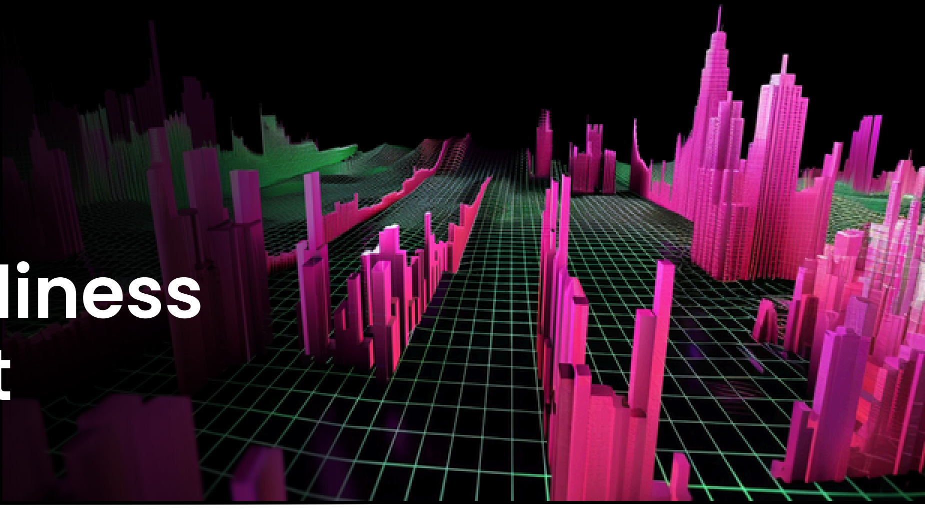


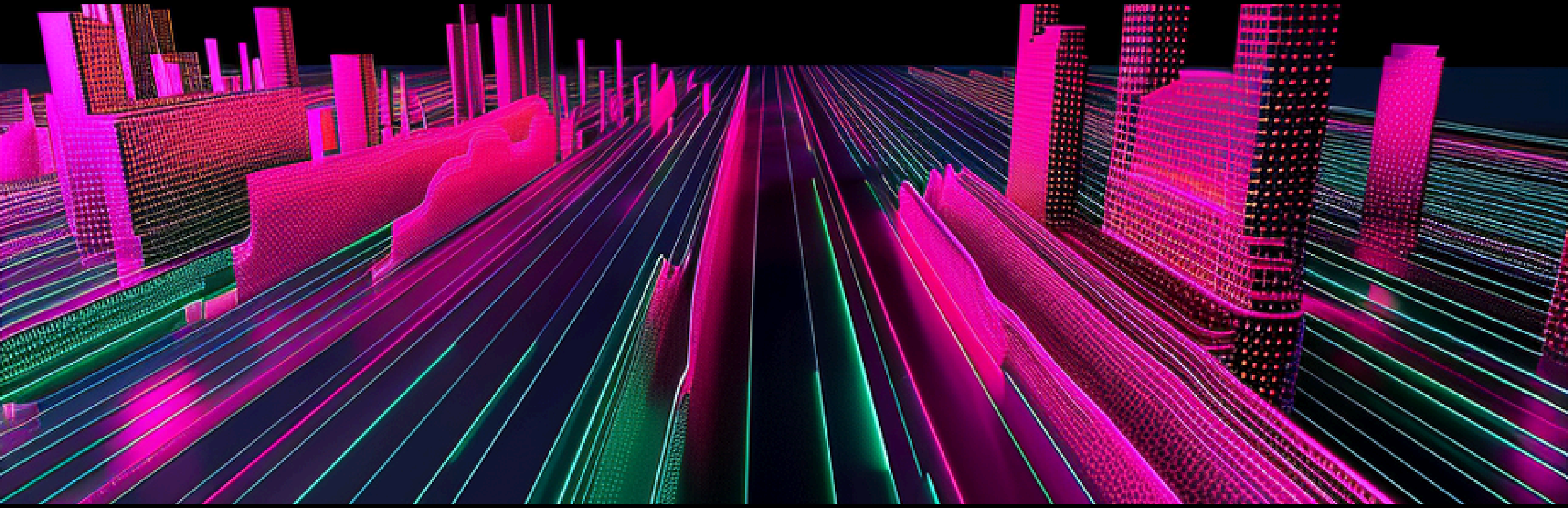
Bug Bounty Readiness Self-Assessment

Engaging with third-party researchers to bring an outsider mindset when looking for flaws in your systems is a core component of security resilience. Security resilience is an ongoing process of implementing best practices to ensure your organization can withstand and mitigate the impact of security incidents and attacks.

