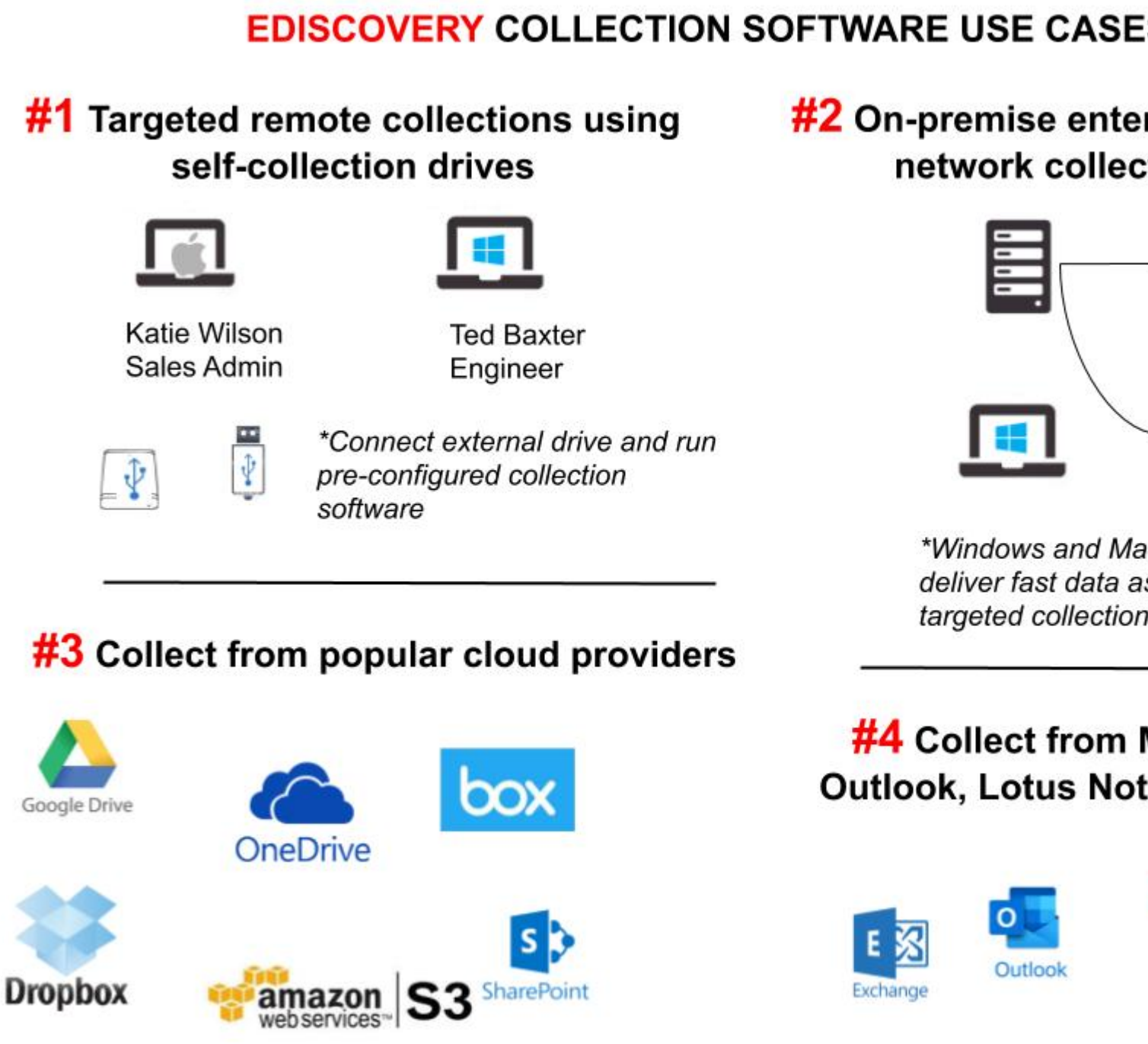
eDiscovery Collection Software | Enterprise Deployment

Description



Pinpoint Labs develops defensible eDiscovery collection software. Pinpoint Labs software collects local, remote, network computers and popular cloud accounts.

USE CASE EXPLANATIONS

#1 Targeted, Remote Self-Collections

Companies and firms performing self-collections use external hard drives because:

1. The cloud or remote server speeds do not allow large data uploads
2. Copying data to remote servers violates security protocols

Ensuring a defensible eDiscovery self-collections approach must be a priority. For example, copying files through Windows Explorer or Mac Finder to an external drive does not retain metadata, create a chain of custody, and will miss files in long paths.

