bugcrowd

Ultimate Guide to Crowdsourced Security

FOR SAAS COMPANIES

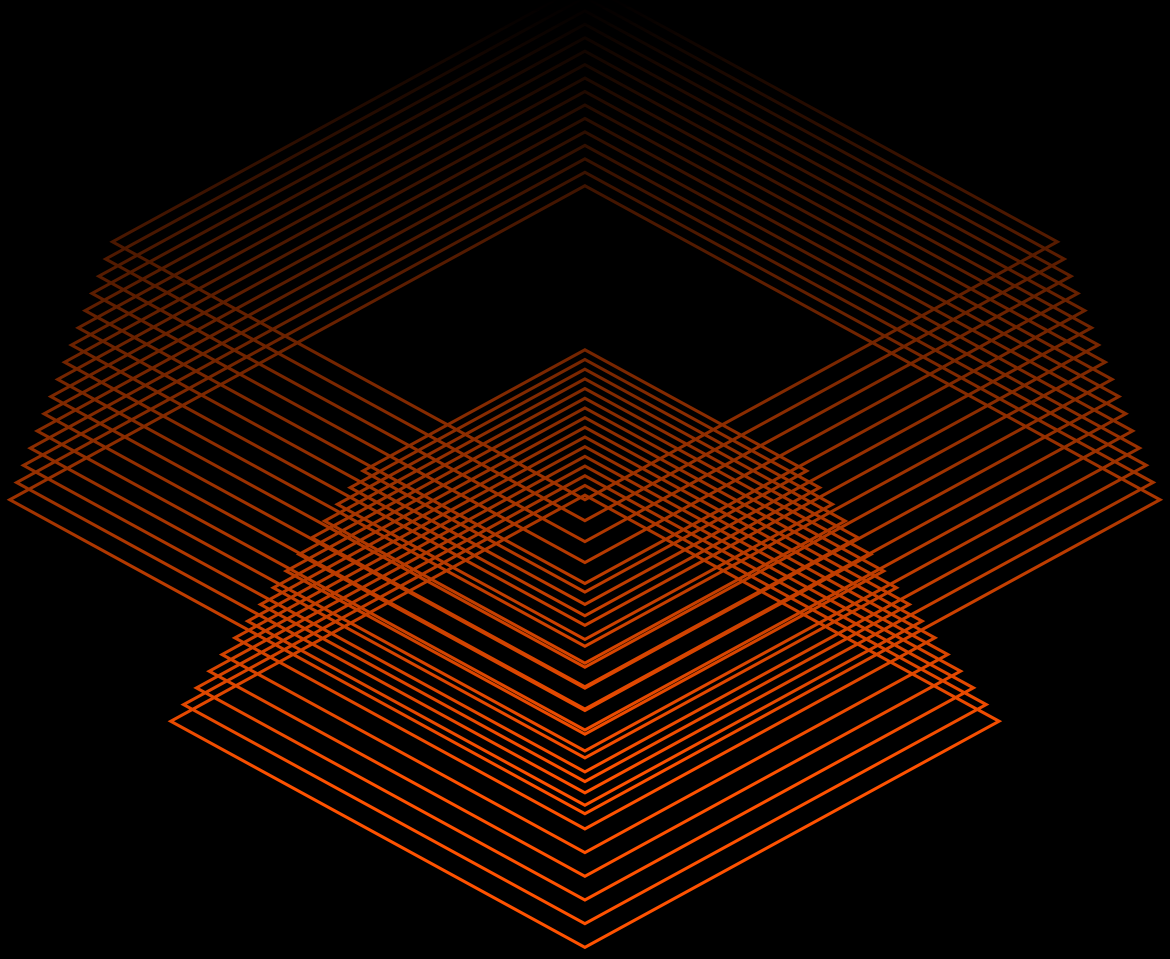


Table of Contents

Ultimate guide to crowdsourced security for SaaS companies

Digital-first companies, such as SaaS providers and platform businesses, are the backbone of the modern digital economy, making security a paramount concern. Any technical disruption to a SaaS provider's operations can cripple its entire workflow, which has network effects across an ecosystem. For example, a payment processor taken offline by hackers instantly paralyzes thousands of businesses relying on the processor's services, which creates a cascade of disruptions for end users. As such, SaaS providers face unique cybersecurity challenges, including the following:

Large and/or complex attack surfaces

Lengthy compliance requirements

Balancing innovation and security

Limited access to skills and capacity

Heightened risk of data exposure

Large and/or complex attack surfaces

SaaS companies often have large and complex technology stacks, encompassing cloud infrastructure, APIs, proprietary LLMs, and third-party integrations. This complexity increases the likelihood of human error, which increases security risk. For example, cloud configurations are particularly risky because common misconfiguration errors can lead to the exposure of critical data.

