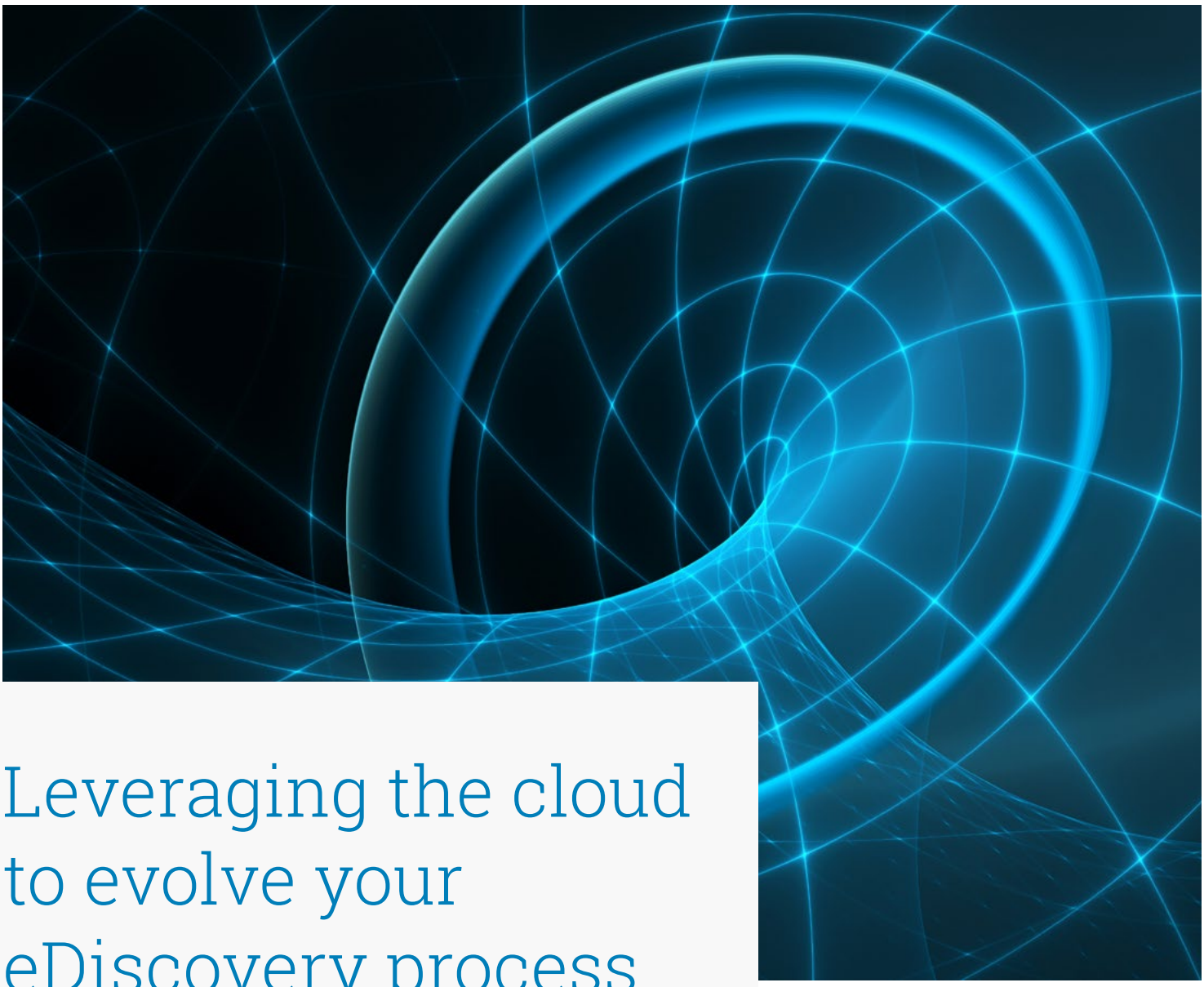
druva

White paper



Leveraging the cloud to evolve your eDiscovery process

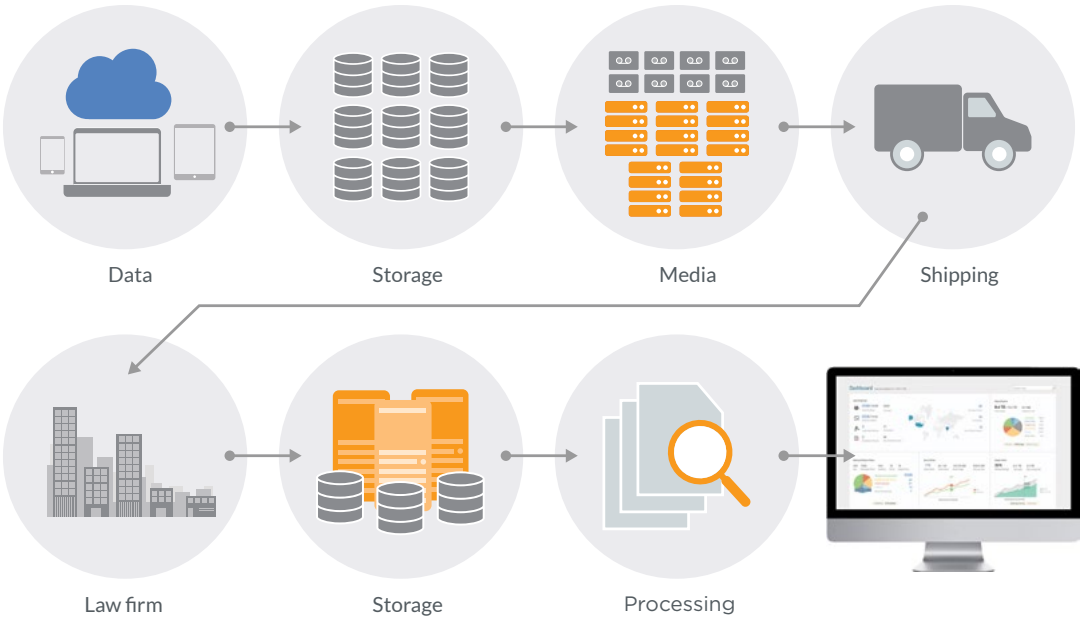
How organizations save up to 50 percent in time and costs

Q420-20098

Accelerate your eDiscovery process while reducing costs and risk

With the accelerating increase in data volumes, cloud service options, and the number of mobile devices deployed throughout organizations, it's no surprise that the eDiscovery process has become more complex. Adding to this complexity is the dispersion of data across various repositories including endpoints, SaaS applications (such as Box, Office 365, Google Drive, and Salesforce), and servers. The collection and preservation of this electronically stored information (ESI) in a distributed environment is often a cumbersome manual process that can be very time consuming and costly. It can also greatly increase the risk of data spoliation as information is copied, deleted, stored, or transferred across unprotected networks.

Traditional eDiscovery workflow



To add to this conundrum of complexity and inefficiency, many eDiscovery teams still use outdated and inadequate legacy data management products. They are often not suited for situations where the collection window is short, and they often require heavy involvement from IT or end users to manually collect content. Such collections can be non-comprehensive, delay the eDiscovery process, and significantly increase costs — while rendering end users unproductive. Many companies don't have internal eDiscovery technology at all. As David Cohen, Esq. Partner and Chair, Records and eDiscovery at Reed Smith says: "… years ago, most companies were leaving it to outside counsel to manage all aspects of eDiscovery, often with mixed results and out-of-control expenses. Now, sophisticated companies are taking control through several means: advanced budgeting, automation, reducing costs through bringing processes in-house, predictive coding, and employing e-discovery specialists."

Using technology to streamline the eDiscovery process

Information governance — visibility and manageability of your data

Most US corporations have accumulated mountains of data, and no two companies manage their data alike. Some feel they must keep everything, while others are determined to store only data that is necessary for business and compliance objectives.

