

InDorse Marketing



# InDorse Technologies: Market Positioning

Information Assurance and Risk Management

## Document Summary

This document positions InDorse Technologies in the Information Assurance, Security, and Risk market segments. It discusses InDorse in relation to point solutions in Information Rights Management (IRM), Digital Information Governance, Regulations, and Compliance (GRC), Digital Rights Management (DRM) and Enforcement, and Data Loss Prevention (DLP), and as well as how InDorse augments, plugs gaps in, or bridges other such information security technology as applied to unstructured data in the form of electronic files.

“You have to understand what kind of sensitive data you have, and do a risk evaluation of what happens if data is exposed or gets in the wrong hands.”

Thomas Raschke  
Senior Analyst, Forrester Research, Inc.



## Table of Contents

Copyright and Confidentiality .....	3
InDorse Technologies .....	4
One step ahead of Risk and Regulators.....	4
Market Leadership .....	5
Addressing Security Problems .....	5
Main Collaborators .....	5
Designing a Better Content-based Security Solution .....	5
Market Leading Products .....	6
Use Cases .....	6
Context Oriented Security .....	7
Information Assurance - The Silo Approach.....	8
Trapping the context and policy at source.....	9
Closed-Loop Assurance .....	11
Key Differentiators for InDorse.....	12
InDorse in Information Assurance - In Context .....	12



## Copyright and Confidentiality

### Copyright Statement

Copyright © 2009 by InDorse Technologies.  
All Rights Reserved. International Patents Pending.

No part of this documentation may be reproduced in any form or by any means or be used to make any derivative work (including translation, transformation or adaptation) without explicit written consent of InDorse Technologies.

### Confidentiality Statement

*All information contained in this document is provided in commercial confidence for the sole purpose of knowledge transfer by InDorse Technologies. The pages of this document shall not be copied published or disclosed wholly or in part to any party without InDorse's prior permission in writing, and shall be held in safe custody. These obligations shall not apply to information which is published or becomes known legitimately from some source other than InDorse Technologies Inc.*

Author	InDorse Marketing
Status	Issued
Issue	1.4
Date	1 May 2009
Distribution	Potential Clients and Partners

## InDorse Technologies

InDorse Technologies is an award-winning software solutions company focused on Information Assurance, Security, and Risk Management. InDorse is ideal for any commercial, government, academic, or military organization that needs to:

- Secure and protect sensitive information;
- Implement or enforce governance, compliance, risk management or security policies, in addition to having audited proof that they are doing so;
- Categorize documents and digital files for ease of management and efficiently controlled distribution of information, .e.g., for consortiums, mergers and acquisitions or business segregation.

## One step ahead of Risk and Regulators

According to Forrester Research, over 80% of secure data loss is caused by accidental exposure. Other analysts estimate that for every deliberate act [of data leakage] there is the potential for several thousand accidental leakages. Moreover, the Ponemon Institute has reported, “The average information leak costs organizations approximately U.S. \$182 per record, averaging roughly U.S. \$4.8M per breach in total.”

The loss or accidental exposure of sensitive information presents a risk exposure to any organization. Depending on the organization, the risk can have catastrophic effects resulting in:

- Financial losses in shareholder value, loss of Intellectual Property Rights, Patent loss or litigation;
- Loss of sensitive customer data, i.e., personally identifiable information (PII);
- Exposure to litigation, regulatory fines;
- Competitive bid losses to competition – even leading to being sued by consortium partners who also suffered from the bid loss;
- Loss of national or military secrets;
- Non-repudiation of knowledge, e.g., health and safety documentation supplied and audited as having been read.

The attendant risks, especially those that fall within regulation and compliance means that information assurance and risk avoidance is a priority for both corporate board members who are culpable for mistakes, and for IT practitioners too. *InDorse therefore is ideal to help any organization stay one step ahead of associated risks and regulators.*

## Market Leadership

“For products to be effective, vendors must provide customers with at least four things,

1. Discover and classify sensitive data;
2. Define and manage policies based on content and context;
3. Monitor and enforce the movement of data;
4. Report, audit and document incidents of data leakage.”

