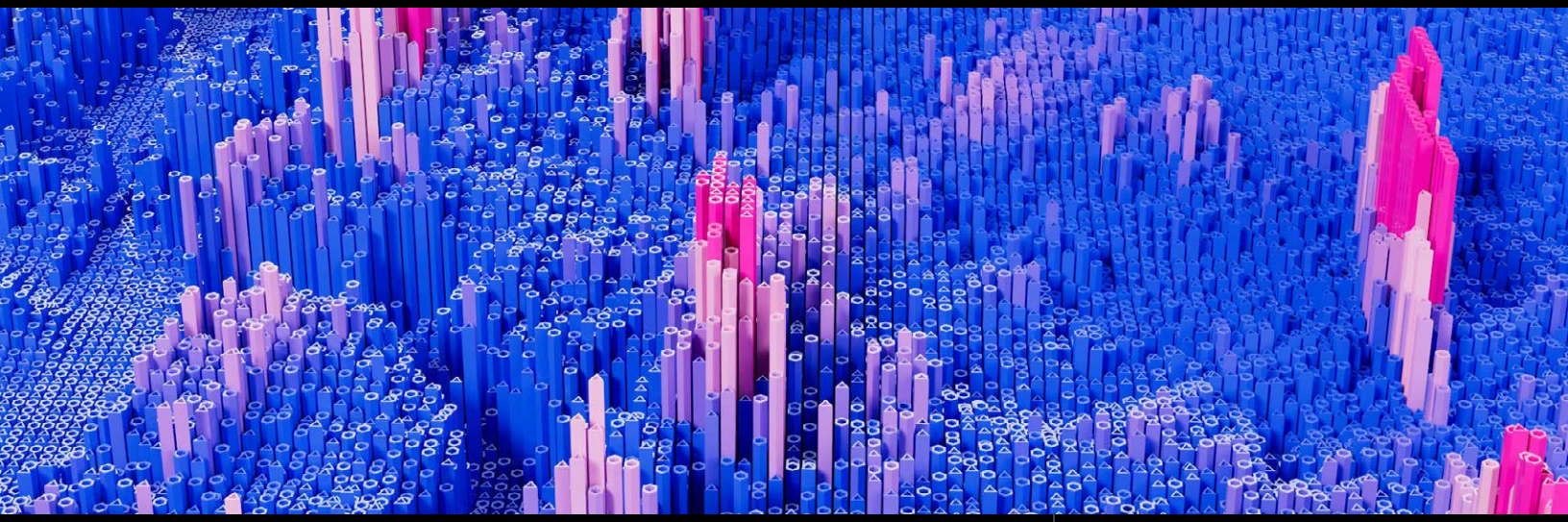
Delivery Hero | hackerone

CASE STUDY



How Delivery Hero Scales a Global Security Strategy with HackerOne

Bringing food to doorsteps in 70+ countries, Delivery Hero's operations are as diverse as the company's threat landscape. With the help of HackerOne, Delivery Hero is fostering a fresh approach to offensive security centered on a global bug bounty program.

4
continents

70
countries

7,000+
domains

Key Takeaways

Initial Challenges

- Exposure to cyber risk across a vast footprint of sites, brands, apps, and customers
- Disjointed security posture due to cultural and language differences
- Previous bug bounty and vulnerability disclosure program (VDP) providers delivered low-quality findings

Security Goals

- Consolidate into one harmonized global security platform
- Partner with ethical hackers familiar with regional nuances
- Uncover more critical vulnerabilities and speed up time to remediation

