Secure communication is an essential part of your email solution

Email security solutions aren’t just about preventing emails from entering or leaving your organization, a well-designed system will also assist employees in performing their jobs effectively and securely. Sometimes sensitive or confidential information needs to be shared outside your organization and so enabling employees to communicate with external contacts in a secure, controlled manner is essential. Mimecast Closed Circuit Messaging (CCM™) enables users to communicate with external parties through secure webmail in accordance with your organization’s email security policy, ensuring the delivery of tamper-proof secure email with non-repudiation.

Benefits-at-a-glance:

• **Secure email communication with all partners and customers**
  Mimecast CCM enables two-way email communication with all external parties via secure webmail, regardless of their mail server capability or encryption technologies used, affording universal secure mail delivery.

• **Enhanced control of sensitive information**
  Even with encrypted email you have no control or visibility of what happens to that email once it arrives in the recipient’s mailbox. With Mimecast CCM the recipient is confined to forwarding the email to users in your domains only.

• **Consistent implementation of email security policy**
  Centrally administered granular policies ensure that email communication is automatically secured in accordance with your organization’s email security policy to protect sensitive information and meet regulatory compliance.

• **Seamless and transparent secure communication for end users**
  Messages identified by administrator-defined policies for secure communication can have the CCM delivery method applied without users having to make that decision or learn any necessary procedures.

• **Complete email security from a single Software-as-a-Service (SaaS) solution minimizes administration**
  Administered from a single web-based interface, Mimecast centrally enforces your organization’s complete email security policy, including secure communication, without any additional hardware or software to deploy or administer.

Key features:

**Universal secure email with Closed Circuit Messaging**

Mimecast CCM enables secure two-way communication between users and external parties. This method of communication is inherently secure as the email never leaves the Mimecast service, remaining within the secure infrastructure at all times, and is also universally applicable as no other service or technology is required by sender or recipient. Recipients are notified by a customizable email that they have a message available for viewing online and a secure URL link is provided which will take them to the Mimecast service. First time recipients will also be sent a password notification message containing initial logon information enabling them to view and respond to this and future secure messages.

**Controlled two-way communication**

With an encrypted email connection you have the benefit of secure delivery, however you have no control of what happens to that email once it arrives in the recipient’s mailbox. Mimecast CCM not only offers secure delivery but gives you control over what action can be taken by the recipient on that email. From within the CCM mailbox users are unable to forward the secure message to any other recipients outside your domain. Alternatively you can choose to apply more stringent controls and prevent them from sending any emails whatsoever from their Mimecast CCM account. This granular control of CCM user capability gives you the benefit of secure, controlled two-way communication with your partners and customers with the flexibility you need to meet your organization’s requirements.
Granular policy definition and enforcement

Granular policy administration within Mimecast lets you accurately reflect your organization's email security policy, enabling you to enforce delivery via CCM when appropriate, ensuring the secure delivery and control of sensitive emails. Administrator defined policies allow CCM to be invoked for email communication between specified users, groups or domains. In addition, it can be activated based on the content of the email, using content examination policies to identify sensitive or confidential information, supporting your organization's compliance and operational needs.

Auditable and secure communication

When Mimecast CCM is invoked for email delivery, the message remains within the highly secure Mimecast infrastructure, removing the risk of eavesdropping associated with traditional email delivery methods that send the message across the Internet. Details of delivery and any subsequent forwarding of the message within CCM are logged to support regulatory compliance and corporate governance needs.

Seamless and transparent to end users

The decision to use CCM for message delivery is made by centrally administered policies within Mimecast, taking the decision away from end users and ensuring that your secure communication policy is applied appropriately and consistently across the organization. In fact when CCM is used to deliver a message, the process is completely transparent to the sender, enabling secure communication with external parties but without the need to learn any new procedures or technologies. Recipients receive clear, concise instructions directly into their mailboxes telling them how to access their secure messages with no need for additional support or cryptographic key management by the customer.

Unified solution for all email security

Mimecast’s single web-based interface lets you centrally enforce and administer your organization's complete email security policy, including secure communication, without the need to deploy and support any additional hardware or software, saving time and freeing up resources.

Note: CCM may be purchased as an add-on service.