bugcrowd

DATA SHEET

PEN TEST AS A SERVICE

Cloud Penetration Testing

Find hidden vulnerabilities with specialized talent

Whether your organization is in the midst of digital transformation and the adoption of cloud services, or a digital native company that was born in the cloud, the use of IaaS, PaaS, and SaaS can be a risky endeavor. The adoption of new solutions, such as cloud data lakes, microservices, containers, the move to cloud-native web applications, and the reliance on new identity stores, tokens, and APIs, all expand an organization's attack surface.

While regular testing can help, organizations face significant trade-offs in available options: Scanners are fast, but typically, they only surface low-hanging fruit and are almost always more noisy than useful. Traditional pen test providers leverage critical human creativity, but they do so as cumbersome consulting engagements that take too long and leave you in the dark about results.

Specialized Cloud Pen Testing

Managed through the Bugcrowd Security Knowledge Platform™, our cloud pen tests cover cloud-native web applications in addition to cloud infrastructure and APIs. They can also be deployed against nearly any target type or environment—AWS, Azure, Google Cloud, and more.

A thorough discovery of flaws in Cloud apps requires specialized knowledge, skills, and experience. For this reason, Bugcrowd Cloud Pen Testing brings the talents of a global community of security researchers, precise crowd matching via our CrowdMatch™ ML technology, 24/7 visibility, and the vast reservoir of vulnerability data in the Bugcrowd Security Knowledge Platform™ to bear on every pen test engagement.

Every assessment includes:

- Dedicated, vetted pentesters matched by skill, experience, and performance
- Strict adherence to Bugcrowd's BugHunter Methodology™ including best practices from the OWASP Testing Guide, SANS Top 25, CREST, WASC, PTES, and more
- 24/7 visibility into timelines, findings, and pentester progress through their checklist via a rich dashboard
- Validation and prioritization according to Bugcrowd's Vulnerability Rating Taxonomy (VRT)
- End-to-end program management with the industry's highest signal-to-noise ratio
- Detailed auditor report

Key Points of Value

Start testing faster

Use the power of the Bugcrowd Platform to start your testing in as little as 72 hours.

Expert testers are matched to your requirements

CrowdMatch™ ML technology helps rapidly align the right skills and experience for the engagement.

See results in real time

Leave opaque pentesting behind. Instead, view prioritized findings as they're reported, and flow them into your SDLC for fast remediation.

Testing can be customized to suit individual testing needs--including expedited launches, re-testing, and special pentester requirements.

Cloud Testing Methodology

With Bugcrowd, you'll have comprehensive visibility of your entire cloud attack surface. Our crowdsourced testing methodology blends industry and operational best practices to drive both risk reduction and compliance for customers with varying priorities. Bugcrowd's Cloud Pen Test methodology is a phased approach. Each phase is executed in a cyclical manner, allowing penetration testers to build upon findings and potentially uncover significant risk.

Reconnaissance and Enumeration

Utilize various search engines and data sources to uncover assets and information helpful for understanding attack vectors. This may include, but is not limited to the following:

- External asset discovery
- Hard-coded and leaked credentials, keys and tokens
- Internal assets, known software, and others.

Scanning

Combine automation, tooling, and human ingenuity

- Fully scan the range of in-scope targets on all cloud accounts, containers, data stores, and others.
- Enumerate and document all in-scope services and version numbers.
- Check for unencrypted services (telnet, HTTP, and others).
- Review services to determine if any of them are exposing sensitive information.
- Conduct optional automated scans to detect "low-hanging fruit".

Exploitation and Documentation

Verify security weaknesses and collect results

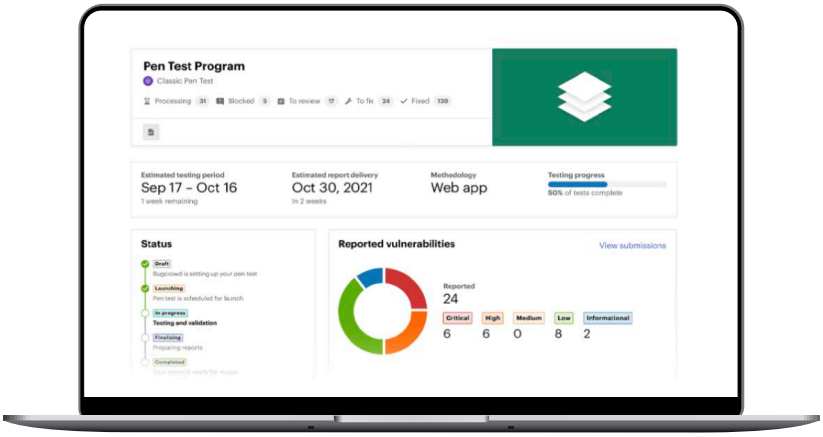
- Test for authorization bypasses (insecure implementations of OAuth, SAML, and others).
- Leverage discovered services to obtain additional information about the targets.
- Check for service misconfigurations and deployment mistakes.
- Attempt to discover exposed files containing sensitive information (database backups, open Git repositories, unsecured storage services, and others).
- Check for default/weak credentials on all available services (HTTP, telnet, SSH, SNMP, and others).
- Check for weak encryption (SSL/TLS ciphers, older protocols, and others).
- Check for known/public exploits on discovered services by cross-referencing software version numbers against public vulnerability databases.
- Attempt calculated brute-forcing on available cloud services based on information gathered earlier in the assessment.
- Test web apps, servers, and APIs for common exploits, such as SQL injection (SQLi), remote code execution (RCE), and others.
- Check for over-exposed endpoints available via APIs, lack of resource and rate limiting, excessive data exposure, and others.

