bugcrowd

DATA SHEET

VULNERABILITY DISCLOSURE

Vulnerability Disclosure Programs

Prove your commitment to security commitment and transparency

All organizations have to earn and maintain the trust of stakeholders by proving that they do everything possible to secure their systems and data. Vulnerability Disclosure Programs (VDPs) are now an industry standard (and often required for compliance) for proving a public commitment to a strong security posture. A complement to bug bounties and penetration testing, VDPs allow anyone on the internet to altruistically report any vulnerability they've found. Adoption of a VDP is proof that your organization understands the inevitability of vulnerabilities, and is committed to security transparency. But, most organizations lack the resources or expertise to stand up and manage a VDP on their own.

Your Managed "Neighborhood Watch"

The solution is a fully managed VDP on the Bugcrowd Platform. Bugcrowd's VDP solution–adopted by CISA in 2020 as the standard for U.S. civilian Federal agencies–includes vulnerability intake and tracking, continuous validation and triage, and program support, as well as developer tool integrations to accelerate discovery and remediation.

You get all the benefits of a well-run VDP, with none of the hassles and overhead of managing a program yourself. And, you can choose a price and entry point that makes sense for you, and even buy your plan directly online!

1 Week
Avg. time to launch Bugcrowd VDP

1 Month
Avg. time to first reported critical vulnerability

23
Avg. number of critical findings in 90 days

Key Points of Value



Meet compliance requirements
Align cybersecurity programs with best practices, as defined by the US Government, NIST, DOJ, FDA, and others.



Formalize security feedback
Create a channel for security feedback and a framework to manage vulnerabilities discovered by researchers.



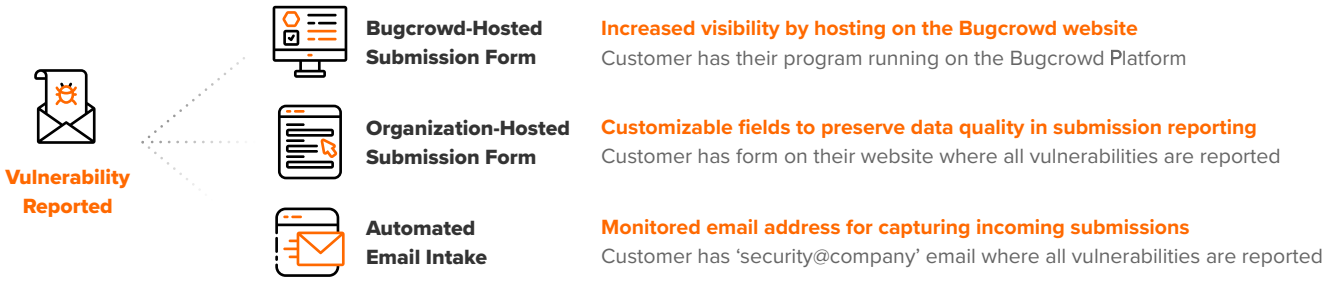
Lower operational overhead
Centralize incoming reports on a cloud-based, managed solution that seamlessly integrates into your existing SDLC.

> Many customers complement this solution with Bug Bounty, Pen Testing as a Service, and Attack Surface Management. With Bugcrowd, you can get them all on a common, multi-service platform with a unified experience.

Get started with Bugcrowd today www.bugcrowd.com/try-bugcrowd

Which Program Is Best For Me?

As part of program setup, customers choose which intake method(s) suit their business goals. Monitored email and the embedded submission form helps capture findings by routine users, while the Bugcrowd hosted intake method in VDP Professional encourages greater participation by promoting the program to all Bugcrowd registered researchers. For organizations just ramping security testing initiatives, email and an embedded submission form (VDP Essentials) are a good start in ensuring vulnerabilities can be actioned quickly. When the program matures, and is ready for a greater volume and velocity of submissions, shifting to VDP Professional can help expand visibility and increase activity.