Lengthy compliance requirements

Many SaaS providers must satisfy customer and regular requirements by meeting multiple regulatory frameworks across different markets. However, maintaining these attestations requires balancing administrative tasks and implementing actual security practices, which can strain already limited resources.

Balancing innovation and security

SaaS organizations struggle to prioritize security alongside innovation delivery as they scale. While companies rely on automated security checks or secure-by-design principles to protect their systems, these tools can't catch new or emerging threats. Growing employee headcounts also introduce unintended insider threats. One common example is shadow IT, where employees might use software, hardware, or cloud services without official IT department approval or insight, inadvertently creating security loopholes.

Heightened risk of data exposure

SaaS providers store large amounts of important customer data, making them attractive targets for attackers seeking high-value information. One common attack path is account takeovers, in which attackers use brute force or social engineering techniques to steal the login credentials of privileged users with access to customer data. If these attacks successfully compromise user data, SaaS providers face significant financial, legal, and reputational impacts that could threaten their survival.

Limited access to skills and capacity

There is a global talent shortage for full-time cybersecurity professionals. In 2024, there were 4.8 million open cybersecurity roles, a 20% increase from the prior year. This shortage severely impacts SaaS companies' ability to scale their security teams. Early-stage companies face an even greater challenge, as limited budgets must stretch to cover both talent acquisition and essential security tooling.

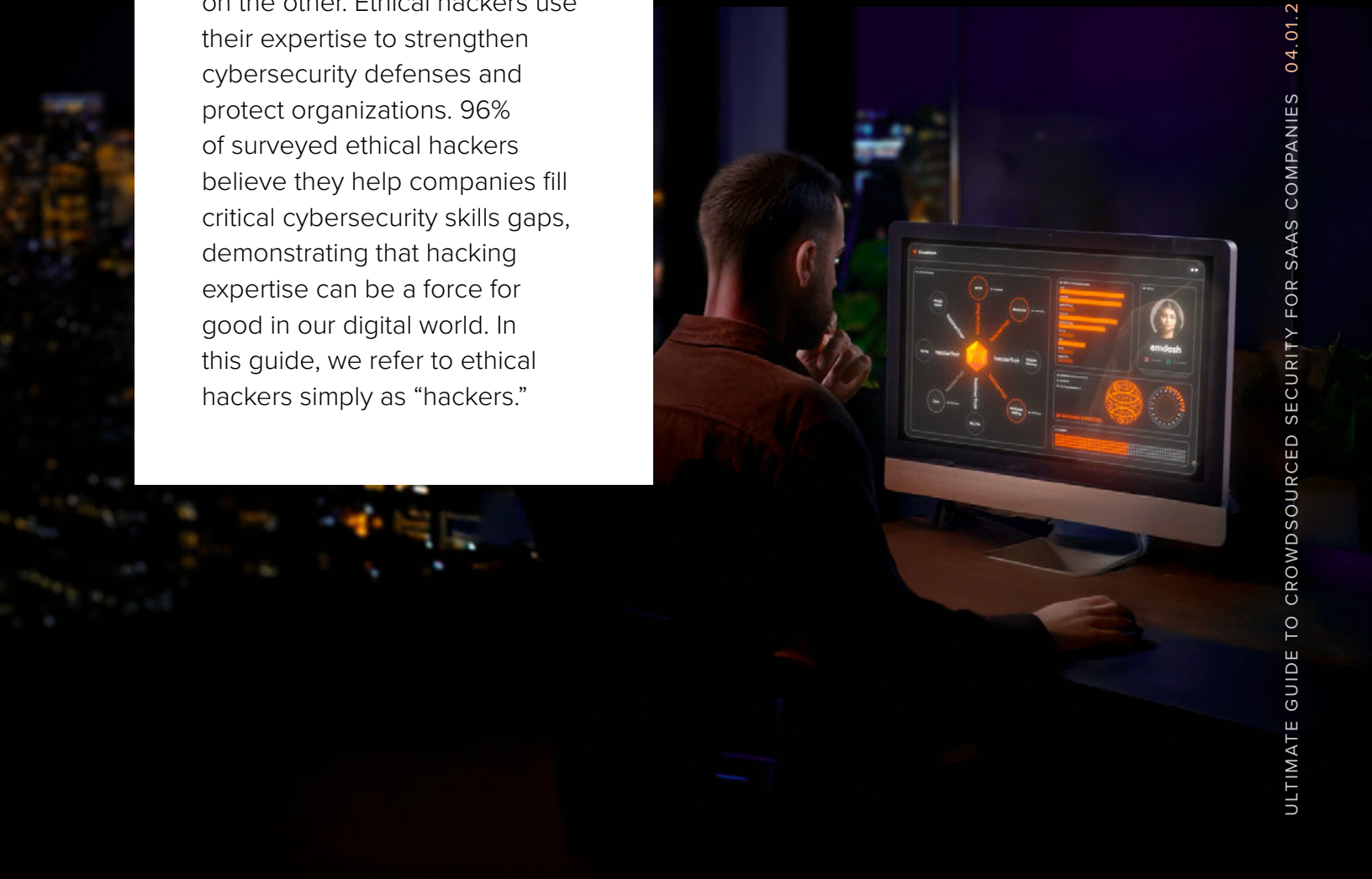
Given this challenging landscape, SaaS providers must adopt an innovative approach to security by applying the same forward-thinking mindset that drives their core operations. Crowdsourced security is one such approach; it involves leveraging human intelligence and SaaS technology to provide cost-effective, scalable protection for SaaS (and digital-first) companies.

