Solution Brochure

SOPHOS

Sophos Advisory Services

Proactive risk reduction and resilience in the face of evolving cyber threats

Tailored, expert-led security assessments

With the ongoing demands of digital transformation, the rise of AI, and ever-evolving cyber threats, forward-thinking organizations recognize that cybersecurity is not just a technical challenge—it's a strategic priority. Advanced adversaries, regulatory scrutiny, and stakeholder expectations demand a proactive and comprehensive approach to securing digital assets. Sophos Advisory Services deliver the independent expertise, experience, and tailored strategies to identify systemic vulnerabilities, fortify defenses, and enhance business resilience.

Using real-world tactics, techniques, and procedures (TTPs) used by threat actors, our highly certified security experts will test your networks, systems, and employees to help your organization:

- Identify vulnerabilities before attackers can exploit them.
- Strengthen defenses against sophisticated threats.
- Meet regulatory compliance requirements.
- Evaluate incident response readiness.
- Build trust with customers, partners, and stakeholders.

Proactively strengthen defenses and security posture

Penetration Testing (Pentesting)

Penetration testing simulates 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.

Why it's valuable:

- Identifies hidden vulnerabilities that routine scans may miss.
- Provides actionable recommendations to strengthen defenses.
- Supports regulatory compliance (e.g., PCI DSS, HIPAA, GDPR, NIS, ISO 27001, SOC 2).
- Demonstrates commitment to proactive risk management.
- Provides comprehensive coverage of both perimeter and internal security risks.

Key questions it helps answer:

- Where are the most critical vulnerabilities in our infrastructure?
- How easily could an attacker breach our defenses externally?
- What risks exist inside our network if an attacker gains access?
- What is the potential impact of a successful attack?
- What steps can we take to fix identified weaknesses?

Wireless Network Penetration Testing

Wireless Network Penetration Testing assesses the security of an organization's Wi-Fi networks and infrastructure and evaluates their compliance with appropriate mandates. Testers attempt to exploit weaknesses in encryption, authentication, and access controls.

There are two scopes of Wireless Network Penetration Testing. 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.

Why it's valuable:

- Protects sensitive data transmitted over wireless networks.
- Identifies rogue access points and misconfigurations.
- Ensures wireless security policies meet best practices.
- Reduces risk of data breaches from Wi-Fi vulnerabilities.
- Evaluates both passive exposure and active exploitation risks.

Key questions it helps answer:

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

Web Application Security Assessments

Web applications often handle critical business and customer data, making them prime targets for attackers. Web Application Security Assessments provide assurance that your web applications are secure by focusing on common vulnerabilities, including SQL injection, cross-site scripting (XSS), and broken authentication.

These assessments can involve Black-box Testing, where the tester simulates an external attacker with no prior knowledge of the application's inner workings or White-box Testing, where the tester has full access to source code and architecture, enabling a deeper analysis of potential vulnerabilities.

Why it's valuable:

- Protects customer and company data handled by web applications.
- Identifies coding and configuration flaws that increase risk.
- Supports compliance with standards like OWASP Top 10 and PCI DSS.
- Reduces the risk of website defacement, data breaches, and reputational damage.
- Provides both an outsider's perspective and an in-depth analysis of application security.

Key questions it helps answer:

- Are our web applications vulnerable to common attack methods?
- Is sensitive data exposed due to coding flaws or misconfigurations?
- Can an external attacker exploit vulnerabilities, or do deeper issues exist in the code?
- How can we secure user authentication and session management?
- What remediation steps are needed to fix web application vulnerabilities?

Security assessment services summary

Assessment type	Focus	Key questions answered	Example scenarios
Penetration Testing (Pentesting)	Infrastructure, systems, and networks	Where are the vulnerabilities? How can an attacker breach our defenses?	External: Testing public-facing websites and services; Internal: Testing internal access controls and privilege escalation
Wireless Network Penetration Testing	Wi-Fi security, encryption, access controls	Is our Wi-Fi secure? Are there unauthorized or rogue devices?	Testing office Wi-Fi security; Identifying rogue access points; Attempting unauthorized connections
Web Application Security Assessment	Web applications, coding flaws, authentication	Are our apps secure? Is sensitive data exposed? How can we fix vulnerabilities?	Testing customer portals, e-commerce sites, internal web apps; Identifying SQL injection, XSS, or authentication flaws

Other cybersecurity testing services

No individual, stand-alone assessment or technique provides a comprehensive picture of an organization's security. 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

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