HACKER-POWERED SECURITY FOR STARTUPS

Supporting growth, reducing risk, and managing costs, all in one.

hackerone

You've proven your model, secured the funds to expand, and now just need to make it happen.

Don't let a product vulnerability or an ill-timed disclosure knock you off course.

You are laser-focused on building the best product, and growing fast without sacrificing quality. But growth can be crippled if customers sense a risk to their data, or, worse, if a public breach undermines confidence in your offerings. Startups also need to be diligent with budgets and tightly control costs outside of what directly contributes to growing market share or mind share.

Hacker-powered security checks off each of those boxes for growth-stage startups. It's a cost-effective means for reducing risk and improving security, while also enabling engineering scalability and efficiency. Harnessing the effectiveness of hacker-powered security in a thoughtful and well-built program also signals to customers, partners, and investors that you're building a high-trust product and brand that makes customer and data security a top priority.

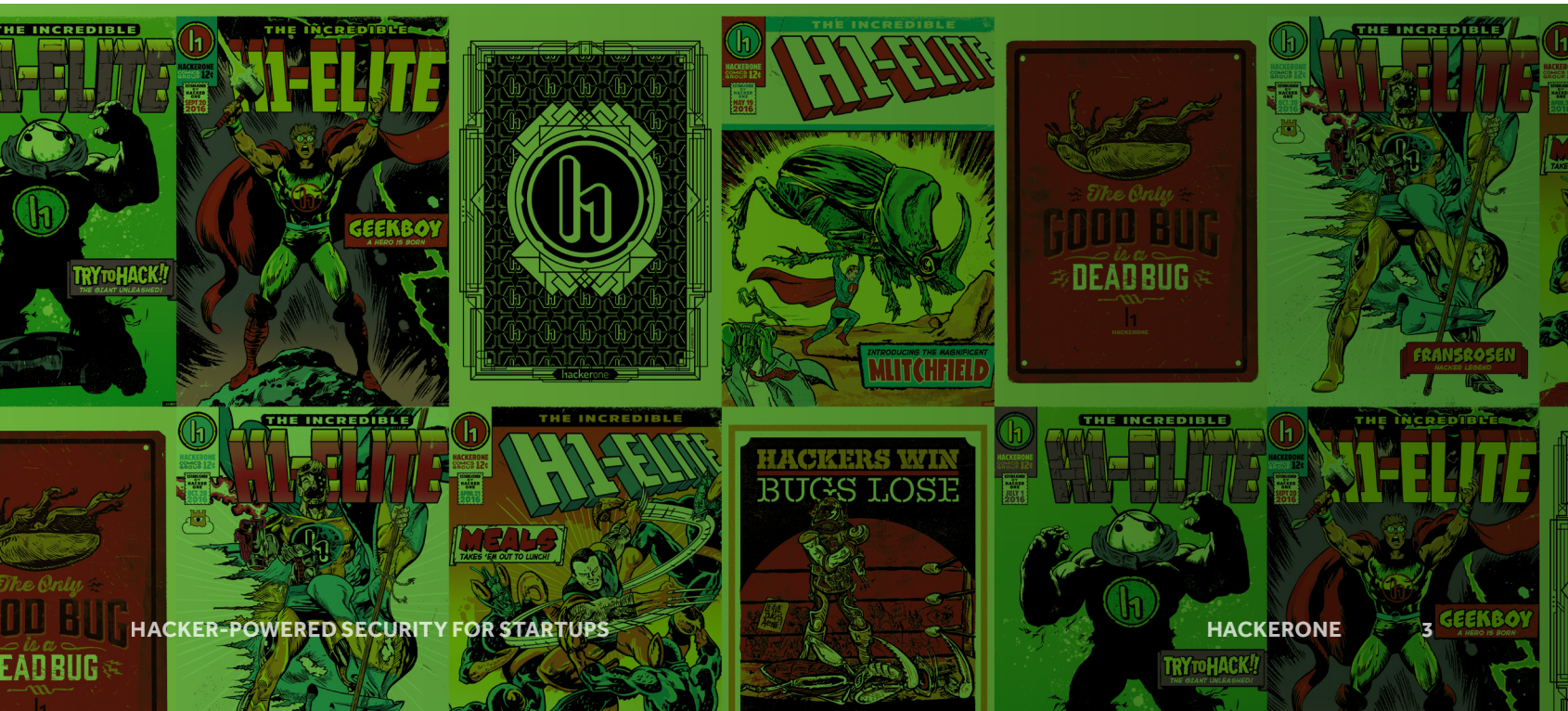
> The diverse perspectives and creativity of the participating hackers was astounding. We were so impressed, we couldn't wait to do another (HackerOne) Challenge.
>
> **GEORGE GERCHOW,**
> **CHIEF SECURITY OFFICER, SUMO LOGIC**

ALIEN VAULT

Like many organizations, **AlienVault** had set up a vulnerability disclosure policy for any bugs found on their website. If someone found a vulnerability, all they had to do was send an email to their security team.

