BUYER'S GUIDE

2026 Penetration Testing Buyer's Guide

A guide to selecting the right penetration test to comprehensively assess your defenses and discover weaknesses before a cyberattack strikes.

SOPHOS

Introduction

Selecting the right penetration testing provider can be challenging.

The market is flooded with offerings from hundreds of vendors, ranging from global cybersecurity giants to boutique firms. And the market is only going to grow. The penetration testing market is valued at $3.09 billion USD in 2026[1], and is anticipated to exceed a $5 billion USD annual valuation by 2031.[2]

How one vendor defines a penetration test often differs greatly from another, adding to the complexity of choosing the right partner for your organization. There are numerous variables to consider, measured against your goals and objectives.

This guide aims to clear up the confusion. It covers why penetration tests matter, the common types of tests available on the market, and the critical components that make up a best-in-class penetration test that truly puts your defenses to the test the way a threat actor would. Armed with these insights, you will be better equipped to make the right decision for your organization.

What is a penetration test?

A penetration test identifies weak spots in an organization's environment and security controls, providing opportunities to fix issues before a real attacker discovers them.

The growing need for penetration testing

Ransomware. Business email compromise. Identity attacks. AI and automation exploitation. An ever-expanding perimeter. Employees lacking cybersecurity awareness. Defending your company is an exponentially difficult task.

A security strategy fully reliant on reactive measures is no longer sufficient. Regardless of company size, industry, or location, you must take stock of your defenses and assess their effectiveness on a regular basis. And the time for that activity is not when a malicious actor knocks on your door or accesses your network.

Penetration tests are designed to discover exploitable vulnerabilities and unknown security gaps before a threat actor can find and use them to breach an organization. Proactive security assessments like penetration tests are more important than ever given the state of the security landscape.

Consider:

141%

Increase in the use of remote ransomware since 2022.[3]

65%

Percentage of organizations citing a known or unknown security gap as a reason for being exposed to a ransomware attack.[4]

63%

Percentage of discovered root cause for adversary entry attributed to either compromised credentials (41%) or exploited vulnerabilities (22%).[5]

$1.53M

Average recovery cost in USD from a ransomware attack.[6]

Why organizations buy penetration testing

Penetration testing has long been a key element of a proactive security approach. Certain compliance regulations recommend annual testing. More organizations are emphasizing the importance of determining the current status of their defenses, for a variety of reasons:

Discover weaknesses in defenses before adversaries find them

- It's one thing to believe your defenses are sound. It is another to validate that belief with penetration testing that truly probes your environment, looking for weak spots to exploit.

Answer the question, "How prepared are we to defend a cyberattack?"

- CISOs face this question from executives and boards constantly. Subjecting your company to a comprehensive penetration test delivers the answer and highlights ways to improve before a threat strikes.

Assess the ability to detect and respond to threats

- Organizations purchase security solutions to detect potential threats and respond when one is identified. A penetration test that emulates real adversary behavior is a great way to test those capabilities.

Satisfy and exceed compliance regulations

- In many industries, passing compliance audits is not just a business objective. It is a requirement, and falling short can lead to serious financial and reputational repercussions. Penetration tests aligned with compliance standards better prepare you for your next audit.

Enhance their cyber insurance position

- Penetration testing helps demonstrate your commitment and investment in security and can pay dividends when searching for favorable cyber insurance terms.

Challenges in testing defenses

Juggling day-to-day IT tasks with security operations is challenging for several reasons.

Lack of budget

When budgets tighten, proactive security measures like penetration testing are often among the first to lose funding. This can turn testing into an irregular, low-priority activity, making it harder for organizations to confidently understand where exploitable gaps may exist in their defenses.

Lack of in-house expertise

96% of smaller businesses find at least one aspect of investigating suspicious alerts challenging.[7] Hiring, training, and retaining security personnel are difficult, which is often why organizations look to work with security vendors. Finding the advanced skills and experience needed to deliver in-house penetration testing — and to apply the human context that comprehensive penetration testing provides — is beyond what most organizations can accomplish on their own.

Lack of context into emerging adversary attack tactics

Organizations may subscribe to threat intelligence feeds, but these sources do not always reflect novel attacker tactics and techniques. Depending solely on internal teams to interpret and test against emerging threats is difficult, especially when many organizations lack dedicated researchers to keep pace with the rapidly evolving adversary landscape.

Lack of awareness into risk

Some organizations assume they are unlikely targets because of their size or industry, leading them to deprioritize proactive security measures. The 2025 Sophos Active Adversary Report studied attacks against businesses spanning 32 industries — 84 percent of those companies employed fewer than 1,000 employees.[8] The reality is that any organization can face a cyberattack, and those that underestimate their risk often face a more difficult and costly recovery when an incident occurs.