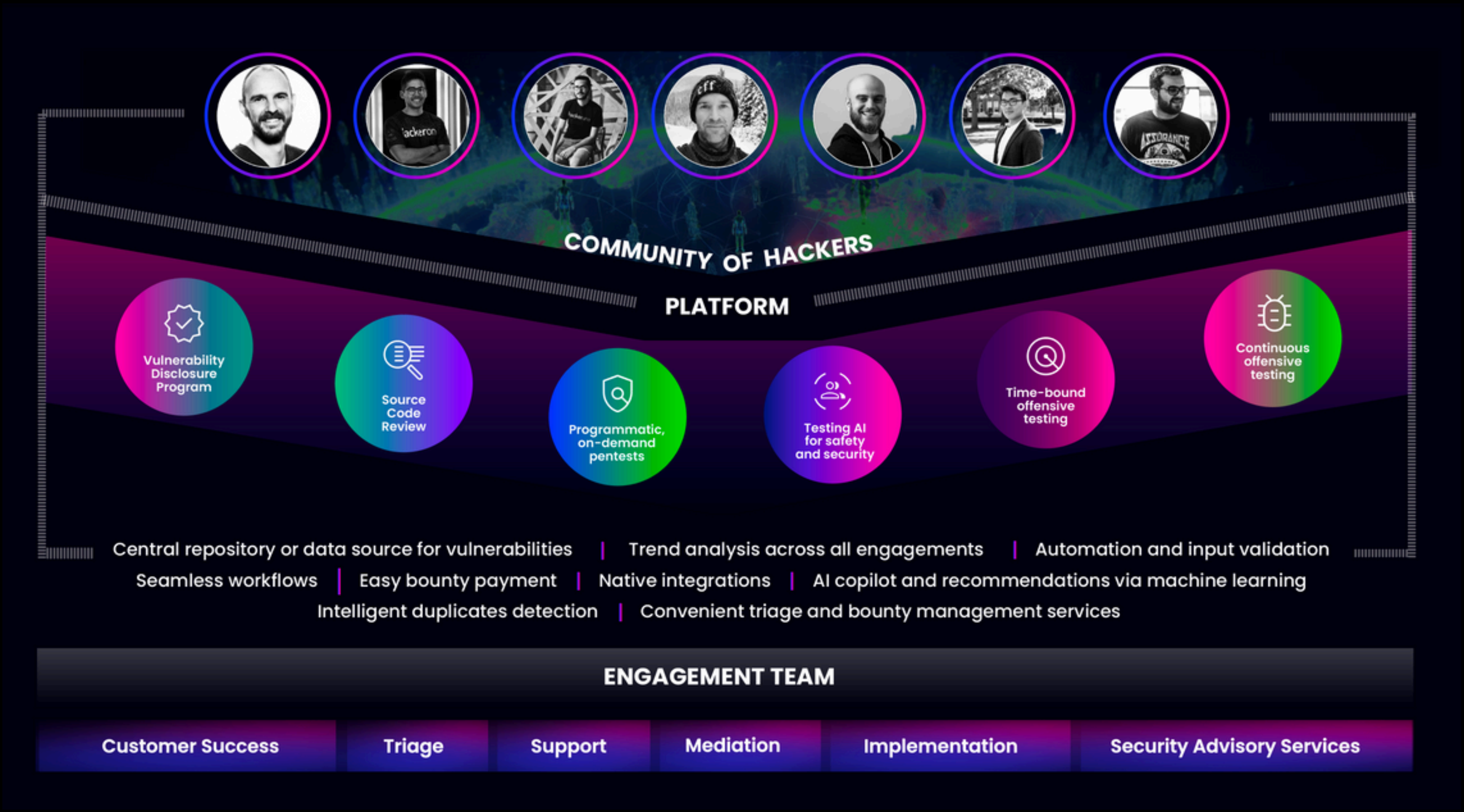
No matter what stage of your maturity journey, there is a human-powered security solution that can scale for your requirements, delivering actionable insights to build resilience from attacks.

