

bugcrowd

PRIORITY ONE

REPORT 2022



A year of vulnerabilities
in review and a look ahead

Contents

Executive Summary	3
<i>Report Highlights</i>	4
 Key Industry Trends	 5
<i>Long Tail of Vulnerabilities</i>	6
<i>Security as a Brand in FinServ</i>	6
<i>Rise in Incentives in Software</i>	6
<i>Government Adoption on the Fast Track</i>	6
<i>Top 10 Vulnerability Types</i>	7
<i>Lifecycle of Vulnerability Incentives</i>	8
 Key Vulnerability Trends	 9
<i>Ransomware Hits Main Street (and the Hounds are Released)</i>	10
<i>Attack Surfaces and Supply Chains Exposed</i>	10
<i>Use of N-days by APTs</i>	11
<i>From Penetration Testing, to Crowdsourced, to Multisourced</i>	11
<i>Policy Changes: Striving for Clarity</i>	12
 Bugcrowd Security Knowledge Platform™	 13

Executive Summary

Judging by activity on the Bugcrowd Security Knowledge Platform™ in 2021, growth in crowdsourced security carried over from 2020, driven by the shift to hybrid/remote workplaces and re-imagined supply chains during the global pandemic and the digital transformation that followed.

With the dust starting to settle but the cybersecurity skills gap still in force (with an estimated [2.7 million cybersecurity roles still to be filled](#) at the time of this writing), the data suggests that organizations are increasingly turning to the Bugcrowd platform's combination of data-driven insights, technology, and human intelligence (including the global security researcher community, aka "the Crowd") to address, as efficiently as possible, critical bugs they've incurred during the digital transformation process.

In the software and financial services sectors in particular, we have seen evidence of increases not only in activity as a function of clearing a long tail of security debt, but also in severity levels and the payouts made to incentivize their discovery.

In its [2021 cybersecurity report](#), Accenture found that the vast majority of respondents (81%, compared to 69% in 2020) believe that "the cost of staying ahead of attackers is unsustainable."

We believe that this perception of a losing battle, despite the billions of dollars spent collectively on cybersecurity technology, continued to fuel an interest in more innovative and proactive approaches, such as Bugcrowd, in 2021.

For this 2022 edition of the Priority One Report, we've analyzed the large amount of vulnerability data processed by the Bugcrowd Security Knowledge Platform™ throughout the third quarter of 2021 to uncover key insights about these trends, which we expect will continue into 2022. (Note: This time period does not capture the discovery of the massive Log4j vulnerability that was discovered in December 2021.) We also provide our point of view about key risks and policy drivers for security-minded organizations in 2021 based on direct customer experiences.

Finally, we've included some highlights from Bugcrowd's complementary flagship report, *Inside the Mind of a Hacker 2021*.

81%

believe that "the cost of staying ahead of attackers is unsustainable"

REPORT HIGHLIGHTS



24%

of all valid submissions were P1s or P2s



82%

Valid submissions increase in the FinServ sector



106%

Payouts increase in the FinServ sector



186%

P1 submissions increase in the FinServ sector



73%

Payouts increase in the Software sector



1000%

Total valid submissions increase in the Govt. sector



XSS was the most commonly identified vulnerability type



Ransomware went mainstream and governments responded



Penetration Testing entered a renaissance



Supply Chains became a primary attack surface



“Policy Fog” started to clear



N-days became the new 0-day vulnerability



Sensitive Data Exposure moved to #3 from #9 on the list of top 10 most commonly identified vulnerability types

KEY

Industry Trends

Putting a price on bugs

Last year's report noted an uptick in valid submissions as more companies turned to Bugcrowd for crowdsourced security. The 2021 data tells us that this growth was not a temporary spike, but rather a sustained shift brought on by

the security demands of our new hybrid work environment. That observation was supported by an increase in payouts relative to valid submissions in 2021—i.e., an increase in the perceived value of a bug.



