



Catelas Relationship Forensics
Solution
For
Early Case Analytics,
Identification
And
Compliance & Security
Monitoring

Contents

Introduction..... 3

Current Approaches, Challenges & Gaps..... 5

How Catelas Relationship Forensics works 7

[1] Catelas Relationship Forensics – Log File Analysis..... 9

[2] Catelas Relationship Forensics – Archive Integration..... 12

[3] Catelas Relationship Forensics – Native File analysis 13

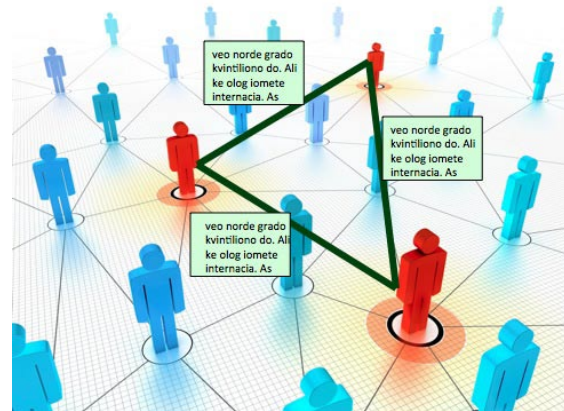
Catelas products for Legal eDiscovery..... 16

Summary of Business Benefits 19

Appendix: Catelas use cases 20

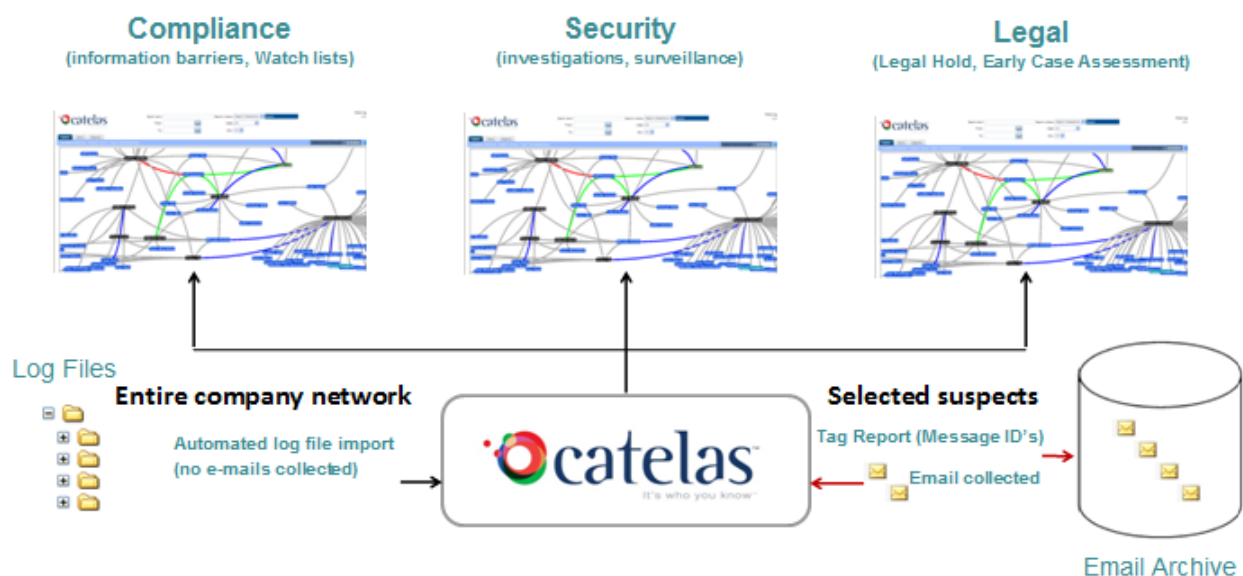
Introduction

Few tools provide visibility into the business practices of a company. Existing solutions focus on what was communicated (content) not on how business gets done (behavior). **'Who' is potentially involved, however, remains the most significant challenge.** Collecting too many custodians increases the cost and complexity of an investigation (30% of the custodians collected are typically peripheral to the issue), while collecting too few increases preservation risk (typically 20% custodians are missed at first pass) while limiting the investigation. Failing to collect the right people means no 'smoking gun' is found.



Only by analyzing every communication in a company not just a sample, can all the right custodians be identified first time; and only by uncovering how business gets done can regulatory risk or anomalous employee behavior (e.g. information theft) be detected and contained. Catelas is the first solution to allow companies to **identify key people & relationships inside and outside the company before collecting a single email.**

With patent-pending technology, Catelas analyzes communications data to automatically display the entire corporate communications network. We do this by leveraging behavioural science & social network analysis algorithms to uncover insights concerning people relationships. Catelas automatically creates networks which clearly and quickly illuminate specific risk factors – information barriers, restricted lists; press & competitor communications, information data theft, FCPA, fraud, anti-trust better serving the needs of Security, Legal & Compliance.



Catelas introduced Relationship Forensics to the market in 2008 and is currently in use by leading financial services companies, technology companies and global consultancies. Catelas is typically used to address the needs of Legal (Identification & Early Case Analytics), Audit (regulatory inquiries, risk assessments), Security (information theft monitoring, investigations) and Compliance (monitoring relationships: FCPA, AML, anti-trust, fraud).

Catelas is currently unique in the market. Deployed in days, Catelas uncovers the entire relationship network of a company globally and displays that network as an easy to use “Google Earth” of the company. Catelas leverages behavioural science and social network analysis to effectively uncover how a company does business, making it easy to identify custodians for preservation and collection, uncover inappropriate relationships (e.g. FCPA), anomalous behaviour (Information theft) or simply to identify the key people in any investigation – ALL WITHOUT COLLECTING A SINGLE EMAIL.

