



AccessData Corporation

# Real-world Application: Enterprise Investigations, Incident Response and eDiscovery

White Paper

Tim Leehealey, CEO  
10/9/2008

## Using AccessData® Enterprise

At its core AccessData (AD) Enterprise is an investigative tool. While many people consider it a forensic product, it was designed for a much broader set of investigations. Using AD Enterprise customers can investigate essentially any type of computer incident to determine what happened, who was involved, and how extensive the issue was. Given this broad range of capabilities some of the common applications are as follows:

- 1) **Employee Malfeasance:** AD Enterprise is ideal for investigating issues of employee malfeasance, including sexual harassment, computer misuse and theft. Using the solution's powerful forensic capabilities, an analyst can fully investigate the activities of an employee in a completely stealthy and forensically sound manner. This not only allows the investigator to determine the user's innocence or guilt, but it also enables them to preserve any evidence in the event that litigation arises.
- 2) **Malware:** AD Enterprise is a powerful tool in the fight against malware for three critical reasons. The first is AD Enterprise allows a company to quickly scan the network and locate all instances of a given piece of malware. This can be invaluable during a zero day attack especially if the malware is new and the antivirus vendors don't yet have the signature to address it. The second reason is because it is able to find advanced malware, such as kernel-level rootkits that other tools are not able to see. Investigators can use AD Enterprise proactively to scan the network and locate all unhooked processes or injected DLLs. The final reason AD Enterprise is a powerful tool in the fight against malware is that it has built-in remediation capabilities. When malware is located, the investigator can kill the offending process with one click of the mouse. Furthermore, with AD Enterprise's Batch Remediation capabilities, authorized investigators are able to select all the affected machines and kill that rogue process on all of them at the same time.
- 3) **White List Policy Compliance:** AD Enterprise can be used as a proactive auditing tool to ensure that no processes are running or installed that are not approved. AD Enterprise allows personnel to easily build hash baselines of a company's gold disks, so that all approved processes are known. The examiner can then set up regular network scans, in which all processes that aren't approved are located. In addition, if the organization doesn't have adequate gold disks, an external hash database can be used to categorize processes as "known", "approved", "known but unapproved", and "unknown". By proactively auditing in this way, AD Enterprise users ensure that no malicious applications are able to exist on the network for extended periods of time.
- 4) **Hacking:** AD Enterprise is an ideal tool to investigate issues of suspected hacking. For example if an analyst sees a suspicious IDS alert, he or she can use AD Enterprise to investigate the machines identified by the alert and determine if an incident has actually occurred. If an incident has occurred, the investigator can then use AD Enterprise to both gather evidence, in the event litigation follows, as well as determine the full scope of the incident. Many times when evidence of hacking is detected it is not an isolated incident. Frankly, more often than not, when a machine is found to be compromised, it is one of many. With its ability to scan large numbers of machines against virtually any criteria AD Enterprise enables an investigator to scan the network and determine not only the number of machines compromised by a given hacker, but also determine the initial entry point and the extent of the information exposed.

## Using AccessData® eDiscovery

The accessData eDiscovery solution is effectively an enterprise search, collect, and process solution. It allows an organization to search the entire enterprise against any basic criteria such as keywords, file types, users, creations dates, etc. While the solution is named eDiscovery, because that is the primary usage demanding this type of capability, the fact is the product has many powerful and common uses:

- 1) **Traditional eDiscovery:** eDiscovery, for which the solution is named, is the act of discovering, collecting, processing, and reviewing documents related primarily to civil litigation. While eDiscovery has always been an issue, it has become particularly important over the last several years as a result of the federal rules that became active in the US in late 2006. Those rules effectively mandate that eDiscovery play a role in every court case subject to US law. The AccessData eDiscovery solution is designed for companies that would like to automate the process of discovering, collecting and processing data for eDiscovery. To help understand the advantages of the eDiscovery solution, we will present two approaches to a discovery issue, one without the eDiscovery solution and one with it:
  - a. **Without eDiscovery:** Without the eDiscovery solution a company would address a discovery matter using what is essentially a manual process, most likely with the help of external consultants. Lawyers involved in the case would determine the relevant custodians (people), data, and time periods. Then the external consultants will travel around the world collecting images (complete copies) of the machines used by the custodians involved. Once the data universe is collected the consultants process the data, which typically means they index it and expose data contained in any complex data types, and then load it into a review tools for the lawyers to review. The problem with this approach is that it is extremely expensive, time consuming, and prone to error. A single discovery matter performed in this manner could easily run many millions of dollars and if critical data is not found it can lead to negative legal outcomes that could have been avoided.
  - b. **With eDiscovery:** Utilizing the AD eDiscovery solution a company can easily avoid all the negative issues associated with a manual eDiscovery process. Because AD eDiscovery automates the collection and processing portions of the eDiscovery process it not only dramatically reduces the time and costs of a given issue but it also ensures that the resulting collection is comprehensive, accurate, and repeatable. Three things that in the context of a litigation can ultimately result in massive savings. Utilizing the AD eDiscovery solution all the investigator needs to do is select the relevant search criteria and the custodians and the software automates the rest, ultimately delivering a single fully processed file containing all of the data reactive to the search. The solution is made even more powerful by the fact that it does all of the collection and processing in a completely forensically sound manner, maintaining all of the relevant meta data and the full chain of custody need to comply with the strictest standards.
- 2) **Records Retention Engagement:** Records retention is generally considered the proactive form of eDiscovery. Organizations that want to limit the amount of data on their networks that is available to be discovered can employ standard data retention rules. A common rule that an organization might implement is a maximum retention period for email. By enforcing rules that limit email retention to 90 or 180 days an organization ensures that old and potentially damaging emails won't be found. As long as these rules are applied evenly and intelligently across an organization they are completely legal and even encouraged under US law. The problem with these rules is that most companies have absolutely no way to ensure that they are respected by the employees. So despite

rules that require the deletion of emails over a year in age users will often have email archives that go five or even ten years back on their computers. AD eDiscovery actually presents a powerful solution for solving this problem. Analyst can input the records retention rules in the eDiscovery solution and the search the entire enterprise against that criteria. The result will be a comprehensive list of files and users that have violated the records retention rules. The offending files can then either be forcibly removed or brought to the attention of the owner so that they can be appropriately dealt with.

- 3) **Document Holds:** A document hold is an order to preserve documents related to a specific issue. They are often issued prior to litigation, but they can also be issued by regulators and are particularly common in the banking the industry. Investment banks, for example, will issue a document hold order when working on a deal, in order to ensure that all data related to the deal is retained in the event that legal or regulatory issues arise. The problem with document hold orders is that they are subject to all the same issues that records retention rules are. In short, they are communicated typically using an email and people simply ignore them. Even worse, when people are guilty of wrong doing a document hold order can serve as valuable warning to delete potentially incriminating data. The AD eDiscovery solution provides a much better solution to the problem of document holds. Instead of simply issuing an email the company can utilize the AD eDiscovery solution to discover and preserve all of the relevant documents. And because the AD eDiscovery solution is completely automated the search can be performed not just on large numbers of people and machines to ensure that all of the important data is captured.
- 4) **Classified Spillage Incident:** A classified spillage incident is a US government term referring to an incident in which a classified document is found on an unclassified network. When this happens, by law the agency must remove the classified document and then certify that no other instances of it exist on the network. While that may sound easy enough it is in fact an awesome challenge. Effectively what it entails is a keyword search of every machine on the network for the documents containing the classified information. Today most agencies have no way to achieve this type of a comprehensive search and so do their best with manual solutions that focus on a small group of high probability machines. The process is extremely expensive, time consuming, and a partial solution at best. Because what is required is a keyword search of a large number of machines, this is another ideal application for AD eDiscovery. By simply entering relevant keywords in AD eDiscovery and searching the entire network, an analyst can quickly and easily locate all of the reactive documents and certify with a high degree of certainty that the network is truly clean. Using AD eDiscovery the process is quick, easy and comprehensive.
- 5) **IP Protection / Confidential Data Leakage:** In the commercial market there are no classified documents, but there are definitely sensitive documents worth millions and millions of dollars. For companies with sensitive IP these documents might be source code or scientific breakthroughs. For other companies it might be customer information, such as credit card or social security numbers. Regardless of what the sensitive information is, companies need to protect it. The challenge that creates is most companies actually have very little idea where all of their sensitive information is. Because it is so easy to email files around the network, sensitive information that should be protected in a single place, often ends up all over the network. Using AD eDiscovery, a company can easily audit the network using keywords, file hashes or file types, then locate this critical data and take the necessary steps to protect it. This can be a particularly powerful money and time saver for companies that are required by the major credit card companies to certify their networks meet the required PII standards.
- 6) **Policy Audit:** AD eDiscovery is also a powerful solution for companies trying to proactively enforce computer usage policies. For example, it is common for companies to

ban the use of MP3s and peer-to-peer programs on their networks. The problem is it is fairly difficult to enforce those bans. There are of course network-based products and techniques that attempt to detect the use of peer-to-peer products, but they are fairly simple to circumvent. Using AD eDiscovery it is possible to automatically audit the network on a recurring basis to locate all programs and files that match a given set of criteria. In this way, companies can ensure the unauthorized programs or files do not exist on employee workstations.