BUGCROWD | PEN TEST AS A SERVICE

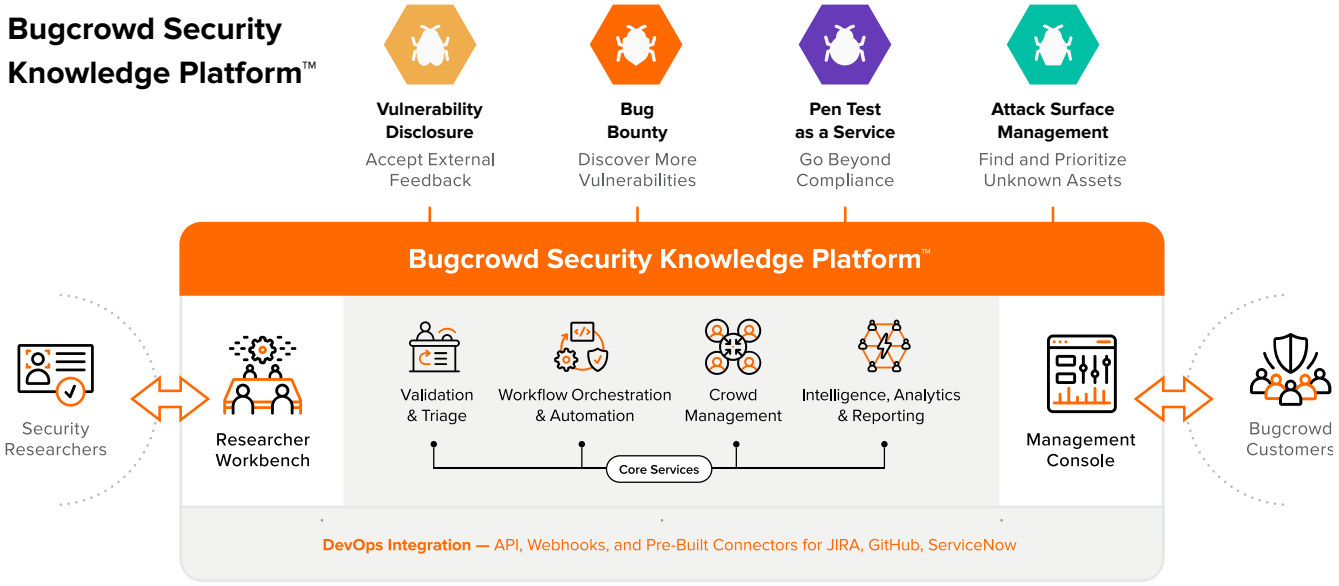
DATA SHEET

How It Works

The Bugcrowd Security Knowledge Platform™ makes it easy to configure and launch pen tests for any asset. After building a pentester team per your exact needs, we'll launch your pen test within days and give you 24/7 access to prioritized results, along with test status and progress, in a rich dashboard. When your test is complete, you can download a detailed report for compliance directly inside your dashboard.



Bugcrowd Security Knowledge Platform™



Right Crowd, Right Time

Need special skills? We match the right trusted hackers to your needs and environment across hundreds of dimensions using AI (CrowdMatch™).

Engineered Triage at Scale

Using an advanced toolbox in our the platform, our global team rapidly validates and triages submissions, with P1s often handled within hours.

Insights From Security Knowledge Graph

We apply knowledge developed over a decade of experience across thousands of customer programs to help you make continuous improvements.

Works With Your Existing Processes

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

TESLA indeed credit karma Walmart mastercard ATLASSIAN

Get started with Bugcrowd today bugcrowd.com/pen-test-pricing