BISHOPFOX

SOLUTION BRIEF

CONTINUOUS SECURITY TESTING

Testing that never stops. Proof that never wavers.

> Your attackers do not wait for your next scheduled test, and neither should your security program. Continuous Security Testing (CST) gives you an always-on, validated view of your attack surface, the exploitable vulnerabilities to remediate fast, and the latest threats that matter to your environment, with Bishop Fox experts standing behind every result.

CONTINUOUS SECURITY TESTING CLOSES THE GAP BETWEEN TESTS AND THREATS

Attackers move fast, and Bishop Fox keeps you a step ahead. CST gives you an up-to-date view of your attack surface, identifies and proves exploitable exposures, and tells you whether a new threat puts you at risk, all backed by our offensive security experts.

[>] **Validated, not just detected.** From asset ownership to vulnerability exploitation, to emerging threat validation, every asset, exploitable finding, and threat determination is confirmed by a Bishop Fox expert and prioritized for you, so your team spends its time and resources only on what is real.

[>] **Always on.** Coverage runs continuously, so new assets, new exposures, and new threats surface as they appear rather than at your next scheduled test.

[>] **A managed service, not another dashboard to run.** Bishop Fox does the work of investigating, prioritizing, and confirming results, and stands behind it, so continuous testing never becomes another program your team has to staff.

[>] **One portal, and the people behind it.** Every result lands in the Bishop Fox Portal with real-time visibility, and the experts who did the work are reachable for context and questions.

[>] **Flexible by Design.** Our services are designed to work seamlessly together and on their own, so you can build the program that fits your priorities.

THREE OFFERINGS, ONE PROGRAM

ASD

ATTACK SURFACE DISCOVERY

What am I exposing, is it really mine, what are the easy ways in?

- Validated, continuously updated inventory, including MCP services and connected cloud accounts
- Evidence-based confidence rating on every asset
- Hygiene issues attackers look for first

AST

ATTACK SURFACE TESTING

What exposures can an attacker actually exploit?

- Expert-proven findings with evidence
- Proven attack path and severity based on business impact
- On-demand retesting to confirm fixes

ETT

EMERGING THREAT TESTING

Does this new threat affect me, am I in the clear?"

- Clear answer on whether new threats affect your environment
- Confirmation that the exposure is closed after you patch

DELIVERED AS A MANAGED SERVICE, MODULAR BY DESIGN TO ADAPT AS YOUR NEEDS CHANGE.

WORK TOGETHER OR STAND ALONE

Start with any one offering and expand from there. Offerings can be added at any time, so your program grows as your needs do. Attack Surface Discovery strengthens the other two services by keeping the inventory they work from validated and current. Here is how each one builds on the others:

- **Start with Discovery:** you get a validated inventory. Add Attack Surface Testing and our experts test that live inventory as it changes. Add Emerging Threat Testing and new threats are checked against the assets you actually have, including newly discovered ones.
- **Start with Attack Surface Testing:** you get proof of what is exploitable. Add Discovery and our experts test your current footprint, not a static list. Add Emerging Threat Testing and a new threat is checked against the same environment our experts are already testing.
- **Start with Emerging Threat Testing:** you get a clear answer on new threats. Add Discovery for a continuously validated inventory to test against. Add Attack Surface Testing and experts are already testing the environment when a threat lands.

None is a prerequisite: bring your own asset list and we will work from it.

WHAT EACH SERVICE PROVIDES

CAPABILITY	ASD	AST	ETT
Continuous discovery of internet-facing assets	✓		
Ownership validation with an evidence-based confidence rating	✓		
Hygiene findings (certificate and TLS, DNS, email, exposed services)	✓	✓	
Proof of exploitability, captured as evidence		✓	✓
Emerging threat notification			✓
Impact determination on newly disclosed vulnerabilities			✓
Expert retesting to confirm your fixes worked		✓	✓
Bishop Fox Portal access	✓	✓	✓

CLARITY WITHOUT THE COMPLEXITY

Every CST offering is delivered through the Bishop Fox Portal, so results, activity, and history live in one place instead of scattered across tools and reports.

- One validated view. Everything lands in one portal, segmented and access-controlled by user and team, so you see your attack surface and testing activity together.
- Always on. The portal stays live between engagements, not just when a report arrives at the end of an annual test.
- Works with your tools. Findings flow to Jira and ServiceNow, data pulls through the public API, and a read-only AI assistant answers questions about results so the program, so CST works seamlessly with the tools your team already uses.

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.

LEARN MORE AT BISHOPFOX.COM
FOLLOW US ON 𝕏

©BISHOPFOX. ALL RIGHTS RESERVED.

BISHOPFOX