bugcrowd

Bugcrowd for Government

Scalable, FedRAMP-authorized security

Bringing elite offensive security talent to federal agencies

Federal agencies are under relentless pressure to do more with less. On the one hand, they face sophisticated adversaries such as state-sponsored actors, ransomware groups, and criminal syndicates. On the other hand, they must compete with the private sector for a limited pool of security talent, a competition intensified by salary caps and lengthy hiring processes. To overcome these challenges, many turn to offensive security methods like crowdsourced security programs. However, they face a 6–12-month provisional authority process before deployment. The result is a widening **gap between the complexity of modern threats and the resources available to counter them.**

Bugcrowd's FedRAMP Moderate Authorization gives federal agencies **immediate access to the power of hundreds of thousands of security researchers on the Bugcrowd Platform.** Hosted in AWS GovCloud, the Bugcrowd Platform supports an entire suite of offensive security testing methods, from Vulnerability Disclosure Programs (VDPs) and Managed Bug Bounty (MBB) programs to pen testing and even red teaming. **Agencies can now deploy proven**, on-demand security coverage in weeks instead of months.

Why federal agencies choose Bugcrowd

FedRAMP Moderate authorized

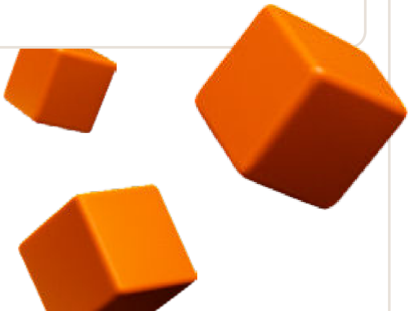
Bugcrowd meets the U.S. government's most rigorous security standard of FedRAMP Moderate Authorization, allowing federal agencies to bypass 6–12-month provisional authority processes and trust that Bugcrowd meets the highest possible security standards.

Data sovereignty and regional compliance

Bugcrowd's regional isolation architecture—required for FedRAMP authorization—enables organizations to maintain data residency compliance across multiple jurisdictions. The architecture supports the GDPR, local data protection laws, and sector-specific mandates for both federal and commercial operations.

Seamless integration

Direct integration with development tools and processes (Jira, GitHub, and ServiceNow) enables continuous testing throughout the development life cycle, allowing teams to catch vulnerabilities without disrupting existing workflows.



Managed triage and validation

Bugcrowd's security experts filter and validate every submission, delivering only exploitable, actionable vulnerabilities—not noise. This capability reduces alert fatigue and accelerates remediation for security teams that are already stretched thin.

Elite, vetted talent matched to your mission

Bugcrowd's CrowdMatch™ AI automatically matches your assets with qualified researchers who have the right expertise, eliminating lengthy sourcing processes and salary competition for security talent. Researchers undergo comprehensive background checks (financial, criminal, and employment), providing additional operational assurance for agencies handling classified, regulated, or mission-critical data.

Compliance and audit-ready reporting

The Bugcrowd Platform provides audit-ready documentation aligned with federal frameworks (NIST SP 800-53, NIST SP 800-171) and industry standards, simplifying compliance reporting and vendor audits. That's part of the reason why CISA selected Bugcrowd to run the BOD 20-01 VDP platform for 60+ federal agencies.

Trusting the Crowd

Historically, federal agencies have hesitated to turn to external security researchers for testing, as they were deterred by concerns about oversight, accountability, and perceptions about the process. Bugcrowd's FedRAMP Moderate Authorization changes that calculus, **giving agencies the confidence to tap into elite global security talent without fear of compromising compliance or control.**

"While there are still a few private companies wrestling with the notion of 'Crowd Fear,' the public sector has embraced working with security researchers, and has mandated the practice in BOD 20-01," says Bugcrowd's VP of Public Sector, Kent Wilson. "By going through the rigorous FedRAMP authorization process, we are **unlocking access to the ingenuity of the global security research community on a platform meeting strict government security standards.** We are providing federal teams with a disciplined, vetted, and secure environment to proactively defend their mission-critical assets with absolute confidence."

This trust is built into the Platform by design. For instance, researchers progress through a "trust journey," starting with public programs and advancing to private engagements only after demonstrating consistent success and ethical behavior.

At Bugcrowd, trust isn't assumed—it's earned. Every security researcher, pentester, and red teamer on our Platform undergoes a rigorous, data-driven vetting process that extends beyond what most organizations require for their own employees. Each member of the Crowd goes through a different level of vetting depending on the role. To learn more about security researchers, check out our eBook, Get to Know the Crowd.

Bugcrowd’s FedRAMP -authorized Platform

Vulnerability Disclosure Programs

Efficiently meet federal mandates with a managed Platform that turns researcher submissions into actionable intelligence.