"Within all groups, there are people who focus on complicated attack chains and business logic exploitations, then there are those who look for simpler issues, but usually in ways that others haven't thought of before—it really does take a crowd."

Casey Ellis • Bugcrowd Founder, Chairman, and CTO



LONG TAIL OF VULNERABILITIES

Global lockdowns and the associated shift to remote work led to a rush to put assets online in 2020, which led to an increase in vulnerabilities. Thus, security buyers invested heavily in incentivizing the Crowd to find critical ones, leading P1 and P2 submissions to make up 24% of all valid submissions for the year.

However, in some sectors, buyers' needs also evolved slightly in 2021 toward clearing residual security debt associated with digital transformation and the shift to hybrid working models. P3 submissions also grew year-on-year as the Crowd cleared a backlog of vulnerabilities brought about by the pandemic.

In Financial Services specifically, valid P1s and less critical submissions increased significantly. This demonstrated the sector's need to both incentivize the Crowd to find most critical vulnerabilities as well as clear security debt at the other end of the scale.

There were some interesting variations in the pattern in other sectors, as well.

SECURITY AS A BRAND IN FINSERV

Companies were forced to put a great deal of assets and services online in 2020 to keep their operations going during the global lockdowns. This accelerated digital transformations and meant that security posture became more important, as a greater share of revenue was now coming from online transactions.

Financial services companies had to move quickly on this issue given the sector's importance to businesses and consumers, with [64% of FinServ executives ranking cybersecurity as their top concern](#) in expected budget increases in 2021, per Deloitte.

This increased investment is supported by the fact that valid submissions, payouts, and P1s were up 82%, 106%, and 186%, respectively, on the Bugcrowd Platform.

In 2020, investment peaked during the second quarter, when significant rewards were paid out to secure financial companies' initial moves online.

This was buttressed by increased overall investment in 2021, rising quarter on quarter from a significant base, to further elevate security standards. By making this double investment in the Crowd, FinServ companies established a reputation for safety online to match the one they had carefully built up using bricks and mortar.

RISE IN INCENTIVES IN SOFTWARE

In the Software sector, a bellwether for the cybersecurity ecosystem as a whole, total payouts increased by 73%.

Digital transformation brought on by the pandemic caused a spike documented in last year's report, and these numbers have been sustained or grown. The more interesting change, however, has been the second-order effect from market forces: Uncovering hidden vulnerabilities, especially critical ones, provided tangible value to buyers and led them to invest more in the form of incentives (payouts) in 2021.











GOVERNMENT ADOPTION ON THE FAST TRACK

In Priority One 2020, we reported how global lockdowns were causing the Crowd to spend more time in front of screens, identifying the new vulnerabilities that were arising as the global economy shifted further online. Organizations that favored continuous coverage saw the benefits of these extra eyeballs and the increase in hacking hours.

In 2021, the Government sector was the main beneficiary of continuous engagement with the Crowd, with valid submissions up over 1000% year-on-year through Q3.

The vast majority of these submissions occurred in the third quarter, when government buyers turned on the taps for crowdsourced security in response to [new federal civilian agency directives](#) that, for example, make vulnerability disclosure a key requirement.

