bugcrowd

Ultimate Guide to **Crowdsourced Security**

FOR TECH STARTUPS

Table of Contents

Introduction

For startups, investing in security can feel like a luxury reserved for big companies. Unfortunately, the reality is that for every company at any stage, security is often the difference between winning and losing deals.

Enterprise prospects move faster when they see you've prioritized security, and investors gain confidence when they know that you're not going to be a liability. Additionally, startups lack the resources and brand power to recover from a breach—one incident can stop growth, erode trust, or even lead to the company's demise.

> **While many startup leaders understand this, executing on the promise of security isn't easy.**

Many small companies are powered by stretched teams that lack the necessary expertise to establish effective security programs. Hiring full-time staff is costly and time-consuming, and traditional security vendors are often too expensive and rigid to keep pace with a startup's needs.

This is where crowdsourced security can be a game changer. It combines a global network of security researchers, referred to as "hackers," with a SaaS platform to quickly deliver the security outcomes stakeholders demand without overwhelming your team.

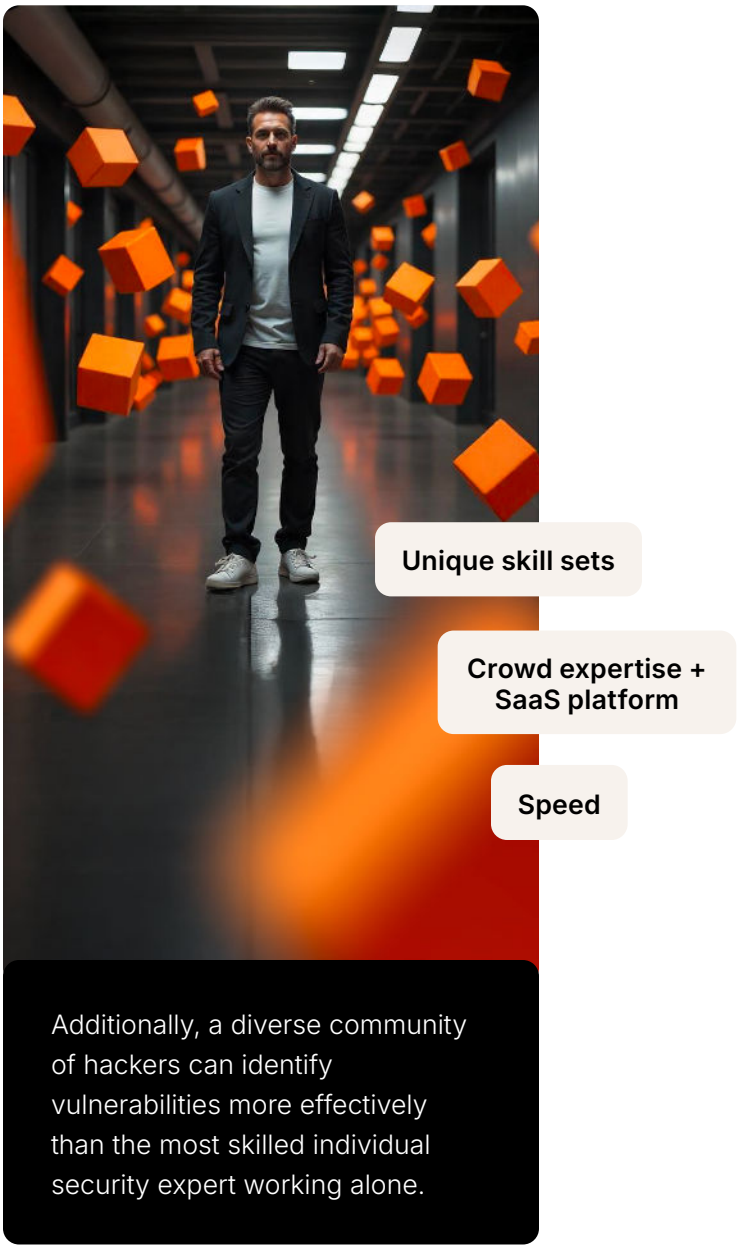
What is crowdsourced security?

Crowdsourced security is an approach to securing digital assets that harnesses the collective skill and experience of the world's community of hackers and pentesters.

These highly capable experts are given the direction, scope, and incentives to identify and report vulnerabilities to organizations. Hackers come from all over the world, bringing hundreds of unique skill sets that can help organizations identify hidden risks in their attack surface before attackers do.