Why HackerOne

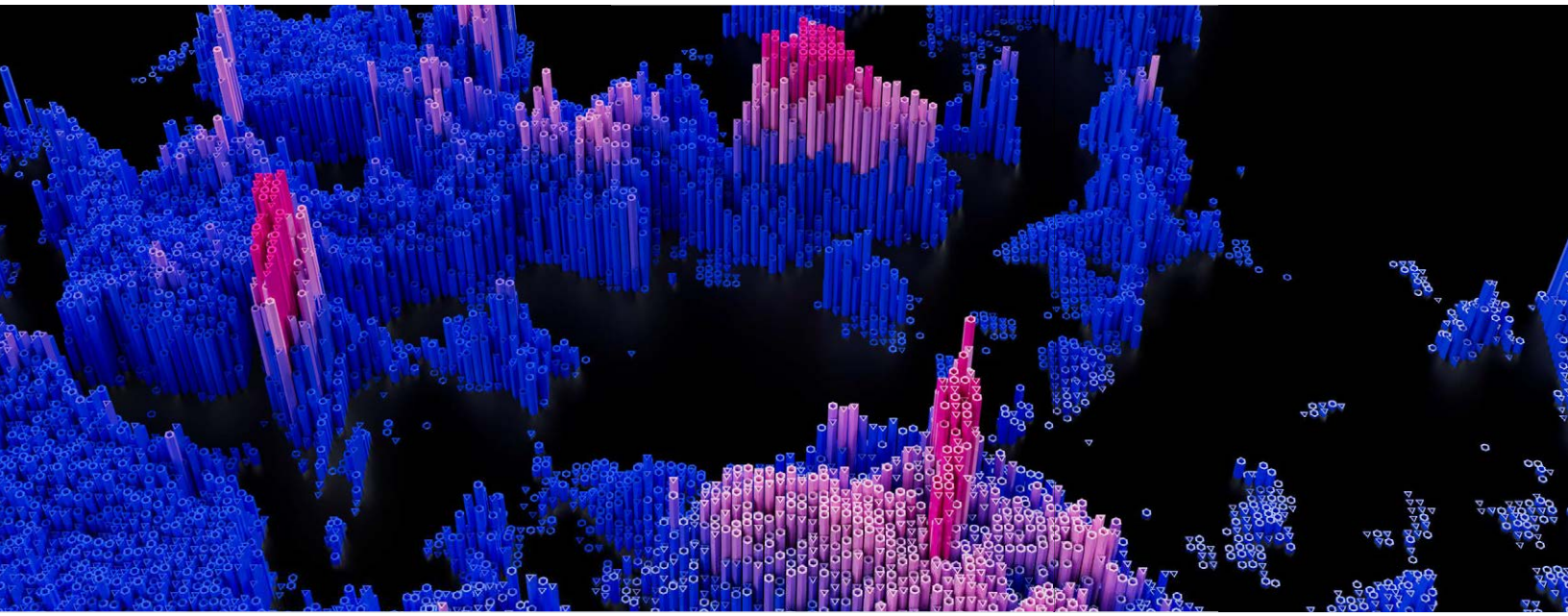
- Robust, proven platform fulfilling all requirements
- Extensive global community of skilled researchers
- Market leader highly rated by customers

Outcomes

- Receives high-impact bugs across entire scope including global subsidiaries
- Faster remediation and less time spent on manual work
- Stronger security awareness within engineering and across the organization

"Delivery Hero recognizes the significance of establishing a partnership to engage with a global network of security researchers. Our primary goal is to detect unique security vulnerabilities that traditional penetration tests might overlook. Consequently, we have chosen to collaborate with HackerOne."

Nouman J. Hashmi
Senior Security Engineering Manager, Delivery Hero



Safeguarding Global Growth

Founded in 2011, Delivery Hero expanded rapidly to 70+ countries, 4 continents, and 7,000+ domains. This vast footprint—including many apps, regions, and brands—sets them apart. Yet it also exposes the company to diverse methods of exploitation through vulnerabilities like insecure direct object references (IDORs), SQL injections, and authentication issues.

Navigating this complex security landscape is further complicated by a variety of supported languages, millions of deployments, and ongoing mergers and acquisitions (M&A).

"Consider that South America has different threat actors and dialects compared to the Middle East," explained Nouman Hashmi, Senior Manager of Security Engineering at Delivery Hero. "We needed a more effective way to attract top talent in each region while streamlining our security efforts globally."