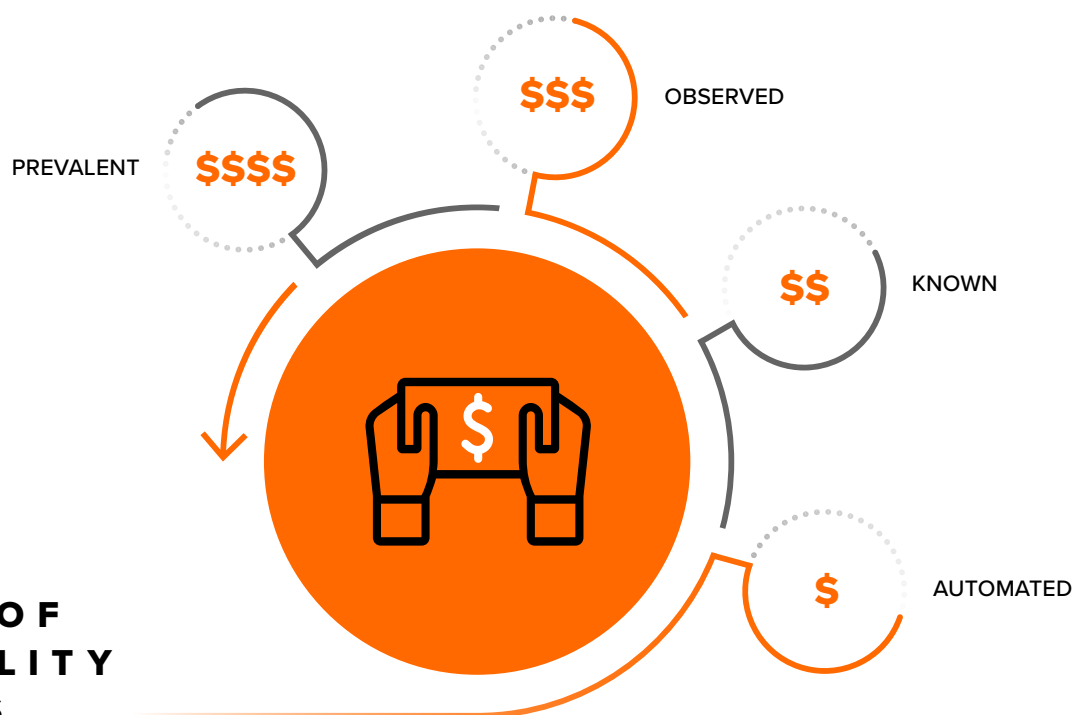
TOP 10 MOST COMMONLY IDENTIFIED VULNERABILITY TYPES IN 2021

1	 Cross-Site Scripting (XSS): Reflected	6	 Sensitive Data Exposure: Disclosure of Secrets for Publicly Accessible Assets
2	 Broken Access Control (BAC): Insecure Direct Object References (IDOR)	7	 Server Security Misconfiguration: No Rate Limiting on Form/Email
3	 Sensitive Data Exposure: Disclosure of Secrets for Internal Assets	8	 Broken Authentication & Session Mgmt: Failure to Invalidate Session
4	 Server Security Misconfiguration: Missing Secure or HTTPOnly Cookie Flag	9	 Unvalidated Redirects & Forwards: Open Redirects
5	 Broken Authentication & Session Mgmt: Privilege Escalation	10	 Server Security Misconfiguration: Directory Listing Enabled

The types of vulnerabilities submitted, as defined by the Vulnerability Rating Taxonomy (VRT) developed by Bugcrowd, are also evolving in the new security environment. There was some change at the top in 2021, where Cross-Site Scripting overtook Broken Access Control as the most commonly identified vulnerability type, reverting to the 2019 top two and reflecting the rapid deployment of home-grown web applications throughout 2020 and 2021. In third place, Sensitive Data Exposure involving Internal Assets leapt six places from ninth last year, brought on by an increased emphasis on scanning as a means of uncovering vulnerabilities.

This was a direct consequence of the expansion and increased complexity of attack surfaces during pandemic-induced digital transformation, as well as the speed at which this transformation took place. The changes in the top 10 most commonly identified vulnerability types demonstrates the natural life cycle of vulnerability categories and the "cat and mouse" nature of the interaction between builders and breakers: the Crowd is incentivized to find new, prevalent vulnerability types, those vulnerabilities are eventually addressed by automated tools (causing incentives to fall), and then new vulnerability types emerge that the Crowd is highly incentivized to find.

LIFECYCLE OF VULNERABILITY INCENTIVES



As automated tools are developed and adopted to detect known vulnerability types, the incentives for finding those vulns shrink in size. But like virus mutations, new types of prevalent vulns are emerging all the time, attracting big payouts.

