

CipherApps for Google Docs is a unique cloud encryption solution that provides an invisible encryption layer to protect your data on the Cloud. CipherApps secures your cloud data in real-time prior to it ever leaving the enterprise network. The customer retains full control of the encryption keys while their data resides securely on the service providers network.

Overview

The push towards cloud technologies is on a huge growth curve. The benefits of moving to the cloud are numerous ranging from lower IT costs, access to data from any location or device, to real-time collaboration. However this in-turn raises new concerns about the privacy and security of corporate data on third-party servers.

For organizations in the financial, healthcare, legal and governmental sectors, there already exist compliance requirements that prevent them from storing any data on the cloud without on-premise encryption.

CipherApps enables the benefits of cloud collaboration (documents, email social media), while ensuring that no third-party or the cloud provider can access your data while it resides on the cloud.

CipherApps encrypts your sensitive data and gives you full control over the cryptographic keys thereby ensuring that no data resides in the cloud in the clear.

How it Works

The CipherApps “reverse-proxy” is a unified gateway solution through which all your corporate data is transmitted securely to-and-from the cloud. The encryption process invisible to the end users and there is no change to the user workflow.

In terms of document collaboration (e.g. Google Docs and Office 365), CipherApps preserves the real-time collaborative aspects of these services, and allows users to simultaneously edit and view documents in the clear, while encrypting all data to-and-from the cloud.

CipherApps makes use of industry standard encryption (AES-256). Our encryption engine is not tied to any particular algorithm, and we can make use of any open encryption standards.

The Key Management System (KMS), which is the cryptographic key repository allows for the seamless exchange of keys between users that wish to collaborate on documents.

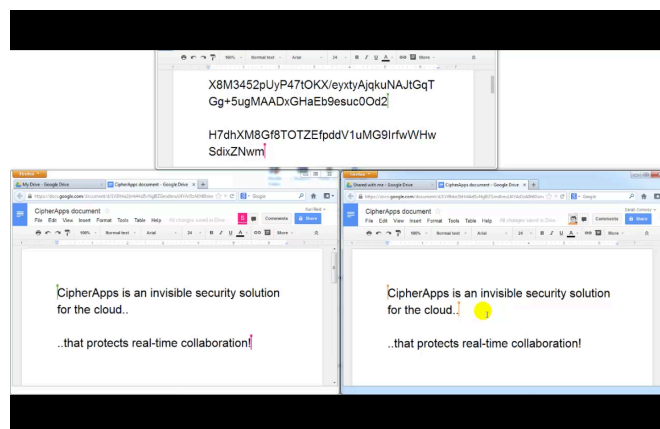
Multiple Deployment Options The security gateway can be hosted and managed by CipherApps. This is an ideal solution for small and medium businesses that can immediately on-board all of their employees onto the system without having to perform any software install or to train their employees to use the system. CipherApps can also provide an on-premise hosted solution.

Support for all Web Browsers and Mobile Employees The CipherApps Security Gateway is browser agnostic i.e. users are able to connect to the Google Docs service through the browser of their choice. Also, the CipherApps gateway can be public facing so that it allows mobile employees to securely access their documents while they are outside the enterprise firewall.

Enterprise Key Management All the keys on the KMS are stored in an encrypted state. Even if the KMS were to be pulled out of the rack, an attacker would not get access to the document keys unless they obtained the administrator credentials. Cryptographic keys can easily be rotated

Military Strength Encryption CipherApps uses standards-based AES 256-bit encryption, which is FIPS-compliant and has been extensively reviewed and tested by many independent organizations. It has become the de-facto encryption standard for commercial transactions in the private sector.

Highly Scalable Architecture The CipherApps architecture is highly scalable and capable of supporting large, deployments with extremely low latency.



Wayra Offices

Sir John Rogerson's Quay

Dublin, Ireland

Email: info@cipherapps.com

Tel: +353-87-2122008

Dublin 2, Ireland