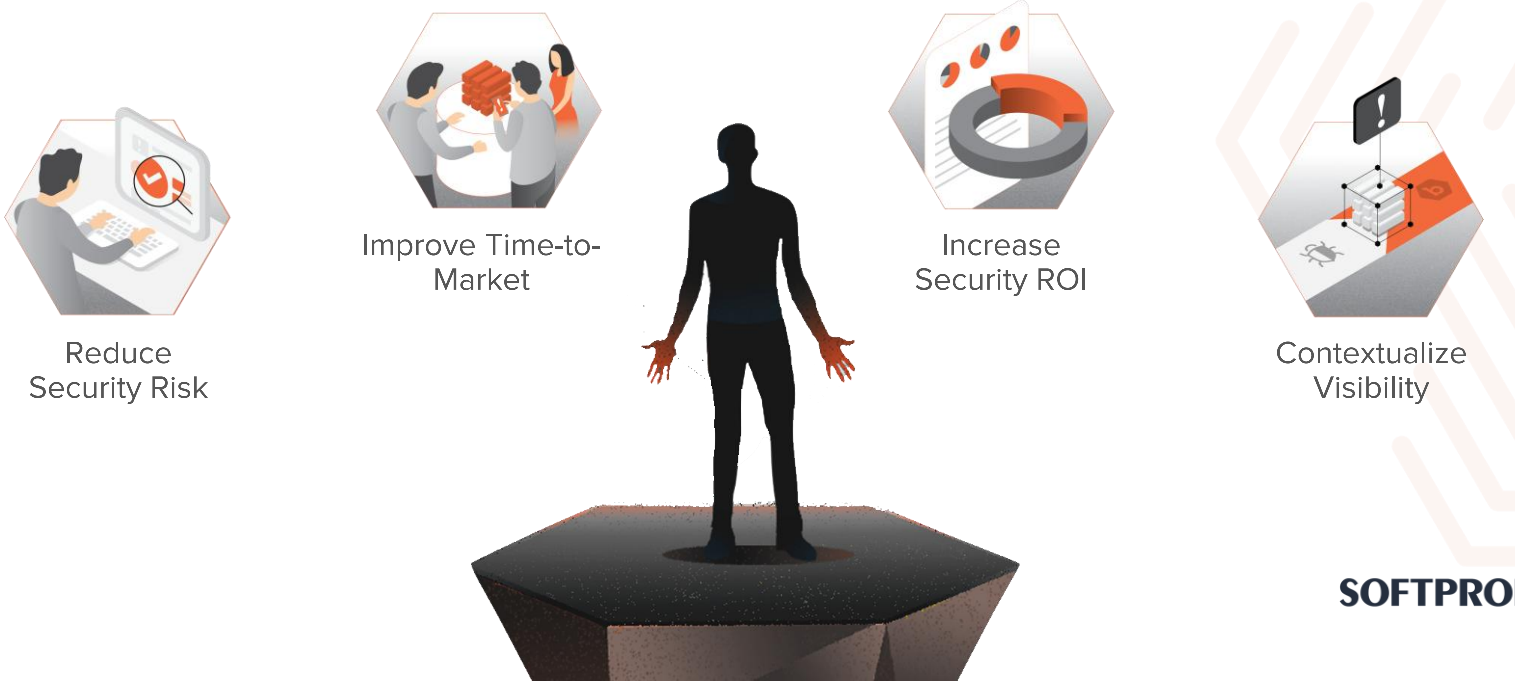
bugcrowd

Vulnerability Disclosure Program (VDP)

Digital transformation is pushing security objectives out of reach



Reduce Security Risk

Improve Time-to-Market

Increase Security ROI

Contextualize Visibility

SOFTPROM

Even with countless security tools, organizations remain vulnerable

Avg. cost of a breach in 2021 was USD $4.24 million

(IBM)

