

Adobe Systems Manages Confidential Information More Securely with Dynamic, Persistent Document Control

The Challenge of Distributing Confidential Information

Protecting intellectual property and safeguarding employee and customer privacy are paramount security concerns for Adobe. While technologies are in place to help prevent outside attacks on Adobe's corporate network, Adobe needed to mitigate the risk of security breaches created inadvertently by well-intentioned employees handling sensitive information. Adobe turned to document-level security technology to help protect information even after it is distributed to employees.

All companies face security risks; the loss of trade secrets and other proprietary information costs U.S. companies tens of billions of dollars annually.¹ Industry reports indicate that more than half of all security breaches are due to insiders, and nearly half of all insider breaches are accidental.² Like most companies, Adobe needed to:

- Securely distribute confidential information and trade secrets in a controlled manner to specific groups
- Prevent sensitive information from being distributed to unauthorized parties
- Ensure that everyone in the organization is working with up-to-date information
- Monitor how documents are used to more easily comply with government regulations

Modern business practices depend on timely access to information, such as price lists, financial reports, product planning documents, and business plans. Strict information security is critical for strategic discussions, partner agreements, acquisitions, and legal negotiations. Although Adobe has a secure intranet, a virtual private network (VPN), and public key infrastructure (PKI) technology, the company had no way to prevent authorized employees from accidentally or intentionally distributing confidential documents to unauthorized people. Adobe had to go beyond traditional security solutions that focus solely on securing the network and focus instead on securing the content, using technology that is easy for employees to adopt. With Adobe® LiveCycle™ Policy Server, Adobe can now protect confidential information at the document level.

Keeping Documents Secure after Delivery

With Adobe LiveCycle Policy Server, Adobe can control who can access a document, when they can access it, and how they can use it. And because document policies are managed dynamically, policy changes can be made without having to reissue documents. Adobe LiveCycle Policy Server enables Adobe to monitor access to documents after they're distributed and produce an audit trail of who accessed the documents and when.

ADOBE SYSTEMS INCORPORATED

Adobe helps people and businesses communicate better through its world-leading digital imaging, design, and document technology platforms for enterprises, creative professionals, and consumers.

- Revenues: More than US\$1.6 billion
- Employees: More than 4,200 worldwide
- Headquarters: San Jose, California
- Founded: 1982

www.adobe.com

INDUSTRY

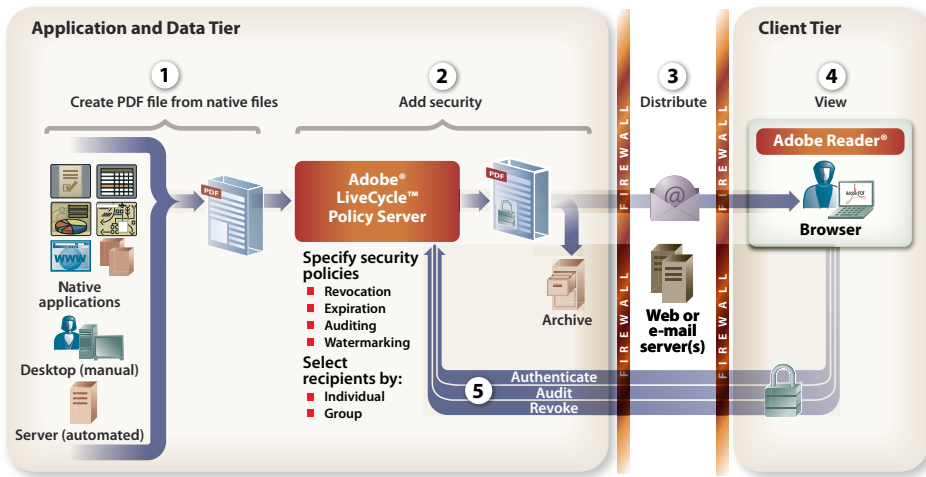
Technology

SOLUTIONS

- Document Policy Management
Persistent control for electronic documents that ensures authorized access, confidentiality, and accountability for the lifetime of the document

¹ American Society for Industrial Security/PricewaterhouseCoopers Trends in Proprietary Information Loss Survey Report (www.pwcglobal.com/extweb/ncsurvres.nsf/DocID/36951FoF6E3C1F9E852567FD006348C5)

² Marguerite Reardon, "Securing data from the threat within"; CNET News.com, Jan. 12, 2005 (www.crime-research.org/news/12.01.2005/893)



Adobe LiveCycle Policy Server enables enterprises to protect the confidentiality of sensitive documents inside and outside the firewall.

