SYNOPSYS®

Enterprise Application Security Buying Guide

How to Build a Powerful AppSec Toolbelt

Table of contents

Application vulnerabilities are the No. 1 attack target for cyber security breaches.

To minimize your risk, your organization must address application security holistically across people, process, and technology and throughout the software development life cycle (SDLC). To ensure you have the technology necessary to build secure software, you'll want to put together a toolbelt of solutions that address specific types of application security weaknesses. By deploying them together, you can ensure there are no holes in their coverage.

Below are 13 application security tools and services to consider and what to look for in each one.

Tools to use during planning

Discover where you are in your software security journey, where you need to go, and how to get there.

1. Strategy & Planning Services

○ Have this ○ Need this ○ Consider this ○ Skip this

What it does: Strategy and planning services help you build security into your development teams (people), processes, and tools (technology).

How it works: Strategy and planning experts show you how to establish a software security initiative (SSI) or improve the one you have based on how you measure up against industry best practices and what other companies in the same sector are doing.

Why you want it: To ensure your SSI meets your unique needs in the best possible way, you need to benchmark and track its growth and evolution. This is a lot easier to do with the help of experienced practitioners who know what works and what doesn't for organizations like yours.

What to look for: Seek a provider with deep expertise in the essentials, such as compliance, training, attack models, architecture analysis, code review, and multiple application testing modes. These activities, along with your provider's knowledge about your peers in the industry, will let you assess the maturity of your SSI.

2. Maturity Action Plan

○ Have this ○ Need this ○ Consider this ○ Skip this

What it does: A maturity action plan provides you with a detailed plan and roadmap to enhance your software security program, including a prioritized list of recommendations.

How it works: Your provider works with your organization to lay out a two-year roadmap in which you set objectives, outline a strategy, and identify resources; determine how to equip your staff to build and operate secure software; define how and when to address each software asset; and plan activities to verify your software security program.

Why you want it: A maturity action plan will help you close the gaps in your SSI, implement security best practices across your organization, and clarify the resources you'll need to get there.

What to look for: Choose a provider that has experience helping customers improve their application security, gain access to budget and resources, define a strategy and plan for their security initiatives, establish mechanisms to measure progress, and communicate their software security posture to customers, partners, and regulators.

3. Threat Modeling

○ Have this ○ Need this ○ Consider this ○ Skip this

What it does: Threat modeling helps your teams design more secure software by analyzing the specific types of attacks you're likely to face.

How it works: Threat modeling assessors identify the objectives and vulnerabilities in a system and determine potential threats to the system in light of any countermeasures you have in place. Threats can be malicious, such as a DDoS attack, or incidental, such as the failure of a storage device, which could compromise crucial data.

Why you want it: Threat modeling can help you determine where to expend the most effort to keep your systems secure. This is a variable that can change over time as you add, remove, and upgrade applications and as user requirements evolve.

What to look for: The ideal threat modeling provider should tailor their approach to your organization's needs and budget. They should review your system's major software components, security controls, assets, and trust boundaries, and then model threats against existing countermeasures to evaluate the potential outcomes.

4. Architecture Risk Analysis

○ Have this ○ Need this ○ Consider this ○ Skip this

What it does: Architecture risk analysis (ARA) helps you ensure that the architecture and design of your applications make them difficult to hack.

How it works: ARA is a risk-management process in which analysts identify flaws in an application's architecture and determine the level of risks to business information assets that result from those flaws.

Why you want it: About half of the software defects that create security problems are flaws in design. If you only test your code for security bugs, you're leaving your organization vulnerable to attack. ARA enables you to find and remediate security problems earlier in the SDLC, which is less expensive and time-consuming than waiting until QA.

What to look for: The ideal ARA service provider will review your application design in depth and look for weaknesses in your architecture that would allow attacks to succeed. They'll go beyond a threat model by performing security reviews to test the feasibility of the identified threat/attack vectors.

Tools to use during coding and build

Build your apps securely from the start.

5. Static Application Security Testing

○ Have this ○ Need this ○ Consider this ○ Skip this

What it does: Static application security testing (SAST) helps teams find and fix quality defects and potential security vulnerabilities in proprietary code as your developers are writing it.

