Solution Brochure

SOPHOS

SOPHOS ADVISORY SERVICES

Wireless Network Penetration Testing

Identify exposures in your wireless network and how attackers may exploit them

Wireless networks allow employees and guests to move throughout a physical location and remain connected. However, wireless technologies also introduce risks to your organization. Misconfigured infrastructure, rogue access points, and wireless clients can introduce unforeseen security risks. Wireless network penetration tests proactively evaluate your organization's Wi-Fi infrastructure and identify how adversaries could use vulnerabilities to breach your network.

Strengthen your wireless network security posture

MAC filtering, WEP encryption, and pre-shared keys are no longer effective defenses to protect the information and clients using your wireless network. Attackers can bypass or break most of these measures within minutes, exposing your internal infrastructure.

Proactive testing to identify devices accessing your network and evaluate the security of your Wi-Fi infrastructure is essential to identify how an attacker could breach your environment before exposures can be exploited.

Sophos Wireless Network Penetration Testing service

The Sophos Wireless Network Penetration Testing service evaluates your wireless networks' security and compliance with appropriate mandates through configuration reviews, technical testing, and scanning for rogue access points. Sophos' highly skilled security testers attempt to exploit weaknesses in encryption, authentication, and access controls, using both "passive" and "active" approaches:

- **Passive assessment:** Involves monitoring wireless traffic to identify unauthorized devices, rogue access points, and misconfigurations without actively attempting to connect.
- **Active assessment:** Simulates an attacker attempting to exploit vulnerabilities in the wireless network by cracking encryption, bypassing authentication, and gaining unauthorized access.

Benefits

- Gain assurance that sensitive data transmitted over your wireless networks is protected from unauthorized access and interception.
- Find out how your wireless connections expose internal networks.
- Identify ways an attacker could breach your wireless network.
- Ensure secure network access by only authorized users.
- Receive actionable guidance for remediation.
- Goes beyond a compliance assessment.

Why test your wireless network?

By performing proactive testing at regular intervals, you can reduce the threat from attackers who continually adapt their techniques, exploiting new vulnerabilities to access sensitive data transmitted over your wireless networks. Regular testing also helps identify weaknesses introduced through changes in your organization's Wi-Fi infrastructure and provides a realistic understanding of your risk exposure.

- Identifies rogue wireless access points and misconfigurations.
- Ensures wireless security policies meet best practices.
- Reduces the risk of data breaches from Wi-Fi vulnerabilities.
- Evaluates both passive exposure and active exploitation risks.
- Understand how your devices respond to a malicious rogue access point.

What's included in your report

Executive summary: A summary of the assessment, key findings, and high-level recommendations.

Testing methodology: Details of the scope of the engagement and what testing activities were performed.

Narrative: Describes the detailed sequence of actions the testers took to achieve the assessment goals.

Findings and recommendations: Details of the key findings identified during the assessment are provided by severity level with a remediation plan and additional information for reference, where applicable.

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 distinct 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.

Service features

- Passive monitoring of your wireless network to determine weaknesses in security architecture, encryption key vulnerabilities, configuration flaws, and defensive measures.
- Highly skilled testers attempt to gain access by breaking encryption keys and impersonating access points to steal user credentials.
- Comprehensive reports provide detailed findings and recommendations from the assessment.
- Rules of engagement are established upfront during introductory sessions for your peace-of-mind.
- Choose the scope of service to meet your needs, to cover one or multiple physical locations.
- Remote testing — delivering the same quality as an on-site test — provides scheduling flexibility and enables testing in locations normally inaccessible due to safety or restricted access.
- Optional on-site testing available — ideal for large or dispersed locations.

Learn more:
sophos.com/advisory-services

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