A Buyer’s Guide to Application Vulnerability Correlation Tools

Every business is a software business

No matter what industry you're in, you rely on software to run your business, which means, in effect, that every business is a software business. Over the past several years, we've seen cyberthreats across every industry, from ransomware attacks that shut down gasoline delivery across the southeastern portion of the United States to hacking exploits of software vulnerabilities that rendered hundreds of consumer and enterprise products susceptible to attack. No one wants to see their organization in the next headline and face potential reputation loss, so businesses need to protect themselves on every front. And one way to do that is by adopting scalable, automated tools that can not only centralize your security testing activities but also reduce the noise by correlating and deduplicating findings to provide clear risk assessment and remediation guidance.

No matter what industry you're in, you rely on software to run your business.

Modern AppSec development poses unique challenges

Integrating tooling, triage, and remediation remains an ongoing challenge for modern software development. Since the software that companies rely on comes from so many different sources—custom code developed in house or by a third party, commercially, or open source—it poses vast challenges that are only compounded by the many different ways in which software is tested, especially when multiplied by the specific issues those tests return.

Organizations typically employ a variety of security testing tools throughout the software development life cycle (SDLC). Common tools for identifying software weaknesses include static, dynamic, and interactive analysis, as well as penetration testing for custom code, software composition analysis for open source components, and context-dependent testing in the form of manual code reviews and threat modeling.

These tools are each necessary and effective, but the result of all this testing is that organizations are faced with an enormous amount of data to sort through. Different teams may be running different testing tools, many of which rely on manual review to assess risk severity for prioritization effort. It is also necessary for many types of security testing data to be audited by a security engineer or developer, and any past audits of an application need to be merged with any new scans or branches. Without the ability to understand this previous audit context at scale, a developer's time will be wasted by presenting previously suppressed issues to be fixed, taking up time that most developers don't have to spare. As a result, vulnerabilities go unmitigated because there is no visibility into their location or remediation advice for fixing them once they're found.

These challenges result in low-efficiency AppSec, which means you risk releasing poor-quality code to production. Faulty code in production leaves your organization open to attacks, including data mining and ransomware. Breaches in your software are not only expensive but lead to reputational damage—while customers understand that software risk is ubiquitous, they want to know that they can trust your organization. Customers want to know that they can trust vendors to be proactive about preventing exploits and to adhere to industry standards, including quality checks and security requirements for software going into production.

The siloed nature of security testing, and the abundance of data that is produced, means that most organizations struggle to determine their most impactful security activities. Because of this, they have difficulty enforcing standards for compliance and risk assessment across their applications, which makes it difficult to standardize secure software development practices.

These structural issues have historically contributed to the security gap between development and security teams that hinders collaboration of data, tools, and process. When you do not know the top vulnerabilities in your organization and lack a central system of record, it is nearly impossible to gain a global perspective of your business risk when it comes to software.

Elevate your AppSec program with Code Dx

The solution to this problem is to adopt an application vulnerability correlation (AVC) solution like Code Dx® to elevate your AppSec program in a scalable, efficient fashion. AVC tools work by aggregating results, normalizing them, and correlating the security findings returned by multiple tools. Code Dx aggregates application security testing (AST) results across your organization, including diverse testing types such as static application security testing (SAST), dynamic application security testing (DAST), interactive application security testing (IAST), and software composition analysis (SCA)—even container security scan results and manual processes such as threat modeling and code reviews—into a single repository. It then normalizes these results and presents them in a consistent, standardized format that can be recorded and viewed in this repository. Code Dx also correlates instances in which the same issue is found by multiple tools and presents them as a single finding. This reduces the number of duplicate tickets, eliminating inefficiencies and unnecessary friction for developers. In addition, Code Dx can deduplicate data to highlight unique issues, providing a clearer understanding of risks and the associated burden of remediating them.

Scaling existing processes in line with a next-gen AppSec approach starts with implementing a robust AVC solution. Here are some questions to ask when evaluating your AppSec needs and determining how an AVC can help.

AVC tools work by aggregating results, normalizing them, and correlating the security findings returned by multiple tools.

Question 1:

How can I make the most of my current application security investment in tools, processes, and people?

The siloed nature of security and development teams means that organizations often invest in multiple AST tools and types across their toolchain. The problem is that, by design, SAST, DAST, and SCA tools work in very different ways against different sources. For instance, SAST tools are leveraged for testing source code issues, while DAST tools test for runtime issues in simulated production environments. For this reason, most teams will use both to test for different types of issues and in specific environments. But there can often be duplicate results between these tools, and without a means to correlate those results, teams are too often left trying to extract what's important from a wall of noise.

Teams that do AST testing have long sought the ability to aggregate findings from SAST, DAST, IAST, SCA, container scans, manual code reviews, and manual penetration tests into a single unified repository that correlates those disparate testing types. An AVC solution like Code Dx correlates all these results, then filters out redundancies and false positives. With support for 100+ security and developer tools, Code Dx offers a rich set of integrations that provides a single AppSec system of record that streamlines visibility into critical testing data, remediation progress, and responsible stakeholders. Code Dx is also able to correlate and present all relevant security data in a consolidated view.