We took a look at some of our most security-resilient customers, and they all had the following attributes in common:

- □ Systems—people, process, and tech—to handle security
- □ Fully defined and documented cybersecurity programs and processes
- □ A process to intake vulnerability reports from third parties
- □ A process to discover, inventory, and prioritize assets
- □ Continuous, manual security testing
- □ All brand assets in security testing scope
- □ Includes suppliers in their security testing programs
- □ Practices secure by design
- □ The ability to remediate vulnerabilities within a defined SLA
- □ An SLA of 1 day or less for fixing critical vulnerabilities
- □ Uses a risk-based asset classification system, defining a minimum bar for what level of security assessments must be done for an asset
- □ Prioritizes the list of vulnerabilities and misconfigurations based on risk level and business criticality
- □ Willingness to disclose vulnerabilities and steps to remediation



HackerOne has helped thousands of organizations scale their security testing through pentest, bug bounty, and vulnerability disclosure. The following self-assessment will help you understand your current level of security resilience and what option is right for your organization.



COMMUNITY OF HACKERS

PLATFORM

Vulnerability Disclosure Program

Source Code Review

Programmatic, on-demand pentests

Testing AI for safety and security

Time-bound offensive testing

Continuous offensive testing

Central repository or data source for vulnerabilities | Trend analysis across all engagements | Automation and input validation
Seamless workflows | Easy bounty payment | Native integrations | AI copilot and recommendations via machine learning
Intelligent duplicates detection | Convenient triage and bounty management services

ENGAGEMENT TEAM

Customer Success | Triage | Support | Mediation | Implementation | Security Advisory Services

What kind of security testing are you currently performing?

1. Some testing by internal security teams before a product release
2. 1-4 pentests a year on priority assets
3. Regular pentests on all assets
4. Continuous testing by third parties (pentest, bug bounty)
5. None of the above

How regularly do you test software manually?

1. Never
2. Annually
3. Bi-annually
4. Quarterly or more
5. None of the above

How much of your attack surface receives security testing/attention?

1. Less than 25%
2. 25% to 50%
3. 50% to 75%
4. More than 75%
5. None of the above

What does your security team look like today?

1. No dedicated security staff, 1-2 engineers focus on security issues
2. 1-2 dedicated security staff, wear all the security hats
3. Structured team of security engineers, 1-2 security-focused executives
4. Several security teams across multiple product areas or acquisitions, each with independent leadership
5. None of the above

What assets do you have in scope for security testing?

1. Flagship products ahead of launch
2. All our products and features ahead of launch
3. Our most important products and assets in a live environment
4. Anything related to our brand
5. None of the above

Have you received vulnerability reports from third parties or security researchers before?

1. No, or just 1 or 2, and we aren't sure how to respond.
2. Yes, we've received a few over the years, with mixed quality and frequency.
3. Yes, we receive a steady flow of reports from researchers and have a process for handling them.
4. Yes, we have a global response team that receives all reports and routes them to different product areas.
5. None of the above

How are you fixing vulnerabilities?

1. We struggle to know how to prioritize vulnerabilities for fixes and don't have a clear process.
2. We try to fix vulnerabilities in a timely manner but have an inconsistent SLA for doing so.
3. We have defined SLAs for fixing vulnerabilities, but we struggle to keep to timeframes (or time frames are undesirably/unreasonably long).
4. We have defined SLAs and are able to quickly prioritize and fix the most critical vulnerabilities.
5. None of the above

How do you communicate vulnerabilities to key stakeholders, including customers?

1. We avoid sharing any details about any vulnerabilities we encounter.
2. We let stakeholders know about vulnerabilities on a need-to-know basis and keep details to a minimum.
3. We let stakeholders know about vulnerabilities, but it takes a long time to get business approval to share details.
4. We let stakeholders know about vulnerabilities as soon as possible and publish the full details of our vulnerability findings and fixes.
5. None of the above

Answered mostly 1s?