Catelas delivers its technology in three key ways:

Catelas Relationship Forensics (log file analysis) – uncovering the entire global company network

- **Identification** – precise custodian identification, reduction of preservation risk & collection cost
- **Investigations** – quickly uncover the key people and follow their relationships to key evidence
- **Monitoring** – Automated Security & Compliance monitoring reports for high risk behaviour

Catelas Relationship Forensics - Archive Integration

- **Intelligent Collection** – use log files to tag & collect from the archive only what you review/read

Catelas Relationship Forensics (native communications analysis) – investigations & analytics

- **Early Case Analytics** – perform fast case analytics to deliver comprehensive case intelligence
- **Investigations** – PST/NSF native email file analytics for investigations
- **Security Impact Reports** – quickly identify key people, uncover evidence and deliver report

All the current approaches to investigations are data-centric, search based and iterative. Their focus is on collecting large volumes of data and processing/reviewing that data using keywords, concepts or manual review.

Catelas identifies anomalous behaviour indicative of a matter, focuses quickly on the right people, and pinpoints the relevant communications faster and earlier. The Return on Investment gain from deploying Catelas is in the cost savings associated with a more precise and efficient workflow. However, while this justifies the purchase of the software, the true value of the product is reduced reputational, regulatory and legal risk for our clients through an automated and comprehensive analysis of all corporate communications behaviour, precise identification and increased accuracy and speed of investigations.

Whitepaper

Current Approaches, Challenges & Gaps

Current Approach

The current approach for legal eDiscovery, security and compliance is to collect communications and custodian data for analysis. For monitoring, email / communications is sampled and analyzed either using a random sampling approach or using a rules approach based either on keywords or search strings as in DLP systems.

In order to investigate an incident content must be collected and searched; **again much of the success of an investigation depends on correctly identifying all the right people** and finding the right content to review by choosing the correct search terms. This is not always possible.



The Regulatory environment has intensified with fines in FCPA alone having doubled from \$1B to \$2B in the last year. Litigation costs continue to grow as email volumes grow each year, and Information Theft continues to be a problem that is well documented by the press. While many of the current solution set and approaches deliver significant value clearly gaps exist.

Current Challenges

Intelligent Guessing of “Who is involved”

The current approach is a process based upon intelligent guessing to determine the custodian list (who is involved) and keywords (discussed below). This process leads to over-collection, under-preservation and false positives because the initial custodian list includes non-relevant people and omits/overlooks other key people. Investigators and Lawyers often believe that the initial collection is accurate and complete, only to discover much later that additional individuals are identified for collection. Extra, non-relevant custodians cause review to take longer and incur more costs, but these inefficiencies are seen as a necessary evil to avoid overlooking key information.

For international investigations, collection is disruptive, costly, and often made difficult by local privacy laws and foreign languages. Being able to complete the Identification piece before going on site and pulling hard drives is clearly of value.

Process is Driven by Key Words or Random Sampling

Traditional technology solutions either leverage keyword based searches (for culling) or random sampling (1% sampling) to monitor and investigate employee communications. It is now generally

accepted that keyword searching produces far too many false positives that then need to be manually reviewed. On the other hand, random sampling produces far too many false negatives – i.e. the process fails to find anything.

DLP has proven itself successful in this area protecting against PII loss such as credit card information or personal information such as social security numbers of specific tagged records. It has however suffered in the same way as other monitoring tools when it has expanded into monitoring for keywords in email communications.

Analysis & Review tools are heavily dependent on keyword search

eDiscovery tools are meant to reduce the review costs, but they require collection and processing of all the data prior to analysis. Once content is collected for analysis and review, keyword or concept search terms are used to 'organize' and 'prioritize' the data for review by legal counsel. As is well understood, this approach generates large volumes of false positives which need to be reviewed linearly before being excluded. Perhaps more importantly much of the evidence is missed at first pass because the incorrect keywords were chosen. This represents significant risk to the process.

When a user performs a search and is returned 10,000 hits for example, the user must now read all of these. No further 'context' is provided to help eliminate the false positives and focus the user quickly on the right communications.

The Gap

In summary, investigations are silo'ed, and effectiveness downstream is determined by the accuracy of the initial collection or search terms used. Investigations are limited if some of the key people are not identified and collected or if the individuals involved used language the investigators are unfamiliar with. Monitoring solutions fail to identify information theft if none of the known keywords are used or if the 'smoking gun' emails are not included in the sample. This high level of false negatives is hard to quantify but experience tells us that much more theft occurs that can be accounted for. For example:

"78% of US companies have suffered unreported insider-related security breaches"

"59% of employees who leave or are asked to leave are stealing company data"

Source: "Data Loss Risks during Downsizing" by Ponemon Institute LLC, February 23, 2009

