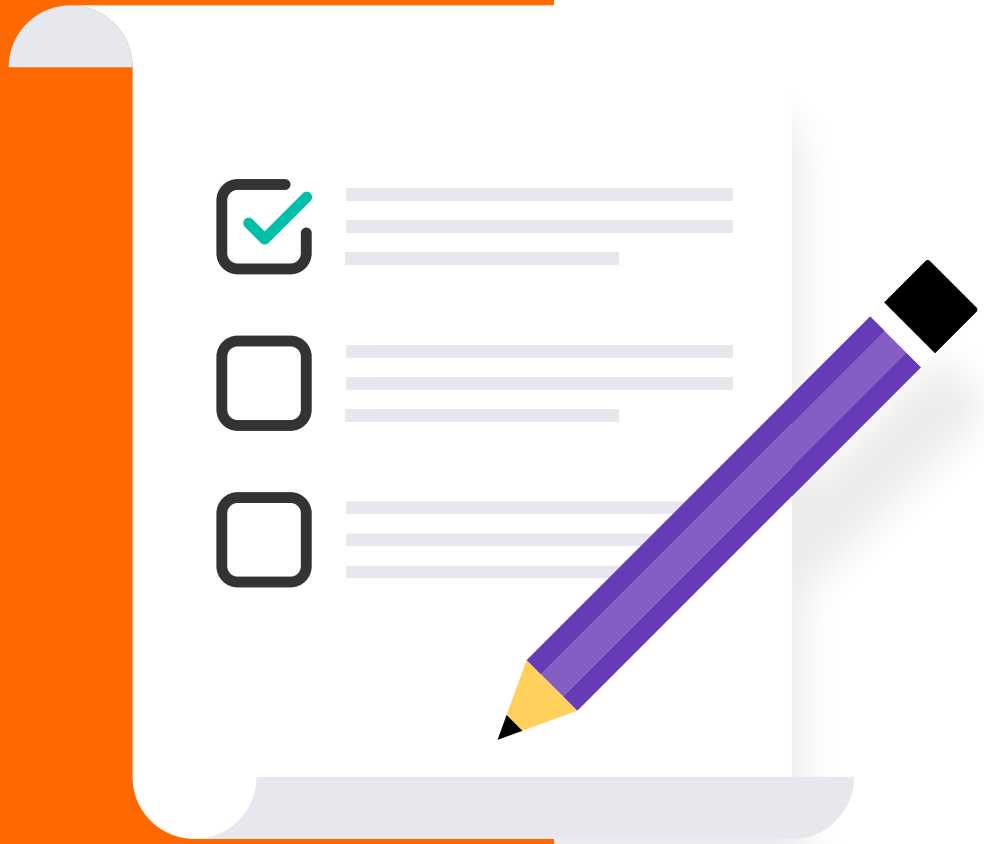
bugcrowd



10 ESSENTIALS
TO LOOK FOR IN A

Crowdsourced Security Platform

Overview

Each year, billions of dollars are spent on cybersecurity technology, but unlike so many other budget line items, the solution doesn't necessarily solve the problem. Cybersecurity isn't a box to be checked—it's a constant tug of war between attackers and the defenders trying to keep their organizations secure.

If a constant tug of war with no end in sight against formidable, dynamic adversaries sounds exhausting, you wouldn't be alone in that thought. **81% of executives say the cost and constant effort required to stay ahead of hackers is unsustainable.**[1]

This struggle is compounded by the cybersecurity skills gap. There were an estimated **2.7 million open security roles** in 2021 ((ISC)[2] Cybersecurity Workforce Study), with most organizations lacking the in-house resources needed to fully understand the risks present in their complicated attack surfaces, let alone secure them.