For example, in 2021...



1. Better scanning techniques caused hackers to identify subdomain takeovers at a higher rate. This created demand for solutions that identified these vulnerabilities, resulting in more frequent use of automated tools within the space.



2. These automated solutions found subdomain takeovers at scale, prompting faster remediation and leaving fewer for ethical hackers to find—however, our heroes had moved on by then to address the hasty digital transformation that had occurred during the pandemic.



3. This, in turn, caused an increase in Sensitive Data Exposure vulnerabilities ranging from exposed company calendars, to passwords and credentials, to public GitHub repos that had been rushed online in default configurations, leaving them vulnerable to hackers with documentation in hand.

Researchers are still working through the backlog to identify this exposed data, and market demand will likely lead to automated solutions for finding them. However, by the time that happens, the Crowd will have identified a new category of vulnerabilities at the bleeding edge of security—because as new software is written, new vulnerabilities become discoverable.

KEY

Vulnerability Trends

The democratization of threats

Cybersecurity breaches captured numerous headlines in 2021, with several high-visibility incidents (e.g., the Log4Shell exploit) focusing the public imagination on emerging threats such as ransomware, and government policy quickly spinning up in response. Notably, we've seen a “democratization” of such

threats due to the appearance of a ransomware economy and a continued blurring of the lines between state actors and eCrime organizations—which, combined with growing and more lucrative attack surfaces, have made for a highly combustible environment. In 2022, we expect more of the same.



RANSOMWARE HITS MAIN STREET (AND THE HOUNDS ARE RELEASED)

Ransomware overtook personal data breaches as the threat that dominated cybersecurity news around the world in 2021. The U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) [reported in June 2021](#) that the total value reflected in ransomware-related suspicious activity reports (SARs) during just the first six months of that year had reached \$590 million, exceeding the \$416 million reported for all of 2020.

We are now seeing ransomware gangs applying lean startup principles to their operations. They begin with skeleton teams making scattergun, speculative attacks and crudely requesting their rewards in crypto. Following one or two successful attacks, these teams treat the ransoms paid as seed capital, using it to grow their operations and invest in better software, talent, and exploits. At the elite end, ransomware teams run processes that include detailed research to identify targets, advanced communications, and media relations to stoke fear and increase the likelihood of a payout occurring, and even IT desks and ticketing systems to allow their clients/victims to get their data back and operations running again. Many attackers now track CVEs to find gaps for exploitation that have remained undetected by organizations that fail to take a proactive approach to their security.

One of the terrifying consequences of the increase in the scale and impact of attacks is that it brings critical national infrastructure and healthcare facilities more into play as targets. In 2021, the [Colonial Pipeline attack](#) shut down gasoline supply to half the US east coast for several days, pushing prices above \$4 per gallon and costing tens of millions of dollars on top of the ransom paid. Research shows that death rates increase when hospitals suffer ransomware attacks, and [the tragic case](#) of an infant death in 2019 may have been the first life lost that can be directly traced to ransomware.

Given the economics of ransomware, this problem will not disappear soon: Director of the NSA and Head of U.S. Cyber Command General Paul Nakasone predicts persistent ransomware threats "[every single day](#)" for the next five years. Log4Shell is likely to have an impact here.

These increased stakes are causing the problem to evolve from a technical security challenge to a national security issue. President Biden addressed this by hosting a "ransomware summit"

that aims to establish a posture of offensive countermeasures in response to ransomware.

In advance, the Dutch government signaled that it would be [countering ransomware with offensive operations](#), and the [head of the UK's National Cybersecurity Centre](#) said that responding to ransomware would include integrating and deploying a range of tools, including economic measures and military capabilities. This gradual legitimization of offensive deterrence follows the "release the hounds" doctrine first proposed by [Bugcrowd back in 2014](#) and [popularized by Patrick Grey on the Risky Business podcast](#).

