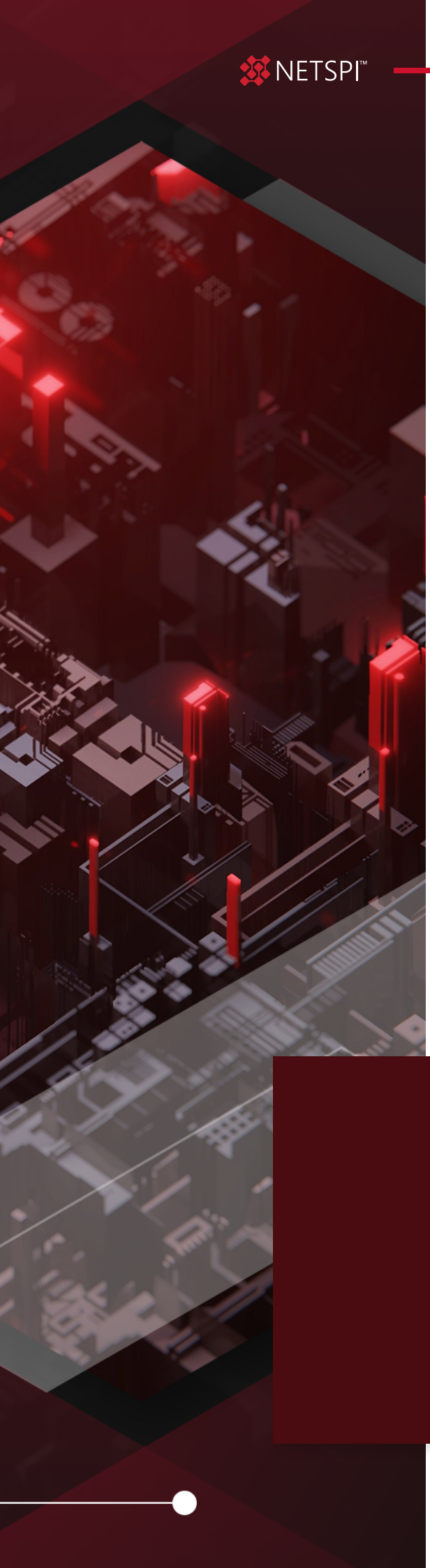
HOW TO CHOOSE THE BEST PENETRATION TESTING COMPANY

NETSPI™



INTRO

Choosing the right penetration testing partner for your organization is an imperative security decision, one that could cost considerable budget, time, and resources if not chosen wisely. It can be a challenging decision given there are hundreds of providers vying for your business, all of which offer varying levels of service, testing methodologies, and use different technologies to perform penetration tests.
This four-part guide will help security and IT leaders make a clear, informed decision and ensure they are getting the most value out of their partnership.

TABLE OF CONTENTS

WHY DOES MY ORGANIZATION NEED A PENETRATION TEST?

There are many reasons organizations seek out a penetration test, however, the decision to perform a penetration test on your applications, network, cloud, or physical security depends on your unique business goals. According to Gartner, one of the key challenges in choosing the best penetration testing company is that "many buyers of penetration testing services fail to define their goals and needs prior to engaging with a provider, resulting in engagement outcomes failing to deliver against expectations." Prior to deciding which provider to partner with, it is important to understand the reasons why you are pursuing the pentest in the first place. Here are nine reasons why organizations partner with third parties for penetration testing:

1. To Deliver Secure Software for Less Money:

Security gaps remediated earlier in the software development life cycle (SDLC) cost less to fix than problems found later. Despite best efforts, security vulnerabilities slip through standard software testing processes. With a penetration test of your software and applications, exploitable vulnerabilities can be identified and mitigated earlier on.

2. To Avoid Breaches:

Discover vulnerabilities and exposures proactively to remediate them and prevent an attack—and avoid the costs of downtime and clean-up resulting from a breach. In addition, preserve the organization's good reputation and protect relationships with business partners and customers.

3. To Think Like an Adversary:

Only a penetration tester or a malicious attacker can chain together seemingly low-risk events to verify which vulnerabilities enable unauthorized control. Understanding and validating the implications of vulnerability scanner results to a specific application or organization requires human insight. Manual testers can also identify business logic vulnerabilities that tools cannot, but malicious hackers can.