Fragmented Solutions
= Poor Visibility

Skills Shortage
= Limited Expertise

Disjointed Workflows
= Inefficient Fixes

Security Blvd 2021 Ponemon 2020

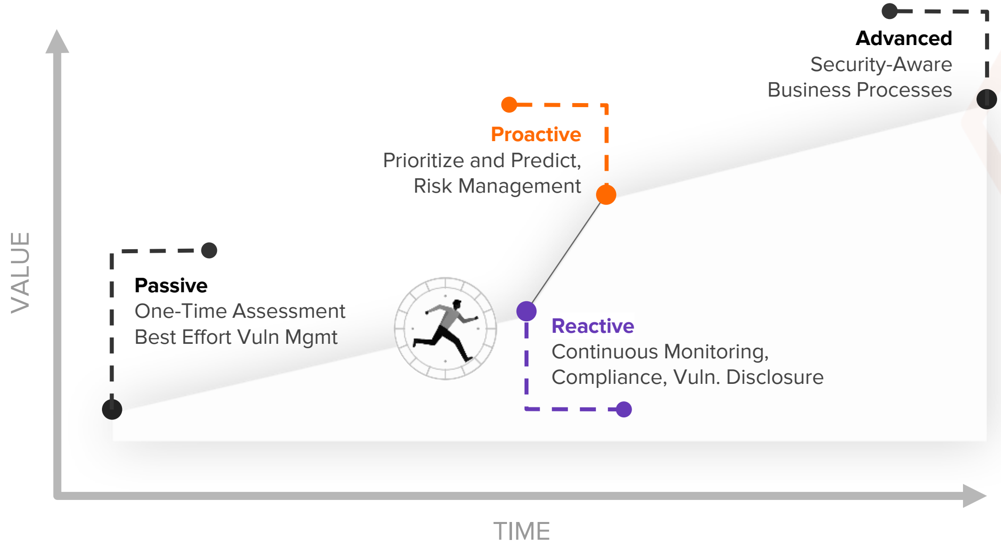
Forbes 2020 (ISC)² 2020

Help Net Security 2021 ZDNet 2021

SOFTPROM

Instead, your organization needs a proactive cybersecurity strategy

4



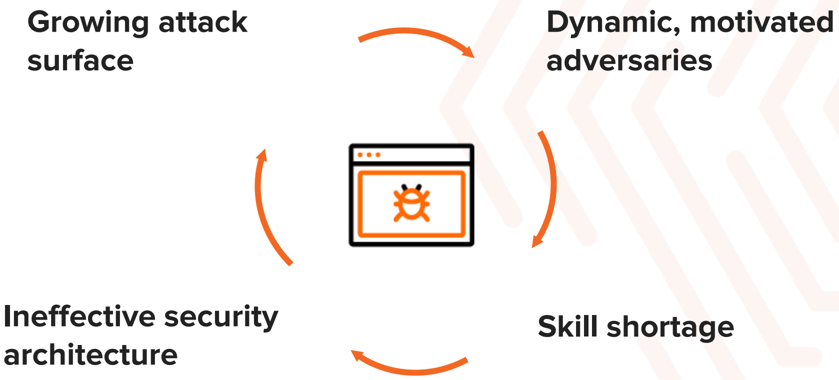
SOFTPROM

Current Situation

Insecure code creates vulnerabilities, which can then be exploited by malicious attackers. Organizations need a mechanism for accepting secure feedback.

