TAG CYBER

Independent Assessment of Bishop Fox: Using Cyber Offensive Methods to Improve Defense

Prepared by
Dr. Edward Amoroso
Chief Executive Officer, TAG Cyber LLC
Distinguished Research Professor, NYU
https://www.tag-cyber.com/
eamoroso@tag-cyber.com

Version 1.0
May 13, 2021

Summary

This report summarizes an independent assessment by TAG Cyber[1] of the effectiveness and value of the Bishop Fox commercial offerings in the areas of continuous attack surface protection, security penetration testing, and expert cyber professional services. Bishop Fox is shown to have created a world-class solution suite that is highly effective, deeply relevant to on-going trends in enterprise security, and favorably positioned with respect to peers. Findings are described in the context of the underlying foundational aspects of securing an attack surface using offensive methods.

Key Takeaways

- **Bishop Fox excels in the areas of continuous attack surface protection, security penetration testing, security-as-a-service, and expert cyber professional services.**
- **Bishop Fox's unique value proposition and clear competitive differentiators are based on its unique blend of human experts (many of whom come from US Department of Defense backgrounds) supported by an advanced security test platform.**
- **Bishop Fox compares favorably with its peers in its blend of automation and security-as-a-service support for enterprise.**

[1] Founded in 2016 by Dr. Edward Amoroso, TAG Cyber provides world class research and advisory services with advanced market reporting for cyber security teams. TAG Cyber's goal is to bridge the communication gap between commercial security vendors and enterprise practitioners. TAG Cyber's insights are delivered through an innovative on-line portal with support for expert on-demand research.

Contents

Introduction

Cybersecurity has always included two dimensions of focus: (1) Protecting systems from threats, and (2) offering assurance that such protection actually works. This bifurcated focus was especially evident in the earliest days of what was then-called *computer security*. For example, the now-defunct National Computer Security Center (NCSC) published a compliance volume called the Orange Book that included requirements for both functional protection and assurance[2].

During the latter portion of the 1990's, and into the emerging Millennium, focus on assurance was dramatically reduced across the now-called *cyber security* community for two reasons: First, most assurance activities were hard to demonstrate[3], so establishing trust was proving to be more difficult than expected. And second – the commercial marketplace for cyber security tools was beginning to explode, and buyers wanted functionality first, with assurance being less relevant.

A key driver in the expansion of the security marketplace was the acceleration of malicious offense that was occurring at the time – and that continues to this day. Cybersecurity, it turns out, is an asymmetric threat – one where the offensive actor has a huge advantage over the defender. This is illustrated by the common aphorism in our field – namely, that the "bad guys need to find one weakness, whereas the good guys must close them all." Such asymmetry also drove emphasis on functionality over assurance.

One aspect, however, of the assurance ecosystem that has survived the many changes in our industry is *testing*. Unlike defunct counterparts such as formal verification, the discipline of security testing has not only perpetuated in cybersecurity deployments but has thrived and grown. In particular, a taxonomy of specialized security testing has emerged to reflect the nuances in how practitioners can demonstrate that their protections are working (or expose that they are not).

[2] The Trusted Computer System Evaluation Criteria (TCSEC) – also known as the Orange book, is available for download at https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf

[3] Demonstrating the absence of a security threat is a difficult exercise and does not easily translate into most commercial product marketing presentations.

This taxonomy includes validation methods such as *penetration testing*, *hybrid assessment*, *red teaming*, *product review*s, *social engineering tests*, and more recently – *continuous evaluation and valuation* of an attack surface. Each of these methods is available in the commercial marketplace from vendors – and each is supported through combinations of automation, tools, experts, platforms, and professional services. Support in these areas is also available from the open-source community.

In this report, we provide an independent assessment of the *Bishop Fox* suite of professional and managed services, with emphasis on the company's consulting services and *continuous attack surface testing* (CAST) platform. In particular, these commercial solution offerings and security-as-a-service platform are shown to address many aspects of the cybersecurity assurance challenge, while also helping to tip the offensive/defensive scale back in the direction of the defender.

Section 1: Using Offense for Continuous Validation

To properly understand the Bishop Fox platform and solution approach, it is instructive to first explore the underlying factors involved in providing assurance that a system is secure. These factors include the asymmetry of offense and defense, the emergence of attack surface as the playing field for security, the key roles of penetration testing and related red, blue, and purple team methods, and finally, the goal of continuous validation using automated platform support.

