FORTRA

GUIDE (Core Security)

When to Use Penetration Testing Software, Services, or Both

You know you need a penetration test. Whether it is from an internal mandate or external compliance requirements, it has to be done. From here, the question is how. Do you leverage software and the analysts you already have, hire an external service provider to do the heavy lifting for you, or use some combination of the two? All are reasonable options depending on your circumstances, but how do you determine which one to pick?

We explore what factors go into choosing one solution over another and discuss the pros and cons of each approach. In addition, we provide guidance to determine when it makes sense to outsource versus doing it yourself, as well as tips for selecting the right partner.

Defining the Scope of Your Pen Test

Selecting the right pen testing solution for your organization necessitates a quick analysis of what assets you have and what constraints are in place. Answering simple questions will help you identify this information and determine the best-fit solutions.

1. What services or technologies do you need to test?
2. Is this test meant to meet compliance requirements?
3. Are there delivery timelines to meet?
4. Does your organization have existing penetration testers?
5. Will this be a one-time test, or will repeated testing be necessary?

Answering these questions will give you the baseline information necessary to determine what solutions will meet your needs for a penetration test. These questions are only intended to help narrow down the selection, which is why in some cases, multiple reasonable options will be available, allowing you to choose what is most appropriate.

Meeting Compliance Needs

One of the primary drivers of needing a penetration test is meeting compliance and regulatory requirements. Several regulatory compliance frameworks, such as PCI and SOX, require penetration testing to validate controls but often leave flexibility on how it is accomplished. By testing controls, organizations can prove that the controls are in place and fully functional.

How this testing is accomplished depends entirely on the compliance mandates to be met. In the cases where a third party is required to remove any potential for bias, there is no choice. In most cases, though, the testing does not have to be done by a third party, though it may still be beneficial to gain a non-biased or fresh perspective for the testing. In these cases, the organization has flexibility and can decide based on other factors.

Analysts Skills and Experience

When looking at a penetration testing engagement, your organization needs to consider if there are individuals with the skills and experience to conduct the test. This information helps determine if you can do testing in-house or externally.

Just because an organization does not have full-time penetration testing personnel or individuals with experience does not necessarily mean that an external tester is required. The most basic third-party testers do little more than run analysis tools and use the reporting from it as their report. Fundamental analysis can be conducted by an interested engineer with a reliable toolset similar to that used by external parties. This approach allows them to "get experience" or "learn to test" while saving time and money, which is an organizational win-win.

It is important to stress that a safe and reliable toolset is crucial for implementing a proper test. Using random open source tools or those found on black-hat sites may get the job done, but they can cause outages or damage infrastructure if improperly used or include malicious code posing a security concern. Properly constructed tools will have safeguards to prevent damaging or disrupting infrastructure, allowing tests to occur without impacting regular users or daily business operation.

If no resources are available and an in-depth test is required, you will need an external testing team for at least part of the testing. Using an external party conducting in-depth testing in conjunction with an internal tester doing the primary analysis can help get the best of both worlds. The internal tester can gather the external party's information to drive deeper, more targeted testing. Splitting the workload reduces the time needed for the engagement, eliminating a sizeable evidence-gathering portion for the external testers.

Targeted Expertise

Even if your team has penetration testing experience and skills, they may not have it in the area needed. Your team's skills may not directly align with the technology for targeted testing, such as Cloud services, mobile applications, networks, and other specific technologies. Additionally, they might also lack the ability to set aside internal bias. In these instances, using some level of external expertise and objectivity can be beneficial.

Temporarily leveraging 3rd party expertise in that area can ensure better results. They can deliver a fresh perspective on the evaluation as they have no pre-existing knowledge or opinion on the environment they are testing. It does not mean they need to be the only testers, but they should be considered a part of the testing engagement, even if their role is tightly scoped.

