2021

ULTIMATE GUIDE TO

Bug Bounty

bugcrowd

TABLE OF CONTENTS

INTRODUCTION

Developers make mistakes. In the last few years the tools and training designed to help avoid or quickly resolve coding errors **has exploded**, helping to eliminate common errors and reduce the number of vulnerabilities per web application by **over a third** between 2018 and 2019. Unfortunately, automated solutions are still woefully behind in surfacing the most critical and complex issues. According to Bugcrowd vulnerability data, one out of five valid vulnerabilities is now rated critical or high severity, with a whopping 73% increase in these categories between 2019 and 2020. As a result, developer-focused security solutions haven't quite absolved security teams from the burden of finding these vulnerabilities before malicious attackers. Unfortunately, with an increase in both attackers and attack surface, this has become increasingly more difficult.

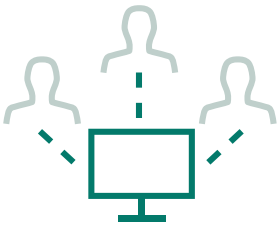
According to a recent ESG report, 66% of security teams feel attack surface management is significantly more challenging than it was just 2 years ago, citing increased attacker sophistication and inability to properly process relevant data as the top two reasons for this increase. And until recently, no testing solution was capable of addressing both points simultaneously. Penetration tests provide human-driven attack emulation, but aren't designed to be scaled (in cost or operation) to meet today's continuous development lifecycles. Automated scanners provide greater coverage for low-hanging fruit, but are riddled with noise. Neither have made much headway in demonstrating the ability to fully integrate into existing processes to provide meaningful, actionable intelligence.

EXECUTIVE SUMMARY

GROWING ATTACK SURFACE

50x more

online data in 2020 than in 2016, with up to 30% contained in unmonitored assets



SKILL SHORTAGE

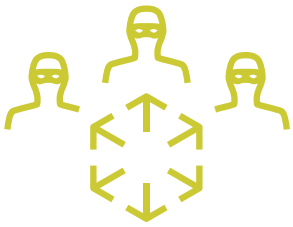
0% cybersecurity unemployment rate

with 1.8 million unfilled jobs by 2022

INEFFECTIVE SECURITY ARCHITECTURE

$32,600

mean cost of a two-week, third-party pen test, though just 30% find more than 10 vulnerabilities



DYNAMIC, MOTIVATED ADVERSARIES

5,000x

bigger than the surface web, the dark web is used by a growing cybercriminal community to trade tools and tactics

THE NEW MATH OF ATTACK SURFACE

Would you rather have many attackers and few defenders, or few attackers and many defenders? The obvious answer is few attackers and many defenders, but of course reality forces a different choice. Regardless of staff on the bench, organizations have increasingly invested in technology designed to augment or replicate human intelligence and intuition at scale. But why replicate? Why do we need human alternatives at all? Some point to reduced availability of security personnel—1.8 million open jobs by next year! But do seats remain vacant because the people don't exist, or because we can't afford them in the volumes necessary to defend against the rising population of skilled attackers? Maybe it's not the resource model that needs adjustment—but the cost. Crowdsourced security was born out of a need to tackle both.

THIS REPORT EXAMINES

- The evolution of crowdsourced security and the emergence of the Crowd (with a capital "C")
- What constitutes a "bug bounty," and how programs differ across organizations
- Why modern crowdsourced security platforms are best placed to close the gap between security and development
- Why organizations of all sizes are shifting away from pen test alternatives
- Top tips for launch, and how to grow and measure the impact of your bug bounty program
- What to ask a prospective bug bounty provider to ensure a good fit

DEFINING CROWDSOURCED SECURITY & BUG BOUNTIES

WHAT IS CROWDSOURCED SECURITY?

Like all forms of crowdsourcing, crowdsourced security unites a disparate set of individuals to work towards a common goal. In this case, the goal is to reduce risk for digitally connected businesses by surfacing the otherwise unknown vulnerabilities and attack surface. Crowdsourced security platforms (CSSPs), like Bugcrowd, are the connection and management layer in this equation. CSSPs develop, nurture, and continually assess the skills, experience, and performance of their community to match security researchers, pen testers, and ethical hackers to the testing opportunity best suited to their expertise. Once matched, CSSPs also ensure fluid vulnerability submission, noise reduction, and integration into software development lifecycles for rapid remediation.

> "By adding the power of the talented researcher community to our Product Security program, we've learned a lot about how people outside the company think about our products, additional scenarios where products can be at risk and what else we could do to protect our products. We've used this information to put a sharper focus on the areas of greatest risk, which has been invaluable to us as we scale."
>
> **COLEEN COOLIDGE, SEGMENT**

WHAT IS A BUG BOUNTY?

Previously, the term "bug bounty" was used synonymously with the term "crowdsourced security." With the arrival of additional ways to leverage the crowd, like pen testing and attack surface management, the two terms have now been decoupled. Crowdsourced security is a resourcing model, while bug bounty represents a particular way of incentivizing and engaging those resources. Bug bounties leverage a competitive model that encourages testing through potential for reward. If security researchers are the first to find a vulnerability within the scope defined, they are rewarded with monetary payments dependent on validity and impact. For example, if a security researcher uncovered a cross-site scripting vulnerability, but the same vulnerability was already noted by the customer's internal security team, or if it was uncovered by another researcher first, the individual is not rewarded, nor are they compensated for their time. In another example, two researchers may uncover different types of server security misconfigurations. If one is email spoofing and the other is use of default credentials, both are paid, but the latter would command a **higher rate** due to greater **potential business impact**. This model greatly reduces the average 'cost per vulnerability' versus other security solutions, and ensures that customers are truly only paying for value received.

THE HISTORY OF BUG BOUNTIES

Pinpointing the first bug bounty program isn't easy if the definition is simply, "A contest to find security flaws." In 1851, Charles Alfred Hobbs was paid 200 gold guineas by a lock manufacturer for **rising to the challenge** of picking one of their strongest locks. Flashing forward to the mid 90s and early 2000's, **Netscape, IDefense, Mozilla, Google, and Facebook** all had their own self-managed bug bounty programs, offering severity-based rewards to anyone that could identify vulnerabilities in their web applications. Companies with large enough security teams still do run their own bug bounty programs, but many more that **started as self-managed** eventually migrated to CSSPs for streamlined operations, and increased visibility to the Crowd.

WHO IS "THE CROWD"?

In crowdsourced security, "the Crowd" (with a capital C) is the term for all security researchers that work through CSSPs to help reduce risk of unknown vulnerabilities or attack surface. These individuals can be thought of as independent, but fully vetted contractors, engaging in the work that they find to be **most fulfilling, most lucrative, or both**. The Crowd is the life-blood of any crowdsourced security program, and the primary reason why this model is more cost-effective and value-laden than any other testing method.

Because researchers can subscribe to multiple platforms, total number registered is often less important than how they are matched and managed. This may be why some platforms boast a much **lower time to value**, and a higher signal-to-noise ratio over their competitors. Afterall, "there's plenty of fish in the sea" only works if all fish are equally skilled (and interested) in the same sort of security testing.

HOW IT WORKS

Bug bounty programs differ in operation across providers and organizations, but all follow roughly the same deployment sequence:

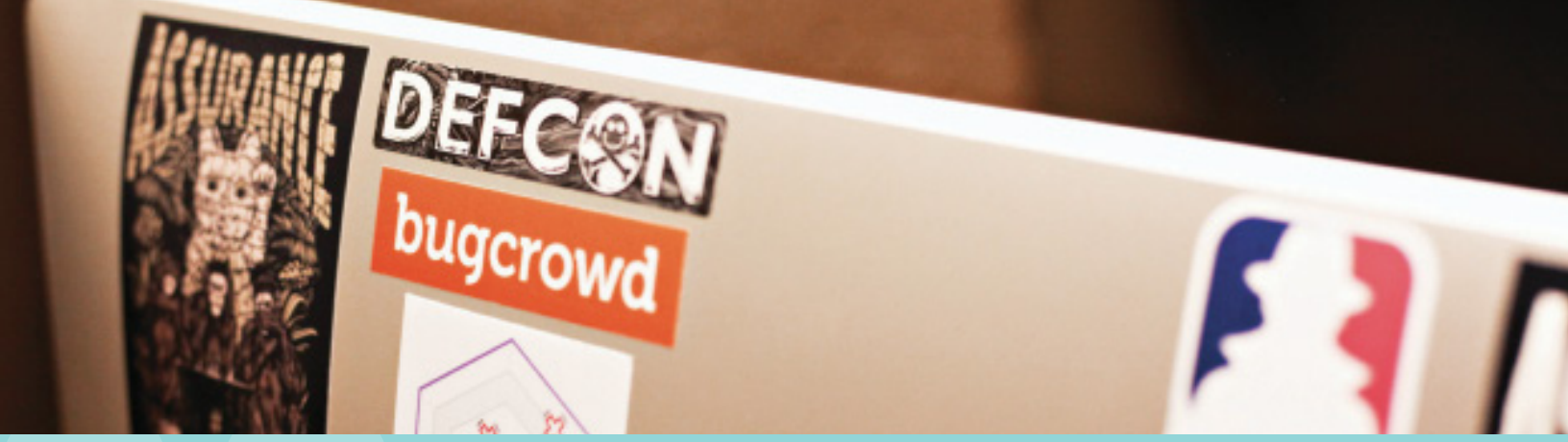
1. **Scope definition:** What assets need testing? Is it a single web application? Are there related mobile versions? Is there an API? Would you prefer to test in development or production? Are credentials required? All of these questions must be answered before any program can be initiated, and the sooner you resolve these, the sooner your program can launch.

