FORRESTER®

The Total Economic Impact™ Of Bugcrowd Managed Bug Bounty

Cost Savings And Business Benefits Enabled By Bugcrowd Managed Bug Bounty

A Forrester Total Economic Impact™ Study
Commissioned By Bugcrowd, April 2024

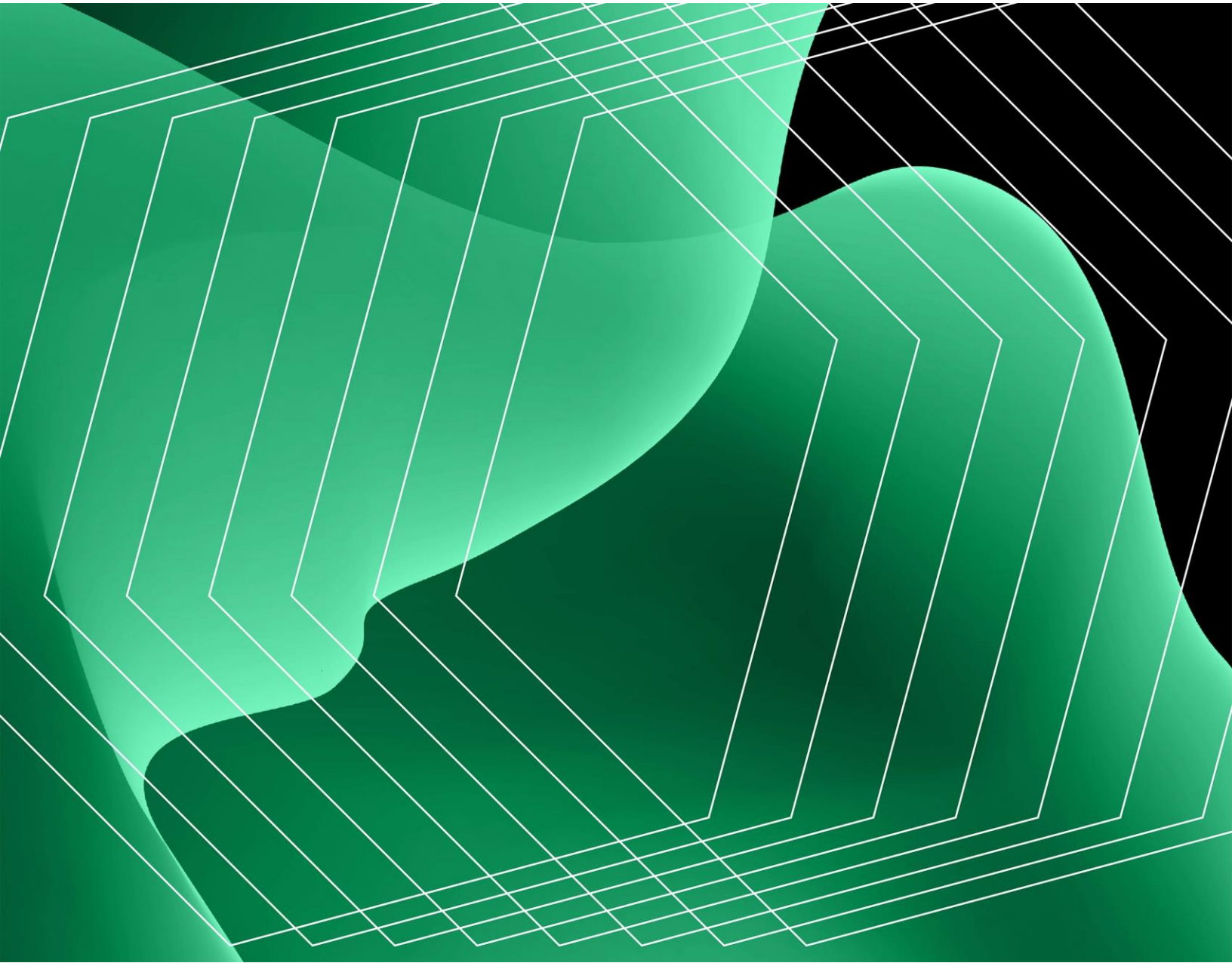


Table Of Contents

Consulting Team:

Luca Son

Marianne Friis

Executive Summary

Investing in crowdsourced security has become an imperative for organizations seeking to bolster their cybersecurity defenses. With the increasing frequency and sophistication of cyberthreats, traditional security measures alone are often insufficient. Bug bounty engagements, among the most popular applications of crowdsourcing, offer a proactive approach by harnessing the collective expertise of ethical hackers in combination with rewards-based incentives. They provide an ongoing and cost-effective means of identifying and addressing vulnerabilities, ultimately reducing the risk of data breaches and reputational damage.

Bugcrowd Managed Bug Bounty is a solution on the multipurpose Bugcrowd Platform that connects organizations with a global community of ethical hackers and security researchers and incentivizes them to identify vulnerabilities that traditional testing will generally miss. It provides a managed approach to bug bounty engagements, offering end-to-end support and expertise to help organizations run their bug bounty initiatives effectively. Bugcrowd's Managed Bug Bounty solution helps organizations discover and address vulnerabilities, enhance their security posture, and reduce the risk of data breaches by leveraging the collective intelligence of trusted, skilled hackers in a controlled, scalable, and structured manner.

Bugcrowd commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Managed Bug Bounty.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Managed Bug Bounty on their organizations.

Return on investment (ROI)

268%

Net present value (NPV)

$1.43M

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using Managed Bug Bounty and surveyed 39 decision-makers at the manager level or above who are responsible for security strategy, vulnerability management, or security operations at an organization that is leveraging ethical hacking engagements. For the purposes of this study, Forrester aggregated the interviewees' and survey respondents' experiences and combined the results into a single composite organization that generates $750 million in annual revenue and has 5,500 employees.

Interviewees said that before using Managed Bug Bounty, their organizations primarily relied on traditional penetration (pen) tests to identify exploitable vulnerabilities. Interviewees' organizations also leveraged vulnerability management tools like vulnerability scanners, user-submitted vulnerability programs, or an alternative crowdsourced security provider. However, prior attempts yielded limited success, leaving them with limited expertise and security resources to effectively manage risk, costly traditional penetration test engagements, high noise from legacy solutions that created operational burdens, and limited continuous monitoring capabilities.

After the investment in Managed Bug Bounty, the interviewees noted their organizations leveraged a mixture of private and public and periodic and continuous bug bounty engagements to cover their applications. Public bug bounty programs are open to the general public and allow any interested individual to participate, while private bug bounty programs are invitation-only or restricted to a specific group of individuals. Key results from the investment include improved security operations efficiency, avoided traditional penetration test costs, material breach risk reduction savings, and reduced cybersecurity insurance premiums.

"Which of the following benefits has your organization experienced as a result of investing in your crowdsourced security program?"

Base: 39 cybersecurity decision-makers at the manager level or higher who are responsible for security strategy, vulnerability management, security operations, or similar areas

Source: A commissioned study conducted by Forrester Consulting on behalf of Bugcrowd, January 2024

KEY FINDINGS

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **Improved security operations efficiency and avoided hiring two FTEs.** Bugcrowd's Managed Bug Bounty engagement pairs the composite organization with experienced ethical hackers to identify high-confidence vulnerabilities that may have been missed by internal security teams and tools in the composite's legacy environment. By providing actionable and triaged findings, Bugcrowd eliminates the need for manual triaging work, freeing up the time and resources of the composite's internal security team. This improves coverage and reduces risk without the need to increase headcount. With the Managed Bug Bounty engagement in place, the composite reallocates existing security teams' time to focus on remediating high-risk priorities and strategic tasks and avoids hiring additional internal security resources to gain the same level of coverage that Bugcrowd provides. The composite organization saves $819,000 in avoided hiring and overhead costs over three years.

