Whitepaper

ENABLING DEFENSIBLE CLOUD ESI COLLECTIONS THAT ALIGN WITH ENTERPRISE POLICIES

GUIDANCE SOFTWARE™

ABSTRACT

Organizations are increasingly choosing to deploy enterprise file synchronization and sharing (EFSS) solutions or cloud repositories as a way of supporting mobile workers, responding to the demand for BYOD (bring your own device), and ensuring easier collaboration within a more complex ecosystem of third-parties, including outside counsel and supply-chain and business partners. This paper explores the importance of defining critical business requirements related to cloud and EFSS solutions and negotiating them into vendor business agreements. The paper also covers the challenges of collecting ESI from the cloud for purposes of e-discovery and highlights the integrations of EnCase® eDiscovery with Amazon S3, Box, Dropbox, Google Drive, and Office 365.

INTRODUCTION

The rapid adoption of cloud collaboration and EFFS solutions by the enterprise is being driven by growing numbers of mobile workers, the BYOD trend, and an ever-expanding, geographically distributed network of third parties such as contractors, resellers, vendors and customers. In an effort to rein in the security and business risks of uncontrolled e-mail circulation, personal cloud storage accounts, and thumb-drive distribution, companies are designating corporate-approved EFSS vendors to facilitate the sharing of documents in a way that supports existing information governance workflows and other business policies.

As organizations select corporate-approved EFSS vendors, it is important that a clear set of requirements and well-defined terms and conditions be set forth in a formal agreement between vendor and corporation. This paper explores some of those technical and business considerations that legal and IT teams should consider when codifying formal relationships.

As part of our commitment to promoting thought leadership in e-discovery, Guidance Software has hosted a number of webinars, lectures, and industry events featuring executives from leading cloud storage and information security vendors. This paper includes emerging best practices and potential solutions for some of the biggest challenges of data-related risk. In this paper we will specifically discuss the ability to defensibly collect ESI from the cloud as a key e-discovery requirement, and show how EnCase eDiscovery has been seamlessly implemented with leading EFSS vendors for greatly simplified and fully defensible ESI collection.

THE THREE-STAGE LIFECYCLE MODEL AND CLOUD VENDOR REQUIREMENTS

In a webinar with *Inside Counsel* magazine held in March of 2014, Justin Somaini, Chief Trust Officer of Box, described using a three-stage lifecycle model to evaluate your business requirements for cloud and EFSS solutions (Figure 1). The three stages are:

- Onboarding
- Management
- Off-boarding

Somaini said that this same model applies to any cloud business solution, including software-as-a-service (SaaS), platform-as-a-service (PaaS), or infrastructure-as-a-service (IaaS).

The onboarding phase includes the activities that occur during the front end of the relationship. This typically includes contract negotiation, receipt of documentation, requirements analysis, definition of vendor/management relationships, and so forth. **The management phase** is after the relationship is established and the day-to-day interaction with the vendor. **Off-boarding** can be initiated by a number of events, either by choice, or perhaps acquisition, bankruptcy, and so forth. It is critical that the contract take into consideration the critical aspects of all three phases so that any eventuality is spelled out and negotiated on the front-end.

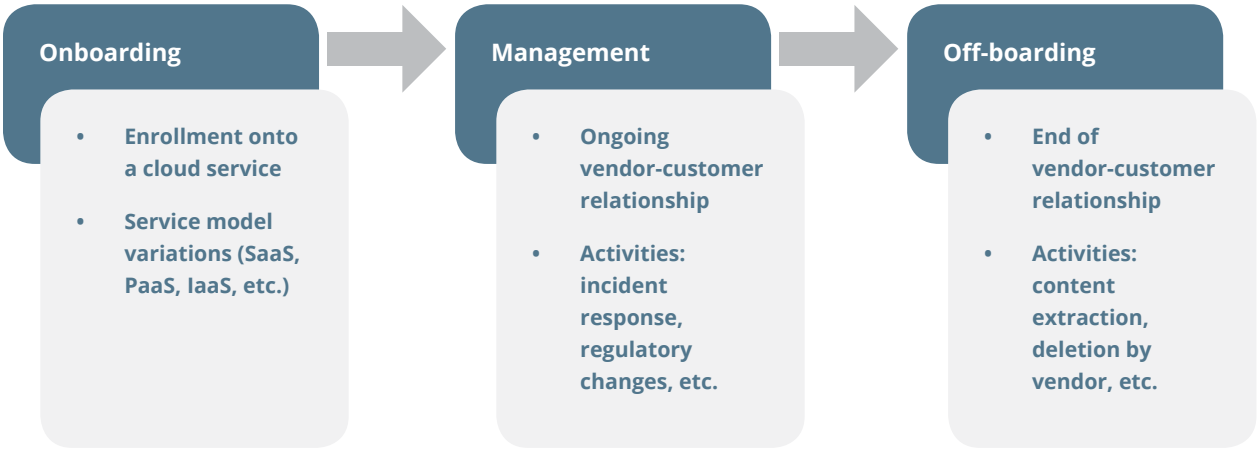

Figure 1: Three Stages of Cloud Usage from Justin Somaini presentation

When establishing a relationship with a cloud service provider, it's important to have a framework that ensures you will be provided with the levels of availability, security, business capabilities, support, and usability required by your users and your business.