2. **Researcher engagement:** Some platforms match resources based on skill, interest, ability, performance, and many other nuanced factors that influence program success. Others retain high-caliber full-time employees, which in turn makes allocation more dependent on availability. When evaluating a potential CSSP, it's important to dig into their matching methodology, to ensure it aligns with goals and expectations.

3. **Vulnerability submission:** Depending on whether the platform offers triage services, incoming submissions may be validated and prioritized according to severity. Some platforms offer this as a separate add-on cost, while others bake it into every deployment by default. In choosing which is right for you, be aware that even "invite-only" mode bug bounties result in significantly more vulnerabilities than you may be used to. Great triage services don't just eliminate noise, they also help prioritize submissions and help direct remediation.

4. **SDLC integration:** Most serious CSSPs will offer integrations into popular developer workflow tools like JIRA, GitHub, ServiceNow, and IBM Resilient. So it's important to ask whether the integration is robust enough to meet your team's most common use cases. In addition to these common developer tools, integrations into Slack and Trello can also improve communication and alerting workflows, while integrations with vulnerability management tools like Qualys can help contextualize and prioritize vulnerabilities from all of your discovery solutions.

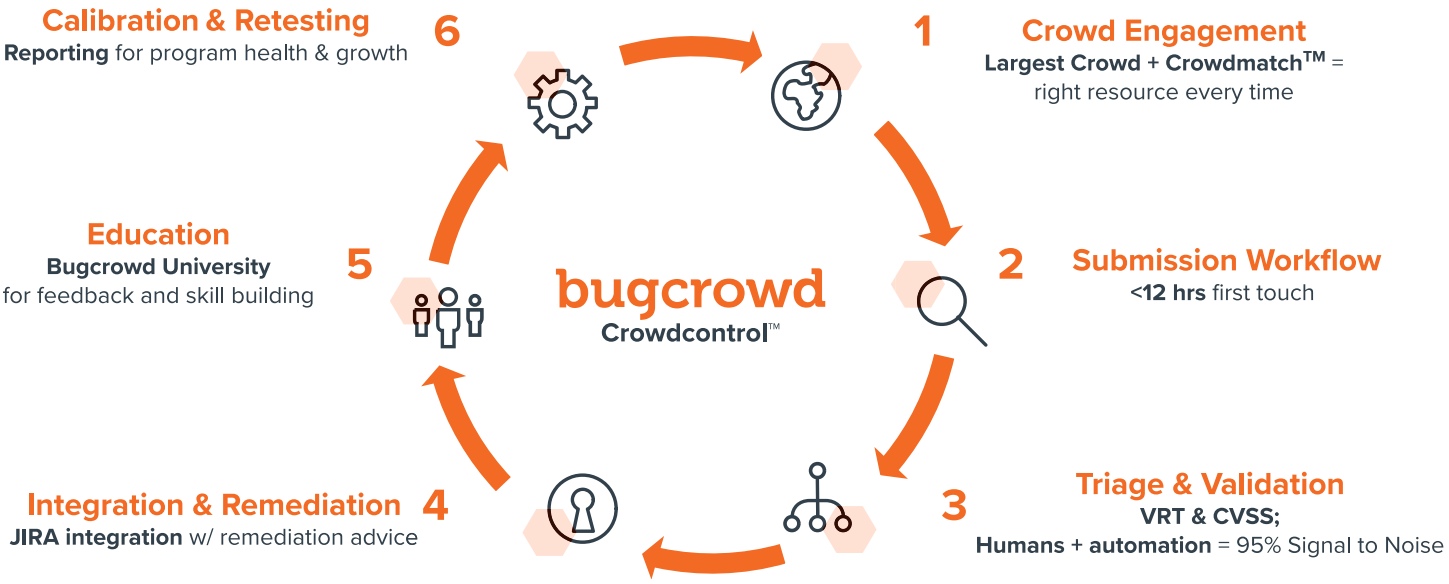
5. **Reward payout:** Valid, non-duplicate, and in-scope vulnerabilities are rewarded from a set-aside sum of money known as the "bounty pool." By allowing an intermediary to handle Crowd payments, organizations avoid the headaches of individual tax procedures that differ by state and country. Some CSSPs will take a cut of every bounty to manage this process, while others ensure all of this money goes directly to the researcher.



"The bug bounty program allows us to have eyes on new features as soon as they're implemented. It helps us detect issues quickly that aren't picked up by our other security processes. The coverage and scale of crowdsourced researchers means we can develop at a much faster pace, and with Bugcrowd dealing with the initial triage we're free to focus solely on valid submissions."

CHRISTIAN MARTORELLA, SECURITY ENGINEERING LEAD, SKYSCANNER

Bugcrowd takes additional steps to ensure it's closing the loop in vulnerability management, as illustrated below:



KEY BENEFITS OF BUG BOUNTY PROGRAMS

Bug bounties are a pay-for-results approach to proactive security testing designed to maximize discovery of high-impact vulnerabilities. Through managed bug bounty programs, organizations are given access to thousands of highly skilled and thoroughly vetted security researchers ready to help organizations find vulnerabilities other tools miss. The global nature of the Crowd means 24/7 talent availability, with launch timelines that blow traditional utilization-based models out of the water. Platform-powered solutions also include 24/7 vulnerability visibility and reporting, high-touch researcher management, and seamless business process integration with your development team's favorite ticketing and vulnerability management solutions.

OTHER KEY BENEFITS INCLUDE:

SHARED ACCESS TO TOP TALENT

The crowdsourced model enables all participants to share the value of something impossible to replicate alone. Bug bounties provide an elastic workforce when you need it, not when you don't.

RAPID LAUNCH AND TIME TO VALUE

A global network of hundreds of thousands of researchers operating in a pay-for-finding model drastically reduces time to launch. A competitive first-to-find incentivization layer also expedites time to find truly impactful bugs.

CONTINUOUS COVERAGE

Not paying per head or per hour means you can afford to have a testing practice that matches today's agile development cycles. Attackers don't take a day off, why should your security program?

UNIQUE SKILLS ON DEMAND

You have a great in-house team, but they're no match for a global team of researchers. The Crowd offers the largest rolodex of vetted, ranked, and highly active researchers with infinite combinations of skill and experience.

RAPID RISK REDUCTION

Competitive, incentive-based testing motivates researchers to think creatively and find high-impact vulnerabilities that present the most risk to the business.

LOWER OPERATIONAL OVERHEAD

No software or virtual appliances to install. Bug bounty providers are cloud-based, and integrate directly into your existing SDLC. Managed solutions also reduce resource drain through triage and prioritization.

BEST VALUE FOR MONEY

A results-driven model means you only pay for valid vulnerabilities, and not for the time or effort it took to find them. High-impact vulnerabilities command higher reward than those ranked as less severe.

REAL-TIME RESULTS

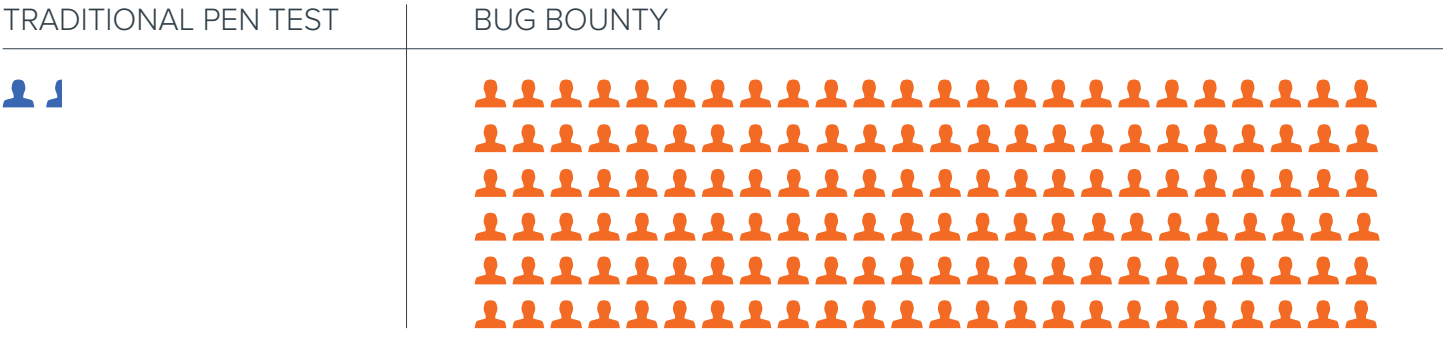
Modern bug bounty providers enable real-time vulnerability view directly in-platform. See and fix your biggest threats today, not weeks later as with traditional testing methods.

