hackerone | ZEBRA

CASE STUDY

Zebra Defends Its Attack Surface from All Angles with HackerOne

As a world leader in digital products, solutions, and software, **Zebra Technologies** enables businesses of all sizes to connect data, assets, and people intelligently. With a mission to scale, Zebra turned to HackerOne to help the company shift left by moving security checks as early and as often in the software development life cycle (SDLC) as possible. The end goal? To defend and arm its security program from every angle.

Key Takeaways

Before Challenges

- Slow, traditional pentesting with insufficient reports led to gaps in testing the attack surface
- Security was not included early enough in development, leading to developers working separately from security
- No formal process for reporting vulnerabilities, exposing the company to more risk
- Business charter from the CEO and CISO to bring unity across siloed security functions

Security Goals

- Gain agility and speed with continuous testing
- Work with a diverse bench of security research experts
- Close the gap by taking control of 100% of the attack surface
- Establish a feedback loop to improve processes earlier in the software development life cycle (SDLC)

Platform Solutions

- HackerOne Pentest: Penetration Testing as a Service
- HackerOne Response: Vulnerability Disclosure Program (VDP)
- HackerOne Bounty: Private Bug Bounty
- HackerOne Challenge: Time-bound security testing
- Advisory Services: Triage, remediation, and custom reporting

Why HackerOne

- A collaborative partner that works closely with Zebra to keep its attack surface covered.

  "The people at HackerOne make a difference. They made it easy to get our program launched, helping us set bounties and expectations that meet industry standards. When we have a challenge, they work hand in hand with us to uncover solutions and ideas." — Dr. Jasyn Voshell, Zebra
- The ability to spin up rapid pentests with findings that go beyond the traditional scanner tools.

  "HackerOne can stand up our pentests three to five times faster than traditional firms." — Dr. Jasyn Voshell, Zebra
- On-demand reports and feedback help Zebra drive root causes back into the SDLC.

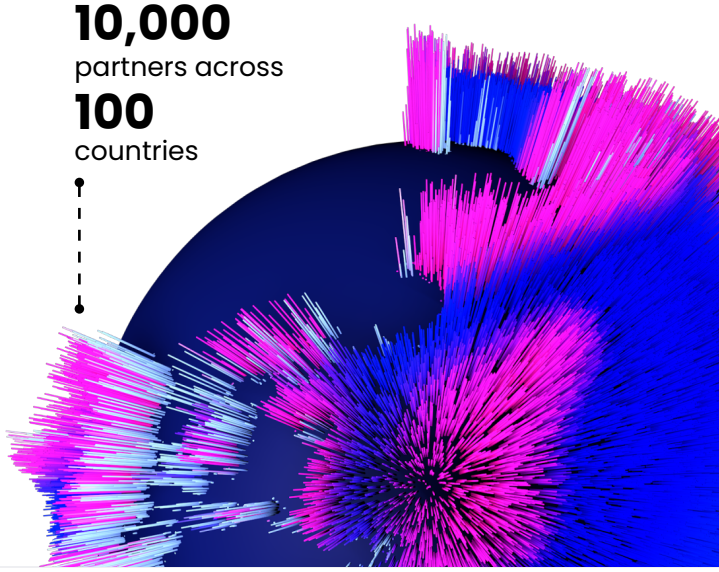
Outcomes

- Security-centric messaging improves consumer and partner trust in Zebra
- Rogue digital assets are now fully covered (uncovered, tested, and secured)
- Key stakeholders have oversight and confidence in the effectiveness of security
- Development teams are more accountable and incentivized to improve coding practices
- Speed and security of delivery practices support revenue and lowers risk

"We have been on a mission to transition from being a hardware company to also providing software and services for our customers. Certainly, that changes one's security lens. It's a completely different environment to have cloud-based, retail execution software available for enterprise-level organizations compared to having hardware-based printers installed and operated by the customer. We realized we needed to evolve ourselves and our security program to enable this transformation."

Mike Zachman
Chief Security Officer, Zebra

Zebra has over
10,000
partners across
100
countries



You may not always see Zebra Technologies, but as a leading brand in industrial printers, scanners, RFID, mobile computers, robotics automation, machine vision & imaging, retail execution software, and much more, Zebra solutions can be found working behind the scenes in industries worldwide. With over 10,000 partners across 100 countries, the company empowers its customers (including 86% of the Fortune 500) with a broad portfolio offering and regularly launches new products through organic innovation and acquisitions.

Because the company operates across numerous business units—each with its own unique blend of products and software—Zebra needed to unify and expand its security processes to decrease risk, protect revenue, and increase brand trust.