*Source: Andrew Jaquith, Forrester Research, May 2009.*

By delivering these four elements ahead of Mr. Jasquith’s statement, InDorse has become a market innovator and, with our route to market strongly supported by Microsoft and other major partners, we are on track to be the leader in Information Assurance.

## Addressing Security Problems

InDorse was founded in 2006 to plug capability gaps, to act as a bridge between security technologies in order to augment the point solution vendor approaches to Information Assurance, “While DLP can’t solve data security, it’s a powerful risk reduction tool,” *Rich Mogull, Securosis May 2009*. This statement is supported by the fact that the primary source of data leakage is known to be during the transit of files from the data store (a problem that InDorse addresses), rather than from the desktop.

The market need came from extensive analysis of the way technology vendors were addressing security and information rights management issues in a silo or disjointed point solution approach. The result is market confusion, product feature and capability overlap, which requires duplication of costs and effort to deploy, integrate and sustain. Yet, collectively, even if integrated, these point solutions fail to address the fundamental requirements of matching the security policy to the digital item on the fly (or as content is evolving within the document), and maintaining this throughout the lifecycle during each usage session. This innovated approach provides an audit trail for the entire file’s lifecycle or “chain of custody.”

### Main Collaborators

InDorse works closely with major corporations such as Microsoft, Credit Suisse and the Venture Capital Bank of Bahrain, who have produced or acquired and deployed in-house security solutions. These corporations soon realized that their selected security solutions still did not provide the life-cycle security required to cover risk and regulation within the changing content associated with various documents.

### Designing a Better Content-based Security Solution

The design aim was to create an easier way to understand dynamic inventory, protect sensitive information and comply with regulatory and security policies. It

had to be, and is, transparent to the end users, easy to deploy and easy to sustain. InDorse's solutions are designed to complement other tools that the industry has already invested in – or intends to deploy.

### Market Leading Products

The aforementioned design elements formed the foundation of InDorse Technologies' core and SPIDR offerings. The offerings quickly garnered the industry's attention:

- 2009 - Best in Category Context Filtering (Network Products Guide, annual Silicon Valley publication);
- 2009 - InDorse SPIDR - SharePoint-InDorse-Document-Remediation, a SharePoint solution enabling better methods for control and manageability of information within Microsoft SharePoint deployments;
- 2009 - InDIA - InDorse Image Assurance, IPR and content protection. The first customer for InDIA is Microsoft's digital advertising division, Massive Inc. Massive's Network offers advertisers the ability to reach and engage the video game audience across the leading game titles. InDorse secures and protects the content (work-in-progress) of these files, throughout the development process and into production release cycles.

## Use Cases

### Major Construction Engineering Company

#### *Sensitive Designs, Drawings, and Health and Safety Information*

A major USA design engineering firm won contracts in China to build refining plants. Their intellectual property and know-how needed for the China contract was held in **only some** of their millions of design drawings, specifications, operation instructions and health and safety manuals. The client needed to segregate documents and drawings to not only support the design and construction process, but the safe operation of the China plant. To protect their IPR, it was essential that they released to China **only** those files need for the job. In one week, InDorse segregated the required documentation. As a result, in the U.S., InDorse is now contracted to run quarterly audit reports and ad-hoc projects to better understand usage of their constantly created business documents.

As the new China projects commence, the InDorse system is ready to apply the correct policies and track and trace who has handled what files during the build process. Also, during both the build and operations phases the client is able to demonstrate a time stamped audit trail that the appropriate people have received the required operation and health and safety training material. This approach to non-repudiation that training has taken place will ensure safe operation, and protect them from future litigation.