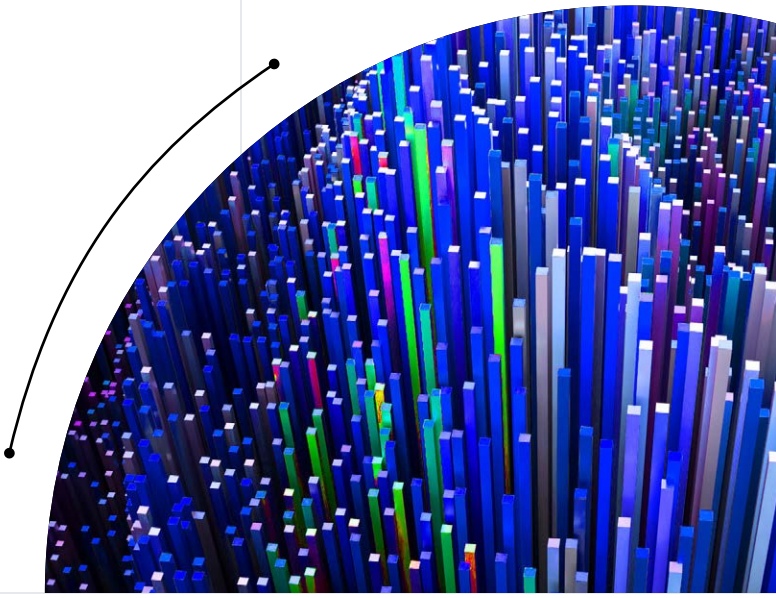
With continued growth in mind, Delivery Hero realized the importance of offering vulnerability discovery coverage for its entire public attack surface. Previous bug bounty programs were siloed and delivered subpar results. So, Delivery Hero set out to consolidate efforts with one vendor capable of accommodating the company's diverse requirements—including researchers with regional expertise and language proficiency.

During this process, they discovered that a recent acquisition, Glovo, had a successful partnership with HackerOne. After a thorough analysis and vendor scoring, Delivery Hero saw that all their needs could be met with HackerOne Bounty, HackerOne Triage, and a VDP.

"Our security landscape is a colorful mix of different languages, threats, and protection tools—all of which impact our people, processes, and compliance. It's a challenge we welcome—and HackerOne is the ideal partner, bringing the strength of a global platform alongside nuanced hacker expertise."

Nouman J. Hashmi
Senior Security Engineering Manager, Delivery Hero

After a thorough analysis and vendor scoring, Delivery Hero saw that all their needs could be met with HackerOne Bounty, HackerOne Triage, and a VDP.



Gaining Traction with a Phased Approach

Adopting HackerOne's best practices for long-term bug bounty success, Nouman and his team made the decision to scale the bounty program one step at a time to ensure the team was prepared ahead of each iteration. He explains, "We started with a small-scale, private program—gradually expanding our efforts quarter by quarter. As we brought in entities, they took charge of identifying relevant issues within their own domains. We quickly noticed an improvement in terms of the number and quality of findings from HackerOne."

Demonstrating the value and impact of these findings is crucial to the program's success. As the security team tracks and shares results, other business units gain the evidence they need to join the program and increase bounty budgets.

Tugay Özçelebi, Security Engineer at Delivery Hero, explains:

"We don't need to persuade them much; the reports speak for themselves. While we conduct our internal pentesting and scanning, the bug bounty program brings in exceptionally valuable niche reports that automated scanning simply can't uncover."

In one instance, the bounty program exposed a vulnerability in an authorization process, which could have allowed unauthorized access to a consumer app. The team that discovered this vulnerability initiated its own security program to collaborate on a solution.

"Some researchers report infrequently, but they work *hard* during that time and uncover something novel," Tugay explains. "Quantifying those vulnerabilities can be somewhat subjective, but they play a crucial role."

In one instance, the bounty program exposed a vulnerability in an authorization process, which could have allowed unauthorized access to a consumer app. The team that discovered this vulnerability initiated its own security program to collaborate on a solution.

Turning to Triage

A key performance indicator for Delivery Hero is *time to remediation*, weighed against other aspects, such as business impact. That's where HackerOne Triage plays a crucial role, customizing processes and reports to help accelerate fixes for the most critical vulnerabilities.

