hackerone

The Executive Guide to Human Security Testing

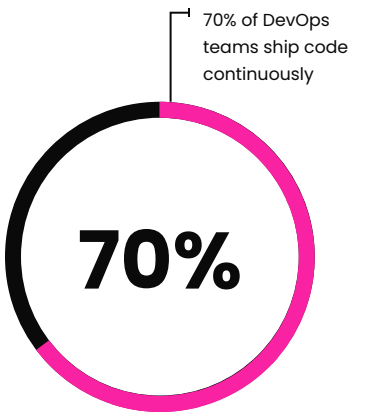
How fully-managed bug bounty and disclosure programs close visibility gaps across your attack surface

Table of Contents

The Digital Economy's Impact On Your Attack Surface

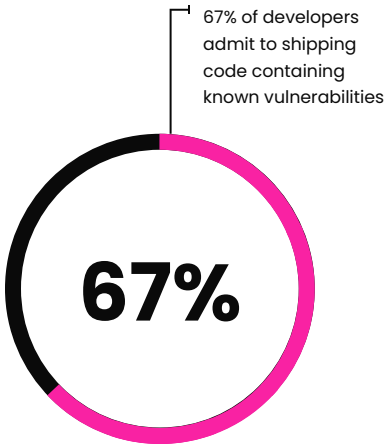
The digital-first economy has spurred a massive proliferation of internet-facing assets. Fueled by emerging technologies like cloud-native workloads and microservices, along with organizational changes from mergers and acquisitions, businesses of all industries have increased their digital landscape to meet the demands of customers worldwide. As the saying goes, every business is now a software business.

As a result of these shifts, the software development lifecycle (SDLC) has evolved drastically over the last decade to prioritize both speed and agility. Agile development and incremental releases allow development teams to get software into customers' hands quickly. **GitLab's 2022 Global DevSecOps Survey** found that 70% of DevOps teams ship code continuously - at least once per day or every few days.



With a ballooning inventory of applications and other web-facing assets, security teams are forced to overcome major challenges with visibility and governance in order to effectively manage their attack surface.

It is recognized that security must be considered and designed from the start in order to mitigate the risk of breaches, which are a major concern for consumers, regulators, and investors. But shifting left doesn't prevent security from becoming a blocker for development or business goals. Engineering teams end up pushing out new code faster than security teams can react, adding security debt and expanding the overall attack surface. **A 2022 survey by Secure Code Warrior** found that 67% of developers admit to shipping code containing known vulnerabilities.



This is proof positive that, despite the risk, speed-to-market is imperative to staying competitive in a digital-first economy. In-house security teams aren't able to respond to security vulnerabilities around-the-clock and adding additional headcount to meet those demands would be prohibitively expensive.

Shifting security left helps, but it still leaves gaps.

Security leaders are looking for ways to balance the need for speed while implementing secure-by-design coding practices.

The current landscape of automated QA, scanners, code review, and point-in-time testing are tools that help but leave these gaps in your SDLC:

- No around-the-clock observability into business-critical digital assets in production.
- Rules-based and automated scanning is limited by their support for specific technologies and does not find critical security risks such as business logic errors or chained exploits.
- External security assessments take too long and don't seamlessly fit into development processes.

With a pervasive skills shortage and growing attack surface, it's critical to look for a solution that closes gaps and enhances any security team, regardless of maturity or size.

What a Bug Bounty Program Can Provide

Bug bounty and, similarly, vulnerability disclosure programs, modernize application security testing with proactive, continuous testing of your internet-facing applications and infrastructure.

Partnering with a bug bounty program provider allows your organization access to a talent pool that may not be available in-house. Program providers like HackerOne, for example, have amassed a community of ethical hackers and security researchers numbering in the hundreds of thousands all with unique skill sets and perspectives to fortify the security of your applications. As of December 2022, HackerOne's community has helped resolve over 76,000 high and critical-severity vulnerabilities.

As of December 2022, HackerOne's community has helped resolve over 76,000 high and critical-severity vulnerabilities.

Hackers perform ongoing testing, finding the vulnerabilities in your internet-facing assets that bad actors seek to exploit. This includes third-party software such as open-source libraries, which are common vectors for cybercrime. No other security tool or practice currently provides that kind of continuous observability of all of your deployed code.

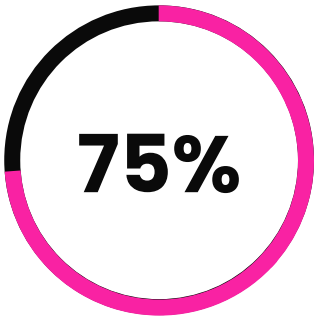
Continuous feedback from hackers regarding the potential impact of vulnerabilities effectively broadens the reach of your security team. The risk of a breach is directly lowered by easily feeding findings from your program to the development team for remediation. The vulnerabilities are an indicator of flaws that occurred during the SDLC and can serve as a blueprint for eliminating the re-creation of the same flaws.