SOPHOS

Types of penetration testing

As its name implies, a penetration test tries to break through or bypass defensive security controls and see what impact a threat actor could have if the tester were actually a cybercriminal.

There are a substantial number of "penetration testing" services on the market that do not necessarily push defenses hard enough, delivering a false sense of security and confidence. These offerings might be labeled a "penetration test," but often fall short of delivering the true depth and expertise required to provide a comprehensive assessment of how well defenses would stand up to a real attack.

Automated scanning

Many "penetration tests" are actually just rebranded automated scans. These are basic vulnerability scans with light or no exploitation of targets, and no involvement by security experts. Often, these activities may not be driven by real-world attacker techniques, do not chain together events, feature no real compromise of your environment, and do not meet compliance standards. In essence, the output is just a list of vulnerabilities, and not a true reflection of how a malicious actor would get into and move through your environment.

The takeaway: This is vulnerability scanning, not a true penetration test.

Penetration testing as a service (PTaaS)

These types of tests also rely heavily on automation but introduce some interaction by security experts. These services tout the power of their technology but may not include the context and expertise of an experienced security tester acting like an adversary. This light touch from a human tester does not probe deep enough to truly evaluate defenses. It often does not incorporate a customer's specific objectives for buying a penetration test in the first place. These solutions also tend not to factor in new information on emerging threats or work well for nuanced testing (such as testing of OT networks).

The takeaway: Delivers streamlined scanning with some flavor of human interaction but does not emulate real threat actor activity.

Breach and attack simulation tools

These activities emulate techniques used by threat actors, but in a scripted manner that does not mirror the flexibility of a human adversary trying to crack your defenses. These tools follow a sequence of activities — often based on security frameworks — but cannot pivot the way a real threat actor would, chain together vulnerabilities, or escalate privileges.

The takeaway: May be useful internally to assess potential issues, but lacks the creative, exploit-focused activity of a true penetration test.

Penetration Testing fundamentals

What makes a best-in-class penetration test that delivers the most valuable results?

Human expertise

Automated tools cannot replicate the creativity and application of contextual judgment that a human penetration tester provides. Expert security testers can chain subtle, seemingly unrelated vulnerabilities into high-impact attack paths, interpret business logic flaws, and improvise during a test, based on their observations and experience.

Incorporation of emerging threat trends

Penetration testing methods must reflect current, real-world adversary behaviors, such as state-sponsored threat group activity and multi-faceted attacks. By integrating threat intelligence research and findings based on the ever-changing global threat landscape, penetration testers can validate whether security controls can withstand modern attack methods.

Emulation of real adversary behaviors

Penetration testers mimicking what a threat actor would do in your environment is critical to deliver a realistic assessment of how well defenses can detect, resist, and respond to attacks. By mirroring real-world attacker techniques and behaviors, testers reveal gaps in defenses that generic or scripted testing approaches often miss.

Smart use of automation and tools

A penetration test should use automation and tools to help detect known or surface-level issues and quickly identify known vulnerabilities. Automation accelerates coverage and ensures nothing obvious is missed, quickly establishing a baseline of risk that testing experts then can probe further using their experience and insights into threat actor behavior.

Tailored testing aligned to customer goals and objectives

A penetration test should start with an exploratory conversation with the vendor to learn what is driving the test in the first place, the customer's objectives, and the outcomes the customer aims to achieve. This ensures testing focuses on the targets and risks that matter most based on the organization's industry and goals, instead of a one-size-fits-all approach.

Meets compliance requirements

Many major regulatory frameworks require or strongly suggest penetration testing to prove the effectiveness of your security controls. Beyond passing audits and avoiding compliance penalties, comprehensive penetration testing provides tangible proof of an organization's current security posture measured against real-world risk and threat actor techniques.

After the test, organizations should receive a comprehensive report containing, at a minimum: a summary for non-technical audiences, plenty of details for your technical staff, an account of all steps taken by the testers, what was found and the criticality of those issues, and recommendations to fix discovered weaknesses.

Any best-in-class penetration test should include retesting of the most critical issues. This gives an organization a defined time period to remediate any serious vulnerabilities, and the vendor an opportunity to validate that the remediation efforts were successful.

SOPHOS

Key considerations

Now that you have a clearer idea of what a best-in-class penetration testing service looks like, here are some questions to ask yourself before evaluating potential vendors.

1 Identify what you want to achieve

- Is your board of directors or leadership team asking for proof that your defenses are sound?
- Did you suffer a prior breach or security incident?
- Do you need to test the effectiveness of your existing security controls and technologies?
- Is there an upcoming regulatory audit or compliance deadline?
- Are you planning next year's security budget and need to build in testing?

2 Identify the depth of testing you need

- Are you content with just an automated scan of your environment for obvious gaps, or do you need a deeper test driven by human expertise?
- Do you require security experts to push your defenses to try and find weak spots, using tactics such as exploitation and privilege escalation?
- Are you satisfied with testing that follows a script, or does testing need to emulate the flexibility of an attacker traversing your environment?
- How much has your environment changed since your last penetration test?