A VDP provides a structured channel for security researchers to report vulnerabilities in public-facing assets, such as websites, APIs, and external applications. Binding Operational Directive 20-01 (BOD 20-01) requires all Federal Civilian Executive Branch agencies to implement a VDP, ensuring that good-faith researchers have a clear path to report security issues before malicious actors can exploit them. With Bugcrowd’s FedRAMP authorization, agencies can meet these requirements without facing lengthy procurement barrier

KEY BENEFITS

- ✓ **BOD 20-01 compliance:** Deploy a fully managed VDP that meets federal requirements in weeks, not months—without building additional internal infrastructure.
- ✓ **Scalable coverage:** Keep pace with an expanding attack surface as new digital services launch, without the delays and costs of traditional hiring.
- ✓ **Elastic testing resources:** Rapidly scale researcher engagement up or down based on deployment cycles, threat landscapes, or budget availability.
- ✓ **Continuous vulnerability discovery:** Leverage a global researcher community that identifies and reports critical issues as they surface, not during annual assessment windows.
- ✓ **Cost-effective:** Pay for validated results instead of competing with private sector salaries for scarce offensive security talent.

Managed Bug Bounty

Proactively secure mission-critical applications and infrastructure through a Platform that connects you with elite security talent on demand.

While VDPs address vulnerabilities in public-facing assets, Managed Bug Bounty programs allow agencies to directly connect with researchers to test private applications. This controlled testing environment means agencies can validate security before deploying new capabilities, assess systems that handle classified or sensitive data, and access specialized expertise that's difficult to maintain in-house—all through a pay-for-results model that eliminates the risk of budget waste.

KEY BENEFITS

- ✓ **Pre-deployment security validation:** Test applications, APIs, and infrastructure before they go live, catching critical vulnerabilities during development rather than after adversaries find them in production.
- ✓ **Ongoing assessment of critical infrastructure:** Maintain continuous security coverage across systems that support essential operations, resulting in the identification of emerging threats before attackers can exploit them.
- ✓ **Specialized expertise matched to your security challenges:** Access researchers with specialized expertise in application security, cloud architecture, and API testing—capabilities that are difficult to develop and retain across diverse federal missions.
- ✓ **Easily scale up or down to augment existing teams:** Scale testing resources up during high-priority initiatives, major deployments, or mergers/acquisitions without long-term staffing commitments.
- ✓ **Pay only for validated vulnerabilities:** Budget goes toward actual security findings, so every dollar spent directly improves security posture.

Penetration Testing as a Service (PTaaS)

Reduce risk and meet compliance needs by finding common vulnerabilities at a flat rate.

PTaaS modernizes the world of traditional pen testing. CREST-certified penetration testers can search for common vulnerabilities on all government assets via a modern Platform integrated with your existing tools and processes.

KEY BENEFITS

- **More speed and scale:** Launch in less than 72 hours with prioritized vulnerabilities flowing directly into existing DevSec tools and processes for fast remediation.
- **Curated pentester teams:** Get expertly matched with a qualified, engaged team of elite pentesters, selected based on your specific requirements.
- **See progress in real time:** View, manage, and analyze findings via a rich dashboard offering statistics and full visibility into methodology checklist progress.
- **Set cost:** Pay a flat rate for pen tests, streamlining budgeting and planning.

Red Team as a Service (RTaaS)

Assess full security posture across people, processes, and technology.

Simulate real-world attacks with speed, scale, and precision. RTaaS helps agencies test their defenses the way attackers would—so they can fix what matters, faster. RTaaS delivers persistent, real-world attack simulations that reflect how today's threats unfold across people, processes, and technology. Unlike traditional approaches, RTaaS gives federal security teams flexibility to act on insights and address vulnerabilities before adversaries can exploit them.

KEY BENEFITS

- **Attack chains, not just findings:** Uncover full attack paths, not just isolated vulnerabilities, to understand how attackers and nation-state threat actors move through federal systems.
- **The right experts for every threat:** Tap into a worldwide network of vetted red team operators with skills matched to the public sector environment and agency-specific threat profiles.
- **Full control of engagement scope:** Federal teams benefit from a structured "go/no-go" process on all attack approval chains, ensuring rigorous risk management and operational stability.

Alignment with federal cyber mandates

The Bugcrowd for Government Platform aligns with the frameworks that federal agencies already use for security and compliance. With FedRAMP authorization, agencies can quickly get set up with the Platform, allowing them to meet these mandates much faster.

Two main mandates that Bugcrowd solutions support include BOD 20-01 and BOD 22-01.

