bugcrowd

DATA SHEET

VULNERABILITY DISCLOSURE

Vulnerability Disclosure Programs

A managed approach to public vulnerability reporting and disclosure

Going Beyond Reactive Cybersecurity

Today, all organizations have to adopt strategies to 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 a required one 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.

Your Managed "Neighborhood Watch"

Bugcrowd's fully managed VDP solution--adopted by CISA in 2020 as the standard for U.S. civilian Federal agencies—comprises platform-powered vulnerability submission and tracking, continuous triage, validation, and program support, as well as developer tool integrations to accelerate discovery and remediation. Risk reduction starts on Day 1, and most VDP Professional customers see results rapidly.

1 Week
Avg. launch time for a VDP with Bugcrowd

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.

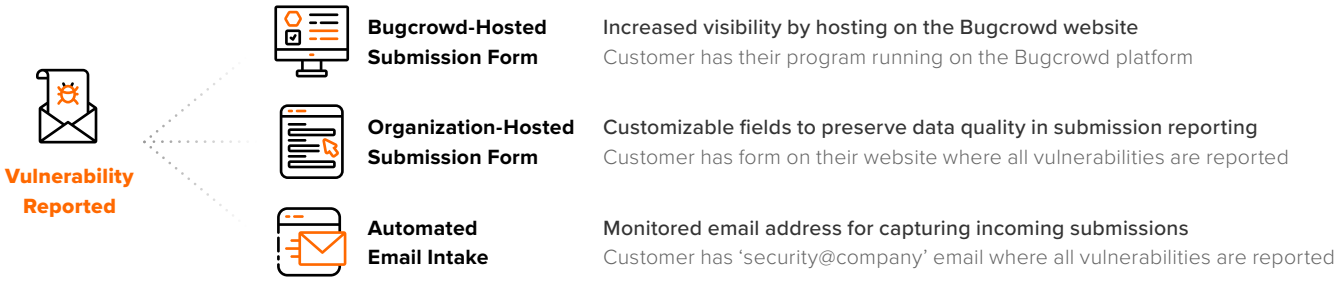
Lower operational overhead
Centralize incoming reports on a cloud-based, managed solution that seamlessly integrates into your existing software development lifecycle (SDLC).

Many customers complement a Bugcrowd VDP 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.

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

How It Works

Bugcrowd VDP improves program health and activity over and above self-managed models by offloading time-consuming, yet vital, VDP operations. Our VDPs are fully managed on the Bugcrowd Platform, so our team handles program design and deployment, as well as vulnerability triage, validation, and prioritization. And because the platform is integrated with your DevSec processes, prioritized VDP findings flow into them for rapid remediation.

Program Onboarded
Bugcrowd documents your disclosure policy and sets up a secure feedback channel.

Vulnerabilities Discovered
Any external party may identify and report a security vulnerability.

Feedback Accepted
The Bugcrowd platform processes security feedback received from external sources.

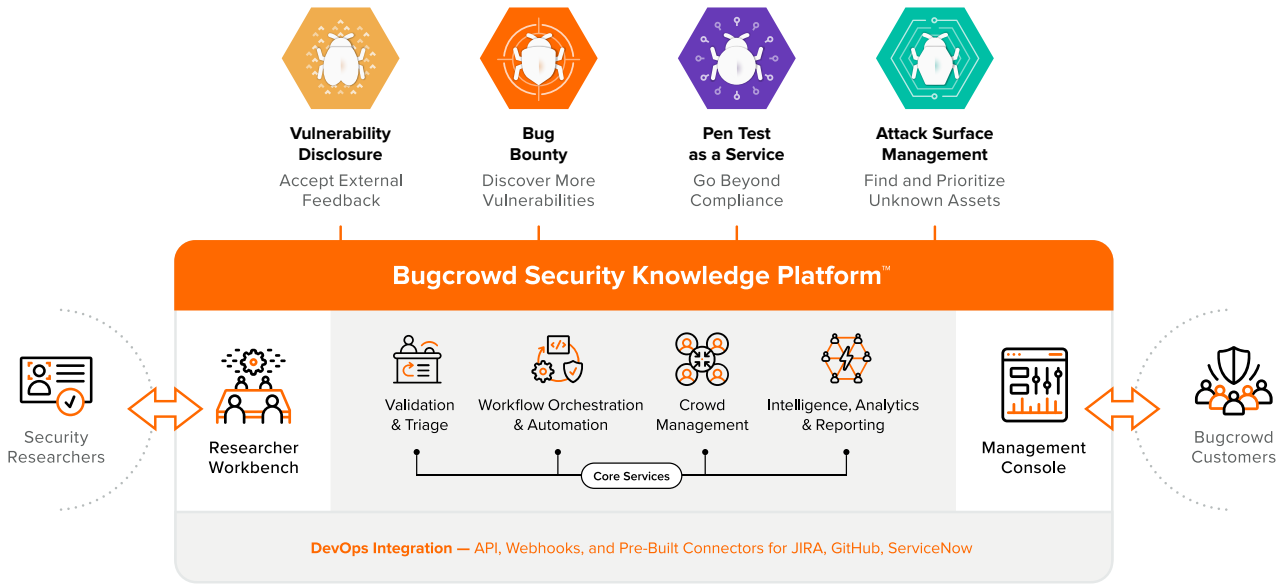
Submissions Triaged
Our team validates, standardizes, and prioritizes all incoming vulnerability reports.

Findings Delivered and Accepted
Your team reviews valid, well-documented findings and confirms submissions.

Workflows Automated
The platform orchestrates a remediation plan with your security team and systems.

Bugcrowd Security Knowledge Platform™

Organizations of all kinds need to do everything proactively possible to protect themselves, their reputation, and their customers from being blindsided by cyber attacks. The Bugcrowd Security Knowledge Platform™ finds hidden vulnerabilities before attackers do by uniquely orchestrating data, technology, and human intelligence—including tapping into the global security researcher community ("the Crowd")—for solutions that span Pen Testing as a Service, Vulnerability Disclosure, Bug Bounty, and Attack Surface Management.



Best Security ROI from The Crowd

We match you with the right trusted security researchers for your needs and environment based on 100s 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 applications and APIs are continuously tested before they ship.