bugcrowd

DATA SHEET

ATTACK SURFACE MANAGEMENT

External Attack Surface Management

Discover your external attack surface in minutes so you can start reducing your cyber risk as quickly as possible

MANAGING THE EXPANDING ATTACK SURFACE

The rapid transition to cloud has made keeping track of digital environments a mounting concern. It is becoming increasingly challenging to get a complete picture of your evolving external attack surface so security strategies must evolve to manage the ever-changing threat landscape to proactively manage risk.

The Bugcrowd Platform is the solution to this problem. You get continuous full visibility into your online environment, giving you real-time risk insights with the aim to speed up remediation.

WHAT IS EXTERNAL ATTACK SURFACE MANAGEMENT (EASM)?

Attack surface management is the continuous discovery, inventory, prioritization, classification, and security monitoring of an organization's external IT ecosystem.

Bugcrowd EASM (formerly Informer EASM) finds your external attack surface using our innovation platform, providing continuous asset discovery in minutes across internet facing on-prem and cloud environments.

In recognition that vulnerabilities emerge constantly, our platform comes with vulnerability discovery to continuously monitor for infrastructure and application-level security weaknesses in external assets.

Bugcrowd EASM is complemented by our ASM Risk offering, which packages results from crowd-powered discovery, attribution, and prioritization as an Executive Report.

Informer.
Acquired by Bugcrowd

Our approach

Map your attack surface
Gain an attacker's perspective using continuous asset discovery to map your external attack surface.

Monitor your assets
Monitor your application and infrastructure layers in real time to detect changes and exposures you need to act on.

Actionable insights
Utilize email alerts, customizable reports, and a JIRA integration to provide security teams with the information you need.

Reduce your risk
Vulnerabilities are risk-rated based on severity and asset critically to improve your security posture.

Key features

ASSET DISCOVERY

Active scanning and hundreds of data sources are used to find online assets in seconds with just your domain as the seed.

VULNERABILITY MANAGEMENT INSIGHTS

Stay one step ahead of attackers by continuously scanning assets for over 40,000 application and infrastructure level vulnerabilities.

SECURITY ALERTS

Receive instant notification of vulnerable assets, misconfigurations, and changes to your IT environment as soon as they are detected.

CONNECT YOUR AWS, AZURE, AND GCP CLOUD

Connect to your cloud environment to monitor your externally facing cloud assets including load balancers, app engines, and data stores.

INTEGRATED PENETRATION TESTING

Enhance your vulnerability assessment program by combining automated security and manual penetration testing.

AUTOMATED RETESTING

Automated regression testing validates your fixes for vulnerabilities found by our scanners.

How it works

Attack surface discovery
We start with your seed domain to search the internet for external assets.

Asset mapping and inventory
Verify ownership of assets and view your up-to-date inventory.

Automated security testing
Choose a vulnerability scan frequency for applications and infrastructure.

Risk-based prioritization
Prioritize remediation using CVSS severity ratings. Automated regression testing validates your fixes.

Insights and reporting
Improve your security posture with actionable insights.

Why Bugcrowd?

- ✔ Right Crowd, Right Time
- ✔ Engineered Triage at Scale
- ✔ Insights From Security Knowledge Graph
- ✔ Works With Your Existing Processes

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