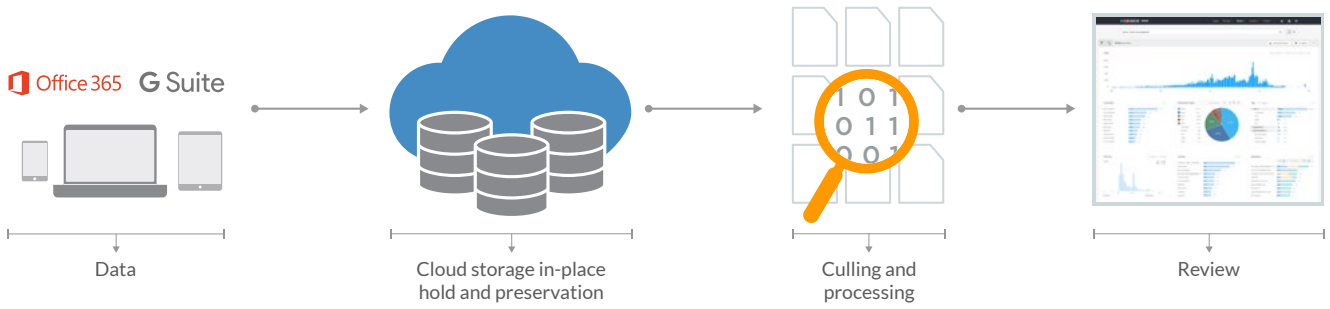
> *"Between turnover, layoffs, and changing positions in a large company, finding the individuals who know where the information may be is difficult.*
>
> — Fortune 500 Attorney

Enterprises have always had to deal with large amounts of data. But efficiently addressing the skyrocketing volumes of data the digital age produces requires new strategies. Nancy Patton, Esq., Senior Solutions Consultant with Exterro, says, "Instead of looking for a needle in a haystack, which was the traditional eDiscovery strategy, we now tend to look at data with a holistic approach, and by using the latest information governance technology, you not only store data in a repository, but you store it in a meaningful way which anticipates future legal needs."

A huge percentage (estimates range from 30-85 percent) of an organization's data is redundant, obsolete, or trivial — otherwise known as ROT. Yet in an Exterro poll, over half of all respondents said their organization does not measure ROT, and another 34 percent said they weren't sure if it was measured. Meaningful work cannot be done effectively without streamlining the collection and management of data, and to do this, the first step is to declutter and organize. Mature enterprises often move to rule-based or retention-on-scheduled policies for automatic deletion of ROT data. As David Cohen puts it, "No one has time to go back and look at old data and make individual decisions regarding data. At the same time, you also have to make sure your system accommodates the need to keep longer-term data for business, legal compliance, and litigation defense."

Information governance — risks and optimizations

Another easily overlooked cause of spoliation is accidentally deleting or modifying information on legal hold when employees change roles or depart from a company. These changes typically involve recycling computer hardware or mobile phones, deleting email or cloud application accounts, purging file shares, and destroying paper files. Yet legal holds must remain intact across all sources of data, even when custodians leave. One misconception is that HR has a handle on who is coming and going, but in a large corporation with thousands of employees in multiple locations, it's virtually impossible for any single team to track the full depth and breadth of an employee's digital footprint without an adequate solution in place.



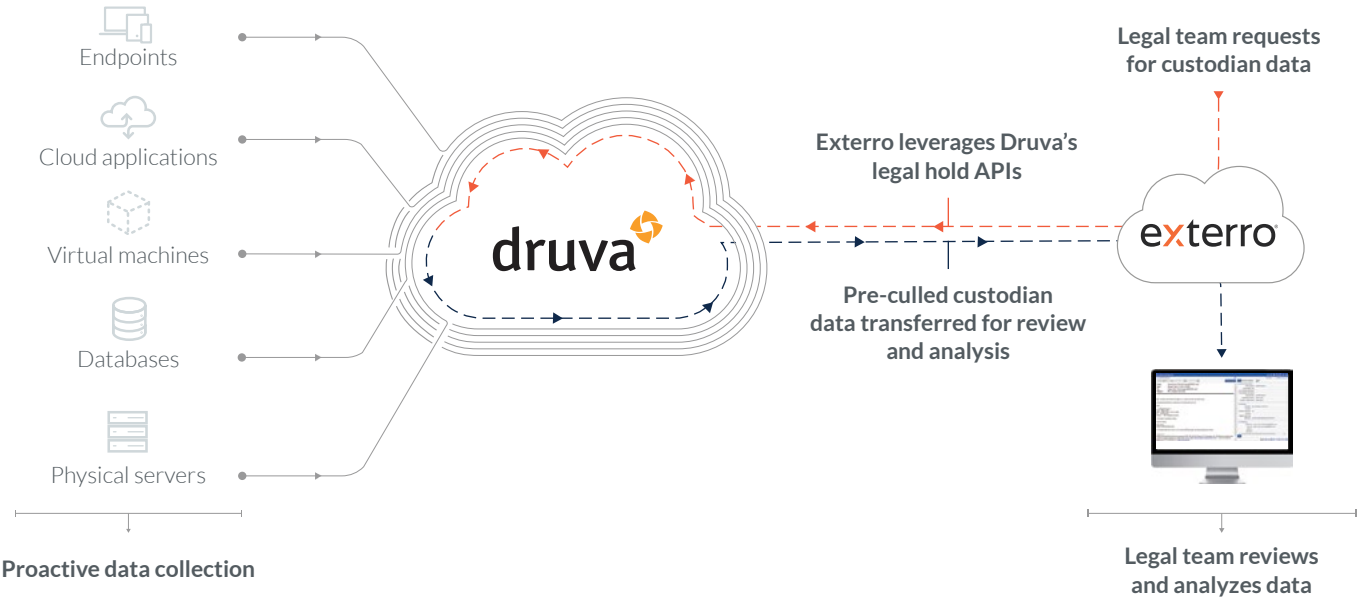
Such a solution can substantially help optimize the information governance process. Important steps in this optimization include:

- Adopt a SaaS platform that lets you view and manage all end-user data across all repositories including endpoints, cloud applications, and servers. With proactively collected end-user data (and metadata) stored in the cloud, custodians easily access and maintain any legal hold content.
- Enforce consistent retention and defensible deletion policies to manage employee information. This helps eliminate ROT data and ensures only necessary data is collected for any litigation needs.
- Apply solutions that address employee movement and preserve end-user data for as long as it is needed, even when an employee departs the organization. Automate this process through policy-based legal holds that prevent undesired data disposal as well as accidental or malicious deletions.
- Use end-user and administrator audit trails that track data access, actions, and events for compliance with eDiscovery requirements and for maintaining chains of custody.

Data collection

Internal counsel, HR, enterprise managers, and IT need to collaborate to get a clear understanding of what data should be collected and how to access it. Working with external counsel and/or experts is also important to ensure a given collection effort is sound in scope, not overly broad or too concise, and is performed in a defensible manner. Bennet Borden, Chief Data Scientist & Chair at IG Group, Drinker Biddle Reath LLP, comments that, "If it isn't in the scope of discovery, then there is no need to preserve it. Astute lawyers will use this to greatly reduce the volume of data preserved and thus reduce the associated burden of doing so."

Automated data collection and immediate access to custodian data for review and analysis

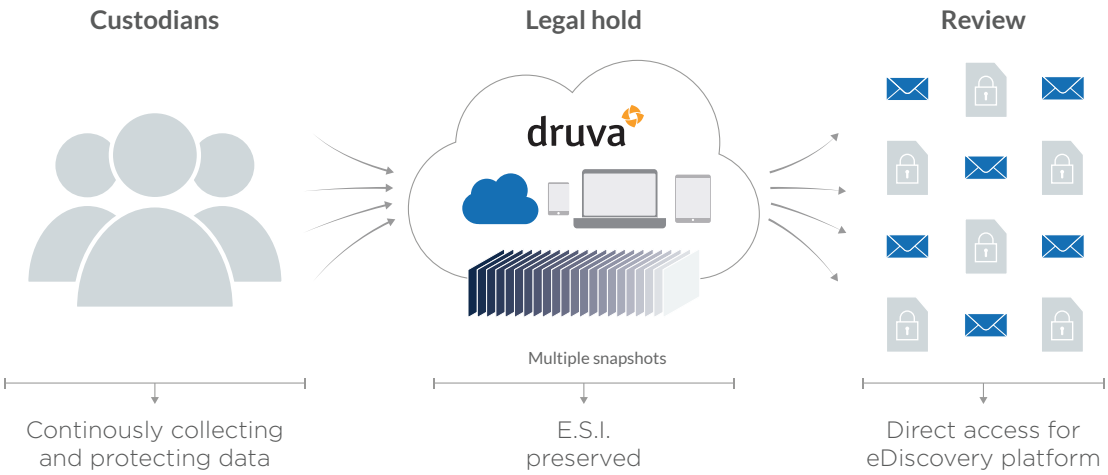


Nancy Patton says that legal teams can do this by using technology to "get to ESI quicker, as well as searching metadata and keyword analytics to give an understanding of which searches are working. There are also cost estimators, which allow you to predict how much production will cost before it takes place."

