



The Value of an Embedded Data Protection Solution

Integration with Digital Asset Protection





The Value of an Embedded Data Protection Solution

Integration with Digital Asset Protection

Overview

Protecting data is increasingly important. Application Developers are finding that customers are looking for ways to secure the data within their applications. Data breaches, whether malicious or accidental, can be very costly and can interfere with business continuity.

This White Paper describes how Digital Asset Protection (DAP) by Softection can be used to secure your application quickly, completely, and in a cost effective manner. If you are aiming to implement or augment the security features within your own application, you will be confronted with a number of technical hurdles. You will see how integrating with DAP to provide security for your application can address these issues.

There are 6 key ways that data can be leaked. Most of these can be dangerous regardless of the intent of users:

- I. Cut and Paste to another application
- II. Printing
- III. Screenshot
- IV. Emailing data as an attachment
- V. Accessing data outside an application (or on another machine)
- VI. Kernel Sniffer/Memory Dump

Patching all possible security holes requires significant time and investment for Application Developers. To properly secure against the above threats, low level kernel code is required. This is time consuming to develop and test. Your developers can be more effectively deployed developing your core product. Integrating with DAP for application & data protection provides a well tested, secure, and timely solution.

Integrating your application with DAP provides your end users with the ability to:

- Stop data leakage
- Control how Data is used
- Log access to secure data
- Log operations (open, copy, edit) on secure data
- Track where Digital Assets exist within an organization

The following section outlines some of the key security risks that can be avoided by integrating your application with DAP rather than developing your own data protection solution from scratch.

Data Security Risks

Use of Data Beyond Your Application

By securing an application you can secure the data within the confines of that application. However, the application data is stored on disk and can be accessed outside the application. DAP secures the data itself. Any attempts to access the information by any other application results in the data being protected. More importantly, attempts to access, modify, or copy the secure data files are logged by DAP. This happens regardless of whether or not your application is running. So, attempts to access data outside of your application will still be secured, and those attempts will be logged, thus providing an audit trail on the data.





The Value of an Embedded Data Protection Solution

Integration with Digital Asset Protection

If your application exports files to other well known formats (PDF, DOC, HTML), DAP can protect those files as well. That data inherits the permissions given to your application data so it can be secured beyond your application.

Copying Data Files to Another Computer

If data is secured within your application, a malicious user can try to access that data on another computer, perhaps even one without your application installed. DAP protects against such a risk in a number of ways. First, any Digital Asset that is being tracked by DAP is encrypted using industry standard strong symmetric encryption algorithms. If a user tries to copy a file to external drive or CD, or if they remove the hard disk and place it into another computer, the data will still be protected. Beyond the encryption, security policies can be implemented such that certain types of data are disallowed from being copied to external drives (USB drives, PDAs, iPods), saved to disk/CD, or even emailed. This means that your application data will stay secure. It can be prevented from leaving a computer, and it is encrypted even if it is allowed to be taken elsewhere.

Enforce Security for Multiple Application Versions

If application data is stored centrally, in many cases, old versions of an application can still access the data. This provides backwards compatibility and prevents forcing a customer to upgrade all copies of an application. If old, insecure versions of an application exist, then securing just the latest version is not enough. DAP can be used to negotiate connections between a server and any connecting clients so that remote access from any insecure application will be refused and logged. DAP ensures the protection of data, regardless of the version of an application, and regardless of where the data is stored.

Blocking Screenshots and Printing

DAP can prevent printing of your data. More importantly, DAP can also prevent screenshots. This functionality requires very low level kernel code, integrated with Windows. Even if an application can prevent printing, a screenshot can get around that. With DAP, you can rest assured that your sensitive application data will not be captured by a screen grab.

Sanitization of Data

In most 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. DAP 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.

The DAP Client Cannot be Side Stepped

A DAP client cannot be uninstalled without access to the original executable. This means a user needs the proper access to uninstall the client. If the client is actually uninstalled, all Digital Assets on a machine are sanitized before DAP is removed. Beyond this, Digital Assets cannot be decrypted without the DAP client, and a valid Windows Authentication.

Guard Against Sophisticated Attacks

Kernel sniffers, and memory dumps are among the more sophisticated attacks that could take place. Data, even if encrypted on disk, exists in memory in decrypted form. DAP guards against this type of attack by detecting and preventing them from running.





The Value of an Embedded Data Protection Solution

Integration with Digital Asset Protection



www.softtection.com

Hiding Files Contents from Administrators

System Administrators need to perform actions on data to do their jobs. Backup & restore, physical storage, recoverability, and other administration concerns are all a vital part of a System Administrator's job. Often, the data and files that need to be administered are highly sensitive. Large numbers of IT employees, high turnover or the existence of highly sensitive data all raise the risk of a security breach. With DAP, System Administrators can be allowed to perform all the regular functions required of them, but access to the names and contents of files can be denied, thus ensuring the data is secure but that nothing prevents it from being properly administered.

Time to Market

DAP runs on a rules based client. Integration with DAP consists of creating business rules specific to your application and is therefore quick to implement. The rules specify to the DAP client what files, processes, and connections need to be kept secure. These rules need to be written and tested once and can then be distributed with the DAP client along with your application. Securing an application, which could otherwise take months of programmers' and testers' time, can be done in a matter of days or weeks with DAP.

Summary

Protecting data is an important selling point for any application. It is also technically challenging, and requires extensive expertise and testing. Let DAP do the lion's share of the work for protecting your application's data. With DAP:

- The above security concerns which extend beyond your application code can still be adequately addressed.
- The other benefits of DAP, including logging and tracking of data, can also be had.
- The testing and security knowledge of Softection's engineers gets passed on to your product.
- Data protection can be implemented quickly and easily.

For more information on how to integrate your application with DAP, please contact Softection.

Web: www.softtection.com
Email: integration@softtection.com
Phone: +61 2 9816 3433



SOFTECTION
DIGITAL ASSET PROTECTION