## SilentRunner®

SilentRunner is AccessData's network forensics product. It records all or selected portions of the network traffic and enables an investigator to piece that traffic back together to determine exactly what was occurring and who was involved. The use cases for this technology are extremely similar to those of AD Enterprise and in fact to gain a full perspective on what is going on, both products should be used together in almost all cases. The simple fact is that only focusing on the data on the host or only focusing on the data on the network doesn't provide the complete picture and can lead to incorrect or incomplete conclusions. By combining host and network data, the investigator has all the information necessary to gain a full appreciation for exactly what transpired and why.

- 1) **Employee Malfeasance:** SilentRunner is commonly used to determine if employee malfeasance has occurred. When an investigator suspects an employee of wrongdoing, SilentRunner can be used to record and investigate all of that user's IP traffic. This capability can be particularly powerful if the employee is using the network to steal information from the employer or to view web content that is inappropriate or unacceptable. In addition, if the employee is a sophisticated user and is using advanced anti-forensics tools to cover their tracks, network traffic can often be the only source of information readily available to the investigator.
- 2) **Malware:** During a malware incident, SilentRunner can be used to quickly determine all of the machines involved. While AD Enterprise can scan the entire network to locate affected machines, utilizing SilentRunner, such a broad scan becomes unnecessary. By placing SilentRunner on the affected network and analyzing the traffic it is often possible to very quickly determine all of the machines involved. This can save time and effort. AD Enterprise can then be used to remediate the processes on the infected machines. This approach is particularly powerful with polymorphic viruses that are more difficult to track utilizing host-based solutions because they are constantly changing.
- 3) **Hacking:** SilentRunner is also a great solution to have during a hacking incident. By putting SilentRunner on a network that is compromised and recording and analyzing the resulting traffic, an investigator can quickly get a complete picture of what a hacker is doing. Here again the synergy between host and network forensics capabilities is incredibly powerful. Utilizing SilentRunner will help an investigator quickly determine what documents were taken and what machines were accessed, but it will not provide all the information that occurred on the host. Likewise, a host-based forensic solution will provide extensive information about what occurred on the host but not necessarily all the information that moved across the network. As a result, combining the two technologies allows an investigator to quickly scope an issue and then fully analyze what is occurring and what has occurred.

## Using AccessData® Lab

AD Lab is AccessData's lab-based forensic solution. The product is designed to address all the major needs of forensic investigators, including the ability to collaborate with each other, as well as with people who are not trained in forensics, and the ability to quickly deal with large cases that have traditionally taken days or even weeks to tackle.

- 1) Collaboration with Legal/HR:** Forensic investigators may be the ones who do the work, but they are rarely the ones that actually requested the investigation. More often than not, the investigation is the result of a request from HR, Legal or some regulator. The result is that the forensic investigator ultimately needs to produce his or her findings to someone who is not trained in forensics. Using AD Lab this is actually extremely easy. The forensic investigator is able to load in the data relevant to a given case, perform whatever forensics operations needed, so that the data is easily consumed (carving unallocated space for example), and then make that data accessible via a simple- to-use web interface. Using the web interface anyone, regardless of their forensic abilities, can search through the data and build their case. The result is the forensic investigator is able to stay focused on issues that require his or her unique abilities, while allowing people in HR or Legal to review the data directly and develop their own conclusions.
- 2) Large Cases – Processing Speeds:** Because AD Lab delivers distributed processing, it allows investigators to utilize a large number of computers to process huge cases in a fraction of the time it would take a single machine. Given the explosive growth in the size of forensic cases, a use case for this capability is not hard to think up. For example, a case involving twenty computers could easily result in the acquisition of several terabytes of data. Without distributed processing it would take several weeks to fully process a case that large. Using distributed process an analyst can tap the power of as many CPUs as needed to process the data as quickly as needed.

## Real-World Application

The following section examines real business problems experienced by real organizations and how those organizations could have utilize AccessData technology to effectively address those challenges.