One of the most important business requirements for legal and litigation support teams is the ability to comply with your company's e-discovery best practices, regardless of where ESI is stored. In a 2015 survey of e-discovery professionals conducted by Guidance Software, 44 percent of the respondents claimed that they will have a business need either now or within the next year for collecting from cloud repositories as part of e-discovery.

E-DISCOVERY ISSUES WITH ENTERPRISE FILE SYNCHRONIZATION AND SHARING SUPPLIERS

Deciding to host your data with an EFSS supplier does not alter your fundamental e-discovery obligations, and you remain legally responsible for the preservation of information that might be discoverable when litigation is reasonably certain. Warning has been given of these challenges by leading judicial commentators such as United States Magistrate Judge John Facciola. To help you understand the exposure, below is a list of key considerations for resolution in the vendor contract. Future e-discovery projects will be greatly simplified by choosing an EFSS vendor who has partnered with a leading e-discovery software provider. The considerations for each phase of e-discovery are as follows:

- **Preservation and Legal Hold:** The lifecycle of data, wherever it is kept, should be the foundation of policies that are defined by those with responsibility for its availability, whether for ordinary business needs or for e-discovery purposes. An EFSS provider may have its own policies providing for the deletion of data after fixed periods regardless of the purpose or potential requirements for particular categories of documents and data. On the other hand, data that is kept for longer than necessary poses an often overlooked risk–data that could properly have been destroyed at some earlier stage (perhaps when a case is over) remains in existence and therefore accessible to be discovered by demands related to subsequent litigation.
  Recommendation: Ensure that your EFSS supplier does not destroy data that ought to be kept, and that the provider is willing and able to identify and destroy data that is not currently required for e-discovery (or any other) purpose.

- **Identification:** The EFSS supplier may have its own method of storing data, which, while it may retain all or most of the primary components of the original, does not meet the reasonable expectations of the demanding party. This may affect the ability to search the data, since the provider's storage protocols may not be compatible with conventional search tools.
  Recommendation: The ability to search and collect data must be defined from the onset.

- **Cross-Border Collection:** There is a growing legal concern about the collection of information from cloud providers who store data in places other than the home jurisdiction. The obvious example is where data with no prior European Union (EU) data-protection limitations becomes subject to EU data-protection laws because the cloud provider elects to store its information on servers in Europe, perhaps even alongside the data of other organizations. To complicate matters further, a cloud provider might scatter data over servers located in multiple jurisdictions for cost, security or other reasons that take no account of United States e-discovery obligations.
  Recommendation: A company planning to move to the cloud should be sure that the cloud provider understands these issues at the contract stage. The organization must be clear that the question "Where's my data?" can always be answered, and that the answer will be acceptable to you and all relevant authorities.

- **Authentication and Production:** Generally speaking, a party producing information and admitting it into evidence must be in a position to validate its authenticity and reliability. That obligation does not change when the data is obtained from the cloud, where it has necessarily been in the possession of a third party (with what is sometimes an open question as to who has control of it). Though authentication issues are rare, a party needs to be able to show that what was obtained from the cloud and what was requested are identical to what was visible on the screen when the document was created and used. Authentication may require forensic analysis to see if the format of data has been altered, something requiring a level of access which, in the absence of a contractual entitlement, may not be forthcoming (and which may raise technical and geographic issues to begin with).
  Recommendation: An organization needs to be able to go one step further, and to be clear how the data, once authenticated, can be produced in compliance with the rules or with any agreement or court order.

- **Compliance with Subpoenas or E-Discovery Requests:** If your organization is ever served with a Rule 34 discovery request, a Rule 45 subpoena or a governmental subpoena, you will need to collect the requisite ESI from your cloud provider and respond to the demands as though the data were located on your own in-house servers. The primary requirement, in contractual terms, is that your legal ownership of the data is not qualified or limited by the cloud provider's de-facto control of it. More complex e-discovery issues arise when it is the cloud provider, rather than the user, who is served with a subpoena or discovery request. Dealing with subpoenas is not a core business activity for cloud providers, and, as the customer, it is your responsibility to anticipate the problems that may arise. Because the cloud provider is merely in possession of potentially responsive ESI, an opposing party can't serve a Rule 34 discovery request on a cloud provider when attempting to obtain your information. However, a cloud provider may be served with a subpoena, either through Rule 45, or from the government.
  Recommendation: The contractual stage is the right time to cover this, with the provider accepting an obligation to notify you upon receipt of the subpoena to give you sufficient notice to assert and protect your rights.[1]

ENCASE® EDISCOVERY INTEGRATION WITH LEADING EFSS PROVIDERS

When selecting an EFSS provider, it is best to select one that offers a well-defined answer to how to support e-discovery in the event of litigation. One way to enable best-practices e-discovery involving cloud ESI is to work with a software product that is integrated with an enterprise-grade cloud service.