87% of organizations receive critical or high priority findings with VDPs*

80% Of hackers encountered a vulnerability they had previously not seen before**



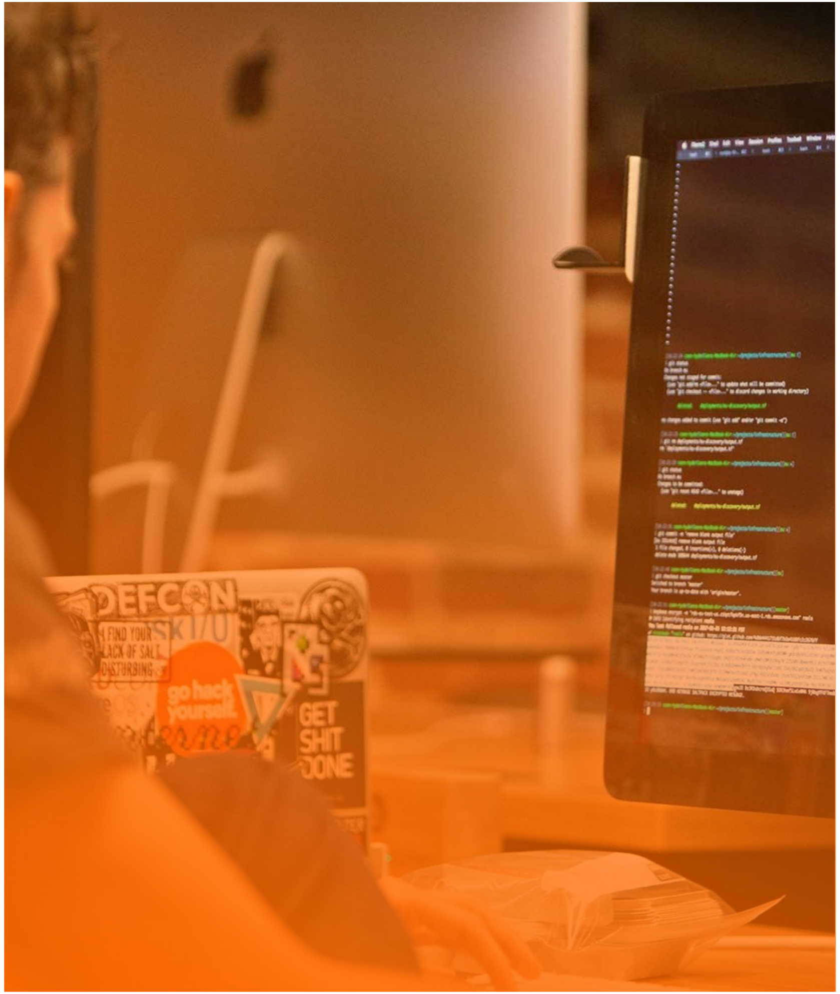
Growing attack surface

Dynamic, motivated adversaries

Skill shortage

Ineffective security architecture

*Ultimate Guide to Vulnerability Disclosure 2021
**In the Mind of Hacker Report 2021



Vulnerability Disclosure Program (VDP)

“See Something, Say Something”

It is a process by which an organization can receive cybersecurity vulnerability reports from any external individual, whether it’s a customer, a private security researcher or a good-faith hacker, a media or government body - via a dedicated channel.

Every VDP is different and should be tailored to the specific threat profile, regulation requirements, and assets of your enterprise.

SOFTPROM

Vulnerability Disclosure programs help extend testing to cover all internet-facing assets, 24/7