In this guide, we will dive into crowdsourced security and how it can fill critical SaaS security gaps, thereby helping safeguard the broader digital ecosystem.

Ethical hacking 101

The term “hacking” often carries negative connotations and is frequently associated with criminal activity. However, at its core, hacking is simply expertise in programming and solving complex computer problems—a skill that can be used for beneficial or harmful purposes.

Today’s security landscape is divided by ethical hackers on one side and malicious attackers on the other. Ethical hackers use their expertise to strengthen cybersecurity defenses and protect organizations. 96% of surveyed ethical hackers believe they help companies fill critical cybersecurity skills gaps, demonstrating that hacking expertise can be a force for good in our digital world. In this guide, we refer to ethical hackers simply as “hackers.”

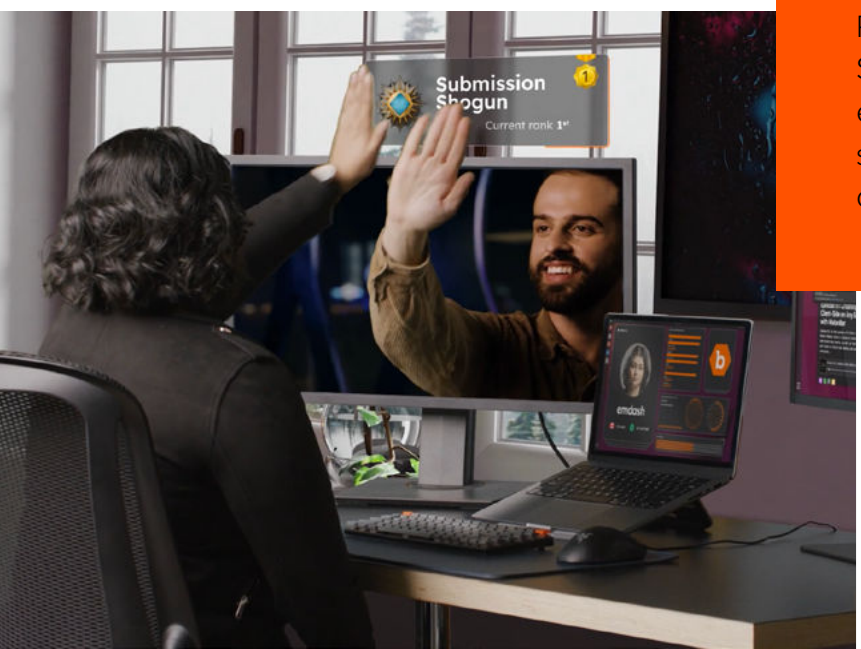


What is crowdsourced security?

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 individuals are given the direction, scope, and incentives to identify and report vulnerabilities. Their work effectively simulates the techniques real-world threat actors use but in a controlled, ethical environment.

The most innovative aspect of crowdsourced security lies in its combination of crowd expertise with a SaaS platform, which enables organizations to access specialized security talent on demand. Unlike traditional security, which relies on ad hoc consulting arrangements, crowdsourced security emphasizes community and collaboration.

It relies on the wisdom of the crowd, a phenomenon in which large groups of people are collectively smarter than individual experts. In the context of security testing, a diverse community of hackers can identify vulnerabilities more effectively than even the most skilled individual security expert.