## International Bank

*Prevention of data leakage; halting information sprawl, enhancing SharePoint roll-out and value*

The bank was deploying Microsoft SharePoint as a collaboration suite to improve knowledge-worker productivity. As sensitive information was removed from secure share files and placed into SharePoint, it became apparent that secure information was reappearing numerous times in a type of SharePoint information sprawl amongst the company's 20,000 users. This exposure created a risk of litigation and fines for regulatory non-compliance. As a result, InDorse was used to index the files, categorize them by instantaneous context – eliminating any ambiguity regarding the security status or approved use policy on any document. InDorse also invokes a built-in workflow process so that the stray documents could be safely categorized by the risk team or the document owner. Filters, or context identification libraries, have now been written for documents under PCI, Sarbanes Oxley and other categories to automatically group documentation and apply policies to them.

## Context Oriented Security

Consider a business evaluation report process where user starts with a blank boilerplate that has little or no risk policy associated with it and he/she then collaborates with others to progressively develop a finished report.



Fig. Finished report



Now consider the finished report where the report may contain secrets, personnel records, and financial data and so on. This changes the context in which the document needs to be treated by compliance or risk policies. InDorse has the ability to recognize the context, based on the file metadata, the indexed content and the history of usage. From these elements, InDorse uses rules to automatically decide the appropriate policy to apply at each stage of the report development cycle. In addition, InDorse also provides a time-stamped audit of who was in possession of each document throughout its entire “chain of custody” in the collaboration cycle.

## Major Differences

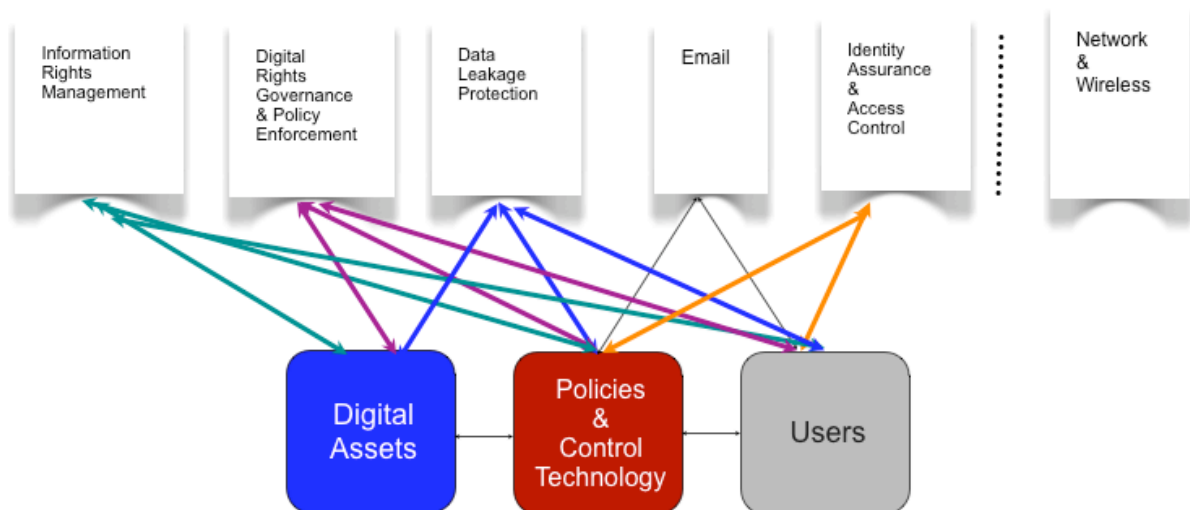
Context oriented security is where InDorse starts to plug the gaps and differentiate from other DRM/ILM/DLP systems that classify on metadata (only). Since other approaches fail to understand a document's *context*, they are therefore unable to

apply the correct classification— on-the-fly— for the correct policy strength, or level of control.

InDorse also recognizes the pedigree and lineage of a document (either a finished one or one as a work in progress) and provides a real-time audit trail throughout the life-cycle of the file. Other systems simply allow the storage of the file under a new name, but without any connection to its history or pedigree.

