Rising bug bounty programs: the last line of defense against growing cyber threats

BY ELEANOR BARLOW · APRIL 10, 2025 · LAST UPDATED ON JANUARY 2, 2026

What you will learn

- **Why bug bounty programs are becoming essential in today's cybersecurity landscape**, driven by evolving threat vectors that make traditional security testing alone insufficient.
- **How bug bounty programs strengthen security posture** by leveraging expert crowdsourced testing to uncover high impact vulnerabilities before exploitation.
- **How organizations can prioritize and remediate critical issues effectively**, using bug bounty insights to focus limited resources on the most significant risks and improve overall resilience.

Every year, the number of vulnerabilities discovered and recorded increases. The sheer volume of vulnerabilities makes it impractical for organizations to patch everything, which is why they focus on prioritizing and remediating the most critical ones.

On top of this, it's very difficult to assess the true criticality of a vulnerability. This is precisely why bug bounty programs have become an important part of a multi-layered defense strategy when it comes to vulnerability management, as they provide a targeted and efficient way to identify and address the highest-impact vulnerabilities, ultimately helping organizations to allocate their resources more effectively and reduce their attack surface.

Vulnerability growth

The rise in vulnerabilities is hard to ignore. Recent reports from leading cybersecurity firms, such as Skybox Security and Verizon, confirm this trend, highlighting the increasing frequency and severity of breaches linked to vulnerability exploitation.

Perhaps most concerning is the fact that vulnerabilities have become a primary entry point for attackers, with many breaches originating from the exploitation of unpatched or poorly managed vulnerabilities. In fact, according to Mandiant *M-Trends 2024 Special Report*, '38% of initial intrusions started with an exploit, making it the number one initial infection vector for attackers'.

This shift underscores the critical importance of effective vulnerability management in preventing cyber-attacks and protecting sensitive data.

Another challenge is that even when companies strive to stay updated on the latest vulnerabilities, they often struggle to stay ahead. As Patrick Garrity highlights in the VulnCheck 2024 Trends in Vulnerability Exploitation report, "23.6% of Known Exploited Vulnerabilities (KEVs) were already being exploited on or before the day their CVEs were publicly disclosed," underscoring the difficulty in outpacing attackers.

Bug bounty market growth

There's been a growing rise in demand for bug bounty programs for companies of all sizes. To enhance security measures, bug bounty programs have grown significantly. In 2024, the bug bounty market was valued at $1.52 billion and, according to Business Research Insights, the industry will continue to grow to $5.74 billion by 2033.

The growth of registered users on bug bounty platforms has also increased, and, because of demand, 'Project Market Growth could reach $1.96 billion by 2025'- vpranks.

Predicted industry market growth

$1.52 Billion in 2024

$1.96 Billion by 2025

$5.72 Billion by 2033

> **"Bug bounty is the last line of defense before an incident happens."**
> **Stijn Jans, CEO, Intigriti**

How bug bounty improves security

Bug bounty hunting programs identify security vulnerabilities in customer environments on a pay-for-impact model. They leverage the knowledge and skillsets of expert security researchers to report issues, identify weaknesses, and improve systems. By pooling resources and utilizing crowdsourced security, potential risks are identified, and successful malicious attacks are reduced.

1. **Improved detection and response.** Bug bounty programs provide comprehensive security assessment beyond code review. By examining the entire security infrastructure, including network monitoring, authentication mechanisms, and detection systems, these programs help identify critical vulnerabilities before attackers can exploit them. This holistic approach strengthens an organization's security posture by addressing weaknesses across the entire defensive framework. Don't just look at code, but the whole security infrastructure so that flaws in elements such as network monitoring, authentication, or detection systems are highlighted so that critical vulnerabilities are identified before exploitation can take place.

2. **Real-world security testing**. Bug bounty programs go beyond being a mere checkbox exercise with a narrow scope—they simulate real-world attacks to assess an organization's resilience against genuine threats. By mimicking the tactics and techniques used by attackers, these programs provide a comprehensive evaluation of security defenses and uncover vulnerabilities that traditional testing often misses.

3. **Prioritization and patching**. Rather than spending time fixing everything and anything under the sun, bug bounty teams prioritize high-impact vulnerabilities that present the greatest risks. With the knowledge of what to tackle first, companies can patch elements before they become issues.

4. **Proactive approach**. Collaboration between ethical white-hat hackers and organizations builds a culture of awareness and a trusted relationship so that knowledge of an environment is built upon and improved together.

The rise of bug bounty programs stems from both the need to counter sophisticated cyber threats and the goal of enhancing overall cybersecurity maturity. Bug bounty programs strengthen defenses, identify and prioritize real-world vulnerabilities for rapid remediation, and build collaborative relationships with the global security research community, addressing the common challenge of skills gaps facing many organizations.

> **"Bug bounty programs have undergone a fundamental shift in perception, evolving from being seen as a luxury reserved for tech giants, to an essential security component for organizations of all sizes. This transformation reflects a growing recognition that traditional point-in-time security assessments alone are insufficient against today's threat landscape. We see companies of all sizes and budgets implement these programs as a necessity, leveraging the power of continuous, real-world security testing across their digital assets to identify vulnerabilities that might otherwise remain undetected and risk exploitation."**
>
> **Mark Wiley, Sales Director, Intigriti**

For more information, contact the team.

AUTHOR

Eleanor Barlow

Eleanor Barlow is a London-based Senior Cyber Security Technical Writer at Intigriti, with 9+ years' experience reporting on and writing for the cyber and tech sector. She specializes in data-driven content on cybersecurity and bug bounty intelligence, helping organizations benefit from the latest trends and insights.