Evaluating penetration testing services: Top questions to ask vendors

Once you have established your requirements, here are some suggested questions to ask a potential penetration testing vendor.

1. Is your testing mostly automated or relies mostly on tools?
2. Will your testers pursue exploitation or only validate scanner findings?
3. Do you chain vulnerabilities to show real attack paths?
4. What percentage of testing activities involve real exploitation that mimics adversary behavior?
5. Do you tailor testing to our industry and objectives?
6. How experienced are the testers performing the work?
7. Will we meet directly with your testers?
8. How does your testing meet PCI, SOC2, ISO, HIPAA, GLBA, NIST, and/or cyber insurance requirements?
9. What type of retesting is included?
10. What type of report will we receive after the test?

Sophos Penetration Testing

Sophos Penetration Testing — part of the Sophos Advisory Services portfolio — identifies vulnerabilities and validates security defenses with independent expertise, experience, and tailored strategies to enhance your security posture, reduce your risk, facilitate compliance, and improve your operational efficiency.

Sophos External Penetration Testing

Focuses on systems that are accessible from the internet: websites, VPNs, and public-facing services.

Discover answers to the following questions:

1. What can an attacker see and access from the internet, and are there unintentional exposures?
2. Are there vulnerabilities in our VPNs and remote access portals, email servers, or cloud environments?
3. Would our IT, security team, or managed security services provider detect a real-world intrusion attempt?
4. Are best practices like HTTPS enforcement, strong TLS configurations, and MFA enabled?

Example scenarios: Testing public-facing websites and services; identifying unpatched vulnerabilities.

Sophos Penetration Testing services

External Penetration Testing

Simulates how an attacker could find and exploit vulnerabilities to breach your network, enabling you to proactively strengthen your security posture and reduce overall attack surface.

Internal Penetration Testing

Mimics internal threat actors and unauthorized outside attackers by emulating attacks from users with legitimate access to the network or those gaining access via compromised accounts.

Wireless Network Penetration Testing

Attempts to compromise wireless networks and evaluates the overall security and compliance posture of an organization's wireless environment.

SOPHOS

Sophos Internal Penetration Testing

Focuses on systems, applications, and data within the internal network.

Discover answers to the following questions:

1. What could an attacker do if they gained access to our internal network?
2. Are there misconfigured systems or services that expose us to risk?
3. Are our security tools generating high-fidelity alerts, and are our security and IT teams able to respond quickly?
4. How well can we detect and respond to insider threats or an attacker moving laterally through our network?

Example scenarios: Testing how easy it would be for an insider threat to escalate privileges and exfiltrate data.

Sophos Wireless Network Penetration Testing

Focuses on Wi-Fi infrastructure, encryption protocols, authentication, and access controls.

Discover answers to the following questions:

1. Are unauthorized users able to access our wireless networks?
2. Are we using strong encryption and secure authentication methods?
3. Are there rogue devices connected to our network?
4. Can an attacker bypass our wireless protections?
5. What steps can we take to enhance wireless security?

Example scenarios: Testing office Wi-Fi security; identifying rogue access points; attempting unauthorized connections.

The Sophos Red Team

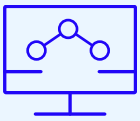
The Sophos Red Team is comprised of expert testers using advanced tools, real-world tactics, current threat intelligence from Sophos X-Ops, and findings from other testing and incident response engagements to simulate the way an adversary would attempt to breach your environment.

- Solely focused on delivering testing and assessment engagements.
- Informed by the latest global threat intelligence and findings from threat hunting and incident response engagements.
- Backed by hundreds of security analysts and threat intelligence team members from Sophos X-Ops.
- Numerous accolades, including multiple victories at DEFCON Wireless Capture the Flag.
- Diverse backgrounds that give us a unique perspective that's not just security vendor-focused.

Comprehensive reporting you can use to inform and improve

When the engagement concludes, you do not receive a simple pass/fail rating. Sophos Penetration Testing includes a detailed report segmented for different audiences in your organization, with a detailed narrative of every action we took in the engagement, what findings we discovered, and actionable recommendations you can take to elevate your security posture.

What's included in your report

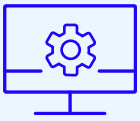


Executive summary

Intended for non-technical stakeholders — senior management, auditors, board of directors, and other important parties.

Detailed findings

Written for technical staff to provide in-depth findings and recommendations.

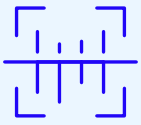


Engagement methodology

Defines the scope of the engagement and what testing activities were performed.

Narrative

Describes the sequence of actions taken by the testers to achieve the goals of the engagement, to assist in understanding blended threats and/or dependent phases.