AlienVault quickly found that this was inefficient, so they switched to **HackerOne Response**. With the help of a dedicated platform, AlienVault can easily manage incoming reports, triage them, and automatically create tickets on their internal ticketing system for only the valid reports. They've reduced their response time from the previous 5 days down to just 1 or 2. Extrapolate that over every incoming bug report and AlienVault is saving a lot of resource time.

But don't take our word for it. Read all about AlienVault's journey to HackerOne Response and their great results on **their own blog post**.



Sustained Hypergrowth and Good Security is Possible with Hacker-Powered Security

It's all too common to see yet another company dealing with the fallout of an unknown (or, all too often, known) vulnerability exploited by criminals.

No matter which industry you target or what size you are, the security of your data, systems, and products has to be top of mind for you.

> **Because security and privacy of your customers' data is top of mind for them, more so now than ever before.**

As part of the leadership team, your job is to reduce the risk of a security incident, protecting your brand and assets, and ensuring the security of your customers and their valuable data. Sure, you can back-burner security and decide to go the "security through obscurity" route (like - who cares about our startup right now?). Resorting to ad hoc last minute breach responses is a disservice to your customers who trust you with their data. And in the age of ultra-transparency and privacy considerations, you can't afford not to think about security.

You must do everything in your power to avoid an incident in the first place, and choosing the right partner in your journey is a big step in the right direction.

The hard reality is, if a security incident happens, you're going to have to take the blame. In fact, **Verizon's 2018 Data Breach Investigations report** found that almost one in five breaches were due to employee errors related to information security. With most of your efforts aimed at quickly growing your business, mistakes will be made. Are you as protected as you can be?

Security is not an expense, it's an investment in your future. Keeping your products and data secure used to be expensive and out of reach for young and hungry startups. In the fast pace of deployment, your limited engineering resources are focused on product development and new features. That's why you need help from a scalable, expert security partner.

Hackers are the answer for "secure hyper growth" in today's speed of development. The continuous coverage from hacker-powered security is something that's just not possible with your internal team. In other words, you require a new and novel approach, one that's been proven by some of the most respected tech companies from across the globe.

Good Business is Good Security

According to **Gartner's** "Emerging Technology Analysis: Bug Bounties and Crowdsourced Security Testing" report, published in June 2018, crowdsourced security testing is "rapidly approaching critical mass". And, according to **The Hacker-Powered Security Report 2018**, customers of HackerOne resolved more than 27,000 hacker-discovered vulnerabilities in the past year alone.

When fast-growing tech leaders as diverse as **Flexport**, **Yelp**, **Wordpress**, **Mapbox**, and others are using crowdsourced security tactics, and seeing this level of success, it's clear your toolset is incomplete without it.

Leveraging the wisdom and power of the vast white-hat hacker community is a new security expectation from your customers, investors, and even **government agencies** and **industry groups**. It improves and scales your security capabilities, helps protect your assets and strengthen your brand, and demonstrates innovation. The best part is that it's pretty easy to get started, to scale your efforts, and to realize immense value without an immense budget. You define the parameters, you set the budget, and you only pay for results.

Read on to learn the best practices for integrating hacker-powered security into your startup.

Why Does Security Matter?

REDUCING COSTS

Baking security & privacy best practices into your culture from the start is cheaper than "bolting it on" later. Breaches can cost millions of dollars; investing in security now can help avoid a disaster later.

STRENGTHEN YOUR BRAND

It's not all doom and gloom; many organizations are using security as a competitive advantage to strengthen their brand. Users want to know their data is safe with you.

SCALABILITY

In order to reach millions of users, work with other businesses, and achieve product goals, you'll need to start early to scale out security & privacy practices as your organization grows.

COMPLIANCE

With new compliance regimes such as GDPR, the earlier you have security & privacy controls in place, the easier it will be to avoid hefty fines from regulators.

What is Hacker-Powered Security?

Hacker-powered security is any technique that utilizes the external hacker community to find unknown security vulnerabilities and reduce cyber risk. Common examples include bug bounty programs (such as **HackerOne Bounty**), time-bound bug bounty programs (**HackerOne Challenge**), and vulnerability disclosure policies (**HackerOne Response**). With hacker-powered security testing, companies get the skills, experience, and nonstop coverage of white-hat hackers and researchers to help identify vulnerabilities before they can be exploited by criminals. It's a fast, structured, and proven model for crowdsourcing the right expertise, applying it when and where you need it, and paying only for results.