1.1 Improving Defense Through Improved Offense

Anyone who works in the field of cybersecurity has noticed the lack of balance that exists between offensive actors trying to find exploitable vulnerabilities and defensive protectors trying to secure valuable resources. In most cybersecurity settings, this balance swings wildly in favor of the offense to the point where security experts generally agree that virtually any non-trivial deployed system will be subjected to break-ins, regardless of the efforts of a security team[4].

This clear offensive advantage can, however, be exploited by enterprise security teams to dramatically improve their protection controls. In fact, three possible defensive strategies emerge that can be used to reduce the cyber risks of malicious attack. The first two scenarios (see below) correspond to the bulk of emphasis in modern cyber security. The third of these strategies, however, involves the creative method of taking advantage of offensive techniques to improve defense:

Directly Improve Defensive Controls – The primary objective of virtually every cybersecurity platform on the market is to improve security posture. This includes encryption, security awareness, network segmentation, strong authentication, and so on. Such measures haven't been as successful as had been originally hoped. A cybersecurity sentiment index managed at NYU, for example, shows a consistently increasing view that cyber defenses are not working[5].

Increase Offensive Costs – The primary objective of most law enforcement, government, political, and policy-based work involves attempts to increase offensive costs for malicious actors. This is done through a combination of political pressure, fines, indictments, negotiations, and other actions. (The

[4] A well-known commentary on the offense having the upper hand is made by William Lynn in a Foreign Affairs article available at https://www.law.upenn.edu/live/files/6465-12-lynn-defending-a-new-.

[5] This research study, which originated with Dan Geer and Mukul Pareek in 2011, is currently managed by Dr. Edward Amoroso at the NYU Center for Cyber Security (CCS). The study provides monthly reports to the general public which can be downloaded at https://cyber.nyu.edu/index-cyber-security/.

author is aware of no reasonable study that suggest that any of this work has had any impact. Offensive teams appear to be as strong as ever.)

Use Offense to Improve Defense – A third objective – one closely associated with the security test community – involves using offensive techniques to help improve defensive controls. This approach involves the defender emulating the attack methods[6] used by offensive actors in order to win the race condition to find any vulnerabilities in targeted systems before they can be maliciously exploited[7]. All security test and validation measures, ultimately, have this objective.

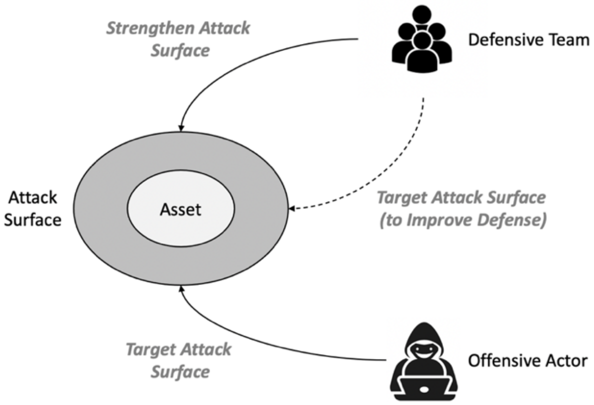


Figure 1. Targeting an Attack Surface to Improve Defense

The process of targeting an attack surface to improve defense is an excellent way to conceptualize the goals of the security test and validation community. Beyond the obvious technical and operational challenges of accurately emulating realistic attacks, perhaps the greatest hurdle involves identifying a complete and accurate view of the attack surface. This includes known and unknown service interfaces, known and unknown access paths, and trusted and untrusted accounts.

Readers should recognize that this concept of targeting an attack surface with an offensive mindset and using a range of offensive cyber methods is the *essence of the Bishop Fox value proposition*. As will be explained in the narrative below, successful execution of this approach to cyber risk management requires that the vendor maintain a *culture of technical security excellence*, a *supportive work environment that attracts and retains experts*, and a *scalable platform to support business growth*.

1.2 Expansion of the Attack Surface

Defining an attack surface has become one of the most challenging aspects of managing an enterprise security program. In the mid-1990's, this task was closely associated with the emerging firewall-protected perimeter and resulted in a so-called edge security discipline that continues to the present

[6] The test community has tried to differentiate between attack emulation, which is highly realistic and involves live actors, and attack simulation which tends to be less realistic, but can be more easily automated. Both methods are intended to play the role of offense to improve defense.

[7] The MITRE ATT&CK framework (https://attack.mitre.org/) is a popular attack taxonomy that purports to include every type of cyber offensive measure observed in practice. Most enterprise security teams and commercial security vendors use the MITRE framework as a completeness check for their program, platform, or tool.

day. De-perimeterization and zero trust security[8], however, have fundamentally changed this equation for defenders, making the protection process much more challenging.