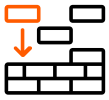


Recognizing these advantages, SaaS organizations have embraced crowdsourced security as a natural extension of their innovative cultures.

Benefits of crowdsourced security for SaaS companies

Crowdsourced security addresses the unique challenges faced by SaaS companies and offers several advantages:

Elastic capacity



For growing SaaS companies, crowdsourced security provides **unlimited testing capacity** quickly. This includes rapid pen testing of new code and continuous monitoring of expanding attack surfaces. Additionally, capacity can be scaled up (or down) to align with a specific business's needs.

Continuous coverage

Crowdsourced security allows you to **quickly scale security testing** as new features or integrations are added to your SaaS platform—with minimal operational overhead. This enables your security teams to focus on remediating security flaws or implementing new security features rather than scaling testing.

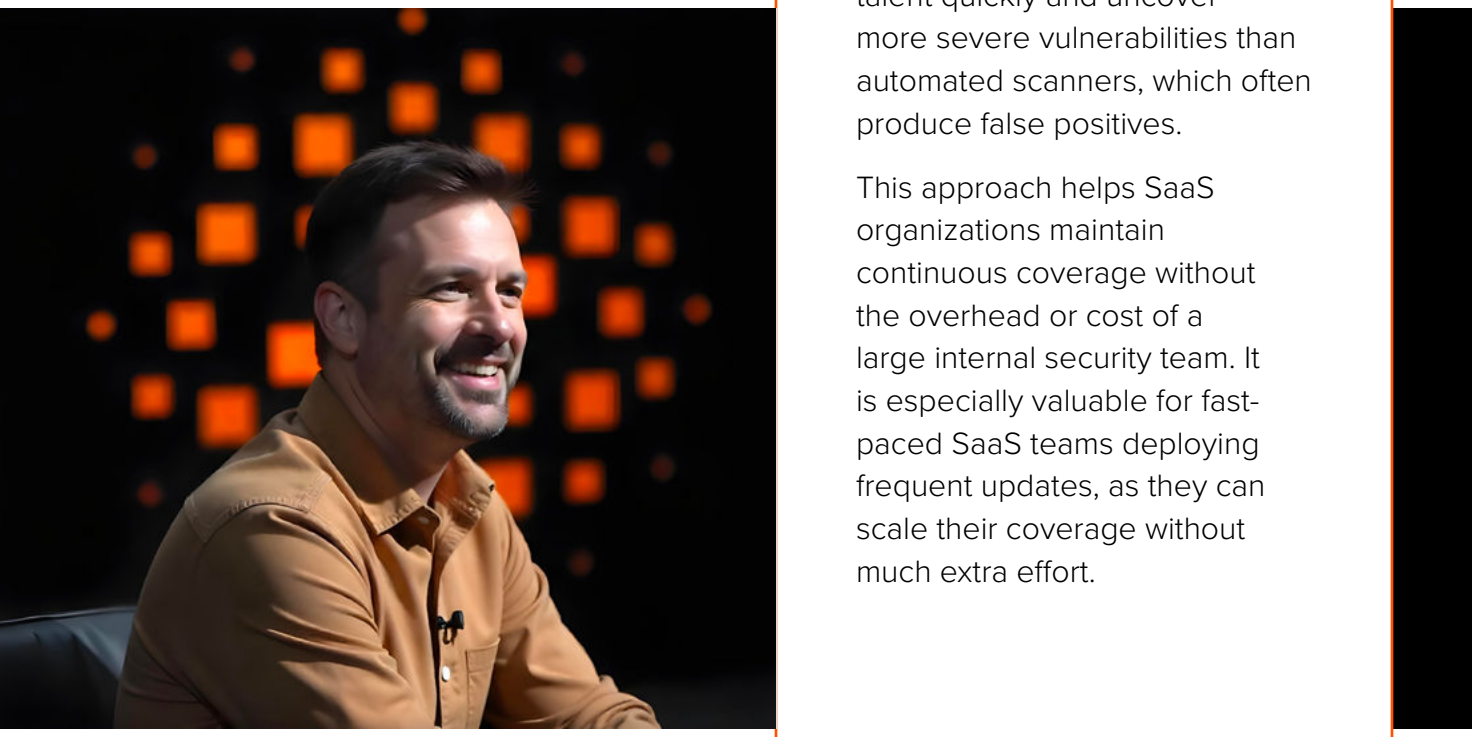
Specialized expertise

Hackers bring their advanced knowledge of specific parts of the stack (cloud, API, mobile, integrations, and AI/LLMs), enabling SaaS companies to **find novel vulnerabilities** that their internal teams or a checklist security approach might miss.

