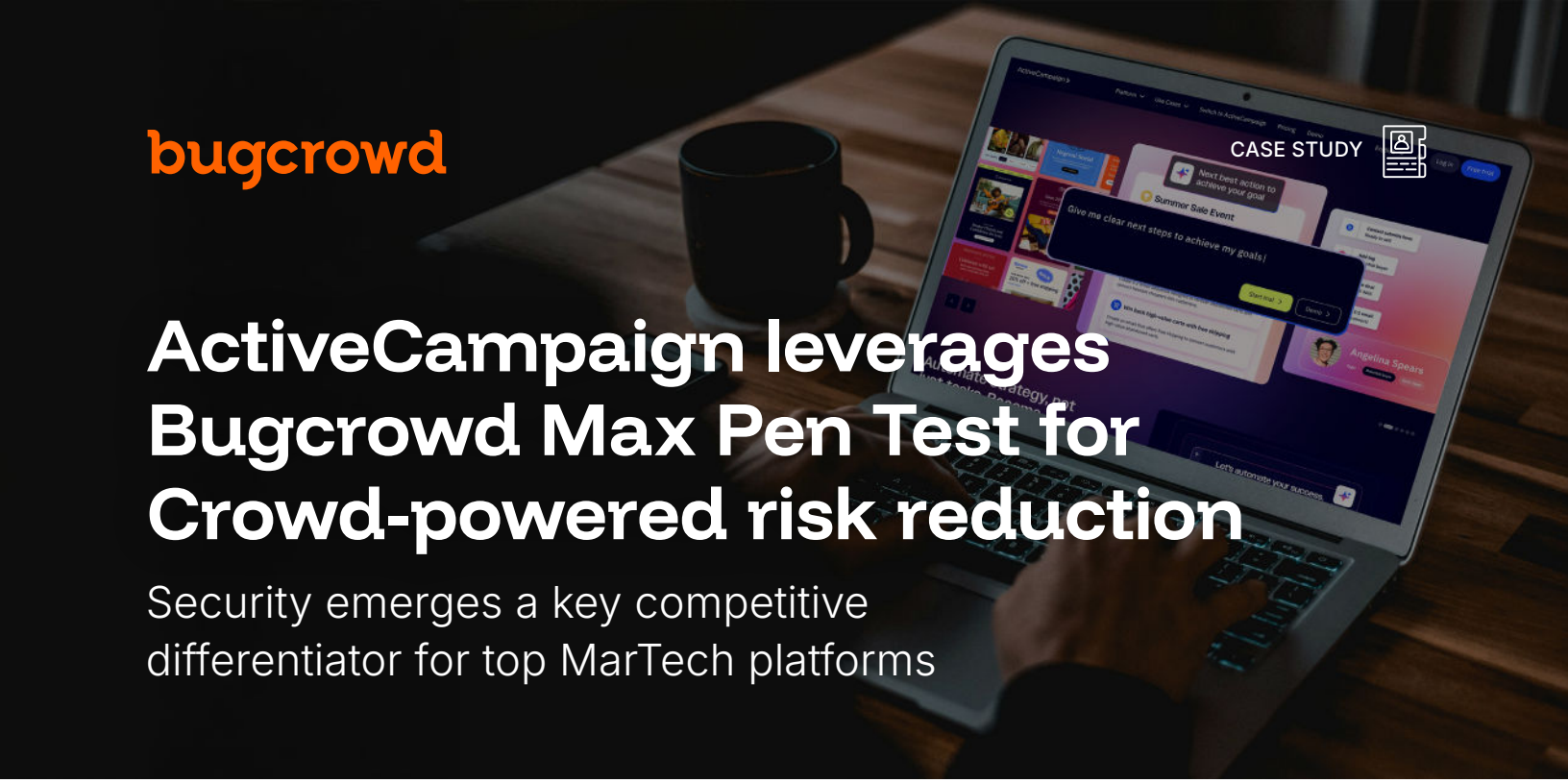
bugcrowd

CASE STUDY



ActiveCampaign leverages Bugcrowd Max Pen Test for Crowd-powered risk reduction

Security emerges a key competitive differentiator for top MarTech platforms

ActiveCampaign

Industry:
Tech

Founding date:
2003

Number of employees:
1,000-5,000

Headquarters:
Chicago, Illinois, USA

Website:
activecampaign.com

The situation

ActiveCampaign is a SaaS marketing technology (MarTech) platform that helps businesses meaningfully connect with customers. With solutions designed to support the full engagement lifecycle, ActiveCampaign enables sales, marketing, and customer success teams to create personalized workflows and experiences that drive customer adoption and growth. But to help organizations gain customer trust, ActiveCampaign knows they must first do the same. That's why they've chosen Bugcrowd to aid in their quest to build consumer confidence with the most trusted MarTech platform in-market today.

