What is a bug bounty platform? And what are the alternatives?

BY ANNA HAMMOND · JULY 25, 2022 · LAST UPDATED ON MARCH 6, 2025

Organizations run bug bounty programs as a way to identify and fix vulnerabilities within their systems, assets, and applications. They work by giving ethical hackers permission to test for vulnerabilities and provide a report of what they discover in an effort to reduce their attack surface.

Alternative security testing methods include penetration tests and vulnerability disclosure policies (VDP). However, for this article, we're looking specifically at bug bounty programs and what processes and platforms are available to run one. But first, let's start with a quick definition of what a bug bounty *platform* is.

What is a bug bounty platform?

Bug bounty *platforms* host bug bounty *programs* that offer rewards (bounties) to ethical hackers (also known as security researchers or bug bounty hunters). Ethical hackers receive compensation when they discover and report valid security vulnerabilities (bugs) in software (including open source software), systems, web services, and other digital assets.

A business typically engages a bug bounty platform to make running bug bounty programs more manageable and effective in terms of cybersecurity and investment. A platform can facilitate the crowdsourcing and payment of security experts from across the globe and provide other services which add value.

What are the alternatives to using a bug bounty platform?

Still relying on ethical hacking methods, the most common bug bounty platform alternative is to self-host your program. Big organizations like Apple, Google, Meta, and the branches of the US government use this approach. Others, like Intel and the European Commission, prefer an independent platform like Intigriti.

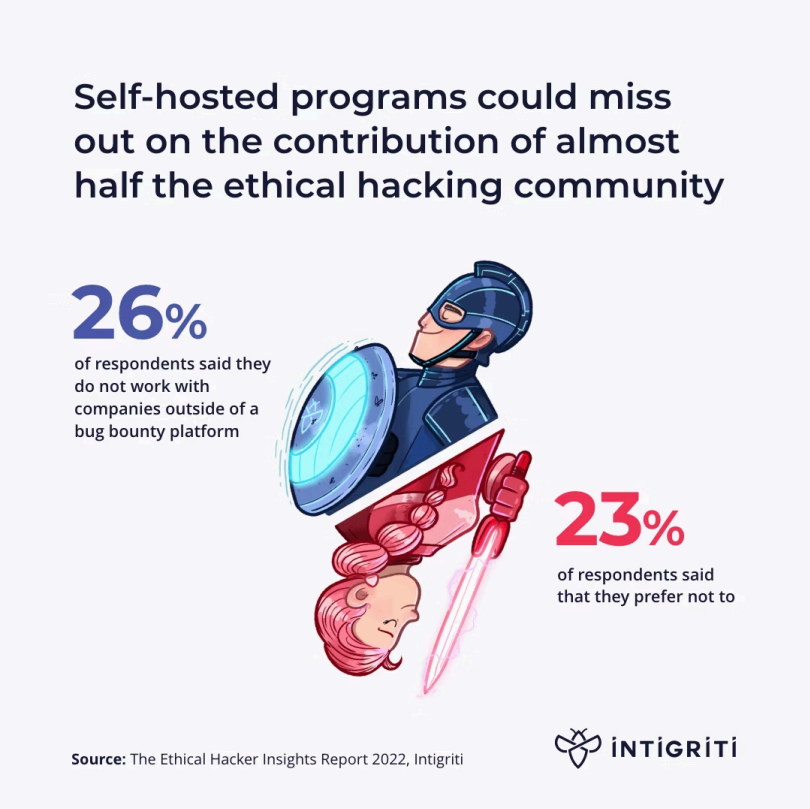
Self-hosted bug bounty programs

While self-hosting a bug bounty program provides a high level of control for organizations, it requires a lot of setup and management of infrastructure. It also requires outreach. Beyond the challenge to your organization of knowing how to define and run a bug bounty program, you'll have to attract large numbers of ethical hackers to your program, typically requiring marketing budget or resources.

Self-hosted programs may also raise concerns for the security experts you are trying to attract. How do they know they'll get paid, for example? What if they find a bug they consider valid, and your internal team deems it not so? Who arbitrates?

Additionally, submitting bug reports in multiple formats is time-consuming. Working with a platform, on the other hand, allows security experts to learn only a single report format that they can use to work on numerous programs.

Sometimes all these factors will add up to make participating in a self-hosted program not worthwhile for the ethical hacker community. According to Intigriti's Ethical Hacker Insights Report 2022, 26% of its community say they do not work with companies outside of a bug bounty platform while 23% prefer not to.



The Ethical Hacker Insights Report 2022 [Source: Intigriti]

Internal bug bounty programs

A variation of running a *public* bug bounty program is to run an *internal* program that only includes the participation of employees. Internal bug bounty programs are a great way to incentivize staff members, such as your software developers, to become interested in your organization's cybersecurity.

Interestingly, many companies opting for this method still use a bug bounty platform for the infrastructure and methodology they provide. If this option sounds like the right fit for your organization, check out our webinar recording, where we discuss the benefits of internal bug bounty programs.

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