BISHOPFOX

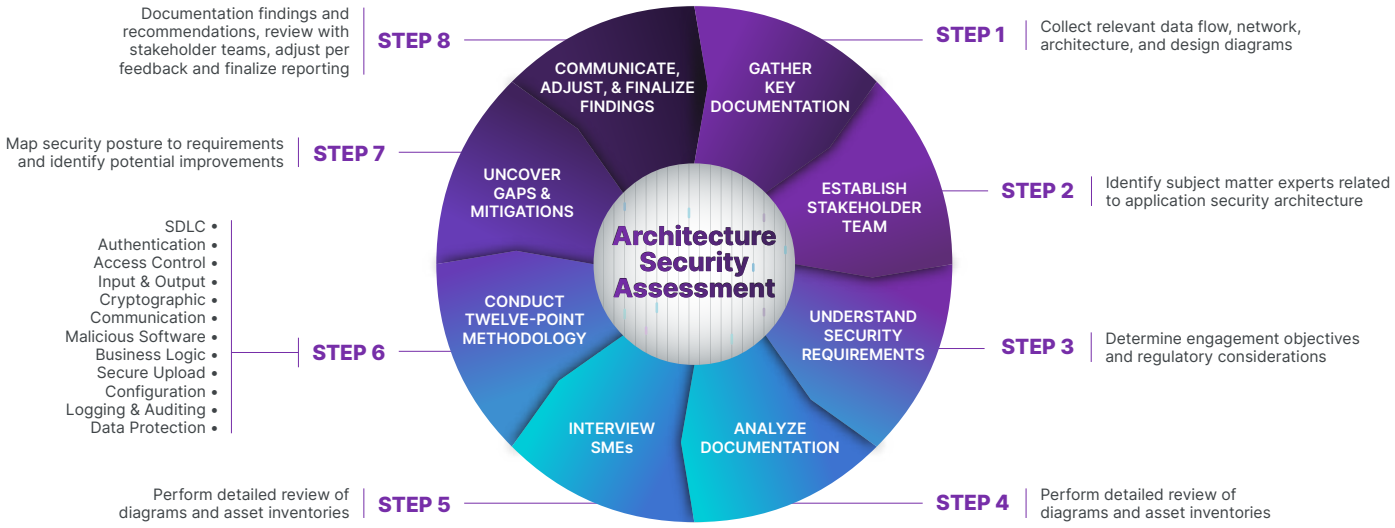
SOLUTIONS BRIEF

Architecture Security Assessment

Bishop Fox's Architecture Security Assessment puts your applications and underlying security architecture under the microscope, illuminating critical flaws and systemic improvements that enhance existing security controls and harden defenses against the speed and precision of modern adversaries.

Secure Applications from the Start

With over 16 years and 3,000 offensive security engagements conducted, we've seen virtually every security architecture and the ways attackers specifically target weaknesses. Leveraging those lessons learned, the Architecture Security Assessment combines Bishop Fox's unparalleled threat intelligence with industry best practices to evaluate your defenses from the mindset of an attacker. Employing a comprehensive twelve-point methodology, our assessors work directly with your subject matter experts collecting critical evidence that enables deep dissection of your data flows, network design, and security controls. Offering flexible options, our assessment puts you in the driver's seat to determine the depth and extension of engagements ensuring we meet your targeted outcomes and regulatory requirements. Arming your team with actionable data, our assessors cover findings with prescriptive recommendations that enhance existing security investments and pave a path to heightened resiliency.



Gain Unmatched Insights from Application Security Experts

Understand how an attacker would target your applications with battle-tested assessors that stay on the cutting-edge of the latest application security intelligence.

Dissect Application Security Architecture Down to Its Core

Deconstruct the full spectrum of your application's security architecture with a twelve-point methodology that leaves no stone unturned.

Uncover Tactical and Strategic Blind Spots Before Attacker Do

Gain deep insight into how a skilled adversary would capitalize on susceptible applications using the latest tactics observed in real-world attack scenarios.

Adapt Engagement to Meet Your Unique Requirements

Put yourself in the driver's seat with flexible options that extends analysis to interconnected devices, regulations, and secure application development practices.

Harden Defenses with Prioritized and Actionable Intelligence

Take the guesswork out of remediation processes with detailed findings that ensure all stakeholders understand their role in addressing risks and recommendations.

Derive Greater Return from Existing Security Investments

Squeeze every bit of value from your investments with prescriptive changes that increase the efficacy of your current security controls.