## Information Assurance - The Silo Approach

The security and information assurance/protection market has evolved with a plethora of point solutions for topical problems; rather like placing different ointments to resolve many symptoms. This approach can be very costly and time consuming to deploy and maintain.



Companies often find themselves asking:

- How many vendors do I need to resolve one problem?
- Do I need them all or only some solutions to achieve complete security and compliance?
- Do I have enough budget to cover all my unsecured information sources?
- How much integration is really needed?
- What if I already have a Digital Rights Governance or Data Leakage Protection system?

The management issue goes beyond buyer confusion and relates to integration and system/policy management issues. In some cases, policies would have to be entered more than once, or synchronized in an unsustainable manner.

## Example Silo Vendors

Silo vendors - but do they understand status and context?



## Trapping the context and policy at source

Business process - request Digital Asset,..... use/edit/save to [approved] store

Index content AND Meta Data  
  
.. both historical in store and WIP

Filter into Logical Groups e.g. PCI Sarbox, or by Project, value, Division, Contract, Policy

Classify by Risk Profile Secret, Secure, Share

Attach Tag that carries the policy in context

Tag records audit trail + time stamp and who/what device sent to



InDorse is a virtual solution applied as software or, more typically, as an appliance acting as a proxy server placed between the users and the data stores. InDorse stores information about the files and does not copy the file or replace the original repositories. Provided the request for the file is configured to pass via InDorse, every time a user requests a file, InDorse follows the process where the metadata and the content are indexed on the fly to understand the context of the file/document. The core process happens in three stages:

**Discover**- find the files and index their content and metadata;

**Tag** - identify the file with the correct policy for the current session of the user;

**Protect** - secure the file via collecting the audit trail (held within the embedded tag) and/or enforcing usage rights at the end-point user or device type.

In concert, InDorse Discover, Tag, and Protect deliver information assurance and risk mitigation on the unstructured files that drive the organization's business processes:

### **1. InDorse Discover, and the remediation of unknowns and ambiguity**

Discovery can be run in two modes: (1) discover all documents/files in target environment, or (2) discover and index documents/data files in sequence as they are collected by users from the data store.

In approach (1), discovery is run on the target data stores, locations, IP address ranges etc, to find all file types, and index all documents (for text search and taxonomy). Based on rules set by information risk and policy makers, the discovered metadata and content is used to auto-categorize the documents into logical groups known as "Clusters," e.g., groups of files for customer financial documents that are governed by, for example: PCI compliance, or drawings that relate to a vehicle type, or an image or a media file that belongs to an artist/photographer/game. The filters, context identification libraries, for clustering can be set at different sensitivity levels of criteria match based on the indexed text in the content and metadata, e.g., a 100% match; a 90% match; an 80% match and so on. Filters can also be based on patterns in the file content (such as Social Security/ National Insurance Number or Credit Card Number patterns); or filters can also be based on previous file usage (the file history of uploads and downloads) and /or on the file's physical location. Aggregate filters can also be based on combinations on all of the above filters. The remediation of unknowns or ambiguity is enabled by InDorse invoking a built-in [SharePoint] workflow engine for document owners or risk managers to validate and confirm the policy to be applied. Policy categories or changes can also be applied on the fly so that the next time a request or session is started; the new policy or category is applied.

### **2. InDorse Tag**

A small digital "Tag" is embedded in the metadata as the document/file is being passed to the user. And if the policy requires it, InDorse can assure the enforcement of the policy (e.g. "For UK eyes only"; no copy and paste, no print, read only).



### 3 InDorse Protect

InDorse “Protect” is the part of the core system that orchestrates, or if you prefer the term choreographs or coordinates, the real-time dynamic policy, that InDorse determines on-the-fly and fuses into the Tag. The Tag is now embedded in the file for immediate delivery to the user.

Either, the policy is enforced by InDorse, or InDorse instructs the preferred third party Digital/Information Rights management product the client wishes to use, which policy to apply.

