# 5 considerations when choosing a bug bounty platform

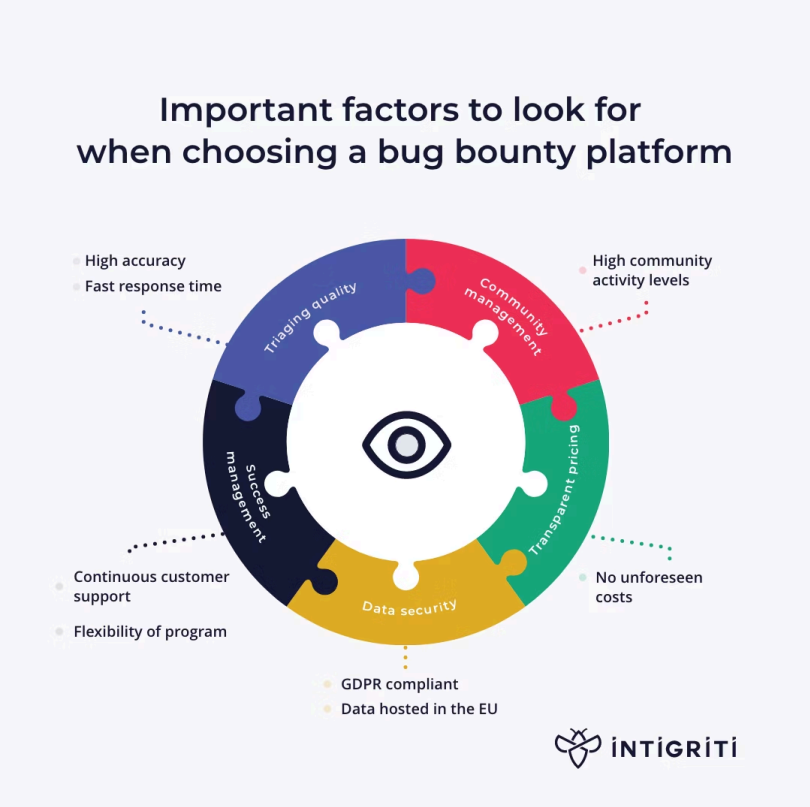
BY ANNA HAMMOND · JULY 20, 2022 · LAST UPDATED ON MARCH 6, 2025

Anyone assessing the best bug bounty platforms will likely encounter many long lists of platform features. These can be overwhelming and leave you uncertain about how to make the right choice for your company's cybersecurity needs. So, how do you make an informed choice from the diversity of platform offerings and marketing?

In this article, we provide some guidelines to help make your decision. We need to mention that Intigriti is a bug bounty platform provider, but we've striven for complete impartiality in what follows. We'd like you to be able to use it as a checklist on your quest for the best bug bounty program for *your* needs.

## What to consider when choosing a bug bounty platform

The good news is that deciding on the best bug bounty platform for your organization isn't complicated once you know five main factors to investigate when choosing a platform. Let's go through these in turn.




5 factors for choosing a bug bounty platform [Source: Intigriti]

## 1. Success management

Cybersecurity is critical to your organization. If you invest in running bug bounty programs, then successfully creating and maintaining these programs with minimal friction will be an important requirement when choosing a platform.

### Customer support and onboarding

Levels of support and guidance will vary from platform to platform, and your decision on what you require will often be based somewhat on your own levels of experience. But structured onboarding, good documentation, and *human* support should be available to all customers. Things to consider:

- Is there an established onboarding process to ensure you get up and running quickly and without mistakes? Is documentation available explaining the process?
- Is an onboarding session available for new customers?
- Does the platform provide support? Is it human or knowledge-based only?
- Is support free or paid-for? Watch out for free support that transitions into a cost at a later date!
- What happens after you become a customer? Is the platform proactive about ensuring your program's success, or are you left to your own devices?
- What happens once you've launched? Do dedicated customer success managers exist for customers? Do these managers check-in?