To collect relevant data in a defensible and timely manner, advanced solutions can:

- Easily collect all relevant custodian data from endpoints, cloud applications, and servers with a few clicks, leveraging a single technology platform, to minimize dependence on IT resources and end users. Furthermore, these solutions work silently to non-intrusively collect data while maintaining end-user productivity.
- Maintain a clear chain of custody and file integrity for custodians without the need for intrusive, time-consuming, and expensive device-level forensic imaging and exporting.
- Set customized policies to seamlessly and consistently collect only relevant data and necessary metadata attributes to maintain defensibility during litigation.
- Reduce storage and bandwidth costs by deduplicating end-user data to store only a single copy, regardless of how many devices store the identical content.
- Leverage the powerful security and simplicity of cloud service platforms such as Amazon Web Services (AWS) or Microsoft Azure. With these platforms, data never traverses an unprotected network and it can move directly from one secure cloud where it is stored to another where it is reviewed and processed — minimizing the risk of data spoliation.

Data preservation



Given that end-user data is often potential evidence in litigations, corporate legal departments depend on IT for not only the collection but also the preservation of relevant ESI. The question of deciding how and when to preserve data is a tricky one. There is no bright-line indicator of when you'll need to start preserving data when anticipating litigation. Judges and courts around the country have used their own discretion to decide when this must be done depending on the circumstances surrounding the case. Under the new Federal Rules of Civil Procedure (FRCP), there are complex questions about what constitutes a defensible preservation tactic: collection, legal hold, or a hybrid method.

You must consider an approach that achieves three major objectives when preserving ESI:

- Ease of applying holds across custodians and data sources.
- Ability to preserve ESI in a forensically-sound manner.
- Ability to authenticate ESI collected from relevant data sources.

To ensure preserving end-user data per the Electronic Discovery Reference Model (EDRM), data preservation tools can help with the following:

- Preserving ESI across all relevant data sources — endpoints, cloud applications, and servers. A solution must let IT administrators and legal teams centrally manage holds across all data sources to help reduce the time required to preserve ESI from disparate data sources.
- Providing chain-of-custody reports to ensure data is fingerprinted for authenticity and collected with extended metadata (as outlined by the Department of Justice and EDRM) to meet defensibility requirements.
- Setting up granular data access policies to cull data by date range, file types, and deleted files so organizations can reduce the data that needs to be passed downstream for processing and review.

