ePrism Email Security

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.

ePrism Email Security

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

4225 Executive Sq., Ste. 1600
La Jolla, CA 92037-1487

Give us a call:
1-800-782-3762

Send us an email:
info@edgewave.com

For more info, visit us at:
www.edgewave.com