clearswift
RUAG Cyber Security

Technical Solution Datasheet
Hosted Encryption Portal

With an ever growing need for secure business communication and collaboration methods, email still remains the primary means for most organizations to do business. However, the challenge for some organizations is how to communicate securely to their customers.

Professional Services

A number of additional consulting options are available to help with the deployment and configuration of this solution:

- Architecture Design
- Policy Design
- Solution Implementation

Products

- Clearswift SECURE Email Gateway
- Clearswift ARgon for Email

Technical Support

Clearswift provides 24/7 global support as standard, with additional options for premium support.

Hosted Portal Pricing
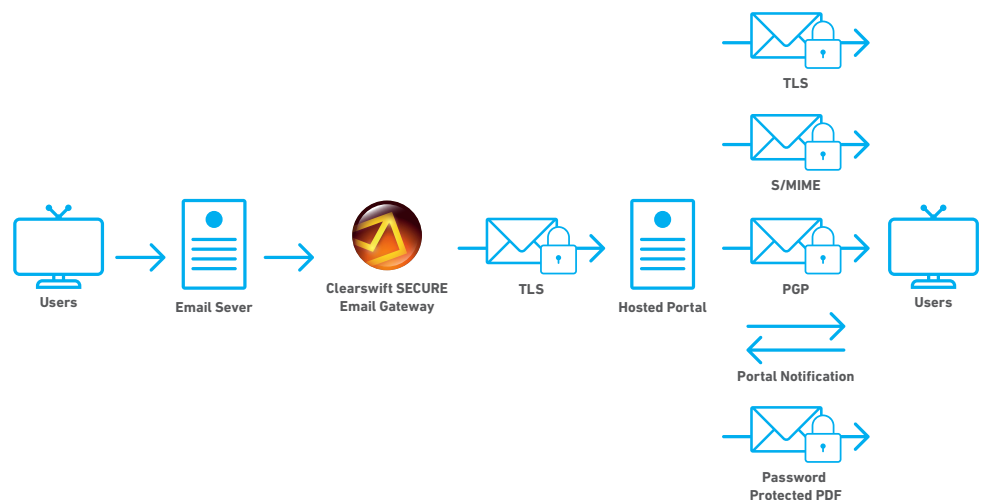
Priced per user.

Business Problem

Today's business run on information and collaboration. Collaboration which used to be internal is now just as likely to include external parties and while communication methods are established, the type of communication and the risks associated have also changed. With the advent of data breaches and the subsequent legal processes to reduce the risk, encrypting emails ensures that messages intercepted can not be viewed by anyone apart from the intended recipient.

With encryption can come complexity and for the techno-savvy power users, they can with that. But when you have a need to communicate to a non-technical consumer then we must adopt an encryption method that works easily for them. If recipients struggle to read and reply to messages, then they will simply stop using the system and the value of providing secure content delivery is lost.

Providing the greatest flexibility to define policy based encryption with the option to allow end users to control aspects of the encryption process ensures the message is delivered securely.

Deployment

As the solution is hosted is secure regional datacenters, deployment is very simple. Using a relay method, deliver messages over TLS to the hosted service and it will do the rest based on how its been configured to deliver mail. This mechanism takes the guess work of which secure delivery method to use as it can try alternative encryption methods.

Architecture

The managed services are delivered utilizing multiple, SSAE 16 SOC2 Type II certified secure, independently operated data centers in the U.S., Canada, and Europe.

User Experience

As the sender of the message, the encryption process maybe fully automated, based on the source/destination or content the Gateway will decide if the content requires encryption. However, the flexibility allows the end user can also have control over encryption through an Outlook (and OWA) plugin allows the sender to be involved in the encryption process. This is particularly useful in call centers allowing senders to encrypt the data using a pass phrase that the recipient knows.
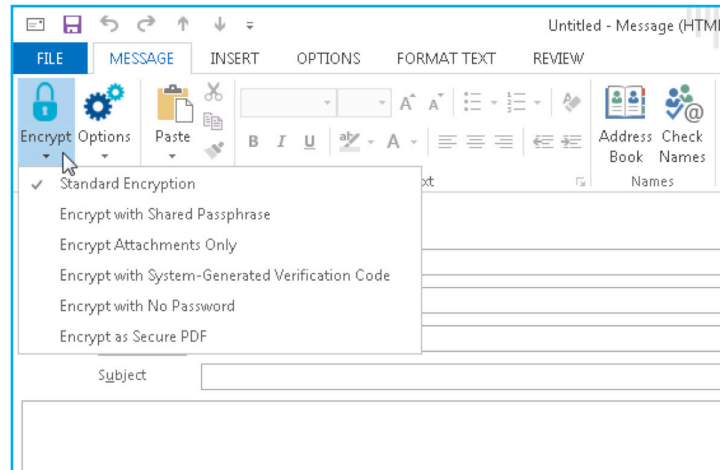
Depending on the method of encryption used the recipient receives a message with either an attachment in the case of PDF or links to a Web based portal where they connect via a browser allowing them to read and reply to messages in a familiar format as other Web based mail systems.