Think of hacker-powered security as an extension of your internal engineering and QA teams, but with nearly limitless capabilities and an elastic, on-demand usage model. Hackers are no longer operating in legal gray areas with legal safe harbor in hacker-powered security programs, and in fact, lawmakers and global government agencies as varied as the European Commission to the U.S. Food and Drug Administration are recommending and promoting hacker-powered security.

With HackerOne, it's easier than ever to get started using proven, online platforms and turnkey solutions that can put either a handful or a few hundred hackers on your security team almost overnight.

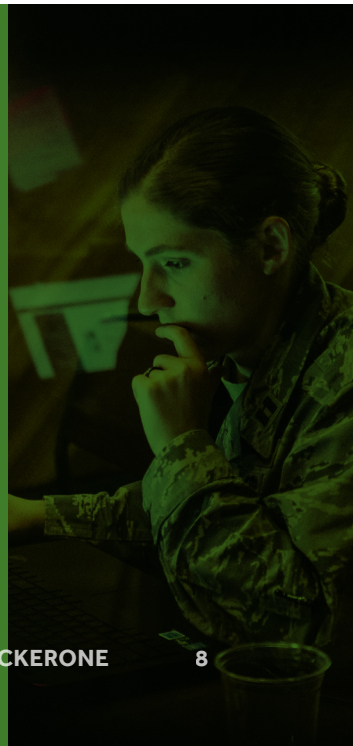
> The first week we launched HackerOne (hackers) found several high priority bugs we fixed immediately. Huge value at the fraction of the costs.
>
> **AMOS ELLISTON, CHIEF TECHNOLOGY OFFICER AT FLEXPORT**

sumologic

As a cloud-based log management and analytics company, **Sumo Logic** is subject to strict compliance and regulation standards. They utilized all the typical security tactics, until they questioned why their penetration test reports kept coming back clean. They knew it meant a hardening of their attack surface, so they set out to try something few in their position would even consider.

Sumo Logic ran their first private, time-bound bug bounty program with **HackerOne Challenge** in late 2017. In just 15 days, 5 hackers found 12 vulnerabilities that had been missed by earlier pen tests. After those results, they enlisted the help of HackerOne managed services to triage reports as they came in, which decreased response times to hackers.

Since then, Sumo Logic has completed two additional HackerOne Challenges with the help of 93 participating hackers. In total, they've identified 30 vulnerabilities, 9 of which were high or critical severity.



New to Hacker-Powered Security? Here's a Quick Glossary to Get You Up to Speed.

HACKER
One who enjoys the intellectual challenge of creatively overcoming limitations.

HACKER-POWERED SECURITY
Any technique that utilizes the external hacker community to find unknown security vulnerabilities and reduce cyber risk. Common examples include private bug bounty programs, public bug bounty programs, time-bound bug bounty programs and vulnerability disclosure policies. With hacker-powered security testing, organizations can identify high-value bugs faster with help from the results-driven ethical hacker community.

HACKTIVITY
Hacker activity published on the HackerOne platform.

PUBLIC BUG BOUNTY PROGRAM
An open program any hackers can participate in for a chance at a bounty reward.

PRIVATE BUG BOUNTY PROGRAM
A limited access program that select hackers are invited to participate in for a chance at a bounty reward.

TIME-BOUND BUG BOUNTY CHALLENGE
A program with a pre-determined limited time frame. In most cases hackers will register or be invited.

VULNERABILITY
Weakness of software, hardware, or online service that can be exploited.

VULNERABILITY DISCLOSURE POLICY (VDP)
An organization's formalized method for receiving vulnerability submissions from the outside world. This often takes the form of a "security@" email address. The practice is outlined in the Department of Justice (DoJ) Framework for a Vulnerability Disclosure Program for Online Systems and defined in ISO standard 29147.

A Security Imperative

Criminals, nation states, and nefarious groups are getting more aggressive and more clever by the second. No matter your size or stage, you cannot afford to ignore proven security techniques. Companies used to have just one option for staying ahead of criminals: hire more security engineers, buy the latest scanner. But that's a "spray and pray" type of approach and, especially for startups, that is expensive and doesn't solve the problem.

What's more, with new laws and regulations, like GDPR, **some even argue that** not doing everything possible to protect systems and data is irresponsible.

A simple vulnerability disclosure policy (VDP) is a logical place to start for many startups, while others jump right to engaging hackers with a time-bound bug bounty challenge or with a continuous bug bounty program. It all depends on the resources you have available and your ability to handle incoming reports. You choose, and that's the beauty of hacker-powered security. It fits your needs, no matter your size or budget or goals, and it can be throttled up or down depending on your stage or business shifts.

