cobweb

LIBERATING TECHNOLOGY

UNCLASSIFIED

26/05/2016 v1.4

Advanced Email Encryption
Service Description

Introduction:

Cobweb have partnered with Cirius to provide a completely secure, standalone solution that integrates seamlessly with Hosted Exchange, Office 365 and On-Premise deployments.

The Cobweb Advanced Email Encryption Service enables professionals to send, receive and track confidential email and attachments on any device, anytime, anywhere. This enables companies to protect their data, meet compliance requirements, and speed up workflow with innovative and secure corporate messaging. Features like ForwardFreeze, For Your Eyes Only and message tracking drive adoption amongst employees and exceed user expectations.

Traditional email encryption, data leak protection and file transfer solutions have a reputation for being difficult to deploy, and most importantly use. Cobweb's Advanced Email Encryption service provides a seamless solution that, once activated, can be up and running in minutes offering users a more enjoyable experience.

1. Benefits of Advanced Email Encryption

- Security without complexity: securely send and receive confidential emails and file attachments from any device, anytime, anywhere
- With Data Leak Protection you can avoid damaging your company's brand and incurring financial liabilities caused by unintended data leaks
- Prevent the forwarding of sensitive information, or immediately recall emails sent in error
- Offers the ability to protect your corporate transactions conducted via email by creating auditable and retrievable corporate records
- Create custom rules to block sensitive content from leaving your company or to prompt users to send their message securely to protect information such as credit card numbers and HR documents.
- Send files of up to 25GB in size without burdening your customer's inbox
- Simple, scalable and flexible deployment from a single department to the entire enterprise so you can have Advanced Email Encryption up and running quickly
- Eliminates costly in-person, paper, phone, fax and courier-based processes

2. Secure Messaging

The Advanced Email Encryption platform enables professionals to send, receive and track confidential emails and attachments on any device, anytime, anywhere. Protect data, meet compliance requirements, and speed up workflow with innovative secure corporate messaging. Features like ForwardFreeze, For Your Eyes Only (F.Y.E.O.) and message tracking drive user adoption and exceed expectations.

- **Email encryption:** Send, receive and track secure corporate messages and attachments using any existing email address or platform.
- **Patented Delivery Slip:** Track and prove when an email is received, read, replied to, forwarded, deleted or printed.
- **Any device, anywhere:** Native apps and secure browser access for all smartphones and tablets.
- **Simplicity:** Secure messaging that works the way you do. Seamless integration with all common email platforms including Office 365, Cobweb Hosted Exchange and Gmail. Simple one-click access for recipients.
- **Unique Security Features:** Message control features such as ForwardFreeze and patented F.Y.E.O. provide enhanced protection for ultrasensitive messages.

3. Data Leak Protection

Data Leak Protection (DLP) offers a simple, powerful data loss protection solution. Enabled via a simple desktop deployment or Gateway, it's the only DLP solution that provides patented Pre-Send and Post-Send message controls. Hit send with confidence.

- **Advanced encryption:** Desktop or Gateway policy-based encryption and content filtering.
- **Unique Pre-Send & Post-Send Controls:** The only DLP solution that provides patented Pre-Send and Post-Send message controls.
- **Prevents data from being sent unsecured:** If certain keywords, number patterns, domains, or attachments are detected.
- **Administration console:** Enables easy global rule management for all staff.
- **API integration:** Integration with existing DLP rules engines.
- **No impact on existing infrastructure:** Cloud deployment does not impact existing infrastructure and requires only Outlook, Office 365 or optional Gateway.
- **Complete Message Recall:** Instant retraction of messages and attachments even after the message has been read. No permission required.

4. Technical Overview & System Security

Cobweb's Advanced Email Encryption platform enables organizations of all sizes to create and deploy a Secure Messaging portal for purposes of exchanging confidential information securely. The portals, or 'customers', are branded messaging communities that complement existing email by adding security, compliance, and productivity. They do not replace existing email servers or require changing end-users' email addresses. Every message is secure, tracked and auditable. It supports asynchronous large file transfers and storing of secure messages decrypted in all mail servers (e.g., Microsoft Exchange®, Office 365®, Google Mail®, or any third-party compliance archiving system or document management system) through a powerful rest-based API.

The Advanced Email Encryption platform is a simplified approach to security that eliminates the use of key distribution systems (Public Key Infrastructure – PKI) allowing easy Cloud deployment, without sacrificing security and privacy levels expected from these types of solutions. It is designed to meet the smallest to the most demanding secure messaging requirements. The email encryption platform acts as a secure message community by adding a more reliable protocol that sits on top of existing email infrastructure while remaining completely backward compatible with existing infrastructure. It is offered both as a Cloud client-side deployment with a Microsoft Outlook plug-in (gateway or mail server integration is not required), or as an enterprise deployment with a Secure Messaging Gateway.

