4 key benefits of launching a successful bug bounty program

BY INTIGRITI · APRIL 6, 2021 · LAST UPDATED ON MARCH 6, 2025

In this article, we highlight four key bug bounty program benefits. We also explain how crowdsourced security models play an essential part in multi-layered security.

From choosing a solid framework and writing secure code to running vulnerability scans, each additional security step you take lowers the chances of attackers finding an exploitable vulnerability in your system. But before we talk specifically about bug bounty program benefits, let's quickly cover what a program involves.

What does a bug bounty program involve?

A bug bounty program pays independent security researchers to find and report vulnerabilities in your digital assets. The media often talks about big technology companies, such as Google, having a bug bounty program to enhance their security. Today, however, companies of all sizes and industries are embracing the power of crowd security.

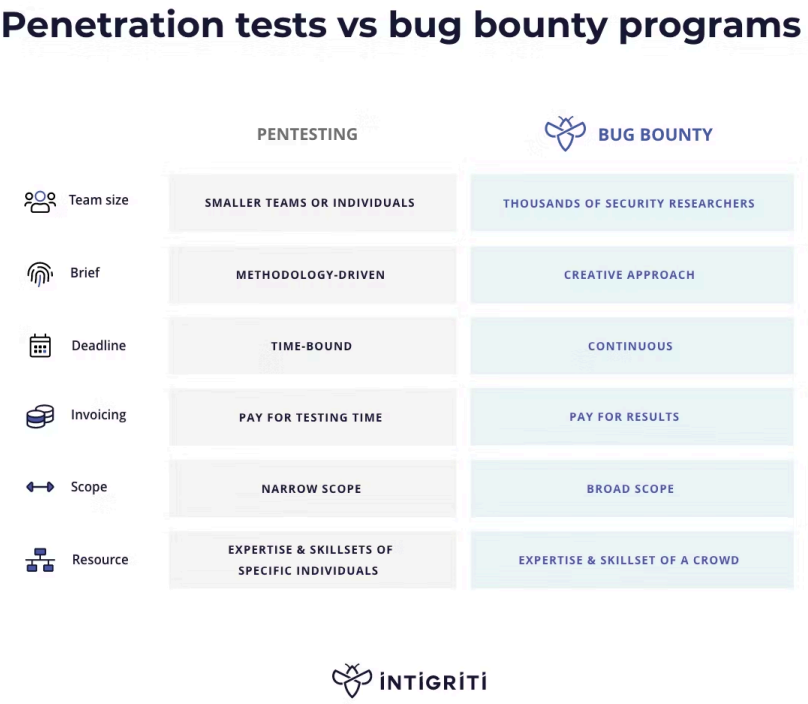
So, what is the value of launching a bug bounty program?

Bug bounty program benefits

1. Bug bounties support proactive security initiatives

Companies who wish to be proactive with their security often conduct penetration tests. A traditional penetration test is a great way to learn what you are unintentionally exposing to cybercriminals. However, the findings of penetration tests are limited to the security knowledge of the hired team. This means there is a high chance of people overlooking some critical vulnerabilities during the process.

This is where bug bounties come in. Bug bounty programs help detect the issues that slip past your security team, vulnerability scanners, and pen testers. Instead of relying on a small group of experts, bug bounties tap into the wisdom of a crowd.



Intigriti's penetration tests vs bug bounty programs comparison chart shows bug bounty program benefits.

By starting a bug bounty program, you invite thousands of ethical hackers to audit your system. Since hackers participating in bug bounty programs are paid for their findings, they are incentivized to use their creativity and find as many ways a hacker could attack as possible.

For companies with short release cycles, bug bounties help you find and squash the bugs that sneak into production. On average, 71% of companies that launch a program on the Intigriti program receive a high to critical report within the first 48 hours of launching. Unlike vulnerability scans and penetration testing, bug bounties continue to monitor systems long after deployment.

2. They demonstrate your dedication to cybersecurity

When customers use a specific product or service, they are trusting that business to keep their data safe. Launching a bug bounty program sends the message that your organization takes information security seriously. The benefit of this public declaration is that it creates an atmosphere of trust and openness among your product users. By publicly demonstrating that security concerns are a priority, you'll also foster goodwill in the security community and encourage curious experimenters to report their findings responsibly.

Similarly, bug bounty programs are a great way to build trust with a community of ethical hackers. Over time, you're likely to build a rapport with specific researchers, which is helpful when bringing out new products or features because they can start testing before you launch.

3. Internal security teams develop their skills and knowledge

Within cybersecurity, there is a widely reported skills gap, but bug bounty programs help to mitigate the impact of a skills shortage in two ways. The first is that companies can lean on a community of thousands of researchers and instantly tap into a much wider range of expertise, knowledge and backgrounds. The second way is that development teams can learn from the vulnerabilities reported through the program, and in turn, advance their cybersecurity knowledge.

Having a team that continuously learns and develops will only enhance the security of future products and services.

4. They're easy to implement via bug bounty platforms

Bug bounties used to be notoriously difficult to run successfully. Managing a bug bounty program took a lot of workforces and specialized knowledge, so they were only reserved for big companies with large security budgets. Then, bug bounty platforms emerged.

Bug bounty platforms provide the infrastructure for organizations to set up programs successfully while providing researchers with a clear and managed way to submit vulnerabilities, and get rewarded. With all the administrative tasks already handled (such as crafting a bulletproof bug bounty policy, triaging reports, dealing with false positives, communicating with researchers, and rewarding them on time), your engineers can focus on the most essential task: fixing vulnerabilities and strengthening your organization's security.

Take advantage of the bug bounty program benefits

Bug bounties are invaluable in helping companies minimize the number of vulnerabilities in their products, web applications, and more. With the help of a third-party platform, like Intigriti, they are easier than ever to implement, too.

Ready to take your security testing up a level by launching a bug bounty program? Schedule a demo with Intigriti today.

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com