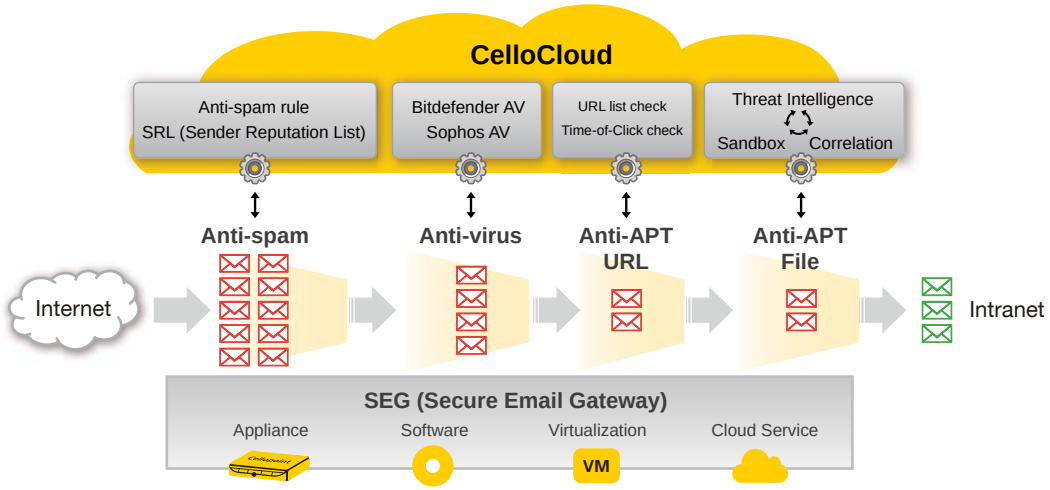
Hassle-free security issues.
Save you time and trouble.

Email UTM

Secure Email Gateway (SEG)

Cellopoint Secure Email Gateway (SEG) is an integrated security gateway solution deployed in front of the Mail Server. Using unique CelloOS™ technology and industry leading CelloCloud™ online threat defense system, SEG adopts multi-layer scanning system to effectively block Advanced Malware, Ransomware, Malicious URL Links, Phishing, Spam, Spyware, Email Bombs, and other threats, relaying malicious mail from entering your network and protecting the email security infrastructure, while improving mail server quality.



Email is still the most used tool of communication within the workplace. However lots of spam flooding your employees' inbox can cause not only the waste of bandwidth, resources and employee time, but also phishing and malware emails can be a threat to your vital information. Cellopoint SEG defends the mail server with three tiers of protection:

Tier One: Anti-spam Protection

Connection Control

SMTP Connection Control blocks 50%up to 80% of all threats before they enter your network, avoiding the improper use of your network resources, processing power and storage space.

DoS (Denial of Service) Defense

Prevent DoS attack from affecting the normal function of your email system.

SRL (Sender Reputation List)

CelloCloud™ monitors the global threat environment 7x24x365 and provides reputation ratings to SRL to distinguish authenticated senders versus spoof senders, and precisely catch abnormal source of mail.

Transaction Check

DHA (Directory Harvest Attack) prevents spammer from guessing real account names and sending spam mails.

Greylist

Using Greylist, SEG can recognize regular email servers, and block automatic mail sending programs from delivering spam. Sender policy framework (SPF) prevents email address spoofing, and verifies the sender identity.

Features

- SMTP Connection Control to defend against DoS attacks
- Individual and Group Black and White lists
- Scheduled Quarantine Notification to every user
- Supports LDAP to import groups and account to the system
- User-friendly, web-based interface
- Diverse Reports and Statistics can be exported as Word, Excel or HTML

Cellopoint
Secure Your Email

Tier Two: Anti-Virus Filtering

Multi-layer Virus Engines

A combination of built-in anti-virus engines offers extensive real time scanning and virus definition updates. Catch a variety of known virus and phishing patterns, spyware, trojans and malware threats.

Content Filter

CelloCloud™ integrates global monitoring, intelligent content analysis, social engineering detection, and URL reputation ratings to effectively block imaged-based spam, malicious spyware, phishing and botnet attacks.

Tier Three: Anti-APT-URL Protection

To protect against the phishing targeted attacks and malicious URL links, Cellopoint SEG will scan and block as follow:

Static Black/Whitelist Database: Over 2 million latest global URL black/whitelist database for quick comparison and quarantine.

Dynamic URL ToC (Time of Click) Scanning: To protect against the unknown, suspicious or malicious URL links, Cellopoint SEG will rewrite the links to go through CelloCloud for real-time examination. The URLs will be examined at the time when the users click them. If a link is unsafe, the users will be warned not to visit the site or informed that the site has been blocked by Cellopoint SEG.

Tier Four: Anti-APT-File Protection

To protect against the unknown, new advanced malware emails and attachment files, Cellopoint SEG will scan and block as follow:

Dynamic Sandbox Scanning: Suspicious email attachements will be sent as encrypted packages to the powerful cloud computing CelloCloud to do dynamic sandbox scanning.

Full-system emulation: Malware as Office and PDF files is captured and induced into a simulated operating system like Windows, Android, Mac OSX.

Correlation Analysis and Threat Scores: Threat Level Analysis that commands SEG to either block or release certain mails.

Professional Summary Report: Analysis report overview shows malicious file name, threats reputation scores, classification, network activity and registry summary.

Specifications

SEG Model	50, 100, 250	500, 1000, 2000	5000, 10K, 20k	Service Provider
Daily Processing Mails	50,000 – 250,000	500,000 – 2Mill	5 Mill – 20 Mill	Above 20 Mill
Active Email Users	50 ~ 250	500 ~ 2,000	5,000 ~ 20,000	20,000 ~ Unlimited
Deployment	Hardware Platform / Software / Virtual Appliance / Cloud Service			
Anti-Spam Module	Anti-Spam License CGAC and Rule Pattern Update - Optional			
Anti-Virus Engine	Bitdefender (BAV) or Sophos (SAV) - Optional			
Anti-APT Engine	Advanced Malware and APT Protection - Optional			
Standard Warranty	1 Year Warranty and Pattern Update (Can be extended to 2 – 5 years)			
Account Calculation	All modules are calculated by the number of email accounts, which includes email accounts and group accounts, but does not include alias.			

Benefits

- Save time on finding important mails
- Save time on deleting spam
- Enhance employee productivity
- Increase email server efficiency
- Save IT personnel management time
- Personal and group flexible management

Groupware and Email Systems supported

- Microsoft Exchange Series: 2003 / 2007 / 2010 / 2013 / Office 365
- IBM Lotus Domino
- Google Apps
- Novell GroupWise
- Sendmail, Qmail, Postfix
- Zimbra
- AWS SES

Cellopoint®
Secure Your Email