> **Crowdsourced security's most innovative benefit lies in its combination of crowd expertise with a SaaS platform, which enables organizations of all sizes to access specialized security talent on demand.**

Unlike traditional enterprise security solutions that require significant investments and dedicated staff, crowdsourced security programs are designed to scale with your needs and budget, without sacrificing speed or adding overhead.



Additionally, a diverse community of hackers can identify vulnerabilities more effectively than the most skilled individual security expert working alone.

The cost of doing nothing

It's easy to deprioritize security because it seems like a "big company problem," but cybercriminals operate under a different model. They are increasingly targeting smaller companies, knowing that most startups operate with minimal cybersecurity investments, making them easy prey.

The data tells this story clearly: 60% of small businesses have reported a data breach, and 75% of ransomware attacks target startups with less than $50 million in revenue. Recovering from these attacks is expensive; the average cost of a data breach is $4.4 million, and that for a ransomware attack is $1.85 million.

There's also long-term reputational and brand damage involved—this can be fatal to an organization.

> **A recent survey revealed that 10% of breached startups pivoted their business due to reputational damage.**

Other modern examples underscore the reality of this threat:

A cyberattack on a popular dating advice app exposed thousands of users' private data (including IDs, messages, and selfies), forcing the startup behind the app to shut off core features.

A marketing agency accidentally exposed its database on a public server, leaking over 340 million records and personal information.

A former disgruntled employee wiped out a grocery delivery company's servers, bringing their services to a halt.

Startups can use traditional tools, such as automated scanners, to address some of these challenges.

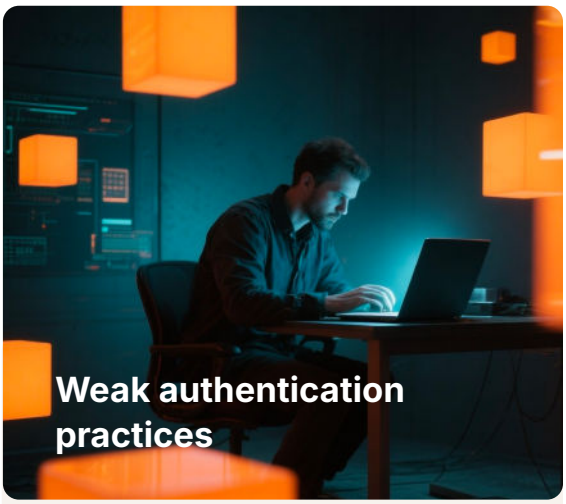
However, these tools aren't designed to detect vulnerabilities in a fast-paced environment. Here are examples of common blind spots traditional tools miss:

Forgotten assets

Startups are constantly iterating, resulting in old domains, test sites, and cloud buckets that aren't actively managed. Automated tools miss vulnerabilities in these assets, resulting in surprise breaches.

Outdated plugins

CMS-based websites often run on outdated plugins and unpatched software, which attackers can exploit to steal data or take down sites. Traditional scanners don't flag these in real time.



Weak authentication practices

With no formalized information security workflows, teams rely on shared logins or skip multifactor authentication. These gaps are often overlooked by traditional tools. Meanwhile, attackers can use these vulnerabilities to break in and commit fraud.

Shadow IT

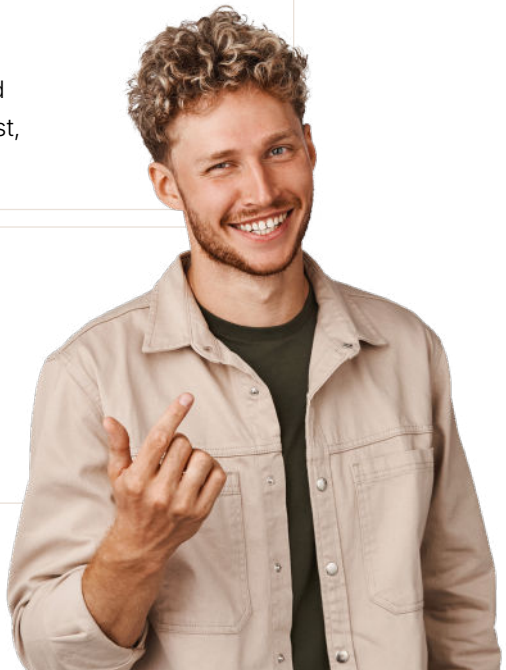
To improve productivity, startup employees may create new accounts for tools without proper oversight. As a result, sensitive data lives in places that can't be secured or monitored using traditional tools.

Benefits of crowdsourced security

By leveraging crowdsourced security, startups gain actionable security insights and reporting that enable sales—all with minimal lift required from their teams.