In addition, the risk of insider attacks has increased the attack surface to include *access* to *any resource* in an organization. This is a profound observation, because it increases the challenge for security teams substantially. With perimeter-based enterprise architectures, any actors operating inside the firewall were trusted implicitly – and while this has proven to be an incorrect assumption, it certainly reduced the attack surface that was being addressed.

Now that enterprise architects have begun the transition toward hybrid and full cloud usage with the goal of a zero trust-based network, the attack surface has expanded accordingly. Security teams must now contend with offensive actors who can target any Internet-visible applications or workloads that have been moved from inside the perimeter to a publicly accessible cloud. The result is that test, validation, and other assurance tasks have had to expand to address this increased attack surface.

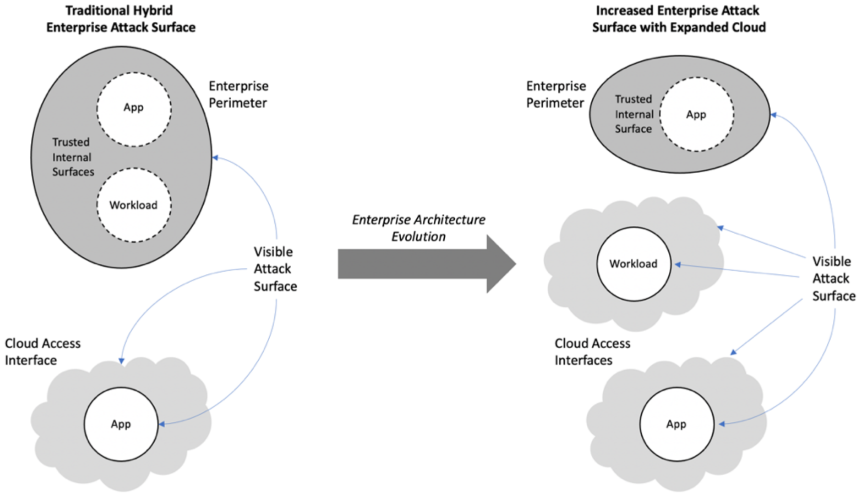


Figure 2. Attack Surface Extension from Increased Cloud Adoption

Note that the attack surface has expanded for many different reasons – not just the loss of the enterprise perimeter. Modern organizations rely increasingly on the use of web applications, cloud services, mobile apps, SaaS-based services, and Internet of Things (IoT) apps. All of these systems are accessible via the Internet or mobile connectivity. Such ubiquitous access fundamentally changes how enterprise networks are organized.

It is also worth mentioning that most organizations have not moved to total public cloud usage with full de-perimeterization, but architectural evolution for enterprise networks is certainly moving in that direction. *This transition is good news for Bishop Fox*, because it increases the attack surface that must be addressed. Where previously, penetration tests, red team assessments, and validation platforms

[8] The concept of *zero trust* was created by industry analysts to model the idea that users, endpoints, applications, workloads, systems, components, and other entities on a network should not have mutual trust by default, simply because they reside within a common local perimeter. The result is that these computing entities are hosted in Internet-visible environments (e.g., public cloud, SaaS) and are made accessible directly to users via their PCs and mobiles (see https://en.wikipedia.org/wiki/Zero_trust_security_model). This approach also has the implication of significantly increasing the attack surface area for the typical enterprise, essentially opening up to the Internet any application interfaces that were previously only present for private access inside the firewall.

were used for high-risk, externally accessible assets, now virtually *all assets* have become fair game for such assurance tasks. This includes firmware on hardware and chipsets since everything is now connected by a smart app.

1.3 Role of Penetration Testing

In the earliest days of computer security, the original concept of security testing involved executing a series of pre-defined functional checks to ensure that certain desired security capabilities were included in the system of interest[9]. These early works included the original references to so-called *penetration testing*, which was included to allow the tester more leverage to be creative and to search for unknown weaknesses or vulnerabilities

Today, most enterprise security teams employ penetration testing either through internal resources or through a contract with an external consulting firm. The process is familiar enough to not require repeat here – but one aspect of the penetration test management process that is germane to the discussion here is the approach taken to selecting and managing a suitable penetration testing partner, if internal resources are not present. Below are some issues regarding how this process is managed[10].