How it works: SAST analyzes application source code, including byte code and binaries, for coding and design conditions that may indicate security vulnerabilities, such as those in the OWASP Top 10 and the CWE/SANS Top 25. Since it analyzes source code, rather than a running application, SAST can begin as soon as your developers start writing code.

Why you want it: SAST finds defects and security weaknesses in code early in the SDLC, so you can fix them when remediation is faster and cheaper.

What to look for: Look for a static analysis tool that provides deep, full path coverage and integrates with your key development tools and CI/CD systems. An automated SAST solution will continuously analyze for weaknesses as your developers write and check in code. Superior tools provide remediation guidance so developers can fix vulnerabilities immediately. You might need a solution that supports thousands of developers and can analyze large projects exceeding 100 million lines of code.

6. Software Composition Analysis

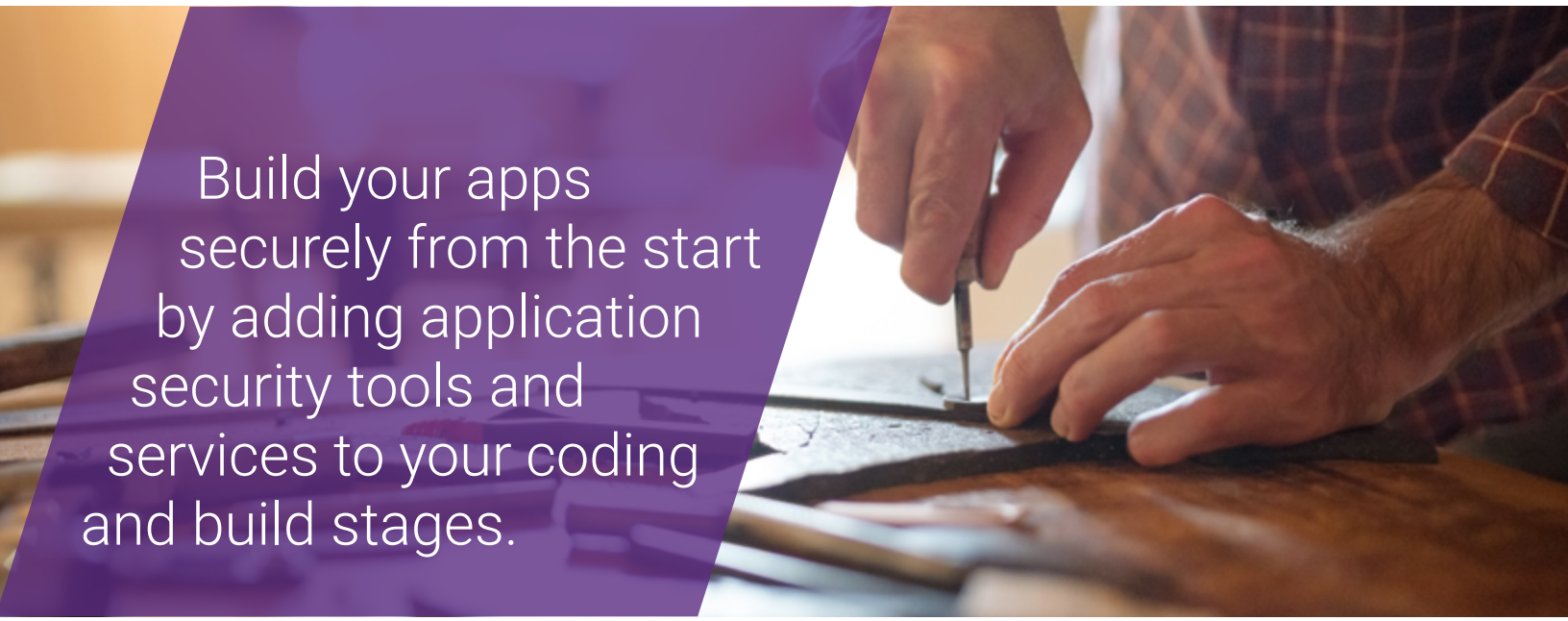
○ Have this ○ Need this ○ Consider this ○ Skip this

What it does: Software composition analysis (SCA) helps teams manage open source security and license compliance risks through automated analysis and policy enforcement.

How it works: Like SAST, SCA statically analyzes source code or binaries. But in contrast to SAST, SCA is focused on identifying open source components in applications and any security vulnerabilities that have been reported against them.