Popular crowdsourced security solutions for the SaaS sector

Vulnerability disclosure programs (VDP)

A VDP is a structured framework that invites hackers to submit vulnerabilities they discover in an organization's infrastructure or applications directly to the organization. Think of it as a "neighborhood watch" for finding vulnerabilities. Once an issue has been reported, organizations should quickly acknowledge, prioritize, remediate, and disclose the vulnerability. The last step is especially important so that hackers receive credit for their work.



Managed bug bounty (MBB) programs

Bug bounty programs are result-focused security initiatives that encourage hackers to uncover and report security vulnerabilities in a SaaS provider's infrastructure and applications. Building on the VDP framework, MBB programs offer a financial reward based on the criticality of a reported vulnerability. These rewards help organizations attract top talent quickly and uncover more severe vulnerabilities than automated scanners, which often produce false positives.

This approach helps SaaS organizations maintain continuous coverage without the overhead or cost of a large internal security team. It is especially valuable for fast-paced SaaS teams deploying frequent updates, as they can scale their coverage without much extra effort.

Penetration testing as a service (PTaaS)

In a traditional pen test, hired hackers use their knowledge of various attack vectors to attempt to break through a company's system defenses. Pentesters operate as a team, working within a defined scope for a set period and reporting the vulnerabilities detected. However, these tests can take a long time to set up and ramp up, which limits their continuous use.

PTaaS solves these operational challenges by implementing many aspects of pen test delivery as software. With a PTaaS engagement, once testing is underway, a customer can monitor the results in real time rather than waiting for a final report to be delivered weeks later. Additionally, with streamlined onboarding and delivery, these tests can easily be repeated at scale, contributing to continuous assurance for organizations.

Contrary to popular belief, PTaaS complements a vulnerability management solution (e.g., VDPs or MBBs). Paired together, these solutions provide organizations with comprehensive protection. This is because this combination integrates the systematic, continuous analysis of PTaaS alongside the scale and ongoing discovery of emerging vulnerabilities made accessible by MBB/VDPs. As a result, organizations that adopt these programs find up to five times more high-impact vulnerabilities.

AI bias assessments

SaaS organizations face mounting AI-related security risks as they race to deploy LLMs in their products. These models can access various user data, making them ideal targets for attackers looking for high-value information. Moreover, if LLMs are not adequately safeguarded, they can become threats—perpetuating biases, promoting hate speech, or participating in criminal activities like hacking power grids.

Unfortunately, such threats are not hypothetical. In 2023, users were rattled when Sydney, Microsoft's AI chatbot, insulted them when they asked for movie showtimes, forcing Microsoft to shut it down. To combat this growing threat, companies must prioritize AI safety.

AI bias assessments are a vital tool in ensuring AI safety. In these assessments, organizations work with trusted, third-party specialists to find and prioritize data bias flaws in LLMs (either open-source or private). Similar to MBBs, specialists receive impact-based compensation, making this approach cost-effective.

How crowdsourced security can meet regulatory requirements for the SaaS sector

Payment security

The Payment Card Industry Security Standards Council (PCI SSC) established data security standards (PCI-DSS) for any organization that accepts consumer payment cards. These guidelines highlight crowdsourced security solutions to effectively meet critical security requirements. Here are two examples:

- PCI-DSS 4.0 / 6.3.1 recommends bug bounty programs as a potential solution for assessing vulnerabilities in internally developed software.
- PCI-DSS 4.0 / 6.4.1, which calls for periodic vulnerability assessment, can be met through pen testing (including PTaaS).

Information security certifications

ISO/IEC 27001 and SOC2 are the leading information security frameworks for digital-first companies, providing standardized approaches to protecting sensitive data and proving security competence to customers, regulators, and partners. Here's how crowdsourced security can meet these frameworks' security guidelines:

- ISO requires organizations to implement a system for identifying vulnerabilities in key assets and recommends implementing a bug bounty program.
- SOC2 has several requirements (like CC7.1) for implementing detection systems to catch new vulnerabilities. Bug bounty programs, VDPs, and pen testing can be used to meet these requirements.

Data privacy regulations

In the last decade, governments have passed significant privacy laws in response to growing concerns about how organizations use and manage user data. This has led to two landmark legislations:

- General Data Protection Regulation (GDPR): Requires organizations operating in the EU to implement secure data-processing practices to protect citizens' privacy.
- California Consumer Privacy Act (CCPA): Requires for-profit businesses operating in California to implement reasonable security measures to protect residents' data and privacy.

