BLACKDUCK®

Consolidate and Simplify: Streamline Application Security to Manage Software Risk

Why everyone is talking about consolidation

It's been more than a decade since Marc Andreessen proclaimed that "software is eating the world." While Andreessen correctly predicted the ways that software would completely disrupt established industries from retail to automotive, agriculture to defense, what he didn't anticipate is how drastically the teams tasked with securing the world's software would need to change the way they operate. No one could have predicted the increase in the ***amount*** of code being written, borrowed, and bought, or the increased demand this would place on application security (AppSec) as those attack surfaces grew exponentially.

The proliferation of software across every industry poses significant challenges for teams that must both keep up with the fast pace of innovation and ensure that the software they put into production is secure. Many organizations have tried to solve this challenge by adding point tools into their software development life cycle (SDLC). The promise of the developer and security toolchain was to increase velocity and agility while securing software, but the reality for most companies is a ***decreased*** ability to ship software quickly. This broken promise has led to a disjointed picture of risk, as teams under pressure to push software to production at velocity wind up skipping security steps.

This, combined with an economic climate that necessitates budget prudency, is why business and software analysts are talking so much right now about consolidating security toolchains. Vendor and security tool consolidation is the solution to three key problems that organizations across all industry sectors are facing: increasing complexity, decreasing ability to manage risk, and resource inefficiencies that are driving up the total cost of ownership (TCO) of these tools.

Tool proliferation introduces complexity

Having so many tools aimed at enabling secure development creates intricate and often convoluted development and security environments. Managing and maintaining these environments poses a series of problems including friction in the SDLC, which leads to longer development cycles; increased risk of errors and security vulnerabilities; and difficulties scaling and integrating new technologies. When development pipelines get bogged down, development teams wind up skipping or ignoring security gates in order to meet development milestones. In the end, although the toolchain is intended to serve the SDLC, when toolchain friction winds up breaking the SDLC, the result is more risk instead of less.

Recent survey results from our cosponsored report with the Enterprise Strategy Group, "Cracking the Code of DevSecOps," found that over 70% of organizations surveyed currently use more than 10 AST tools. And multiplying those 10 tools across the often siloed and disparate development teams at large organizations introduces yet another layer of complexity. Often, each development team is responsible for choosing and implementing its own set of tools. This results in security policies that are implemented inconsistently across different sets of tools and different teams within an organization. Which in turn leads to inconsistent implementation of application security programs, leaving security teams with no way to uniformly assess risk. And when policies are implemented inconsistently, there is no way to measure, enforce, or report on risk across either a set of applications or across an entire organization.

Consolidation means working with fewer essential tools from fewer vendors. It also means consolidating the level of effort required to implement and scale uniform policies and workflows across an organization. This minimizes complexity in the development environment and enables teams to work at the speed that business demands.

The proliferation of software across every industry poses significant challenges for teams that must both keep up with the fast pace of innovation and ensure that the software they put into production is secure.

Over 70% of organizations surveyed currently use more than 10 AST tools.

Resource inefficiencies lead to poor AppSec ROI

Software complexity not only increases risk, it presents management, maintenance, and support challenges that can dramatically affect the TCO of your security tools. Three core areas lead to a negative impact to return on investment (ROI) on AppSec programs: drag on development resources; increased operational resources to procure, implement, and manage multiple tools from multiple vendors; and increased cost to license tools. All these prevent organizations from realizing economies of scale across teams and vendors.

Tool proliferation requires development teams to learn and use multiple UIs. This takes valuable time away from writing code and increases the barrier to switching tools. In addition, developers waste cycles triaging when duplicate issues are pushed into their tracking systems or delivered without context or priority information. Navigating complicated security environments not only diverts these valuable resources away from key development activities, it also impedes agility, making it harder for organizations to respond quickly to changing market and customer demands.

Meanwhile, the likelihood of mistakes and security breaches increases when development pressure results in skipped security steps and shipping software with known issues. This can cause expensive repair efforts and can even trigger legal or regulatory repercussions.

Development teams aren't the only ones bearing the burden of too many tools. Procurement teams are stretched thin by managing multiple vendors and contracts, as well as finding the resources required to implement, maintain, and support these tools. In a time when organizations need to get the most out of their budgets, these increased operational costs become harder to justify.