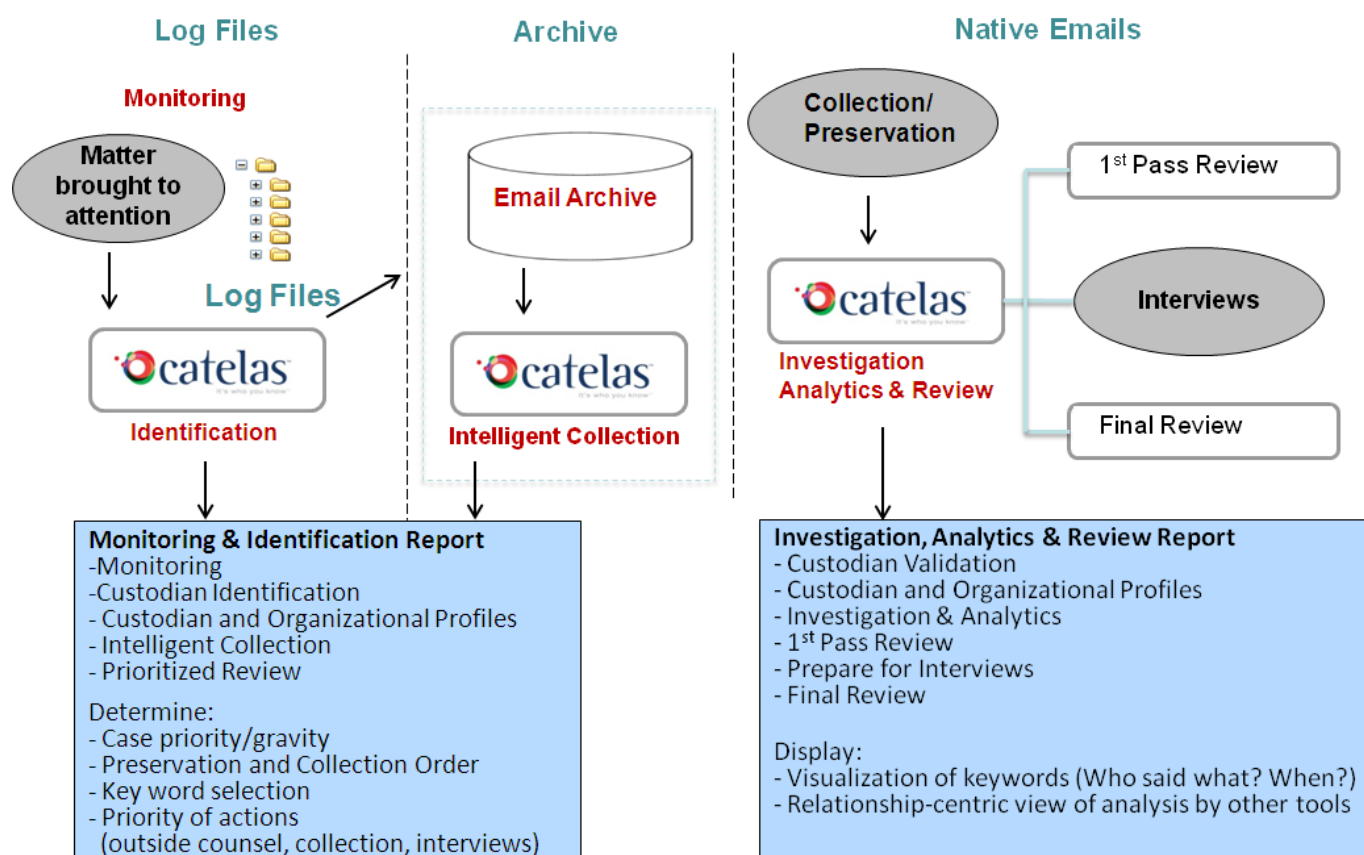
Within Legal, preservation risk is significantly increased when key custodians are not identified and an incomplete legal hold issued – typically 20% of custodians are missed at first pass. On the corollary, eDiscovery costs are typically increased by over 30% by over collection.

How Catelas Relationship Forensics works

The Catelas solution is built on the notion that white collar crime is becoming increasingly sophisticated and that obvious key words (bribes, kickbacks, insider trading) will not be expressly written in email communications. Rather, the approach is behavioural-based, using Relationship Analytics, much the way law enforcement has done for decades. At the outset, Catelas links specific individuals to a crime rather than searching for the smoking gun. Catelas does not analyze the content first, but rather, concentrates on people and relationships first, communications activity second and only reviews content once the relevant people connections have been identified.

By automatically uncovering who is talking to whom, when they connected and how well they know each other, Catelas identifies both the internal and external people most likely involved. Catelas focuses the investigation and collection on the people that matter, saving time and money wasted reviewing irrelevant evidence.

Catelas Workflow: Identification, Monitoring, Intelligent Collection & Investigation



Catelas Identification, Monitoring & Intelligent Collection Workflow

1. Custodian Identification
2. Broad monitoring of traffic to Webmail, press, government entities etc.
3. Intelligent Collection – collect specific emails between custodians to quickly assess the gravity of the case (when available) – insight into key words is also derived from this collection

Catelas Investigation, Analytics & Review Workflow

1. Preservation/Collection completed based upon Identification Report and Intelligent Collection
2. Investigation: identify key people & follow their relationships to key data
3. Generate Catelas Analytics Report:
 - a. Custodian/Organization profiles and interconnections
 - b. Key word visualization
 - c. 1st Pass Review
 - d. Prioritize further review
4. Review – utilize Catelas to complete the review of the collected emails
5. Generate Reports – collect Network Maps and export them for the generation of a final report.
6. Seamless integrations with third party review tools for final review, redaction and production

[1] Catelas Relationship Forensics – Log File Analysis

Catelas log file analysis uncovers the “Google Earth” of the entire global organization and allows the following business value to be delivered to the respective stakeholders:

| Catelas function | Stakeholder | Business impact |
|-----------------------|-----------------------|--|
| Identification | Investigations | Precisely understand who is involved / whose data to collect / who to investigate |
| | Legal | Reduce preservation risk & potential adverse rulings Reduce cost of over-collection |
| Monitoring | Security | Uncover inappropriate high risk relationships with competitors, press or other suspicious entities Uncover information theft to webmail, competitors |
| | Compliance | Uncover regulatory issues, identify risks associated with FCPA, fraud, anti-trust, inappropriate relationships |
| Investigation | Security | Investigate departing employees or audit new employees / contractors within minutes for information theft |
| | Compliance | Uncover regulatory issues, identify risks associated with FCPA, anti-trust, inappropriate relationships |

Monitoring

"Security incidents always come down to people. What they know and who they are telling. The way that Catelas uncovers relationships and visually displays how people are linked together makes them a must-have for any Security Investigations team."