## Closed-Loop Assurance

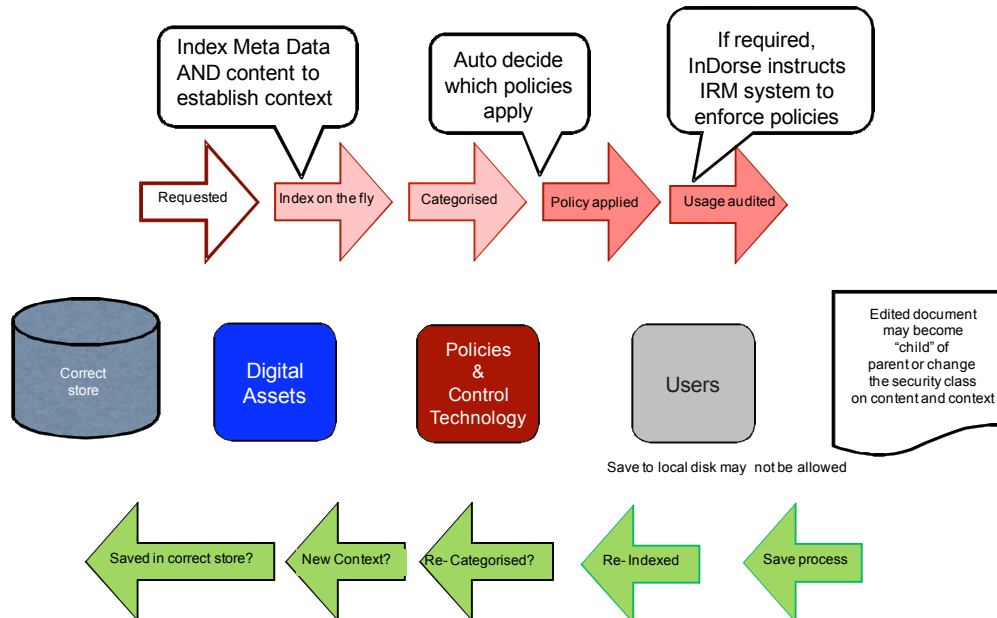
InDorse is unique in that it understands the pedigree (or parent and child relationship) of documents as they go through their normal work in progress.

The InDorse approach to indexing the documents/files and metadata on the outbound trip from file store to the user –as well as on their return– means that InDorse can build, trace and track an audit trail of the evolution and history of documents / images / drawings / etc. For example InDorse can identify:

Who possessed a file, exactly when the file was in their possession?

and exactly what stage the file was in when they received it. When the file is deposited back to store, the InDorse tags are withdrawn, leaving only the pristine files in the store. InDorse can also help enforce that the files are only stored in the correct store.

Fig. Closed-loop Assurance



## Key Differentiators for InDorse

There are many differentiators but the key ones include:

1. Trapping and *immediately* applying the appropriate rules-based policy at the source for each session;
2. Context oriented security;
3. Context classification of document sets - even if you do not need full security and rights enforcement;
4. Orchestration of policy enforcement via other tools;
5. Full audit trail of the “Chain of custody”;
6. Knowledge and recognition of document lineage/pedigree;
7. Easy and economic to deploy and sustain, without end-users having to change any behaviors;
8. Low training and support overhead as typically on the risk management or security is trained on the system
9. Productive because of the workflow remediation and elimination of uncertainty.

## InDorse in Information Assurance - In Context

The UK National Technical Authority for Information Assurance (CESG, a division of GCHQ) has defined five key principles of Information assurance. InDorse can help its customers (organizations, enterprises and collaborators) validate and prove to their satisfaction, and to the satisfaction of their regulators, stakeholders and partners that they are able protect and intelligently share sensitive information under the control of legitimate users.

InDorse is in context-oriented Information Assurance and Risk Management, and helps organizations to secure and intelligently share its business or sensitive information.

