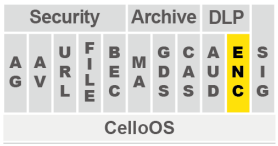
Easy Deployment

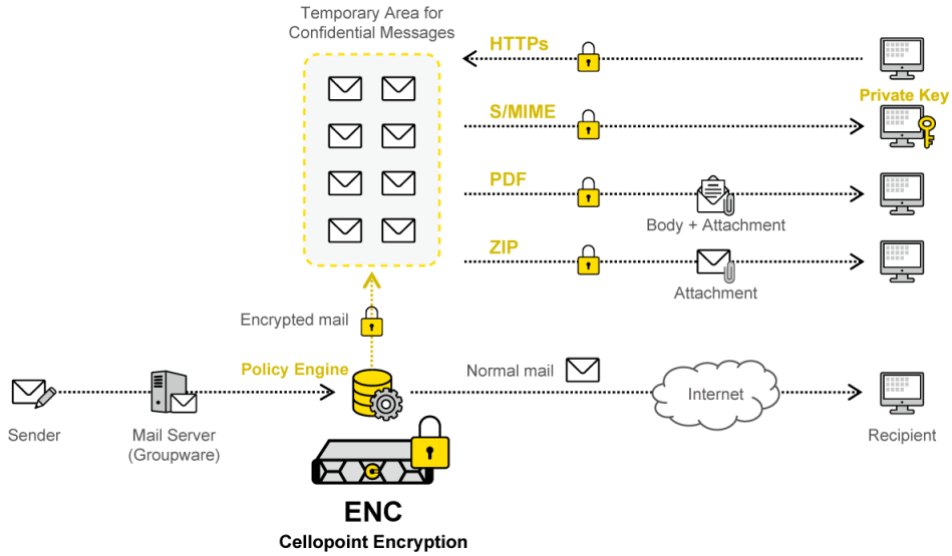
Secure Sensitive Data

Outbound Email DLP

Encryption (ENC)

Cellopoint Encryption (ENC) module is a gateway-based outbound email DLP solution. Utilizing CelloOS™ technology developed by CelloLabs™, it applies pre-defined DLP policies to identify outbound emails with confidential data. When a DLP policy is triggered, the email is encrypted, preventing plaintext transmission and ensuring secure delivery of your sensitive data and preventing data loss.





Email communication is convenient but comes with risks. Sensitive information sent in plaintext can be intercepted by attackers, leading to data leaks, misdirection, or unauthorized access. This can result in financial losses and damage to the company's reputation.

Implementing Cellopoint Encryption (ENC) module allows encrypted emails to be sent through your existing email system, easing the burden on IT staff by simplifying certificate management. This solution doesn't disrupt users' email workflows and provides recipients with a straightforward interface for reading encrypted emails, making the encryption process more efficient.

- **Encryption Policy Engine (PE):** Enables tailored encryption policies for organizational-wide, specific group, or individual needs. Organizations can automatically encrypt emails based on comprehensive AND/OR conditions, including:
  - Who (sender/ recipient/ IP address)
  - What (keywords)
  - When (different times/ dates/ cycles)
  - Where (sent locally/ sent externally and relayed through your organization's server)
  - Attachment Details (filename/ format)
  - Quantity and Size (number of attachments/ email size)

Problem Solving

- Organizational enforcement of encryption policies
- Compliance with data privacy regulations
- Secure email transmission
- Prevents sensitive data leaks

Benefits

- Industry-standard encryption
- Minimal license and maintenance costs
- Hassle-free automated encryption management
- No additional software installation required for users
- Seamless integration with existing email environments
- Issuance of public keys, private keys, and certificates
- Saves audit personnel management time
- Multiple encryption methods

ENC Highlights

- **Simple and Easy to Use:** Gateway-based encryption offer the most convenient deployment and management, avoiding the need for PC encryption software and simplifying secure email communication.
- **Policy-based Encryption:** Centralized, policy-based encryption protects sensitive data without changing existing internal workflows by automatically securing emails based on real-time content scanning.
- **Reduce Operational Costs:** Gateway-based encryption avoids the complexities, high costs, and management issues of client-side encryption.
- **Data Loss Prevention:** Industry-leading email encryption ensures that emails with confidential data are encrypted per policy, safeguarding data confidentiality and preventing sensitive data from being stolen.

How ENC works

- **HTTPs Encryption:** Users securely log in via HTTPS to preview and download encrypted emails ensuring Gateway-to-Client encryption from COENC to the recipient. Most users use web-based browsers, with SSL (Secure Socket Layer) over HTTP and the RSA (3DES) safeguarding confidential data.
- **S/MIME Encryption:** When recipients opt for S/MIME mode during registration, ENC generates a recipient-specific certificate (P12 file) and private key for automatic installation. Emails are sent to recipients using S/MIME encryption, ensuring Gateway-to-Client encryption from ENC to the recipient.
- **PDF Encryption:** ENC encrypts the original email into PDF attachment, requiring a password for access. Senders can specify or the system can generate passwords, providing flexible and convenient options to let the recipient obtain directly from the sender or sent by the system.
- **ZIP Encryption:** ENC encrypts the original email into ZIP attachment, requiring a password to unzip for access. Senders can specify or the system can generate passwords, providing flexible and convenient options to let the recipient obtain from the sender or sent by the system.

Supported Email Systems

- Microsoft Exchange 2016 / 2019 / 2022 / Microsoft 365 / Exchange Online
- Google Workspace
- Zimbra
- HCL Notes
- Sendmail / Qmail / Postfix

Specifications

ENC module	50, 100, 250	500, 1000, 2000	5000, 10K, 20K	Service Provider
Daily capacity	50K ~ 250K	500K ~ 2M	5M ~ 20M	Above 20M
Active email users**	50 ~ 250	500 ~ 2K	5K ~ 20K	20K+
Policy engine	✓	✓	✓	✓
HTTPs encryption	✓	✓	✓	✓
S/MIME encryption	✓	✓	✓	✓
PDF encryption	✓	✓	✓	✓
ZIP encryption	✓	✓	✓	✓

*Flexible module licensing includes an initial fee for first-year license access, followed by maintenance fees.

**The number of licenses is according to the number of email accounts.

***Cellopoint only provides software licenses; the appliance is not included.