Why you want it: Whether you realize it or not, your developers are probably using open source code—anything from complete libraries to snippets of code copied from the internet. SAST tools alone cannot identify all open source vulnerabilities, and they don't monitor for licensing issues that could put your intellectual property at risk. So it's important to incorporate SCA for a secure DevOps pipeline.

What to look for: SCA tools should integrate easily into your development toolkit, most commonly in a CI/CD system. Since open source can be pulled into code in many ways, quality SCA solutions use multiple scanning methodologies to identify all the components (full or partial) and dependencies in an application. Some tools provide remediation guidance for developers as well.



Tools to use during testing and release

Confirm your apps are secure before you ship them.

7. Interactive Application Security Testing

○ Have this ○ Need this ○ Consider this ○ Skip this

What it does: Interactive application security testing (IAST) helps teams accurately identify and verify vulnerabilities and sensitive-data leakage through automated testing of running web applications.

How it works: IAST works in the background during manual and automated functional and security tests. Unlike DAST, it uses code instrumentation to analyze application behavior and dataflow, identifying vulnerabilities and providing developers with the information needed to pinpoint, prioritize, and remediate them.

Why you want it: IAST is a good solution for CI/CD environments, where speed and automation are a priority. It can run earlier in the SDLC than DAST and penetration testing.

What to look for: An ideal IAST solution should show an application's compliance with multiple security standards, such as the OWASP Top 10, PCI DSS, and CWE/SANS Top 25. It should have a very low false-positive rate, showing which vulnerabilities are exploitable while eliminating others. It should provide early warning, finding runtime vulnerabilities during the test/QA stage. It should fit seamlessly into CI/CD workflows. And it should track sensitive data to ensure that applications handle this data securely (e.g., not storing it in log files or databases with weak or no encryption).

Integrate application security tools into your testing and release stages to confirm your apps are secure before you ship them.

8. Dynamic Application Security Testing

○ Have this ○ Need this ○ Consider this ○ Skip this

What it does: Dynamic application security testing (DAST), also known as black box testing, scans web applications while they are running, simulating an attack by a skilled, motivated hacker.

How it works: DAST solutions send hundreds of potentially insecure requests to the HTTP and HTML interfaces of a web-enabled application to see how the application responds. The result is a list of real vulnerabilities that attackers could exploit in the wild.

Why you want it: DAST helps testers find problems that are not contained within specific lines of code but instead emerge when the application is running. Using DAST and SAST in combination can help catch different types of security problems before a product is released or develops a growing user base.

What to look for: Most DAST solutions identify common vulnerabilities, such as SQL injection, cross-site scripting, buffer overflows, and the rest of the OWASP Top 10. Look for a service that tests for vulnerabilities that out-of-the-box tools can't find (e.g., TLS communication, information leakage) and performs manual reviews to identify false positives. Ideally, your DAST solution will also allow you to schedule tests, set the desired depth of testing, and make modifications as business requirements change and threats evolve.

Test your production apps for security during deployment, operations, and monitoring.

Tools to use during deployment and operations

Test your production apps for security.

9. Penetration Testing

○ Have this ○ Need this ○ Consider this ○ Skip this

What it does: Pen testing extends DAST to find exploitable vulnerabilities in web applications and services.

How it works: Pen testers use both automated scans and thorough manual testing focused on exploratory risk analysis and business logic. When they find weaknesses in your system, they document how an attacker could gain access by exploiting those weaknesses.

Why you want it: Even if you regularly scan your code using application security testing tools, missteps in design, implementation, configuration, and other aspects of your application deployment can leave gaps for attackers to gain access to your system. A penetration test will uncover real exploitable weaknesses so you can prioritize them.

What to look for: The ideal pen test service provider will have a team of experts who are skilled in manual testing and have access to an extensive portfolio of automated scanning tools to analyze your web applications. They'll also explore deeper business logic testing, which covers attacks outside a canned list or that may not have been considered otherwise.

10. Red Teaming

○ Have this ○ Need this ○ Consider this ○ Skip this

What it does: Red teaming helps you identify immediately exploitable security holes across your organization's entire attack surface using a variety of composite attack methods.

How it works: A red team assessment simulates an attack to demonstrate how real-world attackers can combine seemingly unrelated exploits to achieve their goal.