4. To Achieve Compliance:

Meet security testing requirements from relevant regulatory bodies. Penetration testing is required to evaluate cyber security efforts and achieve compliance with regulations, such as the payment card industry (PCI) security standard or the Health Insurance Portability and Accountability Act (HIPAA). Other organizations may require penetration tests to comply with specific infosec management standards, vincluding the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS).

5. To Eliminate False Positives:

Automated scans often result in a seemingly endless list of vulnerabilities, but not all are valid. Introducing manual testers to validate the real, business-critical vulnerabilities helps an organization avoid spinning its wheels dealing with inaccurate or incomplete vulnerability assessment data.

6. To Focus Remediation Efforts:

Prioritize remediation for the most important vulnerabilities and receive helpful guidance from your third-party testing team, such as how to remediate specific vulnerabilities and instructions for how to reproduce each vulnerability.

7. To Demonstrate Business Impact:

Penetration testing clarifies the business impact of inaction. Understanding the business impact of each vulnerability helps justify security investments and improve decision making.

8. To Augment the Security Team:

A fresh set of eyes from third-party security experts can help strengthen an organization's vulnerability management program and validate its ability to protect the business from cyberattacks. Hiring a penetration testing partner that can serve as an extension of your team also gives valuable time back to your security teams to focus on remediation.

9. To Evaluate the Effectiveness of Security Controls and Capabilities:

Learn if your security controls are working – or not – with a penetration test.

NETSPI™

10 QUESTIONS TO ASK PENTESTING COMPANIES DURING THE RFP PROCESS

RFPs can turn into a lengthy, taxing process. To narrow your choices down to the best penetration testing companies, it is important to ask the right questions at the start. Here are 10 essential questions to ask potential pentesting companies during the RFP process:

1. How do you source your resources/testers?

Ask this question to understand how a company sources its pentesters, project managers, and other day-to-day practitioners working on your assessment. Would you prefer working with a team that works together often or a team of outsourced experts? The answer should also provide insight into the effort an employer puts into finding the best talent.

2. Which regulatory bodies and compliance frameworks does my organization need to be aware of?

Test the industry knowledge of the pentest companies you are evaluating. Learn how well they understand the external pressures your organization is facing and the additional expertise they can bring to the table.

3. Can you share a breakdown of the tool-based vs. manual effort that goes into a typical penetration testing engagement?

Find the right balance between automated scanning and manual testing based on the requirements of your organization. The answer should also reveal the company's testing methodology and give you an understanding of the tools they use. Remember, to find critical business logic vulnerabilities, manual testing is required.

4. How do you ensure your team is up to date on the latest certifications and training?

The answer to this question will be an indicator of how much the company values its employees continued education and advancement. A company that strives for innovation will have a long list of processes, checklists, peer reviews, and more. Beyond external trainings and certifications, be sure to ask about the internal training efforts in place.

5. How do you ensure return on investment (ROI) from each engagement?

Ensure your testing partner is maximizing your investments to find business impactful vulnerabilities, not focusing on administrative tasks. ROI for security initiatives can be difficult to measure – and pentesting is no exception. Pentest efficiency is a great place to start. Ask the prospective companies how they reduce or eliminate the administrative burden of de-duplication and vulnerability tracking, how they enable multiple testers to work simultaneously, and learn about the automated processes they have in place to enable their pentesters to perform a test efficiently and thoroughly.

6. How do you contribute to the greater security community?

Instead of asking, "how innovative are you?" ask this question. Explore the various ways a pentest company participates in the security community to gauge its drive to innovate. Review its open source tools, GitHub repository, public trainings, conference participation, community involvement, and more.

7. What do you consider your specific focus areas?

A straightforward question that can reveal a lot about a pentest company. Which types of pentests are they hired for most? What types of companies do they work with and in what industries? Which technologies enable their services?

8. How do you ensure consistency and repeatability across all engagements?

Consistency is key in penetration testing. How can you ensure that your pentest isn't only as good as the latest tester? In this response, look for how they maintain centralized communication, repeatable processes, validate vulnerabilities, and track the progress of each test.

