

Answering IT & Security Questions

At larger companies, such as the Fortune 500, there are Security teams that audit new technologies being used inside the company.

If security engineers are interested in your project, some talking points that can help answer their questions include:

- Because Gatsby compiles your site to flat files, rather than having running app servers and databases users are targeting, it reduces the attack surface of the site to outsiders.
- Gatsby adds a layer of indirection which obscures your CMS – so even if your CMS *is* vulnerable, bad actors have no idea where to find it. This is in contrast to systems where bad actors can easily locate the admin dashboard at, e.g., `/wp-admin` and attempt to hack in.
- Gatsby lets you serve your site from a global CDN, likely whatever CDN your company is using (e.g. Akamai, Cloudflare, Fastly...), which effectively eliminates the risk of DDoS attacks.

It's helpful to emphasize to security personnel that these benefits were a factor in why Gatsby was selected for the project. You chose Gatsby, in part, because it is *more* secure.

Read about security in Gatsby: <https://www.gatsbyjs.com/blog/2019-04-06-security-for-modern-web-frameworks/>

Note: do you have additional ideas on how to answer IT and security questions for Gatsby projects? We welcome contributions to the Gatsby docs. Find out how to contribute.