What is a Bug Bounty Program?

A bug bounty is a structured program for ethical hackers and security researchers to safely find and report vulnerabilities to your organization in exchange for a monetary reward.

With a managed bug bounty program, your organization sets the rules of engagement for your program: assets in and out of scope, types of vulnerabilities, allowed testing methodologies, and reward structure. Hackers are assigned to your program, or can find it publicly, and begin continuous testing for security vulnerabilities that elude security teams and cannot be discovered by automated scanning tools.

For example, more than 75% of new bug bounty programs with HackerOne receive their first valid vulnerability report within 24 hours. That's how fast security improves when hackers contribute.



More than **75%** of new bug bounty programs receive their first valid vulnerability report **within 24 hours.**

Bug Bounty or VDP — What's the difference?

The core purpose, and structure, of a Vulnerability Disclosure Program (VDP) is the same as a bug bounty — to invite the hacker community to test your assets and find vulnerabilities. In fact, "VDP" is used as an umbrella term to describe any formalized program that allows ethical hackers to report security vulnerabilities in computer software or hardware. Even bug bounties are considered a category of VDP with monetary incentives.

However, with a VDP there are no monetary rewards. Instead, hackers submit vulnerabilities to VDPs to earn experience and reputation points on our platform.

Vulnerability Disclosure Programs are better suited as a reactive, 'see something, say something,' program for hackers to report vulnerabilities they have found. Bug bounties, on the other hand, actively incentivize targeted testing and attract the top talent of the hacker community.

Typical use cases for bug bounty and VDPs:

Both programs provide a vulnerability reporting and management system structured to match your organization's security maturity and testing goals. The differing rewards create unique strengths and use cases:

- Bug bounties provide the best results when organizations are looking for thorough and diverse security testing and want to harden business-critical applications in production.
  - Public programs provide the widest access to hackers, which can be valuable for large asset inventories, and quick response to 0-days or other active security threats.
  - Competitive bounties attract the top independent security talent on the planet. Organizations can invite hackers that specialize in specific technologies like web or mobile, depending on the assets that are in scope for the program.
- VDPs are a great avenue for organizations who are just getting started with crowdsourced vulnerability testing. Over time, organizations may elect to fund a dedicated bug bounty program to attract a more diverse subset of hackers.
  - VDPs help remediate vulnerability reports more efficiently than is possible with a basic submission form or ad-hoc process.
  - A formal program for submitting vulnerability reports is a security best practice and mandated by some governments including the United States as part of President Biden's **2021 Executive Order to Improve the Nation's Cybersecurity**, and the United Kingdom's **Product Security and Telecommunications Infrastructure (PSTI) Bill**.

Both types of programs are hosted on HackerOne's platform, providing access to vulnerability management.

- Evolve your program alongside your security needs. A VDP can be the starting point to create processes for monitoring, managing, responding to, and fixing reported vulnerabilities.
- Some organizations find benefit in having both private and public programs running simultaneously to cover different asset types operating in pre- and post-deployment environments.

Private or Public?

Why Private?

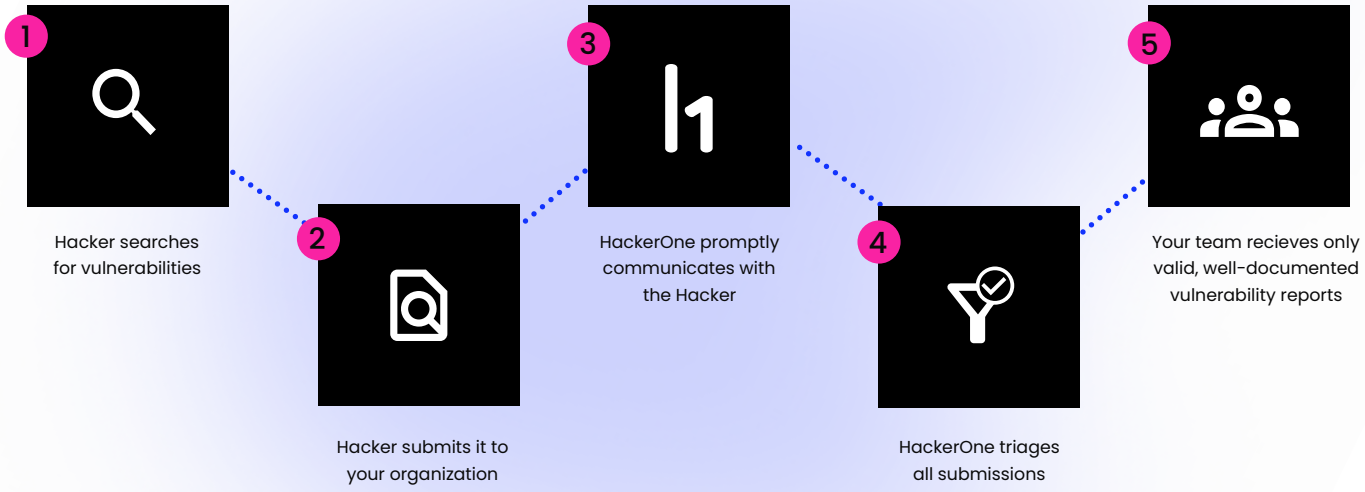
- With a private program, your organization controls every individual hacker that has access and permission to participate.
- Control access to sensitive assets and pre-production environments.
- Find hackers with unique specialties.