Scott Emery, former Head of Investigations, State Street Bank, November, 2009.

Undiscovered breaches in information barriers, information leakage and the flow of restricted information within and outside the firm is a significant source of regulatory risk.

Catelas is the first solution to comprehensively monitor every single email within and outside the firm, to do so without collecting a single email and without disrupting either the business or IT.

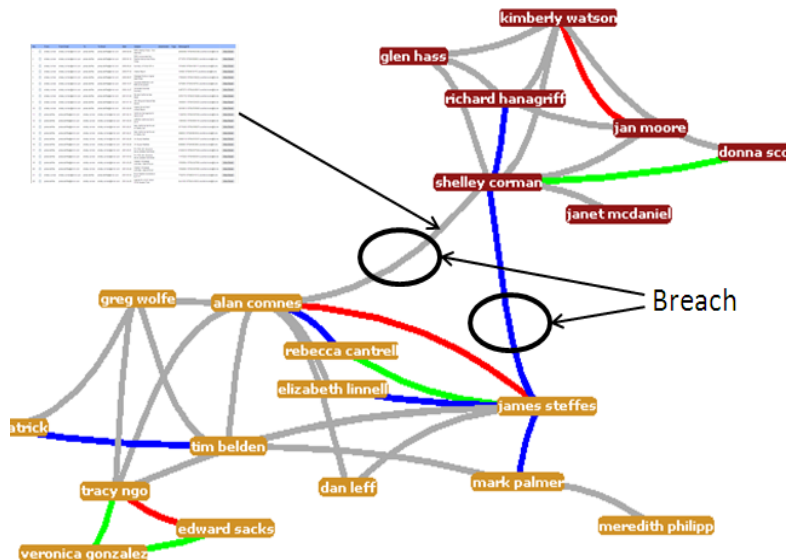
Catelas automatically uncovers who communicated to whom and when, how well people know each other and the levels of activity throughout networks.

Without integrating with any exchange server, Catelas automatically ingests the log files from company exchange servers across globe. The browser-based application can be accessed by authorized resources anywhere in the world. Catelas provides a comprehensive view across each region from a single user interface, enabling a monitoring or identification report on day 1, hour 1 of any investigation.

The log file analysis is exhaustive and uncovers all current relationships within company, between groups and out to partners, clients and external organizations. It is a complete and comprehensive view of how company does business and as such is a perfect solution for addressing the Monitoring & Identification problem.

More specifically Catelas can:

1. **Monitor** all communications to webmail, competitors or suspicious entities. Identify **anomalous behaviour associated with information theft** and identify candidates for deeper investigation.
2. **Always-on visibility of entire network:** conduct investigations over the entire company people network on known or impending matters immediately, within minutes, without the cost and time lost collecting email and supporting data
3. **Information Theft Audits:** audit the activity and behaviour of new and departing employees for inappropriate relationships, theft of important information (software code or trading strategies) or broadly across the entire company for information flow to competitors, webmail or the press.



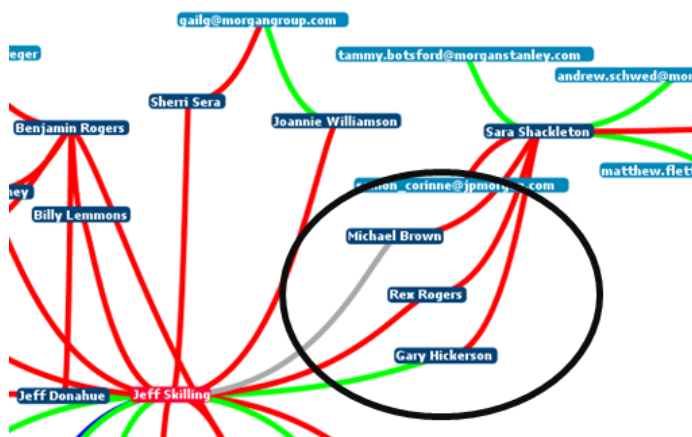
4. **Audits and Compliance:** proactively monitor & investigate entire company people network for communications compliance and specific high risk areas such as FCPA, anti-trust and privacy
5. **Information Barriers:** visually displays the communication networks between business silos / groups, merchants in any country without collecting email, allowing inappropriate or suspicious relationships to be identified.

Companies already leverage advanced DLP solutions to monitor for information theft, privacy breaches and fraud; now using Catelas, companies can monitor the people activity & relationships around those same topics and identify the missed events.

