



# Security Testing Services

Build secure software faster with on-demand expertise

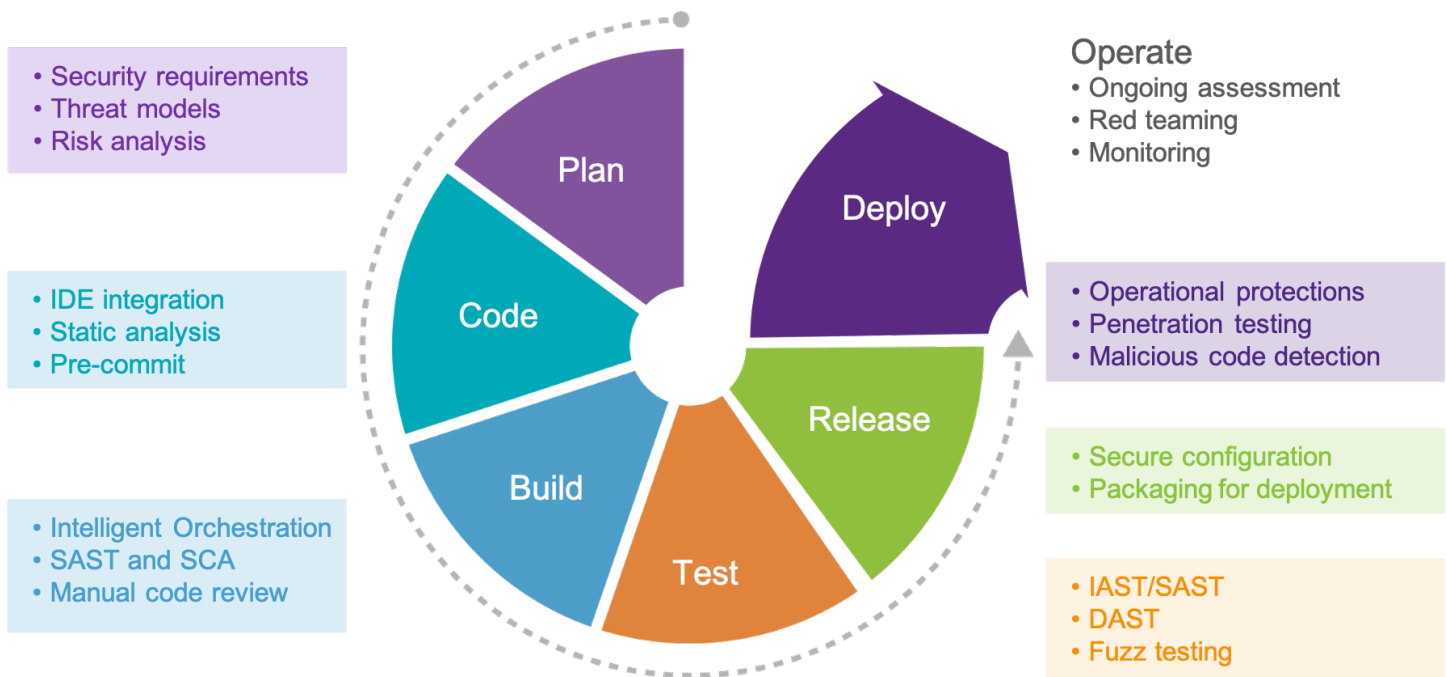






Software development models have evolved rapidly in the last decade, from waterfall, to agile, and now to DevOps, which itself is evolving to DevSecOps thanks to the “shifting left” of security activities in the software development life cycle (SDLC). And this year’s “Building Security in Maturity Model” (BSIMM) report shows that security testing activities are actually shifting everywhere in the SDLC.

Unfortunately, the tools and hacking techniques used in malicious attacks have also improved significantly. Hackers are constantly devising new methods of attacking vulnerable software. Attacks are much more sophisticated and frequent than ever before. It takes decades of software security expertise along with a diverse team of application security experts to understand all the risks and remediation strategies needed to protect your application and its users.



## Complexity and diversity of application security testing

There are a variety of factors that make it extremely difficult for an organization to address all application security requirements.