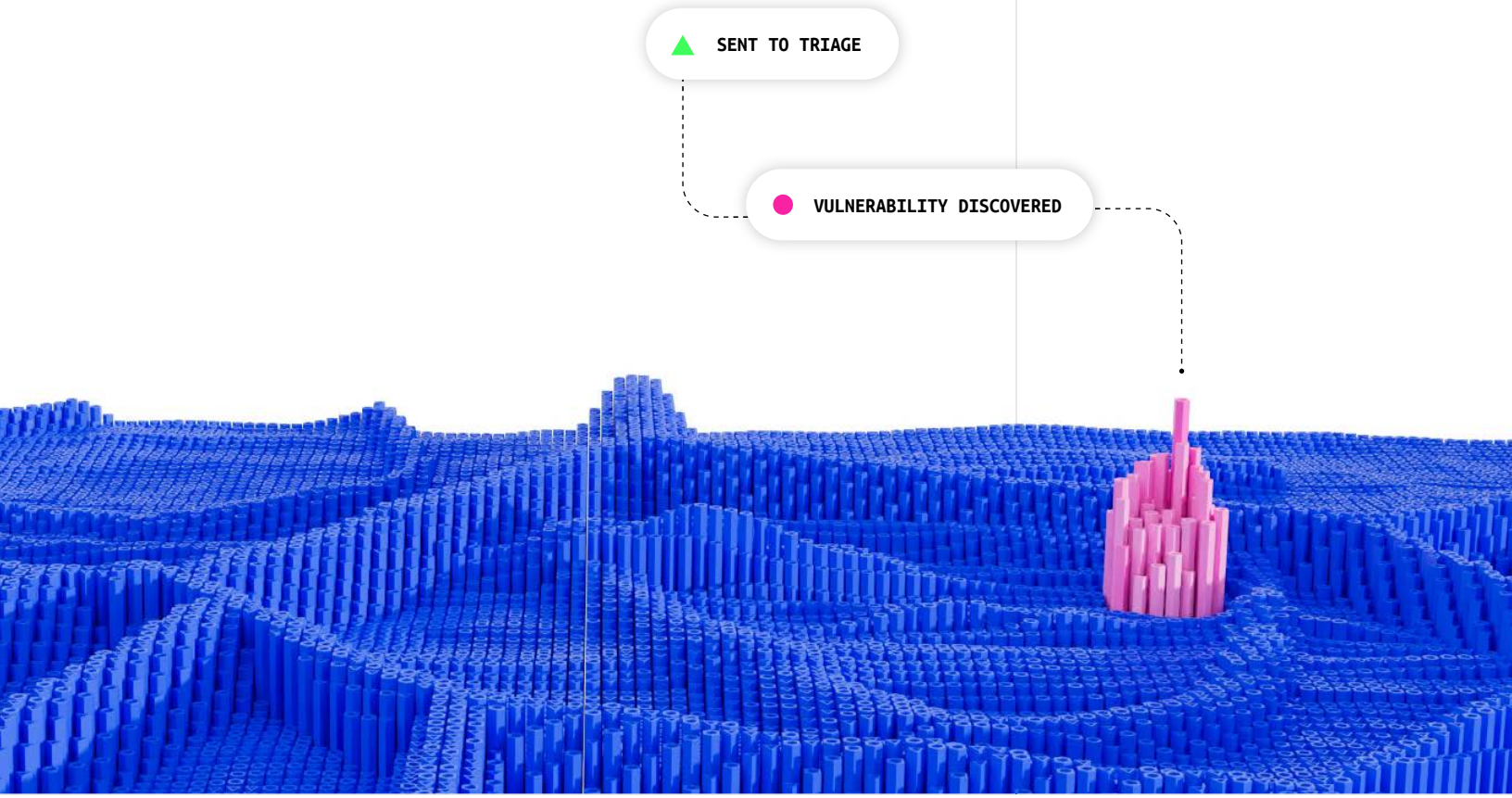
"As soon as a bug arrives from Triage, it falls into our hands," adds Nouman. "We swiftly create a JIRA ticket, closely track its progress, and tackle any challenges, roadblocks, or risk acceptance. We have an SLA in place that targets a seven-day remediation timeline for critical vulnerabilities."

Another time-saving feature? Triage provides concise summaries that distill the intricate and often laborious information typically found in vulnerability reports.

"We no longer need to manually sift through the entire report to find the vital information," notes Nouman. "This insight helps us promptly recreate the vulnerability and easily communicate the fix with other business units."

HackerOne Triage has been really helpful in making sure that top-notch reports get attention right away, with quick responses and efficient resolutions for contributors. This lines up with our commitment to stick to industry response times, making sure our researchers' input is recognized promptly and issues are sorted out fast and effectively.

Nouman J. Hashmi
Senior Security Engineering Manager, Delivery Hero



Creating a Framework for Security

Delivery Hero sees their bug bounty program as a catalyst for change. For example, they've introduced a new metric called *business impact* as part of their global process. This metric helps them gauge the potential consequences of a vulnerability, such as monetary losses. Based on this perceived impact, tickets are assigned and escalated.