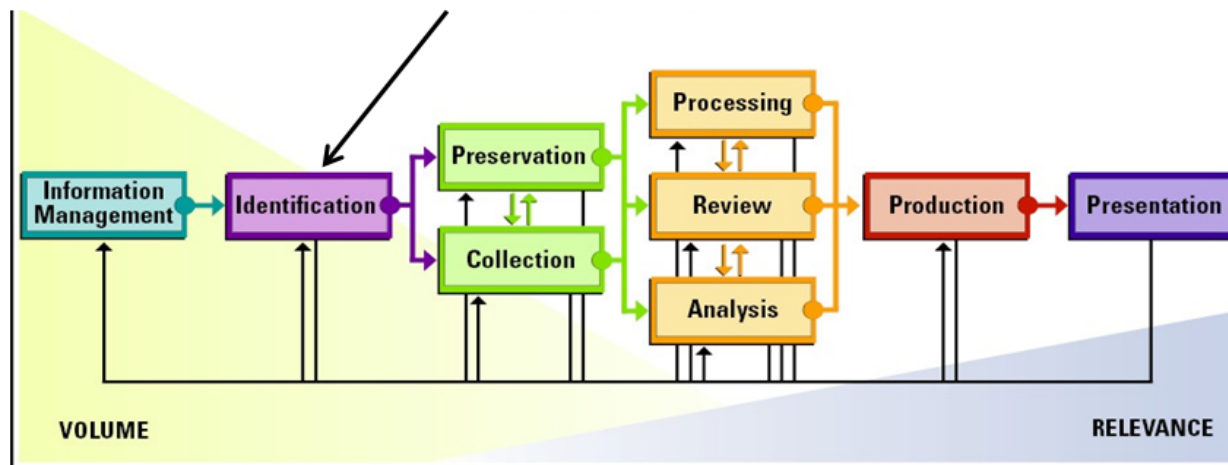
Custodian Identification and Investigation

Log File Analysis enables Catelas to understand both *who knows who, how well and when connections were active* **BEFORE a single email is ever collected.**

- ✓ **Identification:** identify key custodians (and new custodians not previously considered) in a particular matter before collection; avoid under-preservation and subsequent spoliation
- ✓ **Prioritize Cases & perform preliminary investigation** prior to involving IT & collection; determine the scope, cost and risk associated with a matter before assigning resources
- ✓ **Resolve cases** – analysis of custodian and organizational profiles may support discontinuing investigation into a particular matter



Identification & Intelligent Collection (before collection: Log File Analysis)



[2] Catelas Relationship Forensics – Archive Integration

| Catelas function | Stakeholder | Business impact |
|-------------------------------|--|--|
| Intelligent Collection | Legal Security Compliance | Precise email collection directly from Archive Communications data tagged in Catelas (log file) is loaded directly from Archive. Directly review 1% of the content identified by Catelas (log files) Analytics |

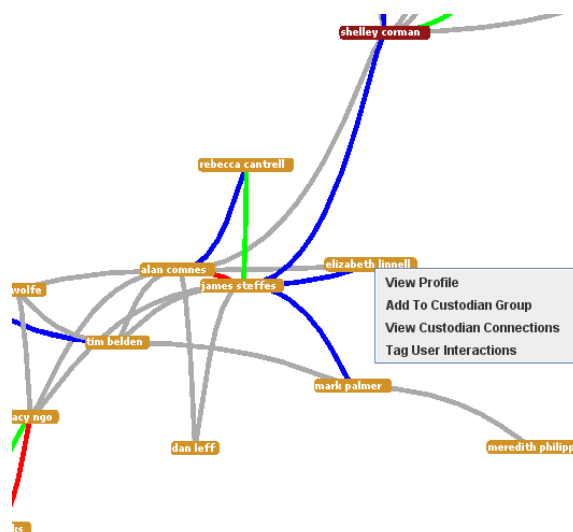
Catelas Intelligent Collection

Once all custodians and key people have been identified within Catelas, their communications can be tagged and Catelas can issue an API call to an underlying archive to retrieve the relevant communications, cross referenced with a unique message ID. Only the relevant emails are loaded and reviewed by investigators rather than each custodian's entire pst files. The Intelligent Collection process is simple, focused and fast and does not involve IT in time consuming collections.

Given only a small fraction (a few percent) of the custodian emails are ever collected, Catelas Intelligent Collection saves company considerable costs in terms of IT time, investigator travel time/cost and, of course, significantly reduces the amount of content that needs to be collected, loaded, searched, and reviewed.

Catelas greatly enhances the benefit of the archive by providing a relationship-based overlay – a virtual table of contents for the archive.

- ✓ **Pinpoint specific custodian communications** for immediate review
- ✓ **Complete investigation within days** – by only collecting precisely what is needed (typically 1%), the investigative process can be completed in days
- ✓ A **“preliminary review”** is concluded within a day vs. today's process that can take weeks
- ✓ Investigations can be completed **without large collections** from the archives (complete custodian psts and key word-based collections)



[3] Catelas Relationship Forensics – Native File analysis

Catelas can import and process a wide variety of native communications such as email, IM & telephony and can also import communications data which has already been processed by other tools such as Clearwell, Autonomy etc..

| Catelas function | Stakeholder | Business impact |
|--|-----------------------|---|
| Investigations & Early Case Analytics | Legal | Early Case Analytics reports Full Analytics & Case Review in a fraction of the time |
| | Investigations | Conduct Investigations in less time Identify key people and relationships; Eliminate unnecessary people / Identify missing ones first time Deliver Investigation reports |
| Network wide Relationship & Behavioral analysis | Legal | Visualize Information Flow within company and between external entities |
| | Security | Identify those people in ‘dialog’ |
| | Compliance | “who spoke to whom about what” : search archives for certain topics, load that content into Catelas and visualize information flow and who specifically was in dialog about those topics |