Existence Rather Than Absence of Vulnerabilities. Inexperienced enterprise security managers are often led to believe mistakenly that penetration tests can fully prove the absence of any vulnerabilities. What these managers need to understand is that penetration tests demonstrate the *existence of problems*, but that some other process is necessary to demonstrate the *absence of problems*, especially if the goal of continuous validation is desired.

The best security teams thus tend to use penetration tests to demonstrate, when necessary, the existence of problems. If, for example, an enterprise security team is having trouble getting the marketing group to follow certain security policies, then a penetration test of the marketing teams apps and systems might help to highlight the consequences of such action. Obviously, however, if the penetration tests find nothing, then this is not reasonable proof that problems do not exist.

Trusted Penetration Tester Partnership. The best security teams generally try to identify an excellent testing partner, and to then invest in the relationship. The advantage is that a trusted partner will not need to be retrained regarding the culture, infrastructure, and support systems of the enterprise. They will instead have absorbed an understanding through repeat engagements – and such insight is valuable in establishing more accurate test results and reducing start-up costs for new projects.

Certainly, some diversity in test methodology and perspective is advised. This can be achieved through combination of internal and external testers, or through a mix of approaches from a test partner. Furthermore, crowdsourced security testing in conjunction with bug bounty programs provides a great complement to penetration testing as a means to achieve such diversity[11]. Using multiple penetration testing firms, however, to achieve diversity can lead to management challenges.

[9] The earliest assurance frameworks, including the Orange Book (see https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf) and the Common Criteria (see https://www.commoncriteriaportal.org/), were written to include security testing requirements designed to show that the system being tested included sufficient support for identification and authentication, auditing, access control, and the like.

[10] The material in this section was originally published by the author in 2017 in an article on penetration test management which is available at https://www.linkedin.com/pulse/penetration-testing-management-tips-edward-amoroso/.

[11] A major segment of the cyber security industry has emerged over the past decade involving the use of crowds of vetted benign hackers to probe at exposed interfaces (this method is explained in more detail later in the narrative in Section 1.6). Such crowdsourced security testing is

Viewing Test Methods Under the Hood. Penetration tests are often executed in a so-called black box mode, where the test team does not share detailed insight into their methods. This is particularly true for buyers with non-technical staff and modest budgets. In such cases, the in-house ability to ask probing questions about methodology, policy, and tools might be lacking. This is unfortunate, because managers should have a detailed understanding of exactly how tests are being performed.

Suppose, for example, that some popular test suite is exposed across the security community to have embedded malware. Knowing immediately whether the test team has deployed this suite on present or previous engagements is vital. Furthermore, the determination as to whether a penetration test has become too aggressive[12] should be based on the organizational culture and your risk tolerance. Unless the security team is directly engaged, the wrong decision might be made.

1.4 Role of Red, Blue, and Purple Teams

One security test method that has evolved largely from the government community involves performing live engagements with teams of human actors who try to simulate the specifics of an actual attack[13]. Since there are several possible combinations for how live engagements might be organized and managed, the community has designated three different offense-versus-defense approaches that are most commonly used in practice:

Red Team – A red team consists of security professionals set up as adversaries to try to overcome cyber security controls. These teams might include employees or independent ethical hackers with the skills to target the attack surface using realistic methods. Red teams utilize all available approaches to try to discover weaknesses in people, processes, and technology to gain unauthorized access. Red teams use the results of their engagement to make recommendations on how to strengthen posture.

Blue Team – A blue team is made up of security professionals with an insider's view of the organization. Their goal during a live test engagement is to protect the organization's assets against threats from red teams or other actors. Blue team members are presumably aware of business objectives and the organization's security strategy. Their task is to leverage their test experiences to strengthen security posture against malicious intruders.

Purple Team – A purple team combines both red and blue teams into a cooperative group that is encouraged to work together as a team to share insights and create a feedback loop for posture improvement. Purple team leaders ensure that both red and blue team members cooperate through resource sharing, results reporting, and discovered insights. Such sharing is the most important aspect of purple teams with respect to their red and blue team components.

closely related to bug bounty programs and is advised for inclusion in a properly designed enterprise security program. Such crowdsourced testing does not, however, remove the need for penetration testing – but rather provides a useful complement.

[12] This question of whether penetration tests are too aggressive often emerges in the context of distributed denial of service (DDOS) testing of live systems. Generally, most enterprise security teams will not allow penetration testers to perform such testing, since the effects on the availability of live networks is considered too much.