Level 1: Pentest

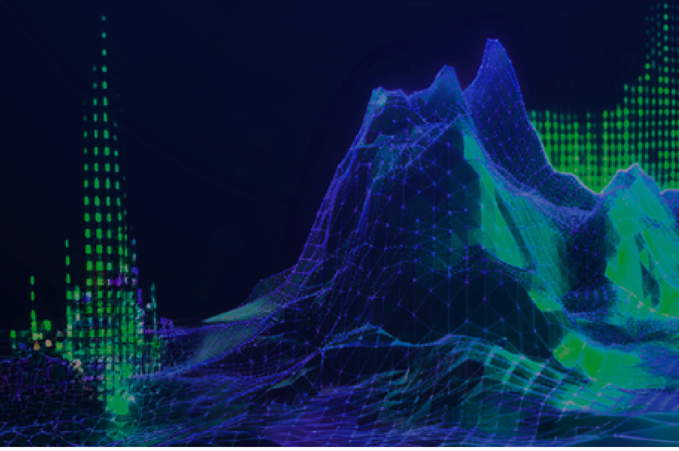
For customers who are beginning their journey with the researcher community, and up to this point have done infrequent and limited testing on their digital assets, we recommend starting with a community-driven pentest. A pentest is a controlled approach to your initial security test where you can specify exactly what vulnerabilities you want researchers to look for and work closely with a select community of researchers to uncover them.

Community: Community pentesters are an elite subset of the security researcher community that is hand-selected and professionally vetted by HackerOne. As part of the vetting process, we evaluate the pentesters' professional experience and performance on existing HackerOne security testing programs, taking their certifications into account, including OSCP, OSCE, OSWE, and CREST. 74% of them have over 5 years industry experience, and 50% of HackerOne pentests unveil at least one vulnerability in the first three days.

Platform: HackerOne's Pentest-as-a-Service operates on a software platform that facilitates seamless workflow integration for addressing the identified vulnerabilities. Get access to the dashboard for full visibility, track testing hours used and remaining, clone pentests from prior years or similar assets, and communicate with pentesters instantly via the portal or Slack for questions, context, clarifications, and more. In addition to visibility throughout the test, your security team will also receive a final report at the conclusion of the pentest to help meet compliance requirements.

Engagement Team: Work with a technical engagement manager (TEM) who will orchestrate testing engagements and ensure they run smoothly. These highly qualified TEMs are responsible for leading the delivery efforts of a pentest and ensuring its success. Each member undergoes rigorous background checks, ensuring they maintain the highest levels of trust and professionalism. Many of our managers hold an array of qualifications and certifications, tailored to meet the unique delivery requirements of our diverse customer base. Should you have specific geographic needs, we are poised to cater to such requests, ensuring seamless, localized engagement.

> Our first pentests revealed a major finding and showed the value of an ethical hacker community combined with PTaaS. Today, our pentests give us full visibility into findings in real-time, allowing us to pivot to fix and retest while the pentest is still running. The result is that we have more trust in the final report and can plan to direct efforts immediately to any weak spots.
>
> **Dr. Jasyn Voshell**
> Director of Product and Solution Security, Zebra Technologies



Answered mostly 2s?

Level 2: Private Bug Bounty Program

For organizations that have a fairly robust internal testing strategy and want to engage with top ethical hackers to find bugs in production, a private bug bounty is a popular starting point. A private launch will invite a small, select group of ethical hackers to focus on a particular scope and is most customers' first step when launching a bug bounty program for continuous security testing. There is a misconception that bounty programs are, by their nature, public; 80% percent of HackerOne's customers have a private program, and you can start with just a few select hackers to ease into the process.

Community: Choose from specialized researchers with tailored skills and expertise for your requirements. HackerOne sources and matches hackers for you and offers additional flexible hacker verification levels to meet complex compliance needs with HackerOne Clear. Clear hackers have proven their skills and professionalism on the HackerOne Platform, and have undergone background checks and ID verification. On average, Clear hackers have been active on the platform for over 25 months and submit 24x more high and critical reports than non-Clear hackers.

Platform: Establish a basic workflow to receive reports and communicate with researchers in a timely fashion. Keep track of each report's state: New, Triaged, Pending Bounty, or Closed. Reports can be closed as Resolved, Duplicate, Informative, Not Applicable, or Spam. With low volume, advanced data analysis will not be especially valuable, so whatever your program data comes with "out of the box" should suffice.