Save while reducing risk

VDPs are volunteer-based, findings are rewarded in recognition

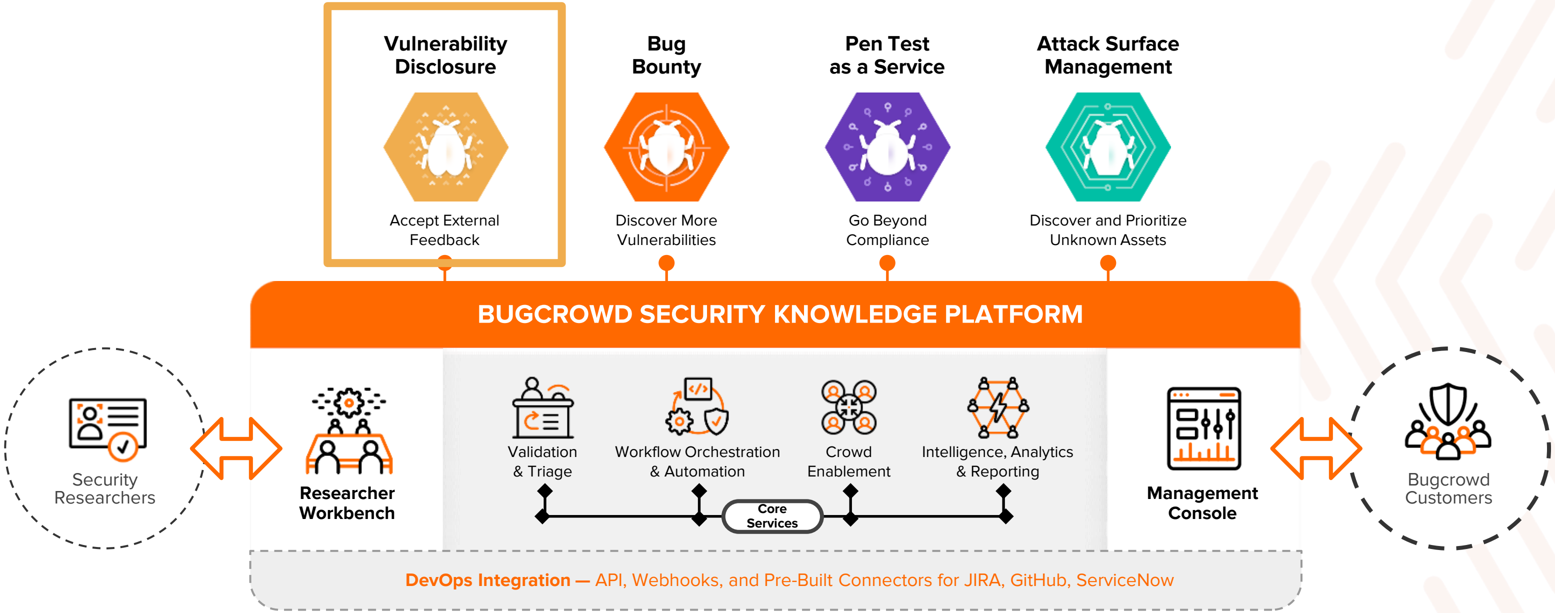
Show customers you care

Demonstrate security maturity with a program that customers can see and understand