This is an especially discouraging statistic in the face of an ever-growing attack surface and more vulnerabilities than ever before. **84% of hackers believe that there are now more vulnerabilities compared to the start of the pandemic.**[2]

Over the past decade, many organizations turned to a crowdsourced security model to address these needs. Crowdsourced security comes in many forms, from bug bounty programs to penetration testing to vulnerability disclosure programs. They connect organizations to the ethical hacker community—tapping into their specialized skill sets, human ingenuity, and competitive mindset—to beat bad actors at their own game. In fact, **96% of ethical hackers agree that they help companies fill their cybersecurity skills gap.**[3]

For organizations considering tapping into the power of crowdsourced security, it can be difficult to know where to start. To smoothen this process, we created this checklist to help organizations break through the buzzwords, vanity statistics, and smoke and mirrors to identify the best solution for them.

1 Accenture 2, 3 Inside the Mind of a Hacker Report (2023)

Multi-solution SaaS platform

Vendor consolidation is a driving force in the security market, partially because resources are limited but also because combining elements of a security testing strategy into one platform brings efficiency at scale, consistency, and contextual intelligence.

A **platform-driven approach that combines data, technology, and human intelligence** ensures that:

- ✓ Collective knowledge about assets, targets, vulnerabilities, environments, and remediation steps is always applied for best outcomes.
- ✓ The right trusted researchers are precisely matched to achieve your unique goals, environments, and use cases at the right time.
- ✓ Issues are validated and triaged quickly, allowing you to assess, prioritize, and remediate as quickly as possible.
- ✓ Workflows integrate deeply with the SDLC so that products and APIs can be continuously tested before they ship.

TIP

Many crowdsourced security vendors are "one-trick ponies" and treat every solution as an ad hoc, consulting-heavy engagement.

Look for a vendor that invests in its platform to support your use cases as they evolve.

Crowdsourcing and engagement that meets specific needs

Traditional crowdsourced security vendors focus on the number of security researchers ethically hacking on their platforms, boasting vanity statistics of hundreds of thousands of participants. **But because hackers are free agents who commonly hunt on multiple platforms, any claims made about community size are misleading at best.**

Most vendors rely on mass signups and "spray-and-pray" tactics to match your programs with hackers. This creates noise and fails to match your program to the people who are the most skilled and engaged for the job while also frustrating hackers.

Ideally, your vendor should use data to source and activate hackers with precisely the right skill sets and experience for your programs to **boost engagement and critical findings—not just "throw bodies" at your problem.**

TIP

More isn't always better!

Don't get tricked by big numbers—a good crowdsourced security vendor relies on modern, data-driven crowd matching.

High signal-to-noise ratio

Separating signal from noise is a key concern for all security teams when either automated tools or humans are involved. Unfortunately, scanners are notoriously noisy, and validating and triaging crowdsourced vulnerability submissions takes a lot of time and skill.

With limited security resources and several competing priorities, it is crucial to find a vendor that takes the steps to provide a high signal-to-noise ratio. **More vulnerabilities can lead to more false positives, which waste company resources and obscure the critical issues that need immediate attention.**

TIP

Many vendors oversimplify crowdsourced security and suggest it works as follows:

But there's a catch!

More vulnerabilities can lead to more false positives. Look for a crowdsourced security platform that provides triage services to reduce noise.