Finally, purchasing point tools from multiple vendors invariably increases the security stack cost to license. Procurement loses purchasing power when managing isolated contracts. This is why partnering with a single vendor across multiple security needs puts you in a better position to realize volume and term pricing advantages.

A fragmented picture of risk

More security tools lead to more tests, which translates to more results and thus more issues. The survey demonstrates that when results are returned from a variety of point tools, they come with a lot of noise. This leaves developers to work through mountains of disconnected findings, some of them duplicates and most with inefficient and noncontextual remediation guidance. As a result, they waste valuable time and resources trying to triage security issues before they can even hope to start fixing them. Without a single picture of prioritized and contextualized issues, developers spend more time sifting through noise than fixing what's critical and moving on. Since the primary job of most developers is to ship software—not necessarily to ship ***secure*** software—they end up releasing software that they know is not secure or that has vulnerabilities.

This is a bigger problem than any single development team struggling to understand the risk of an application, because tool and findings proliferation make it even more difficult for a business to understand risk across its portfolio. When risk data lives within point tools scattered across various teams, every audit turns into a fire drill of wasted cycles. Organizations need a centralized system of record to understand what was tested, what was found, and what was fixed at any point in time to be able to quickly and accurately report on software risk.

As the convergence of economic and practical factors increases pressure on organizations to streamline their AppSec initiatives, consolidation is emerging as a practical solution to not only improve TCO, but reduce complexity and achieve true risk management.

A recent Gartner survey noted that, "On the demand side, the technical security staff necessary to effectively integrate a best-of-breed portfolio of security products is simply not available to most organizations. As a result, 80% of security and risk management leaders are now looking to consolidate their security spending with fewer vendors. These leaders are anticipating that consolidation will result in improvements to the enterprise risk posture and security staff efficiency."

There are steps companies can take to begin to consolidate vendors and tools, effort, and insight.

Consolidate vendors and tools

With organizations already using 10 or more AST tools, the solution isn't adding more tooling, it's figuring out how to optimize the tools they already own. This process begins with identifying the critical security testing your business requires, ensuring you have it covered, and then removing duplicate functionality that creates inefficiencies and increases complexity. Next, you need to improve resource efficiency. There are a few ways to do this.

Start by reducing the number of vendors your teams are managing. By finding an application security partner that can offer strong solutions across multiple critical testing needs, you can reduce the operational strain on your procurement, implementation, and support teams.

Sourcing multiple tools from one vendor can solve part of the problem, but isolated implementations can fall short of achieving the benefits that consolidation offers. Vendors that offer best-of-breed solutions across multiple categories should also be able to offer strong integration points across their tools to make the entire experience more seamless.

Rather than force development teams to learn multiple UIs and triage issues from multiple tools, create an abstraction layer between your development team and the security tooling. An application security posture management (ASPM) solution can do this by orienting your team on a single UI, which not only improves efficiency but also makes it easier to plug in new tools and remove unnecessary ones without causing any disruption to testing.

Isolated implementations can fall short of achieving the benefits that consolidation offers.

According to Gartner, "Application security posture management analyzes security signals across software development, deployment, and operations to improve visibility, better manage vulnerabilities, and enforce controls. Security leaders can use ASPM to improve application security efficacy and better manage risk."

Vetting security vendors

After you decide to consolidate, you need to think about how you want to do that. The first question to address is how to vet security vendors. A good place to start is to look for a vendor whose portfolio can cover all your security demands.

It's not enough for a vendor to offer just one of the essential three automated tools. You need a vendor that offers best-in-class tools for all three: robust, accurate, and efficient solutions for static application security testing (SAST), software composition analysis (SCA), and dynamic application security testing (DAST). If your vendor is lacking in any one of these, you'll have weak links in your security chain. Since one bad link means your whole chain is weak, you're not going to be able to secure your applications with this vendor.

You also want to look for a vendor with an open platform that can allow you to leverage the tools you already have. Consolidating doesn't happen overnight, and most organizations are already using good security tools. The trick is getting them all working in concert, so you're doing the right tests at the right time and at the right depth. According to Black Duck Marketing Vice President Jim Ivers, vendor consolidation is like "changing the tires on a moving vehicle." You need a platform that will enable you to leverage your existing security testing tools and that offers integrations to help you accomplish that.

