



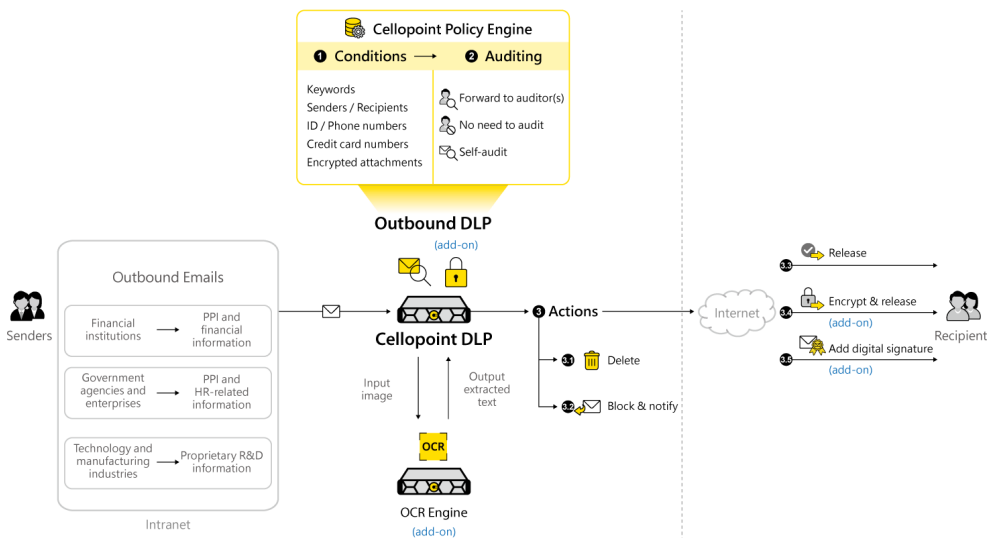
Provide comprehensive data loss prevention (DLP) to your messages.

Outbound Email DLP

Auditing (AUD)

Cellopoint Auditing (AUD) module is an outbound email DLP solution. It uses pre-defined DLP policies to identify outbound emails containing confidential data and apply appropriate actions such as auditing, blocking, forwarding, deleting, notifying, or encryption to prevent data from being misdirected, leaked, or accessed by unintended individuals. It helps organizations prevent data loss, and ensure compliance across cloud services such as Microsoft 365 and Google Workspace, or on-premises platforms like Exchange and Zimbra.

Security				Archive			DLP		
A	A	U	F	B	M	G	C	A	E
G	V	R	L	E	A	D	S	S	S
								A	U
								D	S
								I	N
								C	G
CelloOS									



Auditing Module Features

Real-time Scanning and Analysis: Includes outbound email headers, email bodies, compressed files (ZIP), and attachments (TXT, PDF, RTF, Word, Excel, PowerPoint).

Content-level Filtering: Identifies sensitive data, including built-in ID information and custom keywords using multi-dimensional classification.

Classification Criteria: Provides conditions such as ID numbers and credit card numbers, as well as email size, attachments, and recipients for auditing actions.

Robust Policy Settings: Flexible filter, action settings, compliance checks, integration with organizational policies for individual, departmental, and organizational policy management, ensuring email data loss prevention.

Real-time Audit - Prevent Data Leakage:

AUD scans outbound emails for sensitive data. If data leakage is detected, actions such as blocking, notifying, forwarding, deleting, or encrypting will be taken to help organizations prevent accidental or intentional leakage of confidential data.

Post-event Audit - Identify Unnoticed Risks:

Helps organizations to identify confidential historical email data, track its transmission, users involved, and final destinations. AUD scans, analyzes, and categorizes emails, storing all information in an audit database. Auditors can query email elements like senders, receivers, and sensitive content. Based on identified leaks, such as notifying managers or preserving evidence for litigation will be taken. (Mail Archiving module required)

Problem Solving

- Identifies organizational risks in real-time
- Reduces audit response time
- Flexible policy configuration management
- Efficient collection of legal evidence
- Customizable reporting as needed
- Personal data protection

Benefits

- Prevents sensitive data leaks
- Compliance with data privacy regulations
- Enhanced DLP
- Minimal license and maintenance costs
- Saves audit personnel management time
- Automates audit operations

Auditing Module Capabilities

- Creates a more secure IT environment and eliminates the risk of data loss (DLP)
- Gain a deeper understanding of organizational risks to assist in future policy formulations.
- Enhances the management of intellectual property and regulatory compliance.
- Transforms manual security policies into automated auditing, reducing management time and efforts.
- Responds to potential risks and policy violations in email communication immediately and ensures auditors receive notifications and can take prompt action.
- Customize policy priorities based on risks levels to adjust the order of processing.

Role-based Access Control: Defines permissions for employees, managers, and group administrators, enabling granular control and flexible DLP policy formulation.

Policy Engine: A single console for managing email policy settings, editing, deployment, and execution.

Features

- Data Loss Prevention
- Regulatory compliance
- Role-based access control
- Integration with AD/LDAP groups
- Improved email server performance
- Seamless integration with existing email environments

Supported Email Systems

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

Specifications

AUD 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+
Inbound / Outbound email filtering	✓	✓	✓	✓
Relay mode deployment	✓	✓	✓	✓
Transparent mode deployment	✓	✓	✓	✓
Ethernet	GbEx2	GbEx2	GbEx2	GbEx2

*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.