ATTACK SURFACES AND SUPPLY CHAINS EXPOSED

While security teams have spent countless hours addressing the "new normal" of hybrid work environments (e.g., the use of home wifi with cheap hardware configured to default settings), few have budgeted for it in advance. This means that many remote workers have a lightly defended entry point into the corporate network. Advanced attackers are now using these entry points to gain a foothold there.

The overall effect is a massive expansion of IT footprints and associated attack surface. [Research by the Enterprise Strategy Group](#) found in 2019 that the average organization's attack surface was 40% "unknown." And that was before short-term workarounds to enable working from home that became permanent, and the decision by many organizations to adopt remote working policies.

2021 was also a [record year for mergers and acquisitions \(M&As\)](#). Given that M&A activity is a principal driver of shadow IT and forgotten assets, this will accelerate the trend of vulnerable attack surfaces being exploited by malicious actors. Acquisition activity and entropy, over time, leads to a reliance on legacy software that is often poorly maintained and more likely to contain vulnerabilities.

These can be especially dangerous when there are unmaintained OS components in the mix, as these can enable lateral movement to access high-value assets.

Trends associated with the pandemic have accelerated risks associated with unknown and vulnerable assets, a trend that was already observed prior to the start of the pandemic.

Supply chains have increased in size and complexity, and with them the attack surfaces that each organization needs to secure. For example, [data from BlueVoyant](#) shows that companies with over 1,000 employees share data with more than 1,000 third parties on average, and this number is sure to grow. The risk is even higher for vulnerabilities that touch numerous interdependencies, such as the Log4J vulnerability.

This demand has created a thriving industry of scanners and automated tools. However, automation is hardly a silver bullet. Attackers have access to those same tools and can supplement them with domain knowledge, creativity, and intuition, and they are also skilled in working through OODA loops quickly during the lag times associated with scanners.

Only an approach that turns that weakness into a strength—by adopting the same tools, techniques, and mindset as attackers to uncover vulnerabilities before they do—leads to success.

USE OF N-DAYS BY APTS

Whereas in the past, advanced persistent threats (APTs) were defined by state-of-the-art tactics and clandestine operations, this approach is shifting. Diplomatic norms around hacking have weakened to the point where nation state attackers are less concerned with stealth than they were in the past.

Because APT behavior is determined by the incentives of free markets, they are figuratively willing to put down their sniper rifles and pick up shotguns on occasion. Lower-level targets are now on APTs' radars, and they are willing to use "n-days" (simple exploits of known vulnerabilities) and less sophisticated attacks to crack them. The convergence of tactics between APTs and cyber criminals coincides with an increased willingness for state actors to engage in malicious activity for economic gain or camouflage. For example, CrowdStrike has found that Iranian cyber operations were engaging in eCrime to complicate attempts at attribution, while [Teiss reported](#) that the main source of revenue for the North Korean state is cyber crime.

Researchers on the Bugcrowd Platform have responded by focusing their efforts on commercially available off-the-shelf products, which are being targeted more frequently when n-days drive attacker behavior. Frequently, as in the case of the F5 TMUI RCE (CVE-

2020-5902), Confluence Server Webwork OGNI Injection (CVE-2021-26084), and Apache HTTP Server 2.4.49 (CVE-2021-41773) bugs, these vulnerabilities were reported inside Bugcrowd customer programs well ahead of public exploits emerging in the wild—giving those customers critical advance warnings.

See [Bugcrowd Security Flashes](#) for deep-dive discussions about some of these vulns.

FROM PENETRATION TESTING, TO CROWDSOURCED, TO MULTISOURCED

Penetration testing is the oldest outsourced service in security, with traditional penetration testing dating back to the 1990s in its current form. Arguably, penetration testing extends even further back to the UK government's "tiger teams" of the '60s and '70s, formed to identify and exploit vulnerabilities in computer programs. This evolved into "adversarial simulation," which became incorporated into the PCI-DSS standard in 2006.