Why Public?

- Public programs are listed in the HackerOne directory and any hacker on our platform can participate.
- Cast a wider net to attract hackers with a broader range of expertise.
- More eyes on your program means more continuous feedback on exploitable threats.

How a Typical Bounty Program or VDP with HackerOne Works

Using a standard HackerOne program workflow as an example, we can showcase how a bug bounty or VDP program can be scaled to your needs. Here's how it works:

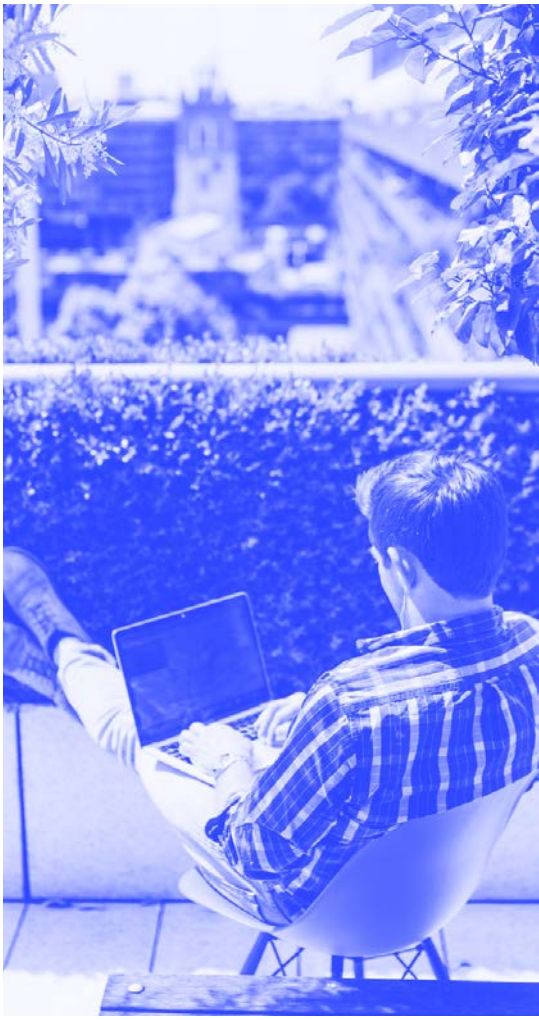


How a Fully-Managed Bounty or Disclosure Program Protects Your Business

Adding a human component to your vulnerability testing regimen eliminates visibility gaps and makes findings actionable for your security and development teams. 30% of developers cite real-world code samples as the most effective means of cultivating good secure coding practices, especially if it's their own code. Continuous feedback from hackers provides a level of peer-to-peer credibility that automated scanners may not provide. A dedicated partner to help manage the influx of incoming vulnerability reports can help extend the reach of your security team by flagging the vulnerabilities that pose real risk while filtering out noise. Helping developers act on vulnerability findings quickly and efficiently can prevent an exploit that leads to unauthorized access, user impersonation, data exfiltration, domain takeover or denial of service.

Vulnerability reports showcasing real-world exploit paths drives developer urgency, leading to a median time-to-remediate that is up to 8x faster than automated scanners.

A fully-managed bug bounty or VDP program will add measurable risk reduction to your attack surface and add a layer of continual security vigilance to your security strategy.



Scale security capabilities without impeding innovation and time to market

- Access to a large community of skilled hackers incentivized to find critical, undiscovered vulnerabilities on a proactive, continuous basis across your entire attack surface.
- Vulnerability reports showcasing real-world exploit paths drives developer urgency, leading to a median time-to-remediate that is *up to 8x faster than automated scanners.*[1]
- Dedicated triage teams remove the burden of manually validating vulnerability findings from your security team.