### The Principles and How Indorse Helps:

Please refer to table that follows from next page.

Information Assurance Principle	How InDorse helps achieve it
<p><b>Confidentiality</b> - ensuring that information is accessible to only those authorized to have access and for those people to do only what they are authorized to do with it;</p>	<p>InDorse digitally tags files and this tag carries with it the policies associated with that file and then records an audit trail of who downloaded the file/document and when. InDorse tracks the file/document throughout its life cycle and “chain of custody”. The audit trail enforces accountability on end-users, while the applied policies are used to secure the information/ content.</p> <p>Additional value concepts include:</p> <p style="padding-left: 40px;">InDorse bases policy on file content, allowing InDorse to automatically determine user-file permissions in real-time based on actual file content (rather than pre-determined rules that might no longer cover all documents, folders, drives, etc)</p> <p style="padding-left: 40px;">InDorse Protect - encrypting file with password</p> <p style="padding-left: 40px;">Integration with leading IRM systems extends all IRM protection functionalities without the traditional, associated complexity. Integration with other IRM systems is available via services.</p>

Information Assurance Principle	How InDorse helps achieve it
<p><b>Integrity</b> - safeguarding the accuracy and completeness of information and processing methods.</p>	<p>InDorse processes include time stamping, categorizing and classifying both finished documents/files and Work In Progress (WIP). Workflow processes are automatically invoked for information risk managers to validate the status and classification of each document/file.</p> <p>Thus providing an end-to-end system that supports information accuracy and completeness.</p> <p>Additional value concepts to include:</p> <p style="padding-left: 40px;">InDorse bases policy on file content, allowing InDorse to automatically determine user-file permissions in real-time based on actual file content (rather than pre-determined rules that might no longer cover all documents, folders, drives, etc)</p> <p style="padding-left: 40px;">Logging and Reporting: InDorse logs all actions including file accesses and administrator actions. All log data can be used to generate reports.</p>

Information Assurance Principle	How InDorse helps achieve it
<p><b>Availability</b> - ensuring that authorized users have access to information and supporting IT communications systems when required.</p>	<p>The InDorse functions are placed unobtrusively between the data stores and the users. SharePoint or other systems are used to access information, or to place or relocate files to specific SharePoint IP addresses so that only authorized users have access to them, e.g., storage at a specific point could be granted for “For UK eyes only” or “project X” documents are stored on, or collected from, specific locations.</p> <p>Additional value concepts to include:</p> <p>In the fault tolerant and highly scalable version - InDorse leverages common, proven fault-tolerant and scalability techniques.</p>
<p><b>Authentication</b> - ensuring that the identity of a subject or a resource is the one claimed</p>	<p>Time-stamped records and logical grouping of files by category and/or security classification helps validate and ensure that right file for the right purpose is stored or used.</p> <p>Additional value concepts to include:</p> <p>InDorse Tag digitally stores identity of the resource</p> <p>InDorse Lockbox viewer gives file recipient the ability to verify the InDorse Tag</p> <p>InDorse tag is encrypted and cannot be manually modified</p>

Information Assurance Principle	How InDorse helps achieve it
<p><b>Non-repudiation</b> - the ability to prove an action or event has taken place so that this event or action cannot be repudiated later.</p>	<p>The time-stamped records of who had what file and when it was downloaded or uploaded (and what policies were applied) provide non-repudiation support. This is enhanced by any change in meta being recorded, so for example, where it is essential that users must validate that they have read and understood the contents of a document, the user taking an action that is recorded as a change in the file’s metadata is recorded by InDorse. Thus, the user cannot in the future deny having seen, read and understood the document. InDorse integrates with any form of authentication and identity management systems.</p> <p>Additional value concepts to include:</p> <p>InDorse Tag digitally stores every action made to a file resource.</p> <p>InDorse Lockbox viewer gives file recipient the ability to view and verify the InDorse Tag.</p> <p>InDorse tag is encrypted and cannot be manually modified.</p>