Other advantages include the following:

Fully managed expertise	Startups rarely have the budget or need for full-time specialists in cloud, API, mobile, or AI/ML security. Crowdsourced platforms tap into a global pool of vetted experts, giving you access to niche skills on demand without the cost or complexity associated with building a team.
Elastic capacity	With crowdsourced security, startups can scale their capacity on demand. You can spin up additional capacity during critical launches or investor diligence, then scale back to save budget when things quiet down.
Sales-ready security	Get instant access to vetted experts who deliver the evidence you need for SOC 2, ISO 27001, and the GDPR, so you can close deals and unlock opportunities without delay.
Rapid speed-to-value	Unlike traditional consultancies with lengthy onboarding processes and retainers, crowdsourced security is quick to launch and results-driven. You get actionable insights fast, so you can keep shipping without delays.
Integrated insights	With the right crowdsourced security platform, startups can take actionable insights from testing right into their software development life cycle. This means you can quickly fix vulnerabilities and prevent delays in shipping.



Common crowdsourced security solutions

Vulnerability disclosure programs

A VDP is a structured framework that invites hackers to submit vulnerabilities they discover in an organization's infrastructure or application directly to the organization. Think of it as a neighborhood watch for finding vulnerabilities. Once an issue is reported, startups should promptly acknowledge, prioritize, remediate, and disclose the vulnerability to maintain a smooth-running program.

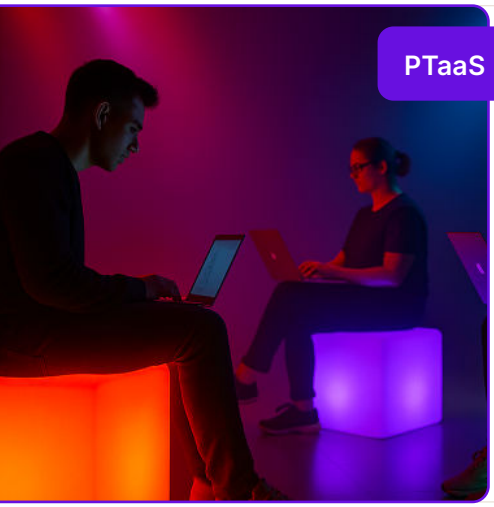
VDPs are widely acknowledged as a security best practice and are often the first step for an organization investing in its security program.

Managed bug bounty programs

Bug bounty programs are result-focused security initiatives that encourage hackers to uncover and report security vulnerabilities in an organization's infrastructure and applications. They're similar to VDPs, except they offer a financial reward based on the criticality of the reported vulnerability.

This "pay-for-impact" model comes with several advantages. First, it can help startups attract top talent quickly and uncover more vulnerabilities than automated scanners. Second, it makes it easier for programs to retain top hackers, which helps create long-lasting programs.

MBBs are especially valuable for fast-paced teams deploying frequent updates, as they provide scalable security coverage with minimal additional effort from internal teams.



Penetration testing

Penetration testing (i.e., pen testing) is a security assessment method in which an organization hires or engages human testers to examine its systems for vulnerabilities against a predetermined methodology, usually for complying with an internal or external control (e.g., the GDPR). These tests are scoped to target specific assets, such as APIs, network infrastructure, web applications, LLM applications, or hardware.

Pen testing can help startups meet regulatory standards (such as SOC 2, ISO 27001, and GDPR requirements) and provide stakeholders assurance that they are meeting a baseline security threshold.

How startups use crowdsourced security

Leading startups are implementing crowdsourced security solutions to build their on-demand security teams and fill the gaps in their security processes.

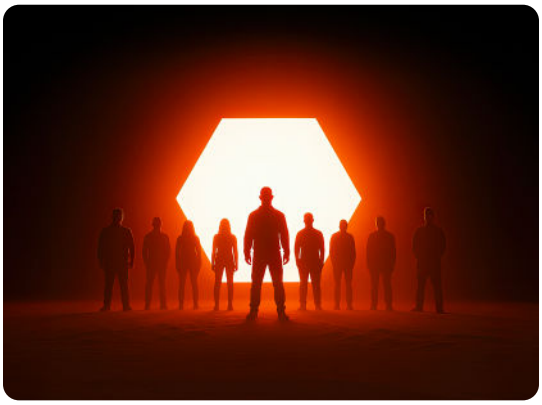
Discover how You Need A Budget (YNAB), Rubrik, and Rewind partnered with Bugcrowd to implement crowdsourced security programs.