"Your bug bounty program is undoubtedly a safety net, but it plays a crucial role in your overall ecosystem," emphasizes Tugay. "Achieving a complete and secure landscape requires this last line of defense. That's why we aim to expand the scope of our bug bounty program and use the insights gained to drive improvements."

Delivery Hero's VDP also acts as a talent funnel for its private bug bounty program, inviting hackers who submit impactful reports via the public VDP to participate in the bounty program to keep its roster fresh. Every business unit that is part of the bug bounty program is also onboarded to the VDP, providing one central global channel for responsibly submitted vulnerabilities that may be out-of-scope for bug bounty.

Delivery Hero's central security engineering team has also built the necessary processes to deliver its HackerOne programs to different business units. Delivery Hero subsidiary CTOs/CISOs can tap into their parent company's global HackerOne service model to ensure that everyone benefits from Delivery Hero's scale while still accurately tracking findings and bounty budget allocation for each business unit. This is the next level of preemptive security maturity: scaling beyond compliance into human-powered efficiencies.

"We don't just view our bug bounty program as a safety net; it's a vital part of our security strategy, playing a key role in creating a fully secure environment. By using our global HackerOne service model, we ensure consistent security standards across Delivery Hero and its subsidiaries, effectively managing vulnerabilities and budget. Our approach goes beyond mere compliance, embracing a proactive security model that's essential for our ongoing growth."

Nouman J. Hashmi
Senior Security Engineering Manager, Delivery Hero

Tracking Success

Continuously monitoring trends and raising awareness remains a top priority, led by the Delivery Hero Security Framework—which includes a cockpit view for each CIO and CISO, alignment to the Delivery Hero Security Framework, and gamification of SLA achievements through a leaderboard. The Delivery Hero Security Framework encompasses 166 commandments born from Delivery Hero's global regulatory and compliance requirements, with commandments including, but not limited to, penetration testing processes, vulnerability management, and security awareness.

Every month, the central security team runs a summary report that shows all the issues created, new fixes, SLAs met or missed, and trends related to critical and high vulnerabilities. The result? Proof for the program, faster remediation, and improved security outcomes across all Delivery Hero entities.

Looking Ahead

In the future, Delivery Hero aims to make their bug bounty program public and establish a well-funded program to attract more top talent. They also intend to incorporate all public assets into the program once they've been internally vetted.

"People sometimes view a bug bounty program solely as a means to uncover bugs, but we also see it as an opportunity to learn and shift left," Tugay says. "We regularly meet to discuss the findings and explore ways to enhance our internal tools, technical capabilities, and scans to prevent similar issues from recurring."

With a unified platform, Delivery Hero continues expanding the global security team. They're working toward a "follow the sun" model, where pentesters across each time zone ensure continuous coverage and scans—a model that also counts on the global hacker community within the HackerOne platform.

"The HackerOne bug bounty program has become indispensable as we unify and grow," adds Nouman. "It goes beyond compliance, helping us embrace the multifaceted challenges posed by our diverse and colorful business."

Every month, the central security team runs a summary report that shows all the issues created, new fixes, SLAs met or missed, and trends related to critical and high vulnerabilities.