BOD 20-01	BOD 22-01
What it covers	**What it covers**
Vulnerability disclosure mandate for all Federal Civilian Executive Branch agencies.	Requirement to reduce the significant risk of known exploited vulnerabilities.
How Bugcrowd supports	**How Bugcrowd supports**
Direct operational support through CISA-trusted VDP platform.	Offensive testing can help agencies find and remediate vulnerabilities faster.

A key framework to note is NIST SP 800-53. This includes 300+ security controls, such as access control, continuous monitoring, incident response, data protection, and change management. Bugcrowd inherits these controls through our moderate FedRAMP authorization.

Here is a quick overview of how different Bugcrowd solutions satisfy different control requirements of the NIST SP 800-53 framework.

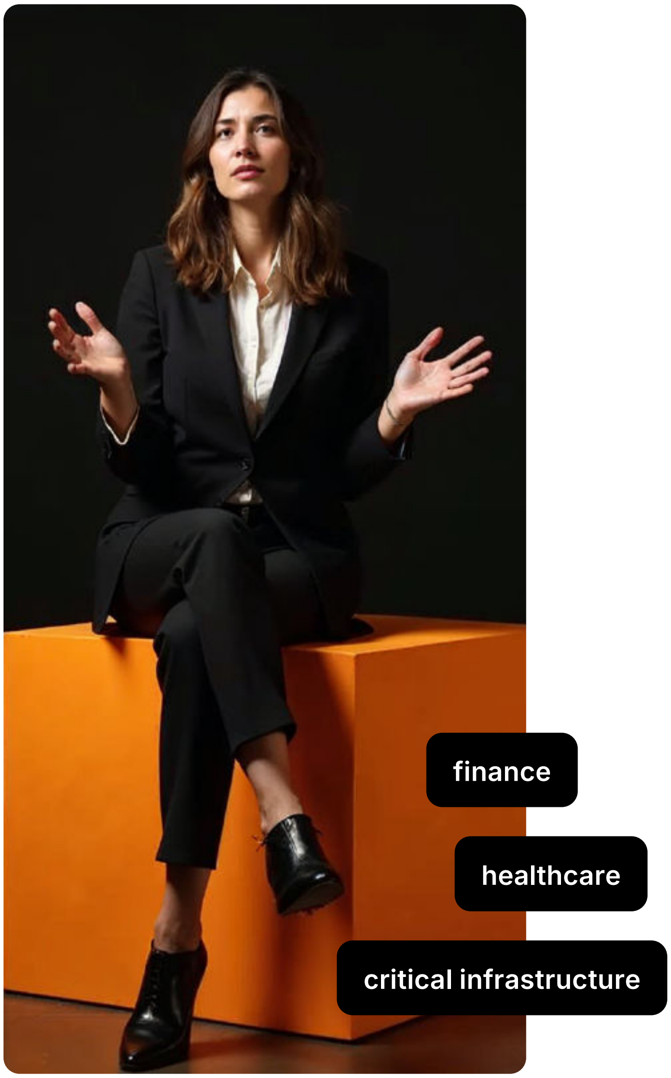
NIST 800-53 control	Description	How Bugcrowd supports
CA-8	Penetration testing	Penetration testing
CA-8(2)	Red team exercises	Red teaming
CA-2	Control assessments	Penetration testing Red teaming
RA-5(11)	VDP	VDP Bug Bounty
RA-5	Vulnerability Monitoring	VDP Bug Bounty Penetration testing
SI-2	Flaw remediation	VDP Bug Bounty (Feeds the process)
IR-3	Incident response testing	Red teaming
AT-2 / AT-3	Security awareness/ role-based training	Red teaming (Testing human controls)

Why FedRAMP authorization matters for the private sector

For organizations in **finance, healthcare, and critical infrastructure,** Bugcrowd's FedRAMP authorization provides a signal of security maturity that resonates with boards, auditors, and regulators alike. It represents a stamp of approval from the U.S. government's rigorous standards while providing organizations with the flexibility and expertise to improve their security posture.

> **Another major benefit to the private sector is this authorization process has unlocked strong controls for customers with data sovereignty concerns or mandates to isolate their data in specific regions of the world.**

Whether you're an organization that has decided to adopt federal standards, one that is handling sensitive data, or one that needs to operate under regulations like GDPR, customers can work with us to deploy a secured platform anywhere in the world.



Get started with Bugcrowd for Government today

Bugcrowd’s FedRAMP-authorized platform enables federal agencies to deploy offensive security testing to meet key federal mandates (like BOD 20-01 and BOD 22-01) and secure existing attack surfaces with full confidence.

Ready to get started?

Request a demo to see Bugcrowd’s Platform in action