Cisco Registered Envelope Service

Contents

Product overview

Organizations of all sizes face the same daunting challenge: email is simultaneously the most important business communication tool and the leading attack vector for security breaches. Cisco® Email Security enables users to communicate securely and helps organizations combat Business Email Compromise (BEC), ransomware, advanced malware, phishing, spam, and data loss with a multilayered approach to security. As part of this layered approach, Cisco® Registered Envelope Service offers a cloud email encryption solution that provides enhanced security and reliable controls for business emails. It is fully integrated with the Cisco Email Security workflow and into a user's daily email routine. The three pillars of the solution are confidentiality, ease of use, and enhanced email controls.

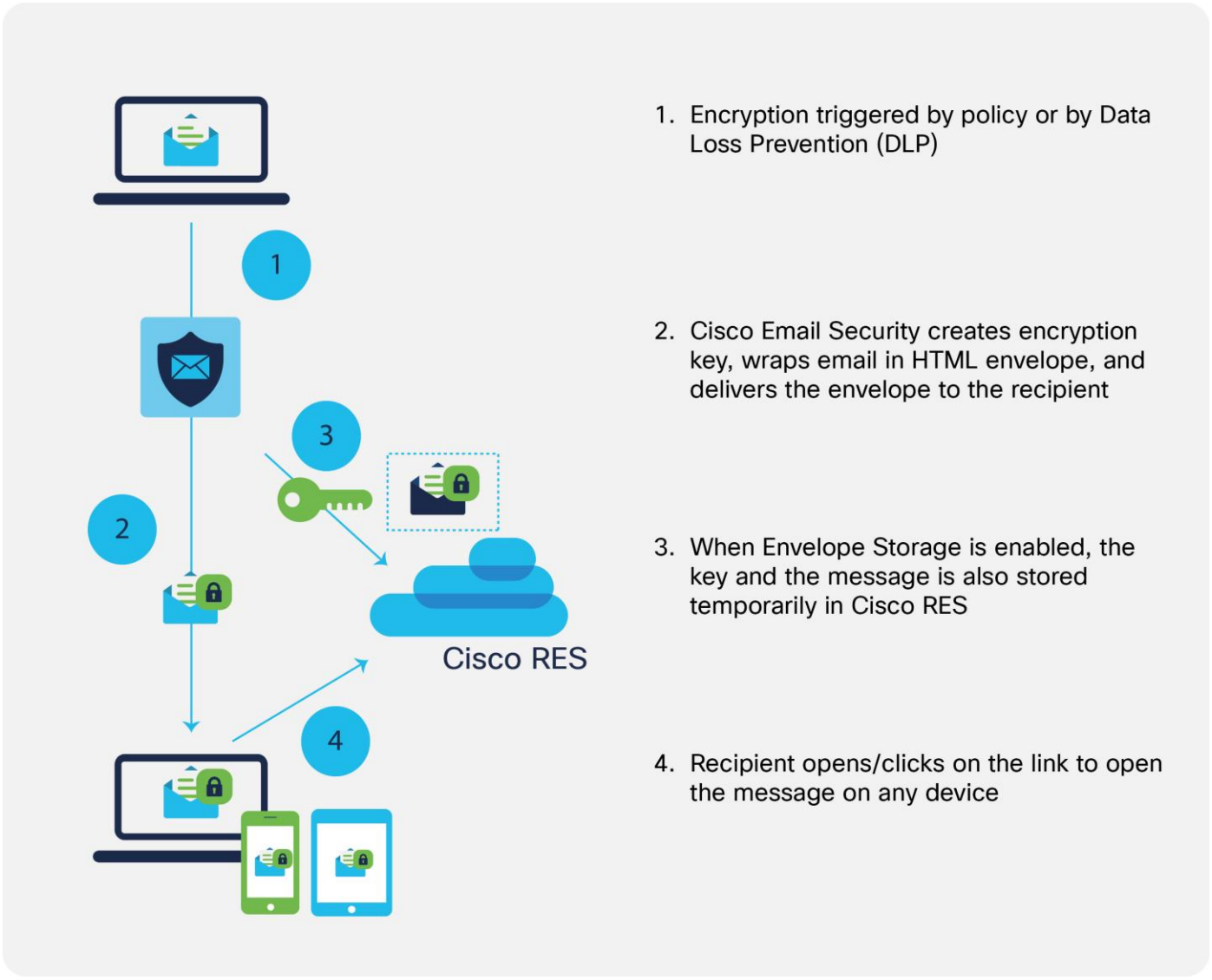

Figure 1.
Cisco Registered Envelope Service (Cisco RES)

Features

Although regular emails are not a secure information exchange medium, encryption and key management are often seen as too complex to be used in everyday communications. The Registered Envelope Service takes away the complexity behind encryption and makes it easy to send and receive highly secure messages, while maintaining confidentiality and control.

