ePrism Email Security

Integrated DLP and Encryption modules protect organizations from data loss

EdgeWave ePrism Data Protection protects outbound email communications by securing corporate data from unauthorized leakage of sensitive data and assuring the secure delivery of business email. ePrism Data Protection Service includes powerful data loss protection and email encryption technologies that provide security and compliance support for organizations in all industries.

The data protection module provides advanced Data Loss Protection (DLP) technology that analyzes information being sent out of your network, to detect private content in data in motion and prevent sensitive and confidential data from leaving. ePrism DLP gives you the powerful tools you need to comply with government regulations, such as HIPAA, SOX, GLBA and others.

The ePrism Encryption module provides secure delivery of email to your customers, vendors, partners and other individuals, with next- generation technology that eliminates the cost and complexity associated with many traditional encryption services. With two encryption options available, there is no hardware or software to implement and encryption can be easily enabled as part of an automated routing policy associated with DLP policies, manually per user with an Outlook plug-in, or using an email subject line keyword.

Data Protection Service

Highlights

- Supports regulatory compliance, AUP and your peace-of mind by protecting confidentiality and privacy
- Easy setup and management and low TCO
- Integrated for multi-layered protection against emerging threats and data loss
- Supports all email gateways
- Requires no additional software or hardware
- Two encryption options to increase flexibility

DLP Module

ePrism DLP gives you the powerful tools you need to comply with government regulations and prevents the outbound communication of email containing all types of private or objectionable data, including:

- Patient healthcare information (PHI)
- Financial information
- Social Security Numbers
- Credit Card Numbers
- Custom word lists specific to your industry

How DLP Works

- 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.
- 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
- Define & Enforce: You can specify what action to take when a content analysis violation is found: Deliver to recipient, hold in quarantine for review, block or send encrypted.

ePrism's 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 ePrism Email Security solution and configure the policies for DLP. ePrism 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: Deliver to recipient, hold in quarantine for review, block or send encrypted

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. ePrism 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

ePrism 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, ePrism DLP analyzes almost 500 types of files for private content. A table listing can be found on a separate data sheet.

Personal Healthcare and Financial Information

ePrism DLP includes built-in word lists (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. Edgewave’s ePrism DLP is designed to help you achieve your regulatory compliance in an easy to use solution.

Objectionable Content

The DLP Service can be configured to monitor for key words that are specific to your industry or corporate policies. Even if your organization is not subject to government regulations there are numerous use cases where certain information should not be sent via email. From Human Resources to Finance content, the ePrism DLP service can help you rest easy knowing that email will be used for only the purpose you specify.

Email Encryption

ePrism Email encryption assures the secure delivery of email to your customers, vendors, partners and other individuals, with nextgeneration technology that is easier to use and less costly than traditional encryption services. Offering several types of encryption, the service can be easily enabled as part of an automated routing policy based on DLP settings. In addition, because it is integrated into ePrism Email Security and DLP services, your outgoing email is inspected for malware, viruses, inappropriate content, compliance breaches and violations of your corporate acceptable use policy (AUP) – a more multi-layered defense than a solo encryption service can offer.

Highlights

- Can be enabled by users or automatically triggered per administrator-defined DLP rules
- Assures the secure delivery of messages
- Supports regulatory compliance, AUP and your peace-of mind by protecting confidentiality and privacy
- Easy setup and management and low TCO
- Integrated with Email Security and DLP for multi-layered protection against emerging threats and data loss
- Supports all email gateways
- Requires no additional software or hardware
- Two encryption options to increase flexibility

Features

Comprehensive Encryption Coverage

It includes two forms of encryption so you receive comprehensive multi-layered protection and secure delivery of all private email leaving your network.

TLS Server-to-Server Encryption

TLS is a delivery method that encrypts communications between two email servers without end user intervention. With ePrism's TLS Server-to-Server encryption, email to specific domains can be sent using TLS based on DLP rules. This method assures that the encryption itself remains totally transparent to both sender and recipient. With a simple test available to confirm whether TLS Server-to-Server is an option you can configure as many domains as necessary thus providing the most transparent encryption solution possible to the maximum number of recipients.

Push Encryption

With Push Encryption, the message is encrypted and put in an html file that is attached to a notification message. The recipient receives the notification and attached encrypted message. Clicking on the attachment opens up a browser window where a login/signup page is displayed and after authentication the message is unencrypted and displayed. The recipient can respond or forward the message and download any attachments. Push encryption is appealing to those users that do not want the message to sit out in the cloud waiting to be picked up.

Park and Pull Encryption Services

ePrism Encryption Service includes park-and-pull technology designed to provide secure communication between the sender and the recipient of messages, even individuals outside and unrelated to your organization. All emails using encryption can be routed based on a variety of rules leveraging EdgeWave's email filtering technology. Park-and-pull encryption is enhanced so that encryption can be triggered by DLP rules. Once an email is routed for encryption, ePrism stores it securely in our secure Encryption Portal and notifies the recipient, who then registers and retrieves the email for further action. The park-and-pull technique does not require the installation of any software by the sender, recipient or on the email hosts of either. Nor does it require an encryption key to deliver the email. Security is assured by holding the email messages in a protected webmail interface until the recipient accesses them.

How Park-and-Pull Encryption Works

The message originator sends an email that is designated to be encrypted whether automatically per DLP rules, or manually per user. These encrypted sent messages are stored on EdgeWave's secured encrypted message portal. A notification message is sent to all recipients containing a link that takes the recipient to the secured web page where the message can be viewed and other actions taken. Recipients are identified by registering just once, after which they access the secured portal and can take action with messages including:

- Read
- Reply
- Delete
- Create
- Recall
- Save
- Print

Reporting

The reporting feature includes message tracking and audit trail, allowing you to manage and troubleshoot. These reports also support compliance with regulatory requirements by providing evidentiary data if legal issues should arise.

Other EdgeWave ePrism 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 Archive

Our affordable Email Archive 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 services