proofpoint essentials

Email Filtering
Content Filtering

Proofpoint Essentials offers intelligent content filtering to effectively address the issue of confidential, malicious or inappropriate email content being sent or received by your business.

Email is vital for facilitating fast, effective corporate communications, however, it is essential that businesses manage the content of all messages entering and leaving their networks. Failure to do so can result in confidential information, offensive jokes, inappropriate language or unsafe attachments flowing in and out of your organisation without your knowledge and with harmful consequences.

How does the Content Rules Engine work?

Proofpoint Essentials offers a powerful, customisable rules engine. This facilitates both content and event-based email management whilst providing highly sensitive levels of control regarding email traffic. The service allows users to control where messages are sent to and how they should be filtered depending on specified rules with full visibility and control of features.

This sophisticated feature allows users to filter their email based on a series of select variables. Rules can be set to cater for a number of different situations offering a wealth of functionality. Users are able to filter emails based on various criteria such as message size, country of origin or destination. The rules can be directed to the user only, to a group of users chosen by the company administrator or even to the entire organization. Users are additionally able to edit and order rules to their own preferences.

Protecting you from Unwanted Content and Attachments

The Proofpoint Essentials Content Control Engine harnesses a range of proprietary technologies which determine whether or not each individual email is allowed into or out of the organisation. Completely configurable to your needs, the Proofpoint Essentials intelligent content filter enables the smaller enterprise to establish and enforce an appropriate 'acceptable use' policy. This functionality helps ensure employees are not jeopardising the security and reputation of the business whilst simultaneously exercises your duty of care by protecting employees from any potentially malicious emails. The email filter can be adjusted to disallow emails based on the content in the subject, body or header, based on the sender or recipient and also based on the type of attachment in the message, among other criteria.

proofpoint essentials

Key Content Filtering Features

- Detection of confidential or inappropriate text-based content.
- Comprehensive, highly flexible and intuitive filtering processes.
- Creation and enforcement of an acceptable use policy.
- Scanning within email header, subject and body.
- Detects a large variety of attachments including:
- Microsoft® Office
- PDF attachments
- Compressed file types
- Executable (EXE) & major media types

Filter rule options

- Filter emails based on size.
- Filter emails on content in subject, body or header.
- Filter emails based on sender or recipient.
- Filter emails based on attachment type.
- Filter emails based on country of origin or destination.
- Actions to allow, block, override spam filter or delete.
- User, Group or Entire Organisation based rules.
- Inbound or outbound options.
- Edit and order rules.
- Total visibility and control of filters.
- Full logging of all messages in real-time.
- Rapid search and audit