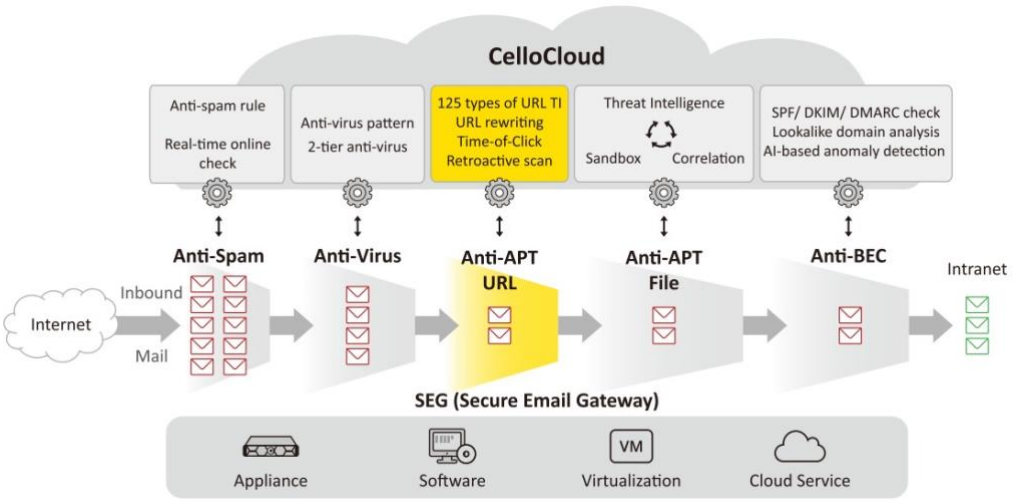
Advanced Threat Protection for URL

Inbound Email Protection

Anti-APT-URL

Cellopoint's Anti-APT-URL module effectively blocks over 20 types of phishing attacks, including traditional phishing, spear phishing, and QR Code attacks. These threats often use social engineering to trick recipients into visiting malicious websites or downloading malware such as Trojans. Such attacks can compromise sensitive information like account details, passwords, and credit card information, and may also enable attackers to control the recipient's device through C&C attacks. Cellopoint Inbound Email Protection offers five layers of email security, with the Anti-APT-URL module as the third layer, positioned after the Anti-Spam and Anti-Virus. This additional layer enhances protection by adding an extra defense against phishing and malicious URLs, complementing the existing spam rule and virus pattern.

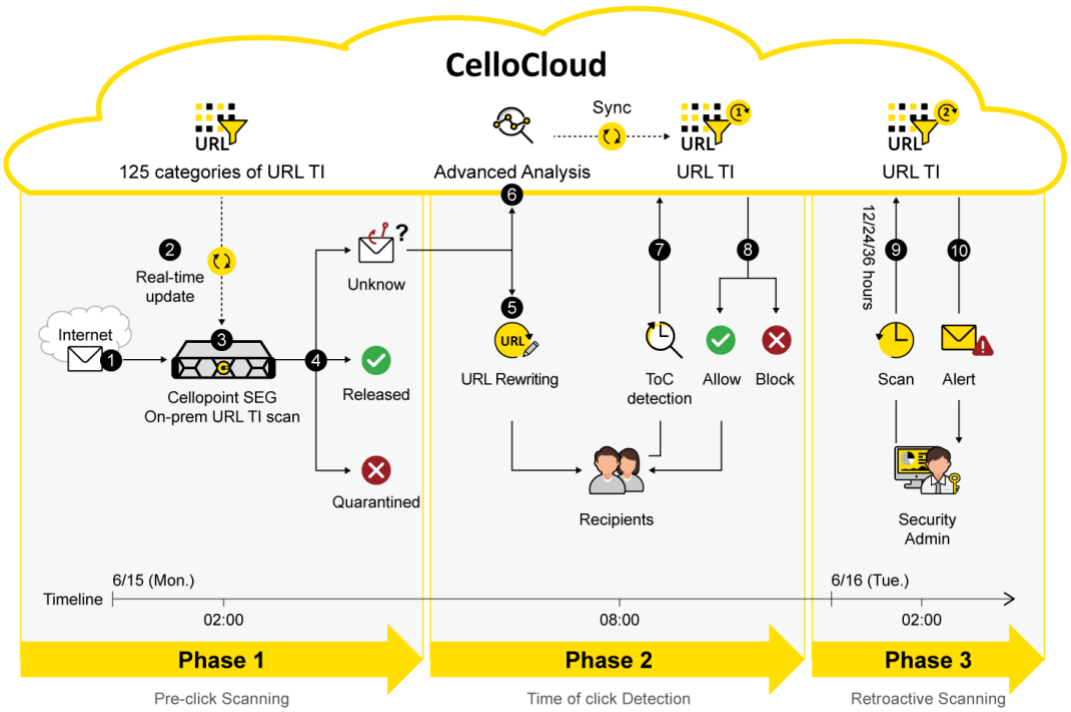


Features

- Phishing URL TI
- Malicious URL TI
- URL Blacklist/Whitelist filtering
- Time of Click (ToC) protection
- User-reporting mechanism
- Global Email Threat Intelligence Network subscription

Benefits

- Improves traditional email security
- Reduces the risk of APT infiltration
- Prevents accidentally clicking malicious emails URL
- Prevents APT attacks
- Enhances email security
- Integrates SIEM correlation analysis



How Anti-APT-URL Works

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.

Cloud Storage File Inspection

Cloud storage file sharing platforms, such as Google Drive, are often targeted by attackers leading to significant security risks. Malicious files can be shared via email with URLs from these services, deceiving recipients into downloading them. The APT-URL and APT-File modules download and analyze these files in a sandbox environment before users access them, effectively intercepting such advanced threats.
(APT-File module is required)

Supported Email Systems

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