WHY SECURITY TEAMS ARE SHIFTING FROM TRADITIONAL TESTING TO BUG BOUNTIES

Crowdsourced security isn't competing against traditional pen testing. It's eliminating it. And it has nothing to do with the talent, support, or experience—it's the model. Two people, two weeks, every two quarters just doesn't make sense in today's agile development world. With an **average cost of $32,000** per pen test, the only way for this model to survive is to reduce caliber of testing talent, reduce frequency, or lengthen time to launch. All options negatively impact a customer's security risk, so it's unrealistic to expect this approach to last much longer. Let's look at what's changed in the last 3-5 years:

1. **Two testers for two weeks is no longer the only cost-effective option:** We haven't always had the technology to pool, parse, and pair the collective creativity of hundreds of thousands of security researchers. With the advances offered by modern crowdsourced security platforms, it's now possible to match, manage, and motivate the right talent for every testing engagement, without paying per-head or per-hour.

SHOULD THE COST OF HUNDREDS OF TESTERS REALLY BE THE SAME AS JUST TWO?



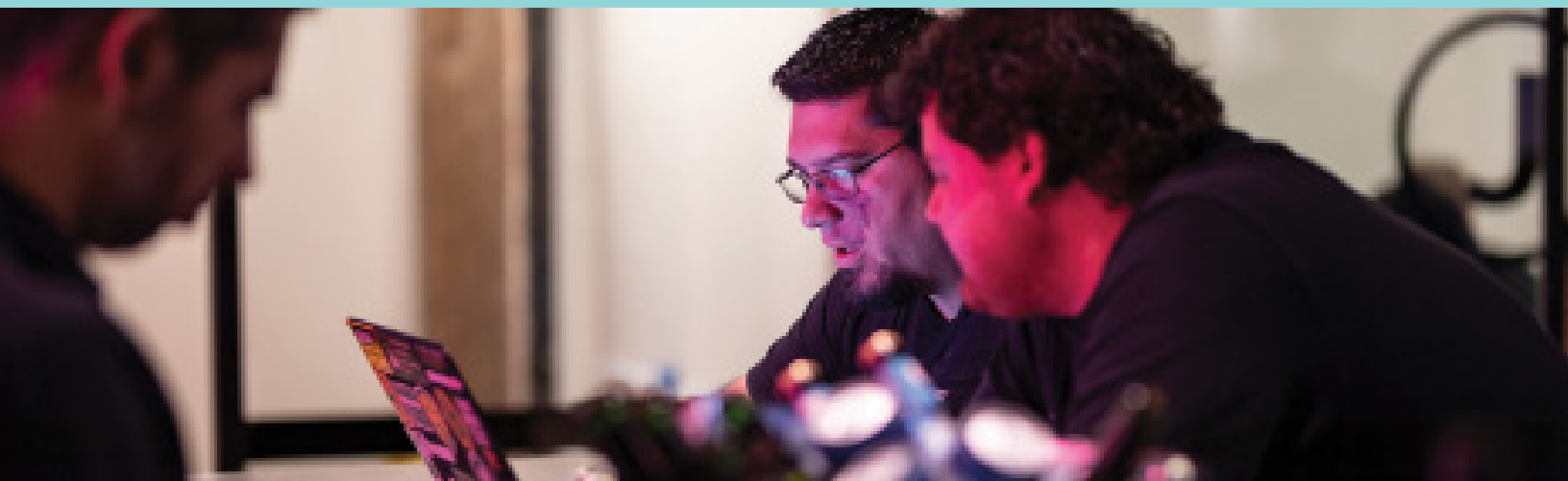
2 **There is no security skills gap:** Testing talent is available all around the world, so the "gap" may instead be in access to the right security skills, when and where you need them. Traditional firms employ full-time testers, limiting the number they can afford to retain. Salary cost is one matter, but the cost of someone "on the bench" is quite another. Utilization targets increase incentive to put less skilled pentesters on projects that don't suit their experience. Billable for the firm doesn't mean valuable for the customer. Bug bounties leverage a pay-for-results model that only rewards valid submissions, not time spent testing. This enables CSSPs to work with hundreds of thousands of researchers, multiplying the set of skills and experience available to any customer, at any time.

BUG BOUNTIES OFFER THOUSANDS OF TESTERS WITH A VARIETY OF SKILLS:

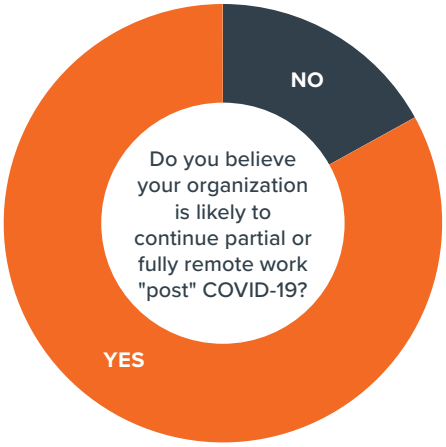
3 **The latest scanning technology isn't enough:** Traditional firms use automated scanners to clear low-hanging fruit. The bad news? They're already out of date, and you're not the only one using them. Attackers have the time and motivation to develop and frequently update their own tooling based on things they see every day. Commercially available varieties are often far behind the curve, making them a futile defense against savvy attackers. The good news? Security researchers have the same skills as attackers but use those powers for good. Many **develop the same tooling**, with innovation driven primarily by the competitive, pay-for-finding nature of bug bounty programs.

"Automation in discovering and reducing attack surface is crucial for tackling this problem at scale. I've **developed several myself** and use another dozen or so open source varieties."

MICHAEL "CODINGO" SKELTON, HACKER & GLOBAL HEAD OF SECURITY OPERATIONS AND RESEARCHER ENABLEMENT, BUGCROWD



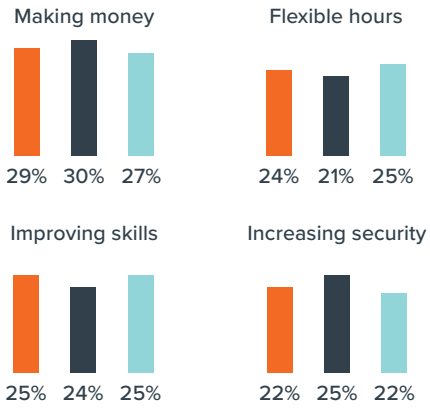
4 **In-person is out:** The 2020 Coronavirus Pandemic took a toll on in-person testing firms, and drastically changed how businesses think about remote work. In fact, **83% of security** professionals stated that their organization would remain partially or fully remote indefinitely, with 85% planning to prioritize remote testing over in-person alternatives as a result.



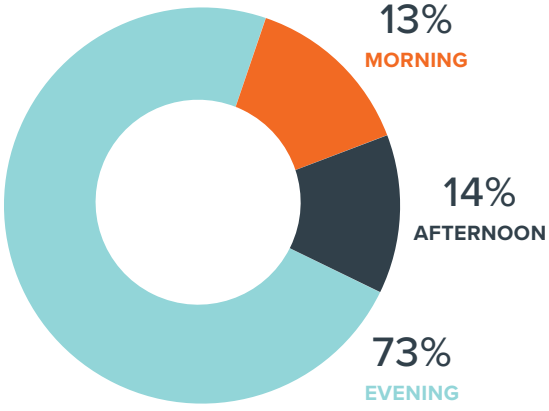
5 **Top talent wants to test on their time:** Millennials and Gen-Z are set to consume **75% of the global workforce** in the next few years. With this shift comes additional appetite, and opportunity for achieving better work-life balance. Flexible working hours are a **top point of value** for elite security researchers, and unlike typical 9-5 firms, bug bounties offer the flexibility to work across time zones, over weekends, before full-time jobs, after family dinners, or anytime that suits personal and professional needs.

