



VULNERABILITY DISCLOSURE PROGRAMS

FROM LUXURY TO NECESSITY

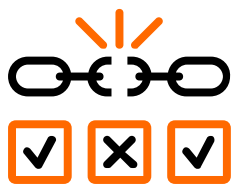
87% of organizations have discovered at least one critical vulnerability through a VDP!



CONSEQUENCES OF NOT HAVING A VDP

1 Unknown Vulnerabilities

Leaves org insecure, while the total number of security issues growing over time



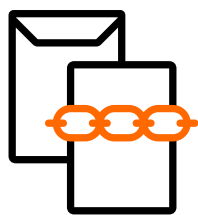
2 Security Breach Risk

High reputational damage and financial repercussions



3 Researchers Unable to Report Findings

Vulnerabilities may be disclosed publicly via social media or other channels before remediation



4 No Secure Process

No secure environment or organized process for submission and acceptance of prioritized vulnerabilities



5 Potential Noncompliance

Inability to meet compliance requirements or government directives



6 Loss of Confidence

Customers/citizens and other stakeholders lose confidence after a breach



A VDP MANAGED BY BUGCROWD

1 Reduce Risk

Securely accept, triage, and rapidly remediate valid vulnerabilities submitted from the security community



2 Improve Security ROI

Visualize and prioritize your entire threat landscape, so you can stay ahead of cyber attacks



3 Accelerate Digital Transformation

Digitize workflows and align security testing with your release cycle so you can ship secure code faster



4 Drive Better Decisions

Deliver context for risks and systems on your entire internet footprint with actionable intelligence for risk management



5 Increase Transparency

Demonstrate transparency to the security community and improve customer confidence



6 Gain Confidence

Identify vulnerabilities while building a stronger security brand



bugcrowd

Organizations of all kinds have transformed their approach to security using Bugcrowd VDP. Get the scoop in [The Ultimate Guide to Vulnerability Disclosure](#)