- **Avoided 60% of traditional penetration test costs.** The composite organization leverages Bugcrowd to supplement and enhance its penetration testing efforts. Managed Bug Bounty engagements offer continuous, clear, and actionable insights into high-impact vulnerabilities within the composite's environment, giving its security team a more comprehensive approach to identifying and addressing vulnerabilities. As a result, the composite reduces the frequency and scope of traditional penetration tests, leading to $552,000 in cost savings over three years.
- **Reduced risk of a material breach by up to 30%.** The composite organization effectively reduces the risk of data breaches by leveraging Managed Bug Bounty engagements. With Bugcrowd, the composite increases its chances of identifying vulnerabilities that might have been overlooked in previous environments. The Managed Bug Bounty engagements also facilitate faster response times by incentivizing prompt reporting of vulnerabilities, leading to quicker fixes and minimizing the potential window of opportunity for malicious attackers. Furthermore, the continuous nature of the Managed Bug Bounty engagements provides a consistent mechanism for ongoing vulnerability identification and remediation, resulting in a gradual reduction of vulnerabilities within the composite organization's systems over time. The composite organization avoids $528,000 of breach costs over three years.
- **Reduced cybersecurity insurance premium costs by 9%.** The Managed Bug Bounty engagement contributes to lower cyber insurance premium costs for the composite organization. This engagement demonstrates a proactive approach to security risk management, which signals to insurers that the composite is taking measures to mitigate potential cyberthreats. Insurers may view organizations with bug bounty engagements as having better security hygiene and reduced risk profile and are less likely to experience a data breach. As a result, insurers may offer lower premium costs as they perceive the composite to be a lower risk. The composite organization saves $57,000 of cyber insurance premium costs over three years.

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified for this study include:

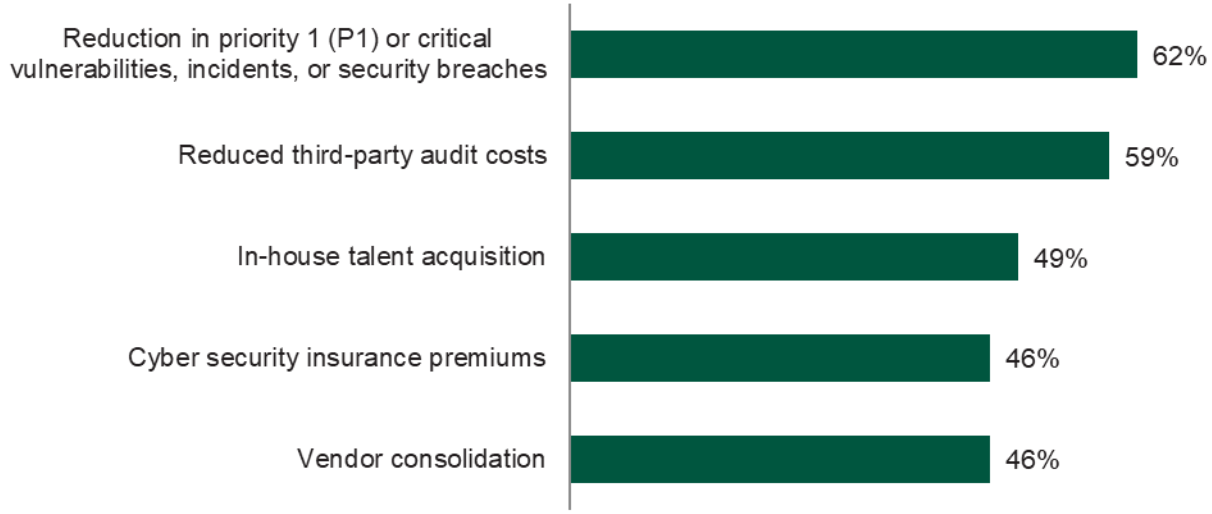
- **Shorter time to remediation.** Managed Bug Bounty engagements lead to shorter vulnerability remediation times for the composite than alternative solutions.
- **Improved relationship between developers and security due to better communication.** Managed Bug Bounty bridges communication gaps between security and developer teams, allowing for more robust security processes.
- **Improved reputation and demonstration of security maturity.** Bugcrowd demonstrates security maturity, bolstering brand and reputation from the vantage point of customers, partners, auditors, and other third-party stakeholders.
- **Improved compliance reporting.** Bugcrowd demonstrates security posture health to regulators and speeds up reporting processes.
- **Effective researcher pairing and strong vendor support.** Managed Bug Bounty provides high-quality and effective researchers, AI algorithms, and required data for sourcing and activating specific skill sets, program management, and overall vendor support. This results in higher accuracy, fewer false positives, and more edge cases identified for the composite organization.
- **Flexibility to adapt to changing threat environments without new hires or onboarding new tools.** Managed Bug Bounty engagements give access to scalable and diverse talent to provide cost-effective and timely response to new threats and security standards. This addition to security risk management engagements allows the composite to forgo onboarding of additional new hires and tools.

Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **Platform and reward pool costs of $522,000 over three years.** Bugcrowd Managed Bug Bounty consists of a platform fee and payments in a rewards pool that are reserved to incentivize and payout to researchers. Platform fees and reward pools vary depending on sizing and requirements. Contact Bugcrowd for additional details.
- **Implementation and change management costs of less than $9,000.** Forrester accounts for upfront internal labor hours dedicated to implementation and change management.

The financial analysis which is based on the interviews and survey found that a composite organization experiences benefits of $1.96 million over three years versus costs of $531,000, adding up to a net present value (NPV) of $1.43 million and an ROI of 268%.

"Which of the following areas have been impacted by your organization's crowdsourced security program?"



Base: 39 cybersecurity decision-makers at the manager level or higher who are responsible for security strategy, vulnerability management, security operations, or similar areas

Source: A commissioned study conducted by Forrester Consulting on behalf of Bugcrowd, January 2024

Avoided headcount with Bugcrowd Managed Bug Bounty

2 FTEs

"The level of quality, thoroughness, and cost-effectiveness is why we keep using Bugcrowd."

