hackerone

Nextcloud Builds Hacker-Powered Security into their Business by Design

Providing cloud-based solutions means security is always a concern. For Stuttgart-based Nextcloud, they doubled-down and made security an integral part of their entire business strategy.

Nextcloud

CUSTOMER DATA

PRODUCT TYPE
HackerOne Bounty

LAUNCH DATE
June 2016

VULNERABILITIES RESOLVED
100+

COMPANY SIZE
25+ employees

INDUSTRY
Technology

PARTICIPATING HACKERS
100+

Nextcloud differentiates from other online file sync and collaboration technology solutions by focusing on security, privacy and control.

Nextcloud solutions excel at giving their business customers the power to "know where data is, who has access, and that even meta-data does not leak." It's a security-first approach to how they design, build, and position their products, and it's no accident.

But putting "security first" in today's world is typically just marketing fluff. With Nextcloud, it's a core component of their entire business strategy, which lets them take an aggressive approach to security. It also gives their small security team the internal capital to realize an impressive average response time on their HackerOne Bounty program of less than 1 hour.

Nextcloud has elevated security from a cost center to an integral part of their business and their message.

NEXTCLOUD CUSTOMERS DEMAND THE BEST SECURITY

Nextcloud is banking on their security message to win more customers. It's an aspect of their positioning in the market that puts security front and center, which is what their customers care about most.

> “Control and compliance are the core differentiators of our solution, and security is of utmost importance,” said Frank Karlitschek, Nextcloud Founder and Managing Director. “We started Nextcloud on the premise of building a more secure solution. Security is considered in everything we do. **Everything.**

Nextcloud has made a conscious decision to put the security of their clients, customers, and others tas job number one. It gives customers more confidence when choosing Nextcloud, and it gives them a leg up on competitors. And when customers start to dig into security, they'll see that Nextcloud can truly back up what they say.

> “We obviously can't hire enough engineers to protect against every possible vulnerability, but we can use our bug bounty program to add on-demand expertise where we need it and continuous coverage nearly everywhere else.”
>
> **FRANK KARLITSCHEK**
> **NEXTCLOUD FOUNDER AND MANAGING DIRECTOR**

MORE SECURITY BANG FOR THEIR EURO

Nextcloud chose HackerOne Bounty to get the most for their security budget while also vastly expanding their security efforts. Their security team embraced the bug bounty program from the beginning as a way to add more resources, more skills, and more experience to their security team without adding more people.

"We wanted to put our money where our mouth is and demonstrate our commitment to security to our customers, partners and users," added Jos Poortvliet, Nextcloud co-founder and head of marketing. "Our security team was also pushing for this, as they knew the wealth of security knowledge available on the HackerOne platform and wished to get access to that. After all, no company can ever dream to employ all the smartest people on the planet, right?"

Security is also an area where Nextcloud chooses to invest, since it's the essence of their message. Nextcloud had always conducted third-party reviews and other typical security measures, but, as Poortlvliet put it, "the quality wasn't always convincing." So they launched bug bounty program to enhance and augment what they were already doing.

> **Security isn't a feature for us, it is a strategy**," said Karlitschek. "Employees are trained, we regularly scan and audit code, everything is double-checked, we work very transparently, and of course we solicit external reviews through HackerOne."

Nextcloud

SECURITY DOESN'T HAVE TO BE SLOW

Nextcloud is a model for how to build a bug bounty triage and response process. Their average response time—the time between a new report arriving and the reporting hacker receiving a human response—is less than one hour! That's their average.

How do they do it, even with a security team of just a few people?

"Good people, that is key in engineering in general," Poortvliet said. "And, of course, we take this extremely serious. We might not be a 1,000-person company but we have expertise that challenges companies many times our size and this is one way it shows."

BOUNTIES AS A GDPR COMPLIANCE TOOL

As a vendor of self-hosted cloud technology within the European Union with customers who often store privacy-sensitive data, Nextcloud was quick to put GDPR compliance into their security plans. They view security as a component of GDPR compliance, and that informs much of their approach to security, which includes putting hacker-powered security to work for their GDPR compliance efforts.

"GDPR demands that you can demonstrate you take the security of your users' data seriously," said Poortvliet. "While there isn't a single thing that proves that, I'd say a well managed security bug bounty program goes a long way to help us show how seriously we take privacy."

Poortvliet sees bug bounty programs as more than just proof of a commitment to security, he sees it as an investment to protect against potential GDPR infractions.

"I see lawsuits coming that will be lost but could have been won with a HackerOne program, both for practical and legal reasons," predicts Poortvliet. "Practical, because it would possibly have exposed issues in your infrastructure. And legal, because it helps you make the case that you did all you could."

SHARING SECURITY SECRETS

Nextcloud is obviously putting their money and effort behind their security efforts. It defines their approach and differentiates their products. It's also given them a leg up on most other companies.

But when asked how they would counsel companies considering a bug bounty program, they didn't claim it was a company secret or try to hide behind the veil of competitive intelligence. Instead, Nextcloud takes a decidedly altruistic approach and offered up three tips:

01

Make sure your security team is VERY much aware when the bounty program will begin and give them time to prepare. It is probably motivational for them to know that the work will receive some real scrutiny.

HackerOne can supplement your internal teams as your bounty program kicks off by either managing your entire program or just managing incoming reports. Learn more.

02

Be ready to handle the initial flood of bug reports. Having a triage plan in place, or using a service like HackerOne, can help you better manage reports and appropriately funnel them to the appropriate teams.

Check out HackerOne's Bug Bounty Field Manual, which offers expert guidance on launching and running a successful bug bounty program. Download the manual.

03

Your defined program scope is usually taken as just a suggestion, even though it's not. Out of scope properties will get scrutiny, but view it as a positive benefit: you're getting reports from friendly hackers, not criminals or the authorities. Don't yell, just thank them and accept that you now have a more secure infrastructure than before, even if that was never part of your plan.

HackerOne lets you start with a private bounty program, where you control who's invited to participate and can better influence where they focus. As you gain more experience, you can easily transition to a public bounty program that's open to all hackers.

"There is a lot of education left to do, both to producers and customers of security-critical code," said Poortvliet. "We hope bug bounty programs becomes an industry-standard, for the sake of security and stability of the entire industry."

Because, when we all work together on security, #TogetherWeHitHarder!

About HackerOne

HackerOne is the #1 hacker-powered security platform, helping organizations receive and resolve critical vulnerabilities before they can be exploited.