GlobalCerts

Fast&Secure™ Managed Services

Fast&Secure™ is a suite of SaaS solutions providing comprehensive email protection designed to meet today's data security challenges. Fast&Secure offers all the same email security features that help organizations overcome the technical hurdles traditionally associated with complicated encryption solutions, but in an easy to use, managed service. Our solution is hosted in redundant, highly secure SSAE 16 server environments. Most importantly, Fast&Secure incorporates sophisticated content inspection features that secure the email path from unwanted viruses, spyware or spam, and ensures that sensitive data and personal information is kept secured.

Email Encryption

Fast&Secure™ uses a variety of methods to automatically encrypt your sensitive emails depending on the situation:

- Automatic S/MIME encryption is used to encrypt outbound email whenever possible. All messages to other GlobalCerts customers, and any recipients that have a discoverable digital certificate will use S/MIME encryption.
- SecureMessenger™ encryption is used to send to 3rd parties that do not have an S/MIME key. This method uses a web-based interface to allow the recipient to authenticate with a password of their choosing, and then view/reply to their secure email through a secure HTTPS interface.
- TLS encryption can also be used with specific partners to automatically encrypt email communications between your organization and their email servers at the server level. TLS is used whenever possible when sending out emails through Fast&Secure, even when other methods are also used.

Content Filtering

Content filtering, or Data Loss Prevention (DLP) fills the largest security holes in a company's email network. Fast&Secure™ can monitor and stop the accidental or intentional disclosure of a company's Intellectual Property, confidential information, or customer/patient information that may be disclosed via email.

- Custom policies are used to search email content and can be applied to incoming or outgoing emails. Each rule has a 'condition set' or dictionary and an 'action' such as: blocking the email, quarantining it, or encrypting it.
- DLP includes multi-language support, word stemming, proximity searching, and deep content analysis, allowing for inspection of most types of attachments. It also supports the use of Regular Expression (RegEx) Searching as well as Advanced Keyword Syntax.
- Automatically send notifications to the sender or an auditor when certain policies are matched.

Advanced Anti-Spam/Anti-Virus

Fast&Secure™ uses multi-tiered spam and virus engines to inspect every email coming into your organization.

- Inspects all attributes of incoming emails, including sender IP addresses, message envelope headers and structure, as well as the unstructured content in the body of messages. It tests numerous connection-level data points, including DNS and MX record verification.
- Includes the fastest inline scanning virus engine available from our technology partner ESET. The AV engine helps administrators protect the organization against blended threats by employing automatic engine updates, zero-hour virus protection, IP reputation technology, and robust group policies.
- Online spam and virus quarantine available for all users, with ability to receive customized daily reports to users.