The last issue you need to consider is verifying the stability and longevity of any potential vendor. Consolidation means entering into a long-term relationship. Does the vendor you're considering have a history of evolving its portfolio to keep pace with rapidly evolving development techniques and threats? Accomplishing your consolidation goals depends on how you go about it. So it's important to take the time to do it in a way that will help you build trust in your software.

Consolidation starts with eliminating tools and reducing the number of vendors, but it quickly becomes about much more. Teams need a way to centralize policy, take in the results from all their security tools, prioritize and contextualize them, and provide a unified place for administration and reporting. Doing this as part of the consolidation initiative ensures that you not only optimize resources, but actually improve risk posture as a result.

Consolidate effort to reduce complexity

Multiple implementations of point tools within single teams leads to large amounts of duplicated effort. Even worse, it leads to inconsistently implemented application security programs.

Once an organization has gone through a tool and vendor rationalization and implemented an ASPM tool to orient teams to a single UI, the complexity of the AppSec program can be further reduced by consolidating the effort associated with managing it. There are several ways to do this.

Centralizing policy management

Using more than 10 AST tools translates to policies not being implemented consistently and a lot of extra work for AppSec teams. By centralizing policy management in an ASPM tool, your organization can set security policies once and enforce them consistently across all applications and teams, regardless of the underlying security tools you're already using. This streamlines policy enforcement, reduces duplication of efforts, and ensures a standardized approach to security across your entire organization.

Automating testing

Centralizing policy management enables teams to set and enforce SLAs for issue remediation and allows you to automatically orchestrate tests based on your specific risk tolerance. Some ASPM solutions offer automation that enables timely and context-aware testing, optimizing scan schedules to align with development milestones. This intelligent automation ensures that security testing is performed when needed, reducing unnecessary scans and avoiding bottlenecks in the development process.

Integrating into the developer environment

Integrating an ASPM tool with your existing development environments is crucial to consolidating your security effort. Developers need to seamlessly access security tools and insights within their familiar toolchains, so they aren't bogged down with learning and managing multiple standalone security tools. Making security an inherent part of the development process enables secure coding practices and enhances your overall software security without disrupting the development workflow. For example, developers should be able to triage, fix, and update the status of an issue without leaving the issue-tracking system, thus increasing their productivity and leaving no room for out-of-sync systems.

Consolidating your security effort in this way is one of the most potent tools to decrease complexity and improve TCO. By breaking down silos, enabling collaboration, centralizing policy management, automating testing, and integrating with the existing development environment, ASPM enables organizations to optimize their security practices, reduce operational overheads, and achieve a robust application security posture efficiently and effectively.

Consolidate insight to enhance risk management

Once you have consolidated the number of vendors and tools your organization relies on, and consolidated the effort associated with implementing and managing your AppSec program, you can consolidate the security insights they deliver.

Consolidating security insights enhances visibility into your security posture by providing a single source of truth and a comprehensive picture of your risk. Having a unified view empowers your decision-makers to mitigate potential threats, shorten time to audit, and resolve new threats quickly.

To consolidate insight, teams must first be able to aggregate, normalize, and prioritize findings across all security tools in one centralized location. This will reduce 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. Identifying and prioritizing critical issues with an accurate business context of applications, components, and associated security data provides teams with an actionable picture of overall software risk at any point in time.

ASPM solutions are at the core of enabling this for organizations. Using ASPM to manage your AppSec program simplifies security for developers, reduces the effort required to implement consistent AppSec policies, pulls all security data into one place to accurately prioritize issues, and provides a single source of truth and a single picture of risk for your organization.

Conclusion

As software continues to revolutionize industries, the increasing amount of code being written, borrowed, and bought presents unique challenges for the teams tasked with securing it. Security tool complexity not only escalates risk but also drives up operational costs, hampers agility, and strains resource efficiency. In the face of these issues, consolidation emerges as a strategic approach to streamline application security efforts, improve your organization's TCO, and enhance risk management.

There are three steps on the path to consolidation that will help you achieve these desired outcomes.

- Consolidate vendors and tools to improve TCO
- Consolidate effort to simplify your AppSec program
- Consolidate insight to enhance risk management

Partnering with a vendor that can offer a strong set of capabilities across your critical testing needs and implementing an ASPM solution to enable the consolidation of tools, effort, and insight will help deliver a more cost-effective and robust security program.

Black Duck is your partner to help you build trust in your software

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**.

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.