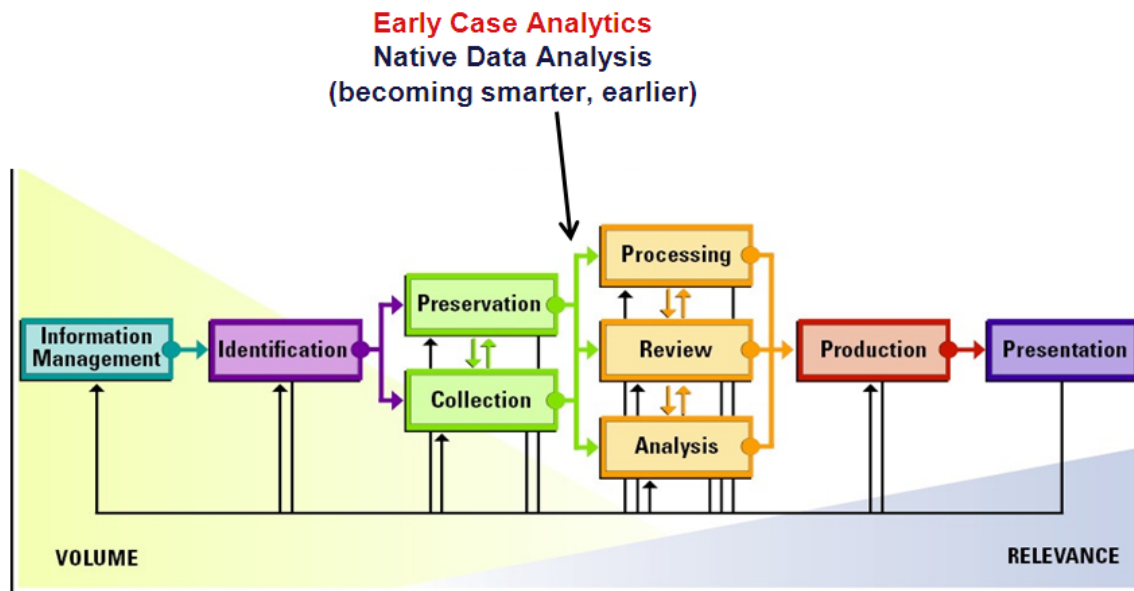
Catelas provides a relationship-centric perspective for performing analysis and review. Catelas network maps serve as a table of contents for large communications datasets. The color-coded visualizations allow users to quickly navigate to the most relevant communications saving valuable time and reducing investigative costs per matter.

Seeing how information flows in a network (who spoke to whom about what – one way communication) and seeing who works/interacts with whom (who is in dialog – two-way communications) helps the investigator quickly understand that nature of the relationships that exist between company and its partners, clients and other internal employees. Additionally, it is easy to understand where sensitive information may flow by looking for the interactivity between people with strong relationships.

Catelas Relationship Forensics illuminates and categorizes relationships, enabling the investigator to follow those relationships to relevant data – a consistently more effective way of finding evidence than inefficient key word searches.

Investigations & Early Case Analytics

Catelas is used within the Process/Review/Analysis stack and quickly imports large volumes of communications content (native psts / nsfs), IM or other forms of data communications.



What it does for you:

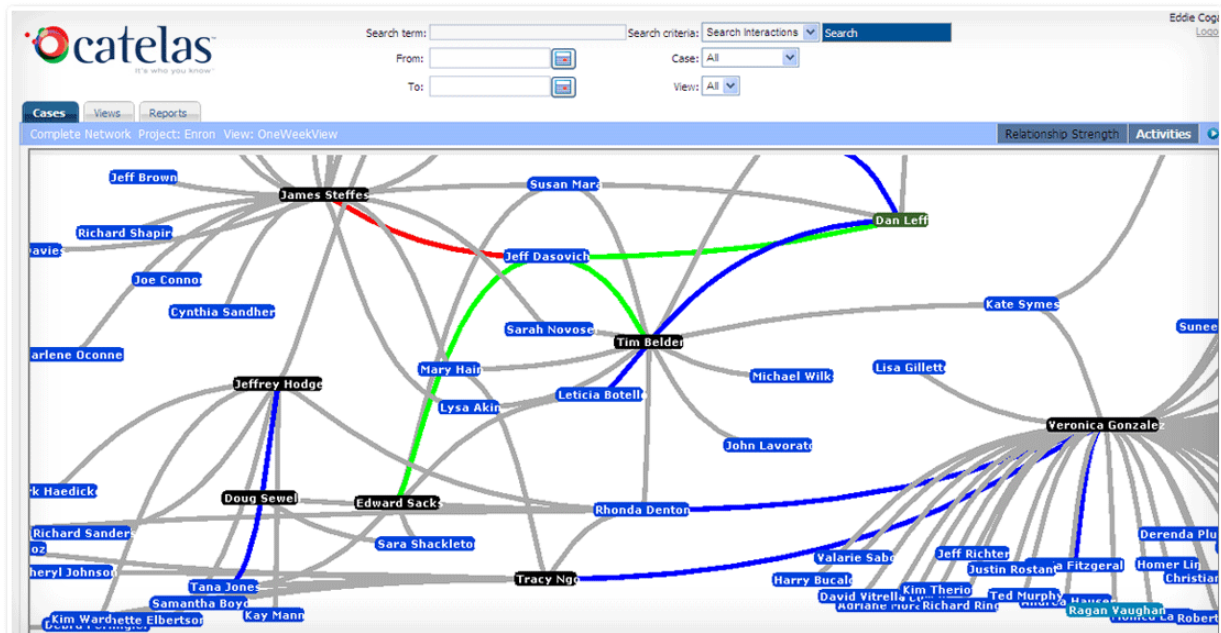
- **Investigations:** quickly determine the liability associated with a case. Perform risk analysis across entire matter portfolio or limit to high risk matters
- **Early Case Analytics:** provide supporting evidence for case strategy immediately when matter arises. Determine quickly how best to proceed (early dismissal, settlement negotiations)
- **Custodian Validation:** At first pass, validate initial list of custodians and identify missing or non-obvious custodians. Eliminate or de-prioritize those custodians clearly not involved and save \$100,000 per custodian per matter. Avoid over-collection.