Streamline remediation

Integrate optimized security workflows with your SDLC, so bugs get fixed faster

One Platform, Many Solutions



Vulnerability Disclosure

Accept External Feedback

Bug Bounty

Discover More Vulnerabilities

Pen Test as a Service

Go Beyond Compliance

Attack Surface Management

Discover and Prioritize Unknown Assets

BUGCROWD SECURITY KNOWLEDGE PLATFORM

Security Researchers

Researcher Workbench

Validation & Triage

Workflow Orchestration & Automation

Crowd Enablement

Intelligence, Analytics & Reporting

Core Services

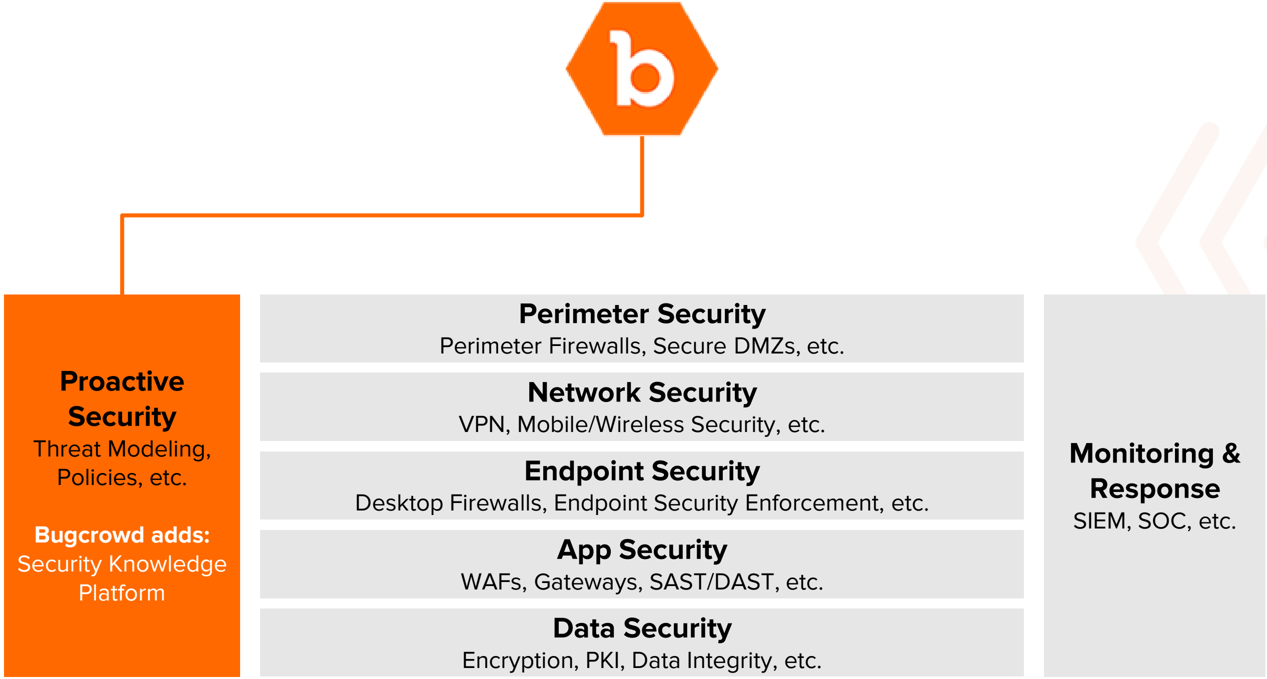
Management Console

Bugcrowd Customers

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

SOFTPROM

Bugcrowd in Your Layered Cybersecurity Architecture



Proactive Security
Threat Modeling, Policies, etc.

Bugcrowd adds:
Security Knowledge Platform

Perimeter Security
Perimeter Firewalls, Secure DMZs, etc.

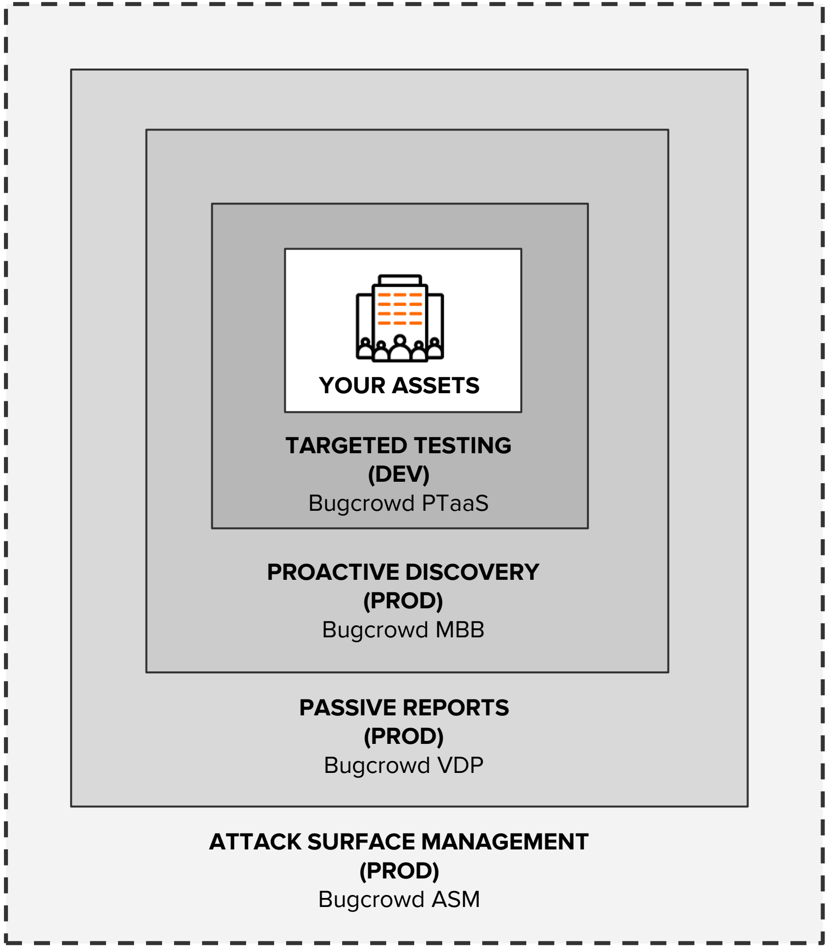
Network Security
VPN, Mobile/Wireless Security, etc.

Endpoint Security
Desktop Firewalls, Endpoint Security Enforcement, etc.

App Security
WAFs, Gateways, SAST/DAST, etc.

Data Security
Encryption, PKI, Data Integrity, etc.

Monitoring & Response
SIEM, SOC, etc.