Traditional Pentests Exposed the Business to Risk

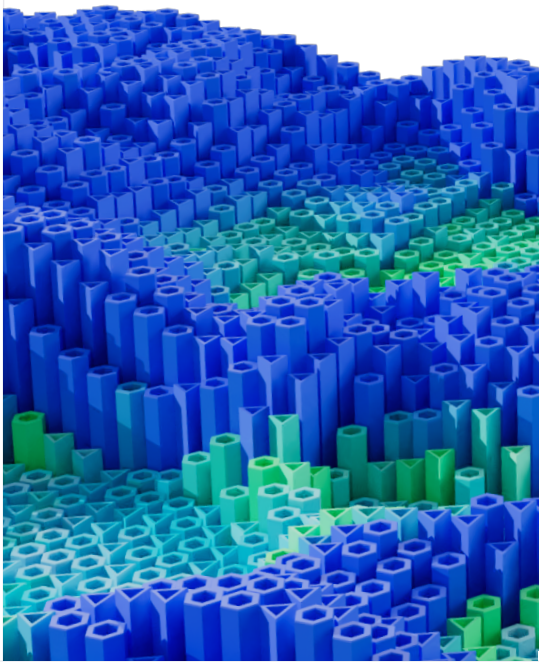
With a business transformation in full swing, Zebra needed to double down on its security approach. Each new product or acquisition increased the potential for unknown assets that could cause gaps, making them more vulnerable to breaches and security risks. Traditional pentesting provided some coverage, but the tests took time to spin up and were costly. Jasyn noted, "Our reports rarely gave us the full story."

Seeking a better solution, Jasyn reached out to a leading research firm, which recommended HackerOne. A rapid proof of concept provided impressive results, fueling the interest of internal decision-makers.

"Our first pentests revealed a major finding and showed the value of an ethical hacker community combined with PTaaS," says Jasyn. "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."

"With HackerOne, we are very targeted about what we need to find and how it's reported. This provides a clear return on our investment and helps us respond quickly to any high or critical vulnerabilities."

Dr. Jasyn Voshell
Director of Product and Solution Security, Zebra



Bug Bounty Keeps 2,700+ Assets Covered

Working with HackerOne, Zebra soon implemented a multi-pronged strategy involving regular code pentesting, a public VDP, and a private bug bounty program—all of which keep their attack surface covered.

"First, our pentests act as a gate check or immediate security checkpoint for new or acquired products. Every product is pentested before it's released to the customer," noted Jasyn. "Once out of the door, the pentested product becomes part of the bug bounty program. So, if any new bugs appear, we can catch them quickly—but we're not paying for things that already surfaced in the pentest, avoiding duplication of efforts."

A VDP Helps Close Any Security Gap

Zebra also casts a wide net of security through its ongoing public VDP, meaning any external party can report a vulnerability. Previously, third-party reports were sporadic and submitted via an email inbox. It took time and manual effort to filter through the messages. Without constant monitoring, vulnerabilities reported through the inbox could also slip through the cracks.

Now, their VDP keeps 100% of their assets covered. Zebra benefits from a streamlined process for receiving reports from any external party. HackerOne filters the results, checks for duplication, and routes verified vulnerabilities into a central portal.

As Jasyn notes, "By having just the essentials on my plate, I can respond to highs and criticals quickly, easily assign vulnerabilities to my team, and devote time to where I'm needed most."

Securing the SDLC

Zebra's enhanced security program enables the company to take a "secure by design" approach, integrating pentests and hackers at various stages of the product development process and into the rhythm of the business.

“Sometimes HackerOne brings us a result. Once we think we’ve fixed it, we want to retest—and it needs to happen fast to fit deadlines that constantly move,” says Jasyn. "Our ongoing service with HackerOne allows us to spin up a test quickly, which is critical to getting our products released quickly and securely.”

The quality of metrics and insights is another significant benefit. Traditional pentests that rely on generic scan tools provide snippets of the results in a single document—giving developers little to go on.

With HackerOne, Zebra leverages highly detailed, on-demand testing reports. Vulnerabilities reported by hackers also typically include proof-of-concept code. The researcher provides details on how they found the problem, the root cause, and suggestions for remediation.

The quality of the results gives credence to Zebra’s program and brings developers into a collaborative process of improving coding practices.

"From the workflows that make life easier to the speed of our pentests and the quality of our product development—all these benefits have led to accolades from the executive team, developers, and customers,"

Dr. Jasyn Voshell
Director of Product and Solution Security, Zebra

The Result: Security That Builds Trust, Quality, and Credibility

A measurable field risk was a top priority for Zebra—and they've collectively achieved that goal per each asset, product family, and business unit. A quarter-over-quarter reduction in vulnerabilities demonstrates the effectiveness of shifting security left into SDLC processes.