- Modern applications have become very complex, and companies often have anywhere from a dozen to thousands of internal and external applications. Additionally, applications can include both static and dynamic pages, and they can deliver content via multiple API calls, adding to testing complexity. The underlying code is just as complex—it consists of thousands of lines of custom code along with open source code. The software language, libraries, and ecosystem are also often open source that may include embedded vulnerabilities.
- The vulnerabilities in the code are evolving and increasing exponentially as well. And they can be exceedingly difficult to find for even the most trained internal developers and testers, increasing the likelihood an exploit.
- The speed with which code is produced in the agile development methodology and DevOps processes often means there just isn't enough time to test all the code being constantly generated.
- There are many ways to deploy software, including in the cloud, within an embedded device, in traditional web or highly customized applications, in mobile applications, in thick clients, and more. Many organizations often embrace a combination of these technology deployments.
- Applications in industries such as financial services, healthcare, medical devices, consumer electronics also have federal and/or industry regulations in place that mandate stringent security.
- In-house developers and testers are busy working on new features—they often just don't have the time or the depth and breadth of knowledge necessary to keep up with all the new vulnerabilities, attack patterns, deployment technology nuances, and industry-specific regulations.

All these factors point to the need for third-party expertise with the appropriate testing techniques/tools to discover vulnerabilities and successfully remediate them.

The vulnerabilities in the code are evolving and increasing exponentially as well. And they can be exceedingly difficult to find for even the most trained internal developers and testers, increasing the likelihood an exploit.





## Black Duck security testing services

The sheer magnitude, diversity, and complexity of modern applications requires a wide range of expertise, tools, and testing techniques. The ability to test for security defects and analyze any application at any depth cost-effectively is important to mitigate risk and address compliance requirements. Many vendors can address only one or a few of the security testing factors involved. Black Duck is the only company that can do it all, under one roof, with systems-level oversight.

With over 400 consultants and the most comprehensive set of DevSecOps tools and services in the AppSec industry, Black Duck can be your partner to mitigate risk across the SDLC. In this solutions guide learn about the application security testing activities, tools, and processes that must be employed to achieve DevSecOps success.

## One unified platform for all your AppSec needs

The AppSec landscape is diverse and in a constant state of evolution. With all the disparate tools, programming languages and ecosystems, and CI/CD processes—plus the ever-increasing number of vulnerabilities and constantly changing hacking methodologies, it's a daunting task to keep up with it all. There is also a shortage of qualified security engineers. Even if you were to find a few with the depth and breadth of expertise needed across the different domains, it's a significant investment to hire and retain top talent. This is especially true as testing demand scales up and down as timely testing is needed—it's just much more cost-effective to outsource testing. Read on to learn about all the security testing services that are essential for a well-rounded software security program.

The ability to test for security defects and analyze any application at any depth cost-effectively is important to mitigate risk and address compliance requirements



## Security testing services

### Penetration testing

Penetration testing (pen testing) is essential for modern applications and complements automated tool-based AppSec testing. Pen testing examines application vulnerabilities and tries to exploit them, including vulnerabilities beyond the typical canned list of attacks, such as the OWASP Top 10 web application security risks. It uses both automated testing tools and manual testing techniques to ensure that false positives are eliminated, and then delivers a detailed vulnerability report along with expert remediation advice, allowing your team to prioritize the most critical vulnerabilities for mitigation. Pen testing focus areas include exploratory risk analysis and business logic testing. Black Duck pen testing is offered through multiple global assessments centers, ensuring that you have 24/7 access to AppSec tools, and experts with the right skills for your specific discipline.

### API pen testing

The current wave of digital transformation includes a multitude of web-based applications that offer a complete package of software products, and this has led to the proliferation of APIs. According to Gartner, "by 2022, API abuses will become the most-frequent attack vector."<sup>1</sup> Hackers take advantage of API vulnerabilities to gain access to business logic and even steal customer data. API pen testing enables you to find and fix API vulnerabilities before hackers can exploit them. Black Duck provides API pen testing that combines automated and manual techniques to cover the OWASP API Security Top 10 list.

### Red teaming

Hackers are constantly looking for new vulnerabilities and techniques to breach your defenses. As a supplement to pen testing, red teaming is an attack on your application on an even wider scale. The goal of red teaming is to find exploitable security holes across your organization's attack surface using a variety of composite attack vectors by chaining together seemingly separate or cross-domain vulnerabilities. This includes relationships between systems, software, and people. Trained professionals approach the application from an attacker's perspective to find gaps in your software system, and then deliver a detailed report that covers vulnerabilities found and mitigation/remediation strategies, the potential impact of a breach on the business, how the organization's engineering and testing can be improved, and more.

