bugcrowd

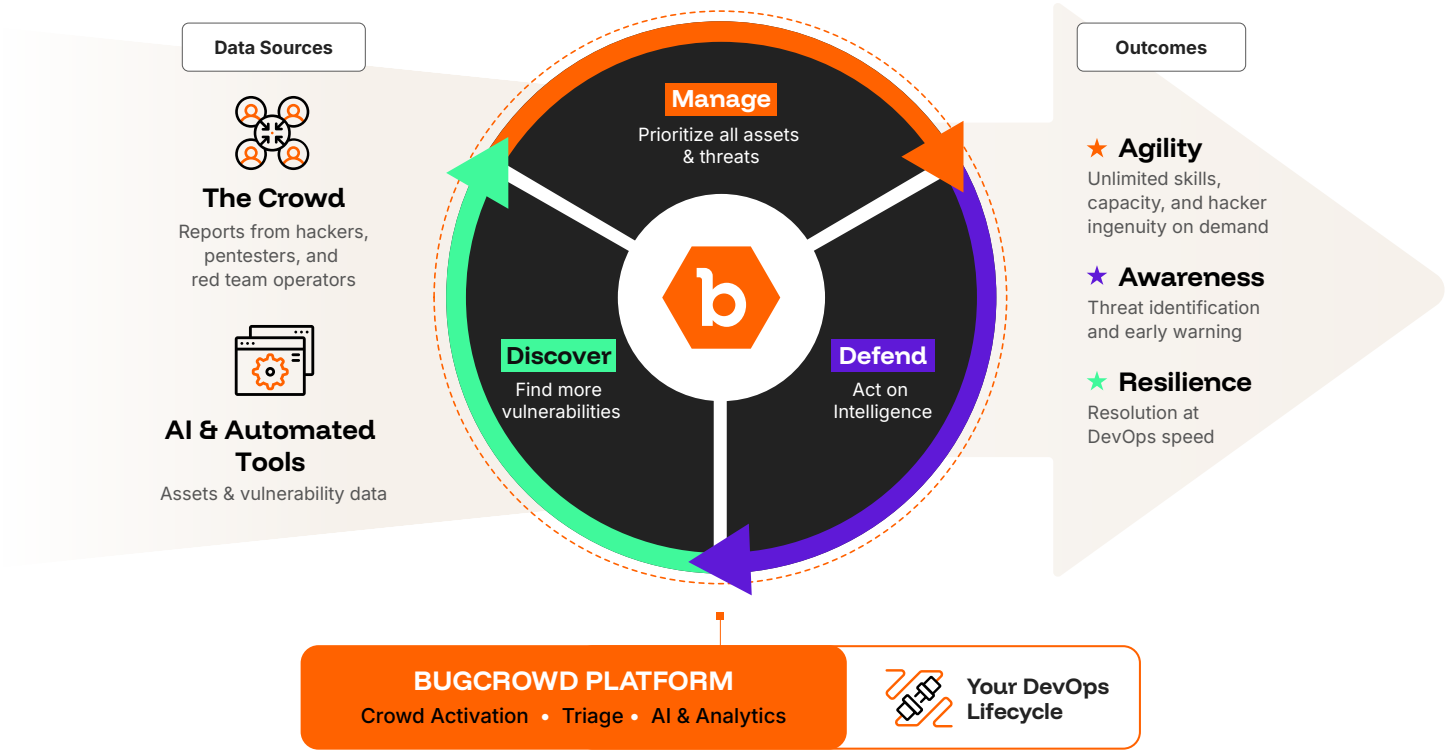
DATA SHEET

Bugcrowd Platform

Unleash human creativity for proactive cybersecurity

Imagine a security strategy where you're not just reacting to threats, but instead actively seeking them out before they cause damage.

That's why Bugcrowd exists: To help you protect assets from sophisticated threat actors before they can strike, taking back control of the attack surface and making proactive security a strategic advantage.