Fast, accurate triage at scale

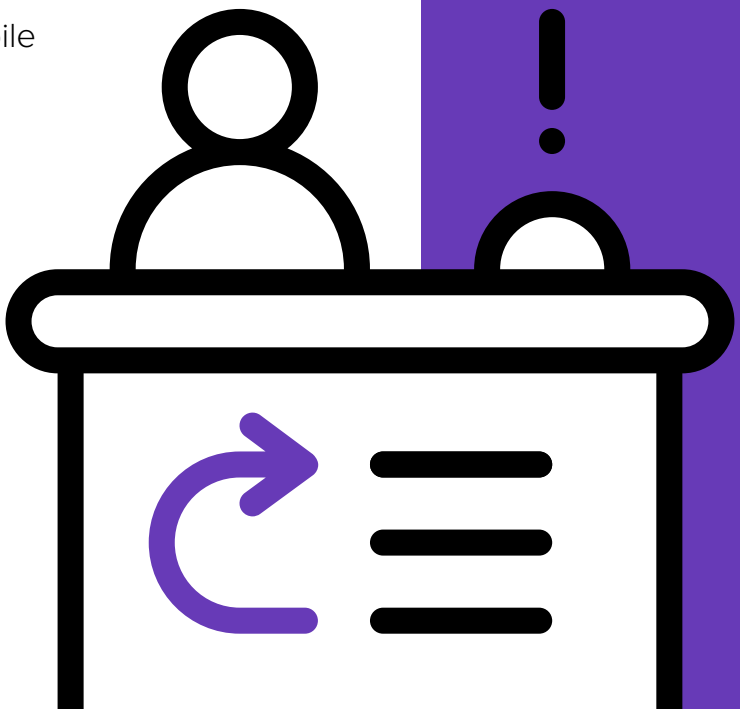
We'll let you in on a little secret—it is common practice in the crowdsourced security industry for vendors to leave submissions to be handled by third parties. Even worse, many vendors treat triage like an afterthought, leaving vulnerability reports untouched for days or weeks. This slows down remediation, frustrating customers and hackers alike.

A good crowdsourced security platform should add critical context to researcher submissions by rapidly validating and triaging bugs, **handling the most critical ones within hours.** Look for platforms with an **SLA success rate of 95%+ for handling critical vulnerabilities,** dedicated staff who specialize in niche areas such as mobile and IoT, and real-time visibility into security decision-making and results.

TIP

Look for a vendor that provides a full life cycle of standardized services, including:

- ☐ Acknowledgement
- ☐ Researcher communications
- ☐ Remediation advice
- ☐ De-duplication and validation
- ☐ Triage and prioritization
- ☐ Retesting and verification



Analytics everywhere

One of the biggest stumbling blocks organizations hit when implementing crowdsourced security is the infamous **“program ceiling.”** The lack of human attention to detail causes programs to decline or plateau.

Hitting this ceiling doesn’t have to be an inevitability. Through reporting and analytics, organizations can continuously improve their programs. A good crowdsourced security platform should provide multiple ways of visualizing data and metrics for your programs, making it easy to monitor program health, benchmark against key metrics, and make actionable improvements.

TIP

You don’t have to go it alone!

Find a vendor who will assign a highly engaged program manager to your account.

A program manager will closely monitor the analytics of engagements you run. They help strengthen your security posture by providing insights into current trends and recommend actions based on your needs, assets, payments, and bug types to establish benchmarks and KPIs.

Real-time visibility into vulnerabilities

Going hand in hand with the importance of analytics is the importance of real-time visibility into vulnerabilities. This is especially true for organizations looking to leverage crowdsourced security for penetration testing. One of the central and most serious criticisms of pen testing vendors is that vulnerabilities aren't surfaced until the initial engagement is complete and results are delivered in a single report 2+ weeks later.

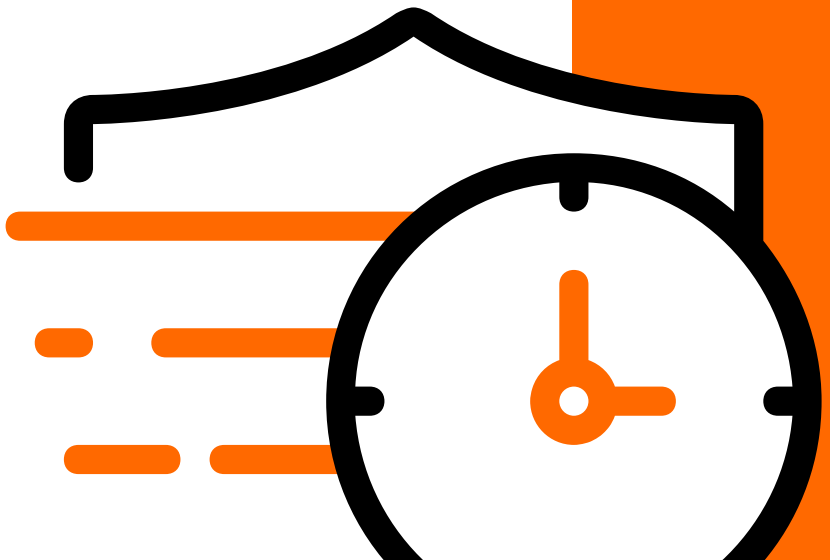
The longer a critical vulnerability sits unremediated, **the higher the chance that bad actors find it and exploit it.** You want to look for a vendor that can provide **Day-one access to streaming vulnerabilities and issues** as soon as they are discovered.

