What to Look for When Evaluating an Application Testing Provider

Some security vendors offer low-budget, limited tests. Others craft expensive, custom solutions. It's not always clear what type of testing support you will receive unless you know the right questions to ask.

Avoid costly mistakes with this checklist.

The right partner will match your risk profile, help fix your vulnerabilities and scale with your needs.

Cigital

12

Questions to Ask Your Application Testing Provider

CAPABILITIES AND EXPERTISE

1

What types of tests do you offer?

The answer should be: any type of test you need, on-demand, at scale.

Available testing options should span from automated to in-depth manual testing. Industry analysts will tell you no single testing tool can detect all application security vulnerabilities. Vendors should have the ability to utilize **multiple best-of-breed tools, with customizations that match your business needs.**

Keep in mind: **automated testing alone is not sufficient** to provide a complete picture of your vulnerabilities. To defend against multi-step attacks or ones that involve social engineering, your vendor should be able to conduct in-depth manual testing to mirror the perspective of a hacker.

2

How will your tests match my risk profile?

Your vendor should have the expertise to apply different testing strategies based on the risk level and unique requirements of each of your applications.

The right vendor will help you create a full inventory of your applications and rank them according to security risk. They'll design a testing plan so you can focus time and money on the things that matter most.

3

When you find vulnerabilities, how will you help me fix them?

Classic application security testing vendors consider their job to be just that—running tests. Vendors with a holistic approach provide remediation guidance to empower you to fix issues and address causes so fewer security issues ever reach the testing phase.

Make sure you understand how reports are created and verified. You'll be more confident if you know **every testing report is reviewed by a security expert** to eliminate false positives. The top vendors will also include contextual remediation guidance in all reports along with the vulnerabilities they find.

Vendors should **review findings with you directly.** They should include developers in report read-outs to detail causes of vulnerabilities and remediation advice. Even after the initial test read-out, they should provide on-demand live remediation support.

4

How well do you know the security compliance requirements for my industry?

If your applications are subject to industry-specific requirements (PCI DSS, HIPAA, etc.), make sure the vendor includes **compliance testing.** As regulations are becoming stricter and penalties for non-compliance are increasing, it's essential that your vendor is proactive in providing guidance to you on any actions you need to make.

Your vendor should help you do more than simply meet minimum requirements for compliance, by including compliance as part of a broader application security strategy.

5

How will you demonstrate success?

To see whether application security testing has been worth the investment, consider how your vendor's approach will help you answer the following:

- How quickly are tests run compared with any previous system you used?
- Are testing methods identifying vulnerabilities previously missed?
- Are you saving time provisioning secure production applications?
- Are your developers improving over time? What is the defect density of new code?
- Is design improving? Or are tests finding the same flaws over and over?
- Do developers now have time they can use on other projects?

6

How easy is it to run tests?

Once you decide to invest in application security testing, you'll want to get going with minimal fuss so that you can start seeing results right away. Make sure your vendor provides **sufficient resources to jumpstart** your testing program.

Make sure your vendor insulates you from the complexities of running an optimized application test.

Dig into the details:

- What does it take to request a test on one or more of your applications?
- Do you need to schedule in advance and confirm testing resources are available? Or, does the vendor allow you to schedule tests and set testing windows?
- Can you specify which applications you want to test and the type of tests you want for each?
- Does only one person have the ability to request tests, or can anyone on your team request a test when needed?

7

How will I know what kinds of tests have been run on my applications?

It is important that you have control to determine when tests take place and what type of tests your vendor runs on your applications. Make sure you have a transparent way to track your vendor's performance and an easy way to **retrieve tests results and share remediation recommendations.** That way, when it's time to make decisions about budget and answer your boss's questions about how money was spent, you can clearly demonstrate the work that was done.

8

Do you have capacity to test all of my applications?

Check that your vendor has a coverage model that **lets you test your full portfolio** at the depth that maps to your application risk profile. Any application in your portfolio can provide a hacker access to reach your most valuable and sensitive data.

Even if you don't test every application at the same depth, it's important to have a full inventory of your applications and a consistent testing schedule so nothing is missed.

9

If my testing needs change, how would that affect my budget?

Let's say your business grows or your organization is part of a merger or acquisition. Or, you may be asked by one of your customers or partners to test applications in a different way to meet their security requirements. Your testing vendor must provide **flexibility to manage your evolving application portfolio** without increasing your costs.

Make sure you are not penalized if you choose to switch testing focus to a different application or test at a different depth.

Find out before you sign what total testing coverage would cost.

10

How do I know I can trust you?

Application testing vendors will be knee-deep in your most sensitive systems and data. If you are allowing vendors access to test applications inside your firewall, all the more reason to choose one with a proven track record and repeat clients.

Check out their funding and their management. Make sure they are stable companies with well-respected leaders who are known in the industry.

Choose someone who has **long-term relationships with customers** that have no tolerance for security risk. Many customers don't want to publically share they are using security services, but are happy to talk with colleagues off the record. Make sure you **get references and ask them about service quality** as well as the vendor's technical proficiency.

11

Are you willing to prove your accuracy in a head-to-head comparison?

Don't be afraid to put your vendors to the **test in a real-life environment** to assess the accuracy of their testing approach. Lower quality application testing services can miss critical vulnerabilities and deliver inconsistent results.

12

Have you been in my shoes?

Too many consultants offer suggestions that only work in theory. A provider with staff that has worked as an in-house security leader or a developer **understands real-life pressures** and working environments and can become a true partner to your team.

Application testing is one of the most important decisions you will make in protecting the integrity of your valuable business assets. Don't be afraid to put your vendors to the test to be sure they can provide what you need to move forward with confidence.

Application Security Testing Vendor Checklist

Use the checklist below as you evaluate each testing vendor.

Vendor Name	
What types of tests do they offer?	
How will their tests match your risk profile?	
When they find vulnerabilities, how will they help you fix them?	
How well do they know the security requirements for your industry?	
How will they demonstrate success?	
How easy is it to run tests?	

How will you know what kinds of tests have been run on your applications?	
Do they have capacity to test all of your applications?	
If your testing needs change, how will that affect your budget?	
How do you know you can trust them?	
Are they willing to prove their accuracy in a head-to-head comparison?	
Have they been in your shoes?	
Notes:	

About Cigital

Cigital is one of the world's largest application security firms. We go beyond traditional testing services to help organizations find, fix and prevent vulnerabilities in the applications that power their business. Our holistic approach to application security offers a balance of managed services, professional services and products tailored to fit your specific needs. We don't stop when the test is over. Our experts also provide remediation guidance, program design services, and training that empower you to build and maintain secure applications.

For more information contact us at: info@cigital.com or +1 800-824-0022.
www.cigital.com