## Real-World Application Scenarios

### Augment Internal Investigation Procedures

Stand-alone forensic analysis technologies do a very good job as a utility to help analyze information on hard drives. However, what happens if you are an investigator in a large, distributed, networked organization and you need to do an investigation on a system on the other side of the country? Using stand-alone utilities, an investigator would have to fly or drive to the site the hard drive is located, do an investigation in the middle of the night or on the weekend, hoping not to get caught, and then return to his or her lab to do the analysis on that hard drive.

### This poses many challenges to an investigation:

What if the person or system in question works in an environment where doing a covert investigation is a challenge, (eg. A 24-hour call center)?

What does the delay in response time do to your investigation?

What happens if it is a laptop and the person in question takes it home?

What happens if it is a mission-critical server that cannot be taken off line?

What happens if the person in question is using a disk encryption utility that encrypts the volume he is storing the data in when the system is shut down?

Using AD Enterprise, organizations have the ability to analyze systems immediately over the network, covertly, without taking them off line and without incurring any travel-related costs in performing an investigation. By providing an infrastructure that allows for network-enabled, covert, remote investigative capabilities, investigators are now able to investigate far more incidents, in much less time, with far less overhead costs. This enables a great reduction in operational risk while facilitating compliance with Sarbanes-Oxley.

### **Augment HR Exit Strategy to Protect Against IP Theft**

When a company is preparing for a reduction in force (RIF), or an employee voluntarily leaves an organization, a great deal of intellectual property tends to go out the door with those individuals. Many customers are augmenting their employee exit procedures by taking an image of employee hard drives when an RIF is going to happen or an employee tenders his or her resignation. What would the impact be on a technology company if a small group of the development team all resigned at one time, prompting questions from senior management about their departures and what risks that might present?

AccessData Enterprise could be implemented for this purpose and could effectively access the remote hard drives to collect either a full image or logical files so that relevant HR data and intellectual property could be quickly identified. The identification of this data will provide knowledge of who possess the targeted data and where it specifically resides on the individual's devices.

This knowledge of who and where is of extreme importance when responding to the threat of intellectual property theft in a timely manner. Isolating high-risk individuals and quickly identifying on their computers any signs that they transferred sensitive information (eg. documents accessed, USB drives or peer-to-peer applications utilized within a certain time frame, even identifying files that have been printed) is paramount in protecting an organization.

Furthermore, by imaging the hard drives and analyzing the activity of employees *prior* to RIFs or the receipt of resignations, the potential of capturing a great deal of information that would otherwise walk out the door is significantly increased. This approach of proactive information gathering can save organizations millions of dollars by preventing fines due to personal data leakage, the creation of competing products and services, and lost sales. Any organization seeking to protect itself from the theft of intellectual property in the form of customer data will reduce the risk of losing or stalling customer sales or service opportunities. Organizations with critical development and design information will see a significant reduction in the risk of enabling the creation of competing products, services and offerings.

An example of this is a large communications organization that held 50% of the wifi component manufacturing market in 2002. This company was not proactive in the discovery of intellectual property. They, in turn, lost several key employees to various competitors. These competitors were able to quickly develop competing products. These competing products were quickly produced and sold to the wifi device manufacturing market and as of 2005 this company held less than 2% of the wifi component manufacturing market. They have since left the wifi component manufacturing market and are now focused on the RFID component market. Had this company taken a proactive approach to intellectual property information gathering using AccessData Enterprise, they could still be the market leader in wifi products. They are now working with AccessData to develop a strategy for the protection of their valuable intellectual property. This use of AccessData Enterprise could have saved the company untold dollars in future sales, market share and stock price.

## **Internal Policy Compliance**

A company, whose credo states, "creating an atmosphere that people enjoy coming to every day" was disturbed to learn through an email filter that a 20-year senior manager, with an impeccable record, had received inappropriate information via email. The senior manager in question sat on one coast, while the corporate headquarters and IT security team were on the opposite coast. The challenge that the organization faced was how to quickly investigate this person, who has been an outstanding employee for so many years, without making it known to his peer group or others. Unfortunately, they were not able to keep the investigation under wraps, due to their manual investigation methods. In most cases, as in this one, an investigator will go to the actual computer and manually investigate. With this approach, the risk of "exposing" that a valuable employee is the subject of an investigation is very high. This often leads to "water cooler" talk about the subject of the investigation, thus creating a hostile work environment.

