BISHOPFOX

DATA SHEET

AI-POWERED APPLICATION PENETRATION TESTING

Trusted Results. Scalable Coverage. Faster Insight.

Most enterprises are securing dozens, sometimes hundreds, of applications with the same constrained budgets and headcount. DAST tools flood teams with noise, manual testing covers only a slice of the portfolio, and fully autonomous tools struggle where complexity begins. Bishop Fox AI-Powered Application Penetration Testing closes that gap. It's a managed service that combines 20 years of offensive security expertise with our Cosmos AI platform to deliver findings across your application portfolio, with service tiers that range from baseline assessments to deep expert-led engagements.

THE BISHOP FOX APPROACH

WHY AI-POWERED

- **Greater coverage at scale:** Test entire application portfolios by exploring more attack paths and surfaces within a fixed timeframe.
- **Attacker-realistic testing:** Focus on realistic attack behavior and chaining rather than isolated, low-value scanner findings.
- **Faster time to insight:** Get findings delivered to your portal as they're validated so you can take action quickly.

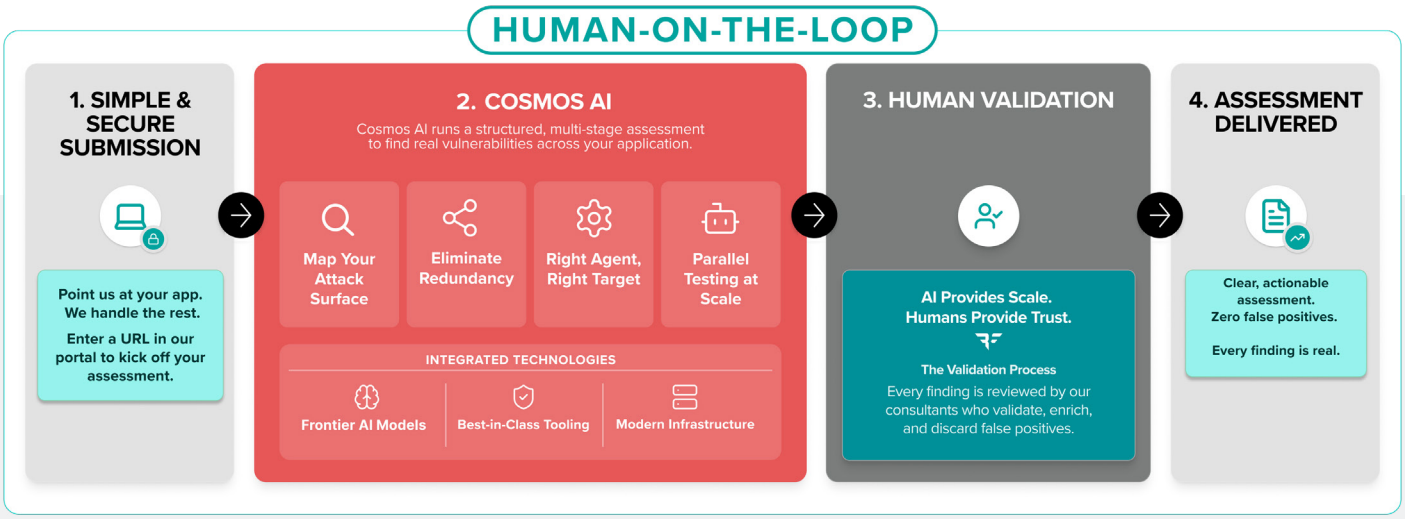
WHY EXPERT VALIDATION

- **Only real, exploitable findings:** A Bishop Fox tester confirms every vulnerability before it reaches you. No false positives.
- **Attacker context & business relevance:** Findings come with the tradecraft and context your team needs to prioritize and act, not just a severity score.
- **Defensible results**: Findings your engineers can remediate, your executives can report on, and your auditors can rely on.

WHAT TO EXPECT

FROM KICKOFF TO FINDINGS

Testing begins through the Bishop Fox portal. Point us at your application, provide credentials, and our team takes it from there. Cosmos AI drives discovery and scale; Bishop Fox testers validate every finding and confirm real-world exploitability. Results arrive as they're confirmed, with Baseline engagements completing within 5 business days. Integrations with vulnerability management and ticketing platforms like ServiceNow and Jira accelerate the time to remediation.



WEB APPLICATION PENETRATION TESTING PACKAGES

From rapid AI-powered exposure assessment to expert-led penetration testing — choose the tier that matches your portfolio, timeline, and depth requirements.

BASELINE

Optimized for coverage, efficiency and scale.

Includes:

- AI-powered application discovery, vulnerability identification, and testing
- One day of human vulnerability validation and exploitation
- Expert findings provided in days
- Slack-chat access to Bishop Fox experts
- Streamlined, portal-based experience with 12-month access to Bishop Fox portal for:
  - Test initiation
  - Progressive findings delivery with final results and prescriptive remediation guidance in ≈ 5 days
  - Statement of engagement letter
- PDF findings report

STANDARD

Balanced coverage and depth for most common business applications.

Includes:

- AI-accelerated application discovery and vulnerability identification
- Human-driven penetration testing, vulnerability exploitation, and attack chaining
- One week of testing focuses on OWASP Top 10 and common business logic vulnerabilities
- Slack-chat access to Bishop Fox experts
- White glove project management including kick off call and formal status updates
- 12-month access to Bishop Fox portal for:
  - Test initiation
  - Progressive findings delivery with prescriptive remediation guidance
  - Statement of engagement letter
  - Remediation testing
- PDF findings report with report readouts upon request

ADVANCED

Deeper testing of critical applications, specific features, and risk areas.

Includes:

- AI-accelerated application discovery and vulnerability identification
- Human-driven penetration testing, vulnerability exploitation, and attack chaining
- Two weeks of testing focuses on OWASP Top 10, business logic, features and risk areas
- Slack-chat access to Bishop Fox experts
- White glove project management including kick off call and formal status updates
- 12-month access to Bishop Fox portal for:
  - Test initiation
  - Progressive findings delivery with prescriptive remediation guidance
  - Statement of engagement letter
  - Remediation testing
- PDF findings report with report readouts upon request

NOT JUST ANOTHER AI SECURITY TOOL

100% VALIDATED FINDINGS

Every vulnerability is confirmed by a Bishop Fox penetration tester before it reaches you. No scanner noise or chasing false positives. What you receive is validated and ready to act on.

BUILT FOR MATURE ENTERPRISES

Built on two decades of experience testing the application portfolios of the largest companies in the world. Workflows are auditable, results are expert-reviewed, and testing can be tailored to your specific compliance requirements.

ATTACKER-REALISTIC TESTING

Real application risks happen after login. That's why our testing focuses on exploitable attack paths and how real adversaries chain weaknesses together, not how scanners report individual bugs.

NO AI OVERHEAD. JUST ANSWERS.

Running effective AI-powered security testing isn't just about having the right tool. It requires deep expertise to tune it, evolve it, and trust its output. As a fully managed service, Bishop Fox carries that operational burden. Our AI engine is continuously updated, and every finding is validated by an expert before it reaches your team.