Solution Brochure

SOPHOS

SOPHOS ADVISORY SERVICES

Penetration Testing

Validate security defenses through real-world, simulated attack methods

Identify vulnerabilities and validate security defenses with independent expertise, experience, and tailored strategies to enhance your security posture, reduce your risk, facilitate compliance, and improve your operational efficiency.

Proactively strengthen defenses and security posture

Unauthorized access to company resources, exploiting existing and new vulnerabilities, leveraging misconfigurations, and taking advantage of poor security policies are serious security concerns. Verifying that applications, networks, and systems are not vulnerable to a security risk is key to addressing these vulnerabilities before they can be used by attackers. While vulnerability scans and assessments are a "light touch" evaluation to identify gaps and vulnerabilities in your network, deeper testing and validation are required to show how an attacker would gain access to your environment and use those systems as a base for attacks deeper into the network.

Sophos Penetration Testing services

Penetration Tests, or "Pentests," identify and demonstrate cybersecurity vulnerabilities, answering the question: "Could an attacker break into my network?" They work by simulating real-world cyberattacks to identify vulnerabilities in systems, networks, and applications. Experienced testers (ethical hackers) attempt to exploit weaknesses to demonstrate what an attacker could achieve.

There are two primary types of Penetration Testing:

- **External Penetration Testing:** Focuses on systems that are accessible from the internet, such as websites, VPNs, and public-facing services. It simulates an attacker trying to breach your perimeter from the outside.
- **Internal Penetration Testing:** Simulates an insider threat or an attacker who has already breached the perimeter, focusing on systems, applications, and data within the internal network.

Sophos approaches every Penetration Test as unique to each organization. Our goal-based methodology is performed by the industry's top security testers, leveraging our proprietary tactics and intelligence from the Sophos X-Ops threat intelligence group, which includes the Counter Threat Unit (CTU), renowned for its intelligence and research into advanced persistent threats (APT) and state-sponsored attackers.

Benefits

- Gain assurance by testing internal and external security controls, including protections around high-value systems and resources.
- Satisfy specific testing goals through a threat model and context that match your unique environment.
- Receive actionable course of action for remediation.
- Support regulatory compliance, including PCI DSS, HIPAA, GDPR, NIS, ISO 27001, SOC 2.
- Insights derived from the latest intelligence from the Sophos X-Ops threat intelligence group.
- Determine your real-world risk of compromise.

Simulate advanced attacks to test your defenses

Organizations conduct regular Penetration Tests not just to comply with industry regulations, but to proactively manage the increasingly complex and evolving cybersecurity threat landscape. By performing Penetration Tests at regular intervals, organizations can stay ahead of attackers who continually adapt their techniques to exploit new vulnerabilities. Regular testing also helps identify weaknesses introduced through changes in infrastructure, applications, or third-party integrations. Moreover, Penetration Testing provides organizations with a realistic understanding of their risk exposure, actionable remediation strategies, and a measurable way to track security improvements over time.

Benefits of Penetration Testing include:

- **Proactive risk reduction:** Organizations that conduct regular Penetration Tests experience 50% fewer security incidents and a 30% reduction in the overall cost of managing security incidents.[1]
- **Compliance support:** Regulatory frameworks like PCI DSS, HIPAA, and ISO 27001 often require penetration testing. In fact, 73% of organizations cite compliance as a driver for Penetration Testing.[2]
- **Cost savings:** The average cost of a data breach is $4.45 million,[3] but many vulnerabilities can be addressed for a fraction of that cost through Penetration Tests.
- **Customer confidence:** 65% of consumers say they are more likely to trust a company that demonstrates strong cybersecurity practices.[4]

Testing your people

Artificial intelligence has dramatically raised the stakes in phishing attacks, creating highly sophisticated and convincing messages that are increasingly difficult to detect. Unlike traditional phishing emails riddled with grammatical errors and generic content, AI-driven phishing can generate personalized, contextually relevant messages tailored to specific individuals or organizations. As a result, security teams and users alike face new challenges in identifying and defending against phishing attacks, emphasizing the need for continuous training.

Our Penetration Testing program can be combined with simulated phishing attacks to gauge your employees' ability to spot and respond to phishing attempts.

Service features

- Tailored Rules of Engagement, including review of target systems for business-critical data.
- Final reports containing detailed findings and executive summary.
- On-premise and remote testing options.
- Option to select External Penetration Testing, Internal Penetration Testing, and Phishing Attack Simulation Training to create a blended threat scenario for your specific use case.
- Tester-driven, manual process that includes tactics used by threat actors.
- Goal-based methodology that ensures systems are tested in the greater context of their environment.

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 of 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 using publicly available tools.

Phishing results (if applicable): Details the phishing attacks used and their success rate.

Other cybersecurity testing services

No individual, stand-alone assessment or technique provides a comprehensive picture of an organization's security posture. Each adversarial test has its own objectives and acceptable levels of risk. Sophos can work with you to determine what combination of assessments and techniques you should use to evaluate your security posture and controls to identify your vulnerabilities.

Learn more:
sophos.com/advisory-services

[1]Ponemon Institute [2]SANS Institute [3]IBM [4]PwC

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

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

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

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

© Copyright 2025. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2025-06-05 BREN (MP)

SOPHOS