[13] One of the most famous live test engagements ever performed was the Eligible Receiver simulated attack project held by the US Department of Defense in 1997 (see https://en.wikipedia.org/wiki/Eligible_Receiver_97).

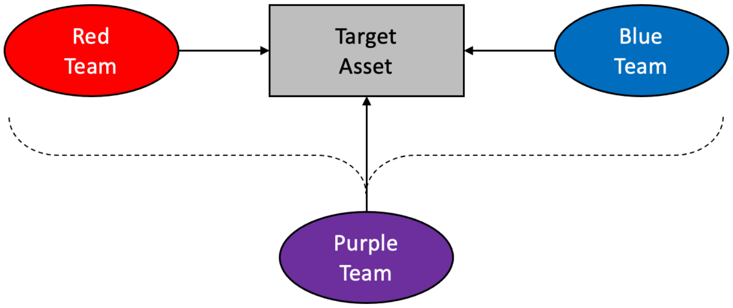


Figure 3. Red, Blue, and Purple Team Methods

Every organization will determine the best set-up and color-coding of their live test engagements. The largest and best funded programs, such as the United States Department of Defense (DoD), will often include all three types of engagements in their overall test strategy. As one might expect, however, these human-led activities are expensive and time consuming, which leads many organizations to have targeted their focus on finding ways to streamline and scale the process.

1.5 Toward Automated Continuous Validation

By automating the continuous validation of an attack surface using offensive methods, the best security test vendors, including Bishop Fox, create an environment where human defenders can more effectively cover the entire target attack surface and engage in the most realistic and scaled offensive security test activities[14]. The functional requirements for any automated continuous validation platform include the following:

Tight Integration with Human-Led Test Activity – Automation for continuous validation must tightly integrate with human-led test activity versus commonly-held views that automation would supplant the need for human curation. Establishing balance between platform automation and human support emulates realistic attack scenarios most accurately.

Flexible Support for Expanded Attack Surface – Automation must be designed flexibly to cover the entire attack surface, which implies support for public cloud and SaaS-based infrastructure. With the attack surface continuing to evolve, automation helps to ensure that test coverage expands to address actual security posture.

Capability to Address Offensive Velocity and Scale – The velocity and scale of malicious actors in their management of attack campaigns demand that realistic test processes include automated support. This allows defensive activity to keep up with the pace established by offensive attackers.

The integration between automation and human-led test activities is one of the strongest value proposition elements for Bishop Fox – as will be described below. This is an attractive differentiator for all the reasons cited above, but it also places the obligation on Bishop Fox to establish a world-class technology plan for its platform as well as a management strategy to attract and retain the best human talent for its professional services.

[14] The Bishop Fox team refers to the interaction between their automated CAST platform and their large team of expert consultants as a so-called Iron Man suit for human defenders (referring to the 2008 film https://en.wikipedia.org/wiki/Iron_Man_(2008_film)).

1.6 Additional Security Test Options

In addition to the penetration testing and red/blue/purple team strategies closely associated with Bishop Fox, several additional options exist to support enterprise test objectives. These are briefly outlined below:

Crowdsourced Testing – Crowdsourced security testing involves the use of a vetted group of experts who perform on-going tests of targeted infrastructure, usually from an external vantage point. Vendors offer curation of this process, including automated platform support and monetary compensation to test experts, so that enterprise teams do not have to deal directly with an external crowd. The result is continuous coverage from a diverse source of test methods.

Vulnerability Management – Vulnerability management involves the identification, assessment, and mitigation of exploitable weaknesses in a target environment. This process is tightly integrated with security testing and is one of the primary means by which vulnerabilities are identified. As such, vulnerability management should be included as an important component of any enterprise security test strategy.

Breach Simulation **–** Breach simulation involves the use of customized agents inserted into a target environment and orchestrated by a management station that simulates attacks to test the effectiveness of designated security controls. Breach simulation offers a useful means to take advantage of automation to provide continual assessment of whether controls of interest such as firewalls continue to serve their intended purpose.

Part 2: Overview of Bishop Fox

Co-founded in 2005[15], headquartered in Tempe, Arizona, and funded by ForgePoint Capital[16], Bishop Fox offers security-as-a-service, consulting services, managed services, and partner programs in the area of cybersecurity test and continuous validation. The company supports many Fortune 100 companies, and has conducted over four thousand engagements in the past sixteen years. With its large team of consultants, Bishop Fox has grown to one of the major cybersecurity professional and managed service companies in the world.

