proofpoint

Proofpoint Essentials Email Filtering

Proofpoint MLX Technology

Key Features

- Contextual, lexical and image-based analysis
- Detection of subcategories of spam such as Phishing Attacks and Pornographic Spam
- Reputation Analysis for IP Addresses and URLs
- Bounce Management
- Obfuscation Detection
- Natural Language Tests
- International Language Analysis
- Outbound Spam Detection

Powered by Proofpoint MLX machine learning technology, Proofpoint Essentials provides the most effective anti-spam solution available to the SME. Mounting an effective defense against spam requires detection techniques that evolve as quickly as the attacks themselves. Proofpoint MLX™ technology uses advanced machine learning techniques to provide comprehensive spam detection that guards against the spam threats of today, as well as tomorrow. Proofpoint MLX continuously analyzes millions of messages and automatically adjusts its detection algorithms to identify even the newest, most cunning types of attacks. Proofpoint MLX provides accurate, adaptive, and continuous protection against spam without requiring manual tuning or administrator intervention.

Machine Learning in Action

Through its pioneering research, Proofpoint has developed a highly configurable message-processing platform that provides a comprehensive defense against spam, viruses, and other messaging threats. The advanced machine learning classifiers and enterprise-strength platform enable the Proofpoint Essentials solution to synthesize large amounts of data, analyze millions of message characteristics, and classify messages with a very high degree of confidence, resulting in a high rate of effectiveness and a very low rate of false positives.

Proofpoint MLX Technology:

- Continuously adapts: to detect new types of spam without manual intervention—the system's ability to identify spam does not degrade as spammers change their tactics.
- Employs next generation machine learning techniques: including logistic regression and information gain techniques to build large-scale statistical models that accurately represent dependencies among spam attributes and delineate the boundary between spam and valid messages.
- Includes image- and attachment- specific machine learning techniques: to accurately identify even the most sophisticated spam messages. Proofpoint continues to identify the latest attachment-based spamming techniques and has built technology to handle these threats proactively and predictably. As new techniques emerge, Proofpoint delivers the latest spam detection technologies to customers automatically.
- Analyzes more than 1,000,000 spam attributes: including message envelope and header characteristics as well as the actual message and attachment content to accurately classify messages and ensure a low rate of false positives.
- Ensures the maximum protection today and improves in performance: even as spam evolves.

Proofpoint MLX Spam Detection Process

The MLX detection process begins at the Proofpoint Attack Response Center, where scientists and engineers build and refine mathematical models that represent Internet spam. These models are constantly updated and delivered to customers to ensure their messaging infrastructures stay ahead of the latest spam attacks.

Proofpoint examines every aspect of incoming messages, from the sender's IP address, to the message envelope, headers, and structure, and finally the content and formatting of the message's attachments and the message itself. At any given time, more than one million possible attributes—representing both content and structural components—may be taken into consideration. A typical message may trigger more than 300 MLX attributes.