A key requirement of both legislations is implementing practices, procedures, and systems to protect user data from security vulnerabilities. The penalties for failing to meet these requirements are severe: GDPR violations can result in fines of up to 4% of annual global revenue and orders to stop data processing. CCPA violations can cost organizations $100–$750 per user per incident and civil penalties.

Given the stringent regulatory environment, SaaS organizations operating in these markets must prioritize robust and innovative security solutions. Crowdsourced security is one of these approaches, combining vulnerability discovery programs (through VDPs and MBBs) with pen testing to ensure thorough, continuous protection.

AI

While AI is still a nascent space, governments are moving quickly to regulate it. The EU AI Act establishes rules for developing, using, and deploying AI systems in the EU. It bans harmful uses like social scoring while requiring high-risk applications (like medical AI) to meet strict security and accuracy standards. As for AI regulation in the US, the situation is a bit more in flux. The Biden Administration passed EO 14410, which established new standards for the use of AI, focusing on safety and equity for all Americans. The Trump Administration recently rolled back this executive order. At the time of writing, replacement legislation hasn't been passed.

Both the EU AI Act and the former EO 14410 required organizations to monitor their system for biases and security vulnerabilities. For example, NIST guidelines (MS-2.11-002) require organizations deploying LLM models to "conduct fairness assessments to measure systemic bias." Similarly, the EU AI Act demands that developers of high-risk AI create a risk management system and monitor it for "appropriate levels of accuracy, robustness, and cybersecurity."

To meet these requirements, organizations can implement AI bias assessments or AI-focused pen tests. These programs can systematically evaluate systems for biases and/or security vulnerabilities, ensuring compliance.

How SaaS companies use crowdsourced security

Leading SaaS companies are implementing crowdsourced security solutions to bolster their security postures. Here are four examples:

ATLASSIAN

Atlassian helps over 107,000 organizations, including small startups and large enterprises like VISA and eBay, collaborate effectively. Atlassian's core products enable project tracking, information sharing, and communication, while its Marketplace hosts third-party apps that extend these capabilities.

However, as Atlassian scaled, its internal teams struggled to balance managing security programs with proactive risk mitigation. Therefore, Atlassian turned to crowdsourced security to expand its security team's capacity. It adopted two programs: an MBB to catch and prioritize vulnerabilities across its core products and quarterly bespoke methodology assessments for its third-party apps.

Through this dual approach, Atlassian accelerated vulnerability discovery across its entire ecosystem. The quarterly assessments alone revealed 116 vulnerabilities across hundreds of apps, of which 21% were crucial or high-severity. These results empowered Atlassian's security team to implement broad security improvements, thereby strengthening Atlassian's security posture.

okta

Okta is a leading provider of identity solutions for enterprises, which requires that it maintains the highest security standards to safeguard customer data. In 2015, Okta sought to augment its internal testing by launching an MBB program in partnership with Bugcrowd. This program significantly increased Okta's monthly testing volume by 3500 hours, equivalent to the output of two full-time resources, without dramatically increasing its spending. Today, Okta pairs the MBB with continuous internal testing to ensure comprehensive, robust security across all its products.

Rapyd

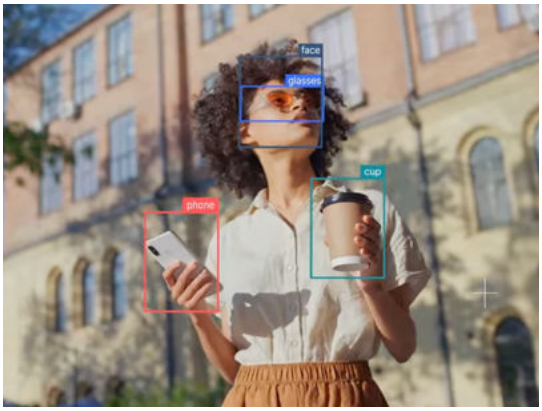
Rapyd powers global commerce for businesses worldwide by developing technology that removes the back-end complexities of cross-border transactions. As Rapyd grew, it wanted to elevate its security posture through continuous security testing, especially for its API products. Therefore, it turned to crowdsourced security as a solution, leveraging a private MBB and PTaaS assessments for continuous and point-in-time testing.

In 2023, this approach resulted in the discovery and remediation of 15 critical vulnerabilities, with an 18-day average time to remediation—13 days fewer than the industry average. Building on this success, Rapyd launched a public bug bounty program to support its continued growth and security needs.