MOST ASSESSMENTS ARE GENERIC AND FORGIVING.

Put Your Application's Architecture Under the Ultimate Security Microscope.

Leverages Battle-Tested Assessors.
Applies extensive domain experience from Bishop Fox's highly certified and accomplished security experts ensuring your objectives are understood and engagements are aligned to targeted outcomes.

Incorporates Standards from the Most Stringent Frameworks.
Combines OWASP's Application Security Verification framework, PCI DSS, Network Architecture best practices, and Bishop Fox's proprietary methodologies for greater depth of assessment.

Applies Proprietary Tools and Processes.
Utilizes Bishop Fox's internally developed capabilities that uncover critical information out of the scope of traditional architecture assessments.

Incorporates Sixteen Years of Offensive Security Testing Experience.
Integrates lessons from over three thousand ethical hacking engagements that identify and capitalize on blind spots and programmatic weaknesses.

BEAT ATTACKERS TO THE PUNCH.

Pinpoint Your Security Blind Spots and Programmatic Missteps Before Attackers Do.

Conducts In-depth Interviews with Key Stakeholders.
Consults with a wide range of subject matter experts to gain clarity on assessment objectives, regulatory requirements, and provided documentation.

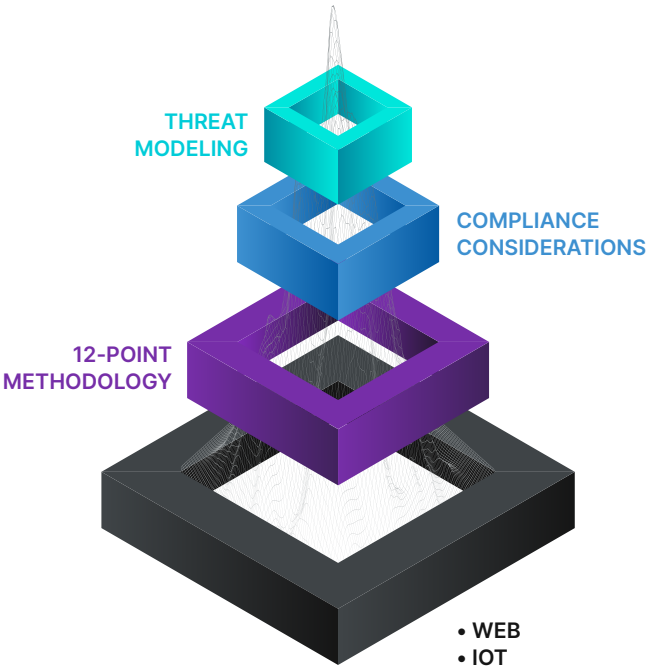
Collects Evidence Critical to Assessment Accuracy.
Defines a list of records and documentation that capture the security posture of systems and enable a greater understanding of the environment.

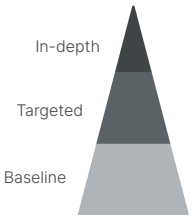
Performs Deep Analysis of Documentation and Configurations.
Inspects every facet of an application's security and underlying infrastructure including design, asset inventories, data flows, and network diagrams.

Uncovers Tactical and Strategic Strengths and Weaknesses.
Pinpoints vulnerable security controls and systemic risks that could put applications and their underlying infrastructure at impending compromise.

ENVIRONMENTS ARE GROWING. ATTACKERS ARE EVOLVING. REGULATIONS ARE CHANGING.

Adapt Assessments to Meet Increasing Demands.





Executes a Twelve-point Macro Methodology.
Covers the full spectrum of an application's security architecture including software development lifecycle, authentication, access control, cryptography, data protection, business logic, configurations, and more.

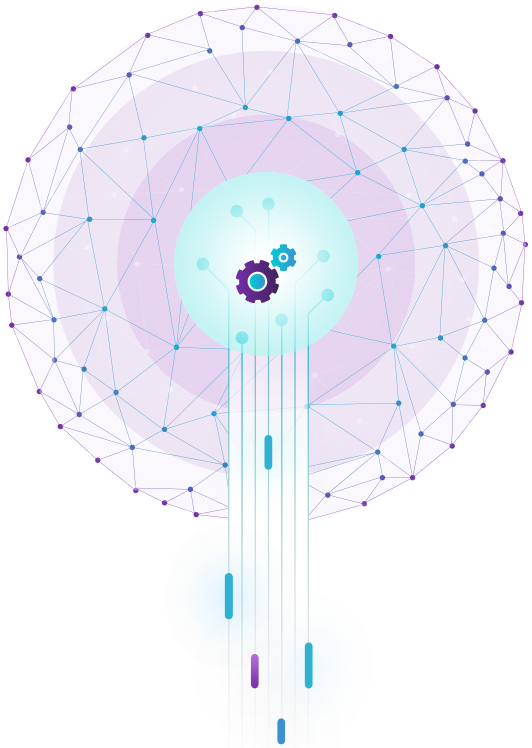
Extends Methodology to Multiple Assessment Types.
Broadens the ASA macro methodology to address the security of interconnected devices including e-commerce web applications, IoT devices, physical products, or other situations.