Some of the benefits are:

- **Faster more precise investigations:** by identifying the right people upfront and subsequently tagging only the most relevant communications, typically less than 1% of the corpus is presented for preliminary investigation, enabling more informed decisions to be made earlier. Less content and more of the right content is selected for review
- **Cost predictability:** identify the precise scope and volume of data to be collected, processed and reviewed; reduce the number of collection/review iterations and allocate predictable costs

Network wide Relationship & Behavioral analysis

- **Visualize communications maps:** load precise keyword culled content or map search results immediately visualizing the networks of 'who spoke to whom about what'



Catelas products for Legal eDiscovery

| Product | Business Benefits |
|---------------------------------------|---|
| Catelas Identification | <ol style="list-style-type: none"> 1. Eliminate unnecessary custodians 2. Identify missing custodians first time 3. focus investigation from start |
| Catelas Early Case Analytics | <ol style="list-style-type: none"> 1.Reduce cost & time lost through travel 2.Increase collaboration; data is hosted and accessed by all 3.Locate relevant content in less time; complete investigation faster |
| Catelas Intelligent Collection | <ol style="list-style-type: none"> 1. Eliminate collection 2. Retrieve emails directly from Archive |

Catelas (log files): Identification

What it is:

Catelas automatically ingests the log files from the company's exchange servers across the entire organization. The browser-based application can be accessed by authorized resources anywhere in the world. Catelas provides a comprehensive view across each region from a single user interface, enabling an identification report on day 1, hour 1 of any investigation. This report provides supporting analysis for identifying, prioritizing and removing custodians from the custodian list before any content is collected or any investigator travels by plane.

The Business Benefits

Currently, the custodian list is drawn up manually based on the roles and org chart position of the people considered to be most probably involved. In typical matters, it has been found that about 20% of relevant custodians were missed and about 30% of those custodians initially listed were not highly relevant so could be de-prioritized or eliminated (depends on matter).

The log file analysis is exhaustive and uncovers all current relationships within the organization, between groups and out to partners, clients and external organizations. It is a complete and comprehensive view of how the company does business and as such is a perfect solution for addressing the Identification problem.

The Identification piece can be completed in hours from any location by any authorized personnel prior to both collection and translation, without losing time through travel. Additionally, there is no longer any need to reach out to the local office to build the custodian list – such actions raise a red flag in the local office that an investigation is active; become disruptive to the business and can spoil subsequent interviews.

Identification becomes faster, exhaustive & complete, first time and by providing prompt investigative focus saves the company money downstream on collection & review costs.

Catelas (pst files): Early Case Analytics

What it is:

Catelas provides a relationship-centric perspective for performing analysis and review. Catelas network maps serve as a table of contents for large communications datasets. The color-coded visualizations allow users to quickly navigate to the most relevant communications saving valuable time and reducing review costs per case.

Seeing how information flows in a network (who spoke to whom about what – one way communication) and seeing who works/interacts with whom (who is in dialog – two-way communications) helps the investigator quickly understand that nature of the relationships that exist between the company and its partners, clients and other internal employees. Additionally, it is easy to understand where sensitive information may flow by looking for the interactivity between people with strong relationships.

Catelas Relationship Forensics illuminates and categorizes relationships, enabling the investigator to follow those relationships to relevant data – a consistently more effective way of finding evidence than inefficient key word searches.

The Business Benefits

The following benefits can be enjoyed:

1. Catelas allows the user to visualize search results in a single network view. Today, when a dataset is searched all the results must be reviewed linearly as there is no way to understand which of the many thousands of results is most important. By displaying the search results as a network, Catelas allows the investigator to quickly discern which communications are relevant for review. The investigator can complete a non-linear review in a fraction of the time of a traditional linear review where all results are considered equal.
2. By displaying networks between custodians and key people in a single view allows the investigator to tag all the communications of importance in one pass, allowing the important communications to be filtered out of the dataset and reviewed in record time.
3. With Catelas, investigators can collaborate on case work simultaneously, enabling a more dynamic resource model to be used, while maintaining a prioritized, big picture perspective of the case
4. Catelas can be integrated with third party review tools, allowing all communications reviewed and tagged in Catelas to also be visible in that review tool for final review, redaction and production.

Catelas Early Case Analytics software is sold on a per case and enterprise licensing basis.

Whitepaper

Catelas (log files): Intelligent Collection

What it is:

Once all custodians and key people have been identified within Catelas, their communications can be tagged and Catelas can issue an API call to an underlying archive to retrieve the relevant communications in Catelas. This end to end process links the log files and the native email analysis pieces with a fully automated single process. Only the relevant emails are loaded and reviewed rather than each custodian's entire pst files as is the current process. The Intelligent Collection process is simple, focused, fast and does not involve IT. Again no local staff is alerted and investigative resources no longer need to go on site to collect and review data.

The Business Benefits

Given only a small fraction (a few percent) of the custodian emails are ever collected, Catelas Intelligent Collection saves the company considerable costs in terms of IT time, investigator travel time/cost and, of course, significantly reduces the amount of content that needs to be collected, loaded, searched, and reviewed.