Augment existing teams and skill sets

You Need A Budget (YNAB) needed to add new skills and expertise to their team fast. They partnered with Bugcrowd to scale up quickly. "As a smaller security team of a fintech company, partnering with Bugcrowd is almost like having an additional employee on board. Their assistance in initial triage and vulnerability testing has been invaluable," explains Kendal Muir Prins, Security Lead at YNAB.

Scaling cost-effectively

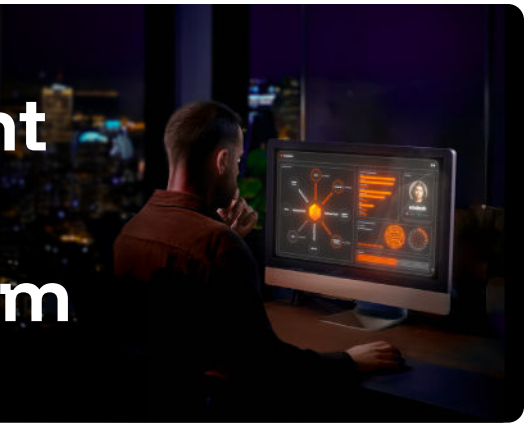
Instead of expanding internal teams, Rewind used crowdsourced security to scale its security operations and expand its team's expertise. "Rather than hiring additional application security engineers, we invested in Bugcrowd and got a 'squad' of folks to triage vulnerabilities," explains Dave North, VP of Cloud Operations and Security at Rewind.



Streamline security operations

Rubrik partnered with Bugcrowd to implement crowdsourced security programs that helped their team rapidly identify and validate vulnerabilities, enabling engineers to focus on shipping. "Bugcrowd's engineering team triages and reviews reported issues before they reach our internal teams, reducing our triage workload by at least 60%," explains Ranjan Kathuria, Cloud Security Architect at Rubrik. "This allows our engineers to focus on remediation rather than initial investigation, accelerating our response times."

Finding the right crowdsourced security platform



Here are some key factors to consider when evaluating potential crowdsourced security platforms:

Immediate speed-to-value

Look for platforms that can be live in days, not weeks or months. Get value right away instead of waiting for hiring or lengthy onboarding processes to complete.

Scalability

Many crowdsourced security vendors are one-trick ponies that treat every solution as an ad hoc, consulting-heavy engagement. Invest in a platform that can easily flex capacity while offering multiple programs to meet emerging use cases.

Low overhead

Ensure that a platform provides a fully managed experience, including program design, researcher management, and triage, so your team isn't burdened with extra administrative work or costs.

Integration friendlines

For a crowdsourced security program to have the most impact, it must be integrated into an organization's broader workflow, including DevOps and the software development life cycle. Confirm that a platform offers these integrations from the get-go.

Built-in deliverables

To meet stakeholder requirements, choose a platform that provides clear, credible deliverables for customer-facing security assurance upfront. Steer clear of platforms that make you do extra work to receive these deliverables.

Customized matching

Many platforms use a "spray-and-dump" approach when inviting hackers to your programs, resulting in a slower engagement and poorer-quality results. Choose a platform that matches you with the right hackers for your program.

About the Bugcrowd Platform

Startups choose Bugcrowd to turn security into a sales enabler, not a roadblock. We deliver fast, fully managed crowdsourced security testing (including pen testing, VDPs, and MBBs).

With our help, you can pass customer reviews, meet investor demands, and stay focused on growth without having to juggle vendors or build an internal security team. Additionally, we can guarantee the following:

Fast turnarounds

Our team scopes and runs everything with you, so you see results quickly.

Seamless workflow integrations

Plug Bugcrowd directly into the tools you already use, like Jira, Slack, ServiceNow, and PagerDuty. For customer integrations, we also offer event-based webhooks for notifications and a rich, easy-to-use API for programmatic access to the platform.

Clear customer proof

We deliver clear, credible reports aligned to SOC 2, ISO 27001, and the GDPR that you can share with prospects and investors to close deals faster.

Elastic expert capacity

We provide unparalleled access to hackers with various skill sets (e.g., API, IoT, AI, and cloud configuration), creating capacity you can't afford to hire in-house. Programs can scale their capacity up and down depending on their needs.

Low triage overhead

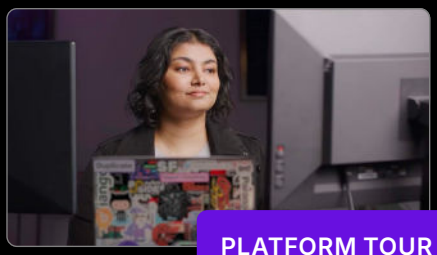
We have an in-house, globally distributed triage team that filters noise and validates findings so you only see actionable results. Bugcrowd saves your team time without compromising on security outcomes.