2.1. Bishop Fox Commercial Solutions

Bishop Fox provides a range of commercial consulting and managed cybersecurity services for enterprise customers. These services are supported by an expert team of security consultants, researchers, architects, and engineers with considerable experience and expertise in all aspects of modern enterprise cybersecurity and offensive technique used by the most capable malicious actors.

2.1.1 Bishop Fox Cybersecurity Consulting Services

The cybersecurity consulting services from Bishop Fox, supported by more than 125 professional security consultants located to support customers around the world[17], include the following specific solution offerings:

[15] Co-founders are Vinnie Liu, CEO and Francis Brown, Board Member.

[16] ForgePoint Capital is one of the most prolific investors in early and growth stage cybersecurity companies with over 50 global cybersecurity investments. The team brings more than eight decades of company building, value creation experience and draws upon the largest network of cybersecurity industry experts and customers to support entrepreneurs who are building companies. Based in the San Francisco Bay Area, the firm partners with cybersecurity entrepreneurs worldwide.

[17] Independent informal review of the Bishop Fox consultants by TAG Cyber using LinkedIn reveals a wide range of backgrounds, education, experiences, expertise, and resumes for consulting team members. Some appear to be freshly graduated from university, others have had non-

2.1.1.1 Application Penetration Testing

This service supports the need for customers to determine their application's security posture by employing the same tactics that real-world attackers use, discovering the attack surface in the most realistic way possible, and identifying the weaknesses that lead to the most likely paths of compromise.

2.1.1.2 Hybrid Application Assessment

This service combines a dynamic penetration test of a deployed application with the depth of source code analysis to test for a broader range of vulnerabilities.

2.1.1.3 Red Teaming

This service allows customers to tap into a custom analytical toolkit and flexible simulated attack methodology to proactively address the most critical security risks to technical systems, day-to-day operations, and long-term strategies.

2.1.1.4 Product Security Review

This service involves conducting specialized hardware and software reviews including binary and protocol analysis, reverse engineering, fuzzing, and physical manipulation to identify security weaknesses in consumer, commercial, and industrial devices.

2.1.1.5 Cloud Security Review

This service involves review of the design, configuration, and architectural implementation of cloud services to identify weaknesses, including Amazon Web Services, Google Cloud, and Microsoft Azure deployments.

2.1.1.6 Internal Penetration Testing

This service simulates an attacker who has gained access to the internal network and locates the most likely vulnerabilities, attack paths, and exploit chains an internal threat actor would leverage to gain access to sensitive data and critical functionality.

2.1.1.7 External Penetration Testing

This service simulates an external attacker attempting to exploit internet-facing networks and applications to help identify exploitable vulnerabilities and weaknesses in the perimeter that leave the organization exposed to breaches.

2.1.1.8 Mobile Application Assessment

This service involves conducting in-depth static and dynamic run-time analyses of iOS and Android devices, irrespective of source code availability, to assess attack vectors and risks.

2.1.2 Bishop Fox Managed Cybersecurity Services

Managed cybersecurity services from Bishop Fox, supported by professional operators – two-thirds of whom possess prior experience from the US Department of Defense and the National Security Agency – include the following specific solution offering:

technical prior roles, and many have more traditional technical backgrounds. During discussions with TAG Cyber, the Bishop Fox leadership team references its team as "best of the best," selected based on their potential ability to perform.

2.1.2.1 Continuous Attack Surface Testing (CAST)

This managed security-as-a-service combines a next-generation attack platform with expert-driven penetration tests to deliver visibility into security posture. The CAST platform generates and maintains a real-time map of the attack surface and leverages automation to continuously identify potential weaknesses on the perimeter. This service leverages data from the platform to perform continuous penetration tests and deliver fully validated and prioritized results on the vulnerabilities that pose a threat to the organization.

