bugcrowd

ASM ASSET INVENTORY

Attack Surface Management
Asset Inventory™

Rapid and Continuous Asset Discovery and Management

Bugcrowd ASM Asset Inventory is a software-based solution for continuous asset discovery and management. One of two modules within the Bugcrowd Attack Surface Management solution, Asset Inventory™ combines human ingenuity with insights gleaned from over 1,200 managed programs to help customers find, connect, and prioritize more of their unknown attack surface before it can be compromised. Asset Inventory complements the second module, Asset Risk, by providing continual discovery, inventory, alerting, and management controls for every organization's internet-facing asset map.

Continuous Control

With configurable alerts and "smart folder" activation, Asset Inventory enables you to quickly see, communicate, and manage changes in your internet-facing digital landscape to reduce risk across even the most dynamic attack surfaces. Fed by years of internet data and powered by flexible querying and rules-based alerting, Asset Inventory provides the visibility and control required to effectively manage the world's most dynamic attack surfaces.

How It Works

Setup is quick and easy, with results populating in a matter of seconds.

Add
Add domain names to your inventory; subdomains get added instantly.

Fingerprint
Extensive technology fingerprinting is applied to each asset in your inventory.

Suggest
Other domain names that you own are suggested to you as possible additions.

Automate
Continuous discovery keeps your inventory up to date and alerts you of changes.

The Value We Deliver

Visibility and Risk Reduction
Leverage a global network of uniquely skilled security researchers incentivized to find forgotten assets and shadow IT exactly as an attacker would, for the most organic and effective approach to risk reduction.

Executive Reporting
Customizable platform reporting with full risk profile, method for attribution, as well as recommendations for securing identified assets, packaged and ready for executive review.

Migration to Active Testing
Discovered assets are available for use in new or existing Bug Bounty or Next Gen Pen Test programs to further reduce risk in assets you need to maintain.

Optimized to Address Key Business Priorities

Asset Inventory fulfills a variety of business use cases, including those particular to security, IT, compliance, and even marketing:

Determine use of publicly accessible technology like server software, JavaScript library, or open ports

Manage certificates and receive alerts before expiration

Compile a complete list of all domain names and subdomains that your organization owns

See and quickly act on changes to your technology, domains, and subdomains

Key Features

Beyond domains and subdomains, Asset Inventory catalogs all IT it encounters via technology fingerprinting to provide more insight and context around every uncovered asset. Because many organizations fail to track changes to infrastructure—servers brought online, ports opened, software changes, etc.—Asset Inventory also enables "smart folder" creation and alerting to quickly categorize and flag high-risk asset-related events. These can then be quickly exported and shipped to the appropriate team via Slack, ServiceNow, or email integrations. Asset Inventory also offers:

- **Near real-time inventory population** of domains and subdomains

- **Continuous discovery** using 18 methodologies for asset identification and attribution

- **Web-based portal** with publicly accessible services for cross-organization collaboration

- **Easy API integration** to fit into your existing security ecosystem

- **Live alerting for aberrant discoveries** like open ports, expired SSL/TLS certs, or new technology

- **In-depth querying** for hundreds of asset attributes like SSH server version
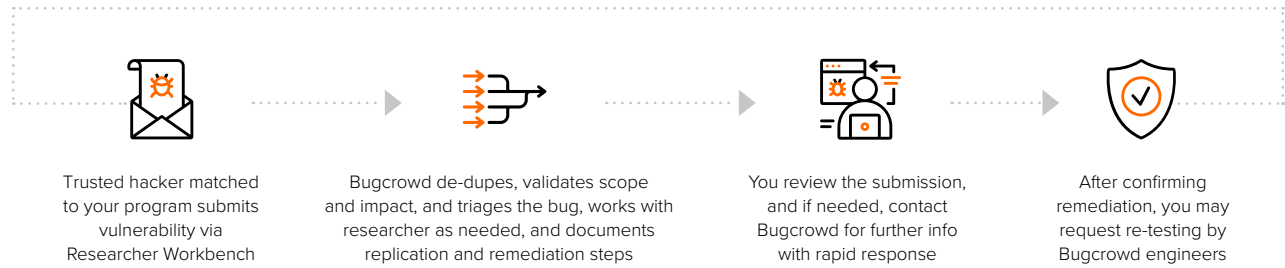
Bugcrowd Attack Surface Management

	ASSET INVENTORY	ASSET RISK	COMBINED
Asset Discovery	✓	✓	✓
Asset Management	✓		✓
Attribution		✓	✓
Prioritization		✓	✓
Frequency of Delivery	Continuous Software-Based	On-Demand Crowd-Enabled	Continuous Crowd + Software

ASM Asset Inventory is the latest step forward in helping organizations take back control of their digital ecosystems.

The two modules within Bugcrowd Attack Surface Management can be operated independently, in combination, or in connection with any of our other platform security solutions.
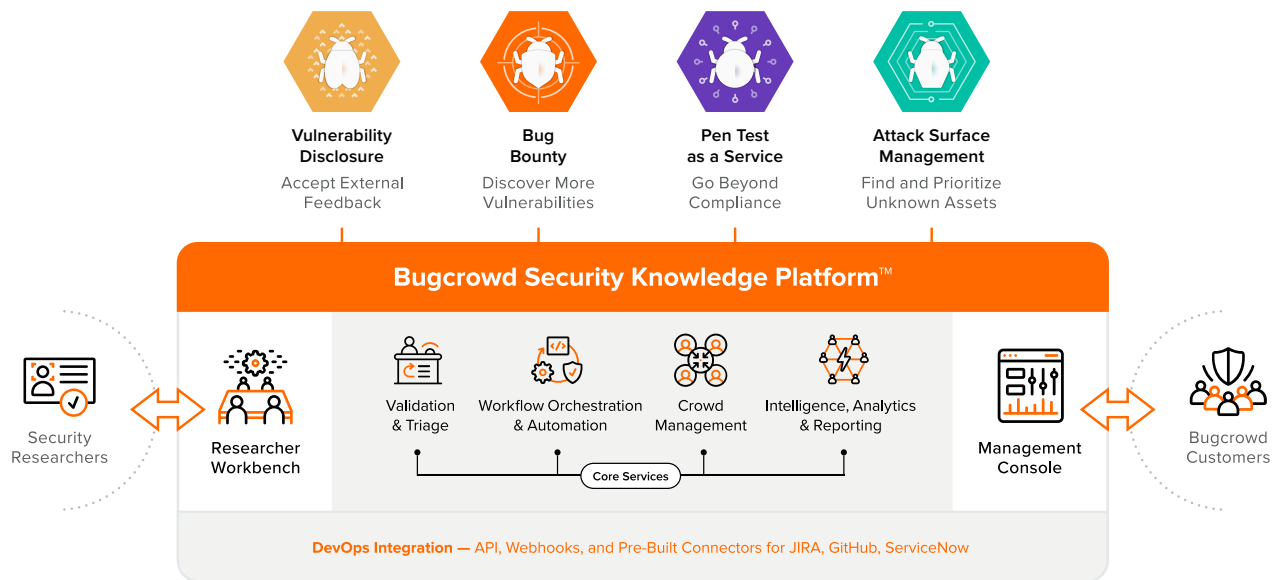
Lifecycle of a Vulnerability

Trusted hacker matched to your program submits vulnerability via Researcher Workbench

Bugcrowd de-dupes, validates scope and impact, and triages the bug, works with researcher as needed, and documents replication and remediation steps

You review the submission, and if needed, contact Bugcrowd for further info with rapid response

After confirming remediation, you may request re-testing by Bugcrowd engineers

Platform Overview

Our AI-powered, multi-solution crowdsourced security platform is built on the industry's most extensive repository of vulnerabilities, assets, and hacker profiles, meticulously curated over the past decade. This ensures that we identify the perfect hacker talent for each unique challenge, providing the scalability and adaptability needed to defend against threats, no matter how unique they may be.

Vulnerability Disclosure
Accept External Feedback

Bug Bounty
Discover More Vulnerabilities

Pen Test as a Service
Go Beyond Compliance

Attack Surface Management
Find and Prioritize Unknown Assets

Bugcrowd Security Knowledge Platform™

Security Researchers

Researcher Workbench

Validation & Triage

Workflow Orchestration & Automation

Crowd Management

Intelligence, Analytics & Reporting

Core Services

Management Console

Bugcrowd Customers

DevOps Integration — API, Webhooks, and Pre-Built Connectors for JIRA, GitHub, ServiceNow

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/try-bugcrowd**