Confidentiality

- Registered Envelope Service is based on robust technology that uses the most reliable email encryption algorithms available. It also manages recipient registration, authentication, and per-message encryption keys with a cloud-based hosted key server.
- Enrollment management is provided for first-time recipients as they are guided through a single screen to create an account on the key server.
- Two-step verification ensures that the intended recipient is registered and authenticated before reading the email.
- Users can view secure messages either with their Cisco RES, corporate, or Google credentials. The corporate credential option is supported with **Security Assertion Markup Language (SAML) 2.0 gateway** integration, an advanced feature for organizations that have implemented an identity gateway allowing them to take advantage of their existing investment in the service.
- The support for both push and pull encryption provides flexibility for administrators to manage email encryption. With "push," encrypted email is delivered in HTML format to be opened by the user. With "pull," the user is directed to a portal to open the secure encrypted message.

Ease of use

- No software or agents to install: Registered Envelopes deliver the encrypted payload to the end recipient. This payload can be decrypted without the need for any software or applications installed on the endpoint.
- Consistent user experience: The Easy Open feature provides a unified method for opening secure messages on any device by temporarily storing the envelope.
- **Universal device support:** This makes it possible for highly secure messages to be read by any recipient regardless of the device used to open the message. Dedicated plug-in applications offer an enhanced user experience for Microsoft Outlook and on Apple iOS and Google Android smartphones.

Enhanced email controls

Cisco Registered Envelope Service provides senders full control to terminate or recall emails, and know exactly when an email was opened.

- **Read receipt:** When a recipient successfully authenticates and receives the encryption key to decrypt the message, the Registered Envelope Service delivers a read receipt to the sender in seconds.
- **Guaranteed message recall:** By selecting the recall option, the key to decrypt the data expires, making it impossible to access the message.

- **Message expiration:** Set an expiration date before sending a message, at which time that message is terminated. After the expiration date, the information becomes inaccessible.
- **Control over forward/reply:** Forward, Reply, and Reply All can be selected or disabled only if your company authorizes it.

Benefits

Helps ensure compliance

Cisco Registered Envelope Service enables customers to flag and then encrypt sensitive messages. This capability can be used by a customer to assist with their compliance with various laws and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI), Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA), Personal Information Protection and Electronic Documents Act (PIPEDA), European Union Data Directive, and European Union **General Data Protection Regulation (GDPR).**

Uses a federated identity gateway

Compatibility with SAML 2.0 gateways removes the need for new recipient registration and makes it possible for recipients to use their corporate identity to decrypt messages.

Provides business-class email

The powerful features support a new class of email, with exceptional visibility and control.

Fosters customer and partner trust

Encryption raises the level of service to customers and partners, exemplifying Cisco's commitment to keep business transactions and communications confidential.

Protects intellectual property

This solution safeguards sensitive business information and intellectual property contained in email outside the firewall, both in transit on the Internet and in storage on destination email servers.

Improves customer service

Organizations and their customers can communicate with an exceptional degree of security using the channels that customers prefer.

Summary

Cisco Registered Envelope Service provides a turnkey, enterprise-class email encryption solution without the need to deploy new hardware. Multiple highly secure delivery methods offer the flexibility to meet diverse business needs, while integrated management and authentication simplifies deployment.

For more information

More information can be found in the following documents:

Privacy data sheet: Cisco Registered Envelope Service

At-a-glance: Cisco Registered Envelope Service

Webpage: Cisco Email Encryption

Cisco environmental sustainability

Information about Cisco's environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the "Environment Sustainability" section of Cisco's Corporate Social Responsibility (CSR) Report.

Reference links to information about key environmental sustainability topics (mentioned in the "Environment Sustainability" section of the CSR Report) are provided in the following table:

Sustainability topic	Reference
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-677121-06 11/19