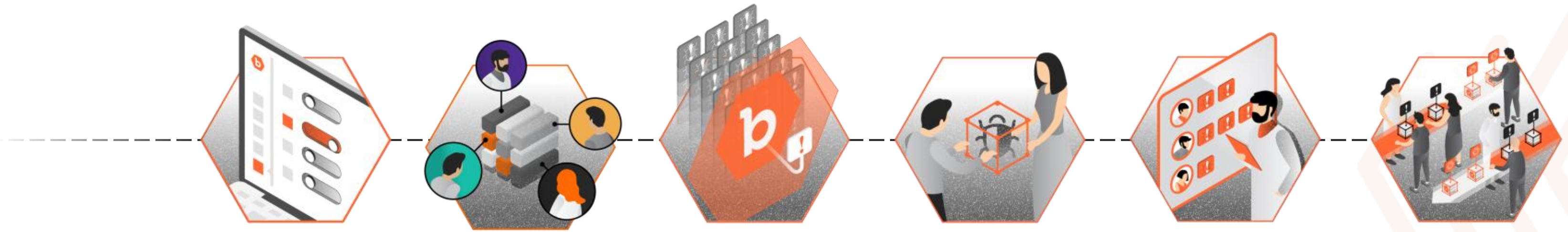
Bugcrowd Solutions Work Together To Protect Your Organization

- → Prove to customers and partners that you have the most possible coverage: Meet specific testing requirements, continuously discover evolving security gaps, passively receive public reports, and understand attack surface at all times
- → Share data about vulns, remediation, targets, etc. across all solutions
- → Powered by a single platform for a unified customer experience
- → Everything integrated in real time with your dev and security processes

SOFTPROM

Vulnerability Disclosure Program **from Bugcrowd**

Bugcrowd's programs provide a framework to securely **accept**, **triage** and **rapidly remediate** vulnerabilities submitted from the global security community.



Program Onboarded

Bugcrowd documents your disclosure policy and sets up a secure channel

Vulnerabilities Discovered

Any external party identifies and reports a vulnerability

Feedback Accepted

The platform processes security feedback from external sources

Submissions Triaged

Our team prioritizes, validates and standardizes all incoming vulnerability reports

Findings Delivered and Accepted

Your team reviews valid, well-documented findings and confirms submissions

Workflows Automated

The platform orchestrates a remediation plan with your security team and systems

SOFTPROM

Bugcrowd offers multiple methods for managing VDP Submissions, including **enabling passive acceptance** from individuals already using your products or **proactively soliciting testing** via Bugcrowd's hosted form.

	Email Intake	**Embedded Submission Form**	**Bugcrowd Hosted**
Method	Passive	Passive	**Active**
Customer Value-add	Receive feedback	Receive feedback + **Create parameters for properly data entry**	Feedback + Proper data entry + **Greatest no. of submissions**
Researcher Incentives	● Improve product or service ● Points	● Improve product or service ● Points	● Improve product or service ● Points ● Easily find programs ● Build credibility and ranking

Why Bugcrowd’s VDP Solution is Different

→ Better Results and Real-time Visibility

Bugcrowd VDPs receive **18x more** submissions on average, with results viewable in real time - resulting in increased visibility for researchers to make their submissions

→ Industry-leading Triage

Our global team of specialists rapidly validates and prioritizes submissions at **99+% SLA achievement** (with critical bugs handled in hours), so you can focus on remediation immediately

→ Platform Powered

The Bugcrowd Security Knowledge Platform offers a unified experience across multiple solutions (seamlessly integrated with your dev and security processes), and adds contextual insights based on a decade of experience managing 1000s of customer programs

VDP Best Practices

How to Start a VDP

1

Decide on Self-Managed or Hosted

Organizations like Bugcrowd offer managed vulnerability disclosure programs to help **alleviate the time and effort** required to construct and run an effective disclosure program.

2

Codify expectations

Organizations initiating a VDP should adhere to principles that **make the program scalable and robust.**

3

Expected to Iterate

Lay out a **timeline and allow time** to build and review a data set.

VDP Best Practices

How to Start a VDP

4

Be Accessible

Give **clear guidance around communications**, within dedicated channels.

5

Factor in Respect

A VDP should **define clear disclosure standards based on good faith.**

VDP Best Practices

Managing a VDP

- Align expectations
- Provide clear legal guidance
- Ground interactions in good faith
- Remediate efficiently
- Start a dialogue
- Troubleshoot the process
- Take an integrated approach
- Know your limits

SOFTPROM

SOFTPROM

Telefonica arlo NETGEAR

HACK THE PENTAGON OWASP mastercard

SAP Concur hp Etsy

MOTOROLA Walmart Adobe

overstock STELLANTIS UNDER ARMOUR

ATLASSIAN Square twilio