Offers Flexible Options for Assessment Depth and Regulatory Alignment.
Enables clients to meet their security and regulatory objectives with three levels of assessment depth including:

- Baseline:
  Macro methodology
- Targeted:
  - Macro Methodology
  - Specific Regulatory (i.e. PCI DSS, HIPAA, GLBA, etc.)
- In-depth:
  - Macro Methodology
  - Specific Regulatory
  - Threat Modeling

ATTACKERS DON'T OPERATE INEFFICIENTLY. NEITHER SHOULD YOUR SECURITY CONTROLS.

Squeeze Every Bit of Value from Your Investments.



Delivers Detailed Executive and Technical Findings.
Supplies technical and Executive level reporting that covers assessment findings and recommendations across individual assessment areas (macro methodology), regulations, and threat models.

Provides Interactive Support for Inquiries and Adjustments.
Conducts a detailed walkthrough of findings, with a live question and answer session, ensuring all stakeholders understand current architecture strengths, risks, and recommendations.

Specifies Technical Changes that Enhance Existing Security Controls.
Provides prescriptive guidance that increases the efficacy of security investments including authentication, access controls, data protection, configurations, and much more.

Guides Decision-makers on Systemic Changes.
Furnishes strategic stakeholders with recommendations and best practices that pave a path for continued security resiliency.

BISHOPFOX

SOLUTIONS BRIEF

Cover the Full Spectrum of Application Security

Attackers have no bounds. Neither should your security testing.

At Bishop Fox, we've designed a comprehensive portfolio of services purpose-built to keep your growing applications safe from disruption. From strategic engagements that integrate security across the software development life cycle to in-depth manual and automated testing, our experts will uncover tactical and strategic security issues that real-world adversaries specifically target.

		Plan	Code	Build	Test
THREAT MODELING	Establish a reusable model that proactively addresses security issues across the software development lifecycle				
ARCHITECTURE SECURITY ASSESSMENT	Identifies flaws and uncovers systemic improvements that enhance existing security controls and harden application defenses				
SECURE CODE REVIEW	Address source-code level vulnerabilities and risks before applications move into production				
HYBRID APPLICATION ASSESSMENT	Uncover application security risks and code-level vulnerabilities with automated and manual testing methods				
APPLICATION PENETRATION TESTING	Discover critical vulnerabilities and logic flaw issues with in-depth manual and automated testing methods				
MOBILE APPLICATION ASSESSMENT	Locate security deficiencies with in-depth manual and dynamic analysis of Android/iOS devices and applications				

By The Numbers

6,000+ Offensive security projects delivered

1,000+ Global customers protected

81 Net promoter score

16+ Years of experience

Trusted By Industry Leading Organizations

amazon · Google · workplace from FACEBOOK · zoom · SONOS

Parrot · eugust · EQUIFAX · CHANGE HEALTHCARE · coinbase

About Bishop Fox

Bishop Fox is the leading authority in offensive security, providing solutions ranging from continuous penetration testing, red teaming, and attack surface management to product, cloud, and application security assessments. We've worked with more than 25% of the Fortune 100, eight of the top 10 tech companies, and hundreds of other organizations to improve their security. Our Cosmos platform was named Best Emerging Technology in the 2021 SC Media Awards, and our offerings are consistently ranked as "world-class" in customer experience surveys. We're an active participant in the security community and have published more than 15 open-source tools and 50 security advisories in the last five years. Learn more at **bishopfox.com** or follow us on Twitter.

Info Security Products Guide 2020 Global Excellence Gold · Cyber Security awards · Cybersecurity Breakthrough Award 2020 · Infosec Awards Winner Cyber Defense Magazine 2020 · Cyber Security Excellence Awards Winner 2020 · SC 2021 awards Best Emerging Technology