Step 1. Create PDF file manually from any member of the Acrobat® family of products or automatically from Adobe Document Server, Adobe Central Pro Output Server, or Adobe LiveCycle Forms software.

Step 2. Apply security policy to the PDF file, which assigns security permissions to users.

Step 3. Store or distribute the PDF file via e-mail, the Web, or CD.

Step 4. User opens the PDF file after logging in to Adobe LiveCycle Policy Server.

Step 5. Adobe LiveCycle Policy Server audits user actions, including printing, opening, and form filling. Permissions are managed or revoked.

Adobe LiveCycle Policy Server ties document security features to individual Adobe Portable Document Format (PDF) files, providing enhanced security even when the files move outside the controlled network. With Adobe LiveCycle Policy Server deployed for use by the entire company, Adobe managers and employees can:

- Set permissions so that people are prevented from printing documents, copying text out of documents, downloading documents to their hard disks, or distributing documents to others
- Manage document access and usage after publishing and distributing a document
- Change document permissions and adjust access rights by adding more recipients or revoking access
- Monitor document usage and provide a detailed audit trail to comply with regulations
- Implement effective version control of documents after they have been distributed

Adobe deploys LiveCycle Policy Server using the IBM® WebSphere Application Server and the Microsoft® Windows® operating system. Because Adobe integrates Adobe LiveCycle Policy Server with Oracle databases and the Lightweight Directory Access Protocol (LDAP) authentication technology used for the company's intranet, employees can use the ID and password they use for accessing the intranet to open protected documents. Adobe even leverages the reporting structure in its SAP deployment to define groups of employees for document distribution.

When employees leave the company, Information Services removes their IDs from the LDAP directory, so they can no longer access protected documents. This level of protection provides significant assurances that confidential information does not leave the premises. "For a former employee, the protection system is like a shredder," says Gloria Swanson, Information Services Manager at Adobe, "Once the former employee's account is deactivated, the documents become unusable."

Adobe employees use Adobe Acrobat Standard or Adobe Acrobat Professional, the same tool used for creating PDF files, to create and edit policies and assign policies to PDF files. "Adobe LiveCycle Policy Server is designed to enable employees to create their own policies," says Swanson. "We also provide a set of corporate-wide policies matching our document classification guidelines that everyone can use; they limit document distribution to Adobe employees. Creating a policy that limits distribution to a few people is very easy to do. As a result, at Adobe we're protecting about 1,100 documents every quarter."

Reporting financial information

In any company, business teams need to receive revenue information in a timely manner in order to monitor their success and make necessary adjustments. However, the risk of someone trading stocks based on this insider information requires companies to limit the distribution of such information.

"Critical business information must be protected at all times as it travels around the organization. With Adobe LiveCycle Policy Server...we can safeguard our intellectual property and trade secrets when sharing information among executives, while increasing the ease and efficiency of our communications, sales, and marketing efforts."

John Landwehr, director of Security Solutions and Strategy, Adobe Systems

Business case	Challenges addressed
Finance reporting	Enable distribution while controlling access to financial information
Sales communications	Distribute protected information and monitor its use to improve communications
Executive communications	Protect confidential information and audit usage to more easily comply with regulations
Legal communications	Control access to documents during reviews and speed up the review process
HR privacy compliance	Provide confidential employee information to a manager by e-mail while limiting access with strict controls
Employee communications	Control who can view and print documents, and how long the documents remain available
Product planning and development	Protect trade secrets and revoke access to older documents when replacing them with new ones

With Adobe LiveCycle Policy Server, Adobe can control access to critical financial information and significantly reduce the risk of unauthorized distribution or dissemination of the information. “Adobe LiveCycle Policy Server gives us more flexibility to control distribution of a report compared to other security solutions, such as a secure portal, that would merely prevent unauthorized access but not prevent printing and redistribution by someone who *has* access,” says Elysse Hack, director of Finance. “With Adobe LiveCycle Policy Server, we can protect confidential information by not only restricting access but also by controlling whether an authorized person, such as a business partner, can print, copy, or distribute the report to other people.”

Adobe uses the SAP® Business Information Warehouse as a global reporting solution that helps improve visibility into marketing and sales efforts. To report on revenues specific to the education market, Adobe accesses information using Business Information Warehouse and processes it in Microsoft Excel. The Finance department then produces a PDF file that can be sent to executives by e-mail.

