Deloitte.

Discovery insights

5 questions about digital forensics in the cloud

5 questions about digital forensics in the cloud

An interview with Michael Weil, managing director, Deloitte Financial Advisory Services LLP

When forensic investigators go data gathering these days, the hunt may well take them to the cloud. Cloud computing has evolved rapidly from a technology of the future into an integral component of many organizations' strategy, operations, and infrastructure. Private and public sector organizations are using it to reduce costs, improve data management, and foster communication and collaboration.

For investigators and analysts, the cloud brings a significant new dimension to the forensics discovery and investigations process. Simply put, if an organization does business in the cloud, it can expect to conduct discovery there too. "Cloud first" strategies have proliferated across industries over the past decade with several major enterprise resource planning (ERP) and application software vendors shifting the foundational IT framework to "cloud only."

While the cloud is not a business-as-usual tool for most organizations today, it soon may be for many. The volumes of data that organizations already have in the cloud, and the multiples of that constantly being added, offer rich opportunities to conduct more thorough investigations and eDiscovery than ever. Organizations that are anticipating, planning, or already conducting cloud-based discovery can benefit from consideration of five questions pertinent to the cloud transformation.

What's the future for business systems outside of the cloud?

Organizations will continue hosting traditional, on-premise data sources such as servers, laptops and mobile devices with end-point devices such as laptops and mobile devices continuing into the foreseeable future. As servers transition from on-premise to cloud infrastructure, forensic preservation and investigation experience related to the on-premise data sources will continue even as organizations layer in or transition to cloud-based data solutions. As such, adding skills to help navigate the intricacies of cloud-based applications and cloud-hosted data is essential to helping organizations address the full scope of their discovery requirements.

In particular, data identification, preservation, collection, and analysis is increasingly challenging in the diversified environments containing both on-premise and cloud data sources that may be

responsive to discovery requests. Sound data governance is essential to successfully navigating this environment. The transition period from on-premise to cloud infrastructure is actually a good time for organizations to evaluate what data is in the cloud, what is not, and how to handle data in the most appropriate manner based on where it resides.

While not immediately imminent, the vision of cloud-only is very real.

How do we keep up with the changing cloud applications?

Cloud application deployments constantly evolve and update and organizations do not necessarily know when the cloud application has changed. IT organizations and business users are familiar with the structured release of versions and subversions in traditional application deployment such as moving from version 8.54 to 8.62 of a software package. The constant and ongoing updates to cloud applications challenge current IT and business process change management approaches. In addition, the fluid cloud environment creates obstacles to data collection and preservation procedures that may impede the discovery process.

The constant change creates new opportunities for fraud as cloud application deployment is becoming easier and more economical providing an opportunity for developers to bypass internal controls, procedures, and discovery requirements that may be viewed as obtrusive hurdles to application delivery and progress. For example, a change to the online credit card processing application may intentionally or unintentionally provide an avenue for exploitation by fraudsters.

Organizations should remain close to product roadmaps for cloud applications looking for changes that could affect organizational compliance or discovery requirements just as they would with applications hosted inside the organization. For example, the introduction of a chat application might provide peer-to-peer file sharing; a file passed along in this manner may inadvertently escape capture for compliance purposes, potentially creating a compliance risk and an impediment to discovery. Organizational policies and procedures should be reviewed and may require rapid adaptation for cloud applications pertaining to data handling requirements.

Another path to maintaining compliance is having the cloud vendors provide a discovery or compliance component to an application so that the organization does not need to be up on the constantly evolving feature set.

How does the cloud change data residence?

Many cloud development and hosting platforms allow organizations to select where their data resides – an important capability for discovery purposes. An organization should exercise that right in adherence to data privacy restrictions and other regulatory considerations relevant to their organization and industry.

In some cases, organizations leveraging cloud-based, multi-tenant applications may not know where their data resides or may not be provided options to control their data residence. Two common examples of these applications are cloud-based office productivity tools and sales and marketing applications. The data residency situation can unknowingly lead to an incident with local data privacy and cross-border data transfer laws.