Implementing an AVC solution that aggregates and correlates multiple security results can help you make the most of the security investments your organization has already made. With Code Dx, this comprehensive approach to AppSec data visibility can cover a diverse set of use cases. For example, infrastructure vulnerabilities that affect specific applications can be viewed within Code Dx, so you can take them into account when prioritizing application vulnerabilities found on that infrastructure.

Additionally, Code Dx offers a highly efficient means to perform analysis on different types of AST tools. Typical security correlation across different types of security analysis (SAST, DAST, IAST, SCA) requires a runtime agent. These agents can often be vendor-specific, and limited in the tools or languages they support. Code Dx supports agent-less correlation, which offers a low-latency solution to correlate between different AST tool types, offering a significant advantage compared to standard AVC solutions.

Code Dx also enables security and development teams to answer some basic yet crucial questions about their existing suite of AST tools.

- When was my software tested?
- What was fixed?
- What was found?
- What is the extent of my exposure/exploitability?

Without a means to correlate results, teams are too often left trying to extract what's important from a wall of noise.

Question 2:

How can I get a perspective of software risk across our organization?

Gaining visibility into software risk and compliance across an entire organization is always a challenge. Most organizations rely on custom-built software applications, which are in turn comprised of components that can themselves carry weaknesses, including open source vulnerabilities, unpatched commercial code, and others. The complexity of modern software multiplies your organization's risk on a massive scale.

While AST tools can provide visibility into specific risks, they can't give you an organizational perspective. Not only do these tools check for very different risks, but vendors may each have their own methodology for scoring severity, criticality, and scope. AVC tools like Code Dx can help you provide a uniform assessment of software risk across your organization by giving context and visibility into your software while making software risk assessment auditable. An AVC platform like Code Dx can use policy management and advanced filtering to translate myriad security findings into a contextually aware report and actionable results for your security and development teams.

Individual AST tools each have their own methods of proprietary risk assessment, and the benefit of Code Dx is that it can normalize these varied risk scoring methodologies to a common system and set of data points. With Code Dx, your teams can also tie high-priority findings to compliance violations, like OWASP and PCI. Code Dx can expose compliance violations, including the source of the issue, as well as report on the overall health of your application according to these controls. This enables your teams to gain visibility into regulatory auditing at the application level, by project.

The complexity of modern software multiplies your organization's risk on a massive scale.

Question 3:

How can I digitally transform my AppSec operations and achieve cyber-resiliency at scale?

The challenge with any AppSec program is implementing security without impeding developer productivity. This is where automation comes in. Automating your decision process for escalating high-priority results can allow your teams to continue to work at velocity without sacrificing security. For instance, technical audit decisions made by developers or security experts can often be time-intensive and expensive to fix. An AVC solution like Code Dx leverages its Triage Assistant, which uses machine learning to automatically understand how your team audits security issues associated with a particular project. By determining what types of issues your team prioritizes, Triage Assistant can predict which new security issues are the most likely to be true positives, ensuring that your teams can act on newly discovered and high-priority weaknesses. Triage Assistant also eliminates backlogs by flagging false positives and providing triage focus, giving teams a trustworthy set of data points about which issues are legitimate, high-priority security issues. Auditing, especially with static analysis results, is the most time-consuming and least scalable activity for security engineers and developers in every application security program. Code Dx uses data from past auditing decisions to improve the way issues are prioritized based on the contextual audit decisions made within the application.

Code Dx also adds value by offering remediation guidance when reporting on vulnerabilities. Often, developers know they need to commit a fix, but they may lack the security context for how to implement it. They may also lack information about how involved the fix is. By contextualizing issue severity, the recommended remediation steps, and the extent of the fix at the continuous integration (CI) stage, an automated AVC can bridge the developer knowledge gap and prevent costly security bottlenecks postproduction. Code Dx does this by offering integration with Secure Code Warrior, which provides context-aware remediation guidance for specific software findings. Historically, developers skipped fixing security issues when they could not understand the issue in the context of their own application, tech stack, or framework. Code Dx renders this a problem of the past by providing language- and framework-specific examples (when available) from Secure Code Warrior in addition to remediation guidance from the individual testing tools themselves.

Implementing Code Dx will improve product quality without slowing down production

AVC solutions like Code Dx offer a holistic solution that allows your teams to build trust into your software and thereby build trust into your business. Code Dx does this by helping your organization design an AppSec program that works in line with your SDLC to provide global visibility of software issues, leveraging your existing tooling and data to provide a management framework for standardizing and auditing security test results. This enables teams to optimize their existing security investment in tools, processes, and people by reducing bottlenecks in triage and remediation, capturing visibility into the level of software risk, and most importantly, providing clarity on critical work.

Want to know how Code Dx can help you?
Request a demo today or visit synopsys.com/codedx to learn more.

The Synopsys difference

Synopsys Software Integrity Group provides integrated solutions that transform the way development teams build and deliver software, accelerating innovation while addressing business risk. Our industry-leading portfolio of software security products and services is the most comprehensive in the world and interoperates with third-party and open source tools, allowing organizations to leverage existing investments to build the security program that's best for them. Only Synopsys offers everything you need to build trust in your software.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

Contact us:
U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com