Manage risk and improve governance

- Flag CVEs that automated tools miss like business logic errors. 98% of hackers say that they find vulnerabilities that scanners miss.
- A platform that orchestrates human security experts provides reporting and analytics that reveal recurring vulnerability trends by asset, product family, business unit, development team, and more. These trends highlight improvement opportunities throughout the SDLC, helping organizations reduce vulnerabilities by up to 98%.
- Ethical hackers are vetted to meet the needs of organizations concerned with outsiders accessing their digital landscape.The U.S. Department of Defense has run a bug bounty with HackerOne since 2016.

(*[1]Based on data provided by Veracode's State of Software Security Report v12 and HackerOne's 2022 Hacker-Powered Security Report)*

Offset operational costs

- Address the security talent shortage and minimize hiring costs by tapping into a community of ethical hackers and researchers tailored to your specific tech stack.
- Program experts onboard, manage, and scale your program with proven vulnerability disclosure and bug bounty best practices.
- Triage services quickly validate incoming vulnerabilities and route actionable reports to your team so you can focus on the important task of actually fixing security flaws.

Strengthen brand trust

- Demonstrate leadership with industry benchmarking in meaningful security metrics like time to first response, time to triage, and time to remediation.
- Public Relation and communications support to foster trust with customers and hacker community along with incident response support.

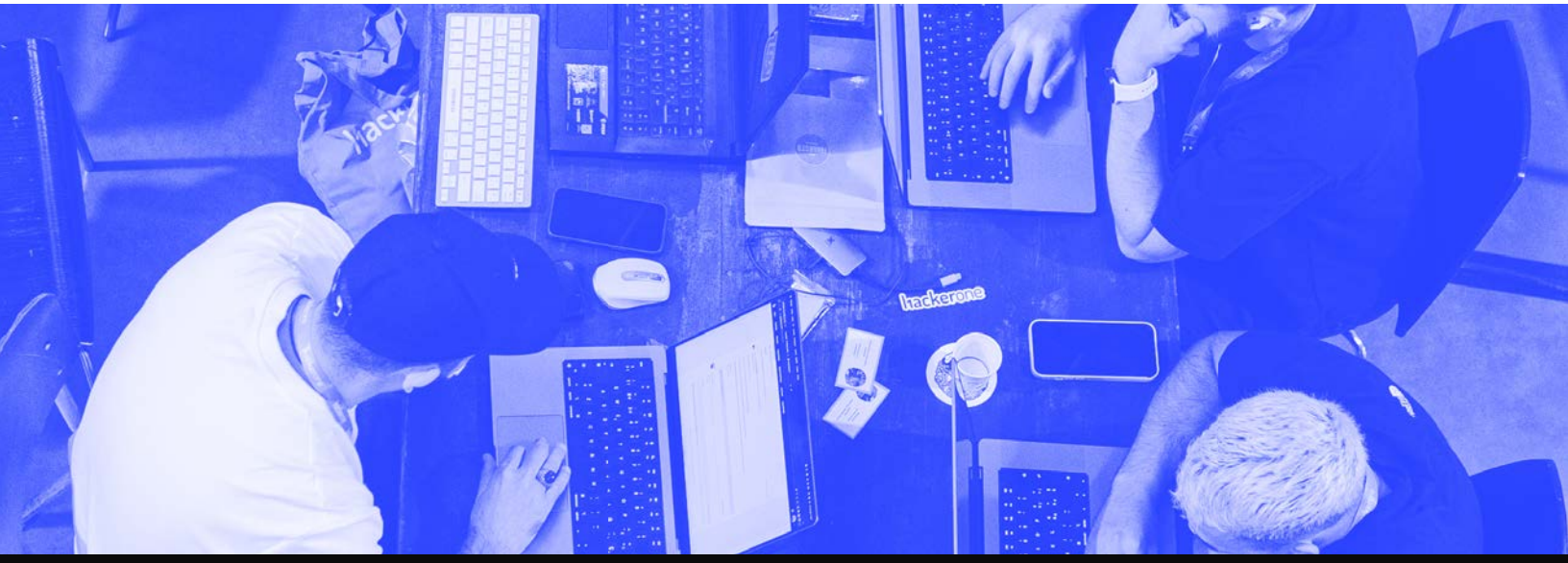
Conclusion

With organizations continuing to invest in their digital landscape, security leadership needs to take a comprehensive view of their attack surface vulnerability and whether they are equipped to take action.

