bugcrowd

DATA SHEET

Engineered Trust

How we build the right trusted hacker team for your program

Trusted hackers, security researchers, and pentesters are the lifeblood of the Bugcrowd Platform™

Our scaled, data-driven approach to vetting goes beyond what most organizations do for their own employees.

Earning Trust on the Bugcrowd Platform

On the Bugcrowd Platform, trust is earned incrementally based on a consistent track record of skill and professional behavior. Scoring is reflected in our CrowdMatch AI engine for matching hackers and pentesters with appropriate opportunities.

As hackers travel this "trust journey", they become eligible to participate in public, then private (including pen tests), and finally in restricted engagements – with their impact and rewards growing along the way.

For customers with special requirements (e.g., geolocation restrictions, security clearances, or specific certifications), we also offer:

- Access to hackers who have passed through optional ID verification and background-check checkpoints. (Note that only hackers and pentesters who have scored high on skill and behavior in past engagements are eligible for background checks.)
- "White-glove" tester sourcing (including customer, staff, and trusted referrals), outreach, interviews, and validation.

Code of Conduct, Standard Disclosure Terms, and Program Contracts

Every hacker who wishes to participate in any Bugcrowd program (public or private) must first agree to our Code of Conduct as well as sign Bugcrowd's Standard Disclosure Terms. Hackers also sign a program-specific contract alongside the Program Brief that stipulates permissible and prohibited methodologies, in and out-of-scope targets, and other expectations like reward tiers, API gateways, and more.

Additional Controls

For globally compliant payments, we automatically screen for and disqualify hackers from banned countries per OFAC, EU, OSFI, and HMT watchlists. When needed, the Bugcrowd Platform also supports safe, controllable access to firewalled targets through our Traffic Control technology. With Traffic Control, we can cut off access to a single user when necessary without adversely affecting the rest of the engagement.

The Trust Journey for Hackers