Timelines

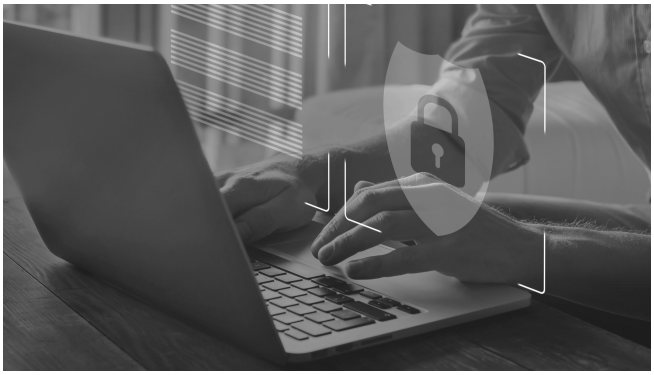
Timelines for having a penetration test can have a massive impact on how your organization can approach a penetration test. Expedited timelines may cost extra for an external tester as you ask them to prioritize your testing over others. Even with extra cash, sometimes the availability is not there, and you might have to take a portion of it in-house.

While it may seem like a surefire need for internal testing, it instead means that internal testing should be an aspect of it. Using a hybrid approach to testing can streamline the testing process. Tools can help organizations conduct the necessary tests to meet deadlines and hold them over until third parties are available, reducing the need to pay extra to expedite. Internal testers eliminate the easy and routine testing portion allowing third parties to hit the ground running and focus on more complex testing.

Available Resources

Even for organizations with the skills and experience, there may not be time for these individuals. They may be booked on higher-priority engagements or understaffed due to the existing skills shortage in cybersecurity which is not unlikely with the shortage of 2.7 million qualified cybersecurity professionals. This situation complicates the process of running a penetration test internally.

To help bridge this gap, organizations can leverage technologically savvy engineers in specialties other than cybersecurity. With the right toolset, these non-penetration testers can conduct testing on their own to help discover critical vulnerabilities. Modern toolsets overcome their lack of specialization and help them prioritize and classify vulnerabilities, allowing them to generate high-quality reports that are on par with many external testers.



Need for Repeated Penetration Testing

A penetration test is only a point-in-time assessment of the existing environment. Rapidly changing environments using cloud and agile-driven systems may drive organizations to have repeated engagements to test their infrastructure so that the evaluation is up-to-date. Change does not always drive this need. Highly-regulated environments may still require repeated testing throughout the year to validate controls.

Using a third party to accomplish this can be costly. In-house may be more cost-effective, but internal availability for repeated testing may limit this or require a hybrid approach with some internal and some external testing. The hybrid approach with external testers conducting the first assessment round generates findings. Then for subsequent testing, internal users can follow up on results by doing remediation validation with tools. Using hybrid approaches, organizations get the best of both worlds with fresh outside perspectives but cost savings by using internal teams.

Infrastructure Size

The size of the IT footprint is a significant factor to consider in determining whether in-house teams should attack it or if it requires an external party to test. For organizations with numerous areas that need testing, utilizing internal teams is often less expensive. Sometimes the organizational IT footprint is just so expansive that it requires more than any penetration testing team could cover in a year. Using tooling to allow non-pen testers to conduct testing helps reduce the load on existing pen testing teams.

Just because internal testing is less expensive does not mean there is no reason for external testers. External testing provides additional load reduction or lends focus to specific areas. This is especially valuable for external teams with very specialized or targeted skillsets. Outsourcing the entire project allows the organization to focus on what they do best – running security operations. By outsourcing, organizations no longer need to worry about managing tools or conducting tests themselves. They can instead focus on securing the rest of their network.

Alternatively, a hybrid approach of internal testers using tools combined with external testers can help divide the project into smaller, more manageable sections. Internal testers running automated tools can focus on less complicated or lower-risk areas of the organization allowing external testers to run more in-depth testing against higher-value targets. By dividing up the load, the organization can save on costs while still gaining the benefits of external testers.

Penetration Testing Software *and* Services

The important thing is that your organization is conducting a penetration test. There is no need to force one route over the other as they synergize well. Organizations can efficiently and repeatedly implement penetration testing by starting small and leveraging tools to start the process. Then by weaving in third-party assessments, they can get fresh perspectives and more profound, more targeted testing, giving you the best results with a minimal strain on resources.

For organizations that wish to reduce costs and take advantage of internal resources, Core Impact places the power in their hands to conduct penetration tests. Core Impact is a professional-level security assessment toolset that allows even inexperienced individuals to run a penetration test on your organization. With Core Impact, testers can run penetration tests against network, client-side, and web applications. Core Impact removes the guesswork of parsing complicated findings and creates risk-prioritized reporting that elevates the most important results to action.

Sign up for a demo today to learn more about how Core Impact can help your organization make the most out of internal penetration tests to reduce costs and facilitate external testing.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.