APPLICATION PORTFOLIO PENETRATION TESTING

COVERAGE YOU CAN TRUST ACROSS EVERY APPLICATION

ATTACKER-REALISTIC PENETRATION TESTING ACROSS YOUR ENTIRE APPLICATION PORTFOLIO — WITH TRUSTED, HUMAN-VALIDATED RESULTS.

- **Portfolio-Scale Coverage**
- **Match Testing Depth to Risk**
- **No Scanner Noise**
- **One Trusted Provider**

THE CHALLENGE: APPLICATION PORTFOLIOS ARE HARD TO SECURE

Modern enterprises operate dozens to hundreds — and often thousands — of web applications. These applications vary widely in risk, business criticality, and rate of change.

Security teams face a persistent challenge: applying **consistent, meaningful testing** across the entire portfolio without overwhelming budgets, teams, or development workflows.

In practice, this forces difficult tradeoffs:

- Deep testing for a small set of critical applications
- Automated testing — or no testing at all — for everything else

THE RESULT:

inconsistent coverage, noisy findings, and limited confidence in the true security posture of the application portfolio.

WHY TRADITIONAL APPROACHES DON'T SCALE

TRADITIONAL PENETRATION TESTING

- High confidence in individual findings
- Slower turnaround for each assessment
- **Cost-prohibitive to apply to every application**
- High coordination overhead to scope, schedule, and manage across many applications

AUTOMATED SCANNERS

- Fast, automated execution
- Broad but shallow coverage
- High volume of unvalidated findings
- Significant internal effort required to tune, triage, and interpret results

Security teams shouldn't have to choose between coverage and confidence.

WHERE AI-ONLY TESTING FALLS SHORT

AI testing platforms promise speed and scale, but in practice they often introduce new challenges for enterprise teams.

Without expert validation, organizations are left to:

- Triage large volumes of unverified findings
- Determine real exploitability and business impact
- Defend results to engineering and leadership

In many cases, this shifts the burden back onto internal teams — recreating the same trust and scale problems in a different form.

Speed alone isn't enough. Accountability and validation still matter.

HOW BISHOP FOX CAN HELP

APPLICATION PORTFOLIO PENETRATION TESTING

A FULLY MANAGED PENETRATION TESTING SERVICE DESIGNED TO SECURE MODERN APPLICATIONS PORTFOLIOS —WITHOUT SACRIFICING TRUST.

WHAT MAKES IT DIFFERENT:

- Attacker-realistic testing applied across many applications
- Testing depth aligned to application risk
- AI embedded to expand coverage and improve speed
- Human experts validate what actually matters

THE RIGHT LEVEL OF TESTING FOR EVERY APPLICATION

Not every application carries the same risk — but every application deserves meaningful coverage. Bishop Fox portfolio testing enables organizations to:

- Apply testing across the entire application inventory
- Focus deeper expert effort where risk is highest
- Avoid scanner noise on lower-risk applications
- Escalate seamlessly when deeper testing is required

OUTCOMES SECURITY LEADERS CARE ABOUT

Portfolio-Wide Coverage
Test dozens to hundreds of applications using a consistent methodology.

Trusted Findings
No unvalidated critical or high-impact findings delivered.

Faster Time to Value
Validated results in days, not weeks.

Operational Simplicity
Fully managed service with minimal coordination overhead.

BUILT FOR REAL-WORLD ENVIRONMENTS

- Authenticated and unauthenticated testing
- Suitable for regulated environments
- Auditable workflows
- Customizable to organizational standards

Application Portfolio Penetration Testing enables organizations to secure every application — with the right depth, at the right time, and results they trust.

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 threat exposure management, red teaming, and penetration testing for applications, cloud, networks, IoT, and AI/LLM.

LEARN MORE AT BISHOPFOX.COM
FOLLOW US ON 𝕏