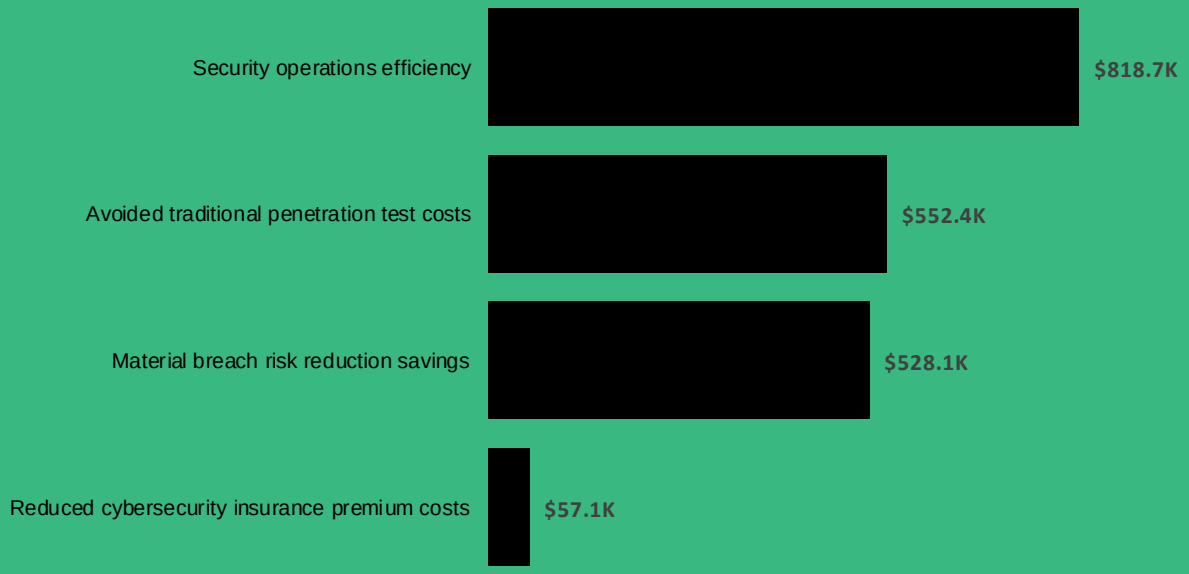
HEAD OF INFORMATION SECURITY, HEALTHCARE

"I truly believe in the crowdsourced mode of operation. I think it's way more effective than the traditional pen test. The fact that we've continued to use Bugcrowd for the past three years is a testament to the quality of the service."

HEAD OF INFORMATION SECURITY, HEALTHCARE

Return on investment (ROI)	Benefits PV	Net present value (NPV)	Payback
268%	**$1.96M**	**$1.43M**	**<6 months**

Benefits (Three-Year)



TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews and survey, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in Managed Bug Bounty.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that Managed Bug Bounty can have on an organization.

Due Diligence
Interviewed Bugcrowd stakeholders and Forrester analysts to gather data relative to Managed Bug Bounty.

Interviews And Survey
Interviewed four representatives at organizations using Managed Bug Bounty to obtain data about costs, benefits, and risks and surveyed 39 respondents at the manager level or above who are responsible for security strategy, vulnerability management, or security operations at organizations leveraging ethical hacking engagements.

Composite Organization
Designed a composite organization based on characteristics of the interviewees' and survey respondents' organizations.

Financial Model Framework
Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees and survey respondents.

Case Study
Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Bugcrowd Managed Bug Bounty Customer Journey

Drivers leading to the Managed Bug Bounty investment

KEY CHALLENGES

Forrester interviewed four representatives with experience using Bugcrowd Managed Bug Bounty at their organization and surveyed 39 respondents with experience using a crowdsourced security vendor, 54% of whom had experience using Bugcrowd. Our survey found that 69% of respondents noted their organization used private engagements across an average of 543 assets. For more details on the interviewees and survey respondents, see Appendix B.

Before Bugcrowd Managed Bug Bounty, interviewees and survey respondents noted their organizations primarily relied on traditional penetration tests to identify exploitable vulnerabilities. Interviewees' organizations also leveraged vulnerability management tools like vulnerability scanners, self-managed vulnerability disclosure programs, or an alternative crowdsourced security provider.

The interviewees noted how their organizations struggled with common challenges, including:

- **Limited expertise and security resources.** Interviewees told Forrester their organizations lacked the security knowledge and resources to identify, triage, and address vulnerabilities. Existing security personnel were already fully utilized with the existing volume of vulnerabilities to address, and hiring additional resources was cost-prohibitive.
- **Traditional penetration test engagements were costly and yielded limited success.** Interviewees told Forrester that traditional penetration tests were expensive, particularly for smaller organizations with limited budgets. Planning, executing, and managing results from traditional penetration test engagements was time-consuming. The quality between providers varied, and assessments missed or failed to prioritize exploitable vulnerabilities. Finally, interviewees struggled to retest and verify fixes in their environments until the next engagement after remediating issues. The senior director of information security

and IT at an automotive organization said: “Prior to [Managed Bug Bounty], we had paid testing engagements with third-party vendors. As you can imagine, that’s expensive, and you pay for a tester’s time instead of per finding.”

The head of information security at a healthcare organization stated: “It takes a long time to do an annual pen test and you might not have a checkpoint between those 365 days to see how you’re progressing from an external attacker perspective. You might have an internal security team monitoring application security or internal SaaS [software-as-a-service] tools, but there’s no substitute for having talented researchers assess your infrastructure from an external perspective.”

- **High noise from legacy solutions created an operational burden.** Interviewees stated that legacy vendor tools, traditional penetration tests, user submissions, and legacy crowdsourced security solutions generated false positives, duplicates, and other noise, creating additional triaging work for already resource-constrained security teams. The senior director of information security and IT at an automotive organization said: “There was a high amount of noise from [our legacy crowdsourced security partner]. It takes someone who is paid well to sit there, sort out findings, and respond to the researcher. It’s a back-and-forth, they complain, and you have to go through it. None of that is our burden with Bugcrowd. Bugcrowd effectively manages the community regarding expectations and gives customers guidance on how to respond and engage with them.”
- **Incomplete coverage and lack of continuous monitoring.** Before Bugcrowd, interviewees’ organizations lacked continuous, red-teaming coverage across their systems, platforms, and technologies, leaving them susceptible to attacks. The head of information security at a healthcare organization stated: “[Before Bugcrowd,] vulnerabilities were not being found because humans are much more creative in finding vulnerabilities than automated systems are. Those vulnerabilities would go undiscovered for long periods without Managed Bug Bounty.”

WHY BUGCROWD MANAGED BUG BOUNTY?

Interviewees and survey respondents noted their organizations required a cost-effective solution to identify and triage vulnerabilities, lower risk, and harden security posture. The interviewees' organizations searched for a solution that could:

- **Leverage expert hackers to keep pace with a quickly evolving threat landscape and to help identify high-risk vulnerabilities.** The head of information security at a healthcare organization said: "The [cybersecurity] field and types of vulnerabilities and hacking emerging is moving super fast. It's important to have intelligent researchers who are tapped into everything that's going on in that sense and are up to date on the latest vulnerabilities, techniques, and procedures. That's one of the most important pieces of using a crowdsourced bug bounty."

  The senior director of information security and IT at an automotive organization said: "Because Bugcrowd is community-based, we benefit from many different perspectives. That's an intrinsic component of the platform itself. Even though we continue to partner with a single vendor, we benefit from the fresh perspective of many different researchers as an individual."

- **Augment traditional penetration tests and vulnerability scanners to increase coverage and insights and reduce cost.** The head of information security at a healthcare organization said: "One of the key things you don't have without a bug bounty engagement is the ongoing support and monitoring from an external perspective and from humans specifically, not just automated tools."

- **Improve operational efficiency with support from the Managed Bug Bounty team.** The senior manager of application security at a technology organization stated: "We are still growing our security maturity. Bugcrowd makes sense because we can get much greater coverage of our environment and systems. It's more efficient."

  The same interviewee stated: "The Bugcrowd Platform has been pretty successful in helping our engineers and application owners understand the impact of vulnerabilities and how they manifest themselves in the outside world. It takes things from the theoretical, where we find the potential vulnerabilities in

SaaS tools and things like that and makes them more real. It's been a good partnership."