Cloudinary

Cloudinary is a leading provider of media management solutions. Since its inception, it has taken security seriously, implementing multiple security measures, such as periodic pen testing and CVE scanners. However, this approach has not consistently yielded sufficient critical and actionable vulnerabilities to ensure comprehensive coverage.

Therefore, Cloudinary partnered with Bugcrowd to increase its testing throughput through a bug bounty program. Through this initiative, Cloudinary uncovered over 500 reported vulnerabilities from 360+ researchers. Armed with these findings, Cloudinary quickly remediated the critical and high-severity issues, strengthening its security posture and increasing customer loyalty by tangibly demonstrating its commitment to security.



Implementing crowdsourced security: Best practices

Implementing successful crowdsourced security programs for SaaS companies requires careful planning and transparent processes.

Here are four best practices SaaS companies should keep in mind when leveraging crowdsourced security:

1. Engage with hackers

Crowdsourced security thrives on strong collaboration between programs and hackers. It's essential to do your part to foster positive relationships and trust with the hacking community. Organizations that respond promptly to hackers and treat them as extensions of their teams quickly become hacker favorites.

2. Incentivize what matters most

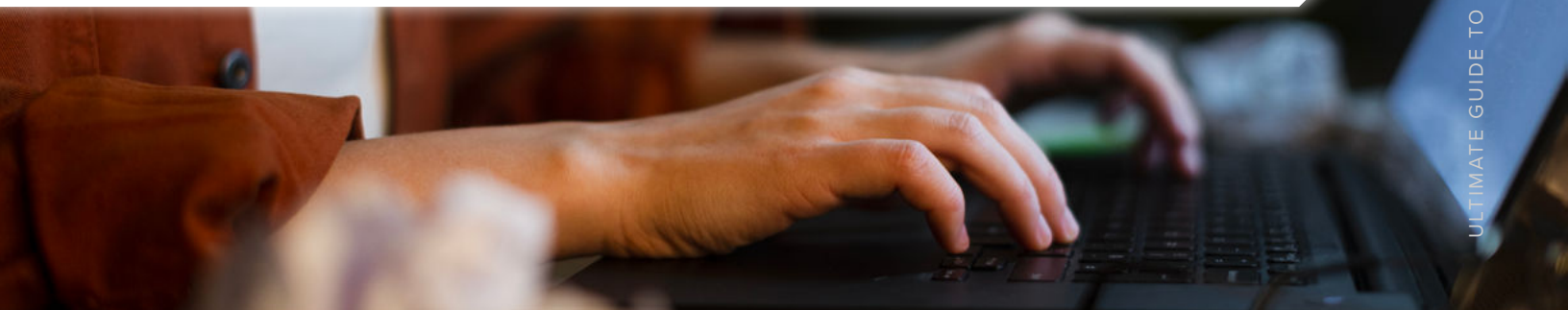
Incentives play a key role in the success and effectiveness of your crowdsourced security program. Implementing fair, market-rate payouts for high-impact vulnerabilities maximizes your chances of attracting the best talent to your program. If you're worried about cost, remember that remediating high-impact vulnerabilities can lead to substantial long-term cost savings. Consider this: The average total cost of a data breach is well over $4 million, but the median payout for a P1 bug in a SaaS application is only $2500.

3. Integrate with existing workflows and systems

For a crowdsourced security program to have maximal impact, it must be integrated into an organization's broader workflow, including DevOps and the software development life cycle. This enables teams to gain real-time visibility into security findings and remediate vulnerabilities efficiently as part of their normal development processes, resulting in safer products.

4. Leverage analytics and metrics for program improvement

When companies don't pay attention to crowdsourced security programs, their performance declines or plateaus. By reviewing reporting and analytics, organizations can continuously improve their programs, ensuring the effectiveness of their crowdsourced security strategies.



Evaluating crowdsourced security platforms

When evaluating potential crowdsourced security platforms, SaaS companies should choose those that can help them raise the bar of their security programs without breaking any budgets.

Here are a few factors to consider when doing a vendor evaluation:

- **Versatile platform**

  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 support multiple offensive security scenarios (simultaneously when needed) and adapt to meet emerging use cases.

- **Noise reduction**

  Effective validation and triage at scale require engineering expertise for rapid validation, prioritization, and remediation guidance. However, many vendors treat triage as an afterthought, creating bottlenecks and slowing down remediation. Look for platforms with expert engineer triage as a core service, not an add-on.

- **Advanced analytics, reporting, and recommendations**

  Continuous improvement is only possible with detailed analytics, reporting, benchmarking, and recommendations. Look for a platform that provides these by default rather than as an add-on.