How do you train remote workers on computer forensic collection software? Well, you donâ€™t have to. Software programs like Harvester Portable, are specialized eDiscovery and forensic backup programs. In other words, they automate the self-collection process.

When a user plugs in the external hard drive running Harvester Portable, they will see a file called, â€˜Click Me.â€™ Also, you can include instructions in an email, or in the package, the drive was shipped to double-click the file. Therefore, Harvester begins an automated and defensible eDiscovery collection on the remote workerâ€™s system.

Targeting specific files and emails

Harvester Portable performs automated email and document backups and very targeted collections. How does it work? Firstly, before the hard drive is shipped, a trained Harvester user configures Harvesterâ€™s options and saves the job to an external drive. Secondly, the remote worker clicks the â€˜Click Meâ€™ file, and Harvester runs the job included on the drive.

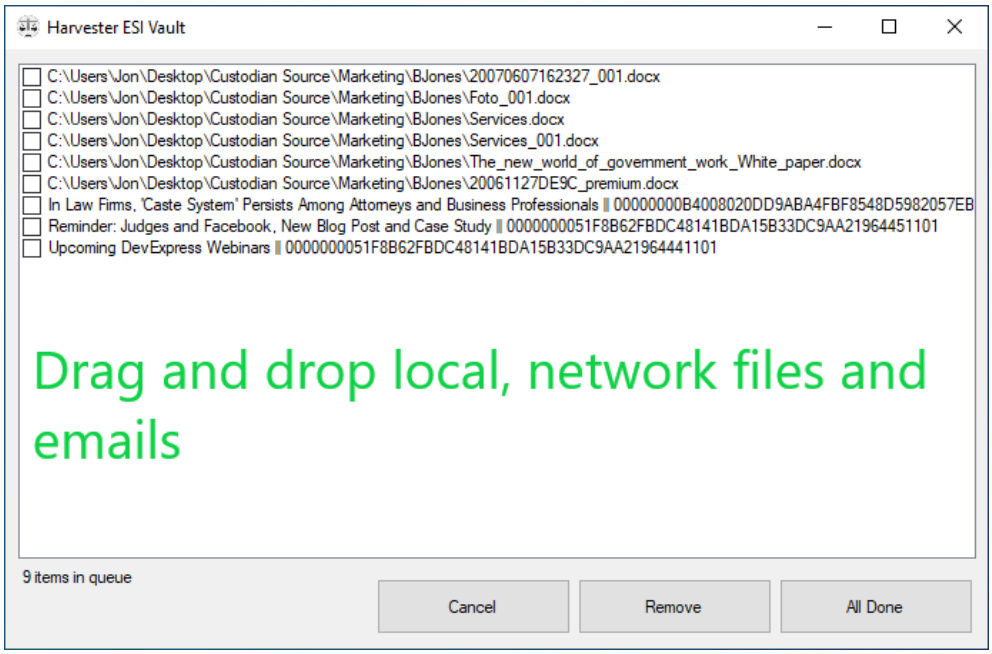
Common filtering options include:

- Keywords
- Date range
- Deduping
- Email searches
- DeNisting

Targeted eDiscovery self-collections often reduce collected data by more than 90%. In other words, skipping standard Windows and application files provide reductions. After the job completes, Harvester notifies the user. After that, place the drive in a shipping box and return after job completion.