TIP

Beware of sticker shock!

Question vendors that offer full visibility into results as a "premium expedited delivery" add-on. This can be expensive.

Real-time visibility and immediacy should be a standard offering.



Integration with existing workflows and systems

A good security strategy cannot exist in a vacuum—it must be part of a broader workflow that extends across DevOps tools and the software development lifecycle (SDLC). Don't forget that today's SDLC emphasizes the **continual release of new codebase versions.** This means that even if an asset is secure immediately following a test, new code releases may leave it **vulnerable to attack** until the next scheduled test.

Chances are, your organization doesn't have the resources or desire to build the necessary integrations from scratch, so look for vendors that offer the following:

- ✓ Pre-built, easy-to-activate connectors for GitHub, JIRA, ServiceNow, Slack, PagerDuty, Qualys, Secure Code Warrior, and more.
- ✓ A rich API that provides lots of options for programmatic access to your crowdsourced security platform.
- ✓ Event-based webhooks that enable event-based notifications complete with bidirectional functionality.

TIP

The relationships between development and security teams can often become strained.

By providing reports with more context and clear priorities, all integrated into existing workflows, security and DevOps can foster a more collaborative relationship and root out non-secure coding practices over time.

MORE CONTEXT = **BETTER COLLABORATION**

Collaboration framework that builds mutual trust between program owners and hackers

Some organizations have avoided crowdsourced security because of longstanding stereotypes of the hacker community. Pop culture paints an unrelatable picture of hackers that anyone might be hesitant to trust.

In reality, ethical hackers are highly skilled, creative, professional security experts who care deeply about helping keep the world safe. **75% of hackers identify non-financial factors as their main motivators to hack.**[4]

With this in mind, there is no need to blindly trust the ethical hackers on the other side of crowdsourced security platforms. Good vendors research each researcher, doing a qualitative and quantitative background check for everyone to understand their skill sets, availability, and track record.

Platforms should provide built-in security workflows to **promote customer and researcher communication.** Look for a vendor that prioritizes balance and mutual trust between program owners and hackers and that reflects that priority in its platform–for example, by ensuring that communication is prompt, clear, and respectful.

It's important to **do your part** in fostering positive relationships and trust within the hacking community. Organizations that respond promptly to hackers and treat them as extensions of their teams quickly become hacker favorites.

TIP

Don't let fear of the Crowd hold you back!

89% of hackers believe that companies are increasingly viewing ethical hackers in a more favorable light.

This means that if you're still hesitant to embrace the skills of ethical hackers, you're falling behind.

4 Inside the Mind of a Hacker Report (2023)

Adaptability and innovation

Innovation can be hard to define, but you know it when you see it. Ask yourself the following questions as a starting point:

- What is this vendor doing to solve common user pain points?
- What is this vendor doing to evolve with the changing security market?
- How is this vendor looking toward the future to get ahead of potential roadblocks?
- Is this vendor investing in an all-in-one platform or is it stuck focusing on point solutions?
- Is this vendor regularly releasing updates based on experience improvements?
- Is this vendor regularly communicating with its customers and listening to their concerns through social media, email, and customer advisory boards?

TIP

For a future-proof crowdsourced security platform, find a vendor that champions creativity and resilience by developing multiple solutions to proactively address your evolving pain points.