- The optional plug-in for Microsoft Outlook® extends the functionality of the system and the patented Delivery Slip without requiring any mail server modifications for both sender and recipient.
- No changes are required to the user's email address, email program or email server. Microsoft Hosted Exchange®, Office365® and Google Apps® are all supported.
- All communications with the browser or Microsoft Outlook® are secured with HTTPS – confidential data is never exposed to an unsecure SMTP route. On 'SEND', Outlook intercepts the command and reroutes the message and file attachments securely via HTTPS, instead of sending the encrypted message via SMTP. At this stage, the user is authenticated. Once the data is transferred securely to the Secure Messaging platform, the message content and file attachments are encrypted 'at rest' using AES 256bit. No complex keys to rotate.
- The email encryption platform cloud servers are hosted in world class tier-1 data centres based in the United Kingdom. All data in transit is secured with a minimum of 128bit SSL and 256bit AES at-rest encryption using Microsoft's .NET Framework AES algorithm (AesCryptoServiceProvider class), a FIPS 140-2 compliant library. The Secure Messaging platform servers are used as a different 'route' (instead of using unsecure SMTP) and do not create a separate mail store.
- Secure messages are stored encrypted using industry standard encryption methods through the use of the patented Interchangeable Cryptographic Engine and can be adapted to the organization's needs. The default configuration uses AES 256-bit encryption for data-at-rest storage – instead of over the internet on unprotected, public SMTP servers, such as with basic email (even if emails are encrypted). AES 256-bit is the only publicly available cipher certified for official government documents classified as 'Top Secret'. It eliminates cross-contamination of data with a multi-tenanted Cloud offering, ensures that the organization's data is not tampered with or edited over time, and is automatically archived indefinitely.

5. Platforms Supported & Access Methods

- **Email:** Microsoft Exchange®, Microsoft Hosted Exchange®, Office365®, IBM Domino® Google Apps®, Yahoo®, Zimbra®, Open-Xchange®
- **Mobile O/S:** iOS®, Android®, Windows Phone 8®, Blackberry 10®
- **Other Web Apps:** Google Chrome extension, Office 365 Web App

If Advanced Email Encryption is used in conjunction with Cobweb's Email Disclaimer, Email Mail Disclaimers and Disclaimers will be applied to standard emails but will not append to emails sent securely.

6. Data Retention

An Administrator has the ability to specify how long the records should be stored in the Secure Messaging platform. Enabling this feature allows setting up a retention period (e.g., 7 years) after which all secure messages and associated file attachments are deleted from the server. By default, this feature is disabled and retains records indefinitely. Note that this feature does not remove or expire messages that were previously downloaded into Outlook or an archive. It simply deletes the records from the central messaging servers. If disabled, records are not deleted until the service is cancelled.

In order to ensure the integrity and confidentiality of all secure content, it is not possible to perform a mass export of secure messages upon service termination. This would compromise the intent of Advanced Email Encryption. It is recommended that any customer wishing to have access to secure content, use the solutions alongside Email Archive.

Advanced Email Encryption is not an Archiving solution as there is no dedicated container of readable data that an administrator would have the ability to access. Advanced Email Encryption does work with any third-party archiving vendor in order to ensure that any secure message that is sent and/or received is captured in a readable format within the archive.

If you cancel your subscription to Advanced Email Encryption, any content that has been sent securely will no longer be accessible outside of an email archive.

7. Data Ownership

At all times, the data stored within the Cobweb Hosted Exchange service is the property of the customer. In the case of service termination. In order to ensure the integrity and confidentiality of all secure content, it is not possible to perform a mass export of secure messages upon service termination. This would compromise the intent of Advanced Email Encryption. It is recommended that any customer wishing to have access to secure content, use the solution alongside Email Archive.

8. Service Availability

The Advanced Email Encryption platform is maintained in such a manner as to provide users with the best possible performance of the operated products. It can take up to 3 days from delivery of the signed order form for this service to be activated. The Service Level Agreement (SLA) does not cover outages due to scheduled or emergency network and/or facility maintenance, which shall be broadcast at least 48 hours in advance for planned maintenance and as soon as practicable (using commercially reasonable efforts to provide 24 hours' notice) for emergency maintenance, including maintenances deemed non-disruptive. This SLA does not cover outages or downtime where the internet from the user to the email encryption platform is unavailable or where the cause is due to a loss of connection from the user or the user's service provider.

9. Standard Support

The service is supported 24/7 via the Email and Online Support Form for all severities and, in addition, by telephone for Severity 1 incidents.

- Severity 1 incidents, as defined by the Service Level Agreement, will be progressed 24/7
- Severity 2, 3 and 4 incidents will be progressed during core hours of business – including service set-up/configuration with 'Cobweb Control Panel' and billing support by telephone
- Access to administrator support is for two named company administrators per customer account
- Core Hours: 08:00 hrs to 18:00 hrs GMT time zone, excluding weekends and UK public holidays

10. Administration

Administration is provided through the web-based "Control Panel" Self Care Administration Portal or via request to support@cobweb.com

- Provisioning with multiple email domains can add alias profiles to each user to maintain communication integrity
- Customers with multiple email domains can add alias profiles to each user to maintain communication integrity
- Custom branding can be added to a Secure Messaging portal via request to support@cobweb.com