After a request for proposal (RFP) and business case process evaluating multiple vendors, the interviewees' organizations chose Managed Bug Bounty and began deployment:

- Interviewees leveraged Managed Bug Bounty to cover external services and customer-facing applications.
- Interviewees ran either continuous or periodic bug bounty engagements.
- All interviewees ran private engagements; one interviewee combined public and private ones.

> "Our partnership with Bugcrowd has been invaluable. Instead of paying per hour, you pay per actionable finding. That is a major differentiator because security expertise is not cheap and can take many hours."
>
> **SENIOR DIRECTOR OF INFORMATION SECURITY AND IT, AUTOMOTIVE**

COMPOSITE ORGANIZATION

Based on the interviews and survey, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the four interviewees and 39 respondents, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The composite organization is a United States-based company that generates $750 million in annual revenue and employs 5,500 employees. On the security side, the composite employs four security operations (SecOps) FTEs who are responsible for all vulnerability management engagements, including Managed Bug Bounty. The composite leverages external traditional penetration tests to find vulnerabilities.

Deployment characteristics. The composite invests in a Bugcrowd Managed Bug Bounty engagement with Bugcrowd to augment traditional penetration tests and expand its vulnerability management maturity. The composite begins with continuous, private bug bounty engagements across its customer-facing assets. As it runs and manages engagements proficiently, the composite expands to public bug bounty engagements. The Managed Bug Bounty engagement includes 500 assets in scope.

KEY ASSUMPTIONS

$750 million revenue

5,500 employees

Four SecOps FTEs

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Security operations efficiency	$514,242	$222,615	$222,615	$959,472	$818,726
Btr	Avoided traditional penetration test costs	$180,000	$225,000	$270,000	$675,000	$552,442
Ctr	Material breach risk reduction savings	$172,062	$215,078	$258,093	$645,233	$528,079
Dtr	Reduced cybersecurity insurance premium costs	$22,950	$22,950	$22,950	$68,850	$57,073
	Total benefits (risk-adjusted)	$889,254	$685,643	$773,658	$2,348,554	$1,956,320

SECURITY OPERATIONS EFFICIENCY

Evidence and data. According to interviewees, Bugcrowd's Managed Bug Bounty solution effectively paired experienced, ethical hackers with organizations to identify high-confidence vulnerabilities that internal security teams and tools may have missed. By providing actionable and triaged findings, Bugcrowd eliminated the need for manual triaging work, freeing up the time and resources of internal security teams. With the Managed Bug Bounty engagement in place, interviewees' organizations could reallocate their existing security teams' time to focus on strategic initiatives and avoid hiring additional internal security resources to gain the same coverage that Bugcrowd provides. This resulted in improved coverage and reduced risk. Interviewees and survey respondent provided the following evidence:

- The senior director of information security and IT at an automotive organization said: "It's much cheaper to pay Bugcrowd engineers than if we were to open a position for an FTE to satisfy that same requirement. The value proposition is incredible on multiple fronts. We have our internal engineers focusing on things that deliver higher ROI and not just waiting for report submissions. Then

Bugcrowd handles the triage, and we only pay researchers when they provide actionable findings. We're not paying them per hour, regardless of their findings. They are strongly incentivized to have meaningful submissions." The same interviewee said, "I would need a staff of at least 15 FTEs, probably costing $200,000 to $250,000 each, to have the same level of engagement and testing that Bugcrowd provides."

- The senior manager of application security at a technology organization stated, "By outsourcing to Managed Bug Bounty, my internal resources can focus on remediation and helping the internal teams fix things rather than just looking and sifting through all the submissions looking for the good ones." The same interviewee estimated: "If we didn't have [Bugcrowd's] Bug Bounty program, we'd have to hire more internal penetration testing resources to replicate that coverage. We would probably have to hire at least three folks to get to any accepted level of coverage."
- The head of information security at a healthcare organization stated: "Given that we don't have a dedicated internal application security team, [Bugcrowd] has helped insofar as we don't have to have full-time employees that are charged with this task, and we can rely on the more cost-effective approach to testing. A seasoned security engineer can cost around $150,000 per year. To have the same level of support [as we do with Bugcrowd], we'd need a couple of them."
- Our survey found that 21 out of 25 survey respondents were able to reassign/save at least two FTEs as a result of their organization's crowdsourced security engagements.

> "The benefit we get from leveraging the external research community is we have folks in that community who have deep expertise in various areas. Each of them can focus on and look for the types of issues that they're most efficient at finding. It makes the overall vulnerability identification piece more cost effective for us than trying to cover that with internal resources, given that we're a small team."
>
> SENIOR MANAGER OF APPLICATION SECURITY, TECHNOLOGY

Modeling and assumptions. Based on the interviews and survey, Forrester assumes the following about the composite organization:

- The composite organization dedicates four security operations FTEs who oversee vulnerability management, including the Bugcrowd Managed Bug Bounty engagement.
- The composite organization requires a 50% increase in SecOps staff for triaging and to provide vulnerability remediation guidance without Bugcrowd.
- The annual fully burdened rate for a SecOps FTE is $130,950, including a 1.35 fully burdened multiplier.
- The hiring cost for a SecOps FTE is calculated by multiplying the fully burdened rate with a 131% hiring cost multiplier.

Risks. Forrester recognizes that these results may not be representative of all experiences. The impact of this benefit will vary depending on:

- Security operations and vulnerability management maturity.
- SecOps fully burdened rate.

- SecOps hiring costs.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $819,000.

50%

Increase in vulnerability management security FTEs needed without Bugcrowd

"We had to pause our program because we had such rich findings that we didn't have the matching engineering bandwidth to address them. It's a white-glove experience. It's further proof that they're competent in operating bug bounty engagements and that they pay attention to their customers' activity on the platform."

SENIOR DIRECTOR OF INFORMATION SECURITY AND IT, AUTOMOTIVE

Security Operations Efficiency					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	SecOps FTEs dedicated to vulnerability management	Composite	4	4	4
A2	Percent increase in staff needed for triaging and to provide vulnerability remediation guidance without Bugcrowd	Interviews	50%	50%	50%
A3	Avoided headcount with Bugcrowd	A1*A2	2	2	2
A4	Annual SecOps fully burdened rate	TEI standard	$130,950	$130,950	$130,950
A5	Avoided hiring cost per SecOps FTE	A4*131%	$171,545		
At	Security operations efficiency	A3*(A4+A5)	$604,990	$261,900	$261,900
	Risk adjustment	↓15%			
Atr	Security operations efficiency (risk-adjusted)		$514,242	$222,615	$222,615
	Three-year total: $959,472		**Three-year present value: $818,726**		

AVOIDED TRADITIONAL PENETRATION TEST COSTS

Evidence and data. Interviewees noted their organizations found traditional penetration tests expensive, resource-intensive, and unable to verify fixes promptly. To address these limitations, interviewees turned to Bugcrowd to supplement and enhance their penetration testing efforts. They quickly realized that the Managed Bug Bounty engagements offered continuous, clear, and actionable insights into high-impact vulnerabilities within their environment. By leveraging Bugcrowd's insights, interviewees' organizations gained a more efficient and cost-effective approach to identifying and addressing vulnerabilities in their systems. As a result, the interviewees' organizations reduced the frequency or scope of traditional penetration tests, leading to significant cost savings. Interviewees and survey respondents provided the following evidence:

- The senior director of information security and IT at an automotive organization said, "For less than $100,000, we had more findings in 60 days when we had over multiple years of paid [traditional penetration test] engagements at an order of magnitude higher cost." The senior director continued: "We have largely replaced most of our third-party pen testing spend with Bugcrowd. … We saved

$350,000 by changing our approach to application security testing by third parties. Instead of engaging a vendor on an ad hoc basis every year, we have a continuous bounty program that operates 24/7, 365 days a year, with the same results."