By working with us, you don't just have access to a platform that helps you check boxes—you have a partner who has your back, no matter what last-minute security demands come up.

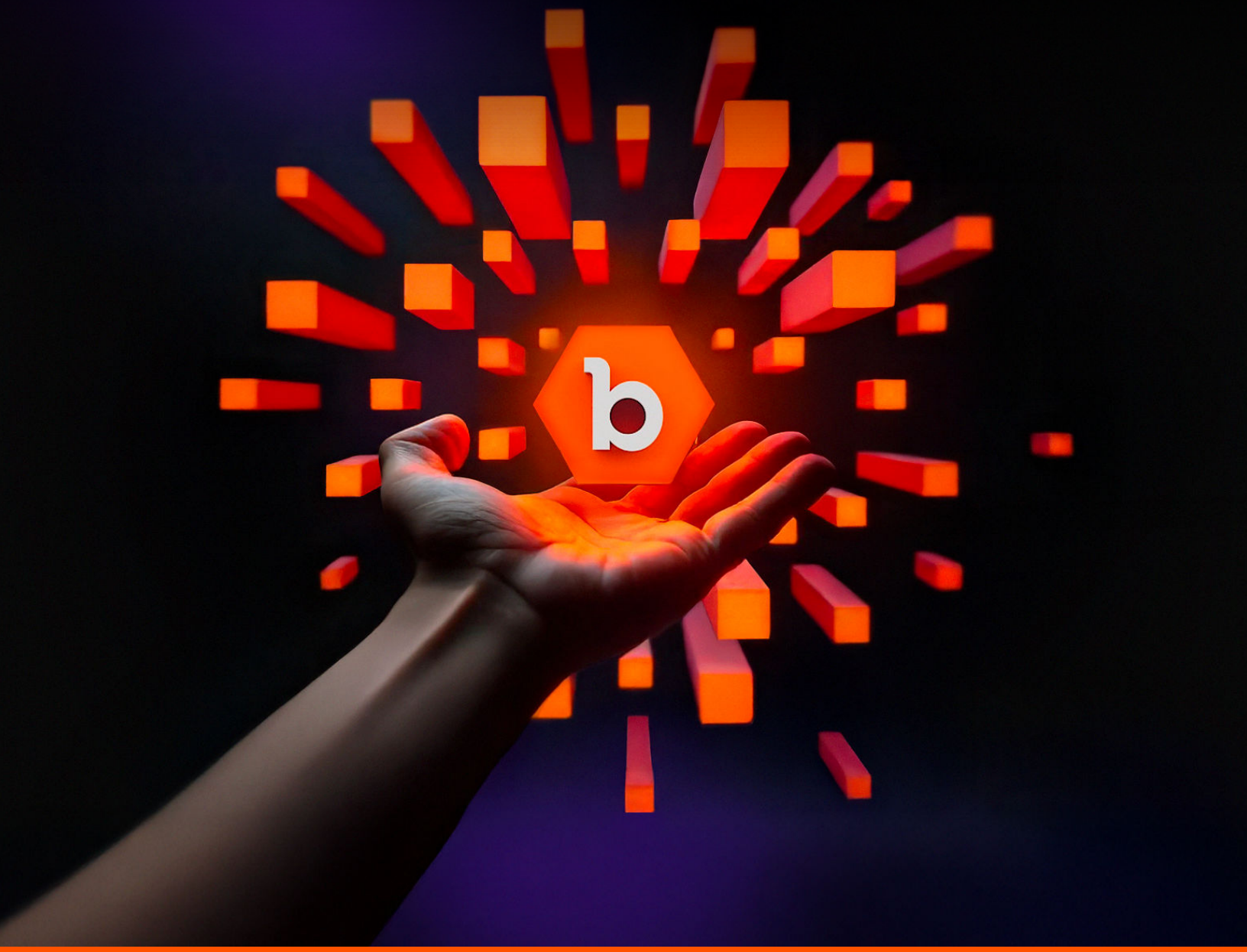
TAKE A 5-MINUTE TOUR

See the Bugcrowd Platform in action

Take a 5-minute tour to get an overview of how the Bugcrowd Platform connects you with trusted hackers to help you take back control and stay ahead of attackers.



PLATFORM TOUR ▶



Unleash Human Creativity for Proactive Security

TRY BUGCROWD