proofpoint.

PROOFPOINT ESSENTIALS
EMAIL ENCRYPTION

Proofpoint Essentials Email Encryption helps small and medium-sized businesses automatically encrypt emails. This helps reduce the potentially negative impacts of data loss. Securing emails that contain sensitive data is one of your top priorities. As you know, losing confidential data or customer information can result in fines, bad press and loss of customer trust. More than two thirds of an organisation's intellectual property is exchanged via email among offices, partners and customers. Your people may be sending sensitive content unencrypted. Without proper compliance and internal policy oversight, you may run the risk of leaks and other exposure.

AUTOMATED AND POLICY-DRIVEN EMAIL ENCRYPTION

Essentials Email Encryption helps you stay compliant through policy-driven data loss prevention (DLP) and email encryption. You can automatically identify and secure sensitive outgoing information. This includes PII, PHI, financial information, GDPR terms and many more with built-in term dictionaries and SmartSearch identifiers.

Essentials Email Encryption allows you to protect your sensitive data—and you can still make it readily available to affiliates, business partners and your people on their desktops and mobile devices. We help you monitor all content in an email communication. When we identify sensitive data, we automatically encrypt the email. This way, you can maximise your security without impacting your users. You create a single point of control through integration with email policy and DLP. This helps you reduce the burden on your administrators.

USER-DEFINED ENCRYPTION

Your users can also encrypt emails in one quick and easy step. They just add a simple identifier in the subject line of the email. Recipients of the encrypted emails can read and respond to these emails through an intuitive Web portal. By authenticating the recipient, you can increase the level of security for the encrypted email. Only a valid recipient can access it. Encrypted emails time out after 15 days. After that, they are removed. Sensitive data is not retained any longer than needed.