Engagement Team: Internal security team members (or DevOps/QA-focused engineers) should monitor HackerOne for new reports and respond in a timely fashion. HackerOne Triage can filter reports initially, so you're only receiving valid reports for review. HackerOne Triage consists of over 40 highly skilled in-house security analysts on five continents, with a broad range of technical skills and industry experience to cover a diverse range of assets, including web, mobile, API, binary, firmware, IoT, and hardware. HackerOne also offers different levels of customer support depending on your requirements.

A Professional subscription offers lighter engagement and is centralized around a pod of experienced customer success managers (CSMs). This option is ideal for customers who are comfortable working directly with hackers but desire additional technical support when needed. Customers can add Advisory Services that offer quarterly touchpoints from their dedicated CSM. This level is ideal for customers establishing and growing their security program.

An Enterprise subscription is a close partnership, providing all the benefits of Customer Success along with weekly touchpoints with your dedicated CSM. This option is ideal for customers utilizing HackerOne as a full-service security testing platform with an eye toward continuous growth.

> Based on our experience running bug bounty programs, we recommend that companies leverage private bug bounty programs before launching any public ones. Private programs are ideal for testing the waters. They help bring the Engineering and Security teams together and get them used to validating and systematically fixing new issues. The most common classes of security vulnerabilities are often found and fixed through private bug bounty programs. Public programs (when pipelined after private programs) are great for finding remaining security loopholes. We suggest that companies open their private programs to the public only when they can devote sufficient engineering resources to resolving issues found. They should also be prepared for the high volume of reports in the first few days of the public program launch.
>
> **Application Security Tech Lead, Yelp**

Answered mostly 3s?

Level 3: Public Bug Bounty Program

A public bug bounty provides the most comprehensive coverage for customers who have strong vulnerability management processes in place and can handle a substantial number of vulnerability reports. It incentivizes the global hacking community to report findings. Announcing that you are ready to receive vulnerabilities from the public signals to your customers, peers, and the world that security is paramount for your organization.

Community: With a public bug bounty, you're incentivizing the world's largest community of security researchers to use their creative and diverse skill sets to identify novel and elusive vulnerabilities in your systems. HackerOne's 7th Annual Hacker-Powered Security Report reveals that hackers have deep specialization and use a plethora of techniques. While 95% of hackers specialize in web application testing, they also span a range of new and emerging technologies: 47% specialize in network application testing, 20% have experience with social engineering, and 63% do vulnerability research. 36% of hackers say they are most skilled at the reconnaissance part of hacking, and 20% say they are best at exploitation.

Platform: Inviting additional researchers to your program will increase the volume of reports. Advanced tools like automatic duplicate detection become important, as multiple researchers may uncover the same issue. Tying into existing organization workflows requires out-of-the-box integrations with popular issue-tracking and team collaboration systems. Accessing program data via API enables flexibility for programs to scale. Leveraging a platform with AI allows organizations to receive report summarization, remediation advice, and best-practice guidance for program optimization. At the same time, industry benchmarks provide insight into how their program compares and highlight areas for improvement. As report volume scales, creating a seamless workflow tailored to your organization is crucial for long-term success. Key stakeholders often need specific filtering and reporting capabilities, while in-platform automation of repetitive tasks and API connectivity become increasingly important, reducing manual overhead as workstreams expand.

Engagement team: Internally, discuss with your team who can take charge of triage duty, in a similar way to how you would assign performance/operations/infrastructure duty. Establish SLAs that you can commit to, and know that program launch can bring the highest volume of reports. It's good to schedule a launch during a time when the security-focused team can devote significant time to validating and escalating issues. At this level, teams may choose to outsource triage management to gain efficiency of scale and maintain response time SLAs while growing. Your CSM will support your public launch and announcement, helping you promote the milestone and attract hackers to your program. Your CSM will also help you manage your expanded relationship with the researcher community. Should you run into any conflicts with researchers, HackerOne's mediation team will review the context of any disagreements, working with both parties to ensure a satisfactory resolution and help you take any disciplinary action required.