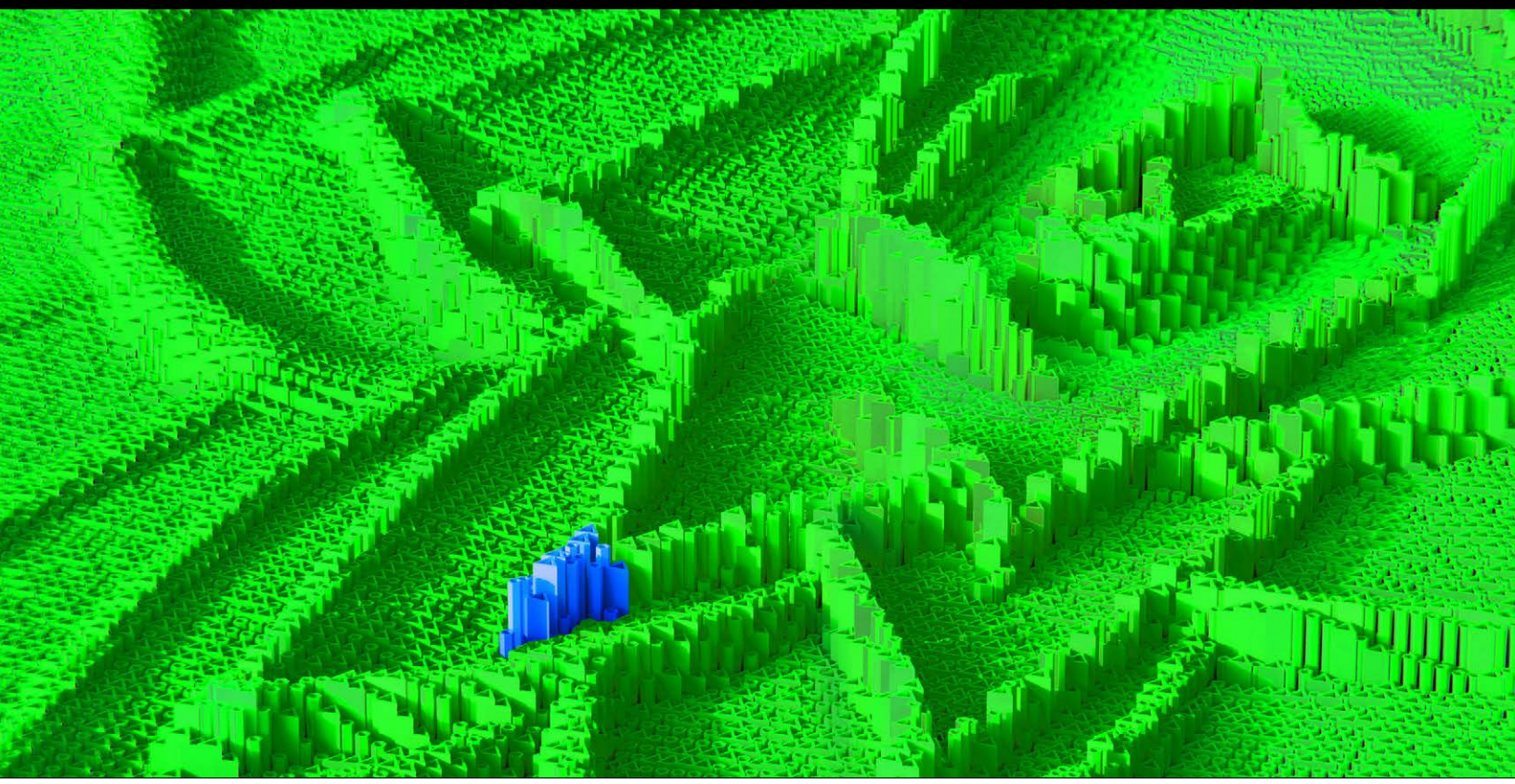
About HackerOne

HackerOne pinpoints the most critical security flaws across an organization's attack surface with continual adversarial testing to outmatch cybercriminals. HackerOne's Attack Resistance Platform blends the security expertise of ethical hackers with asset discovery, continuous assessment, and process enhancement to reduce threat exposure and empower organizations to transform their businesses with confidence. Customers include Citrix, Coinbase, Costa Coffee, General Motors, GitHub, Goldman Sachs, Google, Hyatt, Microsoft, PayPal, Singapore's Ministry of Defense, Slack, the U.S. Department of Defense, and Yahoo. In 2021, HackerOne was named a **'brand that matters'** by Fast Company.

About Delivery Hero

Headquartered in Berlin, Germany, Delivery Hero is the world's leading local delivery platform, with online platforms and mobile apps that seamlessly connect customers to a diverse array of restaurants and food services worldwide.

Recognizing the need for robust security across different entities and regions, the company turned to HackerOne and its global community of skilled researchers. A collaborative approach enables Delivery Hero to uphold stringent security standards and customer data privacy with every delicious order.



HackerOne has vetted hackers for organizations including:

gm · Lufthansa · ZEBRA · zoom · Twitter

Spotify · citrix · PayPal · Uber · HYATT

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

A.S. Watson Group · sumo logic · Snapchat · yahoo! · priceline

shopify · slack · yelp · salesforce · TOYOTA

hackerone

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

Contact Us