Adobe Experience Cloud

Adobe solutions for the U.S. Government

Protect mission-critical content in a zero-trust environment when there's a need to know

Faced with protecting sensitive content and documents, the organizations turn to encryption methods, as evidenced by security compliance frameworks that encrypt data at rest and in motion. Yet all encryption methods aren't equal. Agencies must evaluate each approach against the threat models for a given environment. For instance, whole-disk encryption only defends against physical theft of the drive. Moving up the stack to network protection measures like Secure Sockets Layer (SSL), Transport Layer Security (TLS), or virtual private network (VPN) poses issues. Data is encrypted at one end, only to be decrypted at the other end and exposed to unauthorized activities. Application security measures like transparent encryption in the database are still prone to Structured Query Language (SQL) injection attacks and application exploits to access information. As a result, agencies are moving toward data-centric security solutions like Adobe Experience Manager, shown in Figure 1.

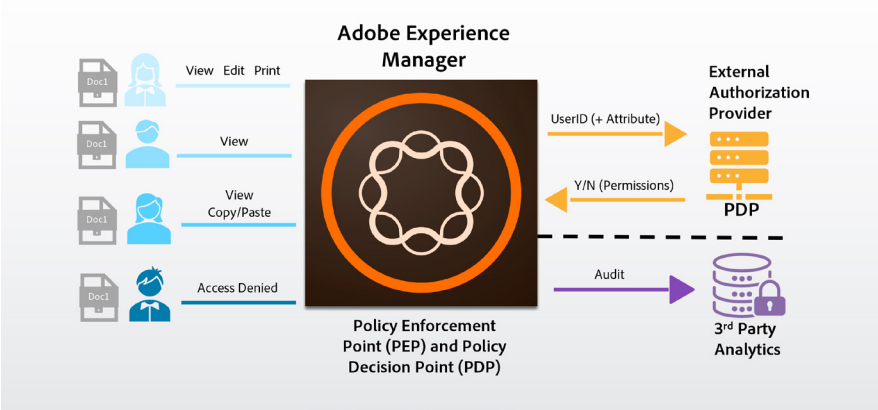

Figure 1. Opening a document and content protection with Adobe Experience Manager

Once content security is applied, the content security policy can restrict user permissions like read, print, copy, modify, and sign throughout the data lifecycle, even when data is removed from the portal or records management system. PDF-based forms support digital signatures using the agency-issued public key infrastructure (PKI) certificate with Security Assertion Markup Language (SAML) authentication to sign, timestamp, and audit individual form field changes. Agencies can safely distribute information saved in a supported format.

If other file types are needed for protection, custom extensions, plug-ins, or applications can be developed using the Document Security software development kit (SDK). Encryption can also be applied in an automated fashion to ensure data protection as part of an agency process.

Security and sharing can co-exist with Adobe data-centric security solutions. Protect content throughout its lifecycle, even when it is removed from the network.

Secure agency content with:

- **Attribute-based access control (ABAC)**—Enforce granular access to portions of sensitive documents dynamically, based on user and informational asset security attributes.
- **Content security**—Encrypt sensitive content and documents at 256-bit FIPS-140 Suite B to persistently and dynamically protect them, independent of storage or transport.
- **Document auditing and analytics**—Monitor document interactions continuously and leverage third-party analytics to alert security staff to potential breaches.
- **Digital signatures**—Automate integrity and authenticity checks on sensitive content.

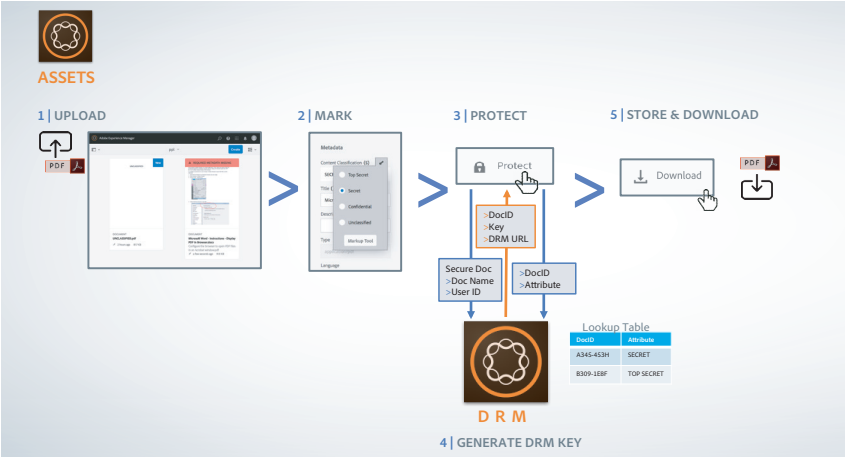

Figure 2. Protection of digital content using Adobe Experience Manager Forms

A document uploaded to a system can be automatically protected. To move toward data-centric security, tag data with security attributes, as shown in Figure 2. Experience Manager allows personnel to quickly and easily apply the appropriate security attributes to informational assets in the repository. Paragraphs, images, videos, titles, and even bullet points can be assigned multiple security attributes like classification level, International Traffic in Arms Regulations (ITAR), and environmental variables.

Once tagged, assets are referenced in assembling content for consumption. For example, a report authored as a web page may include text, images, and video, each containing different security markings. Experience Manager Forms integrates with the enterprise classification markup tool—Dynamic HTML (DHTML) version—to apply marking to an individual piece of content. When users authenticate into the system to view the report, they encounter dynamic redaction and see only the portions that they're authorized to see, based on their own security attributes, as shown in Figure 3, and authorization and libraries in the community. If any asset changes within the repository, such as reclassification of a video, all pages referencing that asset are automatically updated accordingly. If needed, the system can also enable end users to click on the redacted asset to initiate a request for access.

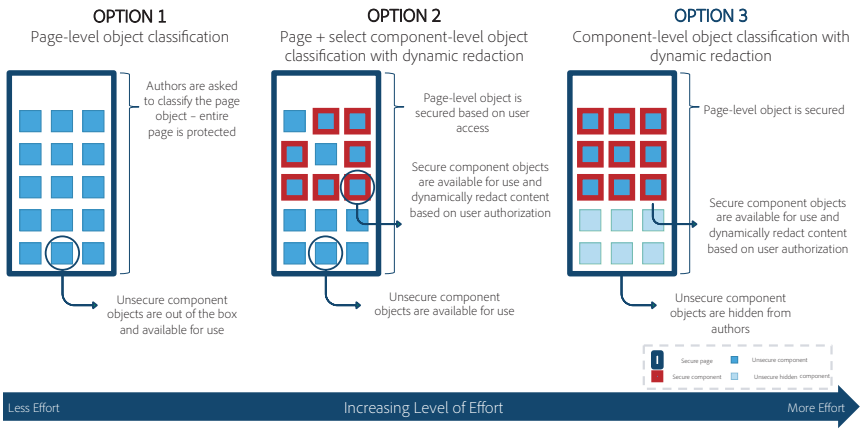

Figure 3. Page and component security within Adobe Experience Manager Forms

Digital content security is more important than ever to the U.S. Government's mission. Protect your valuable content with Adobe solutions.

Adobe data-centric security solutions enable a one-time "Mission Impossible" policy for instant destruction after a document is read.

File formats supported out of the box include:

- Adobe PDF, which can contain text, images, and videos
- Microsoft Office Suite products like Word, Excel, and PowerPoint

For more information.

www.adobe.com/government
1-800-87ADOBE