Remote Custodial Interviews

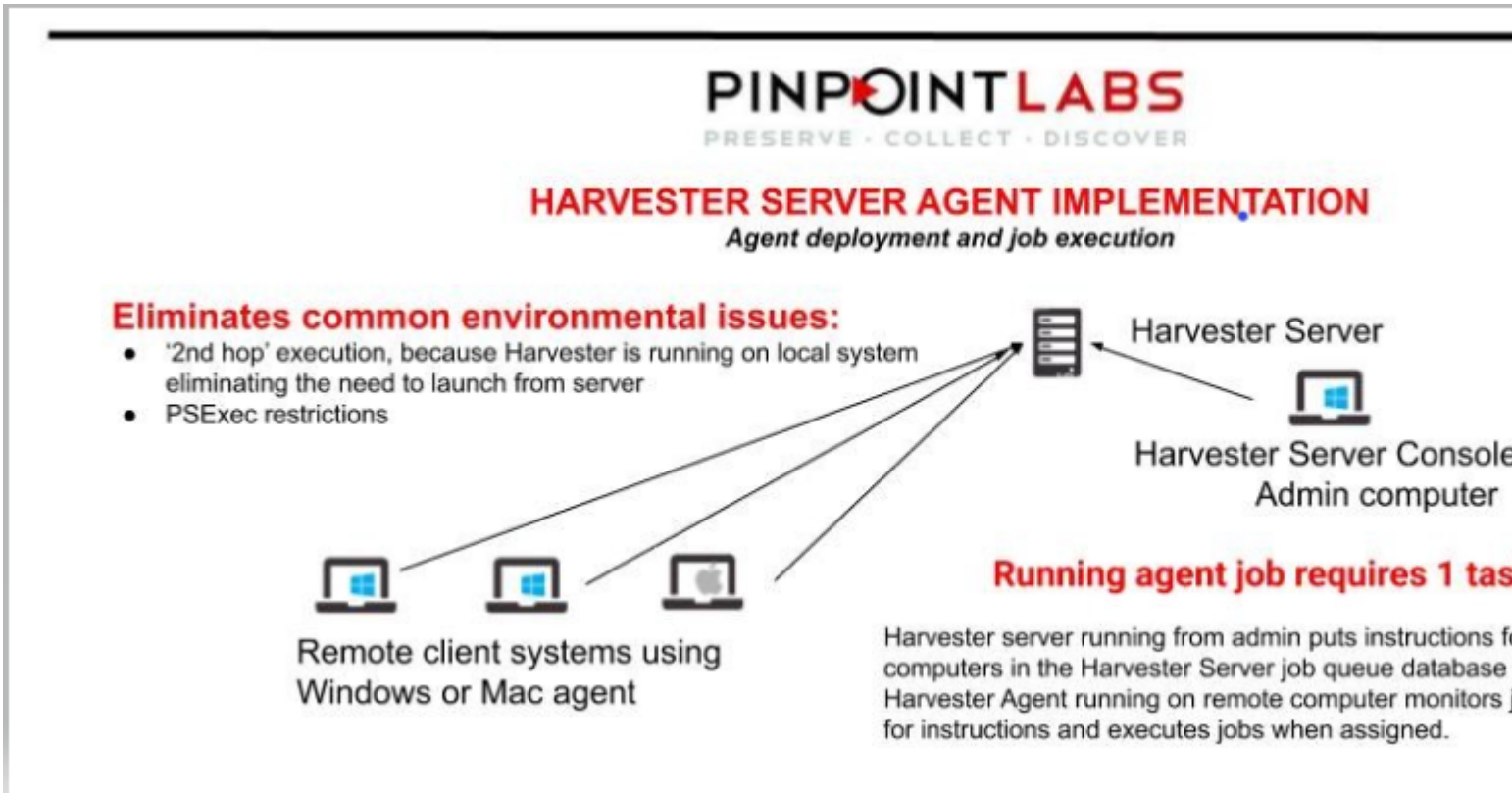
Harvester simplifies custodian interviews. To clarify, an attorney or legal IT professional help locate relevant documents and emails, and the end-user drags and drops the items into the ESI (Easy) Vault window. Using a screen sharing application, the interviewer observes the remote usersâ€™ screen. As a result, interviews expedite and ensure relevant eDiscovery data collections.



In Summary, assisted self-collection target relevant eDiscovery, and with the right tools, collect in a defensible manner. When uploading data to a remote server isnâ€™t practical, use Harvester Portable running on an external hard drive.

#2 On-Premise Enterprise-Wide eDiscovery Network Collections

Corporate and government legal departments need to backup computer data on their network for legal matters. As a result, IT departments must implement defensible eDiscovery collection software and procedures for document requests. Otherwise, data spoliation will occur and not be admissible in court.



Two frequent collections approaches include stealth, and custodian assisted. Firstly, a stealth collection involves backing up documents and emails from systems and servers without end-users knowledge. Stealth or background eDiscovery collections often use agent software on the remote computer. An enterprise-wide software running on a server communicates with the agents that perform the backup.

Secondly, users assist through a legal hold generated email survey or direct custodian interview. During the meeting, the interviewer shares the custodianâ€™s computer screen and helps locate relevant documents and emails. Next, after discovering related items, they are put in the collection queue and copied.

