bugcrowd

DATA SHEET

Crowdsourced Security

in the Public Sector

CHALLENGES

Every public-sector organization, from local utilities to Federal agencies, is under constant threat of attacks at every level of sophistication, including Advanced Persistent Threats from state-sponsored actors. For these regulated orgs (and increasingly, for critical infrastructure providers and government contractors), meeting the highest standards for security means going beyond the traditional solutions.

SOLUTION

The Bugcrowd Platform helps public sector customers defend themselves against cybersecurity attacks by connecting with trusted, skilled security researchers to take back control of the attack surface.

The public sector can benefit from a wide variety of Bugcrowd's crowdsourced solutions, including:

- **Managed Bug Bounty**
- **Vulnerability Disclosure Programs (VDPs)**
- **AI Bias Safety and Security Assessments**
- **Penetration Testing as a Service**
- **Attack Surface Management**

Examples of Bugcrowd's work in the public sector:

- CISA VDP
- AI Bias Bounty Program and Rapid Response Program for CDAO
- Department of Homeland Security VDP
- Bureau of Indian Affairs VDP
- State of CA VDP

Contract vehicles for procurement:

- ✓ NASA-SEWP
- ✓ Hack DHS IDIQ
- ✓ GSA via Carahsoft
- ✓ Tradewinds AI Marketplace

PUBLIC SECTOR USE CASES

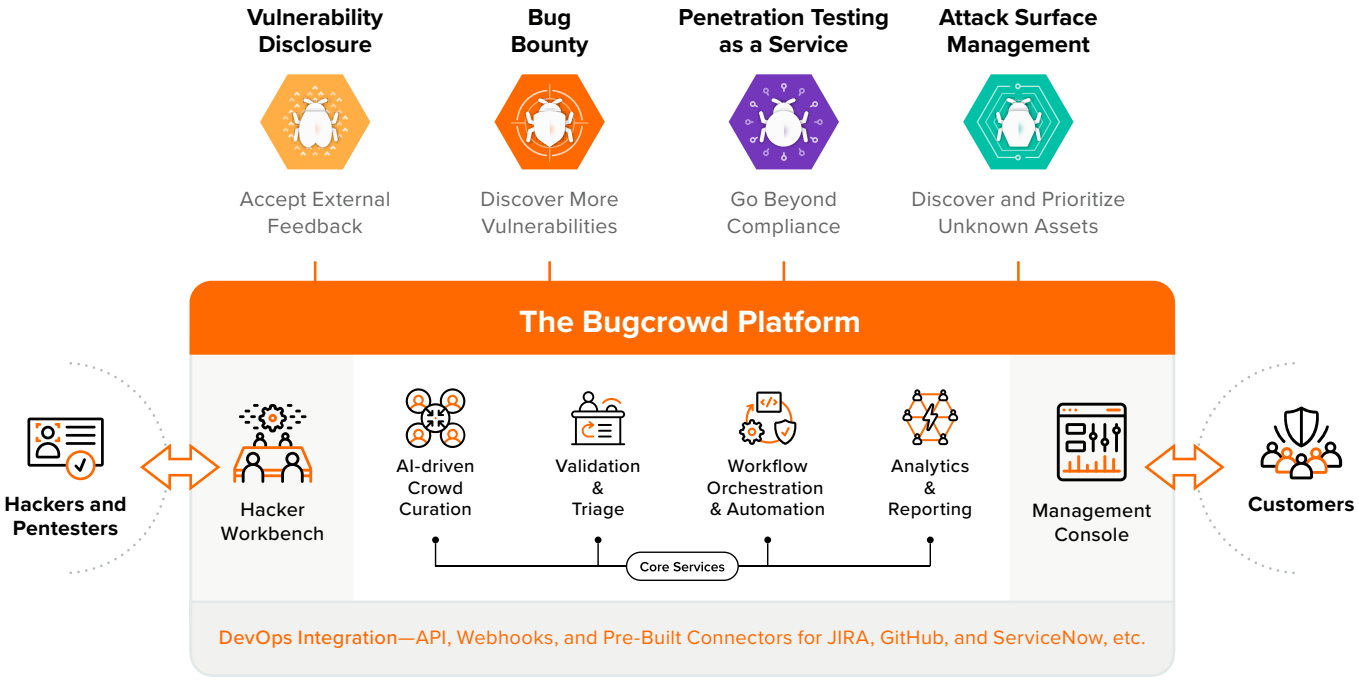
Binding Operational Directive 20-01	AI Safety and Security	Department of Defense (DoD) Cyber Operations	Election Security
VDPs are a federal mandate for Federal Civilian Executive Branch (FCEB) agencies. CISA has partnered with Bugcrowd and EnDyna to provide a VDP-as-a-service free-of-charge.	Executive Order 14410 mandates the safe and secure development and use of AI. AI Bias Assessments and AI Pen Tests take steps to identify and prioritize vulnerabilities and data bias flaws in LLM applications.	DoDI 8531.01 requires all DoD agencies to have a VDP to help confront a landscape where asymmetric threats are the norm. By using a VDP and Managed Bug Bounty, the DoD can significantly extend their reach, tapping into a wealth of knowledge.	Fears that U.S. election integrity is at risk for compromise are widespread. By leveraging a VDP for digital assets and a Managed Bug Bounty engagement for hardware assets, election technology providers can ensure election security and integrity.

Why Bugcrowd?

DATA SHEET

Our AI-powered platform for crowdsourced security is built on the industry's richest repository of data about vulnerabilities and hacker skill sets, activating the ideal hacker talent needed on demand, and bringing scalability and adaptability to address current and emerging threats.

THE BUGCROWD PLATFORM



Best Security ROI from the Crowd

We match you with trusted security researchers who are perfect for your needs and environment across hundreds of dimensions using machine learning.

Instant Focus on Critical Issues

Working as an extension of the platform, our global security engineering team rapidly validates and triages submissions, with P1s often handled within hours.

Contextual Intelligence for Best Results

We apply over a decade of knowledge accumulated from experience devising thousands of customer solutions to achieve your goals for better outcomes.

Continuous, Resilient Security for DevOps

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

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY · TESLA · indeed · credit karma · Pinterest · mastercard

Unleash Human Creativity for Proactive Security

TRY BUGCROWD