- Nine out of 15 survey respondents said their organization saved between $250,000 to $749,000 by reducing or replacing pen testing or other security solutions or processes. This averages out to $320,000.

Modeling and assumptions. Based on the interviews and survey, Forrester assumes the following about the composite organization:

- The composite analysis paid $500,000 to conduct traditional penetration tests in the legacy environment.
- The composite organization augments its traditional penetration testing with Managed Bug Bounty. After doing so, the composite reduces 40% of traditional pen test usage and costs in Year 1, 50% in Year 2, and 60% in Year 3 as the organization's proficiency and efficacy with Managed Bug Bounty engagements matures.
- This results in $200,000 of cost savings in Year 1, $250,000 in Year 2, and $300,000 in Year 3.

Risks. Forrester recognizes that these results may not be representative of all experiences. The impact of this benefit will vary depending on:

- Security and vulnerability management maturity.
- Frequency, scope, and cost of traditional penetration tests.
- Compliance requirements.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $552,000.

60%

Reduced traditional penetration test costs

"[Bugcrowd Managed Bug Bounty researchers] find sophisticated exploits. When they find something, you pay attention to it. I don't know how we'd do it without that because I didn't see another easy-to-implement solution that is very cost-effective for the value you get."

GLOBAL CISO, TELECOMMUNICATIONS

Avoided Traditional Penetration Test Costs

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Traditional penetration test costs in legacy environment	Composite	$500,000	$500,000	$500,000
B2	Reduced traditional penetration test reliance and costs by shifting to Managed Bug Bounty	Interviews	40%	50%	60%
Bt	Avoided traditional penetration test costs	B1*B2	$200,000	$250,000	$300,000
	Risk adjustment	↓10%			
Btr	Avoided traditional penetration test costs (risk-adjusted)		$180,000	$225,000	$270,000
	Three-year total: $675,000			**Three-year present value: $552,442**	

MATERIAL BREACH RISK REDUCTION SAVINGS

Evidence and data. Interviewees told Forrester that Managed Bug Bounty engagements effectively reduced the risk of data breaches. By engaging ethical hackers and security researchers, interviewees' organizations increased their chances of identifying vulnerabilities that might have been overlooked in previous environments. The Managed Bug Bounty engagements also facilitated faster response times by incentivizing prompt reporting of vulnerabilities, leading to quicker fixes and minimizing the potential window of opportunity for malicious attackers. Furthermore, the continuous nature of these Managed Bug Bounty engagements provided a consistent mechanism for ongoing vulnerability identification and remediation, resulting in a gradual reduction of vulnerabilities within the interviewees' organizations' systems over time. Interviewees and survey respondents provided the following evidence:

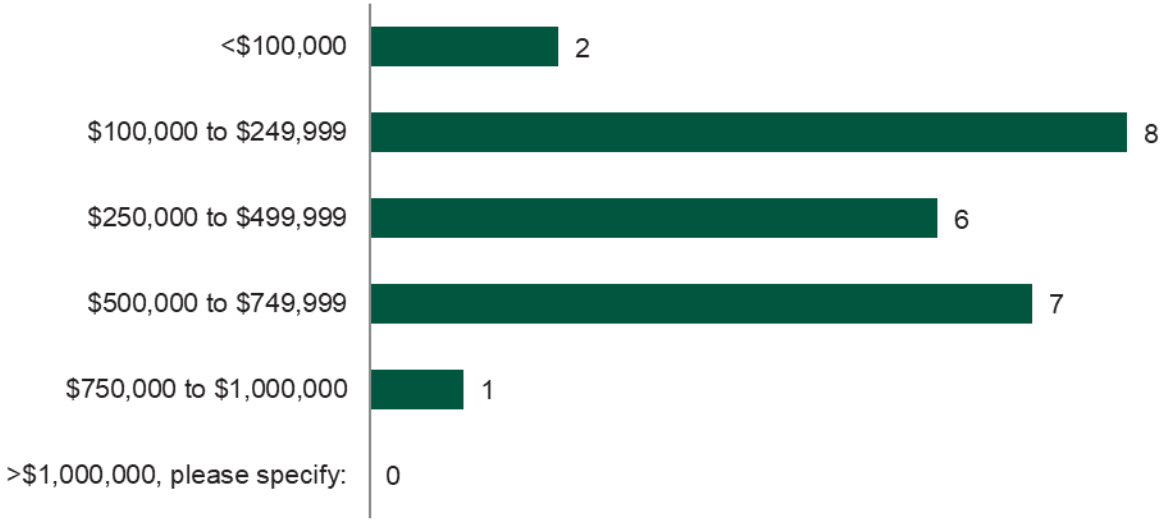
- The senior manager of application security noted their technology organization reduced the number of critical vulnerabilities by 60% with Managed Bug Bounty. The interviewee told Forrester: "We're improving the overall security posture via the Managed Bug Bounty program because we know we're finding out about vulnerabilities faster, closing them faster, and shortening the exposure window. That's the main way we demonstrate the value here."
- The head of information security at a healthcare organization said: "There have been discoveries from the Managed Bug Bounty program that were related to data leakage and therefore were avoided, which could have potentially led to undesired disclosure of information. It was a very important finding. … [Bugcrowd] has substantially lowered the risk of a breach."
- The senior director of information security at an automotive organization explained: "Bugcrowd is now probably 10% of our overall application security findings. But in the program's first year, it was easily 95%. Most of our findings for the program's first year were attributed to Bugcrowd because the body of researchers that we had engaged were providing a lot of really clever and novel threat techniques that effectively found gaps in our security posture."
- Sixteen out of 24 respondents who reduced priority 1 (P1) or critical vulnerabilities, incidents, or security breaches had found two or more critical or

P1 vulnerabilities per month with their organization's crowdsourced security engagements.

- Twenty-four respondents were able to reduce the likelihood of security breach, on average, by 33% with their organization's crowdsourced security engagements.
- Fourteen out of 24 respondents who reduced priority 1 (P1) or critical vulnerabilities, incidents, or security breaches estimated that the average financial impact from a P1 was $250,000.

> "The quality of the findings is very high because Bugcrowd researchers give very detailed instructions on how to duplicate the vulnerability and how to assess it. Then you also have the benefit of having them being able to retest the vulnerabilities after they've been fixed to make sure that they've been remediated. They're typically also very easy to collaborate and work with via the platform."
>
> **HEAD OF INFORMATION SECURITY, HEALTHCARE**

"To the best of your knowledge, what is the average financial impact of a P1 vulnerability, incident, or security breach on your organization?"



Base: 24 cybersecurity decision-makers at the manager level or higher who are responsible for security strategy, vulnerability management, security operations, or similar areas

Source: A commissioned study conducted by Forrester Consulting on behalf of Bugcrowd, January 2024

Modeling and assumptions. Based on the interviews and survey, Forrester assumes the following about the composite organization:

- The composite organization is susceptible to 4.7 material data breaches on average, per year.[2]
- Nearly half (49.1%) of the data breaches originate from external attacks.[3]
- The average cost of each breach is $466,000, which may include response and remediation costs, efforts to notify affected parties, regulatory fines, customer lawsuits, downtime, and more.[4]
- By utilizing Bugcrowd Managed Bug Bounty engagements, the composite organization reduces the likelihood of a material security breach by 20% in Year 1, 25% in Year 2, and 30% in Year 3. The reduction in likelihood increases year over year as the composite organization's proficiency and efficacy with Managed Bug Bounty engagements matures.