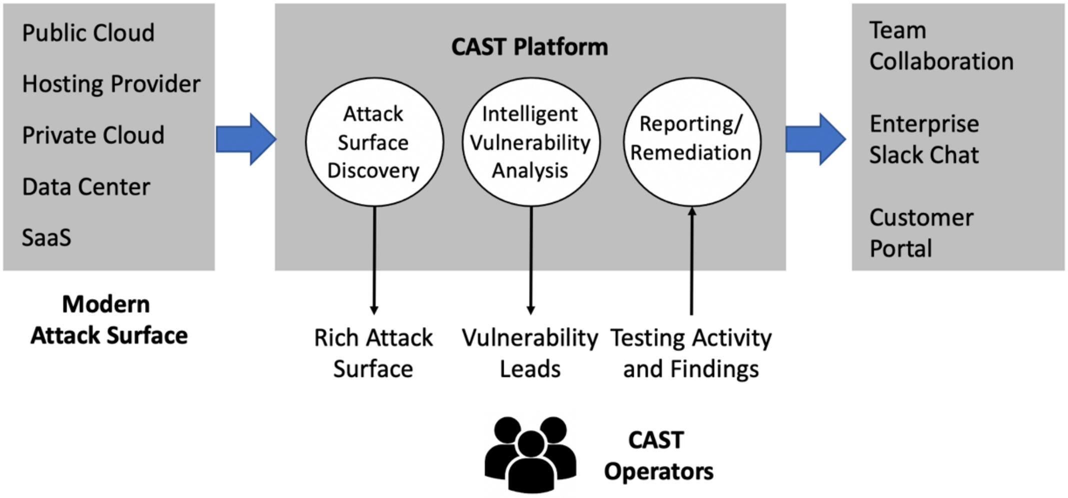


Figure 4. CAST Platform Ecosystem

As depicted in Figure 4, the CAST platform is best represented as an ecosystem involving customer attack surface elements, CAST operators, and the platform automation that supports discovery, profiling, testing, and reporting to the Bishop Fox customer portal. The collaboration and interactions enabled by the CAST platform are key differentiators that drive the desired integration between automation and human support.

2.1.3 Offensive Security Tools

In addition to its CAST platform, Bishop Fox also develops open-source offensive tools that are designed to be helpful to the security community and to advance the ability of professionals to deal with threats and vulnerabilities more effectively[18]. Some of the more prominent publicly available tools from Bishop Fox researchers and shared externally include the following:

Google Hacking Diggity Project – Bishop Fox makes attack and defense tools available through a research and development initiative dedicated to investigating Google hacking. The tools leverage search engine capabilities to quickly identify vulnerable systems and sensitive data that mighty have been exposed from corporate networks.

Dufflebag –The Bishop Fox team developed Dufflebag to help identify exposed EBS volumes and allow organizations to implement security measures.

[18] Bishop Fox makes free resources available to researchers and practitioners at https://resources.bishopfox.com/resources/tools/.

Eyeballer – Eyeballer is an award-winning, AI-powered tool designed to help penetration testers assess large-scale external perimeters.

2.1.4 Partnership Program

Bishop Fox maintains and supports a Partnership Program that has the goal of enabling leading solution providers, MSSPs, and value-added resellers to offer and support Bishop Fox solutions to their growing client base[19]. With minimal initial investment in enablement and training, Bishop Fox partners can begin delivering strategic value to customers while creating a path for a longer-term stream of business.

2.2 Bishop Fox SWOT Analysis

A SWOT (strength, weakness, opportunities, and threats) analysis of Bishop Fox is presented in this section, based on the information and analysis included in this report[20]. The purpose of the SWOT is to offer unbiased assessment of the pros and cons of Bishop Fox's platform and service approach. This is important to establish for buyers, since no commercial solution has zero drawbacks, so any honest assessment must be clear identifying such.

Strengths:

- The primary strength of Bishop Fox is its value proposition, which involves a unique blend of platform automation and professional service capability to deliver enterprise-class security-as-a-service and consultative offerings.
- An additional strength is the technology-based culture, which helps to attract and retain professional service talent inside the company.
- A third strength is the longevity (16 years) of the company and the experience and expertise of the management team, including Vinnie Liu, CEO.

Weaknesses:

- The primary weakness of Bishop Fox, which is true in virtually all professional service businesses, is the low barrier to entry for individual employees or groups of employees to break off from the company and create their own competing consulting firm.

Opportunities:

- The primary opportunity for Bishop Fox is the expanding attack surface across industry, which results in a significantly expanded need to validate security and compliance. This can and should offer Bishop Fox an expanded market opportunity for new and existing customers.