“On a regular basis we send out a revenue update to a list of worldwide recipients,” says Hack. “The information is useful for monitoring trends and course correcting during the quarter. Before, we couldn’t send out the information until after the end of the quarter. Now, with policy-protected documents, we can easily provide more visibility into quarterly revenue during the quarter, which can help improve revenue streams.”

Communicating with the sales force

Adobe needs to provide confidential information to its account managers on a regular, timely basis. This is especially true during a product launch or corporate acquisition, or in response to an announcement by a competitor. Lack of information at a critical moment could delay a sales transaction or cause the loss of a sale.

“We need to provide sales reps with up-to-date information, especially information about competing products and services, pricing, and answers to frequently asked questions,” says Denise Jansen, group manager for Worldwide Sales Communications. To help prevent the use of information if it is accidentally forwarded, Adobe uses Adobe LiveCycle Policy Server to deliver policy-protected documents that can not be printed, copied, or opened by unauthorized people.

Sales Communications also takes advantage of the Adobe LiveCycle Policy Server document usage monitoring feature to measure the effectiveness of sales tools and marketing materials.

“We gain considerable feedback on the value of our communications and considerable insight into what kinds of content to create,” says Jansen. “As a result, we can improve communications with the sales force, which can help to increase sales.”

Pricing guides are an essential sales tool; however, printing out 200 copies and express mailing the document to sales teams every quarter is cost-prohibitive, and if this confidential information fell into a competitor’s hands, the competitor could undercut pricing and win the sale. “I love Adobe LiveCycle Policy Server because I can send the sales teams a PDF they can’t print and can only look at for a certain period of time,” says Frank Tomei, product manager at Adobe. “It’s so simple, it only takes a minute to create a policy.”

“With Adobe LiveCycle Policy Server, we can protect confidential information by not only restricting access but also by controlling whether an authorized person, such as a business partner, can print, copy, or distribute the report to other people.”

Elysse Hack, director of Finance, Adobe Systems

“With Adobe LiveCycle Policy Server, I can revoke access to the old pricing guide when pricing changes,” says Tomei. “This helps Adobe provide accurate pricing in a timely manner for a higher level of customer service.”

Securing executive-level communications and ensuring compliance

Corporate executives need to ensure that when they communicate confidential information, the information won't be leaked. With mergers and acquisitions in particular, the existence of discussions and the identity of the companies involved, as well as negotiating terms, must be kept secret. However, timeliness is critical with negotiations, and executives need to provide real-time feedback to the negotiators.

“Adobe LiveCycle Policy Server provides a very high level of security and the easiest method of communicating confidential information,” says Paul Weiskopf, senior director of M&A and Alliances at Adobe. “It also provides a straightforward method of auditing document usage in order to more easily comply with government regulations.”

Solution	Benefits
Protect files at the document level	Improved confidentiality
Dynamically manage document usage policies	Increased timeliness and effectiveness of communications
Control documents after delivery	Faster collaboration; increased efficiencies; improved version control
Monitor document usage and maintain an audit trail	Improved communications tracking; easier compliance with regulations
Integrate document-level security with existing IT infrastructure	Enhanced IT investments; centralized document control

“Adobe LiveCycle Policy Server provides a very high level of security and the easiest method of communicating confidential information.”

Paul Weiskopf, senior director of M&A and Alliances, Adobe Systems

Public companies such as Adobe have fiduciary obligations to their stockholders and must comply with requirements set by government agencies, such as the Securities and Exchange Commission (SEC), that mandate secrecy and accountability with insider information. “If a company finds itself in a position of having to prove how confidential information was compromised, it's already a disaster, and the company is obligated to diagnose the situation, and quickly,” says Weiskopf. “The auditing features of Adobe LiveCycle Policy Server help mitigate the risks involved with communicating sensitive information.”

Adobe executives regularly exchange e-mails with attachments containing confidential reports on the status of business or plans for future business strategies. However, since most e-mail programs automatically complete an address as you type, it's easy to accidentally enter the wrong address, sending confidential files to the wrong person. Adobe LiveCycle Policy Server eliminates this problem because its policy-protected documents can't be opened by anyone not listed in the policy.

