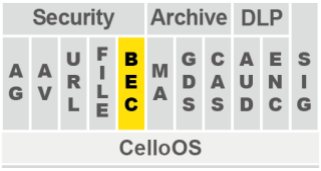
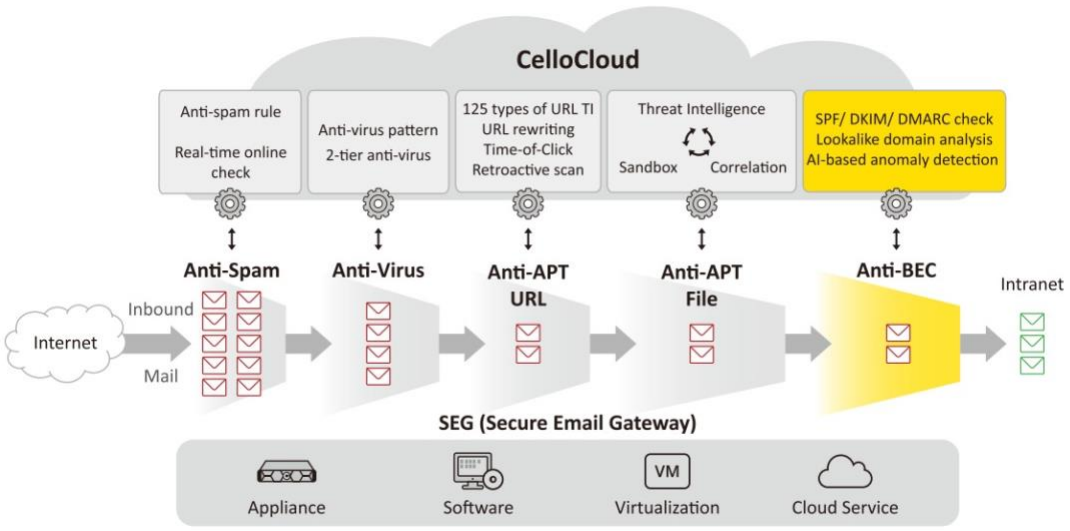
Detect and verify for BEC and fraud email.

Inbound Email Protection

Anti-BEC (BEC)

BEC (Business Email Compromise) refers to attackers impersonating trusted recipients and using social engineering tactics to deceive recipients into transferring funds or providing confidential information. These attacks often leverage spear-phishing or credential theft and given their combination of payload-less (e.g., text only) and payload-based methods, are difficult for legacy email security systems to detect. At Cellopoint, we give you insights into BEC risks and provide the state-of-the-art solution to protect your users effectively.





Cellopoint's Anti-BEC detects BEC scams that traditional security gateways may miss through the following technologies:

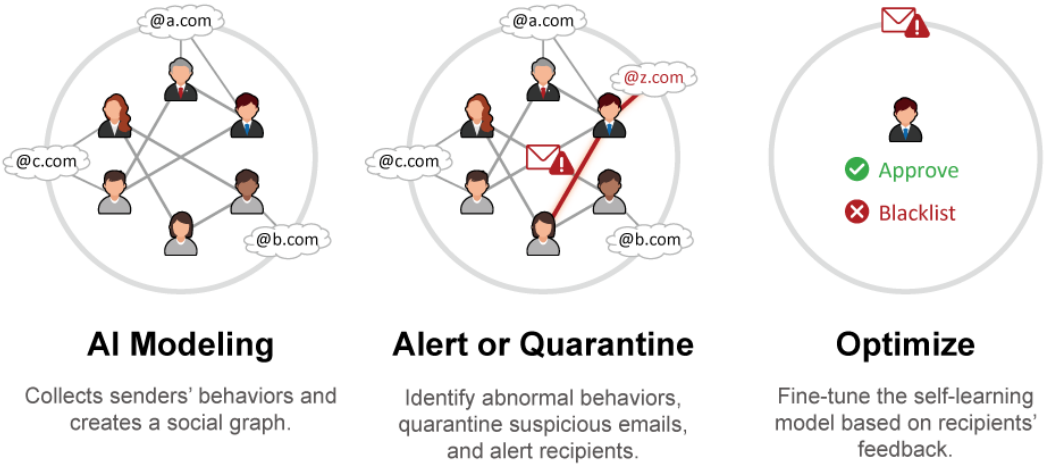
- **Sender Authentication**: SPF, DKIM, and DMARC identity verification.
- **BEC Verification Database:** Uses intelligent detection to identify anomalies and allows users to verify the authenticity of suspicious emails through alerts.
- **Display Name Anomaly Detection:** Detects anomalies like "**Masom Wang** <mason.wang@cellopoint.com>"which impersonates "**Mason Wang** <mason.wang@cellopoint.com>"
- **Sender Account Anomaly Detection:** Detects anomalies like "Mason Wang <**mason_wang**@cellopoint.com>" which impersonates "Mason Wang **<mason.wang**@cellopoint.com>"
- **Cousin Domain Detection:** Detects cousin domains (look-alike domains) like "Mason Wang <mason.wang@**cellop0int**.com>" which impersonates "Mason Wang <mason.wang@**cellopint**.com>"

Features

- Display name spoofing detection
- Sender account anomaly detection
- Cousin domain detection
- BEC verification
- Analysis report
- AI detection and quarantine alerts

Benefits

- Prevents BEC frauds
- Decreases the risk of BEC wire fraud
- Reduces operational risks
- Enhances your email security
- Provides cybersecurity Defense in depth



- **User Behavior Analytics (UBA):** Uses artificial intelligence (AI) algorithms and Human-Computer Interaction (HCI) technology to analyze user email behavior patterns, detecting and responding to anomalies.
- **AI Modeling:** Utilizes AI algorithms to model individual email communication behaviors, identifying normal patterns and legitimate senders to recognize anomalous or spoofed senders.
- **Alert or Quarantine:** Abnormal emails are quarantined directly, while suspicious emails are quarantined with alerts sent to recipients for verification.
- **Optimize:** Once suspicious emails are confirmed by the recipient, they are sent to AI modeling to fine-tune the AI-based anomaly detection system.