AvePoint®

AvePoint Compliance Guardian
FAQs for Business Users

AvePoint Compliance Guardian

A comprehensive risk management solution ensuring information is available and accessible to the people who should have it and protected from the people who should not.

Questions	Answers
What data resources does Compliance Guardian support scanning?	In Compliance Guardian, Compliance Scanner supports scanning SharePoint 2013, SharePoint 2010, MOSS 2007, SharePoint Online, File Systems, and Web. Classification Scanner supports scanning SharePoint 2013, SharePoint 2010, MOSS 2007, SharePoint Online, File Systems, and Yammer. **Note:** Compliance Guardian Service Pack 2 does not support scanning information on the Yammer server directly. It has a special solution which can be deployed on a SharePoint farm for adding a Yammer Connector Web Part on a SharePoint site. The Yammer Connector Web Part can be used to sync the information from the Yammer server to the SharePoint server. Via this Web Part, the Compliance Guardian Classification Scanner can monitor all messages posted to Yammer and block the sensitive information based on the Test Suite.
What file types does Compliance Guardian support scanning?	Please refer to the AvePoint Compliance Guardian Installation and Administration User Guide, Appendix C: Supported File Types in Compliance Guardian.
What kind of actions can Compliance Guardian take on a given item?	For SharePoint Server, Compliance Guardian can take the following actions: Quarantine, Redaction, Encryption, Move, Change Permission, Delete to Recycle Bin, Permanently Delete, Lock (for Newsfeed only) and Block (for the Post though Yammer Web Part Only). For File Systems, Compliance Guardian can take the following actions: Quarantine, Redaction, Encryption, and Move.
How is it determined what action will be taken on the content, such as encryption?	Compliance Guardian can take actions on documents based on the classification given to the document during a scan against defined business rules (a Test Suite). An Action Policy in Compliance Guardian defines what you would like to do when content is found that matches criteria that you have defined, including the ability to change the document permissions, quarantine/move the document, redact information, and encryption. This can happen to data that resides in File Systems as well as within SharePoint. If the user wants to open the encrypted document, s/he needs to log into the Compliance Guardian Incident Manager, and then download the encrypted file locally or decrypt the file in the original location. The encrypted document cannot be opened from SharePoint or the File System server directly.
What service is responsible for updating permissions? Can we define custom permissions?	The Classification Scanner performs the actions for updating permissions. You can create a SharePoint group with custom permissions first and then create a scan job to change document permissions which only allow this SP group to manage the document.
Can we send documents to specific document libraries depending on their security classification?	Yes, documents can be moved to a specific document library possessing unique permissions. However, documents will always be more secure with item-level permissions that don't change based on location of the document, but instead are determined and assigned based on the makeup of the content itself. If you are depending on library-level permissions, a sensitive document inadvertently put into a lower-permissioned library, for example, would inherit that library's lower permissions, giving inappropriate access to users.
Does Compliance Guardian offer any auditing capabilities?	Yes. Compliance Guardian has an Auditor feature which can be used to audit and track information such as who logged into the system, who created a plan or triggered a job, who checked the scan result, and when reports were downloaded. All users' actions can be monitored and recorded by this auditing feature.