When You Consider Kiteworks vs. Nextcloud

Packaged Security and Compliance by Default vs. a Sysadmin's Starter Kit

	With Kiteworks, you get:	*With Nextcloud, you get:*
	**Unmatched Software Security Hardening.** Keeps attackers and employees out of the Kiteworks hardened virtual appliance with a built-in network firewall, WAF, intrusion detection, and internal zero-trust principles. It encapsulates, protects, and updates all components: the OS, application, file system, web servers, and databases. An ongoing bounty program and regular pen testing minimize vulnerabilities, and the entire appliance updates like a smartphone.	**Un-hardened Software Installation.** As a customer, you are on your own to install, configure, and maintain any server hardening. Intrusion detection and penetration testing are your projects at your expense. Server admins have access to the OS, database, and files. When performing updates, admins must manually update and test the application, PHP, DBMS, web server, and OS.
	**No Uninvited Access to Files.** Kiteworks file- plus disk-level double encryption at rest helps protect files even if the OS is compromised, and can't be read by administrators or Kiteworks employees, even when Kiteworks-hosted. Strong encryption is used in transit.	**Intrusions Are Your Problem.** See warning: "The encryption app does not protect your data if your Nextcloud server is compromised, and it does not prevent Nextcloud administrators from reading user's files".
	**Centralized, Normalized Audit Log Drives Compliance & SOC.** The unified Kiteworks audit log continuously feeds a variety of report interfaces appropriate for end users, various admin roles, and compliance teams, as well as one or more syslogs and the Splunk Universal Forwarder.	**Logs Are Another Project.** Audit logs are disabled by default, and don't even have a user interface—admins must access them via the OS or API and provide their own tools to process the JSON format.
	**Really, Really Big Secure File Transfers by Default.** Reliably and securely encrypt, send, share, receive, scan for viruses, view, and save data-intensive, imaging, and CAD files up to 16 terabytes in size, right out of the box. When networks fail, transfers restart where they left off.	**Administrative Tweaking for Large Files.** Increasing the 512 MB default file size limit requires technical OS and web server configurations, increasing the likelihood that users will revert to insecure forms of communication.
	**On-premises, FedRAMP, and Other Secure Hosting Options.** Undergoes yearly product and process audits and continuous monitoring by a certified third-party assessor for FedRAMP hosting. Standard hosting also available.	**Cloud Services Partners to Vet.** It's up to you to ensure the security posture and SOC processes of Nextcloud hosting partners meet your security and compliance needs.

Kiteworks