Penetration testing has evolved more over the past three years than over the previous 20, as ownership on the client side has moved from the governance, risk, and compliance teams to the security team. The change in ownership shifted the focus from meeting strictly regulatory goals to also finding vulnerabilities that go beyond the checklist.

All of this turmoil has caused industry leaders to consider penetration testing from first principles, and to reassess the definition of a penetration test in a world where vulnerabilities can be constantly uncovered by remote hackers.

The traditional model of paying a small team of penetration testers for set-piece projects has evolved, with Bugcrowd now offering a modern [Pen Testing as a Service](#) solution that integrates the Crowd into pen test workflows to replace or complement traditional, compliance-focused testing.

This new approach has broadened the range of models available, enabled rapid launch times, and provided much more flexibility for customers with pen testing needs. Buyers can now consider their needs around compliance, budget, deadlines, and physical security and implement the right pen testing models accordingly.

POLICY CHANGES: STRIVING FOR CLARITY

Government policy remains a source of top-down pressure in driving robust security, along with lateral pressure from peers and adversaries and bottom-up demand from consumers. The US [binding directive](#) that called for all federal civilian agencies to set up VDPs is one example of a progressive move welcomed by the security industry, and Bugcrowd is proud to be helping US federal civilian agencies implement VDP and bug bounty programs under BOD 20-01. Australia followed on from this directive with its own guidelines recommending VDPs in its [Australian Government Security Manual](#), which Bugcrowd is supporting by [offering managed VDPs](#) to Australia's government agencies.

There is also a growing body of legislation and case law that is helping to define and elevate ethical hacking and security research. Hacking has always been a bottom-up phenomenon, and hackers have traditionally been associated with an anti-establishment culture; however, in a world where data security permeates diplomacy, politics, and financial markets, improving clarity on the scope of ethical hacking is welcomed.

When the US Supreme Court ruled on *Van Buren v. United States* in June 2021, it provided some much-needed clarification on the Computer Fraud and Abuse Act (CFAA). At stake was the issue of whether or not violation of software terms of service could constitute a criminal offence, an interpretation that was opposed by the [Electronic Frontier Foundation](#), [criminal law scholars](#), and [several prominent security companies](#), including Bugcrowd. The court opted for a narrow interpretation of the law, meaning that contractual disputes around arbitrary terms of service cannot lead to criminal convictions.

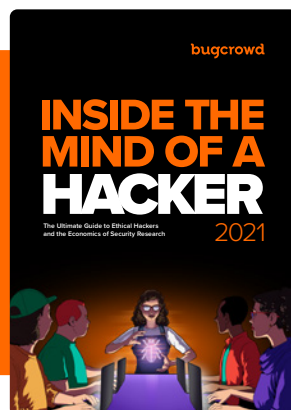
The EU's General Data Protection Regulation (GDPR) has continued to define privacy and security globally. It has raised awareness of the need for tools such as VDPs and increased awareness of security at the board level, improving the budgets of some cash-strapped CISOs. (We have also noticed that European hackers tend to have better mental models around privacy, and their submissions help to drive higher standards internationally.)

The fines are eye-watering: Amazon [disclosed a GDPR fine of \\$877 million](#) in August 2021, 15 times the existing record of \$56.6 million set by Google in 2019.