> "The vulnerability insights from our bug bounty program have enabled us to find improvement opportunities throughout the SDLC, and proactively reduce vulnerabilities like XSS by 98%."
>
> **Alejandro Iacobelli**
> Application Security Senior Manager, Mercado Libre

Answered mostly 4s?

Level 4: Bringing Most of Your Attack Surface in Scope

The most mature organizations recognize that their whole brand is at risk if a vulnerability is exploited. Including your entire attack surface in the scope of your bug bounty program demonstrates your commitment to protecting your brand. These organizations will also consider including their suppliers within the scope of their bug bounty, recognizing the risk the software supply chain can pose. The benefits of brand trust and continuous security are significant.

Community: The world's top hackers are looking for bugs on the most mature programs because they know those organizations are going to be responsive and will prioritize security. HackerOne's 7th Annual Hacker-Powered Security Report shows that while bounties are the main attraction to a program, other attractive factors include the anticipation that a lot of vulnerabilities will be available to find on a target (50% of hackers said this attracted them to a program), and a varied scope (which attracts 46% of hackers). 17% of hackers will spend time on a program due to their relationship with the organization's security team. Work with your CSM to look at organization-wide goals and help build a community engagement plan.

Platform: Global organization leaders should be invited to each program, with appropriate permissions configured. View program-level reporting capabilities and ensure there is support for organization-wide analytics. Consider managing a global organization-wide inbox that can be the front door for any issues that have unclear owners so those issues can be segmented and filtered to the right resources for faster remediation. Mature organizations benefit from data-driven program optimization recommendations and features that continue to encourage hacker engagement. At this level of maturity, an organization should consider taking part in a Live Hacking Event, an in-person engagement that brings the world's top hackers together to collaborate on a single program. Mature programs are more likely to disclose vulnerability findings publicly, to demonstrate transparency and to educate and improve security across the board.

Engagement Team: Establish global SLAs for the metrics that are easiest to control, and custom SLAs for particular assets. For example, "time to initial response" could be an organization-wide SLA, but "time to resolution" may vary widely across different programs. Consider implementing overflow procedures, in which one triage team gets flooded with reports and can "borrow" resources from another. This kind of flexibility and thoughtful planning can ensure an organization meets goals without ballooning headcount. At this level, teams will likely want to outsource triage management to gain efficiency of scale and maintain response time SLAs while growing.

> Hyatt's purpose of care informs all business decisions, and developing a best-in-class cyber security program in order to protect guest, colleague, and customer information is one way we are delivering on our purpose. We believe there is immense value in having a bug bounty program as part of our cyber security strategy, and we encourage all companies[…] to take a similar approach and consider bug bounty as a proactive security initiative.
>
> **Benjamin Vaughn**
> Chief Information Security Officer, Hyatt

Answered mostly 5s?

Talk to us! Please contact sales@hackerone.com. We've encountered just about every bug bounty situation in the book, but we are also hungry to help unique organizations solve unique challenges.

> Having a VDP is a core component to a robust vulnerability management program. Cultivating a positive relationship with the researcher community is incredibly valuable to your overall security program.
>
> **James Johnson**
> CISO, John Deere

Cover the Basics With a Vulnerability Disclosure Policy

Regardless of your level of maturity, having a clear way for members of the public to responsibly report any vulnerabilities found in your systems is a security best practice, and one that is increasingly being mandated by law. A vulnerability disclosure program (VDP) serves as a digital neighborhood watch, providing clear guidelines and a direct channel for external parties to report vulnerabilities as soon as they detect them. Adopting a VDP is not just best practice; it's becoming encouraged by government regulations and global compliance frameworks.

HackerOne Response, our VDP solution, establishes an open channel for third parties to report unknown and potentially harmful vulnerabilities directly to your security team. Streamline vulnerability management through efficient communication with external researchers, evaluation of their impact based on CVSS, and prioritization of the remediation of the most critical vulnerabilities. Implementing a VDP publicly demonstrates your commitment to security, showcasing transparency, accountability, and a proactive approach to safeguarding your systems.

