SMRT Systems Help Center

🔍 Search

Articles in this section ⌄
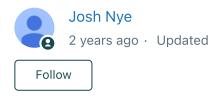
SMRT Data Security

Josh Nye
2 years ago · Updated

Follow

SMRT Realizes that trusting another company with your customer data can feel risky. But we assure you that not letting us protect your data is far more dangerous.

We use Amazon Web Services to host all the data. If you're interested you can read about it here: https://aws.amazon.com/security/ but the summary is that they have data security covered! Fortune 500 companies use AWS for data hosting.

We also use a service call Cloudflare that monitors incoming traffic and alerts us if there's strange activity, like someone from Russia trying to log onto any of our customer's sites, and also protects against DDoS attacks, we call it our badass firewall.

The third service we use for data security is called Threat Stack. Threat Stack was created by "White Hat Hackers" (good guys). Threat Stack essentially lives on our servers and looks for activity that shouldn't be happening. Because we never need to actually work on our servers that means that any activity is flagged by Threat Stack. If a "hacker" ever got into our servers our entire development team would receive an alarm and phone call alerting them that there'd be a breach. If that were to happen we could simply drop those servers, eliminating the ha access, and spin up another cloud without any data loss under an hour. That's the bea

Help

cloud software, we have clouds running simultaneously and can simply drop one and reboot it without any data loss.

Was this article helpful?

Yes	No

1 out of 1 found this helpful

Return to top ⌃

Recently viewed articles

Sales Tax Report

Rewards Program Setup

Registering a Twilio Phone Number for 10DLC A2P

Linking / Merging Duplicate Accounts

KPI Data Fields

Related articles

SMRT External Connections

Employee Levels

Email Blasts Through Mailchimp

Admin Panel Reports

Comments

0 comments

Be the first to write a comment.

SMRT Systems Help Center