proofpoint.

PROOFPOINT ESSENTIALS

EMAIL ENCRYPTION

HIGHLIGHTS

- You can create filters that automatically identify outbound emails that should be encrypted
- Your users can trigger encryption by using a pre-defined tag in the subject line
- Your internal users, including the original sender and internal recipients, can compose, read and respond to encrypted emails in their inboxes
- External users can use Secure Mail, a web-based interface, in order to read and respond to encrypted emails they receive

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 organization'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 maximize 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.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.