bugcrowd

CLOUDINARY TURNS TO CROWDSOURCED SECURITY WITH BUGCROWD

THE CHALLENGE:

Staying Competitive in a Security-Driven Age

89% of organizations have prioritized a digital-first strategy this year, with 62% saying the ability to deliver excellent customer experience will dictate the success of this initiative. So it's no surprise that securing the entire customer journey is a top priority for the world's top companies. Cloudinary, a leading provider of media management solutions supporting many of the world's biggest brands, is one such company.

With thousands of users and billions of assets relying on its platform, ensuring the highest levels of data security and protection is central to Cloudinary's work. Since its inception it has taken steps to ensure that user trust is earned and maintained year over year through code reviews, developer training, and continuous and dynamic application security best practices. Yet, even with periodic penetration testing, and continual use of CVE scanners, Cloudinary wasn't seeing the volume of critical, actionable vulnerabilities they expected from their testing investments.

"We were using various forms of application security tests, but still saw an area for improvement," says Netanel Fisher, CISO at Cloudinary.

Wanting to double down on data security audits and protections, Cloudinary sought a scalable solution that would enhance their existing security stack.

Cloudinary

Industry: Technology
Bugcrowd Product: Managed Bug Bounty

SUMMARY

Challenge — Enhance cyber posture in a rapidly evolving digital era.

Solution — Cloudinary partnered with Bugcrowd to decrease vulnerabilities and increase security posture.

Outcomes —

- Improved application security by remediating all valid submissions with high to critical severity
- Minimized risk through 500+ vulnerability submissions from nearly 360 researchers
- Increased customer loyalty

THE SOLUTION:

Harnessing the Full Business Value of Crowdsourced Security

With a firm commitment to ensuring the utmost data protections, Cloudinary decided to partner with Bugcrowd to design and launch their first crowdsourced security program. After identifying the needs of the organization and the scope of the program, the two teams determined a bug bounty program was the ideal choice.

Leveraging a community of white hat hackers and working with Bugcrowd to outline the program details like testing scope, timeline, crowd skills, and reward ranges, Cloudinary was able to deploy its program for immediate results.

The impact the researcher community had to the bug bounty program was the “single largest enhancement to our overall vulnerability management processes,” as stated by Fisher.

“Scanners are limited to their technical capabilities, and penetration tests will always represent a ‘snapshot in time’ status of your systems and applications security posture,” says Fisher. With the bug bounty program, Cloudinary benefits from countless uniquely skilled researchers that together, provide 24/7, 365-day testing coverage.

Since its initial launch in 2018, Cloudinary has made several adjustments to the program description and scope to ensure alignment with changing business requirements and priorities. Although it is important to define a tight scope, it also proved beneficial to later enable researchers to submit out-of-scope submissions.

By expanding the purview of the initial program, Cloudinary has seen a larger number of critical vulnerabilities against assets that they didn’t originally realize should be targeted. In fact, as Fisher explained, “almost half of the rewards that were provided were for out-of-scope submissions.” With Bugcrowd’s triage and validation services, volume is now not a concern, as Cloudinary only receives valid, actionable submissions.

> “We were using various forms of application security tests, but still saw an area for improvement.
>
> “With Bugcrowd’s help, we were able to move quickly in an ever-threatening environment.”

Netanel Fisher
CISO, Cloudinary

THE OUTCOMES:

A Safer Experience for Customers

Cloudinary's bug bounty program is a great example of how an army of researchers can help to stay ahead of adversaries. As Fisher stated, "Our primary goal in executing this program was to find vulnerabilities so we can mitigate them immediately, before they'll be exploited."

Today, the outcomes Cloudinary has seen from its bug bounty program are substantial. They have:

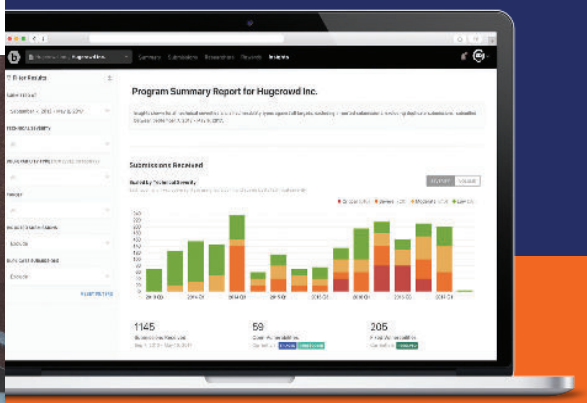
- Ensured continuous, comprehensive testing coverage through 500+ submissions from nearly 360 researchers.
- Quickly prioritized remediation for all valid submissions which were high or critical severity.
- Increased customer loyalty by demonstrating continued commitment to application security in a way that is easily understood.

For application security programs to be successful, multiple stakeholders must see tangible benefits to people, process, or technology. Bugcrowd offers a fully managed service that helps affect change across each of these vectors, helping you do more with less, faster. "With Bugcrowd's help, we were able to move quickly in an ever-threatening environment" comments Fisher.

Bugcrowd's expertise has helped ensure the successful deployment and continual evolution of Cloudinary's bug bounty program. "By partnering with Bugcrowd, we are now able to address and resolve vulnerabilities of our platform in a quicker and more agile manner, while also having the support and partnership from Bugcrowd's team to help us along the way," confirms Fisher.

> "Our primary goal in executing this program was to find vulnerabilities so we can mitigate them immediately, before they'll be exploited.
>
> "By partnering with Bugcrowd, we are now able to address and resolve vulnerabilities of our platform in a quicker and more agile manner, while also having the support and partnership from Bugcrowd's team to help us along the way."

Netanel Fisher
CISO, Cloudinary



Learn why hundreds of companies have turned to Bugcrowd:

www.bugcrowd.com/get-started