Why you want it: Red teaming shows that even the most sophisticated firewall in the world means very little if an attacker can walk out of your data center with an unencrypted hard drive. It demonstrates how you should take a defense-in-depth approach and continuously improve your people, process, and technology, instead of relying on a single network appliance to secure sensitive data.

What to look for: Proficient red teamers know there are many ways to breach an organization. Look for a service provider that uses these tactics, among others:

- Email and phone-based social engineering
- Physical facility exploitation
- Network service exploitation
- Application layer exploitation

Tools to use during cloud migration

Keep your apps secure as you migrate to the cloud.

11. Cloud Maturity Action Plan

○ Have this ○ Need this ○ Consider this ○ Skip this

What it does: A cloud maturity action plan provides a structured roadmap customized for your migration to the cloud.

How it works: A team of experts helps you establish the principles and actions necessary to address security in the cloud. These principles and actions cover governance, risk, compliance, threat mitigation, visibility and transparency, and controls for detecting and responding to attacks.

Why you want it: A cloud maturity action plan can help you set cloud security objectives, outline a strategy to reach those objectives from where you are today, and evaluate the resources and processes you'll need to attain your cloud security goals.

What to look for: The ideal cloud maturity action plan should define a strategy for security in the cloud. It should help you deliver a security program to develop and implement robust security, privacy, compliance, and risk-management capabilities that will continue to mature and improve.

12. Cloud Security Assessment

○ Have this ○ Need this ○ Consider this ○ Skip this

What it does: A cloud security assessment identifies specific security risks and opportunities associated with a target cloud platform.

How it works: Cloud experts evaluate your applications for cloud preparedness across multiple domains, including:

- Container and virtual machine security
- Encryption, key management, and protecting secrets in the cloud
- Security for data at rest and in transit
- Authentication, authorization, and data residency

Why you want it: It is impossible to address security risks if you don't know what they are. A good security assessment will give you the information you need to focus your security resources the most effectively.

What to look for: The ideal cloud security assessment will determine whether the target platform has an advanced perimeter firewall, intrusion detection systems with event logging, internal firewalls for individual applications and databases, data-at-rest encryption, and Tier IV data centers.

13. Cloud Security Blueprint

○ Have this ○ Need this ○ Consider this ○ Skip this

What it does: A cloud security blueprint provides a consumable reference architecture with baseline security controls that can help guide development teams and systems integrators building or deploying cloud applications.

How it works: The service provider delivers blueprints using infrastructure-as-code tools. A security control matrix maps the solutions outlined in the blueprint to the regulatory standards that many organizations must adhere to when implementing computing services.

Why you want it: As you migrate to the cloud, you'll encounter new security risks. Cloud security blueprints help your security, development, and operations teams understand and address these risks before they become threats.

What to look for: The ideal cloud security blueprint will address the crucial security risks that you face when building cloud workloads. It should cover federation and identity management, CI/CD, container security, logging and monitoring, backup and disaster recovery, secrets and credentials management, and service hardening.

How Synopsys can help

Application security is not a one-time event. It is a continuous journey. Doing it effectively means building security into your SDLC without slowing down delivery times. It requires managed services by a team of experts that are deployed at the right place and time in your development environment. It also requires multiple tools that:

- Are easy to deploy and use.
- Have broad language and framework support.
- Integrate with a broad set of development and DevOps tools.
- Provide easy-to-consume reports and dashboards.

Synopsys is the only vendor equipped to help you build an AppSec toolbelt that brings together all the solutions you need to address your risks. With Synopsys, you can manage application security no matter what your development environment or deployment model requires. Our flexible pairing of products and services means you can personalize your solution to meet your specific challenges.

How powerful is your AppSec toolbelt?

Synopsys' portfolio of application security tools allows teams to optimize their AppSec toolbelt with integrated solutions that address application security risks end-to-end, providing analysis of vulnerabilities in proprietary code, open source components, and runtime configuration and behavior.

Pair that with our managed services, such as DAST and pen testing; our professional services, such as threat modeling and BSIMM; and our comprehensive training both online and offline, and you'll have a toolbelt rigorous enough to conquer any vulnerability.

Let Synopsys help you build secure, high-quality software faster.

READY TO GET STARTED?

SYNOPSYS®

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

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

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

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