



ACTIVECAMPAIGN LEVERAGES BUGCROWD NEXT GEN PEN TEST FOR CROWD-POWERED RISK REDUCTION

Security emerges a key competitive differentiator for top MarTech platforms

ActiveCampaign's Mission

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.

The Question Marketing Technology Platforms Must Answer

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?"

Security at ActiveCampaign

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 Security Researcher turned App Sec 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.

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.

ActiveCampaign >

Launched: September 2019

Type: Next Gen Pen Test

“Know us. Like us. Trust us. Without the third piece, we have nothing. It's impossible to be #1 if you're not the #1 most trusted.”

Chaim Mazal
Head of Global Information Security



Bugcrowd for ActiveCampaign

In 2018, ActiveCampaign met Bugcrowd for the first time. Though it wouldn't be a first for their new CISO, Chaim Mazal, who had run multiple successful Bugcrowd Bug Bounty programs with previous organizations. Having seen the value of crowdsourced security first-hand, Chaim was intent on incorporating this approach in ActiveCampaign's 2019 security strategy.


By this point, 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.

As it happens, around the same time in late 2018, Bugcrowd launched a new, crowd-powered pen test solution. 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 Next Gen Pen Test solution was the right fit for their security need, timeline, and budget.

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.

The Value of Bugcrowd at ActiveCampaign:

- **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.




“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.”

Not only did we want a great report, we wanted a great partner.”

Chaim Mazal
Head of Global Information Security

A Note to Security Researchers

ActiveCampaign prides itself on an extremely intuitive and easy-to-use platform. However, with great simplicity, comes great complexity (under the hood). Security Researchers on ActiveCampaign's Bugcrowd programs are thus encouraged to think outside the box when diving into the multitude of unique user workflows.



Overcoming Security Challenges, Together

Back to the CISO's question.. "Will this platform keep our data safe?" It's a serious question for organizations to consider when shopping for email, marketing, or sales automation software. If an attacker exploits a vulnerability in a MarTech platform, customer data could be at risk. In the case of malware attacks — one of the most frequent types of cyber attacks for this segment — customer data becomes more like a list of targets, with the platform serving as a direct line for malware distribution.

In order to avoid potentially crippling legal and reputational ramifications, organizations looking to purchase MarTech solutions should consider implementing more rigorous vendor security assessments before purchase. This should include a requirement for continuous security testing, as traditional point-in-time assessments may miss much — only providing a slice of your true risk profile.

As for MarTech vendors looking to implement their own controls, forget the archaic tradeoff between rapid or secure development. While the rise of vendor security assessments has revealed that you can't win on features and functionality alone, many of the cutting-edge capabilities offered by MarTech vendors today, were built in development frameworks and environments selected specifically for, rather than despite, their focus on security. As is the case with ActiveCampaign, security needn't be a cost center to the business, or inhibitor to development. If executed in balance, it can be an investment, and facilitator of growth. And as customers of crowdsourced testing solutions know, attackers are always on the hunt for a way in — shouldn't you be doing the same?

A Note to Customers Shopping for MarTech Platforms

Marketing technology platforms have evolved to help organizations capture and leverage a wealth of new data points about their customers. With this increased reach and accessibility comes a serious responsibility to secure that data. To that end, ActiveCampaign has 3 suggestions of what to look for when evaluating MarTech vendors:



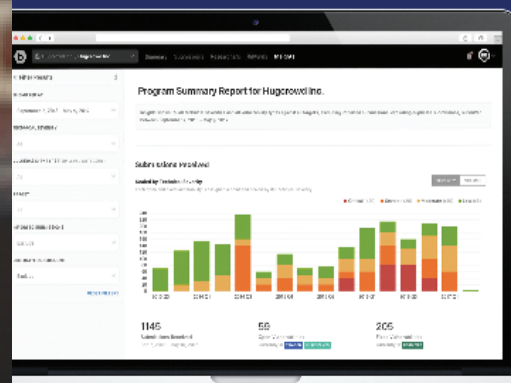
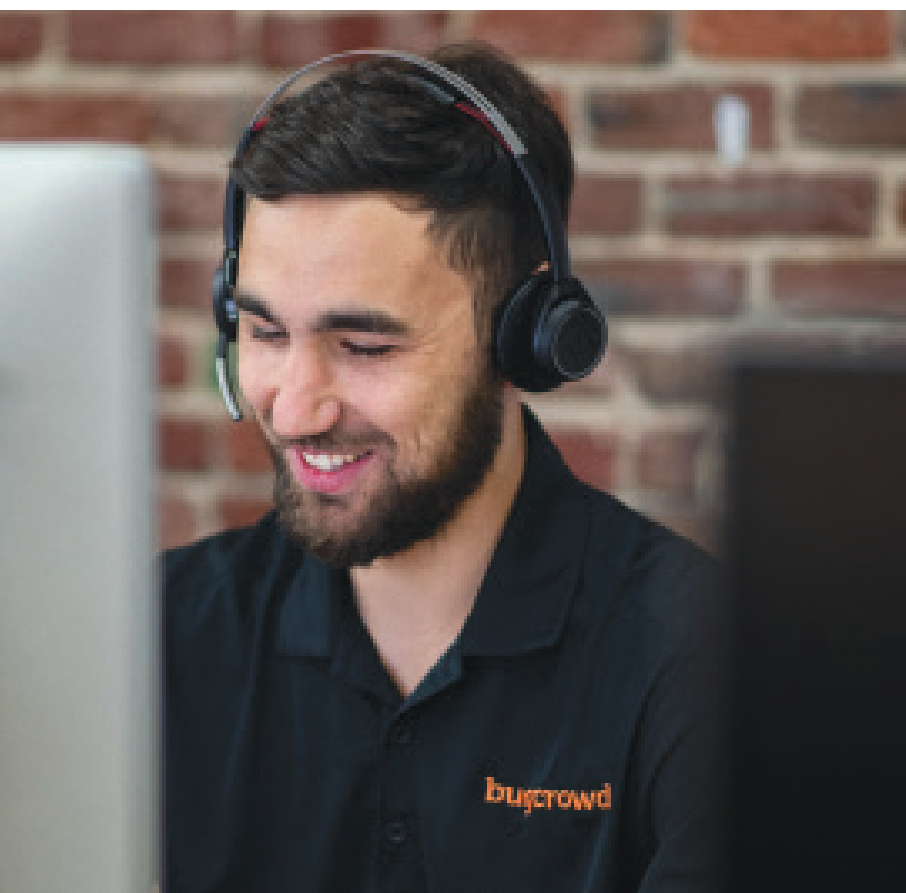
Adherence to compliance and regulatory standards like SOC 2, ISO 27001, PCI, GDPR, and HIPAA, which include active security testing initiatives.



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.



Learn why hundreds of companies have turned to Bugcrowd:

www.bugcrowd.com/get-started