing number of applications with a growing number of security tools. A report by the Enterprise Strategy Group discovered that over 70% of enterprise organizations are using 10 or more AST tools. Teams are struggling to manage application security testing environments where hundreds of applications are being tested by dozens of tools, often across multiple teams. More tools, running more tests, and delivering more results means teams are processing a lot of noise, and the struggle to manage, support, prioritize, and report on overall software application risk is very real.

As the amount of software has increased, so too has the attack surface targeted by malicious actors. Digitalization, cloud adoption, the Internet of Things, mobile applications, and the rise of AI all mean that developers are faced with an increasingly complex software supply chain. More code from more sources leads to more risk end-to-end, and this increased risk is paired with decreased visibility into where that code comes from, and the security risks it poses.

Added regulatory pressure is also a challenge. Some regulations, like PCI and HIPAA, have been in place for quite some time, but teams are sorting through the requirements of new executive orders on software supply chain security, secure software development frameworks, and DHS/CISA self-attestation. This all amounts to increased scrutiny and monumental reputational, financial, and legal risks for teams that are struggling to maintain and attest to the security of their applications.

Many of these developments are not new; however, the task of managing it all at the scale an enterprise demands has grown increasingly complex.

This constellation of issues, in combination with the velocity of current development cycles, poses a daunting problem for enterprise organizations, but there are solutions that can bring the chaos under control. By implementing uniform policies, and integrating, automating, and consolidating tools and training resources, organizations can begin to get on top of this issue.

Create a uniform method to implement policy

To rein in security sprawl, you need a comprehensive strategy that maps out your software security program. To begin, you need to determine

- Your risk appetite
- The policies that will enforce your SLAs
- Your critical testing needs
- The requirements for tools and vendors

Pulling this information together in a strategic manner will allow you to begin consolidating your tools, tests, and results so that you can centralize activities like implementing policy, test orchestration, and reporting.

Integrate and automate

The best way to gain control of security policy implementation, testing results, and issue remediation is by using an application security posture management (ASPM) tool.

ASPM allows security teams to centrally manage application security findings via a consolidated view of security and risk status across the entire software development environment. An ASPM tool provides

- A layer of abstraction between your application security team and your development team
- A central point of control to manage your AppSec program and remove developers from the complexity of the security tools themselves
- A way for AppSec teams to implement and manage consistent workflows and policies across an organization, without needing to replicate those policies across multiple tools and teams, or train development teams on how to use them
- A management and orchestration layer for security tools, enabling controls and the enforcement of security policies

Once you've implemented an ASPM tool to integrate your AST tools into a single point of visibility and management, you can simplify issue interpretation, triage, and remediation. And because a good ASPM solution will correlate and analyze data from a variety of sources, it allows you to administer and orchestrate security tools and automate your security policies.

Access the right tools and resources

Although policy and automation are key to building security at enterprise scale, it can't be done without the right tools and training the right people to use them. Moving to "shift everywhere" security relies on using a wide variety of tools at the right depth and at the right time in your SDLC, and that makes it less likely that any one in-house security team has the expertise to oversee such a wide range of security tools. Since most ASPM solutions are tool-agnostic, they can provide visibility into which of your current tools are most effective. As you begin to gain control over tooling across your enterprise, you'll want to make sure you're

- Enabling teams with internal and external resources to analyze development cost-effectively, at any depth and at the right time
- Building testing policies and processes that can scale up and down as needed across business units and teams
- Identifying gaps in your teams and augmenting as necessary with external resources and expertise

To scale testing as needed, you need access to tools that can handle large applications and high volume. It's critical to find an AppSec vendor that can provide multiple core testing types that can integrate across the security tool stack, the developer tool stack, and the SDLC.

You also need the right people. Finding skilled security engineers can be a challenge in an environment where the increased volume and variety of testing types requires a spectrum of security expertise. Third-party experts can help bridge these gaps, and many organizations in heavily regulated industries like finance regularly employ third-party pen testing on their applications to remain compliant.

Success at Scale

Let's take a look at how one organization uses ASPM solutions to increase their security at scale.

Rajesh Subramani, an application security engineer at CGI business consulting, faced challenges in managing numerous software projects without a centralized view of risks and solutions. Subramani had over 100 projects undergoing development and deployment simultaneously, and he was struggling to find a way to consolidate security reports so he could streamline CGI's security testing processes.

CGI opted for Black Duck Software Risk Manager, a comprehensive ASPM solution that integrates security activities seamlessly throughout the SDLC. This unified solution offers policy management, orchestration, and correlation, and it incorporates both static application security testing (SAST) and software composition analysis (SCA) engines. This integration provided CGI with a holistic view of its security risk, enabling quick and informed decision-making based on a singular, reliable data source. Subramani noted how effective Software Risk Manager is at consolidating results from multiple tools into one platform, facilitating efficient filtering of pertinent information.

And although ASPM plays a crucial role in centralized security management, it's not the only essential component of a robust AppSec management program. Be sure to partner with vendors capable of offering scalable tools and third-party consultants to supplement in-house expertise, ensuring comprehensive security testing across the entire SDLC.

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, allowing you to scale security for your enterprise. Black Duck AST solutions are an open ecosystem, enabling customers to utilize their current AST tools to enhance risk management and development efficiency. Black Duck tools can aggregate and prioritize findings from over 155 sources, including third-party and open source tools, as well as additional testing types like threat modeling and penetration testing, providing organizations with a consolidated, transparent view of their software risk landscape.

Black Duck provides best-in-class solutions for all three crucial AST types: SAST, SCA, and DAST. Moreover, Black Duck offers both on-premises and SaaS solutions, along with a services team of over 500 security experts. Black Duck is recognized as the Leader in the Gartner® Magic Quadrant™ for Application Security Testing for seven consecutive years, providing you with a trusted partner for comprehensive software integrity solutions.

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

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.