9. How do you plan to grow with my organization over time?

Maintaining a relationship with one pentest company over time has its benefits, but only if that company can scale with your business. Talk about the plans for your organization and learn how each company can support you at every part of your growth journey.

10. What services would you recommend to this organization that aren't currently addressed within the original list of needs – and why?

A key benefit of working with a third-party penetration testing company is that it should be able to look at your security program holistically. Ask this question to explore other possible areas of weakness and, as a bonus, learn how the company delivers its recommendations.

NETSPI™

5 PENTESTING USE CASES THAT ARE OFTEN OVERLOOKED

At the most basic level, the goal of a traditional penetration test is to uncover vulnerabilities that are potentially exploitable by cyber adversaries. While this is the main objective for a pentester, penetration testing has evolved over the years – and its use cases have, too. Below are five ways your penetration testing provider can add value to your vulnerability management program beyond discovering vulnerabilities.

Reduce Time Spent On Vulnerability Management Administrative Tasks

Penetration testing and automation go hand in hand. Automating mundane vulnerability management tasks, such as report generation, ticketing integrations, deduplication, and vulnerability correlation, will save your security team valuable time and resources. Notably, ticketing integrations, with systems like Jira or Service Now, eliminates an extra step in the vulnerability remediation process.

Remediation Recommendations and Replication Instructions

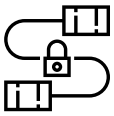
You've received a list of your vulnerabilities – now what? Without guidance provided by the testers who discovered the vulnerability, assigned remediators are left in the dark. To better support your remediators, look for a penetration testing partner that provides clear instructions for remediation with every vulnerability.

Support with Communicating Results to Various Stakeholders

Communication is a common challenge across security assessments. Communicating the results of a penetration test to an audience that may not have a deep technical understanding, the c-suite for example, has proven difficult. Pentesting companies consistently communicate with multiple stakeholders across many technical levels and should be able to help you identify the metrics that matter to each audience and educate them on the business impact of any given vulnerability if it goes un-remediated.

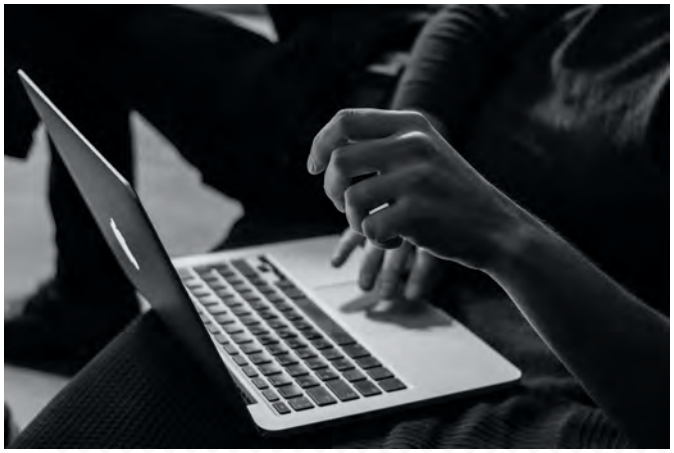
Your Guide to a Mature Security Program

A penetration testing company's role should not end after the final vulnerability report is shared. Look to your penetration testing team for guidance on how to mature your security program.



Track the Progress of Your Vulnerability Management Program Over Time

There are benefits to working with a single pentest company over time. One key benefit to seek out is the ability to track the status of your vulnerability management program over time. Benchmarking the progress of your vulnerability management efforts is a tangible, data-driven solution to communication security program return on investment (ROI).



NETSPI™

4 CRITERIA FOR EVALUATING PENETRATION TESTING COMPANIES

Today, businesses find that the pentesting industry is made up of a lot of providers offering vulnerability management services. But does that mean all penetration testing services offer the same results? Simply stated, the answer is no. To help organizations choose the right team for their pentesting and vulnerability management programs, consider the following four paradoxical criteria that should help CISOs, security leaders, among others select a top penetration testing partner.

