



SHARE DIGITAL ASSETS AND DATA WITH NO RISK OF LEAKS OR LOSS

The protection of vital Digital Asset Data is becoming more complex and the costs are continually increasing. Law Firms are looking for ways to securely control all their critical digital data assets both within existing installed systems (File Management Systems, Case Management Systems, Billing Systems, Data Collection Systems, ETC) and outside these still being able to efficiently, effectively and seamlessly share this data as and where required - both inside and outside the firm, without risk and still ensuring they meet their compliance, regulatory and confidentiality requirements - a very difficult task.

Softtection Inc. has developed its Digital Asset Protection (DAP) software solution to truly protect and manage an organization's electronic data. Unlike other security products that are typically defensive or passive, Softtection's technology provides active security; data is prevented from being manipulated by unauthorized people in *real time*. Softtection controls data at the individual file or item level, for a specific application, by individual user and by individual device.

Digital Asset and Data access breaches or losses, whether malicious or accidental, are now more common place and are becoming more costly and can interfere with the integrity or even the success of a case. Notwithstanding the financial liability of a data security breach the damage to the reputation of a firm may be irreparable. Softtection is designed to address these issues and much more.

This article describes how Softtection DAP Solution can be used to secure multiple digital data assets types and sources quickly, completely and in a cost effective and totally reliable, controlled and audited manner. Existing applications and system security features often leave many gaps leaving a number of technical hurdles to overcome, that are often the most common areas of weakness.

Below are a number of key ways that digital asset data can leak. All of them dangerous regardless of the intent of users:

1. Cut and Paste to another application
2. Printing
3. Screenshot
4. Emailing data as an attachment
5. Accessing data outside an application (or on another machine)
6. Kernel Sniffer/Memory Dump

Patching all the possible security loop holes requires significant time and investment and is extremely complex. In order to properly secure against the above and many other threats, this can only really be achieved by the use of low level kernel code. Softection provides this low level code and its capabilities for integration with vital internal third party systems that firms may be using e.g. SAP, Exchange, Oracle and more, offer the complete Digital Asset Data Protection solution firms need in a timely and flexible manner. Softection protects against all of these weaknesses and more.

In addition, Softection DAP provides effective and controlled information barriers between internal groups such as HR, finance, or upper management, plus the IT department, as well as external sharing groups such as advisors, clients etc, all without significant impact on the users. By using the DAP Information Barriers, any confidential corporate data can be identified as a Digital Asset and hence totally protected without format or application change. This Digital Asset can then be shared and worked on by authorized users or groups as needed. The Digital Asset Server then manages the files in encrypted form with obfuscated names.

Integrating your installed systems and applications with Softection provides you the additional security of knowing that whoever accesses the data you have effectively:

- Stopped deliberate or accidental data leakage
- Controlled how Data is used or shared
- Logged any and all access to secure data
- Logged any and all operations (open, copy, edit) on secure data
- Tracked where Digital Assets exist within your firm

By securing only via a third party system or application, the related digital data can generally only be secured within the confines of that application, however, some of the data can or needs to often be accessed outside that application, introducing many additional data integrity weaknesses and security issues that the application cannot handle. A good Data Protection solution should secure the data itself, causing any attempts to access the information by any other application, to result in the data being defended and this is what Softection does. More importantly, attempts to access, modify, or copy these secured data files are logged and audited by Softection. This happens regardless of whether or not the primary application or system is running, so attempts to access data from outside or non authorized users will be stopped and the digital data remains totally secured and those attempts will be logged, thus providing a full audit trail on the data.

Also, if the primary application or subsequent systems exports data to other well known formats (PDF, DOC, and HTML etc), Softection can still protect those files as well as the

digital data within them. Policies can be established to inherit the permissions given to the original applications digital data, hence, extending the security model on more accurately and effectively. In addition, any Digital Asset that is being tracked by Softection can be encrypted plus if a user tries to copy data to an external drive or CD, or if they remove the hard disk and place it into another computer, the digital data will still remain protected by encryption, security policies and by external device controls and management utilities USB drives, PDAs, iPods, CDs, Laptops or even email. This means that application data will stay secure regardless of location. It can even be used to destroy the digital data if the policies for a digital asset are not satisfied. Also, in many cases, a deleted file still physically exists on a hard drive as 1s and 0s. Tools exist to recover this data in its raw form. Again, Softection meets the challenge; it has built in sanitization procedures which wipe data to the US Department of Defense standards. This means that deleted data is not recoverable, even by forensic methods – hence the security life cycle is completed.

I-Quest is the sole distributor of DAP from Softection in the UK and Ireland.

For more information on how to integrate your application or system with DAP, please contact: Kevin Mackay Kevin.mackay@i-questltd.com Office: 0207 902 1970 or Mobile: 07958 708848 or Chris Prier chris.prier@i-questltd.com Mobile: 07766 910013