Risks. Forrester recognizes that these results may not be representative of all experiences. The impact of this benefit will vary depending on:

- Security and vulnerability management maturity.
- Organization size and industry.
- Frequency and severity of data breaches.
- Data breach size and costs.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $528,000.

30%

Reduced likelihood of a breach with Bugcrowd

"The Managed Bug Bounty program is a critical piece of our security program. We would be at substantially more risk if we were not using a bug bounty program."

HEAD OF INFORMATION SECURITY, HEALTHCARE

Material Breach Risk Reduction Savings					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Average number of data breaches per year	Survey	4.7	4.7	4.7
C2	Percent of breaches originating from external attacks	Forrester research	49.1%	49.1%	49.1%
C3	Average potential cost of data breach	Survey	$466,000	$466,000	$466,000
C4	Reduced likelihood of a breach due to Bugcrowd	Interviews	20%	25%	30%
Ct	Material breach risk reduction savings	C1*C2*C3*C4	$215,078	$268,847	$322,616
		↓20%			
Ctr	Material breach risk reduction savings (risk-adjusted)		$172,062	$215,078	$258,093
	Three-year total: $645,233		**Three-year present value: $528,079**		

REDUCED CYBERSECURITY INSURANCE PREMIUM COSTS

Evidence and data. Interviewees told Forrester that having Managed Bug Bounty engagements contributed to lower cyber insurance premium costs. By actively engaging ethical hackers and security researchers to identify vulnerabilities in their systems, the interviewees' organizations demonstrated a proactive approach to security risk management. Interviewees noted that this proactive stance signaled to insurers that their organizations were taking measures to mitigate potential cyberthreats. Because of this, insurers viewed the interviewees' organizations with bug bounty engagements as having better security hygiene and reduced risk profile and were less likely to experience a data breach. As a result, insurers may offer lower premium costs as they perceived the interviewees' organization to be a lower risk. Interviewees stated that the reduced likelihood and potential impact of a data breach and lower risk profile further contributed to reduced insurance premiums. Interviewees and survey respondents provided the following evidence:

- The senior director of information security and IT at an automotive company told Forrester: "We've had a significant increase in our security posture, and we've been able to recognize substantial savings on our cybersecurity assurance premiums as a result of not only Bugcrowd but all the other good work that we've

done and moving forward and maturing our security posture. I would say we save around 40% on our premium. … Bugcrowd is a significant component of our application security testing program and probably accounts for one-third of our overall security posture and impact because all the vulnerabilities, data disclosures, or breaches happen at the application layer."

- Twelve out of 18 survey respondents whose crowdsourced security engagement impacted cyber insurance premiums said their organization paid more than $250,000 in annual cyber security insurance premiums prior to its crowdsourced security engagement. Eleven out of 18 survey respondents said their organization reduced cybersecurity insurance premiums by three to less than 10% due to using a crowdsourced security engagement.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

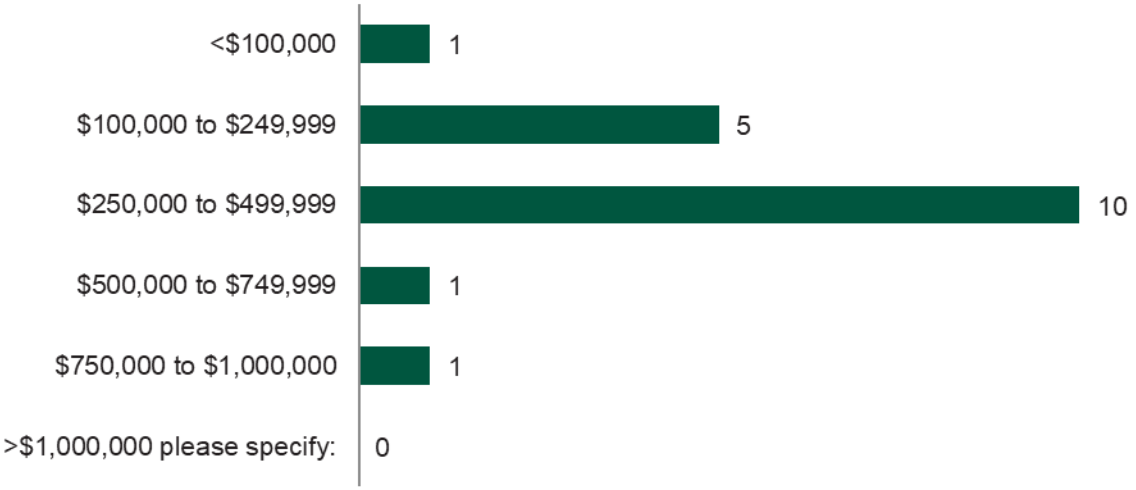
- The composite organization pays $300,000 a year in cybersecurity insurance premiums in its legacy environment.
- The composite organization reduces its cyber insurance premiums by 9% due to Bugcrowd, saving $27,000 annually.

Risks. Forrester recognizes that these results may not be representative of all experiences. The impact of this benefit will vary depending on:

- Internal security maturity.
- Cybersecurity insurance premium costs, which vary depending on scope, assets, and more.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $57,000.

"How much were your annual cyber security insurance premiums prior to your organization's crowdsourced security program?"



Base: 24 cybersecurity decision-makers at the manager level or higher who are responsible for security strategy, vulnerability management, security operations, or similar areas

Source: A commissioned study conducted by Forrester Consulting on behalf of Bugcrowd, January 2024

9%

Reduction in cybersecurity insurance premiums

Reduced Cybersecurity Insurance Premium Costs					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Cybersecurity insurance premiums in legacy environment	Composite	$300,000	$300,000	$300,000
D2	Reduction in cybersecurity insurance premiums attributable to Bugcrowd	Interviews	9%	9%	9%
Dt	Avoided cybersecurity insurance premium costs	D1*D2	$27,000	$27,000	$27,000
	Risk adjustment	↓15%			
Dtr	Reduced cybersecurity insurance premium costs (risk-adjusted)		$22,950	$22,950	$22,950
	Three-year total: $68,850			**Three-year present value: $57,073**	

UNQUANTIFIED BENEFITS

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify:

- **Shorter time to remediation.** Several interviewees noted that insights provided by Managed Bug Bounty led to shorter vulnerability remediation times than solutions in their organizations' prior environments. The head of information security at a healthcare organization said, "So much of the research and discovery is handled by Bugcrowd and then the remediation advice gets us 80% to 90% of the way there for how to fix the vulnerability." Additionally, 19 survey respondents improved patching efficiency by 63% on average and improved efficiency retesting vulnerabilities by 66% on average with their organization's crowdsourced security engagement.
    - The senior manager of application security at a technology organization said: "Our confidence level from Managed Bug Bounty far exceeds any other detection mechanism we have. That's one of the areas where it provides a lot of value for us because we can immediately start working with a team on vulnerabilities. We don't need to do additional work to vet findings."
- **Improved relationship between developers and security due to better communication.** Interviewees noted that Managed Bug Bounty helped bridge communication gaps between security and developer teams, allowing for more robust security processes. The head of information security at a healthcare organization said: "[The relationship between developers and security] has improved because it's evident that the security team is concerned with the quality of our products, and [having Bugcrowd] allows us to communicate more frequently about security issues. It also highlights the importance of staying on top of our security posture. It creates more opportunities for ongoing conversations with our engineering teams and application owners."
- **Improved reputation and demonstration of security maturity.** Interviewees and survey respondents reported that Bugcrowd helped demonstrate security maturity, bolstering their brand and reputation from the vantage point of customers, partners, auditors, and other third-party stakeholders. Sixty-four

percent of respondents strongly agreed that their organization's crowdsourced security program builds their organization's brand confidence; 59% strongly agreed that their organization has improved customer retention or growth with security. The senior director of information security at an automotive company said: "A bug bounty program, or at least a vulnerability disclosure program, is now the new table stakes for vendor evaluations. I would think negatively of them if they don't have that."

