A Better Protection and More: APF Information Protection and Access Control Solution (IPAC)

In today's uncertain world, predicting and preventing worst-case situations is essential. APF's IPAC is designed to make that reality.

As the First of its kind, the IPAC levels advancement of the big data technology to give the company total control of the information flow and unprecedented visibility into information consumption by individuals, while ensure the information are fully protected against out invasions as well inside misuses. It plugs a few loopholes that exist in most company's security system including:

1. Admin users has unrestricted access. Once it is compromised, the damage could be extremely severe
2. Once an individual is allowed to access files, they can get hold of those for life with a local copy.
3. With today's file sharing technology, there is no sure way to always find out when a file was accessed and by who in real time, or who owns a copy of file.
4. There is no easy way to determine if an individual's behaviors is deviating from the historic norm and take preventive action, when it comes down to information access, since they can always have a copy of the files on their own storage.
5. The laptops has too many plain files and once it is hacked, all the information on the computers is prone to be taken.

IPAC protects the files through strong encryption with different keys for each file. If hacker get one key, he could open exactly one file, and that is only if he also possess the encrypted file. Without the keys, the gigabytes of files is just gigabytes of random bits. The keys are centrally managed. A request for the key is evaluated against access policy to determine if the request will be given access. Those access policies are also centrally managed in align with organization's information governing policies. With IPAC, to access a protected file requires the user to 1) has APF client manager software, 2) valid account with IPAC, 3) have access to the protected files and 4) has permission to access the file by the access policy. Malwares and vires like X-agent won't be able to access any protected files with APF manager even if it get the account password because the APF manager is GUI driven and no command line access.

Another advanced design of APF's IPAC is that it allows Admin to manage the physical file as well as the file properties, but it doesn't give admin the access to the information the file contains. If Admin want to access the content of a protected file, he still need to go through access policy evaluation.

Not only the APF IPAC protects against outside invasion, but it also prevents internal misuses. The access policy is designed to allow only those personal who need the information for their work will have access, and their access will be changed as they change their role, or revoked as soon as they leave the

organization. The change take effect on all protected file, even those in their possession. The continuation of monitoring for unusual behave can be enabled with big data analysis option. It can monitor and alert in real time of any individual who behaviors is deviating from the historic norm.

The benefits from having IPAC can be game changer for many organizations

1. There will be no more plain files with your company's confidential information on any employee laptop or mobile device, so you can be sure that when your employee connects to a public Wi-Fi hotspot, the potential discovery and damage to your files will be nearly eliminated - though the chances of being hacked or infected by a virus remain the same.
2. Now, you can afford a few mistakes made by employees accidentally exposing confidential files to the unintended audience or public, through cloud storage like AWS or dropped or stolen USB drives, because without APF authorization, those files are just random bits.
3. You won't have to worry about the confidential information ending up in the hands of your competitors because they won't be able to read them.
4. No employee will have any excuses to keep plain files that contain the company's confidential information in their possession.
5. When an employee leaves the company, they won't be able to carry the company's confidential information with them.
6. Confidential information no longer needs to be accessed by individuals who don't need to, such as your IT team. They still can access and manage the files, just not the information they contain.
7. Above all, the information access is controlled by the central server and is in alignment with the company's governing policy, to meet any government or regulatory requirement.
8. The work flow for most employees is simplified to two buttons: open and create.