### Flexibility of programs

Bug bounty programs are not a *one size fits all* affair. Your company will want the ability to tailor its programs to specific requirements and, importantly, continuously update your programs' configurations as your experience and knowledge of the most effective increases. Ensure you factor in:

- Can you tweak the program for optimization once you're live?
- How easily can security researchers participate? For example, can you onboard a community of researchers with whom you've already built a relationship, or are you restricted to the pool the platform provides?
- Are private programs an option? (Private programs are invite-only to select ethical hackers. They are not publicly listed.)
- Does the platform enable you to switch between public and private programs?

## 2. Triaging services

Triaging is the process whereby a security expert assesses vulnerability reports for validity and filters out duplicates. These gatekeepers can sometimes become arbitrators when there is a dispute about a bug's validity, so their impartiality is critical.

Why would you want triage services? Primarily, by outsourcing the responsibility of vetting every submission you receive for validity and uniqueness, you will save your team significant amounts of time. They also help you prioritize bug severity fast. So, make sure to consider:

- Is triage offered as an option or part of the core service?
- The quality of the triage (to what degree do they assess reports? For validity? Severity? Uniqueness?)
- What is their speed of response? Delays in the triage process will cause frustration for your company and the security researcher.
- The perceived impartiality of the triage team: this is critical for trust.

## 3. Community engagement

Crowdsourcing has enormous potential, but crowd *engagement* is the key to success. You need motivated and skilled ethical hackers working on your programs, so it would help if you had a platform that attracts a large talent pool of researchers, or you won't get good results. Make sure to look into how each platform interacts with its crowdsourced community.

- What is the platform doing to nurture hacker engagement on an ongoing basis? Participation in live hacking events is one good way to assess this.
- How active and proactive are the security experts? Some platforms publish hacker league tables where you can assess this in a fun way.

## 4. Pricing

Given the high cost of security breaches, the best bug bounty platforms are an excellent investment. Platforms vary greatly in their pricing models, so it is definitely worth getting granular on this before committing to one platform.

- Start with the big picture pricing model. Is it subscription, pay-as-you-go, or pay-per-bounty, for example?
- Is there an overall service fee, and if yes, when is it payable?
- How much will you need to put aside for bounties? And how do you calculate this? Does the platform have a bounty calculator or something similar to help with this?

As ever with signing contracts or hitting "Subscribe," watch out for unforeseen costs. For example, does the platform charge a percentage or fixed bounty fee? Is this fixed to the severity tier of the bug? It's worth noting that when there is no fee on top, there is a greater chance of impartiality from the triage team because they won't gain anything from exaggerating the tier and impact of a vulnerability.

Finally, check whether triaging services are free or paid for. Without triage, you'll be using many internal resources to assess the bug reports you receive, but paying for triage per bounty can quickly add up if you have an active program.

## 5. Data security & platform

A bug bounty platform aims to increase your cybersecurity and not expose you to risk. Make sure to find out the following about any bug bounty platform you're considering using:

- Does the platform have clearly stated data policies? Do these meet your internal requirements?

- What level of data encryption is the platform using for stored data?
- Is the platform backed-up offsite? Is the provider reliant on just one data center, or do they have backups?
- For companies doing business in the EU, are GDPR and data processing agreements honored? Note that storing data in the EU is a requirement for suppliers.

## Other factors you should also consider

### Company values

Does the platform provider have a clear value statement, and does it align with yours? Are they transparent about how your program is running/performing? Do they have an internal ethics policy? What legal agreements are in place with the security experts to ensure your privacy?

### Platform usability

Finally, there's no shame in considering the subjective question of whether you enjoy the platform UX and UI–it's an important part of working with the tool, after all. How straightforward is setting up an account, program, and payment? Is receiving, approving, or rejecting vulnerability submissions simple or time-consuming?

## Why Intigriti?

Okay, we stated at the top that we would strive for complete impartiality, and we did. So we'll keep this part of the article separate and to the point. We sincerely hope that Intigriti will be one of the bug bounty platforms you consider as you do your own research. It's a platform that satisfies many of the criteria outlined above and has earned satisfied customers in a wide range of businesses and organizations of every size.

### Learn more

Intrigued by what you have read about bug bounty platforms? Want to know more about Intigriti's platform and managed bug bounty programs? Get in touch to request a demo with a member of our team today.


**REQUEST A DEMO**
intigriti.com/demo

**VISIT THE WEBSITE**
intigriti.com

**GET IN TOUCH**
hello@intigriti.com