"Internally, we are faster at fixing a HackerOne finding than a finding from anywhere else," notes Jasyn. "We also get nearly zero false positives from HackerOne, thanks to triage. This speaks to the findings' quality and our confidence in HackerOne."

Regular testing also helps build customer trust and loyalty, which leads to more referrals and opportunities. For example, Zebra strengthened its relationship with a major retail customer through a shared fascination with bug bounty findings. Jasyn describes the scene:

"As part of our contract, a major European retail customer asks for a pentest report each year, and they are very tough on us if a critical vulnerability is surfaced. Last year, we shared what we were doing with bug bounty in terms of providing that layer of continuous security. That got them interested, and the next time we met with them, they were less focused on the pentest report and instead wanted to hear about what was found through the bug bounty program that other tools had missed. Talking about these programs transparently helps drive value with customers, who can see how committed we are to protecting their products."

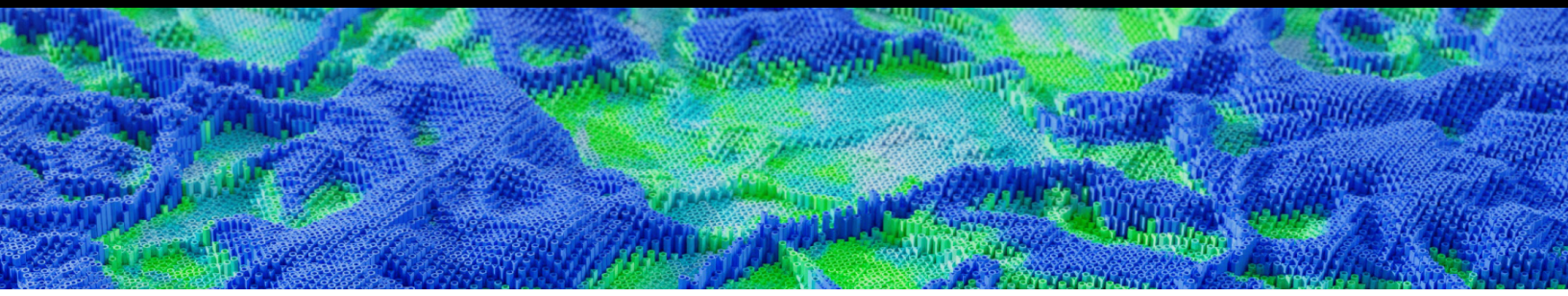
With such success and leadership support, Zebra plans to continue to expand its security program. Assets are regularly added to the scope of the VDP to help keep the program fresh. They also harden what goes into the bug bounty so that they can raise bounties and stand out as a marquee program for hackers.

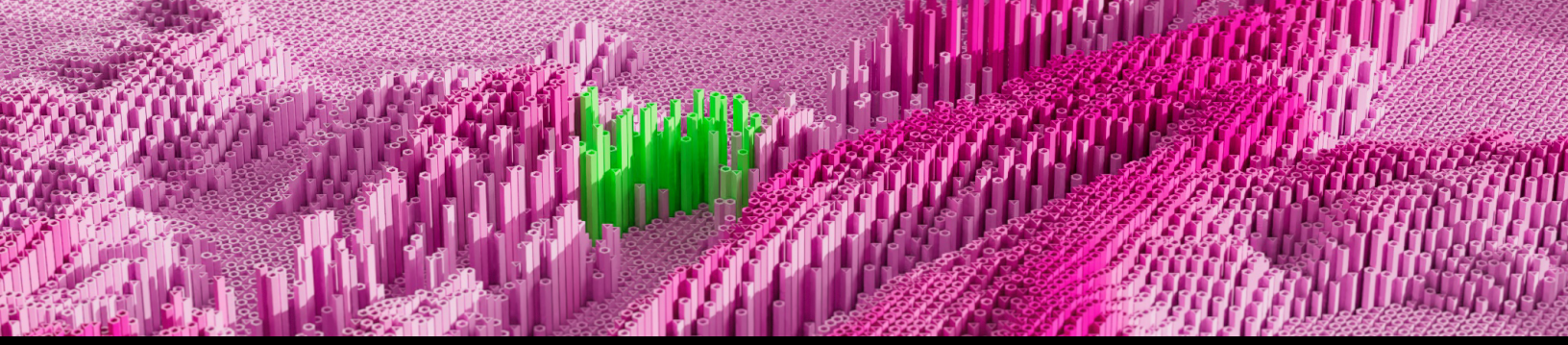
Creative Tip: Use Insights for Training

Every quarter, Zebra pulls the top findings and shares lessons learned through webinars with development teams. It's a valuable feedback loop that's primarily powered by HackerOne findings.

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.





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