Vulnerability scanners vs bug bounty programs: What does your business need?

BY ANNA HAMMOND · FEBRUARY 8, 2022 · LAST UPDATED ON SEPTEMBER 26, 2025

To compare vulnerability scanners vs bug bounty programs is, in many ways, to bring the long-standing debate about humans vs machines to the realm of cybersecurity.

Automated tools, like security scanners, have been helping protect computers and networks for decades now. Recently, automation has progressed so rapidly that the battle of human vs machine might seem a foregone conclusion. But only humans can *innovate* — and crowdsourced security might be one of our greatest innovations yet.

Today we'll take a look at the capabilities of both vulnerability scanners and bug bounty programs. Plus, we'll uncover how each can play a role in protecting systems and organizations against cyber threats.

What is a vulnerability scanner?

Vulnerability scanners are software that runs automatically, searching for known weaknesses in systems or software. They provide immediate protection (such as blocking an email virus from opening) and vulnerability information (network scan reports, etc.) which allow security experts to deal with bugs before they are discovered and exploited.

Given the huge financial cost of data breaches ($3.92 million on *average* in 2021 according to IBM), it's unsurprising that a wide range of tools is commercially available.

Security scanner tools deliver a host of specialized functions, but broadly, they fall under one of three classifications:

1. Network-based
2. Agent/Host-based
3. Web-application.

Most businesses and organizations today deploy some or many types of security scanners as part of their cyber defenses.

Vulnerability scanner advantages

Reasons for the popularity of vulnerability scanners include their price and ease of setup. It's worth noting that most popular scanners come with yearly subscriptions. But, when compared to the $3.92 million data breach figure cited above, this subscription represents good value. Moreover, given their popularity, they have large communities of users in addition to paid support to help in deployment and maintenance.

Vulnerability scanners provide the ability to run automated scans 24/7, as well as when a user performs a particular action, such as trying to log in to a server or opening an email. Security stakeholders can receive instant notifications or detailed reports of threats.

The wide range of specialized tools available also means that you'll probably have no problem finding a vulnerability scanner that fits your needs and budget.

Vulnerability scanner challenges

Given the advantages, deploying a vulnerability scanner is clearly a good call. However, there are some drawbacks.

Vulnerability scanners are automated, and so they often produce very verbose reports of potential threats that require triage in order to assess the severity of the risks reported. In some cases, this step can be extremely time consuming.

Many security vulnerabilities are also the result of multi-step attacks, and this is something that vulnerability scanners struggle to replicate during their tests.

Perhaps the greatest challenge to relying exclusively on vulnerability scanners is that automated tests cannot replicate the human ingenuity of a malicious hacker. They will only ever test for *known* vulnerabilities. Cybercrime has grown by 60% since 2013, according to McAfee, and that growth is a clear indication that hackers are always inventing new and innovative ways to penetrate your attack surface. Even the best vulnerability scanner software cannot predict what they will dream up next.

What is a bug bounty program?

Where vulnerability scanners use automation technology, bug bounty programs use human brains — lots and lots of them.

A bug bounty program uses the crowdsourcing of independent security researchers to test an organization's security and then report bugs in a legally compliant matter. These "ethical" or "white hat" hackers are motivated by reasons that include learning, cash bounties, status, and swag.

While some organizations still set up their own bug bounty programs, increasingly trustworthy bug bounty platforms are being used because of the many advantages they provide.

Bug bounty program advantages

Bug bounty programs have evolved as an ideal and agile response to rapidly developing cybersecurity needs, and provide the following solutions to common challenges:

1. **Tap into a vast network of security experts**

Crowdsourcing leverages the creative thinking, experiences and expertise of thousands of security experts, helping to close cybersecurity skills gaps in your organization.

1. **Test security continuously**

Bug bounty programs are changeable, can run continuously, and can quickly scale when requirements change. This means security teams gain awareness of vulnerabilities faster and head off ever-increasing

cyber threats.

1. **Pay only for results**

With bug bounty programs, security experts only receive a reward if they expose a new, realistic, actionable, and in-scope bug. This makes bug bounty programs very cost-effective, especially when compared to high quality pentests.

1. **Test for the unknown**

When using a bug bounty platform, thousands of security experts use their ingenuity to discover new entry points and vulnerabilities on your attack surface — in the same way malicious hackers do. This leads to the discovery of both *known* and *unknown* security weaknesses.

1. **Centralize security testing**

Bug bounty platforms allow you to centralize your cybersecurity defenses around a vast team of expert, crowdsourced talent, providing pain-free scaling of your organization's growing security needs.

1. **Train your team on-the-fly**

Using a bug bounty platform, you will be able to interact with the researchers about incoming submissions. This boosts your security awareness and helps your team stay up-to-date on cyber threats without the need for formal, time-consuming training.

Bug bounty program challenges

Organizations choosing to launch their own bug bounties can face challenges in running a successful program.

- Without a triage team in place, there is a strong risk of receiving duplicate bug submissions, and the filtering of these can be a time-consuming business.
- Assessing the validity of any bug report submissions requires both time and expert knowledge.
- If you don't have a mechanism in place for capping budgets and maintaining clarity on the value of bounties, there's the risk of runaway costs.
- Attracting high-quality researchers to a self-hosted bug bounty program is also difficult. If no one knows about your program or the administrative bar is high, you're unlikely to attract the skilled white hat hackers you need.
- Without a sufficient number of quality hackers testing your security, there is no guarantee that your bug bounty program will turn up any vulnerabilities.

While these are significant challenges for self-hosted bug bounty programs, the good news is that a decent bug bounty platform successfully addresses these obstacles.

What is a bug bounty platform?

Bug bounty platforms are software used to deploy a bug bounty program. However, they also provide expert teams and services that make running a bounty program more efficient and secure.

A dedicated bug bounty platform provider will work to build a strong community of crowdsourced security experts. Plus, platform providers will have a team of in-house experts that offer triage and support for the program. This human touch is key to how they provide secure and agile security testing, powered by a crowd.

A bug bounty platform is deployed in several steps

- A client defines the scope of their public or private program, and posts it on the platform
- Crowdsourced researchers begin searching for vulnerabilities
- Researchers submit their found vulnerabilities to the platform's triage team
- The triage team communicates with researchers
- The triage team applies quality assurance steps
- In-scope, unique reports are submitted to the client for review
- The client accepts the bug report, and payment is automatically processed through the bug bounty platform.

When selecting a bug bounty platform, it's worth checking whether triaging services come with the cost of your subscription.

Vulnerability scanners and bounty programs complement each other

Both vulnerability scanners and bug bounty programs play an important role in cybersecurity. Vulnerability scanners provide a solid first level of defense against known threats. However, to replicate the ingenuity of real world, malicious hackers, bug bounty programs are the more suitable solution.

The most efficient way to deploy a bug bounty program is through a bug bounty platform. Intigriti offers managed bug bounty programs as a service with a customer-centric and trustworthy team behind it. This will help streamline and guarantee your cybersecurity as an on-going and affordable process.

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