	Self-Managed	bugcrowd VDP Essentials	bugcrowd VDP Professional
Accept security feedback from a global community	✓	✓	✓
Dedicated Security@Company e-mail monitoring	✗	✓	✓
Customized embedded submission form for improved data quality	✗	✓	✓
Real-time vulnerability view & on-demand platform reporting	✗	✓	✓
Fully managed vulnerability triage and prioritization	✗	✓	✓
Embedded remediation advice on every valid vulnerability	✗	✓	✓
Relationship management to reduce friction between expectant researchers	✗	✓	✓
Continuous availability for rapid development cycles and greatest risk reduction	✗	✓	✓
Developer tool integrations like JIRA, GitHub, and Service Now for faster fixes	✗	✓	✓
Options for retesting available on all resolved vulnerabilities	✗	✓	✓
Publicize program through Bugcrowd.com hosted page to promote increased activity	✗	✗	✓

BUGCROWD | VULNERABILITY DISCLOSURE

DATA SHEET

Lifecycle of a Vulnerability

External party on the internet submits a vulnerability via your preferred intake method

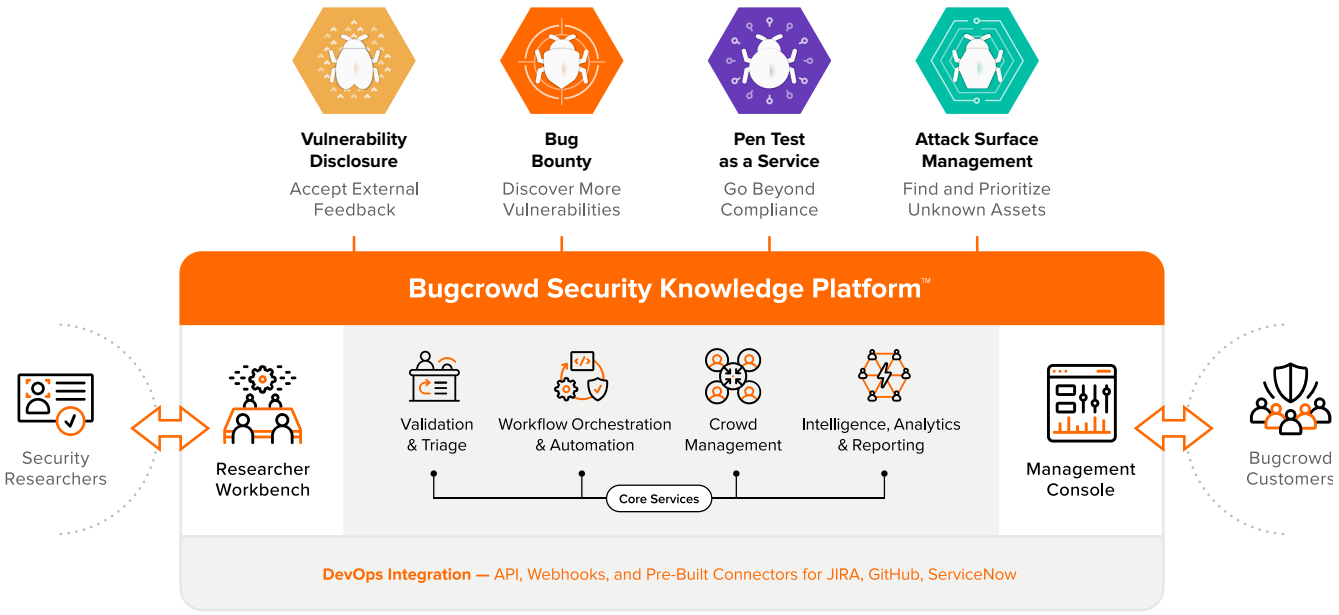
Bugcrowd de-dupes, validates scope and impact, and triages the bug, works with reporter as needed, and documents replication and remediation steps

You review the submission, and if needed, contact Bugcrowd for further info with rapid response

After confirming remediation, you may request re-testing by Bugcrowd engineers

Bugcrowd Security Knowledge Platform™

Bugcrowd is more than just a crowdsourced security company; we are a community of cybersecurity enthusiasts, united by a common purpose: to safeguard organizations from attackers. Our AI-powered, multi-solution crowdsourced security platform is built on the industry's most extensive repository of vulnerabilities, assets, and hacker profiles. This ensures that we identify the perfect hacker talent for each unique challenge, providing the scalability and adaptability needed to defend against threats, no matter how unique they may be.



Right Crowd, Right Time

Need special skills? We match the right trusted hackers to your needs and environment across 100s of dimensions using AI (CrowdMatch™).

Engineered Triage At Scale

Using an advanced toolbox in our the platform, our global team rapidly validates and triages submissions, with P1s often handled within hours.

Insights From Security Knowledge Graph

We apply knowledge developed over a decade of experience across thousands of customer programs to help you make continuous improvements.

Works With Your Existing Processes

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

TESLA indeed credit karma Walmart mastercard ATLASSIAN

Get started with Bugcrowd today: bugcrowd.com/try-bugcrowd