

The Top 10 Questions

You Should Ask Vendors When Evaluating an In-House eDiscovery Solution.

Will the solution:	Your ideal solution:
<p>Automates a wide range of the eDiscovery process as defined by the EDRM model from Information Management through preparing load file formats for litigation review tools?</p>	<p>Automates more of the eDiscovery lifecycle within a single solution compared to other vendors. This translates to faster time to production, reduced administration and maintenance of separate disjoint tools, reduced errors resulting from manual integration work and hand-offs, and more robust and complete audit logging.</p>
<p>Provide an open integration platform to support various email systems, storage systems, archiving systems, and content / document management systems without the need to install software on the target system?</p>	<p>Should support a wide variety of technologies and platforms to identify potentially responsive data for preservation and collection including:</p> <ul style="list-style-type: none"> • File systems, including <ul style="list-style-type: none"> • CIFS • NFS • Netware • Email systems and archives, including <ul style="list-style-type: none"> • Microsoft Exchange • Lotus Notes • Symantec Enterprise Vault • Content management systems, including <ul style="list-style-type: none"> • Microsoft SharePoint • EMC Documentum • Storage systems, including <ul style="list-style-type: none"> • NetApp Snaplock • EMC Celerra • EMC Centera • IBM DR550 • Hitachi HCAP
<p>Execute without impacting employee productivity?</p>	<p>Should provide flexible job scheduling to allow any processing task to occur after hours when employees are not impacted. The ability to perform litigation holds to preserve responsive electronically stored information for on-going legal matters should preserve the necessary data content and metadata without disrupting the production environments of knowledge workers.</p>
<p>Implement litigation hold policies without disrupting the normal course of business?</p>	<p>Your litigation hold management system should work in conjunction with existing corporate records management policies and HSM (Hierarchical Storage Management) systems so that legal requests for managing litigation holds and producing responsive electronically stored information do not disrupt existing on-going IT data management functions such as data backup, migration, and expiration of files and content.</p>

<p>Create a data topology map identifying electronically stored information by system, custodian, access time, size, and content type?</p>	<p>Profile your electronically stored information in order to perform pre-discovery so you can “know your hand” for early case assessment, be better prepared for Rule 26(f) conferences and target responsive data in order to “right size” collection and preservation.</p>
<p>Be able to output electronically stored information to legal, HR or audit teams prior to the completion of the collection process?</p>	<p>Provide the ability to perform rolling productions while collection and preservation are still in process.</p> <p>To accurately perform rolling productions, the system should provide comprehensive production policy support, including intelligent management of containers such as PST, NSF and ZIP files, advanced de-duplication capabilities, and automatic creation of load files supporting a variety of formats including Concordance, Summation, Ringtail, and the EDRM XML standard.</p>
<p>Interact with electronically stored information on active systems without changing metadata?</p>	<p>Should only require backup administrator rights on the network. Backup operators can read, copy and save (“backup”) files without changing file metadata regardless of the permissions that protect those files.</p>
<p>Execute forensically-sound collection policies while providing defensible, comprehensive audit logs?</p>	<p>Authenticates collection and preservation by preserving information such as access control lists (ACLs) and security identifiers (SIDs). This information identifies the file owner as tracked by the network file system. This is extremely beneficial when collecting from shared network directories.</p> <p>Collection audit logging should include the status of collections, object information and exceptions/errors. For preservation reporting, the product should create a hash value of objects before and after collection, proving authenticity. Audit history should be able to trace through from where data originally resided, what filter rules and queries were applied to cull it, any copies made and actions performed, and how that data was ultimately delivered.</p>
<p>Provide rich metadata tagging and classification capabilities?</p>	<p>Should provide advanced tagging and classification features such as the ability to create rules and filters based on Boolean expressions, system attributes, and custom content. Should be able to tag information at the system level, object level, and also be able to search and identify terms, expressions, and natural language concepts within the content of file objects. Basic linguistic concepts should be supported for more relevant data tagging and extraction such as names, cities, dates, addresses, as well as supporting more advanced concepts such as financial references, medical terms, and personal information like Social Security and credit card values.</p>
<p>Be easy to deploy and maintain, accelerating the speed from installation to productivity?</p>	<p>Should be deployable as a self-contained, out-of-the-box appliance eliminating the need to purchase and install hardware, software and storage necessary to support your eDiscovery application.</p>

If vendors cannot demonstrate their ability to perform each of these critical functions, there are better in-house reactive and proactive eDiscovery solution alternatives.