Secure Hosting with CloudLinux OS

The main reason of hacking is so easy on shared hosting servers is because Linux was never meant to be used by a large number of not vetted users. It is too easy for a hacker to obtain an account on your server (by using a stolen credit card and signing up or by abusing some outdated script one of your customers has not updated for years). After that, a hacker has inside access to the server and can begin poking around, finding low hanging fruit and hacking your server.

CloudLinux stops that. With our CageFS and SecureLinks technologies, users are virtualized to their own file systems, preventing any individual user from seeing any other users on the server. All tenants on the server are isolated from each other so if one goes down everyone else is still safe and stable.

CageFS Technology

CageFS is a virtualized per-user file system that uniquely encapsulates each customer, preventing users from seeing each other and viewing sensitive information. Additionally, CageFS prevents a large number of attacks, including most of the privilege escalation and information disclosure attacks. This innovation is completely transparent to your customers—without any need for them to change their scripts.

CageFS Benefits:

- Only safe binaries are available to user;
- User will not see any other users, and would have no way to detect presence of other users & their user names on the server;
- User will not be able to see server configuration files, such as Apache config files;
- User's will have limited view of /proc file system, and will not be able to see other' user’s processes.

At the same time, user's environment will be fully functional, and user should not feel in any way restricted. No adjustments to user's scripts are needed.