AD Enterprise could have been used in this case to triage the data found in the email filter. With AccessData Enterprise, an agent could quickly be pushed to the endpoint to conduct a covert investigation and either validate the email filter or exonerate the individual of wrongdoing. In short, an investigation could have been completed quickly and covertly, protecting the interests of the organization while protecting the privacy and reputation of the investigated employee who was cleared of any wrongdoing. Had AccessData Enterprise been utilized, the subject and his peers would have had no knowledge of the investigation and the creation of a hostile work environment — and a disgruntled employee — could have been avoided.

## **SEC Regulatory Compliance - Insider Trading**

An organization realized that information was being leaked to public blog sites after internal meetings. This type of information can cause serious problems prior to official earnings announcements. It can appear that an insider is creating posts with privileged information in a public arena. This organization could have installed AccessData Enterprise and placed agents on the systems of those in attendance at the meetings where the private information was being released. In total, there could be more than one hundred systems to target, so this level of visibility would be impossible with any traditional forensic tool. The use of AccessData Enterprise in this situation allows the organization to isolate the target system and verify that it was used to post the not yet public data. This age-old problem is not unique, and on several occasions, insiders have posted this type of information to fatten their wallets. Using AD Enterprise, an organization can identify the individual within a matter of hours, issue the appropriate information to the SEC and relieve the individual of his or her duties. The individual will also be obligated to face the SEC for insider trading.

## **IT Security Operations**

Creating a secure IT infrastructure that enables productivity among customers, partners and employees is a growing challenge. There have been many investments made in technology that helps organizations protect against information security breaches — testing how vulnerable the infrastructure is to an attack and detecting when an apparent attack has been attempted. However, there has not been a great deal of investment in resources or technology that helps to determine what actually took place when all the other information security architecture components fail. Please find the following example as a source of education on a growing problem that has occurred at hundreds of large and small organizations both in the public and private sectors:

An organization was targeted by a hacker, possibly a group of hackers that have covered their tracks very well. Using AccessData Enterprise to uncover one system that was obviously breached by an exploit can prove to be extremely valuable in highlighting the specific exploit that was used to breach this system. However, many organizations would stop there. AccessData Enterprise enables IT security personnel to not only identify the exploit, but then expand their search of that exploit to include all systems physically and logically connected to the exploited system. This step is critical to any effective security policy, and AccessData's engineers help

organizations like this one implement such policies to ensure security incidents are resolved thoroughly and lessons learned are applied to prevent the recurrence of that same incident.

AD Enterprise enables IT personnel to effectively interrogate the raw memory and validate the users, ports, process, dlls and open files on every system that is either physically connected to the same LAN segment or logically connected to the exploited system via service, application or software. It is usually the case that when an exploited system is discovered, that system is NOT the only compromised system affected by the breach. There can be dozens of systems compromised. AD Enterprise enables personnel to thoroughly remediate the breach, killing the rogue processes on all affected machines, and patch the systems to remove the potential exploit.

Worms and viruses cost organizations millions of dollars each outbreak. Avoiding or mitigating the effects of such an event provides a tangible benefit to customers in time and dollars saved while maintaining business continuity. AD Enterprise not only enables quick and thorough response once an incident has occurred but it allows organizations to implement a proactive approach that identifies any changes to the volatile data on mission critical systems. This proactive approach proves to be of immeasurable value to organizations looking to mitigate risk, protect information assets and maintain system availability.

### **Proactive Identification of Rogue Processes – Known and Unknown**

By using the capabilities of AD Enterprise, customers can proactively sweep the volatile data of the systems on their network to identify and classify known good, known bad and even unknown processes that are running in their environment.

An organization had the very common opinion that there was no security breach they could not handle. In fact many organizations when asked about the status of it network security replies with something along the lines of, "We have not been penetrated by an attack that we have not identified, responded to and remediated against as far as we know." However, after proactively running AD Enterprise across the environment to interrogate the volatile data of networked systems, this particular organization learned otherwise.

The ability to proactively identify the existence of, for example, FU rootkits within an environment can be of great value in preventing and discovering breaches. Once a rogue application is identified an organization can perform a forensic analysis of the same systems to determine how long this rootkit has resided on those systems. It is very common for an organization to uncover that a system has been unknowingly exploited for periods of more than two years.

Untold amounts of data could have been retrieved from an environment over this lengthy period of time. By proactively sweeping the environment with AD Enterprise, organizations can mitigate operational risk by identifying known bad and even unknown processes (which antivirus tools are not able to detect) and remediating those processes quickly and efficiently.