REPORT

Inside the Mind of a Hacker

DOWNLOAD NOW



Report Highlights

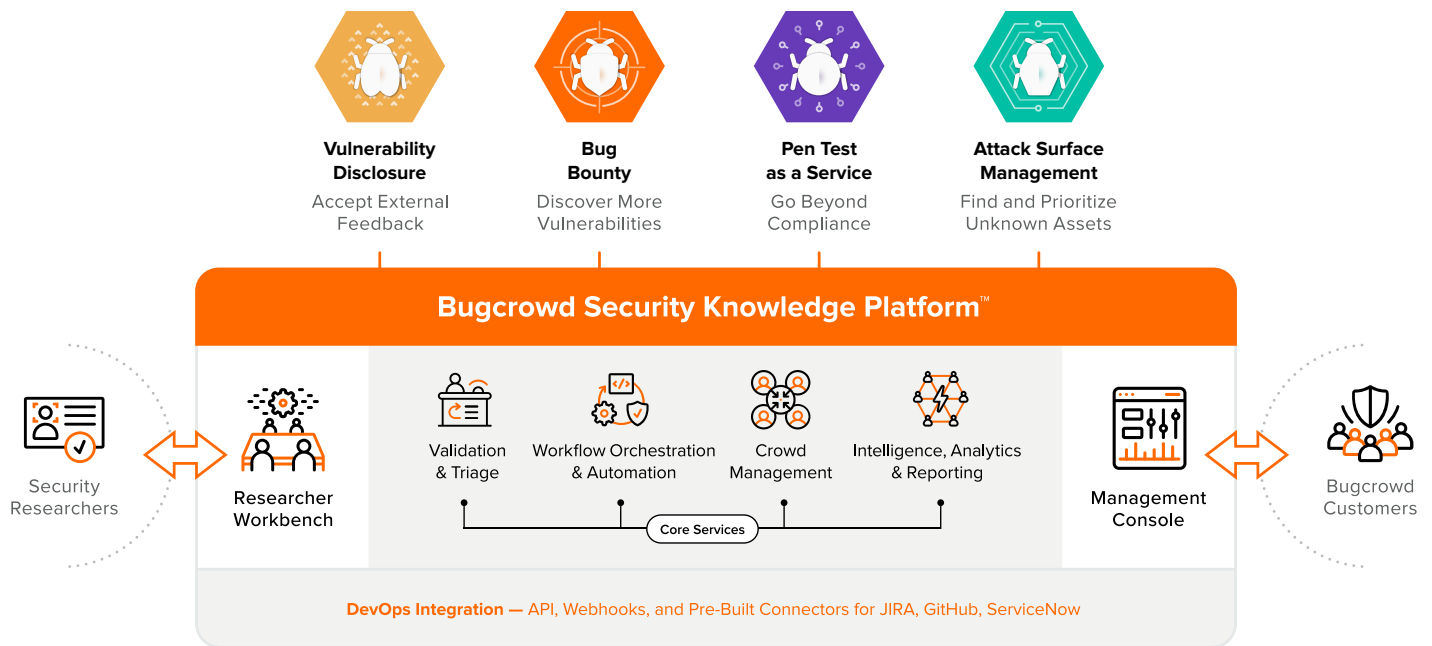
- **\$27B of cybercrime** prevented by Bugcrowd security researchers.
- **91% of ethical hackers** agree that point-in-time testing can't secure companies year-round.

One Platform, Many Solutions

*Do everything proactively possible to defend your organization, reputation, and customers against being blindsided by cyber attacks with the **Bugcrowd Security Knowledge Platform™***

We live in a digital first world where threats are relentless and businesses are constantly under siege. Regardless of how many security tools you're managing, you are still at risk. Organizations of all kinds need a defense that addresses the incomplete solutions that leave cybersecurity environments vulnerable.

The Bugcrowd Security Knowledge Platform™ uniquely enables organizations to do everything proactively possible to protect themselves, their reputations, and their customers by orchestrating data, technology, and human intelligence—including a global community of security researchers—to expose blind spots before attackers do.



Best Security ROI from the Crowd

We match you with the right trusted security researchers for your needs and environment across hundreds of dimensions using ML.

Instant Focus on Critical Issues

Working as an extension of the platform, our global security engineer team rapidly validates and triages submissions, with P1s often handled within hours.

Contextual Intelligence for Best Results

We apply accumulated knowledge from over a decade of experience across 1000s of customer solutions to your goals for better outcomes.

Continuous, Resilient Security for DevOps

The platform integrates workflows with your existing tools and processes to ensure that applications and APIs are continuously tested before they ship.

[LEARN MORE](#)