RESULTS FROM BUGCROWD'S 2020 INSIDE THE MIND OF A HACKER REPORT, REFLECTING 3,493 HACKER VOICES

MOST IMPORTANT ISSUES FOR HACKERS



TIME SPENT HACKING BY TIME OF DAY



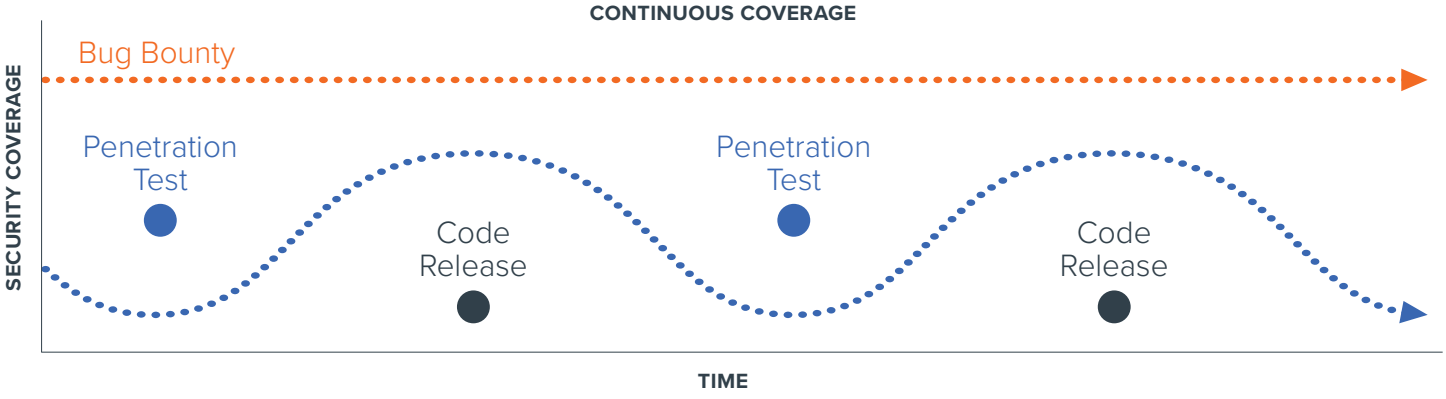
19% ↑
more hacking on Saturdays

LEGEND: Regulars Elite Newcomers

6 **Traditional firms can accommodate remote work, but CSSPs were built for it:** CSSPs were designed for remote-first work, enabling them to provide coverage during tumultuous times, while also offering an opportunity to re-examine the things that make remote testing unique and valuable. Security teams can now benefit from asynchronous work, round-the-clock testing, democratization of opportunity, and increased diversity of geography, education, skills, and experience.

BUGCROWD SECURITY RESEARCHERS REPRESENT A VARIETY OF BACKGROUNDS AND LIVE ALL AROUND THE WORLD

7 **Periodic pen testing is for periodic development:** When code changes were infrequent, bi-annual testing worked, and cost and coverage could remain relatively balanced. Times have changed. Developers now have the tools to launch and integrate new code with never-before-possible speed and efficiency. Pay-per-hour testing models now force a choice between cost and coverage. Bug bounties provide a more cost-effective means of infusing critical human insights, at scale, on a continuous basis.



8 **You're not the only one with a lot of tools:** Pen tests provide a list of vulnerabilities and exploitation details, but often lack the "so what/then what" that already tool-fatigued developers need to action results. Crowdsourced security platforms plug directly into software development lifecycles through integrations like JIRA and GitHub to present mission-critical vulnerabilities for prioritized remediation. Some bug bounty programs, like those offered through Bugcrowd, even provide remediation advice and re-testing to help fix, and make sure it sticks.

7x more attacks on IoT devices in the last 3 years

65% of vulnerabilities are in web application code

20% of valid vulnerabilities are high or critical severity

"It's huge to be able to directly push vulnerabilities into our Jira queue. We don't have to treat it any differently, depending on what part of our application is affected, a ticket is created and tasked to the team responsible for building it."

MARTIN RUES, CISO OUTREACH

"Bugcrowd gives us the ability to rapidly analyze a situation using global perspectives from hackers — who already understand how our applications work — that collectively augment their unique backgrounds and sociocultural influences to keep us ahead of cybercriminals."

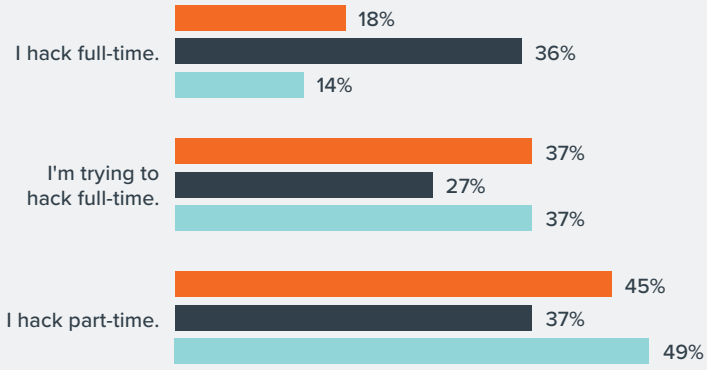
ADRIAN LUDWIG, CISO, ATLASSIAN

WHAT MOTIVATES RESEARCHERS?

Security researchers go by a variety of names (researchers, ethical hackers, hackers, security superheroes), but all share one critical feature—a desire to improve the lives of their customers, families, and themselves. **61% hack for personal development**, while many already-elite hackers are primarily motivated by the ability to make the world a safer place. Only 36% of elite hackers hack full-time, while the majority split hours between full-time employment as analysts, engineers, and even CISOs. The bug bounty community is a global group of well-intentioned individuals, from all walks of life, with diverse backgrounds, technical skills and expertise. This diversity is what makes bug bounties so impactful—the ability to connect uniquely skilled individuals with organizations that need fresh perspectives.

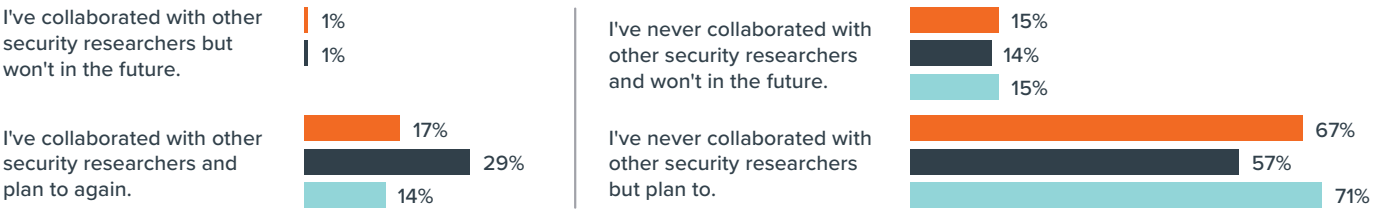
LEGEND: Regulars Elite Newcomers

EMPLOYMENT STATUS OF HACKERS



EARNING EXPECTATIONS AMONG HACKERS GOING FULL-TIME

COLLABORATION AMONG HACKERS



SCALING THE TRUST MODEL

Ten years ago, a handshake and a background check were all that stood between aspiring pentesters and your data. Trust was binary, fixed, and assumed by employment. But times have changed. Bug bounty programs have provided us the opportunity to think critically about how trust is defined, measured, allocated, and revoked. Does a background check make someone more trustworthy than 3,000+ vulnerability submissions? For some, yes. Others would say the promise of reward serves as a greater incentive to follow the rules. And that's ok. Modern bug bounty programs now have the technology to dynamically assess talent by both traditional measures of trust, as well as those that additionally consider performance and behavior.

CODE OF CONDUCT

While each platform differs in how they allocate and manage trust, many start similarly, with a pre-program agreement. Researchers on the Bugcrowd platform, for example, must agree to our **Standard Disclosure Terms**, which includes a charter to do no harm in testing, nor in subsequent communications. *Note: This is similar to what would be called a Non-Disclosure Agreement, but oftentimes customers choose to work with researchers to safely disclose resolved findings for the good of all involved.* In addition to this understanding, Bugcrowd researchers also agree to abide by our **Code of Conduct**, which outlines the expected behavior of all Bugcrowd community members both on and off platform.

"We looked at the bug bounty program as a key mechanism for taking our security posture to the next level. By leveraging a community of security researchers to find some of those obscure issues no one else has found. This is the message that convinced our executives to support the program."