EnCase® eDiscovery is a comprehensive, unified e-discovery platform that reduces risks and lowers costs associated with e-discovery. EnCase eDiscovery has been in the leaders' quadrant of the Gartner E-Discovery Magic Quadrant for the last four years and is considered the gold standard for collection because of its ability to reliably collect ESI from almost any operating system, data repository, and e-mail server.

[1] This duty may be restricted where criminal allegations are involved or where the Stored Communications Act might also obstruct communication between the cloud provider and its customer. In addition, the contract should discuss the provider's specific responsibilities when responding to the subpoena as well as the allocation of costs.

Guidance Software, to address our customers' needs for streamlined, defensible collection from cloud repositories, has established integrations of EnCase eDiscovery with Amazon S3, Box, Dropbox, Google Drive, and Office 365. These integrations let you implement the EDRM process consistently whether your data is stored on premise or in the cloud, from the point of litigation hold, collection and preservation of ESI, and collaborative review all the way through production of evidence for opposing counsel.

Integrations are easily implemented through completion of a configuration step for the EFSS provider within your EnCase eDiscovery deployment process. The communication is secure and requires administration privileges to deploy.

These proven technology integrations offer you the following benefits:

- **Instant data visibility for risk management and legal:** EnCase eDiscovery cloud-provider integrations support the ability to identify and defensibly collect all potentially relevant ESI. The product's fast, scalable, and patented search supports pre-collection analytics reports to determine the volume of data, types of data, and keyword results. In addition, you can:
    - Audit all information for inclusion in a legal matter based on specified criteria (file type, date, keywords, metadata, and more)
    - Produce reports of location (including file path) and meta-data information
    - Cull at point of collection, being able to identify just the relevant ESI reducing the required workload and cost associated with ESI processing and document volume for attorney review.
- **Centralized access to data from the EFSS required for an e-discovery matter:** EnCase provides swift, centralized access for parties involved in the e-discovery process. Direct integration eliminates multiple manual steps (copying files, burning DVDs). In addition, integration provides faster response to legal matters and regulatory requests.
- **Judicially acceptable:** Collections provide all metadata, including creation and last update dates, file path, size, file extension and more. EnCase collections are stored within the Guidance Software-invented Logical Evidence File (LEF). EnCase eDiscovery has time after time provided a defensible chain of custody for ESI and metadata with a defensible, repeatable process. EnCase eDiscovery has been judicially proven in hundreds of cases and the LEF is known as a highly reliable format for the submission of evidence.
- **Lifecycle control** supports a defensible process for retention, deletion (dispensation) of data relevant in legal matters. In addition, EnCase eDiscovery helps you identify and track documents for deletion according to your retention policies. This helps eliminates large e-discovery collections and keeps data relevant.
- **Mobile collection:** EnCase eDiscovery operates without requiring special efforts from mobile workers. It enables the collection of data associated with mobile users that is likely stored on the centralized EFSS platform.

CONCLUSION

Organizations have chosen to deploy enterprise file synchronization and sharing market (EFSS) or cloud repositories as a way of supporting mobile workers, BYOD trends, and collaboration with third parties. It is mission-critical to define EFSS requirements upfront and negotiate them into any business agreement with a cloud service provider. A decision to host your data with an EFSS supplier does not alter your fundamental e-discovery obligations, and you remain responsible for the preservation of information that might be discoverable when litigation is reasonably certain.

EnCase eDiscovery provides integrations with leading EFSS solutions from Amazon S3, Box, Dropbox, Google Drive, and Office 365 within a comprehensive implementation of the EDRM such that there is consistency whether you collect ESI that is stored on premise or in the cloud. In addition to dramatically simplifying e-discovery, EnCase eDiscovery enables instant visibility for risk management and legal support, centralized access to data from the EFSS required for an e-discovery matter, delivery of ESI in a judicially accepted manner, and the ability to do holistic lifecycle management for data stored in the cloud.

GUIDANCE SOFTWARE

ABOUT GUIDANCE

Guidance exists to turn chaos and the unknown into order and the known-so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. The makers of EnCase®, the gold standard in forensic security, Guidance provides a mission-critical foundation of market-leading applications that offer deep 360-degree visibility across all endpoints, devices and networks, allowing proactive identification and remediation of threats. From retail to financial institutions, our field-tested and court-proven solutions are deployed on an estimated 33 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, from beginning to endpoint.