

Top 5 Requirements for Selecting an Encrypted eMail Security Solution.

1. **Ad-hoc eMail Communication:** Simple, intuitive authentication and user interface to deliver emails to anyone with a web browser.

Why Proofpoint Emerges from the Pack:

2. **No Key Management:** No keys to back up, no single root master secrets to protect, no PKI Certificates. Proofpoint manages the hard part of the encryption so the enterprise does not have to.

3. **Control Over the eMail:** No need to contact mail administrators! Users have the power to revoke that email on their own from their desktop or via a policy. Recipients are unable to open or forward the message reducing the overall risk of the enterprise.

4. **Seamless Mobile Messaging:** Users follow a link from their mobile devices to authenticate and read encrypted messages. No forwarding the email to an unknown address or secondary email answerback queues.

5. **Applying Encryption Intelligently:** Proofpoint's content filtering has the same power as the most sophisticated DLP tools including:

Structured Data Matches: Such as the presence of protected healthcare or financial information such as HIPAA codes, ABA routing numbers, domestic and international credit card numbers, US social security numbers, UK National Identity Card numbers and other "smart identifiers" as detected by Proofpoint Regulatory Compliance.

Unstructured Data Matches: Such as the presence of confidential information as detected by Proofpoint Digital Asset Security.

Keywords and Regular Expressions: found in the subject line or content of messages as defined in Proofpoint's email firewall.

Message Origin or Destination: Encrypt messages based on destination (e.g., a specific business partner or supplier) or sender. Messages can also be encrypted based on other message attributes such as attachment type.

Call S&L International for a 15-day demonstration.