SHIVAUN ALBRIGHT, CHIEF TECHNOLOGIST, PRINT SECURITY, HP

MEASURES OF TRUST

There are several ways CSSPs assess trust:

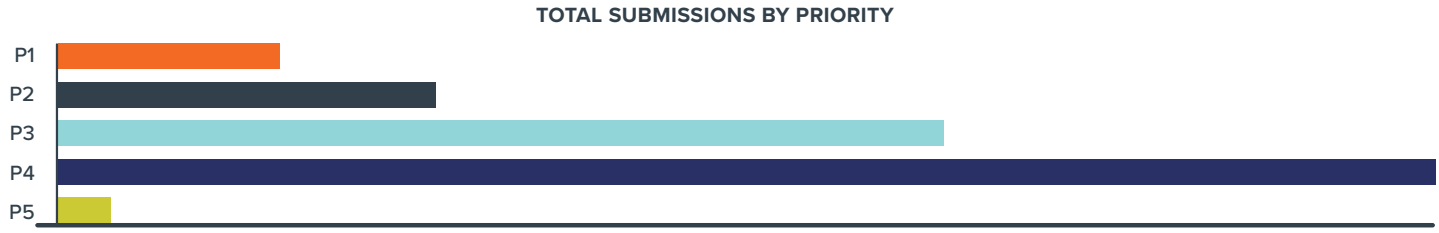
1. **Background checks:** Background checks look for felony and major misdemeanor criminal convictions at the country, state, and federal level, as well as sex offender registries and international watch lists. Researchers must provide their full name, email, and countries they have lived in the last 7 years. While some platforms background check all of their researchers, Bugcrowd takes the reverse approach—only researchers that have proven themselves to be both skilled and professional are invited to complete a confidential criminal background check if they so choose. This approach ensures that participants in programs requiring background checks also comprise our most elite hackers.

2. **ID-verification:** ID-verification is sometimes required to ensure researchers are who they say they are and operating from the locations that we expect. Bugcrowd researchers can choose to be verified through a service known as NetVerify. Researchers initiate this process by uploading a picture of their face and photo ID. NetVerify then uses this information to validate identity and confirm location. This is useful for programs that require only nationals are invited, but it also helps researchers are not operating from any areas on the **OFAC global banned list**.

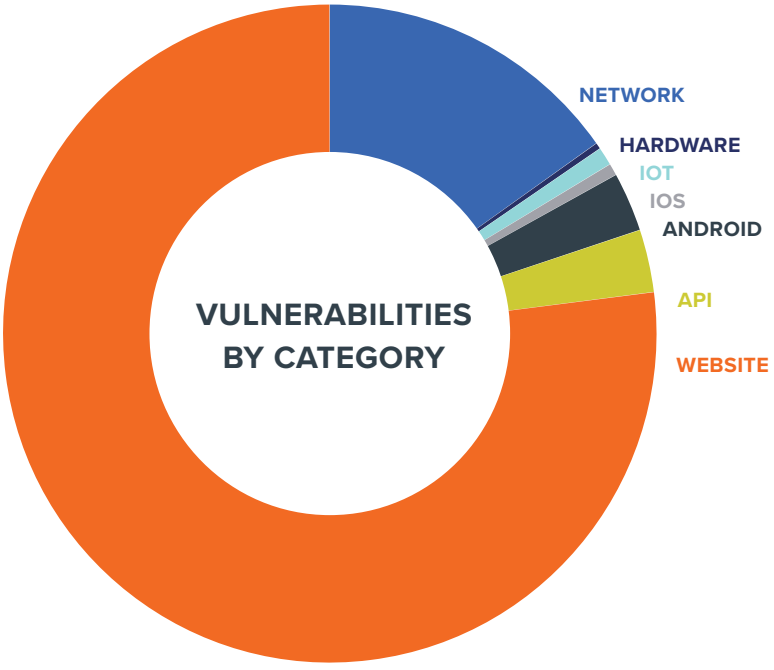
3. **Behavior/communication:** Like security testing, trust is not a point-in-time assessment. It is based on a holistic, and continuous view of a person's behavior and interactions. Bugcrowd's Researcher Operations team maintains vigilance over every active researcher's interactions both on and off platform, in order to address any gaps or de-escalate misunderstandings. Just as a full-time employee that can be removed for egregious behavior on social platforms, so too can a member of the Crowd be banned from individual programs, or the platform as a whole.

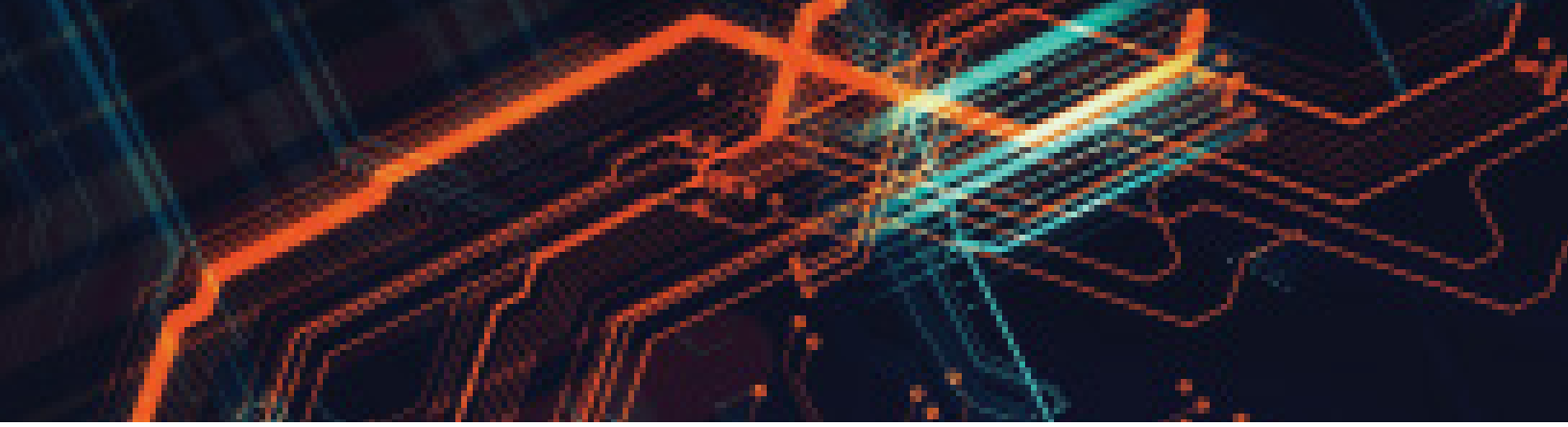
THE RESULTS

Bug bounty programs are increasing in popularity, scope, average rewards, and total findings across all industries from government and healthcare to tech and financial services. Valid submissions are up 30% for bug bounties alone, with 20% of valid submissions categorized as critical or high severity. The volume of critical vulnerabilities surfaced in bug bounty programs is also up from last year—by 48%. And bounty hunters aren't just hacking more, they're sharpening their skills. 2020 revealed the lowest average time to find for bug bounty programs—(75% faster than last year), as well as the greatest drop in ratio of invalid to valid vulnerabilities (13 percentage points lower).



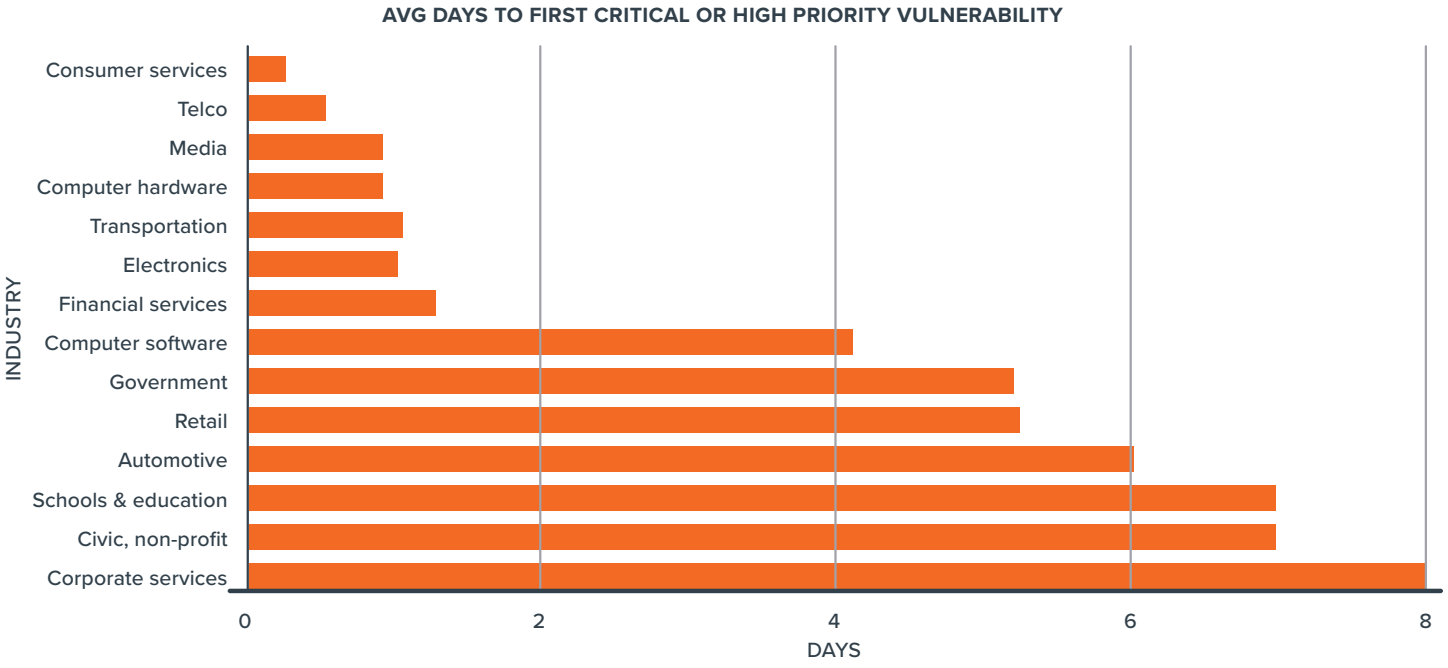
Web apps are still responsible for the majority of vulnerabilities, but other categories are gaining ground as security researcher skillsets diversify to stay competitive in an increasingly crowded space. In the last year Bugcrowd saw submissions to all targets increase, though notably, API vulnerabilities doubled, while those found in Android targets more than tripled.