HackerOne has vetted hackers for hundreds of organizations including:

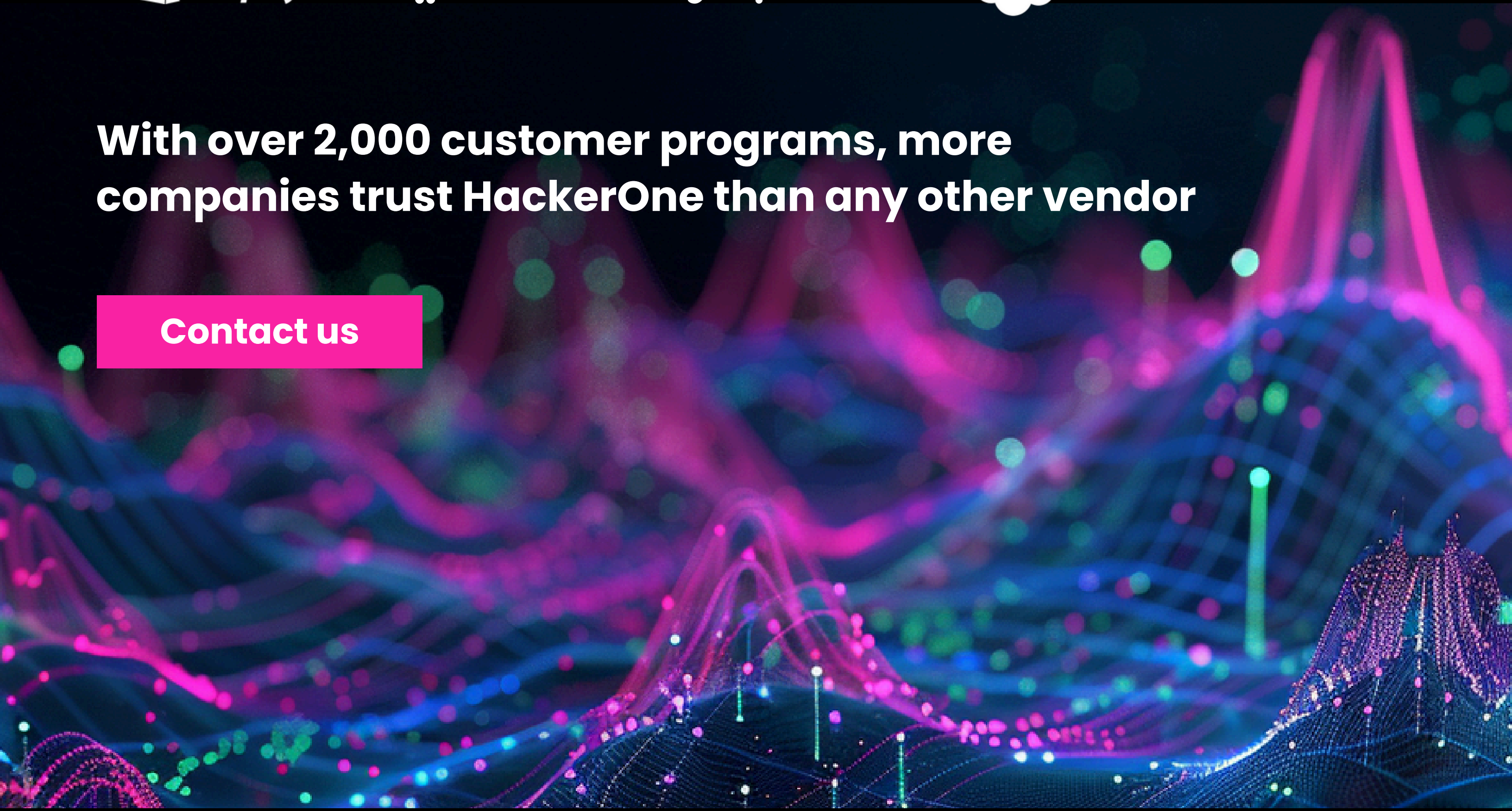
gm | Lufthansa | ZEBRA | European Commission

Spotify | citrix | PayPal | Uber | HYATT

U.S. Department of Defense | Google | reddit | Nintendo | Adobe

A.S. Watson Group | Dropbox | yahoo! | priceline

shopify | slack | yelp | salesforce | TOYOTA



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

Contact us