Pentesting Should be Agile, Yet Consistent Over Time

It's important to hire a talented penetration testing team – one that's able to look at the environment through the eyes of an attacker and bring their insights of technical risk to the table as the environment and technology become more complex over time. A pentesting team needs to be agile to continuously improve and evolve to meet the ever-changing and elevated risk and complexities that your business may face.

While evaluating agility, it is important to also look at consistency. Does your potential pentesting partner have a team orientation versus an individual or outsourced consultant. Who owns the knowledge? What if that individual moves on to a new role? You shouldn't consider a white hat tester who acts alone. Rather, choose a pentesting team built around a consistent delivery of quality, service, and results, that can be an extension of your internal team and will bring you the foundational support you need in your vulnerability management program.

The Pentesting Process Should be Custom Yet Standard

With 640 terabytes of data tripping around the globe every minute, is it possible to put standards around your vulnerability management program? It's not only possible, it is a necessity. Who you get doesn't have to be what you get, as people so often think. From project management workflows and practitioner guides to standardized pentest checklists and testing playbooks, ensure formalized quality assurance and oversight to receive consistent results, no matter who your assigned security consultants are.

Understanding that no organization is the same, there may be some commonalities between industries, such as similar regulatory bodies to comply with, for example. This allows pentesters to put some standardization into their process while allowing for customization and flexibility that is unique to the client environment from a business or technical perspective.

Technology Should be Automated to Increase Manual Pentesting

Automated scanning is foundational to any penetration testing program. It's how an organization handles the thousands of results from those scans that is critical – as there will be duplicates, false positives, and many, many data points, oftentimes delivered in spreadsheets or PDFs. Your internal security/IT team is then tasked with sifting through, sorting, and evaluating that data. Is that administrative work the best use of their time?

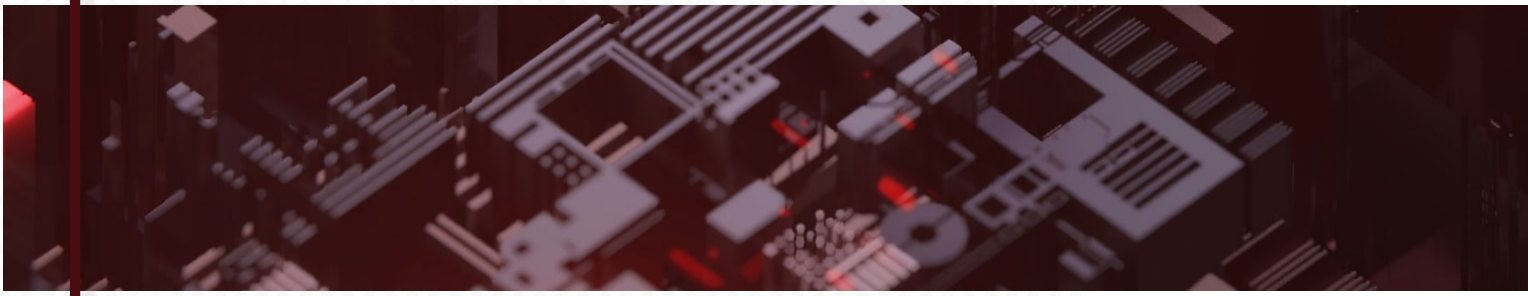
Focus your internal team on finding solutions for effective and fast vulnerability remediation, rather than spending their time heads down in administrative tasks. It's up to your pentesting team to identify and communicate the priority vulnerabilities, not hand you a document and wish you luck. Look for a penetration testing provider who has tools in place to automate pentest reporting functions and deliver results that can be easily sorted and acted upon so that the majority of human capital investment is focused on finding business logic vulnerabilities that tools cannot.

A Focus on Internal R&D Will Strengthen the Entire Security Community

Being able to collaborate with a team is critical in our client relationships. Why dedicate so much time to continued education and mentorship? Pentesters are consistently asked to be forward-thinking and penetration test increasingly complex environments. Training and collaboration are key to helping grow and scale pentesting talent to meet the industry's evolving needs.