### Mobile application security testing

Mobile applications have been an integral part of many organizations' portfolios, and with the emergence of 5G they are gaining even more prominence. In addition to the up to 100x increase in network velocity and cell density, 5G also brings with it a whole host of new technology such as software-defined networking, network function virtualization, edge computing, and more. It will enable large-scale machine-to-machine communication and new applications such as smart cars, next-generation internet of Things (IoT), virtualization, and more. The new opportunities also bring never-before-seen threats and a much wider and more complex attack surface that is even more prone to security breaches. Black Duck experts understand the nuances of mobile application security testing (MAST) including local authentication/authorization, code quality, data storage, endpoint communication, APIs, use of open source / third-party libraries, and more. Black Duck MAST implements client / server-side code and third-party library analysis quickly so you can systematically find and fix security vulnerabilities in your mobile applications, without the need for source code.

## Static application security testing

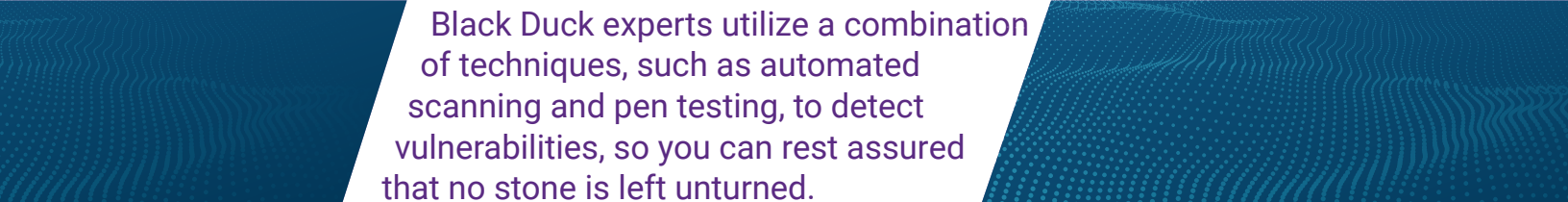
Static application security testing (SAST) is an integral part of AppSec. It performs a thorough analysis of the source code in a nonruntime environment and without executing it. SAST detects common to critical software security vulnerabilities and other quality issues early in the SDLC, which helps avoid costly changes later—potentially saving millions of dollars. Black Duck SAST offers multiple depths of secure code review, so you can tune the level of testing based on the risk profile of each tested application.

## Dynamic application security testing

While SAST scans for security vulnerabilities and quality issues early on in the SDLC, dynamic application security testing (DAST) identifies security issues during runtime. Black Duck DAST utilizes market-leading automated tools to identify common vulnerabilities, such as SQL injection, cross-site scripting, security misconfigurations, and other common issues detailed in lists such as OWASP Top 10, CWE/SANS Top 25, and more. DAST also includes manual penetration testing to find vulnerabilities that can't be found by out-of-the-box tools, such as vulnerabilities pertaining to authentication / session management, access control, information leakage, and more. Consultants perform a thorough review, identify false positives, and provide actionable mitigation and remediation strategies.

## Network security testing

The network is one of the most exposed components of your infrastructure. Network devices, the Domain Name System, and servers should be periodically tested for vulnerabilities. Network security testing involves a thorough assessment of routers, switches, web servers, and firewalls. Black Duck experts utilize a combination of techniques, such as automated scanning and pen testing, to detect vulnerabilities, so you can rest assured that no stone is left unturned. The manual testing checklist includes test cases for encrypted transport protocols, SSL certificate scoping issues, use of administrative services, and others. Defects discovered are triaged manually by our experts and included, along with recommended fixes, in the final report.



**Black Duck experts utilize a combination of techniques, such as automated scanning and pen testing, to detect vulnerabilities, so you can rest assured that no stone is left unturned.**

## Embedded software testing

Unlike traditional application software, which can run on a variety of computer systems, embedded software systems are designed to run on a unique individual device. Such a software system is restricted by its device's memory, processing, and other requirements. The IoT, automobiles, consumer electronic devices, and medical devices are some examples of embedded systems. Initially commercial/proprietary software was more common in embedded systems, but open source software is gaining popularity. However, while cost-effective, open source software comes with its own security and license concerns. Embedded software systems in general are far more complex than traditional application software. A lot of embedded devices are now always connected to the web by default (IoT) and they number in the thousands to even millions.

