proofpoint

Proofpoint Essentials

Email Encryption

Easy to use and Simple to Administer

- Organizations can create filters that automatically identify outbound emails that should be encrypted.
- End-users can trigger encryption by using a pre-defined tag in the email subject line.
- Internal users, including the original sender and internal recipients can compose, read and respond to all encrypted emails in their inbox.
- External users must use Secure Mail (web-based interface) in order read and respond to encrypted emails they have been sent.

Proofpoint Essentials Email Encryption is purpose built to help small and medium enterprises reduce the potential negative impacts of data loss by automatically encrypting email. The need to secure communications that contain sensitive data has never been greater. Fines, negative publicity and loss of customer trust await companies, both large and small, who lose confidential or customer information.

More than two thirds of an organization's intellectual property is typically exchanged by email between offices, partners, and customers. If sensitive content is being sent out without proper oversight regarding its compliance to government regulations as well as your own policies, it might not be encrypted—and you run the risk of leaks and other exposure.

Tailored for Small and Medium Enterprises

Small and medium enterprises need to remove the risk of sensitive material leaving the company. In order to cater for the bespoke requirements and changing needs of SMEs, organizations need an encryption solution that is cost effective, flexible and scalable. With limited time and resources, SMEs can find that training staff in the proper use of encryption systems can be a significant barrier to successful deployment of secure communications, but with Proofpoint Essentials, this process is much simpler.

Email encryption, as part of Proofpoint Essentials, enables organizations to send encrypted emails automatically—without end users having to take any action. Proofpoint makes sure information control is extended beyond the borders of the building—and so information risk is correspondingly reduced.

Automated Data Protection Policy

Proofpoint Essentials Email Encryption offers powerful, policy-driven encryption features that mitigate the risks associated with regulatory violations, data loss and corporate policy violations, while positively enabling critical business communications. Email Encryption is ideal for any organization that needs to protect sensitive data, while still making it readily available to appropriate affiliates, business partners and end users—on their desktops and mobile devices.

Proofpoint Essentials monitors all content being sent in an email communication, and if sensitive data is identified, the email is automatically encrypted. In this way security is maximized, without impacting end-users. The integration with email policy and Data Loss Prevention (DLP) creates a single point of control that can reduce the burden on administrators.

User Invoked Encryption

End users can also make the decision themselves to encrypt emails with the addition of a simple identifier in the subject line of the email. This quick and easy step encrypts the email to secure the communication.

Recipients of the encrypted emails have an intuitive web portal through which they can read and respond to the email. Authenticating the recipient further increases the level of security around the encrypted email ensuring that only the valid recipient can access it. All encrypted emails time out after 15 days and are removed from the service, ensuring that sensitive data is not retained for longer than necessary.