BLACKDUCK®

Consolidation Is More Than Tools: Three Steps to Improving AppSec Program TCO and Risk Posture

More software, more tools, more risk

Organizations are seeing steep increases in the amount and speed of code being written, and as a result, they need solutions to address the subsequent increase in application security (AppSec) risk. When teams are working to innovate at the speed of business, they face challenges securing their applications without impeding that velocity.

To address this increased security risk, firms are adding multiple point tools throughout their software development life cycle (SDLC). However, increased tooling adds complexity to the SDLC, which slows down development teams and creates resource inefficiencies. And despite all these tools, businesses still struggle to gain actionable risk insight. Too many tests, too many tools, and too many findings get in the way of shipping software quickly. In a budget-conscious economy, this is why you're hearing so much right now from business and software leaders about security tool consolidation.

Consolidation needs to be about more than just tools. By consolidating the effort required to implement and manage your AppSec program, and consolidating the insights gained across tools, organizations can address the growing complexity, diminished risk management, and resource inefficiencies that raise total cost of ownership (TCO). What organizations are looking for is a way to stop duplicating effort across teams that are using multiple, and often diverse, security tools. Consolidation can help you do that. Here are some ways to get started.

Consolidate effort

Most development teams have tools and processes they're accustomed to and want to keep using. On the micro level of a single team, this might make sense, but when you multiply teams by business units, and business units across an entire enterprise, you can wind up with hundreds of different tools enforcing inconsistent AppSec policies across your organization. This leaves your risk data scattered in a way that makes it nearly unusable.

That's why inserting a layer of abstraction between your development teams and your security tools is a good way to begin harnessing this proliferation. By inserting this layer, you can achieve three core goals for your AppSec program.

- Your development teams don't need to learn multiple UIs—they can continue working with the tools they already know.
- Your AppSec team can implement standard and consistent policies across the multitude of point tools being used across your organization.
- All your security tools are run through a single abstracted tool, providing a consolidated view into what was tested, what was found, what was fixed, and what your overall risk is at any point in time.

Application security posture management (ASPM) tools provide this layer of abstraction and provide several key benefits.

- They act as a translation layer between AppSec and development, allowing AppSec teams to control and implement policies, SLAs, dashboards, and reporting, while communicating to development what needs to be fixed and how to fix it within the tools they are already using.
- They orchestrate critical tests based on policies set by the AppSec team. And they integrate into existing development tools and workflows, so developers no longer have to learn multiple UIs, enabling triage and remediation to happen more efficiently.
- They aggregate, normalize, and prioritize findings across the security tools you already use, all in one centralized location. This reduces noise for development teams so they can focus on what to fix, in what order, and by what date, enabling them to keep the development process moving.

Consolidating effort for both your AppSec and development teams streamlines your ability to produce secure code at the velocity your business demands. It also sets you up to consolidate or swap out the point tools themselves, because you no longer have policies, processes, or findings woven into each one.

Consolidate insight

Once you have your policies and findings centralized in an ASPM tool, you can access consolidated insights across your entire business. ASPM tools aggregate, normalize, and prioritize findings across all your security tools and report them in a single, centralized location. This not only provides actionable, comprehensive, and real-time risk insight, but it also vastly reduces time to audit for compliance. With consolidated insight you can

- Identify and prioritize critical issues with an accurate business context of applications, components, and associated security data, providing teams with single, correlated list of issues for remediation. This improves efficiency for development and gives leaders a single source of truth for application risk.
- Quickly assess what was tested, what was found, and what was fixed across all your security tools, providing a real-time understanding of risk.
- Reduce time to audit by implementing a single source of truth. A unified view empowers your decision-makers to resolve new threats quickly and respond to compliance requirements accurately and on time.

Consolidating insight provides you with a uniform risk assessment across all software components, so you get real-time risk status of any project or application across the entire business.

Consolidate vendors and tools

Start by consolidating your tools. You'll want to identify the critical security testing your business requires and ensure you have it covered. Once you understand what's critical and what isn't, you can remove duplicate or unnecessary tools and identify potential gaps.

When you have your critical testing needs identified, you can begin consolidating the vendors you are managing. A good place to start is to

- Look for a vendor whose portfolio can cover multiple tools. It's not enough to have strength in a single testing type—you need a vendor that can demonstrate strength across the major core application security testing categories. This not only ensures the security of your applications, but it can reduce the operational strain on your procurement, implementation, and support teams.
- Ensure the vendor you choose does more than just offer multiple testing types. Sourcing multiple tools from one vendor can solve part of the problem, but isolated implementations can fall short of achieving all the benefits of consolidation. Vendors that offer best-of-breed solutions across multiple categories should also be able to offer strong integration points across their tools to deliver a fully unified experience.
- Choose a vendor with an open platform that can help you get the most out of the investment you have already made in security. Consolidating doesn't happen overnight, and most organizations will need to tackle it in phases. A vendor that can unify your application security program, regardless of the tools you already use and your schedule for swapping them, is key to avoiding testing disruptions and maximizing your existing investment.
- Ensure the tools are optimized to the requirements of your development teams. You can achieve this by leveraging integration points into your existing SDLC as well as into the tools your development team is already using. By relieving your teams of the requirement to learn multiple UIs, and giving them the security insight they need where they are already working, you can reduce friction and improve efficiency.

Having an ASPM tool to centralize policy management and risk insight across your security tool stack makes consolidating tools and vendors much simpler. ASPM tools pull policies and reporting out of isolated point tools and centralizes them. Doing this not only provides relief from an effort and resource perspective, but it makes it easier to swap out the tools and vendors underneath. One of the biggest hurdles to undertaking a consolidation project is the disruption to workflows and policies that have already been established and adopted.

This is why we recommend starting with ASPM. Implementing an ASPM system involves upfront work to document and establish program management to provide the insight you need to run an optimal and compliant AppSec program. And putting the effort in at the beginning saves you from having to repeat it each time you want to change vendors or tools. Once it's done, you can swap tests and tools in and out without any disruption to development or security.

By following these three steps to consolidation, you can shift your initiative from simply reducing the number of vendors to delivering high-impact value to your organization.

- Reduce complexity. Security tool sprawl leads to friction, and friction causes development to skip security steps. Consolidating effort removes complexity, reduces friction, and ensures that policies are implemented consistently.
- Improve risk posture. Disconnected findings mean that critical issues get missed. Consolidating insight provides development with a clear picture of what needs to be fixed and when, and gives your business a single view of what was tested, found, and fixed for complete risk insight.
- Reduce AppSec TCO. When developers are implementing and managing multiple tools, they get bogged down triaging issues that lack context or prioritization. Consolidating vendors and tools reduces operational strain. Finding a partner with industry-best and integrated technology makes developers more efficient and your applications more secure.

Consolidate with Black Duck

Black Duck® offers the most comprehensive portfolio in the application security market, including market-leading solutions for the "essential three" testing types—software composition analysis (SCA), static application security testing (SAST), and dynamic application security testing (DAST)—and a host of other testing types including interactive application security testing (IAST) and fuzzing, container, and API security solutions. And our ASPM solution is an open ecosystem, providing over 135 integrations into third-party and open source security tools, so you have the flexibility to integrate your existing tooling across your entire security program. Black Duck is a one-stop partner for application security.

Learn more

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.