

## Data Loss Protection (DLP)

The EdgeWave Messaging Security Suite includes a content analysis and policy engine that uses proprietary technology to protect private information transmitted via outgoing email. This data protection technology analyzes information being sent out of your network, to detect private content in data in motion and prevent sensitive and confidential data from leaving your network. EdgeWave DLP gives you the powerful tools you need to comply with government regulations, such as HIPAA and GLBA, and prevents the outbound communication of all types of private or objectionable data, including:

- Patient healthcare information
- Financial information
- Social Security Numbers
- Credit Card Numbers
- Profanity



## Proprietary Algorithms, Pattern Matching Technology

This DLP Service can be enabled in the EdgeWave Email Security solution whether you are using the hosted solution or have an appliance installed at the edge of your network to monitor all outbound SMTP traffic. In this configuration, EdgeWave DLP can perform the following:

- **Initial Detection:** DLP analyzes the content of data in motion to identify any sensitive data, such as private health or financial information, leaving the network.
- **Define & Enforce:** You can specify what action to take when a content analysis violation is found: deliver to recipient, hold in quarantine for review, or block.
- **Content Analysis:** Performs deep packet inspection in data and files being transferred on your network to analyze the content of reassembled network packets and identify private information that may be leaving your network. Content analysis is performed across numerous file types.

EdgeWave built-in content analysis helps you comply with regulatory legislation and defend against:

- Exposure of personal healthcare information
- Capture of financial information
- Credit Card Matching
- Social Security Number Matching

## Benefits

- Easy To Deploy
- Unprecedented Accuracy – Lexicons and logic engine allows precise deterministic analysis
- Low Latency – Proprietary technology rapidly analyzes and detects data triggering compliance enforcement

## Implementation Is Easy

Just route your SMTP email to the EdgeWave Email Security solution and configure the policies for DLP. The EdgeWave solution then analyzes the email leaving your organization for violations of any content analysis types that are enabled. You can also specify what action to take when a content analysis violation is found: hold in quarantine until further review or block. You may define rules that apply to all users or only to specified sender email addresses or content analysis types.

## Credit Card Matching

Major credit card companies use standard numbering sequences that are unique to each brand of card, such as Visa, MasterCard, or Discover. EdgeWave DLP catches any credit card numbers that might be leaving your organization with matching technology that recognizes the identifiable patterns of numbers all major credit card companies use. In addition, we employ the LUHN algorithm to validate the number, which virtually eliminates the possibility that messages will be incorrectly identified as policy violations.

## Social Security Numbers

EdgeWave DLP has a built-in extended regular expression that identifies U. S. Social Security numbers contained in data and files being transferred from your network. With identity theft still a critical, global problem, keeping this information from leaving your organization is vitally important.

## File Types Analyzed

In addition to the features mentioned, EdgeWave DLP analyzes many other types of files for private content. A table listing can be found on a separate data sheet



## Personal Healthcare and Financial Information

A lexicon is an xml file that contains a list of specialized vocabulary and phrases unique to a specific subject. EdgeWave DLP includes built-in lexicons for the financial and healthcare industries that prevent accidental or malicious exposure of personal health or financial information – a critical factor in complying with regulatory requirements. Our solution uses these and other lexicons to examine the contents of data and files, identifying specific words and phrases unique to the financial and healthcare industries. This feature also requires a match on information that would identify the person, helping prevent false positives. For example, if the phrase “broken tibia” is matched, information that would identify the person involved must also be matched, such as “client John Doe” or “patient number 0123456”.

Personal health information (PHI) is protected by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule enacted in 1996. Protection of personal financial information is required by the Gramm-Leach-Bliley Act (GLBA) enacted by the U.S. Congress in 1999.

## Objectionable Content

The DLP Service can be configured to filter out profanity using a common American English profanity lexicon.

---

## Other EdgeWave Messaging Security Services

### Email Security

Email Security provides unrivalled email defense against internal and external threats such as spam, viruses, spyware, phishing schemes, identity theft, and other dangerous or offensive content.

### Email Continuity

EdgeWave Email Continuity provides an uninterrupted flow of your email stream in case of unplanned or planned shutdown.

### Email Encryption

EdgeWave Email Encryption services assure the secure delivery of your email in accordance with your organization’s Security Policy, and provides confirmation of message delivery. Comprehensive reporting offers message tracking and an audit trail to support regulatory and other requirements.

### Email Archive

Our affordable Email Archive, with unlimited capacity, retains your email in an unalterable state to help you meet requirements for regulatory compliance, litigation issues and storage management needs.

**For more information see individual data sheets covering each of the above service in the EdgeWave Messaging Security Suite**

---

## About EdgeWave

The EdgeWave portfolio of Web, Email and Data Protection Technologies deliver comprehensive secure content management to 6,500 customers worldwide. Our award-winning iPrism Web Security and EdgeWave Email Security products are now complemented by Email Archiving and Data Protection Solutions, delivered as hosted, on-premises, and hybrid services. EdgeWave solutions protect your organization’s bottom line with unrivalled ease of deployment and the lowest TCO on the market.

### Contact Us

1-800-782-3762

[www.edgewave.com](http://www.edgewave.com)

### Corporate Office

15333 Avenue of Science, San Diego, CA 92128

Phone: 858-676-2277

Toll Free: 800-782-3762

Fax: 858-676-2299

Email: [info@edgewave.com](mailto:info@edgewave.com)