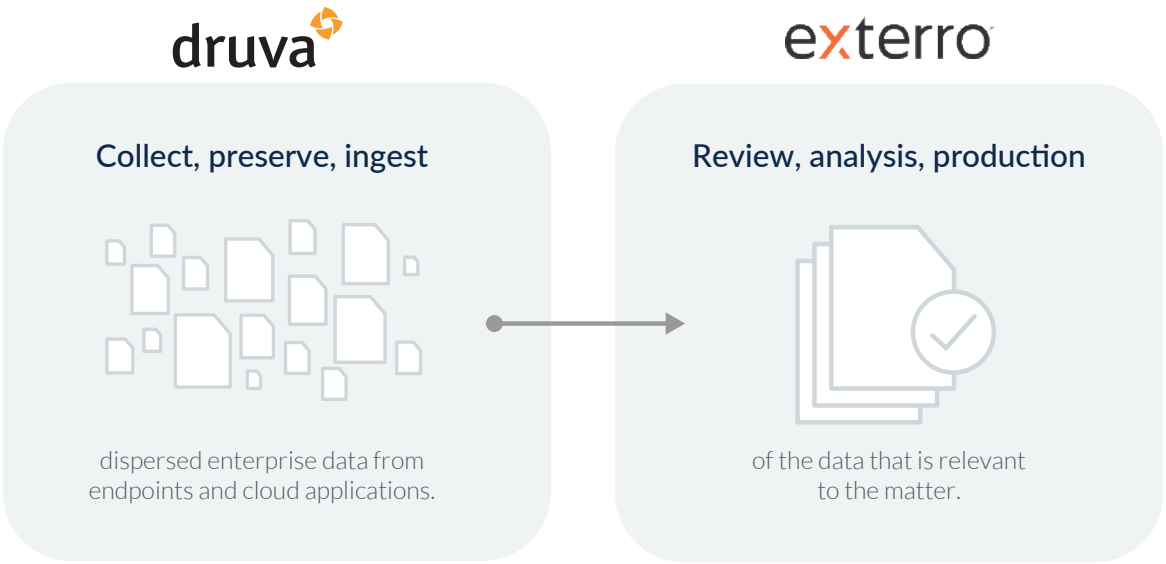
Managing the review process

Attempts to reduce review costs often fail because they don't go to the root of the problem: too much data is preserved, collected, and sent to outside entities. By taking measures to streamline all the steps leading up to review, legal teams can reduce up to 50 percent or more of total eDiscovery costs.

David Cohen reminds us how things have changed quickly in the world of eDiscovery: "Technology greatly cuts volume in review. In a big case, you used to need 40 to 50 lawyers to review documents. Now, four to eight lawyers who know how to use technology can accomplish this task quickly and more accurately, while reducing review volume."

How Druva and Exterro can help cut eDiscovery costs in half

Druva and Exterro have expanded their respective data protection and eDiscovery platforms to significantly reduce the time, costs, and risks associated with traditional approaches to eDiscovery.



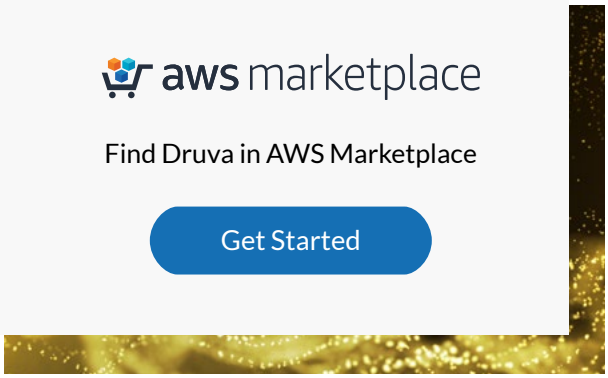
Features include:

- **Automatic legal hold, in place preservation, collection, and processing from Exterro —** Exterro's eDiscovery suite leverages Druva to seamlessly collect, preserve, and ingest dispersed enterprise data from all endpoints, cloud applications, and servers.
- **Data collection and preservation —** Druva proactively collects and manages all the data across an organization's laptops, desktops, mobile devices, as well as its cloud applications. Organizations can then immediately put legal holds in place without any action needed by the custodians. Druva stores secured, immutable information in the cloud, outside of custodians' devices, until review. The data can't be tampered with or deleted once it is collected, which is especially important when it involves exiting employees. Once content is on legal hold, it's ready for transfer to the Exterro platform within seconds, augmenting data collected from other enterprise sources through the Exterro platform.
- **Data transfer and ingestion —** Druva and Exterro are both cloud-native technologies, leveraging the proven infrastructure of AWS. Data moves quickly and securely within the Amazon cloud, eliminating the risk associated with unsecure networks or the time-consuming and costly handling of physical media. In addition, critical administrator and end-user audit trails maintain clear records for chains of custody.
- **Data review —** With rapid ingestion by Druva, without the legacy challenges of limited compute and fixed infrastructure, Exterro makes data easily available for early analysis and review.

Conclusion

Efficiency should be at the forefront of any legal team's process in order to save precious time and address rising costs throughout the litigation process. Organizations leveraging cloud applications have been able to easily cut their eDiscovery time in half while saving significant costs and minimizing data spoliation risks. Legal teams now have the ability to quickly and selectively collect and analyze the most relevant data at the very beginning of case assessments and use that data offensively to gain a significant advantage over opposing counsel. Before legal teams are even served with discovery demands, they can use proactively collected information to help win either a dispositive motion or a more favorable settlement.

Visit druva.com/endpoint-ediscovery/ to learn more.



druva

Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729

Druva™ delivers data protection and management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted worldwide by over 4,000 companies at the forefront of embracing cloud. Druva is a privately held company headquartered in Sunnyvale, California and is funded by Sequoia Capital, Tenaya Capital, Riverwood Capital, Viking Global Investors, and Nexus Partners. Visit Druva and follow us @druvainc.