Testing and securing embedded software systems is crucial, as a breach could lead not just to financial and brand equity losses, but potentially also to loss of life. Due to the complexity, variety, and diversity of embedded software systems, it's just not possible for an individual or even a small team of experts to know everything about them. Black Duck has a dedicated team of hundreds of embedded software security experts with decades of experience in testing and securing complex systems. Our embedded software testing process takes a risk-based systems approach and covers communication, client, and server analysis. This risk-based approach prioritizes and tackles the defects that matter most to your business.

## Thick client testing

Thick or fat clients are self-sufficient and have their own operating system and software, which allows them to perform the vast majority of processing on their own. But because of the lack of general industry standards in thick clients, it's easier for a hacker to find and exploit vulnerabilities in them. The most common vulnerabilities seen within thick clients are memory corruption, injection, cryptographic weaknesses, and client-side trust issues. These vulnerabilities can lead to a complete compromise of systems where the thick client software is installed, unauthorized access to server-side information, and more.



Thick client applications involve both local and server-side processing and often use proprietary protocols for communication. They may also contain multiple client-side components running at different trust levels. Simple, automated vulnerability assessment scanning isn't enough. That's why Black Duck consultants customize every thick client test to the individual application. The risk-based analysis focuses on the thick client software and the server-side APIs it communicates with. Each customized assessment includes automated scanning, configuration, network communication, server, and client analysis. Black Duck expert analysis ensures that your thick clients remain protected from attackers.

## Open source audits

Open source has proliferated in virtually every sphere of software development. Most applications now either have some components of open source or have open source as their foundation. Open source, however, can come with significant security and licensing risks that if not handled correctly can lead to penalties and public embarrassment. It's imperative to perform an open source audit to comprehend the open source license obligations, application security, and code quality risks that are not always evident.

An automated software composition analysis (SCA) scan that integrates seamlessly into the SDLC can help identify vulnerabilities that need to be addressed and aid with license compliance. However, some open source code can easily go undetected during an automated scan, so evaluating scan results requires expertise. The Black Duck open source audits team includes dedicated experts with decades of experience auditing open source software. They can help you detect and patch vulnerabilities hidden in your code and mitigate potential legal exposure by identifying third-party and open source code within your codebase.

## Malicious code detection

Forrester predicts that "one-third of security breaches will be caused by insider threats in 2021."<sup>2</sup> Disgruntled developers may plant malicious code in your software system that they can exploit in the future. The problem with this kind of malicious code is that since it is planted by someone with intimate knowledge of the software system, the infected system can appear to be completely normal. Malicious code detection (MCD) finds suspicious constructs in production binaries, configurations, and data. It also (privately) identifies the malicious code that typical security tools can't find, along with the insider threat actors. MCD provides expert advice on malicious code management and delivers vulnerability remediation strategies.



## Real-world results

Here are a few organizations that have protected their most valuable asset—their applications—with the help of Black Duck security testing services.

- **A leading global food and beverage company** needed to standardize and scale its pen testing and SCA across the globe. It also wanted to train all its developers. By leveraging the services that Black Duck offers through a flexible subscription licensing model, the company was able to meet testing demands and train developers on security best practices consistently across the globe.
- **Asian Life insurance company** had its website security compromised a few times due to subpar security testing, so it brought in a new CISO to improve security testing quality and also migrate applications to the cloud. The CISO worked with the Black Duck security testing team to develop a comprehensive cloud security program that consisted of rigorous security testing coupled with eLearning and developer training. The company securely migrated applications to the cloud and also developed new custom solutions such as biometric testing.

### References

1. Dionisio Zumerle, Jeremy D'Hoinne, Mark O'Neill, [How to Build an Effective API Security Strategy](#), Gartner, December 8, 2017.
2. Heidi Shay, [Predictions 2021: The Path to a New Normal Demands Increased Cybersecurity Resilience](#), Forrester, October 26, 2020.

## About Black Duck

Black Duck<sup>®</sup> 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](https://www.blackduck.com).