CyberHive Secure Cloud Storage Product Datasheet

A New Online Storage Solution, to ensure that even when you are on the move, you can continually access your data securely.

With the development of technology, people and businesses alike have created a much higher demand to have access to work files and data from anywhere on the planet. There are now multiple forms of online storage that an individual or business can choose to access their data from anywhere in the world. However, these standard solutions eliminate the security aspects required for a lot of important data, just to give the customer ease of use. At CyberHive, we believe that you should not have to have either a secure cloud solution or an easy to use accessible anywhere cloud solution, so we have created a Secure Online Cloud solution, which matches global accessibility, with world class security, to deliver a truly secure access point to your data.

To build the most secure online storage solution, CyberHive has combined our Trusted Cloud solution, with the world's leading cloud storage software, NextCloud. This brings a secure, effective and well-priced solution to the community.

Key features of Secure Cloud Storage

- Your data is accessible wherever you are – in the office, at home or on the move
- Use multiple devices to access your data including laptops, smartphones and web browsers.
- Take control of users and groups – NextCloud offers the ability to define new users and groups and define who can access your company data through a simple web interface.
- World class security:
  - All data is encrypted on disk
  - Secure communications to and from the cloud
  - Protected by Trusted Cloud cutting edge security
  - All data is stored in our secure tier-3 datacenter in central London

What is Trusted Cloud?

Trusted Cloud is a cutting-edge cyber security solution developed by CyberHive with researchers from The University of Oxford. It protects your critical data by ensuring that no unauthorised code can run undetected on our critical server infrastructure.

The technology employed is a cutting edge approach called distributed hardware-backed whitelisting. Every few seconds, each server in our estate will generate an audit list of all programmes and configuration running on the server. This list is digitally signed using a cryptographically secure hardware module. This audit data is then sent to one or more verification servers where it will be cross-checked against a previously generated and signed whitelist. Even a single line of unauthorised code will be instantly detected and flagged, allowing CyberHive's security team to stop an attack in its tracks before any damage can be inflicted or data lost.

Wessex House, Oxford Road, Newbury, Berkshire, RG14 1PA
01635 881 880
www.cyberhive.com