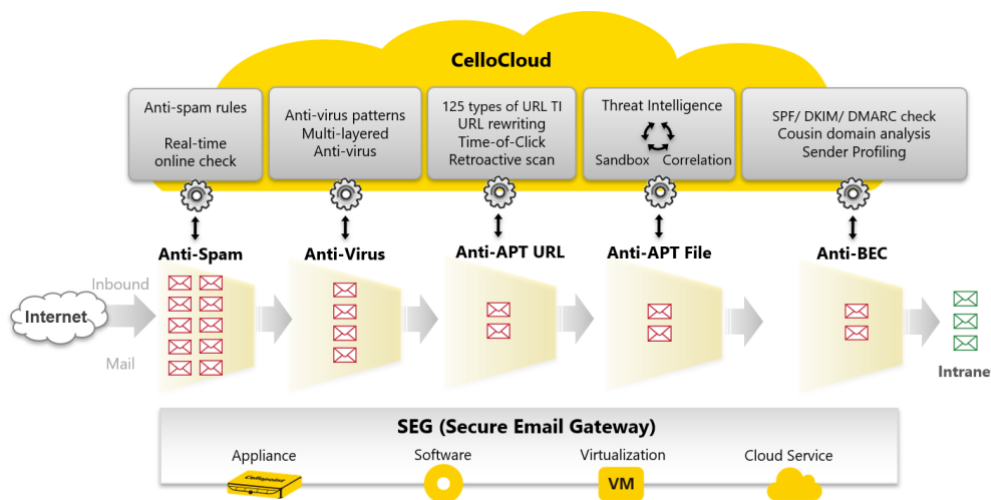**Hassle-free security issues.**
Save you time and trouble.

Secure Email Gateway (SEG)

Cellopoint Secure Email Gateway (SEG) is deployed in front of the email server. Utilizing the proprietary CelloOS™ and the advanced CelloCloud™ system, it features a multi-layer scanning mechanism for pre-delivery protection. This approach effectively thwarts all email threats, including advanced malware, ransomware, spam, viruses, phishing, BEC, spyware, email bombs, and relay attacks. It provides robust protection across cloud services like Microsoft 365, Exchange Online, and Google Workspace, or on-premises platforms such as Microsoft Exchange and Zimbra.

Problem Solving

- Prevents important emails from being buried in spam
- Avoids virus attacks
- Reduces external bandwidth waste
- Protects email servers from attacks
- Prevents APT email attacks
- Avoids ransomware attacks
- Prevents BEC fraud

Features

- 99.9% spam detection rate
- 99% virus detection rate
- 99% APT email attachment detection rate
- 99% APT email URL detection rate
- CelloCloud™ global monitoring
- Real-time email threat intelligence updates
- Personalized quarantine area
- AD/LDAP synchronization
- Web-based management interface
- Syslog and CEF log integration

First Layer: Anti-Spam (AG)

Connection Control

Blocks 50% to 80% of threats at initial SMTP connections, optimizing performance, saving network resources, and conserving storage.

DoS (Denial of Service) Defense

Protects against attacks aiming to overwhelm and disrupt the email system, ensuring continuous and reliable email service.

SRL (Sender Reputation List)

Monitors global sender IPs 24/7 via the CGAC (Cellopoint Global Anti-Spam Center), assigning reputation scores to block abnormal sender sources.

Anti-Relay

Prevents unauthorized use of an email server to relay large volumes of spam or unsolicited emails, thus avoiding IP blacklisting by RBLs.

Greylisting

Temporarily rejects emails from unknown senders to identify legitimate mail servers and block automated spam-sending programs.

SPF (Sender Policy Framework)

Verifies sender identity to prevent sender email address spoofing.

Multi-Layer Spam Filtering

Uses the CelloCloud™ database to collect and analyze spam characteristics to maintain a spam defense rate of over 99.9%.

Second Layer: Anti-Virus (AV)

Multi-layer Virus Scan

Uses advanced antivirus engines to provide virus scanning and online virus pattern updates, effectively eliminating various known email viruses, worms, spyware, trojans, ransomware, and other malware.

Third Layer: Anti-APT-URL

It provides three-phased defense: pre-click, time-of-click (ToC), and post-click, effectively detecting and blocking phishing URLs and malicious URLs that may trigger credential phishing, malware downloads, and the latest QR code phishing attacks.

Pre-click Protection

Utilizes Cellopoint's 125 types of URL threat intelligence to scan all URLs, swiftly comparing them against the latest URL blacklists and whitelists, and quarantining phishing and malicious links.

Time-of-Click (ToC) Protection

Rewrites suspicious URLs and offers real-time Time-of-Click (ToC) detection upon user interaction to prevent delayed attacks.

Post-click Protection

Performs retrospective scanning on URLs to ensure security after they have been clicked.

Fourth Layer: Anti-APT-File

Anti-APT-File module provides the following mechanisms to intercept attachments containing the latest, unknown advanced malware.

Dynamic Sandbox Scanning

Suspicious attachments are securely encrypted and sent to the sandbox for software execution and monitoring.

Full-System Emulation

Within the sandbox, simulates and executes entire computer systems, including Windows, Android, Office documents, and PDF files, swiftly detecting and capturing latent malicious programs.

Correlation and Threat Scoring

Conducts threat level analysis and provides feedback to the SEG for quarantine or release decisions.

Professional Forensic Summary Report

Includes threat scoring, the software's names and actions, network activities, process histories, and registry changes.

Fifth Layer: Anti-BEC

Business Email Compromise (BEC) involves attackers impersonating trusted contacts to deceive recipients. Cellopoint's Anti-BEC detects scams missed by traditional security gateways using:

Sender Authentication: SPF, DKIM, and DMARC identity verification.

BEC Verification Database: Intelligent detection and user alerts for suspicious emails.

Anomaly Detection: Display Name, Sender Account, and Cousin Domain Detection.

User Behavior Analytics (UBA): AI and HCI technology analyze email behavior patterns.

AI Modeling: Uses AI to model email behaviors and recognize anomalous or spoofed senders.

Alerting or Quarantine: Quarantines abnormal emails and alerts recipients, refining detection through machine learning.

Benefits

- Saves time searching for important emails
- Reduces spam deletion time
- Increases email server performance
- Saves IT staff time
- Controls email traffic
- Offers flexible management for individuals and groups
- Lowers the risk of ransomware
- Reduces the risks of APT infiltration
- Decreases the risk of BEC wire fraud

Supported Email Systems

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

Specifications

SEG model	50, 100, 250	500, 1000, 2000	5000, 10K, 20k	Service Provider
Daily Capacity	50k – 250k	500k – 2Mill	5 Mill – 20 Mill	Above 20 Mill
Active Email Users**	50 ~ 250	500 ~ 2,000	5,000 ~ 20,000	20,000+
Deployment ***	Hardware Platform/ Software / Virtualization / Cloud Service			
Anti-Spam Module	**Optional** - Anti-Spam			
Anti-Virus Module	**Optional** - Anti-Virus			
Anti-APT-URL Module	**Optional** - APT-URL			
Anti-APT-File Module	**Optional** - APT-File			
Anti-BEC Module	**Optional -** Anti-BEC			

*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.