Complicating matters is the location from which public cloud applications are accessed, which may open a company to the possibility of having to produce more data than anticipated or desired. For example, a legal action against a company in the United States may result in a demand from the opposing party for data that resides in another country. These conditions can lead to parties fishing for data in places with less restrictive privacy and security protections. Accounting for data residence requirements during the planning stages for cloud hosting assists in understanding data privacy restrictions and regulatory requirements.

For forensic investigators, cloud applications and data provide an opportunity to connect remotely from anywhere to preserve and analyze organizational data more efficiently as compared to traditional discovery which requires on-site handling of data from servers, laptops, mobile devices, and other sources. This capability can save in travel costs and impact on the organization location hosting the data collectors, which reduces the time and cost of collecting and analyzing the data.

How do we determine where to analyze the data?

Several factors warrant consideration in deciding where to conduct analysis, including data volume, availability of data analysis tools, and financial impact. Careful evaluation of these factors is required to determine the most effective analysis solution that meets defensibility standards.

Traditional forensic data collection methodologies leverage preservation techniques to read-only environments for analysis to minimize negative impacts to production environments. However, there may be feasibility concerns with transferring high volumes of data depending on the cloud vendor's technical constraints, such as limited data transfer rates or capped data transfer volumes, limiting the amount the of data allowed to exit the cloud. Just as with on-premise architectures, live collection of data from cloud production environments should also be considered as the collection may still cause dramatic performance issues for active users in the systems. Another data collection methodology involves collecting data into another cloud location so as to have a cloud-to-cloud collection rather than a traditional cloud-to-disk collection.

Alternatively, cloud solutions often include data analysis tools allowing immediate and direct access to an organization's data. Understanding the cloud platform's analytic capabilities and limitations is essential to determine if in-cloud analysis is an acceptable option. If the analytics tools available in the cloud are sufficient for the investigation, it may be appropriate to preserve the data in place to perform data analysis in the cloud.

Careful consideration is required to determine the optimal location for conducting data analysis against cloud data. With a growing number of analytical tools directly available to cloud applications, forensic professionals must be mindful of the impact when leveraging in-cloud analysis against production systems. Defensible analysis techniques must be chosen understanding the parameters of the investigation, as scope of data and availability of analysis tools greatly influence the appropriate choice.

How does the role of discovery delivery change, and how are legal and IT roles changing?

Increasingly organizations have the ability to quickly build out low cost, cloud-based solutions for application development and data analysis, often without involving IT. Accordingly, IT may no longer be the sole source of all data for an organization, which can cause potential challenges with regulatory requirements or discovery requests. Applications also have the ability to source data from cloud-based systems and on-premise systems alike, leading to complex data preservation and analysis situations. Legal teams will likely be further challenged as concepts of data ownership and custodianship evolve with cloud-based data sources and cloud accessible applications.

Involving IT, legal, compliance and business leaders within an organization as cloud-based applications are being planned and developed is critical to addressing these issues. All parties must understand how cloud applications operate and the data flow implications on their respective area of responsibility before cloud-based applications become operational.

Our take: Defensible cloud discovery is essential . . . and possible

As organizations move more applications and data into cloud-based solutions, thoughtful planning around regulatory, compliance and data residence issues is essential to the success of managing data in the cloud. Forensics and discovery practices must evolve to address new and complex data challenges while remaining mindful of real-time data analysis concerns and overall discovery costs accompanying large volume cloud datasets. Collaboration among relevant stakeholders in the organization, legal counsel, discovery professionals and forensics investigators can assist in establishing sound, defensible solutions for identification, preservation, collection, and analysis of cloud-based data.

Contacts:

Mike Weil
Managing Director
Deloitte Financial
Advisory Services LLP
miweil@deloitte.com
+1 312 486 0207

Deloitte.