- **Real-time visibility into vulnerabilities**

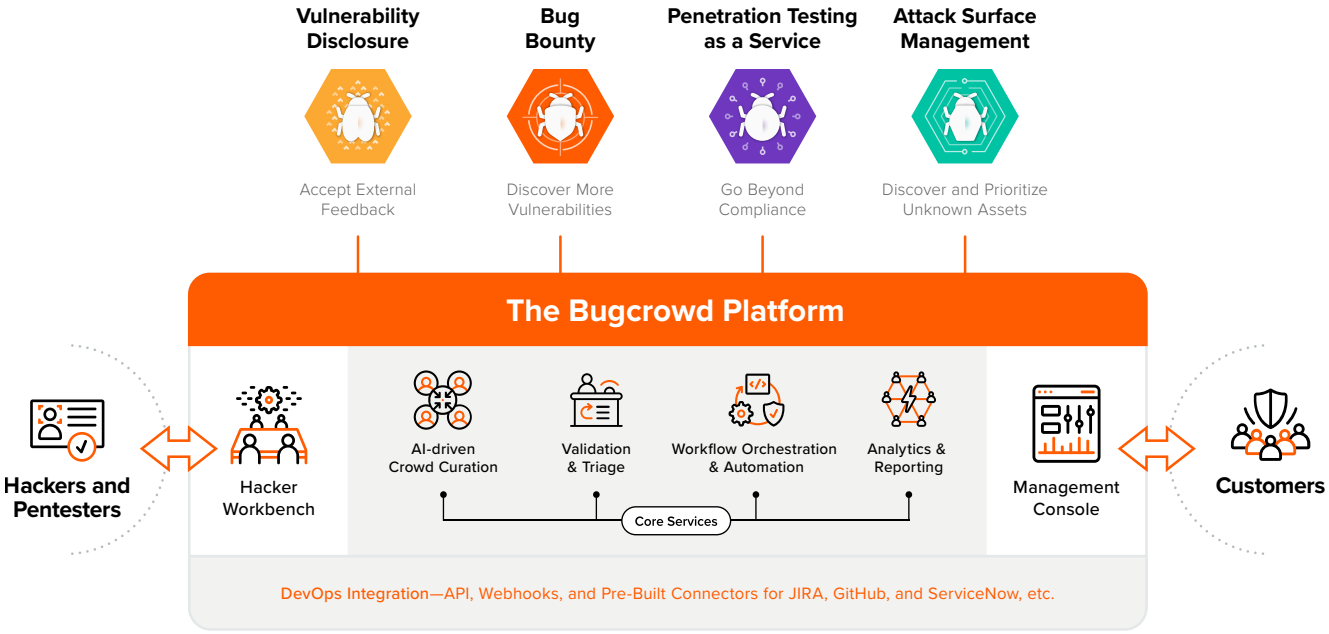
  The longer a critical vulnerability exists, the higher the chance that bad actors find it and exploit it. You want to look for a vendor that can provide day-one access to streaming vulnerabilities and issues as soon as they are discovered.

- **Scalable capacity with diverse expertise**

  The platform should provide unlimited testing capacity across hundreds of areas of expertise, such as cloud infrastructure, APIs, and LLMs. When needed, it should be able to quickly source specialists who meet specific requirements for skills, location, certifications, and track records.

About the Bugcrowd Platform

Bugcrowd frees SaaS organizations from the challenges of setting up and scaling their crowdsourced security strategies, regardless of their infrastructure's complexity. We have 12+ years of experience designing, launching, managing, and improving successful crowdsourced security and pen testing engagements for 1200+ customers of every size and industry.



✓

Augment your security team on demand

We provide unlimited hacker capacity across various skill sets (API, IoT, AI, cloud configuration, etc.), enabling SaaS organizations to quickly catch vulnerabilities arising from nested misconfigurations, complex user journeys, and other risks common to "digital natives" that only humans can assess.

✓

Remove risk while meeting compliance requirements

Our platform enables SaaS companies to proactively discover hidden critical vulnerabilities, helping them reduce risk and meet compliance requirements (e.g., PCI, SOC 2, and GDPR). Additionally, we offer many integrations with existing tools and processes to support remediation at DevOps speed.

✓

Improve security resilience

We use the best of human and data/AI intelligence to set up our customers for long-term security success. Our recommendations draw from a rich knowledge graph of vulnerabilities and assets, providing detailed remediation guidance. Additionally, we ensure each security engagement scales effectively to deliver lasting protection by aligning it to your organization's structure.

bugcrowd

PLATFORM 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.

Unleash Human Creativity for Proactive Security

Try Bugcrowd