The policies also enable authorized executives to take documents with them while traveling and access them offline. The first time the executive opens a policy-protected document, it synchronizes online with Adobe LiveCycle Policy Server. “Policy-protected documents are better than password-protected Microsoft Word documents or e-mails,” explains Weiskopf, “because you can set policies such that the documents can't be printed or viewed by anyone other than designated recipients, even if the documents are forwarded the protection travels with them.”

Collaborating and distributing legal documents

Gary Spiegel, Adobe corporate counsel, knows the risks involved in distributing confidential contracts and other legal documents to clients and colleagues for internal review. “One of the biggest risks for a lawyer is the lack of control over documents, particularly draft documents, after they've been sent to clients,” says Spiegel. “You never know what they might do with files.”

The workflow for revising legal documents requires internal collaboration and review of the documents. “I typically use a PDF document with attached comments that I intend only for my clients,” explains Spiegel. “The problem is that these comments might be included accidentally in a contract forwarded to the other side in a negotiation, leaking valuable information to the other side that could put Adobe at a disadvantage or even disclose proprietary information.”

Spiegel uses Adobe LiveCycle Policy Server to control access to documents during reviews and to speed up the review process. “With Adobe LiveCycle Policy Server, I create a unique policy for each document and monitor the document’s access,” says Spiegel. “That way I can know not only how broadly the document has been distributed, but also if the intended recipients have reviewed it.” Spiegel’s policies enable him to place a time limit on each draft and revoke access when the document needs to be replaced with a new version. “The policies help me save time, keep the documents up-to-date, and keep the information confidential. Adobe LiveCycle Policy Server helps maintain attorney-client privilege.”

Maintaining strict privacy with employee information

Like all organizations, Adobe must protect employee information from unauthorized access, disclosure, copying, and use, and establish safeguards to protect information confidentiality and integrity. Typically organizations allow managers to review confidential information such as employee performance appraisal files only in a strictly controlled environment. Before Adobe’s HR department began using Adobe LiveCycle Policy Server to control access to documents, managers had to visit the department to review their staff’s employee information. “We had to control who could view the employee file,” says Susan Burke-Diquisto, director, Adobe Global HR Systems. “We would put them in an empty office with the file so that they couldn’t copy the file or take it away.”

Adobe LiveCycle Policy Server streamlines this process, enabling HR to provide an employee’s confidential file to a manager by e-mail while limiting access with strict controls. HR creates specific policies for managers that are designed to ensure that the only people who can open the employee files are the intended recipients. “Managers can see the employee file, but they can’t change it or print it, and access expires in a few days,” says Burke-Diquisto. “We’ve made the process more convenient for managers while maintaining strict confidentiality. Adobe LiveCycle Policy Server helps us comply with Adobe’s data privacy policy, which is in line with government regulations. And employees know their information will not fall into the wrong hands.”

HR also uses Adobe LiveCycle Policy Server to control access to confidential employee information distributed to the Adobe executive team. The policies for a PDF document also protect other attachments in the same e-mail. “We find this very useful for exchanging confidential spreadsheets that need to be manipulated by the recipients,” says Burke-Diquisto. “We can replace documents that need to be updated, and change a specific document’s policy to add another recipient.”

Distributing confidential information internally

Adobe Employee Communications produces and distributes everything from highly confidential executive-team communications to all-employee bulletins. Developing, approving, and distributing such a variety of information requires the group to adopt successful strategies for controlling who can view and print documents, and how long the documents remain available.

When documents are ready for distribution, the Employee Communications staff uses Adobe LiveCycle Policy Server to assign policies that limit the people who can view or print the documents. The policies also place limits on documents so that they are available only for a set amount of time. “Employees might unintentionally forward an e-mail or attachment,” says Andrea Brant, group manager of Internal Communications. “By using Adobe LiveCycle Policy Server we can better control access to the document even if it is accidentally forwarded, reducing the possibility that confidential information might leak out.”

The staff can also use capabilities in Adobe LiveCycle Policy Server to audit who viewed the documents. By monitoring document usage, the staff can track whether or not employees are opening documents and improve the effectiveness of communications. “We can see if people are really accessing the information,” says Brant. “For example, after we do an all-hands meeting, we typically send out a protected version of the presentation. With the tracking capabilities in Adobe LiveCycle Policy Server, we can see how many people actually looked at the presentation and measure its effectiveness.”

Controlling versions of product planning documents

As part of the process of developing and marketing software products, Adobe’s Product Marketing and Engineering teams regularly collaborate on and review confidential information in policy-protected documents, such as product requirements and product road maps. These documents need protection against accidental or intentional distribution so that trade secrets don’t fall into the hands of competitors.

