VERITAS

eDiscovery for SaaS Application Data

Veritas Alta SaaS Protection for eDiscovery and compliance.

Electronic discovery (eDiscovery) has become a critical component of compliance and governance solutions. The term comes from the discovery phase of litigation or governmental requests where the information being sought is stored in a digital or electronic format. Discovery usually involves reviewing the data for privilege and relevance before turning it over to the requesting party.

It is obvious that a business needs discovery capabilities for its data, but sometimes data from software as a service (SaaS) applications such as Microsoft 365 or Salesforce is overlooked. This brief will explore how Veritas Alta™ SaaS Protection can help enterprises with discovery and compliance for their SaaS application data.

Obviously, SaaS application data only represents a portion of an organization's data, so discovery for this data should be viewed as a necessary part of a larger overall compliance and discovery process.

eDiscovery

eDiscovery differs from discovery of paper documents for two main reasons:The first reason is metadata, which is data about the data. Metadata includes information such as the type of data, its size, when it was initially created, when it was most recently modified, and more. In eDiscovery, one is required to turn over the metadata along with the data.

The second reason is that because it's often easier to alter an online document than its paper version, businesses need to be able to prove that their data has been stored immutably—in a form or method where it cannot be altered—and keep a record of any attempts to alter the data.

In most cases, a business must remain in compliance with any regulations that apply to the data, generally having to do with the minimum length of time they are required to retain the data.

Email and Chat Messages

In 2006, the US Supreme Court amended the US Federal Rules of Civil Procedure (FRCP) to address the definition of discovery of electronically-stored information. These amendments explicitly made email and chat messages subject to eDiscovery, not just traditional documents.

In order to avoid sanctions or fines, organizations need to be able to demonstrate that they are in compliance with any regulations with regard to preserving these messages, and that they are capable of applying a legal hold on them.

Terms

Here are the definitions of a number of terms related to eDiscovery:

- **Compliance:** Handling data in accordance with all applicable regulations. The regulations that apply to your business will depend on the geographic jurisdiction of your business, as well as on the type of business you are in. For example, financial data and medical records are each subject to different standards of regulatory compliance.
- **Governance:** The organization's overall approach to managing the entire organization, which includes handling management of data. Governance-related concerns about data include its completeness, accuracy, and whether or not it reaches the right people in a timely manner.
- **Legal Hold:** A process an organization uses to preserve all forms of information that are potentially relevant to pending or anticipated litigation.
- **Spoliation:** This is the intentional, reckless, or negligent withholding, hiding, altering, fabricating, or destruction of evidence relevant to a legal proceeding. Each organization involved in a legal proceeding is responsible for demonstrating the steps they have taken to prevent spoliation.

Stages of eDiscovery

To meet the requirements of legal proceedings, discovery processes follow the stages defined in the Electronic Discovery Reference Model (EDRM), summarized below. The first three stages are what your organization would need to manage. Stages 4 through 8 are managed by legal counsel.

1. **Identification:** This is the process of identifying documents and data that are potentially relevant to the specific inquiry. This starts with casting a wide net and then narrowing down the specific criteria. This could be any documents or messages that include certain words or phrases, documents shared, messages sent during a specific date range, or documents created by specific people or a specific group. Most often, you'll use a combination of criteria.
2. **Preservation:** This is the process of ensuring that you preserve all the relevant data from deletion or alteration. This is called placing a legal hold on the documents and data. Any and all data under a legal hold must not be deleted or altered while the hold is in place, even if that exceeds any previously-set retention period. Legal holds are commonly set with no end date specified, forcing a manual action to release the hold. In litigation, failure to preserve the relevant data can result in sanctions and fines.
3. **Collection:** This is the process of pulling the data together to prepare it for transfer to legal counsel, who will determine the relevance of the data. The scope of the data shared is determined during the Identification stage.
4. **Processing:** This is where the files and data are prepared for review. This often involves extracting text and metadata from the files. It may also involve converting files from their native format to something more difficult to alter, such as a PDF format.
5. **Review:** During this phase, legal counsel reviews the set of documents for privilege and for responsiveness to the discovery request(s). This typically includes identifying which documents are the most relevant.
6. **Analysis:** While the Review phase focuses on the files themselves, the Analysis phase focuses on the data in the files. It is important that any evidence within the data be viewed in context. To assist with that, legal counsel may create one or more structures in which to present the data. For example, counsel might separate documents into categories by specific topic, or counsel might create a timeline to help enhance the context for the documents.
7. **Production:** This is the process of turning the documents over to opposing counsel, based on previously agreed-upon specifications. For eDiscovery, this involves providing digital files or a Zip archive rather than boxes of paper documents.
8. **Presentation:** This is where the evidence gathered by the discovery process is displayed and explained to an audience. The focus is on clarity and ease of understanding, enabling non-professionals to follow the interpretation. Most often this involves presenting the analysis of the data, rather than the data itself as a whole.

