CUSTOMER STORY

SCALING UP GOOGLE'S THIRD-PARTY SECURITY PROGRAM

When Google needed to ensure that their user data was being handled securely, they partnered with Bishop Fox to design a security assessment program that could validate the security posture of their 1,000+ G Suite partners. The result: the largest and most successful public third-party ecosystem testing program ever.

As the keeper of the world's user data, Google is committed to securing their users' information — in both their own offerings and the products within their third-party ecosystem, also known as the G Suite Marketplace. As integrations with Google products have grown both in number and complexity, Google decided to expand their security efforts to ensure that any application interfacing with their user data was secure.

One of their objectives: confirm the security posture of their G Suite partners. For each of their partners, Google wanted to know:

- Is Google customer data being protected?
- Can their applications be exploited by attackers?
- Do they have the most effective security practices in place?

Google's focus on proactive security drove them to partner with Bishop Fox to build a security assessment program that could be used at scale. Over the course of nine months, Bishop Fox researched and designed a program that would ensure that effective security measures were in place, but would also be approachable and actionable for every one of the 1,000+ Google partners.

BUILDING FROM EXPERIENCE

With over seven years of experience building and running third-party security assessment programs for a number of the Fortune 500, six years of experience participating in large enterprise program reviews, and three years running assessments for select Google partners, Bishop Fox understands what makes a strong security assessment program, as well as the pitfalls that can leave gaps in security reviews and risk exposures in applications.

CUSTOMER
Google

WEBSITE
https://about.google/

INDUSTRY
Technology

SERVICES PROVIDED
Application Penetration Testing
External Penetration Testing
Cloud Deployment Review
Security Program Review

ABOUT GOOGLE
Google is a global technology leader focused on improving the ways people connect with information. Google's innovations in web search and advertising have made its website a top internet property and its brand one of the most recognized in the world.

In addition to their work with internet platforms like Google, Bishop Fox has performed countless security assessments on hardware such as consumer devices, industrial Internet of Things devices (SCADA and IoT devices for utilities, for example), and smart device ecosystems.

Given the technological and operational differences across all the G Suite partner applications, Bishop Fox understood that a consistent, scalable program would need to focus on:

1. Business-critical threats
2. The implementation of best practice security measures

With these goals in mind, Bishop Fox designed 21 testing models (taking into consideration application size and criticality, best practices across industries, and the testing time needed to thoroughly assess the environments), and analyzed each one to determine which would be most effective across all of Google's G Suite partners.

After taking all of Google's requirements into consideration, the selected security program model focused on two core components:

1. Active penetration testing that comprehensively tests each partner's application, network, and cloud exposures
2. Ensuring the most effective security controls that the G Suite partners must have in place in order to protect user data

TESTING AT SCALE

The cornerstone to any security program is the penetration tests delivered by impartial security vendors. To ensure that all approved third-party security vendors would deliver an assessment that met Google's stringent security requirements, Bishop Fox identified four tests and reviews that would comprehensively assess the G Suite partner's security posture:

1. Application Penetration Testing
2. External Penetration Testing
3. Cloud Deployment Review
4. Security Program Review

To reduce the variability of third-party security engagements, Bishop Fox defined methodologies for each of the penetration tests and in doing so, established a security standard for Google's approved security vendors. The methodologies highlighted areas that required review, established severity rankings, and set report expectations, honing in specifically on how to best protect user data.

These standards were designed to give Google confidence that their third-party security vendors were accurately and effectively reviewing and reporting on G Suite partners' overall security posture and ability to protect user data.

ASKING THE QUESTIONS THAT MATTER

When it comes to reviewing security controls, the process for assessing third-party partners and performing security risk assessments is often overwhelming and costly. Existing frameworks rely on a litany of 800+ questions that security teams do not realistically have the time or energy to deal with. Instead, Google and Bishop Fox wanted to make it as easy and seamless as possible for partners to self-assess their security posture.

To streamline the process and allow it to scale to a thousand partners, Bishop Fox developed a first-of-its-kind Self-Assessment Questionnaire (SAQ). Bishop Fox security experts researched today's most common and burgeoning threats and identified the most important controls that have the greatest impact towards preventing attackers from successfully exploiting a system.

By defining 25 consistent and logical categories that cover the most critical security functions, the SAQ gave Google partners the means to quickly and accurately assess their security posture against top attack vectors including malware, supply chain attacks, stolen or weak passwords, phishing, and spam.

The SAQ includes practical questions, such as:

- Does the company have a vulnerability disclosure program? This should be a dedicated page for security issues, accessible by anyone (not only users of the application).
- How does the company store tokens provided by users to access Google APIs?
- Is your email protection system configured to sandbox email attachments?
- Is two-factor authentication enforced for all administrative accounts in production environments?
- Are customer data backups encrypted?

Alongside these questions, the assessment includes actionable solutions and tips from the Bishop Fox and Google security teams to improve any areas of potential weakness. Ultimately, this unique proponent of the G Suite Assessment Program reveals which partner security controls are in place and working, and which ones need to be added.

BIG PROGRAM, BIG DEAL.

In January 2019, Google rolled out its new G Suite Marketplace Security Assessment Program to over 1,000 of its partners, from small start-ups to the Fortune 100 – making it the largest, public third-party ecosystem testing program in the world. Google selected Bishop Fox as their primary partner for this project, eventually approving two additional security firms to help support G Suite Marketplace partners.

With the visibility and insights they needed right at their fingertips, G Suite partners were able to focus on improving their security posture and mitigating unnecessary risks in order to better protect user data.

In developing the new security assessment program, Google can now quantify the security of all of their G Suite partners and maintain their commitment to quality for their users and data. As Google continues to expand their G Suite Marketplace Security Assessment Program, Bishop Fox will continue to evolve the program with Google to best meet their changing security needs.