No matter what you choose, HackerOne can help. Over 1,000 organizations, from stealthy startups to global conglomerates, trust us to be their hacker-powered security partner. **We streamline the process of finding and attracting top hacker talent, providing data and guidance on bounty values, integrating reports into your existing bug tracking workflow, and facilitating bounty payments across countries and currencies.** Plus, we offer services to help you triage incoming reports or manage the entire process, and HackerOne does it better than anyone.

FLEXPORT

Flexport is sometimes referred to as "Uber of the Oceans," which is a great way to describe this international freight forwarder and customs broker. In a nutshell, they handle freight that's too large for FedEx or UPS.

But while Flexport moves tons of physical freight every day, they also manage petabytes of digital data that is critical to the supply chains of their global manufacturing customers. The data from Flexport shipping manifests gives customers a clear picture of each shipment's contents and destination, which they use to choose the most cost-effective shipping methods.

To help protect that data, Flexport turned to **HackerOne Bounty**.

Better Security on Your Terms

Hacker-powered security means engaging a community of experts and rewarding them for their efforts. It could be as simple as providing a channel for them to report potential bugs, to enlisting the help of a few hackers with specific skills to focus on a new product, to a continuous bug bounty program. Here are the key flavors of hacker-powered security.

- **VDP:** A vulnerability disclosure policy provides the mechanism for anyone to report a potential vulnerability is table stakes for security in today's digital world. That's the easiest entry point for hacker-powered security. There's no bounty to be awarded, but it does require you to think through your program scope and the internal process for evaluating reports and communicating with hackers.

- **Time-bound:** Short-term hacker-powered, bounty-driven programs can be used to replace or augment your existing penetration tests by having hackers focus on a specific attack surface for a limited time. It's a great way to evaluate the benefits and impact of a broader bug bounty program and get more from your pen test budget. How you set bounty values can also help you manage report volumes or aim attention at specific areas of concern.

- **Private bounty:** A continuous but private, targeted bug bounty program limits the number of hackers involved, the volume of incoming reports, and public awareness of the program. It also lets you view the potential size and cost of a broader bounty program so you can scale your internal teams and processes to match.

- **Public bounty:** Public bug bounty programs are continuous and open to everyone, so they represent the highest hacker diversity and produce superior results. On average, public programs engage 3.5 times the number of hackers reporting valid vulnerabilities.

The best part of hacker-powered security is that you're always in control!

Reduce Risk. Enable Uninterrupted Growth. Launch Products Faster... Get it all With Hacker-Powered Security!

The benefits of hacker-powered security are many, from improving on traditional pen tests by identifying 10-times the number of critical vulnerabilities to identifying dozens or hundreds of vulnerabilities in a few days to spending just a fraction of a security engineer's salary while paying only for validated results.

For growth-stage startups, consider the benefits working with a proven platform that's built a stellar reputation with the hacker community, and has experience tracking, categorizing, and triaging tens of thousands of reports.

No matter how you structure your own program, hacker-powered security is right for you. Working with HackerOne gives you access to vetted, trusted hackers. It provides several layers of control for selecting, inviting, and approving hackers based on their reputation, past program participation, specific skills, and more.

HackerOne has helped all types of organizations manage thousands of programs since 2012, resolving more than 75,000 vulnerabilities and paying out more than $35 million in bug bounties. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security partner. That means we're trusted by some of the most demanding and visible organizations across the globe, from the biggest global organizations, like the U.S. Department of Defense, Google, Yelp, GitHub, and the CERT Coordination Center, to the most successful startups, like Mapbox, Yext, Flexport, and AlienVault.

And we can help you, too! Learn more by visiting our website or **contacting us** today.

References

For more information on hacker-powered security, check out the resources below or view all of our guides, case studies, infographics, and more at **hackerone.com/resources**.

- **Vulnerability Disclosure Policy Basics: 5 Critical Components**
- **7-step Roadmap To Hacker-Powered Security Success by 451 Research**
- **The Bug Bounty Field Manual**
- **Hacker-Powered Pen Tests and the Power of More**
- **HackerOne Challenge Customer Testimonials**
- **The Hacker-Powered Security Report 2018**
- **Hacker Vetting: Trusted Security Talent for the Enterprise**

hackerone

ABOUT US

HackerOne is the #1 **hacker-powered security platform**, helping organizations find and fix critical vulnerabilities before they can be exploited. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security alternative. The U.S. Department of Defense, General Motors, Google, Twitter, GitHub, Nintendo, Lufthansa, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel, the CERT Coordination Center and over 1,000 other organizations have partnered with HackerOne to resolve over 80,000 vulnerabilities and award over $35M in **bug bounties**. HackerOne is headquartered in San Francisco with offices in London, New York, and the Netherlands.

Contact us to get started.