ActiveCampaign understands the value of keeping customer data safe, and the role of security in building reliable products and services. With the addition of former hacker turned application security engineer turned CISO, Chaim Mazal, **they have also adopted a newfound commitment to showing customers that the security of their personal information is paramount** to ActiveCampaign's vision for success.

Key takeaways

Detection of 50+ valid vulnerabilities within the testing window

Leveraged multiple points of view outside the internal team

Achieved true risk reduction beyond compliance

The situation

Today, ActiveCampaign utilizes a variety of security solutions that together weave a strong story of compliance, assurance, resilience, and true risk reduction. The recent completion of their SOC 2 Type 2 captures many of these initiatives, but also includes static code analysis, open source code analysis, architecture reviews, user behavior analytics, threat modeling, and of course, crowdsourced pen testing through the Bugcrowd Platform.

The challenge

While MarTech platforms specialize in the collection, transformation, and/or application of critical consumer data, some organizations may be surprised to learn that adoption of data aggregators like these can actually help meet data privacy and security regulations like GDPR. Having a single view of where your customer data is, who has access, how it will be used, and how easily it can be erased, are the core tenants of secure data storage, and all direct benefits of using marketing automation software. When looking to purchase such technology, this argument might help convince your CISO, but expect one important question in return:

> **"Are you confident that this platform will keep our data safe?"**

ActiveCampaign was conducting regular penetration tests, to set their annual baseline of known and accepted risk. While they utilized a well-known and respected pen test firm to perform these assessments, the team was also interested in **pressure testing results,** always striving to reduce risk as much as possible.

The Bugcrowd solution

In 2018, ActiveCampaign met Bugcrowd for the first time. It was not the first engagement for their new CISO, Chaim Mazal, who had run multiple successful Bugcrowd programs with previous organizations. Having seen the value of crowdsourced security first-hand, Chaim was intent on incorporating this approach in ActiveCampaign's security strategy.

With the prospect of uncovering more high priority vulnerabilities in less time, while still retaining the methodology-driven reporting artefacts required by their compliance initiatives, ActiveCampaign determined that Bugcrowd's Max Pen Test solution, **a penetration testing as a service offering, was the right fit for their security need, timeline, and budget.**

When evaluating vendors, ActiveCampaign suggests looking for:

- ✓ Adherence to compliance and regulatory standards like SOC 2, ISO 27001, PCI, GDPR, and HIPAA, which include active security testing initiatives
- ✓ A robust set of user access controls for granular permissions around access to customer data, as well as multi-factor authentication (MFA) and single-sign on (SSO)
- ✓ A comprehensive suite of secure integrations built into the platform to enable end user data and credential management.

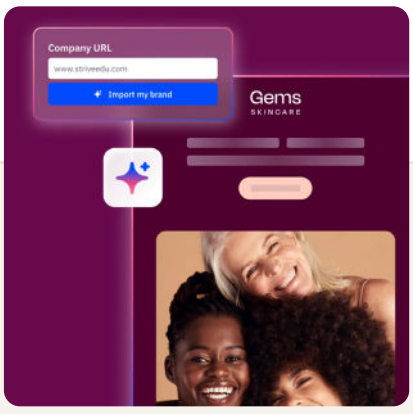
The outcome

ActiveCampaign saw immediate results from their program, smashing the previous baseline for risk. Since this assessment, ActiveCampaign has noted several points of value, which have also translated into their commitment to partnering with Bugcrowd for any number of additional crowdsourced testing initiatives.

ActiveCampaign has experienced value from their program, including:

- **Expertise:** Ability to leverage multiple points-of-view outside that of their internal team
- **Support:** Bugcrowd's extensive support team provides the flexibility and guidance needed to help ActiveCampaign meet security testing initiatives their way
- **Vulnerabilities:** Detection of 50+ valid vulnerabilities within the testing window
- **Extensibility:** Bugcrowd's extensible platform enables ActiveCampaign to add additional crowdsourced security solutions to meet unique security needs
- **Company-wide security awareness:** Security testing and secure coding best practices are now more readily infused throughout the development process.

"It's impossible to be #1 if you're not the #1 most trusted. Not only did we want a great report, we wanted a great partner to enable trust," Mazal said.

> I could have called anyone to get a clean bill of health, but that's not our business. We called Bugcrowd because we wanted the most in-depth vetting of our security posture. It's beyond compliance—it's about true risk reduction.

Chaim Mazal, Head of Global Information Security, Active Campaign