

EMC Documentum Information Rights Management for Manufacturing

Protecting intellectual property across the global supply chain

The Big Picture

- Helps manufacturers actively control, secure, and track intellectual property across the global supply chain
- Ensures that only authorized recipients can view, copy, print, or edit information such as quality assurance documentation
- Prevents the use of fraudulent invoices and shipping orders
- Allows content owners to revoke access to price lists and engineering designs after external distribution
- Protects documents and e-mail—easily and intuitively
- Integrates tightly with content management systems, e-mail gateways, and portal technology

The “flat” world of Thomas Friedman may make historical and geographical divisions among global manufacturers irrelevant. But this more level playing field also increases the risk of fraud and intellectual property theft. Today, the global manufacturing enterprise relies on outsourcing and complex networks of suppliers linked by data networks. Over these networks, a manufacturing enterprise is compelled to share intellectual property such as product specifications, engineering drawings, product roadmaps, customer lists, and price catalogs with colleagues, partners, and customers.

Most organizations are fairly well equipped to protect their networks from malicious intrusion. But the intellectual property these networks transport is much more vulnerable—not just vulnerable to attack from competitors but also from employees. In fact, industry research estimates that insiders are responsible for as much as 70 percent of corporate data theft. Intellectual property can be copied to portable media and physically removed from a secure facility—or pirated once it has moved outside the corporate firewall via the Internet.

Nor does a breach need to originate from malice. A recent RSA survey found that 60 percent of American executives routinely leave their businesses carrying a mobile device such as a laptop, Smartphone, or USB flash drive that holds sensitive information.

Under these circumstances, it’s not unusual for a company to see a story published in a trade publication about a product that is still months from release. Who is to blame—the contract production facility, the offsite designer, an advertising agency, a market research firm, or a disgruntled employee?

Protect intellectual property wherever it resides with information rights management

EMC® Documentum® Information Rights Management (IRM) helps global companies actively control, secure, and track valuable intellectual property wherever it resides—even when it is shared with partners and suppliers outside the firewall.

For example, manufacturing executives are particularly concerned about the security of price lists. Unscrupulous manufacturers even offer bounties to retrieve competitors’ lists. With the tremendous capital investment at risk from ruthless price cutting, the protection and control of price lists is critical.

Documentum IRM, a suite of products that provides information rights management, allows content owners to dynamically control and manage access to intellectual property. With Documentum IRM, you decide who may or may not view, edit, or print intellectual property in any form. Whether it’s a Microsoft Office document, Microsoft Outlook or Lotus Notes e-mail, or Adobe PDF, Documentum IRM protects your data regardless of file format, without altering existing workflows. In the case of price list protection, the version control features of Documentum IRM empower manufacturers to expire outdated listings—which are often customized and contingent upon volume—and to provide resellers with up-to-the-minute details on how to sell their products.

Available as a stand-alone application or tightly integrated with the Documentum content management platform, the solution is easy to deploy and leverages existing enterprise investments in content management, e-mail gateways, and portal technology. At the same time, it helps reduce printing, postage, and overnight delivery expenses by distributing proprietary information electronically.

Documentum IRM complements the security capabilities of the Documentum platform, which features authentication, access control, auditing, SSL and repository encryption, electronic signatures, and digital shredding. This combination delivers the most secure content infrastructure on the market.

Securing documents

A complex global supply chain thrives on information, most of which is shared via documents in a variety of forms. The greater the complexity—the more links in the chain—the greater the risk that information will fall victim to fraud. And that fraud may happen anywhere and well out of reach of an organization's internal controls. Product designs sent to a contract manufacturer are just one example. Moreover, foreign countries vary widely in the strength of their legal protections for intellectual property and in the rigor of enforcement efforts.

Documentum IRM enables organizations to securely share documents that contain sensitive intellectual property. Information is encrypted and protected at rest, in transit, and while it's viewed by recipients. This frees content owners to collaborate with colleagues and partners anywhere while ensuring that sensitive information doesn't end up where it shouldn't.

Leveraging patented rights management technology, Documentum IRM provides the ability to:

- Determine who can access a document
- Prevent documents from being viewed by unauthorized recipients
- Prohibit printing of an entire document or selected portions
- Disable copy/paste and screen capture capabilities
- Watermark pages if printing privileges are granted
- Expire or revoke document access at any time
- Track all document activity through a complete audit trail

To secure documents, EMC offers EMC Documentum IRM Client for Microsoft Office and EMC Documentum IRM Client for Adobe Acrobat.

Securing e-mail

EMC Documentum IRM Client for E-Mail supports Microsoft Outlook and Lotus Notes and helps organizations protect information that must be shared via e-mail. Unlike traditional secure delivery solutions, Documentum IRM protects e-mail and attachments during and after delivery—ensuring that content remains confidential and tamper proof no matter where it is distributed or stored.

Using simple check boxes, mail senders can control who may read a message, when it can be read, and whether or not recipients can copy and paste from a message or forward it. Users may also assign an expiration date to messages, which appears alongside the message in the recipient's inbox.

If a message sender recalls a message, all copies are automatically expired from sender and recipient desktops, servers, or backup media. A detailed audit trail provides proof of compliance with corporate security policies and regulatory requirements.

Key IRM features

As the following table illustrates, no other IRM solution provides the level of granular security and control offered by Documentum IRM.

Feature	Benefit
Persistent protection	Ensures that documents, messages, and attachments are protected at rest, in transit, in use, and after they are distributed to recipients regardless of location or device (laptop, desktop, portable USB storage, or mobile appliance).
Dynamic information policy management	Allows content owners to define and change user permissions (view, copy, or print) and recall or expire content after distribution inside or outside the firewall.
Automatic expiration	Provides the ability to automatically revoke access to documents, e-mails, and attachments at any point, allowing security policies to be enforced wherever content is distributed or stored.
Information access auditing	Confirms that content was delivered and viewed and offers proof of compliance with security policies.
Support for existing authentication security infrastructure	Reduces administrator involvement and speeds deployment by leveraging user and group information that exists in directories and authentication systems.
Mapping for repository access control lists (ACLs)	Automatically maps ACL-based permissions to policies that control content outside the repository.
Broad application support	Secures information created in native application file formats such as PDF, Microsoft Word, Excel, PowerPoint, Lotus Notes, and Microsoft Outlook. Leverages SDK framework to protect any file format or business application.
Simple, seamless protection through ECM integration	Automates protection of sensitive content through native integration with Documentum ECM platform and solutions.
Version control and offline access	Enables automatic revocation of access to outdated files. Makes links to current versions available as they are published. Grants recipients the right to access documents offline for a specified time while maintaining audit capabilities.



EMC Corporation
Hopkinton
Massachusetts
01748-9103
1-508-435-1000
In North America 1-866-464-7381
www.EMC.com

Take the next step

To learn more about EMC Documentum Information Rights Management for Manufacturing, visit www.EMC.com or call 800.607.9546 (outside the U.S.: +1.925.600.5802).