

EdgeWave Email Encryption

EdgeWave Email encryption assures the 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. As a completely hosted service, there is no hardware or software to implement and encryption can be easily enabled on a per user basis or as part of an automated routing policy. In addition, because it is integrated into our Hosted Email Security and Data Loss Protection 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. As part of our comprehensive suite of secure messaging solutions, EdgeWave Encryption Service is the most cost-effective way to assure the confidentiality and secure delivery of private and sensitive communications leaving your network.



Highlights

- Can be enabled by users or automatically triggered per administrator-defined rules
- Assures the secure delivery of messages
- Supports regulatory compliance, AUP and your peace-of-mind by protecting confidentiality and privacy
- Completely hosted service with easy setup and management and low TCO
- Is integrated with Email Security and DLP for multi-layered protection against emerging threats and data loss
- Supports all email gateways
- Requires no software because the recipient interacts with messages via secure webmail interface
- Combines with EdgeWave TLS encryption for comprehensive protection

Features

Comprehensive Encryption Coverage

EdgeWave includes server-to-server encryption using standard transport layer security (TLS) as part of our Email Security service. When you add our optional park and pull encryption services, 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 by first having each mail server authenticate to the other, making it harder to send spoofed email. Then, the contents of the emails sent between the two servers are encrypted, protecting them while in transit. The encryption itself remains totally transparent to both sender and recipient.

Park and Pull Encryption Services

EdgeWave 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 by EdgeWave DLP so that encryption can be triggered by DLP violations. Once an email is routed for encryption, EdgeWave stores it securely in our Encryption Portal and notifies the recipient, who then registers and retrieves the email for further action. Unlike end-to-end encryption, 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 automatic per rules or manual per user. These encrypted sent messages are stored on EdgeWave's secured encrypted message portal and delivered to the recipient with an HTTPS page on the Web. 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 have a secured portal and can take action with messages including:

- Read
- Reply
- Delete
- Forward
- 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 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.

Data Loss Protection

This data protection technology analyzes data being sent out of your network to detect private content in data in motion and prevent sensitive and protected data from leaving your company.

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 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

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