bugcrowd

DATA SHEET

ATTACK SURFACE MANAGEMENT

Attack Surface Management

Get Comprehensive Visibility Into Your **Entire Attack Surface**

As an organization becomes increasingly digital—and adopts more web and mobile applications, such as application programming interfaces (APIs) and cloud-oriented services—its attack surface can rapidly expand and become more exposed to abuse and attacks. Bugcrowd's Attack Surface Management solutions provide comprehensive visibility into your entire information technology (IT) and digital footprint. They enable you to quickly identify weaknesses and vulnerabilities in known and unknown assets and then prioritize those issues for remediation before attackers can find and exploit them.

EMERGING FROM THE SHADOWS

The widespread adoption of software-as-a-service (SaaS) and cloud offerings has caused seemingly insurmountable IT sprawl, while bring your own device (BYOD) and shadow IT are combining to create numerous blind spots for IT security leaders. Whether through merger activities or organic growth, the sheer number of digital assets that need to be protected—domain names, certificates, websites, devices and data stores—can be overwhelming. Further, in mergers and acquisitions (M&A) situations, acquired entities often bring along technical debt from unknown and neglected assets, many containing vulnerabilities waiting to be exploited by attackers. For all these reasons, fully a third of successful attacks today involve unmanaged or virtually unknown assets.

POWERFUL TOOLS BACKED BY DOMAIN INTELLIGENCE

Bugcrowd's Attack Surface Management (ASM) solutions help organizations reduce risk by mapping their entire digital environment. Bugcrowd ASM is built on the powerful, proven Bugcrowd Security Knowledge Platform™, which provides a knowledge base built up over ten years and thousands of vulnerability disclosure, bug bounty, and pen testing programs. This deep well of domain intelligence underpins the complex reconnaissance strategies employed by our elite, crowdsourced group of ethical hackers. Paired with the platform's advanced discovery and monitoring capabilities, Bugcrowd ASM solutions enable you to discover and identify vulnerable assets and helps prioritize those assets for fast remediation.

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, and 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.

How It Works

Hacker Selection

Bugcrowd selects the right trusted hackers for your needs from a highly vetted bench

Reconnaissance Workflows

Platform-powered workflows augment and expedite complex recon strategies

Mapping and Attribution

Reduce noise with intelligent attribution to see only the assets that really belong to you

Risk-Based Prioritization

Data from thousands of programs help determine true risk of exploitation

Executive Reporting

Risk-ranked reporting with attribution method and proposed next steps

Bugcrowd Attack Surface Management

Available on the Bugcrowd Security Knowledge Platform in two complementary formats:

Bugcrowd Security Knowledge Platform

ASM

Bugcrowd Attack Surface Management (ASM)

AR

Asset Risk™ (AR)

Find, Prioritize, and Secure Your Entire Attack Surface

Asset Risk is powered by trusted hackers skilled in reconnaissance and risk-based prioritization. By pairing human ingenuity and experience with insights gleaned from over thousands of managed programs, Asset Risk helps customers find, connect, and prioritize more of their unknown attack surface, faster.

AI

Asset Inventory™ (AI)

Rapid and Continuous Asset Discovery and Management

Asset Inventory is a software-based solution for continuous asset discovery and management. With configurable alerts and “smart folder” activation, organizations can quickly see, communicate, and manage changes in their internet-facing digital landscape to reduce risk across even the most dynamic attack surfaces.

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

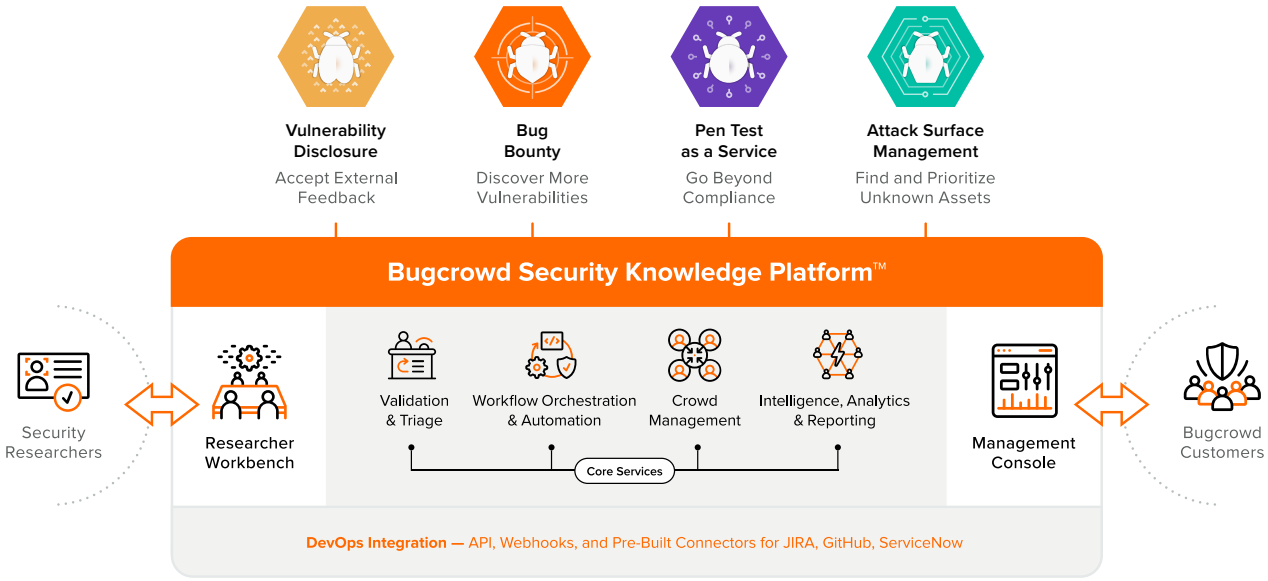
Bugcrowd de-dupes, validates scope and impact, and triages the bug, works with researcher as needed, and documents replication and remediation steps

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.



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.