Agility

Augment Your Team On Demand

- Attacker mindset on tap for vulnerability discovery, pen testing, and red teaming
- 350+ skill sets and certifications available
- Crowd curation and activation guided by data and AI

Awareness

See and Prioritize Emerging Threats

- Continuous vulnerability intake, validation, and triage at scale
- 24/7 triage coverage with same-day response for P1s
- Early warning of emerging vulnerabilities

Resilience

Continuously Improve Security Posture

- Actionable reporting, benchmarking, and recommendations
- Directly integrates with existing tools for change at DevOps speed
- Deep bench of solution & support specialists at your side for quick wins and long-term ROI

Products

Our platform brings the agility and scale of crowdsourcing to multiple types of proactive testing, including:

Pen Testing as a Service

Test web apps, APIs, LLM apps, hardware devices, and other assets for common vulnerabilities in conformance with internal and external controls at a flat rate.

- ✓ Launch within 72 hours, with scoping enriched by full attack surface visibility and asset risk scores
- ✓ Get 24/7 visibility into timelines, prioritized findings, and tester progress
- ✓ On-demand, continuous, and subscription-based offerings available

Red Team as a Service

Simulate real-world attacks, on-demand or continuously, to assess resilience across people, processes, and technology.

- ✓ Tap into a worldwide network of vetted red team operators with skills matched to your environment and threat profile
- ✓ Uncover full attack paths, not just isolated vulnerabilities, to understand how threats move across your systems
- ✓ Choose a model that fits your organization's size, goals, and budget

AI Safety and Security Testing

Be confident that your AI/LLM applications are free of critical AI-specific flaws that can lead to high-profile incidents.

- ✓ Rely on experts in LLM prompts, social engineering, and AI to find issues only humans can find
- ✓ Uncover symptoms of multiple flaws, including security vulnerabilities and data bias
- ✓ Consume either as incentivized bug bounty or flat-rate pentesting, depending on the need

Bug Bashes | Live Hacking Events

Host a highly-skilled team of hand-picked specialists for a few days of intensive, onsite testing of software, infrastructure, or even hardware and devices.

- ✓ Build relationships with elite hackers who have the skill sets you need
- ✓ Find significantly more critical vulnerabilities than purely remote engagements, on average
- ✓ Rely on us for event/program design, planning, logistics, and management

Managed Bug Bounty

Incentivize hackers to discover hidden vulnerabilities that scanners miss, with scope and rewards determined by you.

- ✓ Uncover up to 7x more critical vulnerabilities than traditional testing
- ✓ Remove duplicates/false positives and prioritize findings, with critical issues handled in day
- ✓ Understand program health, ROI, and performance versus benchmarks

Managed Vulnerability Disclosure

Provide visual proof of security maturity by inviting the public to report flaws in your external-facing assets.

- ✓ Meet regulatory requirements for transparent vulnerability management
- ✓ Build initial relationships with the hacker community as a precursor to bug bounty
- ✓ Create initial integrations to engineering for fast remediation

Solutions for Every Maturity Stage

Different organizations address security in different ways. For customers on a crowdsourced security journey, we've found that as their capabilities and comfort level develops over time, they adopt increasingly proactive testing while building tighter integrations with engineering processes, with different stages reached either in part or as a whole.

Typical crowdsourcing journey

STAGE 1	STAGE 2	STAGE 3	STAGE 4
Testing is reactive and driven by controls & compliance	Results from traditional testing alone have become inadequate	Connection to Engineering is being fully built out, including feedback for training	Desire to "go deep" with intensive testing in specific business-critical areas
Tests are always time-bound *E.g. monthly scans & annual pentests*	First structured processes for routing validated findings to Engineering	Continuous testing is a standard, with full attack surface visibility	Pressure testing of overall security posture also becomes a goal
Focus is on common application vulnerabilities	First direct interactions with hackers	Economic levers are established for sourcing, activating, and rewarding external testers	Interest in identifying entire attack chains, not just vulnerabilities
Partial attack surface visibility and false positives are norms	First efforts at continuous testing with validation and prioritization	Testers are added to the virtual team on demand	Security culture and reputation are considered as important as resilience
KEY TOOLS			
Traditional Pentesting SAST/DAST	Vulnerability Disclosure Programs	Continuous Pentesting Bug Bounty	Red Team as a Service