Threats:

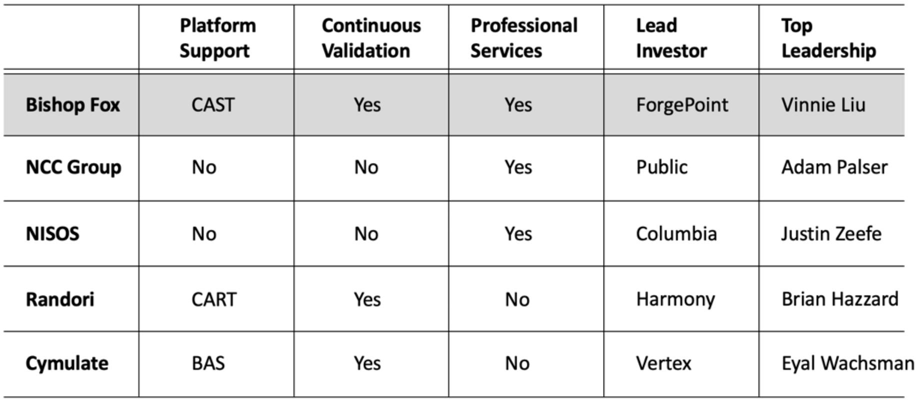
- The primary threat to Bishop Fox is the competitive landscape which include many different commercial options for buyers.
- An additional threat is the low barrier to entry for new companies who are intent on getting into the attack surface validation business.

[19] Key partners include Google, Nest, and Amazon. These are collaborative efforts to protect the partner, customer, and Google/Nest/Amazon data by increasing the security of partners' applications and networks that integrate with these ecosystems.

[20] As part of its industry analysis business, TAG Cyber creates and maintains SWOT analyses for many hundreds of commercial cyber security vendors. These SWOT summaries are delivered to enterprise buyers, commercial vendors, venture capitalists, government officials, research teams, and other groups through an on-line portal with an innovative on-demand research capability (see https://www.tag-cyber.com).

2.3 Bishop Fox Competitive Assessment

To best understand Bishop Fox's positioning, it is instructive to perform a peer comparison of commercial solutions that involve using offensive methods to validate the security of an attack surface. While it would be possible to include many dozens of companies in adjacent areas such as bug bounty or vulnerability management, the summary focuses on companies trying to provide continuous validation through a platform that employs offensive measures.



	Platform Support	Continuous Validation	Professional Services	Lead Investor	Top Leadership
Bishop Fox	CAST	Yes	Yes	ForgePoint	Vinnie Liu
NCC Group	No	No	Yes	Public	Adam Palser
NISOS	No	No	Yes	Columbia	Justin Zeefe
Randori	CART	Yes	No	Harmony	Brian Hazzard
Cymulate	BAS	Yes	No	Vertex	Eyal Wachsman

Figure 5. Peer Comparison Summary

The analysis summarized in Figure 5 suggests that Bishop Fox compares favorably to similar companies[21]. It also, however, suggests some similarities in offerings, especially with platforms such as Bishop Fox that automate the penetration testing process. It is clear that continued growth for Bishop Fox will require carefully crafted market messaging to help enterprise customers understand exactly how the CAST platform and associated services are different from competing offers[22].

Section 3: Assessment Conclusions

Based on the review and analysis described in this report, three major conclusions can be drawn with respect to Bishop Fox's security solution for enterprise.

Bishop Fox Offers an Attractive Suite of Commercial Offers – Bishop Fox excels in the areas of continuous attack surface protection, security penetration testing, and expert cyber professional services. The market trending toward increased and more complex attack surface areas is conducive to excellent growth prospects for the types of services offered by Bishop Fox.

Bishop Fox Supports a Unique Blend of Automation and Human Support – Bishop Fox's unique value proposition and clear competitive differentiators are based on its unique blend of human experts supported by an advanced security test platform. The reference to "Iron Man suit" for penetration testers is an excellent metaphor for this unique strength of Bishop Fox.

[21] Information on the Bishop Fox customer base was not included here to protect the sensitivity of those customer relationships. The company shared, however, that nearly 80% of its revenues are for web application testing for the online home-grown apps for large companies.

[22] The independent assessment summarized in this report from TAG Cyber **does not** include or address financial health, sales results, revenue growth, and other monetary measures of corporate success. This report focuses instead on platform functionality, automated capability, service types, security strategy, and threat coverage.

Bishop Fox Compares Favorably to Peer Companies – Bishop Fox compares favorably with its peers in its blend of automation and professional service support for enterprise. In addition, the company has established a unique ability to attract and retain consultants, which is especially difficult in the present market. This is done through maintenance of a technical culture and a program that supports and advances the careers of employees.

CAST Productivity – An additional important benefit that Bishop Fox brings to the table is the increased productivity enabled for the security team. Such enhancement of work productivity has been an important aspect of growth stories for many successful companies such as CrowdStrike and FireEye/Mandiant. Bishop Fox certainly has the opportunity to repeat this success in the enterprise security market.