Bugcrowd prides itself on the industry's best program matching technology and diligent program management. We believe these traits are illustrated best by our high signal-to-noise ratio (95%), as well as both the number and ratio of high-value submissions to each target, and the time it takes to uncover these submissions.

We believe having the right people on the program is the #1 accelerator of program value. The following table represents a sampling of industries that use Bugcrowd for private, on-demand bug bounty programs, along with the average time it takes researchers on that program to surface the first critical or high severity vulnerability.



"What excites me is the process of learning, not the outcome. I feel participating in every bug bounty program teaches me something new and fuels my desire to keep going. Plus, I love that moment when I get an email from Bugcrowd letting me know a bug has been triaged, it feels very rewarding."

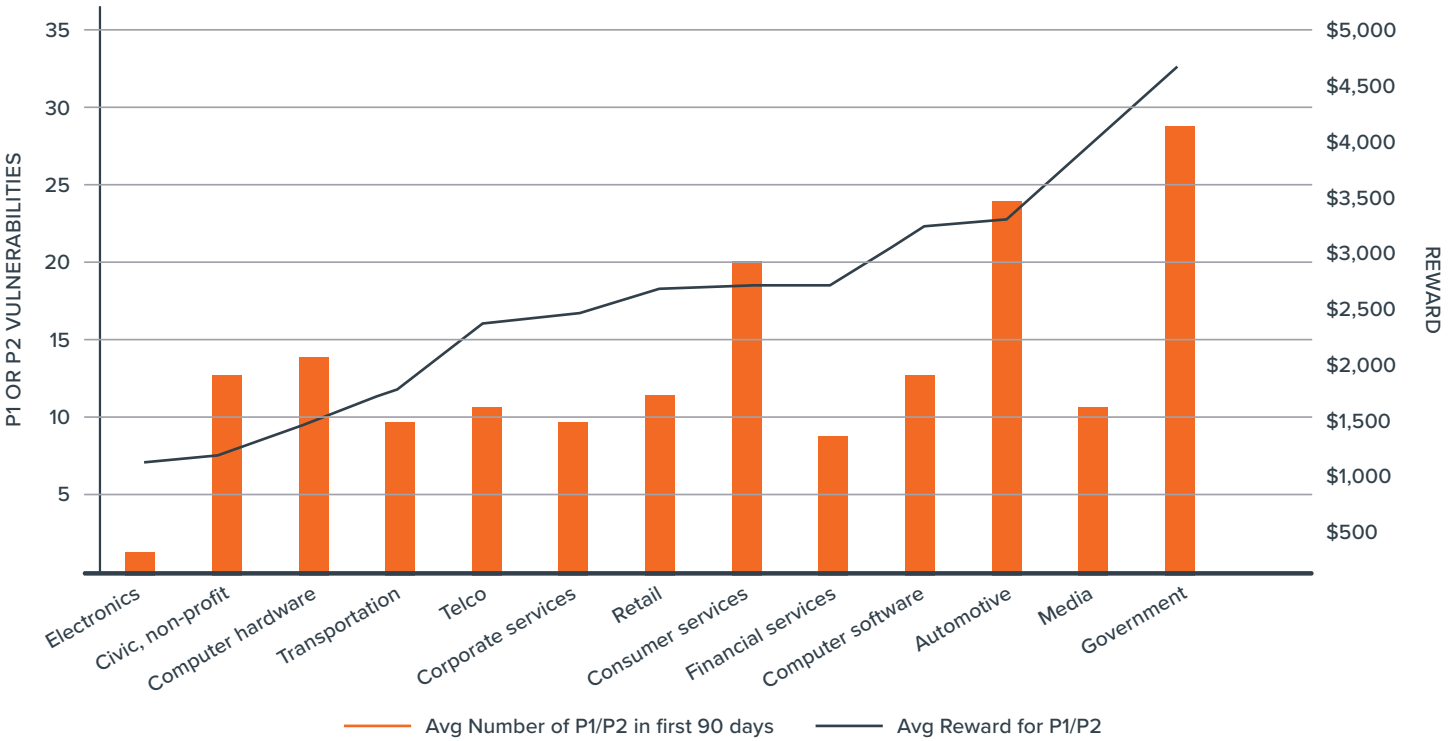
MICO

"Bug bounties give me the opportunity to work with some great companies, learn about their business models, products and technologies. Along with making the web more secure, I get to learn something new every day."

SYNTAXERROR

Of course, many factors influence this number beyond the caliber of talent engaged. Industries with highly hardened targets might take longer to crack, while industries with softer targets but lower incentives may be unable to attract the right talent in a timely manner. The next graph shows the correlation between the average number of critical and high severity vulnerabilities surfaced in the first 90 days, versus the average reward amount offered for those same vulnerability categories. Generally, higher rewards attract higher quality talent. Of course, outliers can occur, as is the case with non-profit organizations that hackers may donate their time to, or industries like hospitals and medical centers that historically offer low rewards but also have incredibly soft targets where critical vulnerabilities abound.

AVG NUMBER OF CRITICAL VULNERABILITIES IN FIRST 90 DAYS VS. REWARD OFFERED



"The biggest benefit we see from Bugcrowd is the team's ability to help in managing the bug bounty program so that once reports get to our security team, the are already deduped, validated and triaged. All our security team has to do is fix the bug. Bugcrowd has the best managed services."

ED BELLIS, CO-FOUNDER, CTO, KENNA SECURITY

READY TO GET STARTED?

Bug Bounty programs can take on many different forms depending on your organization's goals, budget, testing timelines, and interest in specific skills. Before engaging with a bug bounty provider, ask yourself these questions:

SELF-MANAGED OR MANAGED?

While a few large enterprises do have the team in place to manage their own bug bounty programs, these are usually highly visible, well-known, and reputable brands that can attract the attention of the broader security community. Organizations of all sizes typically opt for managed programs for a few reasons:

1. **Payment processing:** This can be a nightmare for even the largest organizations to manage, because it does involve draining resources in departments outside of Security, like Finance. Managing who gets paid when, and ensuring tax forms are provisioned for each, is no easy task.

2. **Relationship management:** Like all communities, every member of the Crowd has their own unique way of interacting, hunting, and communicating that is often more an exercise in psychology than it is in operations. Most platform providers typically employ a dedicated team of experts that either come from the community or are well-trained in the nuanced issues that security researchers face. This can drastically reduce the chance of miscommunication or misunderstanding between two parties.

3. **Triage and Prioritization:** CSSPs that offer this service drastically reduce the burden of vulnerability validation and prioritization. Some platforms enable customers to perform their own triage, though others prefer to steer clear of this option for one specific reason. CSSPs put an enormous amount of time into caring for the researcher community and ensuring that their needs are met. Without an objective intermediary, relationships can sour, resulting in a sudden drop in engagement, that can spread *quickly* throughout the community. For example, a Bugcrowd customer in the communications space began their bug bounty program self-managed, but failed to assign competitive payout rates, and were lax in their responses to submissions. This resulted in a sudden drop in engagement, with just 4 P1s over two years. After switching to Bugcrowd's managed model, they received 50 P1s (critical severity), and 90 P2s (high severity) in the following two years.

Choosing to partner on your bug bounty program is the right choice for most organizations, but it can be daunting! That's why we've included a handy checklist at the back of this guide to help you choose the right partner.

If you decide to go the self-managed route, it's important you build a team with the following skills:

- **Technical depth:** Ability to replicate vulnerability exploitation to ensure validity
- **VRT or CVSS expertise:** Ability to properly assign categorization, and associated reward
- **Strong communication skills:** Ability to balance two sometimes conflicting perspectives and needs
- **Patience:** Triage is quite repetitive in nature, but requires constant attention to detail, which can lead to burnout on your team. Researchers also often require constant communication, which can leave those responsible feeling more like a Help Desk than a valued security engineer.
- **Commitment to security above all else:** Escalations of valid vulnerabilities that aren't being addressed sometimes require a bit of tough love to push through to acceptance and remediation.
- **Marketing manager:** For ensuring your program is visible to all of the right talent

Even with such a team, sustaining success in the long run may prove challenging without previous experience managing bounty programs. Unfortunately, engaging the Crowd isn't something you'll get many chances to get right.