- **Improved compliance reporting.** Interviewees said Bugcrowd demonstrated security posture health to regulators and sped up reporting processes. The head of information security at a healthcare organization said: "[Having Bugcrowd] helps to show that we take security seriously and satisfy regulatory reporting requirements for SOC 2 that has penetration testing requirements, and so does HIPAA, even if there's no reporting requirement there. We save 10 to 15 hours annually [on reporting]."
- **Effective researcher pairing and strong vendor support.** Interviewees said Managed Bug Bounty provided high-quality and effective researchers, AI algorithms, and required data for sourcing and activating specific skill sets, program management, and overall vendor support. This resulted in higher accuracy, fewer false positives, and more edge cases identified. The head of information security at a healthcare organization said: "I have found that the researchers that I've been paired with via Bugcrowd and their 'secret sauce' platform have resulted in very high-quality interactions with their researchers. The communication has been very fast and efficient." The same interviewee said: "I'm thrilled to have Bugcrowd in my corner. They're an essential part of keeping our organization and our customers data safe. I'm very glad that they're my partner."
- **Flexibility to adapt to changing threat environments without new hires or onboarding new tools.** Interviewees noted that Managed Bug Bounty engagements gave them access to scalable, diverse talent to provide cost effective and timely response to threats. This addition to their security risk management program allowed interviewees' organizations to forgo onboarding additional new hires and tools. The head of information security in a healthcare organization said, "[Bugcrowd] is competitive and cost-effective with an increase in quality from what I've seen in the market, which is quite amazing."

> "It's often difficult for developers to understand all the ways hackers can abuse our systems. When the Bugcrowd researchers submit their submissions with sometimes very creative findings, it helps our engineering teams better understand how to protect the next update or change they will make next."
>
> SENIOR MANAGER OF APPLICATION SECURITY, TECHNOLOGY

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Managed Bug Bounty and later realize additional uses and business opportunities, including:

- **Opportunities to expand bug bounty engagement type and cadence.** Interviewees noted that Bugcrowd provides several paths to expand bug bounty engagements to maximize value. Organizations can choose between periodic or continuous engagements; to test preproduction environments or production environments; to run engagements privately or publicly; and to evolve toward a fully open scope for testing. This flexibility allows organizations to tailor Managed Bug Bounty services for specific security needs. The head of information security at a healthcare organization said: "My projection and intent is to launch a continuous Bug Bounty engagement in 2024, a private Bug Bounty engagement that ideally will evolve to a public Bug Bounty engagement in the following year or two. That's a good progression for leveraging Bug Bounty. Once you get to the point where you can leverage a public Bug Bounty engagement, you're really

demonstrating that you're working with the security community and also taking your security posture very seriously."

- **Increase internal awareness of the importance of continuous security testing.** Conveying the importance of a rigorous security programs can be difficult. The head of information security at a healthcare organization told Forrester that using Managed Bug Bounty helped elevate that message: "[Using Bugcrowd] has internally elevated the awareness of the importance of continually testing the security of your product. Every time that we run a Bug Bounty, there's a lot of internal communication about it and it conveys the fact that we care a great deal about our security posture. As a result, it has raised the security awareness of the entire organization, which is one of the positive side effects that I maybe wouldn't have thought of but I certainly welcome. It makes security an ongoing conversation in the leadership level of the organization."

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Etr	Managed Bug Bounty costs	$0	$210,000	$210,000	$210,000	$630,000	$522,239
Ftr	Implementation and change management	$11,316	$0	$0	$0	$11,316	$11,316
	Total costs (risk-adjusted)	$11,316	$210,000	$210,000	$210,000	$641,316	$533,555

MANAGED BUG BOUNTY COSTS

Evidence and data. Interviewees noted that Bugcrowd Managed Bug Bounty consisted of a platform fee and payments in a rewards pool that were reserved to incentivize and payout to researchers. Platform fees and reward pools varied depending on sizing and requirements. Contact Bugcrowd for additional details.

Modeling and assumptions. Based on the interviews and survey, Forrester assumes the following about the composite organization:

- The composite organization incurs a $100,000 annual platform cost. Platform fees may vary.
- The composite organization spends $100,000 annually on the rewards pool that is used to pay researchers. Reward pool size may vary.

Risks. Forrester recognizes that these results may not be representative of all experiences. The impact of this cost will vary depending on:

- Organization size, employee count, and assets in scope.
- Bug Bounty engagement type, frequency, and rewards structure.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $522,000.

Managed Bug Bounty Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Managed Bug Bounty platform costs	Composite		$100,000	$100,000	$100,000
E2	Managed Bug Bounty rewards pool costs	Composite		$100,000	$100,000	$100,000
Et	Managed Bug Bounty costs	E1+E2		$200,000	$200,000	$200,000
	Risk adjustment	↑5%				
Etr	Managed Bug Bounty costs (risk-adjusted)		$0	$210,000	$210,000	$210,000
	Three-year total: $630,000		**Three-year present value: $522,239**			

IMPLEMENTATION AND CHANGE MANAGEMENT

Evidence and data. Interviewees told Forrester that the change management and implementation to launch their organizations' Managed Bug Bounty engagements were low effort. The senior director of information security and IT at an automotive organization told Forrester: "We spent 40 hours combined starting up our Bug Bounty program, very low effort. It's a white-glove experience. They are good at what they do. They do this all the time, making it very easy and convenient and saying it's almost intuitive."

Modeling and assumptions. Based on the interviews and survey, Forrester assumes the following about the composite organization:

- The composite organization handles all change management and implementation requirements to begin its continuous Managed Bug Bounty engagements with three SecOps FTEs who dedicate 40 hours each.
- The hourly fully burdened rate for the SecOps FTEs is $63.

Risks. Forrester recognizes that these results may not be representative of all experiences. The impact of this cost will vary depending on:

- Security maturity and internal expertise.
- Engagement type and scope.

- Additional ongoing costs incurred for internal security teams triaging findings or integrating Bugcrowd with internal vulnerability tracking changes.