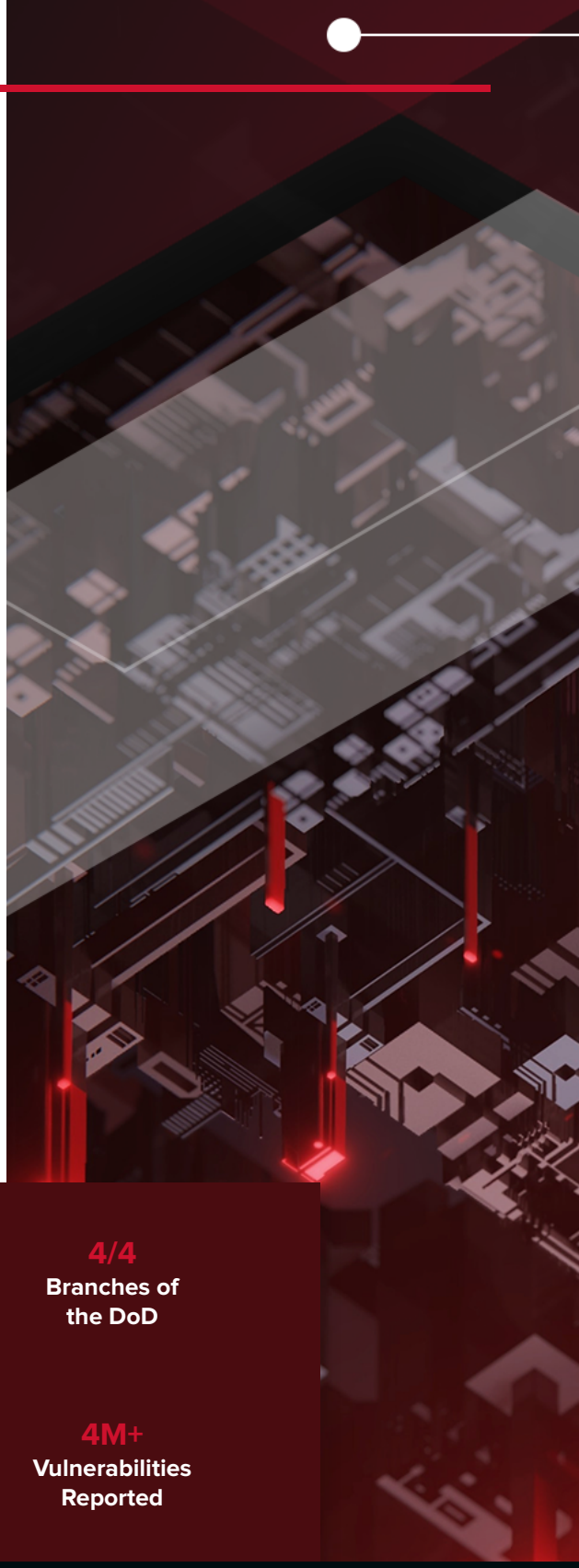
Collaboration and innovation are key to evolving as an enterprise and as an industry. Pentesters are intensely creative and have highly curious technical minds. The effort a pentest company places in research and development should be shared with the broader security community.

Penetration testing services are the same by definition, but none are created equal. When hiring a penetration testing company to test your applications, cloud, network, or perform a red team, consider pentesting talent, processes, technology, and culture to ensure you're getting the most value out of your partnership.



ABOUT NETSPI

NetSPI is the leader in enterprise security testing and vulnerability management. We are proud to partner with nine of the top 10 U.S. banks, the largest global cloud providers, and many of the Fortune® 500. Our experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces. We uniquely deliver Penetration Testing as a Service (PTaaS) through our Resolve platform. Clients love PTaaS for the simplicity of scoping new engagements, viewing their testing results in real-time, orchestrating remediation, and the ability to perform always-on continuous testing. We find vulnerabilities that others miss and deliver clear, actionable guidance allowing our customers to find, track, and fix their vulnerabilities faster.



2/3 Largest Global Cloud Providers

9/10 Top U.S. Banks

3/5 World's Largest Healthcare Companies

4/4 Branches of the DoD

15K+ Completed Engagements

150K+ Hours of Testing Annually

1M+ Assets Tested

4M+ Vulnerabilities Reported

Email sales@netspi.com to learn more or call us at 612-465-8880