COVERTIX keep x safe

COVERTIX USE CASE: SECURING FILES IN THE CLOUD

File Sharing Today

Your organization may be using a cloud-based storage service, or individuals in your organization may be using Dropbox, Google Drive or Gmail, or SkyDrive to share their documents. How safe are those files?

Today we know two things. One is that many of these cloud-based services have suffered security breaches or attacks. Almost all of them have one-step authentication, and most passwords aren't secure. We've all been spammed by friends or colleagues who had their e-mail account compromised. The second fact that's hit headlines lately is that the very organizations that are storing your data may be passing on parts of it to government agencies or even viewing it for their own use.

Simply put, any file in the cloud could be vulnerable. It's sometimes necessary to use the public cloud for practical reasons, despite security concerns.

Any file or document can be secured regardless of the cloud service used

Essential Solution Attributes

An effective information protection solution for file sharing in the cloud needs the following key capabilities:

- Ability to protect documents outside the company.
- Protects files seamlessly with any type of cloud service: Dropbox, Google Drive, or any other cloud provider.
- Simple to use and manage, requiring no changes to workflow.
- Dynamically controls the ability to edit, copy, print, and view files.
- Ensures only authorized users access.

Covertix SmartCipher Cloud

Using Covertix SmartCipher for Cloud, the organization can protect all documents shared in the cloud including those outside of the organization. The solution protects documents from unauthorized use, including use by the cloud service provider. In other words, even if a document is stored as an attachment on a webmail server, the webmail company cannot access it (intentionally or unintentionally). As the rule set is embedded in each file, when a file is accessed, the file itself allows or prevents access, so you are completely safe under any circumstances.

Solution Benefits

- Automatic protection: Rules are applied whenever an employee posts a file to the cloud or sends it through a SaaS application. The file is protected before being posted or sent anywhere.
- Security stays with the file: When a file is copied, forwarded, or otherwise edited, the rule set stays in the file, ensuring only authorized users with the SmartCipher client can open it.
- Cloud providers have no access to the file's data.
- Rules control where and when a file can be viewed, edited, printed. Rules can include time limits, geography, domain and IP address specifications.
- Protects any type of file, including Microsoft Office documents, PDFs, video and audio files, etc.

ABOUT COVERTIX SMARTCIPHER

Covertix SmartCipher protects any type of file used anywhere inside or outside the organization. A simple yet sophisticated rule set embedded in the file determines where, when, and by whom materials can be viewed, printed, changed and shared.

United States and Canada: + (866) 885-4148 | International: +972 (0)9-765-7726
info@covertix.com | www.covertix.com