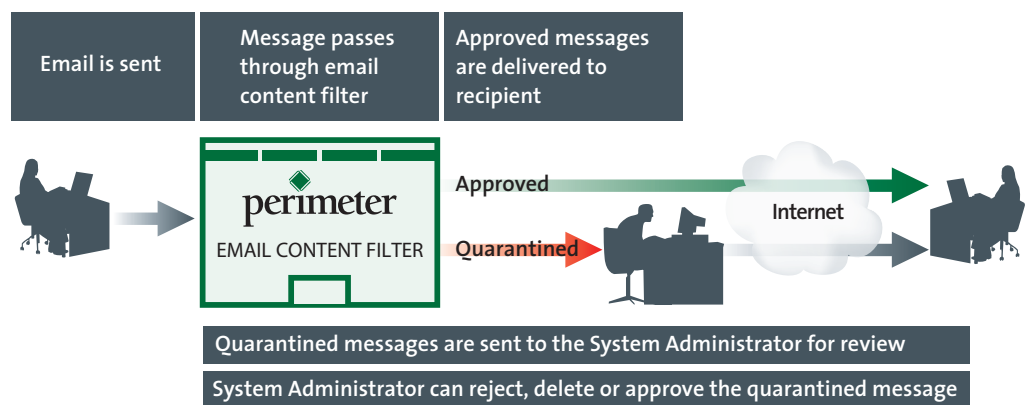# Email Content Filtering Service

THE PROBLEM OVERVIEW

Perimeter's Email Content Filtering Service helps organizations implement company policies associated with compliance, liability, reputation, and protection of confidential information:

- Intentional or unintentional communication of company confidential and non-public information

- Communication of inappropriate information or language exposing the company to legal liability and damage to reputation

Although the use of email technology has changed the way companies do business, it also brings with it many potential risks. Without visibility and control over the information leaving corporate email networks, organizations risk legal liability, regulatory violations and penalties, abuse of email resources, competitive threats and loss of priceless information – all resulting in significant costs and exposure. Enforcing an organization's Acceptable Use Policy with regard to email can be difficult without the right solution.

At Perimeter, we make it easy to implement and manage corporate communications policies that protect against these threats. By utilizing our Email Content Filtering Service, your organization can enforce communication policies that ensure compliance with government regulations (GLBA, HIPAA, SOX) and defined corporate policies, reduce legal liability by identifying risky language, protect confidential information from leaving the network, and cut operational costs by reducing the need for manual review and auditing.

Email is sent	Message passes through email content filter	Approved messages are delivered to recipient

perimeter
EMAIL CONTENT FILTER

Approved

Quarantined

Internet

Quarantined messages are sent to the System Administrator for review

System Administrator can reject, delete or approve the quarantined message

perimeter
eSecurity™

Complete. On Demand. Affordable.

THE PERIMETER SOLUTION

Perimeter's Email Content Filtering Service scans and filters all outbound email for categories of words, phrases, and numbers using dictionaries and rules preset according to best practices. Categories can be turned off and on, rules can be modified, and dictionaries can be added to or modified according to an individual company's policies. When a rule violation is detected, the specific email is quarantined by reason – word/phrase, number or custom rule. Then according to your own policy, the administrator has the ability to either approve the email for delivery, return to the user for modification with violating information highlighted (optionally copied to others for internal review), or delete the offending email. Management reports are compiled by period (this month, last month, year-to-date, all time) and summaries by rule violation, offenders, and message volume are available.

THE BENEFITS OF PERIMETER'S SOLUTION

Key Features	Benefits
Scans email for SSN, CCN, and custom numbers	Prevents inadvertent or intentional loss of confidential or non-public information
Scans email for inappropriate words & phrases	Protects company from legal liability and damage to reputation caused by offensive language
Administrator can set options for notification	Provides flexibility in timing of notification
Scans files and attachments	Protects against sending sensitive data in files or attachments

CATEGORIES/TYPES SCANNED INCLUDING:

Words/Phrases

- Adult
- Alcohol/Tobacco/Drugs
- Confidential (Custom)
- Gambling
- Hate Speech
- Violence/Weapons

Numbers

- ATM/Debit Card
- Bank Account
- Credit Card
- Patient Identifier
- Social Security
- Trade Account

INTRUSION DEFENSE
SYSTEM DEFENSE
USER DEFENSE
NETWORK DEFENSE
VULNERABILITY DEFENSE

perimeter
eSecurity™

EMAIL DEFENSE

Email Anti-Virus	eMessage Archiving
Content Filtering	Encrypted Email
SPAM Filtering	Hosted Exchange