Summary of Business Benefits

Catelas dramatically impacts investigation efforts in addition to providing a broad company-wide proactive monitoring, surveillance and Identification solution. This new approach is automated, always-on and allows investigations to be conducted in a few hours - using email log files, before having to collect native emails and once collected allowing rapid analysis of the native communications.

| Catelas function | Benefit | Business impact |
|--------------------------------|---|---|
| Identification | Identify key people BEFORE a single email is collected. 1. Reduce preservation risk 2. Reduce over-collection costs 3. Focus downstream review | Identify who is involved and who is important; validate precisely who should be subject to preservation and what custodians identified for collection. Ensure downstream investigative & review efforts are looking at right people, right data |
| Monitoring | Pro-active, 'always-on' visibility of entire company email network. Fill the gap left by DLP & random sampling | Monitor entire company for anomalous behavior, information theft, compliance breaches and automatically generate weekly reports |
| Intelligent Collection | Precise email collection directly from Archive | Communications data tagged in Catelas (log file) is loaded directly from Archive. Directly review 1% of the content identified by Catelas (log files) Analytics |
| Investigations | Smarter, faster, more focused investigations | Any suspicious activity or incident can be investigated immediately, within minutes |
| Early Case Analytics | Within 24 hours of data load generate an Early Case Analytics report detailing the evidentiary basis of the matter | Rapid relationship and data analysis enable a top down investigative approach similar to law enforcement. Relationships navigate the investigator to the 'smoking gun' without the need for keyword searching |
| Security Impact Reports | Automated and customized security reports. Automatically understand WHAT & WHO to investigate with other deep dive network investigative solutions e.g. Netwitness etc. | Weekly reports track emails to competitors, press and personal webmail accounts, departing employees or anomalous behavior |

Whitepaper

Appendix: Catelas use cases

FCPA investigation

Our client is in the international commodity trading business and was subject to regulatory investigation. Already four traders were under formal investigation and it was believed that certain illegal practices were widespread.

The Catelas Early Case Analytics report that was generated quickly uncovered the risk associated with this matter and guided General Counsel as to the best approach to take with respect to the regulators. By fully understanding the severity of the issue, our client was able to seek early resolution with the regulators and we believe the penalties imposed were significantly lower as a result. Catelas is now being deployed as an always-on Compliance surveillance solution to monitor the client's global communications network (inside and outside the company) for suspicious trading relationships.

Business impact: cost savings were not disclosed (believed to be significant), but the matter was resolved promptly, there was minimal PR exposure and procedures were put in place to monitor compliance going forward.

IP theft

Our client needed to prove that a competitor's product originated in their IP. Data was collected from the target company based on a mutually agreed custodian list. This list was analysed using keywords based on the product and its market but nothing was discovered.

Catelas was brought in and analysed the same data and began to uncover who were the key people that connected to the original custodians (all were executives of the target company). The Catelas report was used to request further data from these new individuals; this uncovered a network of people many layers down the target company (involved in R & D, new product development and marketing) who would typically never have been considered for depositions. This data was then analysed and reviewed within Catelas and yielded much information about this case and other ongoing cases.

Business impact: had Catelas been used from the outset, discovery cost savings were anticipated to be in the region of \$1M, but importantly the right data (and people) would have been requested from opposing counsel at the outset.

Product Liability

A manufacturing client was sued as part of a class action lawsuit where the claimants sought damages associated with a faulty product that led to serious health issues in some cases. The claim stated that the manufacturer knew of these health risks but failed to act responsibly.

Our client needed to reconstruct the communications chain with regard to the manufacturing defects which led to the hazard. Catelas was used to uncover the communications network that illustrated how

Whitepaper

the manufacturer connected with its supply chain across 3 continents and its distribution channel across the US.

Catelas was able to quickly uncover the information flow from the relevant parties illustrating how information about product quality issues flowed from suppliers through the company and then out into the distribution channels. This illustrated how product issues was reported, reviewed and how decisions were made within the company and out to its network of suppliers and distributors. While this did illustrate a disconnect in communications between marketing and manufacturing, it also clearly re-enforced the company's claim that it did not have prior knowledge of the defects nor did the company choose to ignore the health effects of such issues.

Fraud

The client worked in the consumer telecoms reseller space. A competitor began to gain significant market share over the incumbent using fraudulent marketing techniques. While the evidence was clear, and an injunction was granted against the competitor and the marketing efforts stopped, it was not possible to prove that what happened was intentional as opposed to an error & omission. After 18 months of investigation and many millions spent on the case, the client had failed to prove fraud and the judge began to refuse further depositions.

Catelas was able to quickly take the data collected so far and link all 7 companies involved in the case and immediately highlighted 3 people who were non-obvious but who were clearly at the centre. This allowed the client to seek new depositions and request further data based on the reasoned argument provided by the Catelas report.

Trade Exchange

Catelas is currently exploring our application within Trade Exchange. We are working with a large Asian bank where 40% of their international business is trade finance. Trade Finance is coming under increasing regulatory scrutiny because of the Money Laundering and Terrorist opportunities associated with such business.

In this case, Catelas integrates email communications with transactional data found in databases. The intent here is both to be able to cut the costs and save time responding to the increasing demands from the regulators and to better ascertain the risk exposure of the bank to these illegal activities.

Employment

The client is a major financial services organisation which is being restructured whilst supported by government funding. During this time of change a large number of employees are leaving the company. Catelas is being used to investigate whether:

1. information theft has occurred – 59% of all people who leave a company take company information with them
2. breach of contract primarily with respect to working for 2 companies

3. collaborating with competitors

The typical case size is 1 to 17 custodians. The benefits achieved (which the client is happy to be quoted on) are a reduction in time to investigate each case from over 3 weeks to a few hours – a gain of 90%. As important, however, is the ability of the Chief Risk Officer & Corporate Counsel to both stem the flow of information theft and to quickly ascertain risks by business unit and apply corrective measures.