

ATTACK SURFACE DISCOVERY

Know what's exposed. Know it's yours. Close the easy ways in.

Internet-facing exposure is attackers' number one way in and most security teams cannot see all of theirs. Spreadsheets go stale the moment a new cloud service, brand domain, or acquisition goes live. Do-it-yourself discovery tools return thousands of assets without telling you which ones are actually yours, and traditional IP-centric tools can misassign assets to your organization or miss them altogether. The result is an inventory your team cannot trust, and blind spots that turn into incidents.

THE BISHOP FOX APPROACH

We continuously discover, validate, and maintain an accurate view of your perimeter assets, and catch the exposed services, certificate issues, and DNS risks attackers look for first.

01

Discover and Expand

Map your attack surface the way an attacker would, pivoting from known assets to connected systems, services and applications, with safe, non-intrusive checks.

02

Validate and Attribute

Our Attack Surface Intelligence team confirms ownership, and every asset carries an evidence-based confidence rating.

04

Monitor and Improve

Ongoing change detection alerts you to new assets, ownership questions, hygiene issues, and assets leaving scope, and each pass adds context that strengthens the next.

03

Surface Hygiene Risks

We surface the hygiene risks attackers look for first: exposed services, certificate and TLS issues, spoofable email, and risky DNS.

ALWAYS ON
Your validated inventory

WHAT YOU GET

[✓] WITH EVERY ASSET

- What it is, where it is, and how it is exposed
- An ownership determination, validated by our Attack Surface Intelligence (ASI) team
- An evidence-based confidence rating showing why it is attributed to you
- Hygiene observations, delivered as exposure facts

[✓] ACROSS THE SERVICE

- Cloud account enumeration through cloud connectors
- Public API access and a read-only AI assistant
- Review of assets you submit, held to the same validation standard as the assets we discover
- A validated, continuously updated inventory in the Bishop Fox Portal
- Activity alerts through the portal and email when your surface changes

Getting started. Onboarding is light: you share your known starting points, such as domains, IP ranges, cloud accounts, and organization names, and confirm or reject ownership questions as they come up. Discovery expands from there.

KEY BENEFITS



FIND WHAT YOU DID NOT KNOW WAS EXPOSED

Shadow IT, forgotten infrastructure, and assets from an acquisition surface on our side before they become a blind spot on yours.



AN ATTACKER'S VIEW

Brand-centric discovery maps your domains, subdomains, and internet-facing assets the way an adversary would find them, not just what a static IP list shows.



TRUST YOUR INVENTORY

Every asset carries an evidence-based confidence rating, so you know why it is attributed to you instead of taking a tool's word for it.



A VALIDATED INVENTORY, NOT A RAW FEED

Our Attack Surface Intelligence (ASI) team absorbs the noise and confirms ownership before an asset enters your inventory, so your team stops spending effort on assets that were never yours.



ALWAYS CURRENT

Ongoing discovery means your inventory reflects your actual, changing footprint, not a snapshot.



THE EASY WAYS IN, CLOSED EARLY

Continuous hygiene checks catch expiring certificates, spoofable domains, hijackable DNS records, and risky services before they become an attacker's entry point.



WORKS IN YOUR WORKFLOW

Your inventory lives in the Bishop Fox Portal. Connect it to the tools your teams already use, like Jira and ServiceNow, pull it through the public API, or ask about it in plain language with a read-only AI assistant.

A STRONG FOUNDATION FOR CONTINUOUS SECURITY TESTING

Start with Attack Surface Discovery on its own, or use it to give the rest of our Continuous Security Testing offerings a validated inventory to work from. Pair it with Attack Surface Testing so our experts test your live, validated inventory as it changes, and with Emerging Threat Testing so new threats are checked against the assets you actually have. Already have an asset list? Discovery turns a static list into a live, validated scope.

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.

GET STARTED AT [BISHOPFOX.COM](https://bishopfox.com)