

ATTACK SURFACE TESTING

Proven Exposures, Not Noise.

Threat actors probe your perimeter constantly, and a point-in-time penetration test shows only where you stood on the day of the test.

Automated tools fill the gap with long lists of findings, but they miss the attacks that matter most, such as an attacker chaining several small weaknesses into one serious breach or working out an exploit with no ready-made playbook. Your team is left sorting noise from real risk.

Attack Surface Testing closes that gap. Our fully managed service pairs automation with Bishop Fox experts who continuously test your external attack surface the way real attackers would, chain weaknesses, and prove which are real, so your team acts on confirmed risk, not a long list of possibilities.

HOW IT WORKS

You get accurate, noise-free security intelligence, with all false positives removed before you ever see them.

01 Exposure Identification

Automation covers ground. Experts go deeper. Automated testing sweeps your external attack surface, then our experts investigate each exposure and prove whether these weaknesses are real attacker entry points.

02 Eliminate Noise and False Positives

Automated and manual checks remove duplicates and false positives, and every lead is triaged and prioritized before hands-on validation.

03 Validate Exploitability

Our Adversarial Operations Team confirms exploitability by emulating real-world attack scenarios, chaining separate weaknesses into attack paths and pursuing exploits with no ready-made playbook. Proven exposures are taken far enough to show business impact, safely and within your rules of engagement.

04 Prioritize Remediation and Support

You receive validated vulnerabilities with actionable guidance, detailed evidence of exploitation, and direct access to our testers. On-demand retesting confirms the fix worked and removes doubt about whether an issue is resolved.

05 Reporting and Compliance

Findings and remediation progress arrive in real time through the Bishop Fox Portal, with compliance-ready reports and historical trends to help prove risk reduction.

WHAT YOU GET

✓ WITH EVERY FINDING

- Detailed technical findings
- Evidence of exploitation, from entry point to impact, proven by a Bishop Fox expert
- A severity rating based on business impact, not theoretical scoring
- Actionable remediation guidance

✓ ACROSS THE SERVICE

- Findings published in real time to the Bishop Fox Portal
- Direct access to the Adversarial Operations Team for clarification and guidance
- On-demand retesting to confirm fixes
- Compliance-ready reports and audit documentation
- Historical trends

KEY BENEFITS



FIND THE EXPOSURES ATTACKERS TARGET

Operators exploit known-exploited vulnerabilities, risky services, and web and API weaknesses, using automation to cover ground and people to prove and extend. AI-specific vulnerability checks run against the model servers, large language model (LLM) endpoints, and Model Context Protocol (MCP) services found in your inventory.



DEPTH A SCANNER CANNOT REACH

Operators chain separate weaknesses into one real attack path a machine would never link together, and investigate novel exploits with no ready-made playbook.



A RESULT YOU CAN DEFEND

A Bishop Fox expert proves the finding, provides the evidence behind it, and explains what it means for your business. When you need to show a board, auditor, or major customer that a risk was real and is now closed, you have human-backed proof.



CONFIRM FIXES WITH CONFIDENCE

An operator retests what you fixed and confirms it is closed, so closure is verified, not assumed.

IMPACT, NOT JUST EXPLOITABILITY

Once an exploit is verified, our experts take it far enough to show what an attacker could actually accomplish, safely and within your rules of engagement.



FINDINGS LAND WHERE FIXES HAPPEN

Validated findings open in the tools your teams already use, like Jira and ServiceNow, and status flows back to the Bishop Fox Portal, so security and engineering see the same information.

PART OF CONTINUOUS SECURITY TESTING

Attack Surface Testing works alongside the rest of our Continuous Security Testing offerings. Pair it with Attack Surface Discovery so our experts always test your live, validated inventory, and with Emerging Threat Testing for fast answers when a new vulnerability makes headlines.

ABOUT BISHOP FOX

Bishop Fox is the leading authority in offensive security, providing solutions that help organizations secure their most critical assets against sophisticated cyber threats. Since 2005, we've partnered with Fortune 100 enterprises and high-growth innovators to deliver high-impact security testing and advisory services. Our comprehensive service offerings include tech-enabled, human-driven Continuous Security Testing, red teaming, and penetration testing for applications, cloud, networks, IoT, and AI/LLM.

REQUEST A DEMO AT [BISHOPFOX.COM](https://bishopfox.com)