Where SaaS Comes In

All information that an organization stores electronically is subject to discovery, regardless of where that data resides. This means that it is not enough to meet legal requirements to produce data stored on-premises. Any and all data stored in the cloud—including in SaaS application platforms—is subject to regulations related to discovery.

Information stored in SaaS applications that could be relevant to discovery requests includes, but is not limited to, shared documents (text files, Word documents, PDF files, PowerPoint presentations, Excel workbooks, etc.), information in customer relationship management (CRM) platforms, email messages, group chats, one-on-one chats, and meeting recordings.

Your organization's plan for eDiscovery and compliance needs to include data in your SaaS applications or you may be liable for sanctions and large fines.

How Veritas Alta SaaS Protection Helps

Veritas Alta SaaS Protection is our solution for protecting SaaS application data. This means that it provides backup, recovery, and archiving of data from your SaaS applications. There are many ways in which features built into Veritas Alta SaaS Protection provide eDiscovery and compliance capabilities:

- **Immutable Storage:** Veritas Alta SaaS Protection stores all backup data on immutable storage, that is, storage that does not allow alteration of the data and does not allow anyone—even administrators—to delete any of the data before the expiration of its set retention period.
- **Data Retention:** Customers can create custom retention policies. This will set the retention period (5 years, 10 years, etc.) for the backup data. These policies provide the flexibility to set different data retention periods for different types of data. This effectively provides automated compliance with data retention regulations.
- **Data Location Controls:** Organizations operating internationally may come across data sovereignty regulations. These regulations require that any data related to business conducted in a specific country or with customers residing in a specific country must be stored within the borders of that country. Not all countries have such regulations today, but over time more have adopted them. Veritas Alta SaaS Protection allows customers to set data location controls to determine where to store different backup data. This provides automated compliance with data sovereignty regulations.
- **Federated Search:** Veritas Alta SaaS Protection indexes all backup data it ingests and can perform full-text indexing of its content. This allows for blazingly-fast results when searching the backup data. You can run a single search across one or multiple SaaS applications, multiple locations, and multiple domains. This makes it easy to find specific data quickly.
- **Advanced Search Filters:** For eDiscovery, you only want to collect data relevant to the specific inquiry. The more data you provide, the longer it takes to review, which results in more time billed by the lawyers. If you provide too little data, however, you may be subject to fines or be accused of attempting to obstruct the proceedings. Your goal, therefore, is to provide all relevant data and only the relevant data. Veritas Alta SaaS Protection offers highly-configurable search filters for the inclusion and/or exclusion of data based on any combination of criteria you care to define. For example, you could search for any email messages that mention a specific term, sent or received by a specified group of users, between two specific dates. Using the right combination of filters allows you to get all the data you want, and only that data.
- **Ad Hoc Searches:** As you might imagine, defining the right search parameters for a particular discovery request can be a process of trial and error as you refine the filters you're using. Veritas Alta SaaS Protection allows you to perform multiple searches without actually collecting the data or placing it under legal hold, allowing you the time and freedom to refine your search parameters.
- **Cases:** Once you have determined that your particular search parameters give you the appropriate search results for the specific eDiscovery request, Veritas Alta SaaS Protection lets you save that search. You can simply save it as a repeatable search that you can easily perform again in the future. You also have the option of saving the search as a case. A case is a logical construct that allows you to treat all the items returned by your search as a single object or grouping.

- **Legal Hold:** Once you have defined a case, you can apply a legal hold on all items within the case in a single step. This makes applying the hold quite simple and allows you to apply it quickly, demonstrating that you have acted in good faith to preserve the data.
- **Exporting Data:** Veritas Alta SaaS Protection makes it easy to export a copy of all data associated with a specific case, making it simple for you to fulfill your duties during the collection phase of eDiscovery.

Summary

In today's litigious environment, organizations need to be prepared to respond quickly and thoroughly to any eDiscovery requests in response to litigation, whether it has actually started or if it's simply anticipated.

Data in SaaS application platforms is subject to eDiscovery requests, as well as any other data, and eDiscovery and compliance for SaaS application data needs to be part of an organization's overall plans in these areas.

Veritas Alta SaaS Protection can easily allow your organization to meet all your eDiscovery and compliance requirements for your SaaS data, in addition to providing you with full data protection and cyber resiliency.

You can find more information about Veritas Alta SaaS Protection on our website. You can also contact us today to set up a call or schedule a demo.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V1914 05/23