# APF Information Protection and Access Control (IPAC) Solution User Case for Financial Firms Compliance and E-Surveillance

Research analysts play an important role in the relationship between companies and investors, both retail and institutional. Research analysts study companies and industries, analyze the disparate raw data, and often make forecasts and recommendations about whether to buy, sell or hold securities. Investors often view analysts as experts on and important sources of information about the securities they cover and rely on their advice. However, analysts (also referred to in this Report as securities analysts or sell-side analysts) employed by full-service investment firms often face conflicts of interest that can interfere with the objectivity of their analysis. Conflicts arise because these firms ("firms" means in this Report full-service investment firms unless otherwise stated) often undertake many, potentially conflicting, roles – for example, firms may act as retail brokerage houses for individuals wishing to purchase or sell securities, while at the same time offering underwriting services to issuers of those securities – and research analysts are often called upon to assist with these conflicting activities. If an analyst's firm's activities place the analyst in conflict situations – for example, if the analyst has powerful financial incentives to direct clients towards specific securities, or if the analyst's job security depends on dissuading clients from selling certain shares – the advice the analyst offers may no longer be objective.

Current regulation for the firms that has both buy side brokerage and cell side analysis to ensure the separation of information flow between the 2 sides. Firms has already in place e-surveillance program that monitors employee's communications via email or chat channels. The email and chat messages are also being achieved for several years so it can be searched and verified. But the issue information sharing can be also be done through documents, which can be shared without going through the email or chat that are being monitored. A cloud storage can be used and the activity will not be monitored and reported. Given the documents being primary tools of information exchange, it is a significant loophole in current e-surveillance process.

APF Information Protection and Access Control (IPAC) is created to close this loophole with many other benefits. IPAC uses centralized access policy to control who can access what file at when and records every access attempt by anyone to any protected files. It allows company to build virtual wall between sell-side and buy-side teams to block the sharing. It also maintains the record that can be used to satisfy prove of regulatory compliances.

## Information flow management and access control

IPAC's access policy can be used to enforce the separation of information flow in a timely fashion. The access policies is set company wide and can be changed only by authorized team. It affect all the files that fits the policy condition not matter where the file being stored or accessed. This gives the company the highest level of confidence that information access in being controlled and audited.

## Audit Records

With IPAC, every access to the documents and every change that could impact the access of the documents are recorded and audited. Externally, this provide the firm with the data to confidently satisfy client's demand to audit the access of their information. The data is feed into advanced artificial intelligence analytic tool to detect early signs of possible breaches so preventive measures can be taken internally, as well as to better understand the team performance.

## Protection for every document anywhere at all time

With IPAC, documents are protected by the strongest encryption at all time no matter if they are stored on backend servers, cloud storage, personal laptops or mobile devices. No documents will be stored plainly - anywhere.

Rest assured, IPAC's protection doesn't compromise productivity and the information flow. The protected document can be shared through email, shared cloud storage. Although document flow remains the same, the access to the content, however, is subject to IPAC's access control to further limit the exposure of the information.

## Document life cycle management

In today's connected world, managing documents life cycle is more challenging than ever. Documents can easily be shared, copied and stored anywhere, so to truly remove a time sensitive document is a difficult task if plausible at all. IPAC provide 2 ways to handle the task properly. First, it allows access policies to temporally disable access to the content after a set date. Reversing the policy would reverse the access control and allow the documents to be viewed again. Second, IPAC digit "shred" the document to permanently prevent the content of the document to be accessed, regardless of the number and location of the copies exists.

## Meta data management

IPAC protects the contents of document so those document will not be exposed to any internal search engine, which is potentially security volubility. To make the protected document reachable, IPAC provide effective Meta data management for the protected document. The Meta data of protected document has a description, tag and version, so the protected documents can be categorized and searchable.

IPAC is the cyber security solution that gives the firm the confidence of knowing their information and reputation are being protected to their best capability and no less.