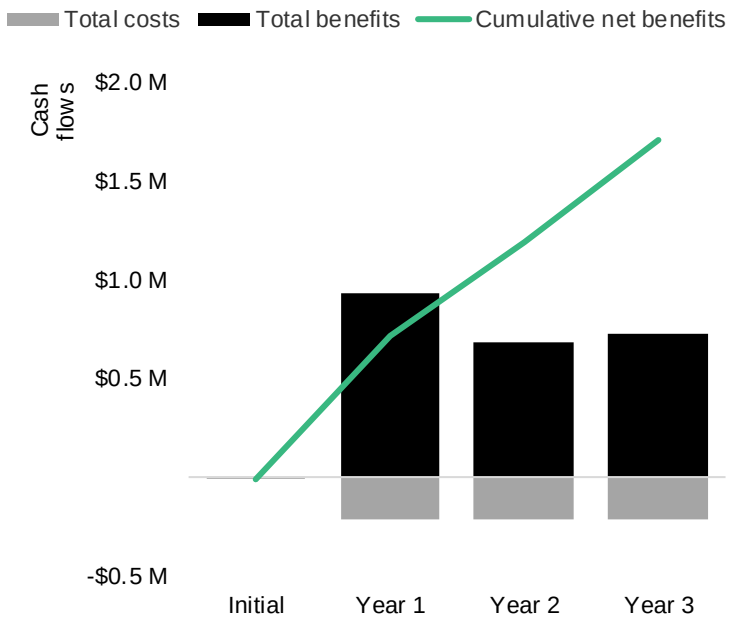
Results. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $11,000.

Implementation And Change Management						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Total hours spent implementing Bugcrowd	Interviews	40			
F2	Number of SecOps FTEs	Composite	3			
F3	Hourly SecOps fully burdened rate	TEI standard	$82			
Ft	Implementation and change management	F1*F2*F3	$9,840	$0	$0	$0
	Risk adjustment	↑15%				
Ftr	Implementation and change management (risk-adjusted)		$11,316	$0	$0	$0
	Three-year total: $11,316			**Three-year present value: $11,316**		

Financial Summary

Consolidated Three-Year, Risk-Adjusted Metrics

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($8,694)	($210,000)	($210,000)	($210,000)	($638,694)	($530,933)
Total benefits	$0	$889,254	$685,643	$773,658	$2,348,554	$1,956,320
Net benefits	($8,694)	$679,254	$475,643	$563,658	$1,709,860	$1,425,387
ROI						268%
Payback						<6 months

APPENDIX A: TOTAL ECONOMIC IMPACT

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

Total Economic Impact Approach

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

PRESENT VALUE (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

NET PRESENT VALUE (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made unless other projects have higher NPVs.

RETURN ON INVESTMENT (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

DISCOUNT RATE

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

PAYBACK PERIOD

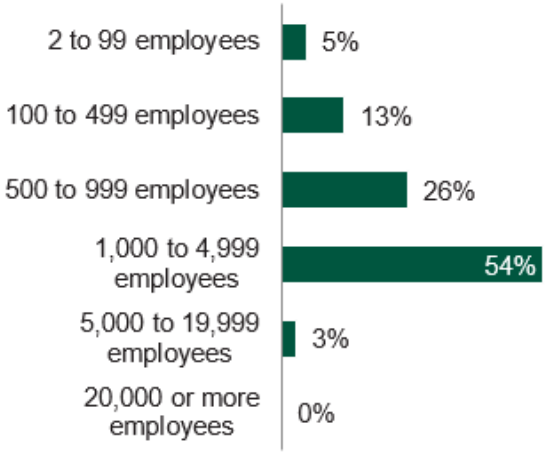
The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

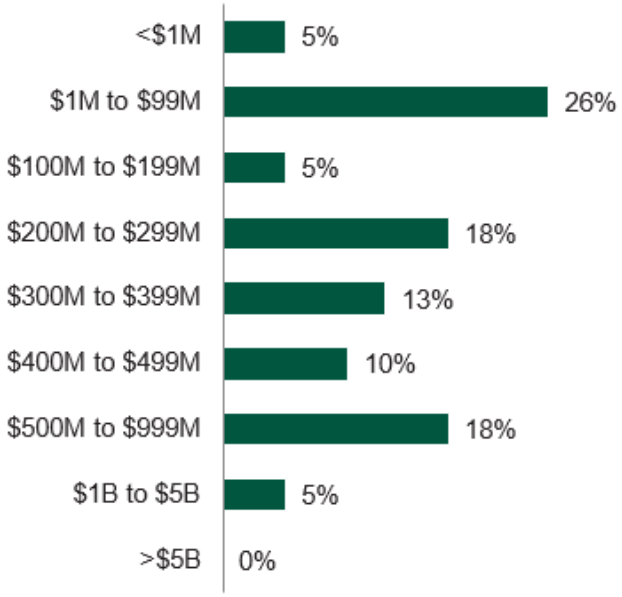
APPENDIX B: INTERVIEW AND SURVEY DEMOGRAPHICS

Interviews			
Role	**Industry**	**Region**	**Annual Revenue**
Global CISO	Telecommunications	Australia HQ, international operations	$15B+
Senior director of information security and IT	Automotive	US HQ	$2.5B+
Senior manager of application security	Technology	US HQ, international operations	NA
Head of information security	Healthcare	US HQ	$300M+

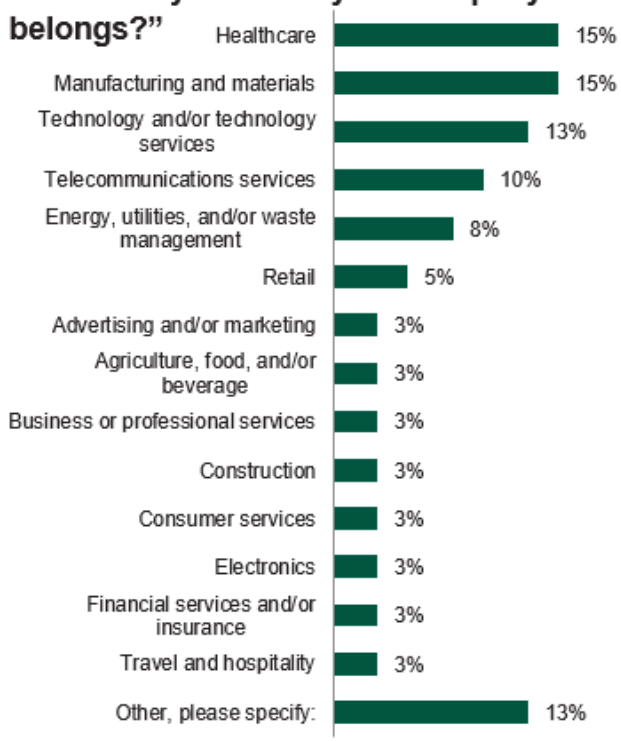
"Using your best estimate, how many employees work for your firm/organization worldwide?"



"Using your best estimate, what is your organization's annual revenue (USD)?"



"Which of the following best describes the industry to which your company belongs?"



"What is your level of responsibility when it comes to cybersecurity technology and services at your organization?"

Base: 39 cybersecurity decision-makers at the manager level or higher who are responsible for security strategy, vulnerability management, security operations, or similar areas

Source: A commissioned study conducted by Forrester Consulting on behalf of Bugcrowd, January 2024

APPENDIX C: ENDNOTES

[1] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

[2] Base: 39 cybersecurity decision-makers at the manager level or higher who are responsible for security strategy, vulnerability management, security operations, or similar areas; source: A commissioned study conducted by Forrester Consulting on behalf of Bugcrowd, January 2024.

[3] Forrester Business Technographics, Security Survey, 2023

[4] Base: 39 cybersecurity decision-makers at the manager level or higher who are responsible for security strategy, vulnerability management, security operations, or similar areas; source: A commissioned study conducted by Forrester Consulting on behalf of Bugcrowd, January 2024.

FORRESTER®