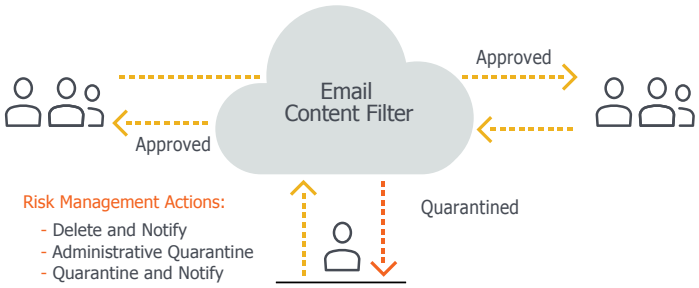
BAE SYSTEMS

Content Filtering

Powerful content filtering solution controlled by unified and web-based security management console

Content filtering technology from BAE Systems

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. Our content filtering service provides the tools you need to control email and minimize liability associated with inappropriate content via a sophisticated Web-based policy management tool. Email administrators can set rules to scan inbound and outbound email message attributes for specific keywords, file types, specific senders, phrases or patterns to help build powerful content security rules that map to corporate communication policies, regulatory requirements, or intellectual property practices.



Security management console

The Web-based Security Management Console from BAE Systems allows all content filtering policies to be centrally defined and managed for specific communication between internal and external parties and can play a critical role in enforcing an organization's security and compliance policies. The solution allows company administrators to manage the transmission of private or confidential information, maintain records of communication, and monitor all email traffic. It also provides the granular control needed to handle complex messaging scenarios, such as messages with multiple recipients.

www.baesystems.com/businessdefence

DMARC, DKIM and SPF support

The content filtering service from BAE Systems uses leading authentication protocols for a complete message validation solution:

- DMARC – Domain-based Message Authentication, Reporting and Conformance
- DKIM – DomainKeys Identified Mail
- SPF – Sender Policy Framework.

Our DMARC policy expands on the SPF and DKIM authentication mechanisms, and standardizes how email receivers perform email authentication, so that senders will experience consistent authentication results. DMARC effectively removes guesswork from the receiver's handling of these failed messages, and eliminates the user's exposure to potentially fraudulent and harmful messages.

Our content filtering service provides:

- Strong brand and reputation protection
- Visibility into exactly who's sending mail from your domain
- More reliable email messaging for safe and consistent business communications No migration or integration required.

Benefits of content filtering

- Rapid, effortless activation. No migration or integration required
- No up front costs. Decreased IT and administrative costs
- Sophisticated and intuitive web-based Security Management Console
- Regularly emailed message quarantine "digests" facilitate timely management of quarantine
- Increased employee productivity and reduced corporate liability

Categories/types scanned:

Words/Phrases

- Adult
- Alcohol/tobacco/ drugs + confidential (custom) + gambling
- Hate speech.
- Violence/weapons.

Numbers

- ATM/debit and credit cards/bank accounts
- Social security
- Patient identifiers
- Trade account.

Policy configuration options

- Global inbound and outbound quarantine polices for inappropriate language; suspect attachments (e.g. .exe); [SPAM] in the subject line; image attachments; video and audio attachments. Plus, all policies with the exception of the global policies support "glob style" matching that matches strings against patterns containing characters such as '*' (wildcard) and '?' (joker)
- Email address blacklists and whitelists
- User-specific policies such as filename analysis to prevent certain users within your domain from receiving messages with attachments
- Outbound document prevention containing a list of email addresses that match against the FROM address list to prevent certain users within your domain from sending messages with attachments
- Text analysis of a list of words or phrases that match against the text portions of messages
- Text (legal) disclaimers which can be added to all outbound email messages.

Content filtering vs. Data Loss Prevention

While the Email DLP solution from BAE Systems offers a powerful and effective method for many applications, the following comparison chart shows the key differences between our content filtering technology and our Data Loss Prevention solution.

Content filtering	Data Loss Prevention
Comprehensive policy support.	Complex, multi-layered policy support.
5 inbound/outbound tests for credit cards, social security numbers, profane language and customer banned content, including regular expressions.	50+ inbound/outbound logical tests, including credit cards, social security numbers, regular expressions, country of origin, sender, contextual and proximity analysis and much more.
4 risk management policy actions: delete and notify, administrative quarantine, and quarantine and notify.	25+ risk management policy actions including blocking, quarantines, encryption, archiving, and review/approval workflows.
Nearly 30 managed lists.	Scores of both managed and custom lists, ability to create new custom lists, scored word lists and regex lists.
General reporting capabilities.	Custom tags available for advanced reporting capabilities

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

UK: +44 (0) 1483 816000

E: learn@baesystems.com | W: baesystems.com/businessdefence

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai