SECURITY TESTING AND ASSESSMENT SERVICES

Find your weaknesses before attackers do.

62%

of organizations hit by ransomware cite a known or unknown security gap as a reason they were exposed.[1]

31%

of breaches start with an exploited vulnerability, now the top way attackers get in.[2]

$4.99M

global average cost of a data breach (USD), a record high and up 12% in 2026.[3]

Sophos testing experts find the weak spots threat actors could exploit across your applications, identities, networks, and people. Our assessments and adversary exercises show how your defenses hold up and where to focus.

KEY BENEFITS



Know where you're exposed

See the vulnerabilities, misconfigurations, and attack paths across your applications, identities, networks, and cloud before an adversary does.



Prove your defenses work

Find out how your security controls and team hold up against realistic attack techniques, not just how they look on paper.



Fix what matters most

Get prioritized findings and expert guidance you can act on, plus evidence to share with leadership, auditors, and insurers.

1. Sophos, The State of Ransomware 2026.
2. Verizon, 2026 Data Breach Investigations Report.
3. IBM and Ponemon Institute, Cost of a Data Breach Report 2026.

THE CHALLENGE

Your defenses look strong on paper. Put them to the test.

Every new AI tool, application, cloud workload, identity, and connected device can open a gap. Over time, small weaknesses add up, and threat actors are skilled at chaining them together into a path to your most valuable data and systems.

Leadership, auditors, regulators, cyber insurers, and customers increasingly demand evidence that your security works. Policies and tool dashboards alone rarely answer the questions that matter most:

- **Where are we exposed, and what would an adversary target first?**
- **Would our controls and our team detect and respond to a determined attacker?**
- **What should we prioritize to lower our risk?**

The most reliable way to answer these questions is to test your defenses before a real adversary does.

THE SOLUTION

Assess your defenses the way attackers would

Sophos' extensive range of security testing and assessment services gives you clear answers. Our specialists deliver targeted assessments, penetration testing, and realistic adversary exercises to show where you're vulnerable, how your defenses perform, and what to do next.

Find weaknesses.

Assessments and penetration tests uncover vulnerabilities, misconfigurations, and attack paths across the areas that matter most to your business.

Validate defenses.

Red and Purple Team exercises show how your controls and team respond when challenged by realistic threat actor techniques.

Prioritize action.

Every engagement delivers findings and expert guidance so your team can focus remediation where it reduces the most risk.

Engagements can focus on a single application or attack surface, or simulate broader adversary activity to show how attackers could chain individual gaps into an attack path.

THE PORTFOLIO

Choose the testing that fits your priorities

Our range of security testing and assessment services is organized into six service areas:



Application security

Are the applications and APIs we build and rely on secure?

Assess web, mobile, and custom applications, web APIs, and source code to uncover weaknesses before they become an entry point.



Assessment services

How secure are our identity systems and AI deployments, and are attackers already inside?

Take a deeper look at Active Directory, Microsoft Entra ID, and AI/LLM systems, and hunt for signs of compromise through threat hunting and compromise assessments.



Network penetration testing

What could an attacker exploit in our networks, cloud, and wireless environments?

Test external, internal, cloud, and wireless environments from an attacker's perspective to expose exploitable vulnerabilities and attack paths.



Red and Purple Team exercises

Would our controls and team detect and respond to a real adversary?

Red Team exercises simulate realistic attacks against your organization. Purple Team exercises bring offensive and defensive experts together to strengthen detection and response.



Social engineering and physical security

Could an attacker get in through our people or our buildings?

Phishing drills and physical security testing show whether attackers could trick employees or bypass physical safeguards.



Custom scoped engagement and project management

What about needs that don't fit a standard engagement?

Get specialized testing scoped to your environment, such as medical devices, operational technology, or SAP, with project management available for tailored work.

Explore the full range in the Services Catalog →

PROVEN EXPERTISE

Why Sophos for security testing and assessment?

Testing is only as valuable as the expertise behind it. Sophos brings together offensive and defensive specialists who understand how real attacks unfold.

01

Globally accredited experts

The team delivering these services holds global accreditations, including CIR Standard and Enhanced (UK), BSI (Germany), and SSS (Japan).

02

A real-world attacker's perspective

Our Red and Purple Team expertise helps you understand how a capable adversary could pursue an objective in your environment, revealing weaknesses and attack paths that isolated technical checks may miss.

03

Informed by threat research and incident response

Our testing is shaped by Sophos threat research and frontline incident response experience.

See the Sophos Red Team in action

Watch how realistic testing **uncovers serious weaknesses in complex environments →**

SERVICE FEATURES

Human-led testing, not just automated scans

Automated scans find known vulnerabilities. They don't show how an attacker would chain those weaknesses together to reach your critical systems. Sophos testers do.

Goals agreed to up front

Before testing starts, we agree on your goals and objectives so each test looks at your systems in the context of your wider environment.

Clear reporting for technical and business readers

Reports cover every step taken, what we discovered, the real potential impact on your organization, and recommendations you can act on. They're built around your objectives, not a simple pass/fail.

Direct access to the experts

Work directly with the testers throughout the engagement, with technical deep dives and executive briefings for non-technical stakeholders.

Informed by threat intelligence

Testing draws on Sophos X-Ops research and insights from thousands of testing engagements. Testers come from law enforcement, military, and threat intelligence backgrounds.

HOW TO BUY

Flexible access through the Sophos Security Services Retainer

Security testing and assessment services are available through the Sophos Security Services Retainer. Simply purchase Service Units up front, then use them for the testing, assessment, and readiness services you need, when you need them. As your priorities change, your plan can change with them.

Explore the full Security Services Retainer Catalog →

Find your weaknesses before attackers do.

Talk to a Sophos expert or your Sophos partner to choose the right testing for your environment and goals.

sophos.com/security-testing →



















© Copyright 2026. 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.

2026-11-10 BR (TA)

SOPHOS