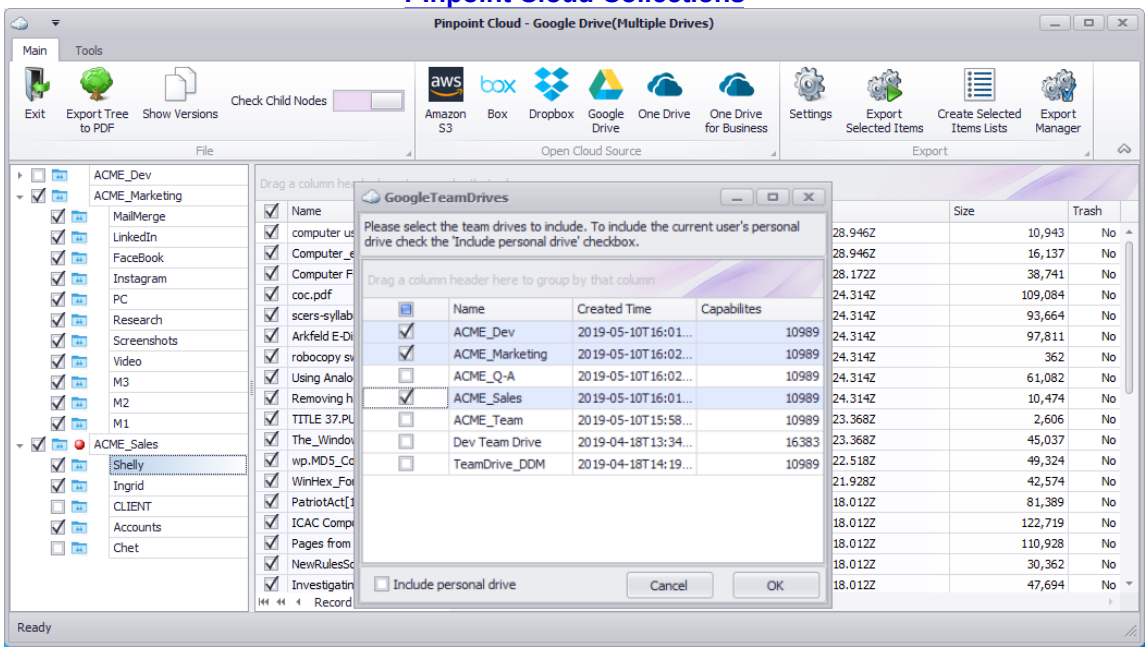
Preserving metadata, hash verification, and an electronic chain of custody is critical during an eDiscovery collection. For a defensible collection, data verification and preservation proof shown in logs and reports is necessary. Additionally, the job settings that show any exclusion filters should be readily available.

Clients use Harvester Server for the most demanding eDiscovery network collections. Harvester Server handles both stealth and custodial interview collections. Also, Harvester Server creates defensible audit reports and documentation.

#3 eDiscovery Cloud Collections

Cloud-based document storage providers now host many corporate and government document repositories. For example, corporations and government agencies store data in Google Drive, OneDrive, box, Dropbox, Amazon A3, and others instead of network file shares. As a result, legal IT professionals need to use defensible eDiscovery collection software that logs in, accesses, and backs up repository contents.

PInpoint Cloud Collections



Cloud computing and cloud-based data storage continues to gain momentum. Some of the driving factors include convenience, collaborative opportunities, hardware, and IT infrastructure savings. Even Federal Government agencies and corporations with highly confidential information are storing content with various cloud providers.

As with other collections, cloud-based eDiscovery collection software needs to verify items were collected and provide an electronic chain of custody. Our Pinpoint Cloud software creates a chain of custody, hash values for collected data, provides the audit information for a defensible collection.

#4 Collections for MS Exchange, Outlook, Lotus Notes, Gmail, Yahoo, and other webmail accounts

Messages and attachments are often the most critical sources in an eDiscovery collection. Therefore, preserving and defensibly collecting from conventional email stores is essential to the discovery process. However, there are many different applications custodians use.

Complications arise during eDiscovery collections when a company uses multiple email systems. For example, a company may use Microsoft Exchange for its primary email storage, but custodians also backup emails to local OST files. Due to retention policies, some companies automatically archive older emails, and employees will store their local backups for easy access. Additionally, many corporations and government agencies store emails in the cloud. As a result, eDiscovery collections from cloud and webmail accounts introduce new eDiscovery collection challenges.

Hashing email data during eDiscovery email collections differ from files. For example, a file hash value is of the entire content of the file. While an email hash value is from specific fields and message contents. A common hashing method for message verification could include the following fields and content:

1. Sender(s)
2. Recipient(s)
3. CC
4. BCC
5. Sent date and time
6. Subject
7. Attachment file names
8. Attachment file sizes
9. Message content

As with other collections, email eDiscovery collection software needs to verify items were collected and provide an electronic chain of custody. Our Harvester software creates a chain of custody, hash values for collected data, provides the audit information for a defensible collection.

In summary, several eDiscovery collection use cases call for flexible and defensible applications. Furthermore, purchasing fewer products with consistent chain of custody and audit reporting minimizes licensing costs and end-user training. Pinpoint Labs products provide the versatility and scalability the legal landscape requires.

Date
12/07/2025
Date Created
10/04/2019