Recommendations

Details findings, web page links for further reading, and recommendations for remediation or risk reduction. Testers supply evidence of their findings where applicable and, if possible, sufficient information to replicate the findings.

Why Sophos Penetration Testing is superior

Real-world testing by security experts

The Sophos Red Team brings extensive penetration testing experience and a wide range of industry recognized certifications. The Sophos Red Team is backed by hundreds of security analysts and threat intelligence experts, ensuring testing reflects the current threat landscape and emerging threat activity.

Goal-based methodology

Sophos follows a goal-based methodology tailored to you and where you are in your security journey. We meet with you before testing begins to understand your challenges and objectives and use our years of experience to deliver testing and assessment services to organizations of all sizes, across all industries, to ensure your goals are met.

The benefit of human expertise

Automation and tools are useful in effective penetration testing but must be reinforced by human expertise. Tools can inform decision-making, but real exploitation must be performed by experienced testers who know what threat actors are doing and can emulate those activities. Tests focused exclusively on automated scanning and exporting vulnerabilities do not reflect real adversary activity; the Sophos Red Team does.

Detailed reporting, not a checkbox

When testing concludes, we provide you with a detailed report for technical and non-technical audiences. This report reflects your goals and objectives and is not a check-the-box, pass/fail document. Reports include all steps taken during the engagement, our findings, the real potential impact to your organization if you were to be compromised, and actionable recommendations you can use to strengthen your organization's security posture.

Engaging you throughout the process

Testing that relies solely on automated scanning fails to provide direct interaction with security experts, technical deep dives that deliver true understanding of results, and executive briefings tailored for non-technical audiences. You get all of that with Sophos.

Validating your remediation work

Many penetration testing vendors step away as soon as the engagement concludes, leaving you to figure out the next steps on your own. Sophos External Penetration Testing and Internal Penetration Testing include remediation validation for critical and high findings. Fix identified issues within 90 days after the test, and we will retest those areas at no additional cost.

Delivering high value for your purchase

"Penetration testing" services that lack a human-led, intelligence-informed approach and rely heavily on tools or automated scanning may have a lower price point. These solutions might check a box that you have conducted a "penetration test," but do not fundamentally achieve the real goal of emulating what a threat actor would do in your environment and delivering actionable recommendations to help you stop an attack before it happens.

Why choose Sophos for penetration testing

Assess your risk of being breached.	Discover your real-world risk of being impacted by an incident.
Get an independent and proactive assessment of your security controls to find weak spots.	Uncover vulnerabilities in defenses to fortify your security resiliency before a threat actor strikes.
Expert security guidance on how to better secure your environment.	Receive actionable recommendations from a dedicated team of testers with proven results from thousands of engagements.
Testing that incorporates the latest intelligence into current and emerging threats.	Gain insights informed by real-world threat research, threat hunting, and incident response engagements.
Demonstrate strong security to stakeholders and partners.	Show customers, channel partners, business stakeholders, and your cyber insurance provider that security is a priority for your organization.

Testing and assessment skills you can trust

World-class security experts possessing years of experience testing and assessing organizations of all sizes, in all industries.

Three consecutive wins, DEFCON Wireless Capture the Flag (our testers now help host the competition).

Two consecutive wins at DEFCON Biohacking Capture the Flag competition.

Six consecutive wins at GrrCON Car Hacking Capture the Flag.

Illustrating the wide range of expertise Sophos Red Team members possess.

Leading accreditation body for cyber security service providers.

Accredited for security testing, validating an organization's technical capabilities, processes, and governance.

Summary

Sophos Advisory Services evaluates an organization's controls and policies as an adversary would through a variety of proactive technical testing and assessment services.

These services provide expert, independent guidance that supports a proactive and strategic approach to cybersecurity, helping to identify vulnerabilities in a customer's environment, strengthen defenses, and enhance resilience.

Penetration testing is an important element of a proactive security strategy. Working with a vendor like Sophos that delivers comprehensive penetration testing provides you with the assurance that we have put your security controls to the test and identified weak spots that can be addressed to keep you ahead of threat actors.

Footnotes

1 - Fortune Business Insights, Penetration Testing Market, 2025
2 - Penetration Testing Statistics, 2024 – Cybersecurity Ventures
3 - The Sophos Annual Threat Report: Cybercrime on Main Street 2025 – Sophos
4 - The State of Ransomware 2025 - Sophos
5 - The 2025 Sophos Active Adversary Report - Sophos
6 - The State of Ransomware 2025 - Sophos
7 - Addressing the Cybersecurity Skills Shortage in SMB – Sophos
8 - The 2025 Sophos Active Adversary Report – Sophos

SOPHOS

For more information about Sophos Penetration Testing, speak with your Sophos Partner or visit www.sophos.com/advisoryservices

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com