> "We wanted to do something more focused around genuine security than just about checking a box for some audit. We needed a process that offers a more real-world approach."
>
> **SHAN LEE, CHIEF INFORMATION SECURITY OFFICER, TRANSFERWISE**

IN SCOPE OR OUT OF SCOPE?

The first step in choosing which assets should be part of your bug bounty program is understanding your entire attack surface. Solutions like Bugcrowd Attack Surface Management (ASM) are a great place to start, if you're not sure where to start. ASM leverages a combination of software-based scanners and human reconnaissance experts to suss out which assets in your environment might have fallen off the radar, aren't receiving proper attention, and therefore might be more vulnerable than others.

By understanding your attack surface, you can more readily convey to researchers what is (and isn't) in scope, ensuring that you get the results you want. Do you have multiple web apps? APIs? All of these can go in "scope" for a single program, or you can divide them if you have teams to support each. Once you establish what's in scope, you're ready to begin writing the "bounty brief" that will help communicate to researchers your targets, priorities, exclusions, and incentive scheme.

STAGING OR PRODUCTION?

Now that you've determined what's in scope, it's time to consider where in your development lifecycle it's most appropriate for focused testing.

Where possible, we suggest utilizing pre-production/staging environments, as opposed to production. There are many reasons to consider this option, including reduced impact to customers, ease of credential provisioning for researchers, and much more:

- Researchers can help identify issues in new app versions before each release
- There's no chance of affecting users if the staging environment is made unstable from the volume and type of researcher testing
- It's typically far less expensive to fix a vulnerability identified in pre-production before wide spread availability.
- If there is a purchase point on the application, it's usually much easier to provision fake credit cards/SSNs/etc. in non-production environments
- It's typically easier to mass create staging credentials for researchers
- It's much easier to restrict access to only certain researchers (only allowing access from a specific IP address), thereby providing better visibility into researcher testing/coverage.

PUBLIC OR PRIVATE?

The power of crowdsourced security is power in numbers. While that can refer to the total number of people on your program, it also refers to the broader network of *available* talent. More thoroughly vetted, and continuously ranked security researchers means you'll always have the team that's best fit for your testing environment. Because more people on your program also means more vulnerabilities, many CSSPs including Bugcrowd recommend starting small, with invite-only access, until vulnerabilities reach a manageable level and you feel comfortable graduating to public access (if appropriate for your business).

Private Program: Invite-only programs which target a select group of researchers based on technical and business requirements. No one else in the community, or beyond, will be able to see details on, or access private programs.

Public Program: Anyone registered through your chosen CSSP can see, access, and work on public programs. Public programs typically have a much broader scope which allows for a wider range of potential vulnerabilities to be identified by a larger set of unique skills and experiences. Check out some of Bugcrowd's public programs on our **website**.

ON-DEMAND OR ONGOING?

While the structure of crowdsourced security programs enables continuous testing where it was previously not possible, it may be the case that testing or budget cycles limit you to only ~2-week testing sprints.

On-Demand: A time-boxed point in time testing engagement that may be run in isolation, or periodically throughout the year.

Continuous: An ongoing testing engagement that is best fit for high-value targets or agile development environments where the asset may face frequent change.

WHICH INTEGRATIONS MATTER MOST?

A strong vulnerability discovery solution is weak without a way to facilitate rapid remediation. While security teams aren't responsible for providing the fix, they are better served if they can make that process as easy as possible for the development team. Ensuring your CSSP can provide vulnerability-specific remediation advice and deciding which integrations matter most to your development team for presentation of that information is crucial. Most modern bug bounty platforms offer developer tool integrations like JIRA, GitHub, ServiceNow, Trello, and Slack, making it easier for security to enqueue prioritized vulnerabilities, and for developers to see what should be addressed first, how to do it, and whether anything else stands in the way. Context is key. As JIRA is the most common ticketing and management system for most users, it's important to make sure your CSSP can accommodate the following top three use cases:

Centralized JIRA security project: Appsec team has one "security" JIRA project to manage their security work. Having one security JIRA project between security and development is a great way to centralize work; it is simple to maintain as there is no logic needed to understand where tickets are created.

In Developer JIRA projects: Appsec team pushes security tickets into developer's JIRA projects while respecting developer's ownership. Enterprise organizations typically have more than one development team or business application, which requires more than one JIRA project.

Hybrid: A hybrid of both with one "security" project and a linked issue in developer's JIRA projects. The primary benefit of this approach is maintaining control if development makes edits. This provides an additional layer of accountability and visibility. This integration should be done in partnership with engineering so they are not surprised by these new tickets. It takes a partnership between engineering and security to help secure your organization and customers, which is why we have invested so much in this integration.

LONG-TERM SUCCESS

SETTING EXPECTATIONS

Bug bounties can greatly reduce risk of vulnerabilities to your organization. Leveraging a CSSP to help manage your program can relieve a lot of the burden. But this doesn't completely remove program owners from the equation. Bug bounty programs do take time, and a broader organizational commitment. It's important for you to have an open dialogue with your executive team about the implications of such a program. This could include potential impact to budget structure (to accommodate a variable bounty pool), as well as impact to engineering should a sudden influx of vulnerabilities be disruptive to current processes. Additionally, bug bounty program owners must commit to timely platform response, including accepting validated vulnerabilities, or addressing program issues raised by your CSSP.

CRAWL, WALK, RUN

Approaching your bug bounty program with "crawl/walk/run" in mind is a recipe for success for any organization, of any size. Big public launches drive press coverage and broader awareness, but that isn't always appropriate if you're not quite ready for that volume of vulnerabilities. Processing and paying is one matter, but once you know about the issues, you should also be prepared, and equipped to promptly resolve them.

Launch private bug bounty with limited scope

Transition to public program

Increase rewards, add targets, boost researcher engagement

GEARING UP FOR GROWTH

Iteration is an important part of any successful bug bounty program. What worked to fuel researcher engagement yesterday, might not work today. CSSPs like Bugcrowd are well versed in early identification of any growth inhibitors, and as a result will rely on three key "levers" to encourage long-term success:

1 **Evolve your scope:**

Re-evaluate your attack surface: Many programs start with publicly available web targets. As time goes on, it's important to explore your organization's full attack surface. Researchers are most committed to programs with varied and evolving scope.

Consider your product pipeline: New and recent product features or code changes are often overlooked for bug bounty inclusion. Working your bug program into any Security/Product interface can reduce chances that something is missed.

Review your bounty brief: If you have chosen to work with a bug bounty vendor, they'll be well-practiced in re-structuring your bounty brief to ensure your interests are being clearly communicated. Perhaps you were hoping for more testing in a certain area. If you're not explicit about it in your brief, it's possible researchers missed the information.

2 Keep up with reward rates:

Grow with your Program: The longer programs run, the higher rewards should be to reflect the increased difficulty of finding new vulnerabilities. Your CSSP can also provide insight into the market rate for vulnerabilities as they change over time. Don't forget that researchers can choose from many different programs, the right reward range can help you stay competitive.

Demonstrate Code Confidence: Increasing rewards typically signifies confidence in the products you've launched. Higher rewards attract more skilled researchers, who are happy to accept the challenge. "Hardened" targets with smaller scope should increase rewards to ensure proper attention from skilled researchers.

Highlight Areas of Interest: If your scope includes multiple targets, but you've recently updated code to one particular asset and want to ensure it's thoroughly tested, temporarily increasing rewards for that asset is likely to boost engagement

3 Focus on relationships:

Reduce Response Time: Response time is measured as the time between when a customer receives a triaged bug, to the time the submission is reviewed by the customer. Typically, customers should at least respond (accept or reject) submissions within one week.

Invest in Communication: Managed bug bounty programs thrive off of a very symbiotic relationship; researchers and customers must work together and understand one another's needs.

Act with Empathy: It's important to remember that your researchers are human and have families and lifestyles to support. Having a reputation of accepting vulnerabilities in a timely fashion helps researchers identify which programs they can rely on for timely payouts.

"Our bug bounty program is an important part of vulnerability management at ExpressVPN. We decided to join a crowdsourced program to get even more eyes on our products."