### **Litigation Support / Electronic Discovery Collection**

A utility company was faced with a discovery motion that was brought against their organization by the SEC. They were mandated to acquire 60 hard drives from 7 different locations throughout the United States within a 3 week period. AccessData Enterprise could have been implemented to allow this organization to covertly acquire the 60 hard drives (20 GB average) across both the LAN and WAN within a few days, all while allowing the CERT team members to stay in their offices working on other projects at hand.

This could not be possible with FTK or any other tool for that matter, within this timeframe. This would have saved the organization a significant amount of time and money.

## **In-House eDiscovery: Beyond Search & Collection**

In an attempt to bring eDiscovery in-house, a large communications company purchased an automated, in-house eDiscovery solution, which took months to implement and even months more to learn how to use. While this automated search and collection tool did a great deal to reduce the amount of data they were pulling back from individuals' workstations, they were not able to use it to view, search and collect from their structured data repositories or email servers. Furthermore, they found that they were limited in their ability to manipulate that data for further refinement and were still experiencing the common logistical issues encountered by non-IT parties who are responsible for the tracking and review of those collections.

This company has now turned to AccessData for an in-house eDiscovery solution. AccessData eDiscovery is far more than a search and collection tool. It is a whole solution that walks users through each phase of the eDiscovery lifecycle, from identification to production. So, in addition to search and collection from custodian computers, AD eDiscovery enables this company to achieve the following:

- Pre-collection assessment/testing
- Smart-target collection/preservation of potentially relevant data from unstructured (workstations/laptops/networks shares) and structured data repositories, such as email servers and document repositories.
- Secondary processing and refinement of collected data using a variety of search options, including concept searching and complex filters
- Horizontal and vertical de-duplication
- Custodian-based, first-pass native review via an easy to use web application
- Real-time tracking of eDiscovery project status
- Load file creation and native file production
- Matter, collection and custodian management

Using AD eDiscovery, the organization is able to see what the results of a collection will be — down to which files are responsive to which keywords — *before* they actually collect the data, ensuring a thorough collection from the beginning. Because AD eDiscovery treats all data equally, this company is able to conduct targeted search and collection from email servers, structured data repositories (e.g. Documentum and SharePoint), as well as individuals' computers and network shares — pulling back only potentially relevant data from all sources. Once the data is collected, the solution automatically processes the data and allows them to further refine the data set through an easy-to-use “first-pass native review” web application. They can fine tune the responsive data via de-duplication, filters, labels and advanced searching from simple keyword to conceptual searches. After refinement, this company will utilize AD eDiscovery to export a responsive-only native-filed data set or generate a load file for export into a popular review tool of their choosing.

Every player in the eDiscovery engagement is able to utilize AD eDiscovery to perform their specific tasks, because the secure, web-based interface is incredibly easy to use and follows a project-based eDiscovery workflow. Paralegals and technical staff can define and track the status of collections, and legal personnel can approve and review the data to facilitate refinement. Collaboration becomes very easy, and the status of various tasks can be tracked and controlled on a granular level. No longer will somebody have to keep a notebook and physically record who was involved in which matters, when they were collected and from where, and what was collected. Furthermore, the solution's ease-of-use also means that this organization doesn't need to waste months training everybody how to use the product.

In addition, since several of their legal matters require data from the same small group of key custodians, AccessData eDiscovery allows litigation support personnel to leverage existing custodian records and mapping (custodian data maps), as well as search criteria, to eliminate having to repeat work they just did on a previous matter. This greatly increases the speed at which they are able to initiate future collections.

Finally, with regard to the company's ongoing litigation matters, this organization will soon be able to schedule ongoing collections over a specified time frame. For example, litigation support personnel can schedule a monthly collection from specified custodians, based on the agreed upon search criteria. This scheduled collection will automatically collect new incremental data each month for the selected time frame — whether that be a year or five years — dramatically reducing their FRCP compliance risk.

When compared to the company's previous automated, in-house eDiscovery technology, AccessData eDiscovery delivered more comprehensive access to both structured and unstructured data across the enterprise, as well as more control over their collected data sets and the eDiscovery process as a whole. The solution was easier to use and walked them through each phase of the eDiscovery engagement in an automated manner. By broadening their targeted collection capabilities to include email servers and structured data, by enabling collaboration among all participants (IT, HR, Legal, Paralegal), and by leveraging a simple interface anybody can use, this organization will increase its time and cost savings well beyond what they achieved with their previous in-house solution.

**To learn more about AccessData solutions, please visit [www.accessdata.com](http://www.accessdata.com)**