“Adobe LiveCycle Policy Server helps us comply with Adobe’s data privacy policy, which is in line with government regulations. And employees know their information will not fall into the wrong hands.”

Susan Burke-Diquisto, director of
Global HR Systems, Adobe Systems

“If intellectual property leaked out, it would do irreparable damage to sales. With Adobe LiveCycle Policy Server, I can keep tight control over who uses our documents.”

Steve Gottwals, product manager,
Adobe Systems

“If intellectual property leaked out, it would do irreparable damage to sales,” says Steve Gottwals, product manager at Adobe. “With Adobe LiveCycle Policy Server, I can keep tight control over who uses our documents. I can grant access to the collaboration tools in Adobe Acrobat Professional so that only designated people can add comments. All comments can be incorporated back into the document while still controlling document access by policy.”

Product planning and development documents also need version control. With Adobe LiveCycle Policy Server, product managers can ensure that their teams always use the most up-to-date version of a document by revoking access to the old version after a new version is distributed. “Version management helps prevent a lot of wasted work,” says Gottwals. “You don’t want people using information that has gone stale.” As product development progresses, more and more activities have to be coordinated. “You gain efficiencies and speed up time to market by reducing any possibility that teams are working out of sync with outdated documents,” Gottwals adds. “We’re under strict time constraints, so we use the monitoring feature of Adobe LiveCycle Policy Server to make sure people are using the documents, and to prod them with e-mails if they aren’t. This helps us meet deadlines.”

Maintaining Control over Sensitive Information

With Adobe LiveCycle Policy Server, Adobe has significantly increased the security of its internal documents beyond the security measures that safeguard the company’s servers and intranet. The results are:

Improved confidentiality: Adobe LiveCycle Policy Server helps prevent information leaks and safeguards Adobe’s intellectual property. Protection is tied to the document no matter how or where the document is distributed.

Increased timeliness and effectiveness of communications: Adobe LiveCycle Policy Server features for controlling document access enable Adobe executives to exchange highly sensitive information, and finance and marketing to distribute vital confidential information to the sales force. Monitoring features enable feedback on document usage to help improve the content and effectiveness of information.

Faster collaboration and time to market: The Adobe LiveCycle Policy Server version control feature helps ensure that production teams remain synchronized with up-to-date information. It also enables more secure document review processes and the monitoring of document access to speed up production efforts.

Improved compliance with corporate governance regulations: Adobe LiveCycle Policy Server provides a complete and detailed audit trail that keeps track of what each recipient did with a document and when.

Enhanced value of current IT investments: Built on industry-standard technologies, Adobe LiveCycle Policy Server extends Adobe’s existing IT infrastructure, integrating with IBM WebSphere Application Server, Oracle databases, and LDAP authentication for cost-effective, centralized document control and administration.

“Critical business information must be protected at all times as it travels around the organization,” says John Landwehr, director of Security Solutions and Strategy, Adobe Systems. “With LiveCycle Policy Server, our employees can apply security parameters to individual documents and effectively manage the distribution of confidential information without having to secure the communication line or storage location. We can safeguard our intellectual property and trade secrets when sharing information among executives, while increasing the ease and efficiency of our communications, sales, and marketing efforts.”

Adobe LiveCycle Policy Server enables Adobe to more effectively manage the use of electronic documents by providing persistent protection. As a result, Adobe can distribute confidential information with greater assurances that the documents are effectively protected and regulatory requirements for maintaining information privacy are met.

SYSTEMS AT A GLANCE

- Adobe LiveCycle Policy Server
- Adobe Acrobat Professional
- Adobe Acrobat Standard
- Adobe Reader®

- IBM WebSphere Application Server
- SAP Business Information Warehouse
- Oracle 9i Database
- Sun™ Java System Directory Server, Enterprise Edition

Better by Adobe.™

Adobe Systems Incorporated
345 Park Avenue, San Jose, CA 95110-2704 USA
www.adobe.com

Adobe, the Adobe logo, Acrobat, Adobe LiveCycle, Reader, and Better by Adobe are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. IBM is a trademark of International Business Machines Corporation in the United States and/or other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Sun is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries. SAP is the trademark or registered trademark of SAP AG in Germany and in several other countries. All other trademarks are the property of their respective owners.

© 2005 Adobe Systems Incorporated. All rights reserved.
Printed in the USA.

95005588 10/05A