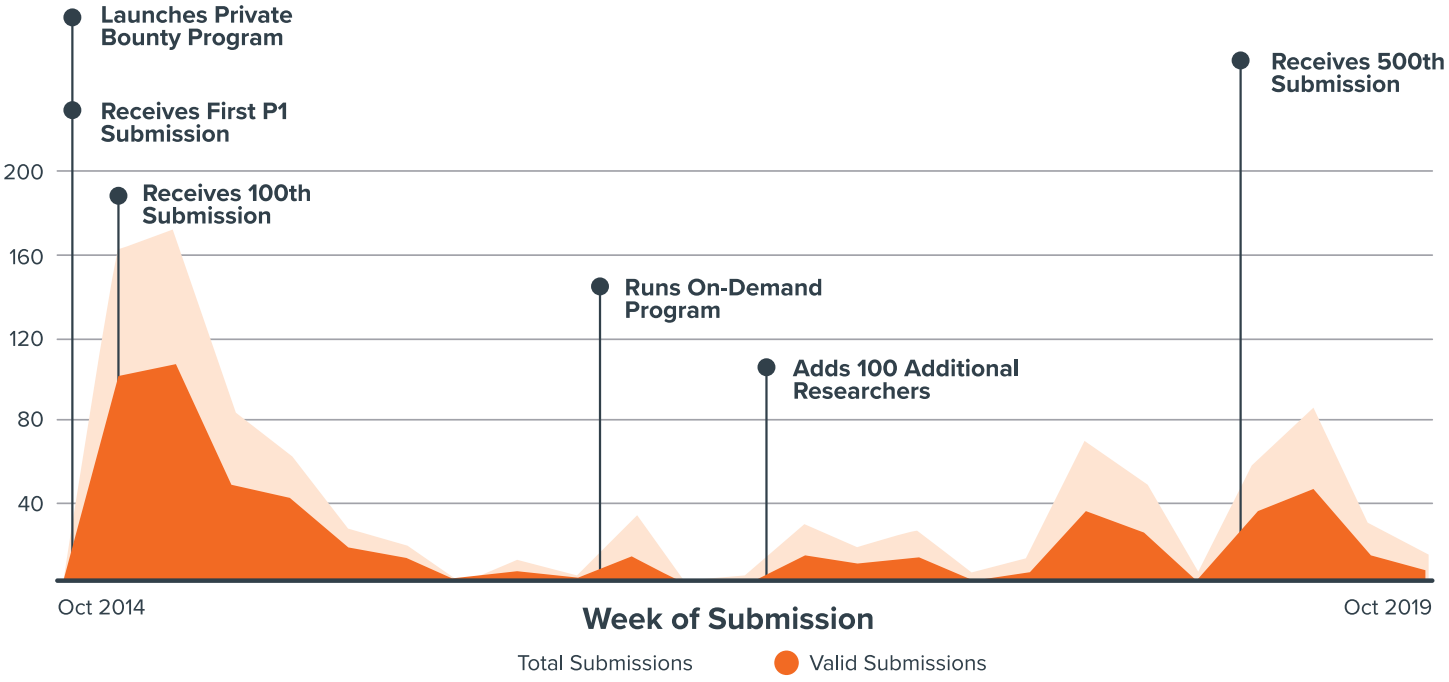
HAROLD LI, VICE PRESIDENT, EXPRESSVPN

The following depicts how these levers can positively impact researcher engagement and performance:

IOT

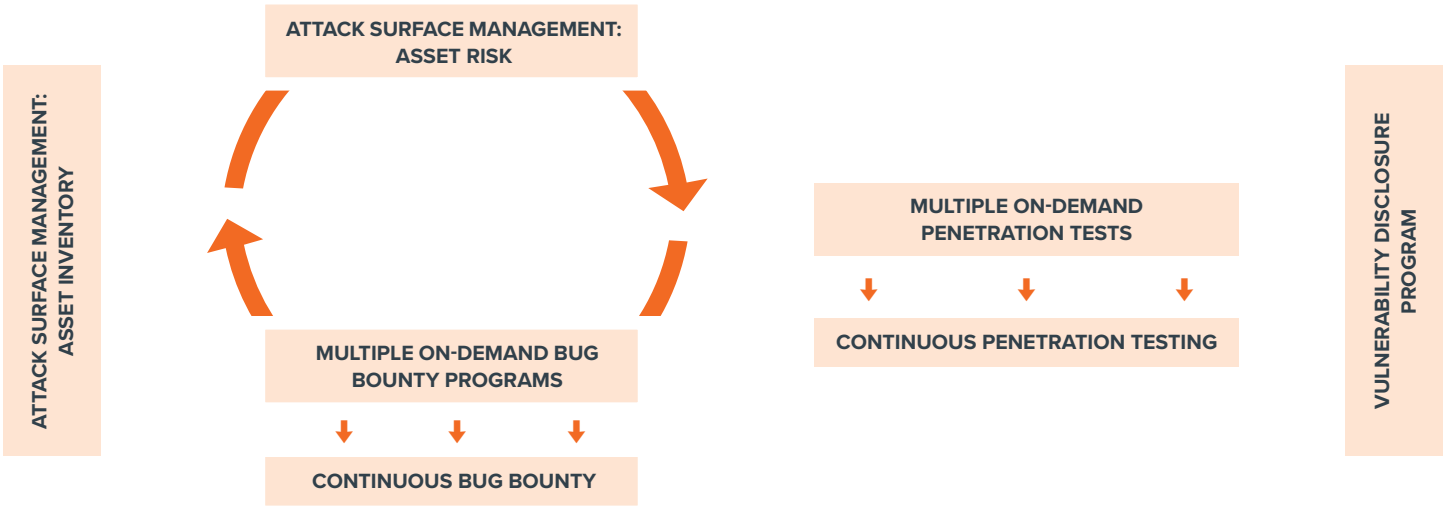
aruba
a Hewlett Packard Enterprise company

Launch: Oct 2014 (Private)
P1s: 204
P2s: 147
Rewards: $100–$5,000



BUG BOUNTY AS PART OF A LAYERED APPROACH TO SECURITY

Bug bounty programs aren't the only way to leverage the power of the Crowd. Bugcrowd offers a variety of complementary solutions to address more security testing use cases than any other provider:



PUBLIC AND PRIVATE BUG BOUNTY

Bug bounty programs enable organizations to incentivize trusted security researchers to continuously hunt for vulnerabilities across a variety of designated attack surfaces. Bugcrowd's fully managed approach comprises researcher matching, vulnerability prioritization, and program health monitoring.

- Top Talent: Access to thousands of uniquely skilled, trusted researchers motivated and incentivized to continuously hunt for vulnerabilities across a variety of attack surfaces.
- Rapid Risk Reduction: An incentive-based approach motivates researchers to think creatively and find high-impact vulnerabilities.
- Cost-Effective: A results-driven model ensures you pay for vulnerabilities that present a risk, and not the time or effort it took to find them.

VULNERABILITY DISCLOSURE PROGRAMS

Bugcrowd VDP provides a coordinated channel and framework to enable anyone, anywhere, to responsibly disclose security vulnerabilities found in publicly accessible assets. Bugcrowd's fully managed approach reduces noise, and accelerates remediation.

- Demonstrate Security Maturity: Build stakeholder confidence and trust by protecting digital assets and responding to known risks.
- Formalize Security Feedback: Create a channel for security feedback and a framework to manage vulnerabilities discovered by researchers.
- Meet Compliance Requirements: Align cybersecurity programs with best practices, as defined by the US Government, NIST, DOJ, FDA, and others.

CLASSIC AND NEXT GEN PEN TEST

Bugcrowd's Pen Test portfolio infuses platform-powered Crowd intelligence into both pay-per-project and pay-per-finding penetration testing. Testers follow a set methodology with QSAC-assessed final reporting to help meet compliance objectives.

- Continuous Coverage: Choose between on-demand or continuous testing styles, with options for vulnerability-based incentivization to increase coverage and reduce risk
- Faster Launch: Ditch scheduling delays with access to more skilled and available testers. Most programs launch in as little as 72 hours.
- Day 1 Vuln View: Don't wait until final report delivery to see what's wrong. Bugcrowd's platform provides visibility into vulnerabilities the second they are submitted.

ATTACK SURFACE MANAGEMENT

Bugcrowd's Attack Surface Management portfolio helps organizations reduce risk from unknown, or unprioritized assets that often become a primary target for attackers. Asset recon experts hunt for unseen assets, while a software-based solution continually scans for new connections and activity.

- Reduce Unknown Attack Surface: Find forgotten assets that scanners can't. Receive priority risk-ranking based on each asset's potential for vulnerability
- Continuous Scanning: Asset Inventory leverages a pre-indexed snapshot of the internet which continues to grow. New assets are added to your inventory as they are discovered and attributed
- Live Alerting: Receive alerts on high-risk events like open ports, or soon to be expired security certificates. Share findings with external teams like Marketing, Sales, and Product to ensure quick fixes

Want to learn more about how your organization can leverage crowdsourced security testing to start discovering and fixing high value vulnerabilities missed by traditional discovery methods? Start building your program today at **bugcrowd.com/try-bugcrowd**.