Making security testing proactive helps your organization bring more secure products to market. A well-managed bug bounty or Vulnerability Disclosure Program leverages a community of ethical hackers to flag the flaws that automated scanners miss, while also satisfying the need for continuous observability into business-critical applications in production. Security leaders who need to expand the scope of their vulnerability testing program but lack the people resources can realize immediate ROI by partnering with a managed bug bounty or VDP platform provider.

HackerOne's **Bounty** and **Response** (VDP) are managed, turnkey security solutions with all the flexibility, expertise, and resources needed to be successfully included in your security strategy with little disruption. HackerOne and its community of ethical hackers do the work of finding and validating application flaws, allowing your team to focus on securely thriving in the digital-first economy.

HackerOne Bounty and Response are key components of our Attack Resistance Management platform, which integrates attack surface management and proactive security testing to help organizations increase risk awareness, security efficacy, and operational efficiencies. Working together, our solutions create a unified asset inventory that can be secured through targeted and crowdsourced testing to reduce your organization's cybersecurity risk.

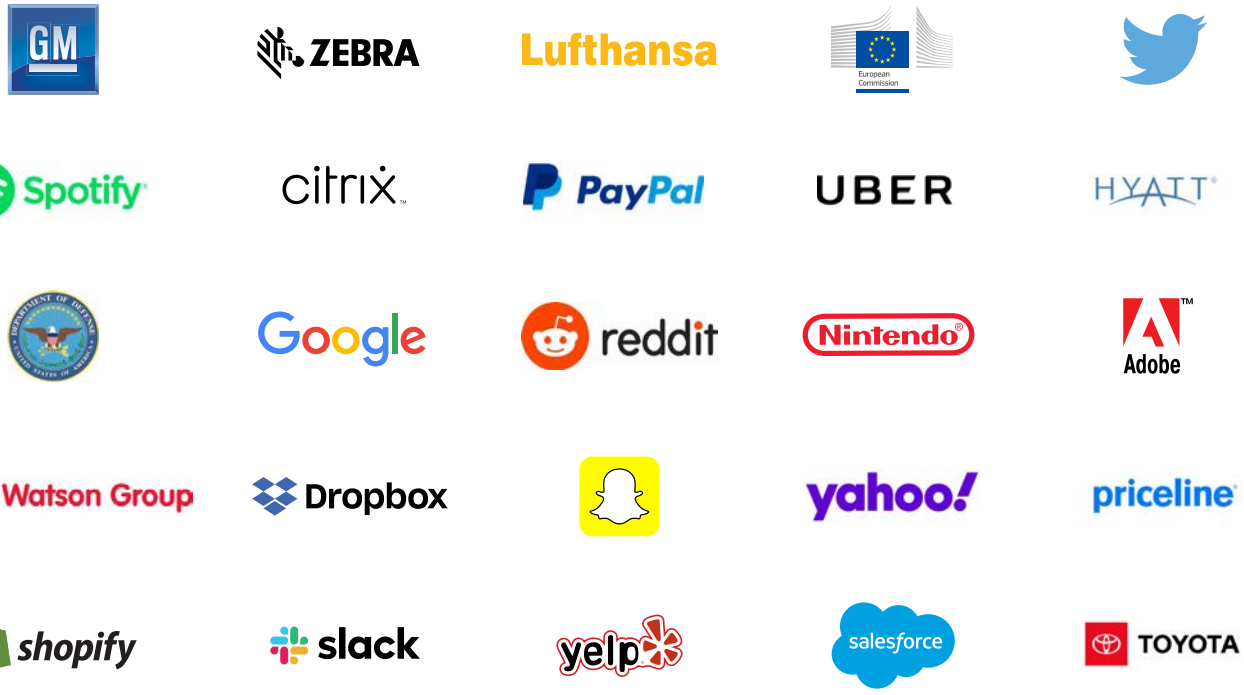


About HackerOne

HackerOne closes the security gap between what organizations own and what they can protect. HackerOne's Attack Resistance Management blends the security expertise of ethical hackers with asset discovery, continuous assessment, and process enhancement to find and close gaps in the ever-evolving digital attack surface. This approach enables organizations to transform their business while staying ahead of threats. Customers include The U.S. Department of Defense, Dropbox, General Motors, GitHub, Goldman Sachs, Google, Hyatt, Lufthansa, Microsoft, MINDEF Singapore, Nintendo, PayPal, Slack, Twitter, and Yahoo. In 2021, HackerOne was named a 'brand that matters' by Fast Company.

hackerone

HackerOne has vetted hackers for hundreds of organizations including:



With over 2,000 customer programs, more companies trust HackerOne than any other vendor

Contact Us