Customer success and satisfaction

We all know what it's like to be charmed by a fast-talking salesperson, but what happens after the contract ink is dry? Is your chosen vendor dedicated to continue helping your programs grow and improve?

Technology is only one piece of the puzzle. It's important to find a vendor who makes **long-term customer success and satisfaction** a top priority. A customer success team should **act as an extension of your security team**—committed to helping you launch, manage, grow, and get value from your programs using data-driven insights as their guide.

TIP

Seek authentic customer stories and reviews.

A great crowdsourced security company has loyal customers who trust them.

Check out their websites and look for familiar logos, customer quotes, and case studies that share how organizations like yours partner with the vendor. You can also find vendor reviews on software insight tools like G2 and Gartner Peer Insights.

Why Customers Choose Bugcrowd

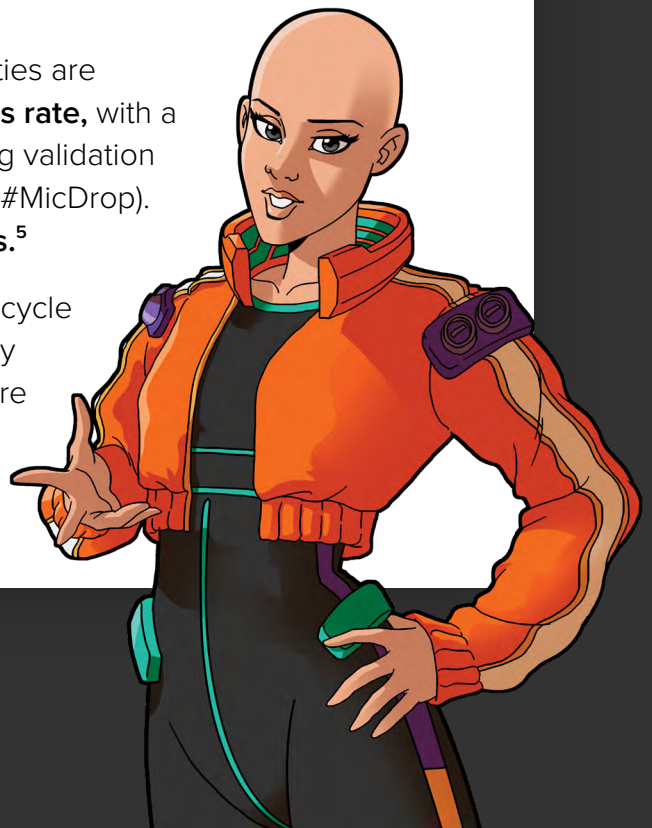
Bugcrowd excels in meeting the ten essential requirements for a crowdsourced security vendor.

Bugcrowd **pioneered the multi-solution SaaS platform** for crowdsourced security. Years ago, we started investing in a multi-solution SaaS platform that combines technology, data, and engineered services to bring the value of crowdsourcing to pen testing, attack surface management, and other goals as customer needs evolve—going far beyond bug bounty and vulnerability disclosure program use cases.

The platform provides additional value with our **proprietary CrowdMatch technology**—precisely matching the most qualified, trusted ethical hackers to your needs and environments across hundreds of dimensions.

Once the right researchers are matched with your platform, vulnerabilities are validated and triaged. Bugcrowd's Triage Team has a **99% SLA success rate,** with a proven track record of handling large-scale vulnerabilities (we're talking validation and triage for Log4j submissions completed within one business day... #MicDrop). Plus, a whopping **91% of hackers are satisfied with our triage services.**[5]

Finally, workflows extend into your DevOps tools and development lifecycle through an **end-to-end integration library,** enabling customers to easily integrate platform workflows with existing tools and processes to ensure that applications and APIs are **continuously tested** before they ship.



bugcrowd

The Bugcrowd platform orchestrates data, technology, and human intelligence better than any crowdsourced company in the world, helping businesses take a proactive approach to protecting their organizations, reputations, and customers.

Get Started