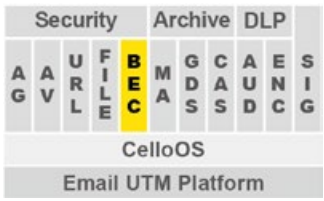
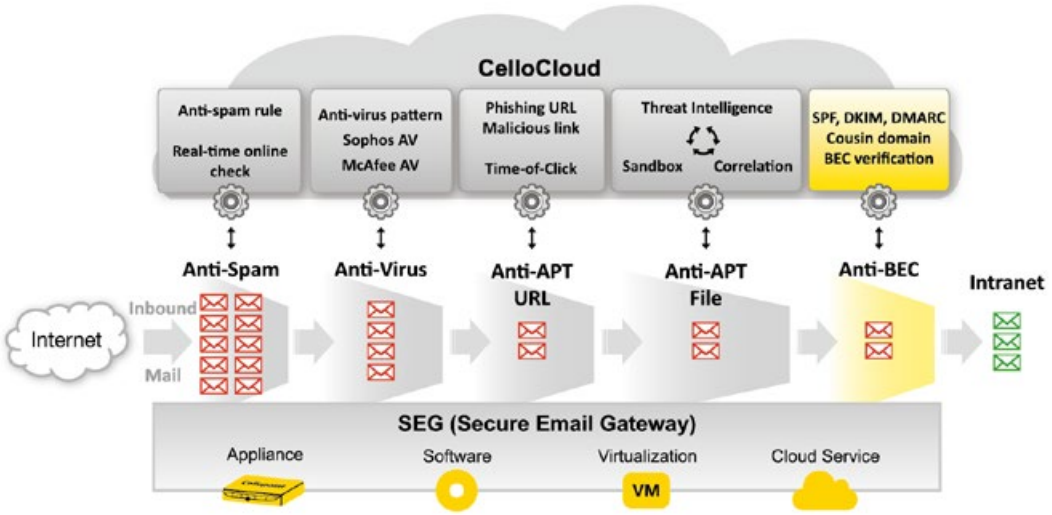
电子邮件 BEC 侦测防护

BEC (Business Email Compromise) 商业电子邮件欺诈又称为变脸欺诈，这是针对工作邮箱入侵、伪冒、潜伏观察，再利用社交工程手法，诱骗公司或单位财务人员做转账汇款，造成巨额损失。这些精心设计的电子邮件，它通常只有在前期通过钓鱼 URL 或附件安插后门程序，在取得财务人员的邮箱密码后，黑客持续观察邮件往返内容直到出现大额转账信息时，伪造对方发送 BEC 变脸欺诈邮件，要求将该笔汇款转到另外指定银行账户，由于此邮件不带有 URL 或附件特征，因此传统安全网关或防火墙几乎侦测不到。





功能特色

- 显示名称侦测
- 发件账号侦测
- 发件网域侦测
- 欺诈情报验证
- 拦截分析报告
- 智慧侦测与告警

使用效益

- 避免遭受变脸欺诈
- 避免欺诈汇款损失
- 降低营运风险
- 提高邮件安全强度
- 加深信息安全纵深防御

邮件的传输已成为企业组织最重要的通信工具，Anti-BEC 高级侦测防御模块，除了传统发件人验证方式，诸如 SPF、DKIM 或 DMARC 之外，此模块采用以下侦测技术，包括：

- 变脸欺诈验证 (BEC verification) 数据库，通过智能型侦测与告警系统，让用戶验证真正往来邮件与伪造邮件。
- 显示名称 (Display name) 异常侦测，例如：

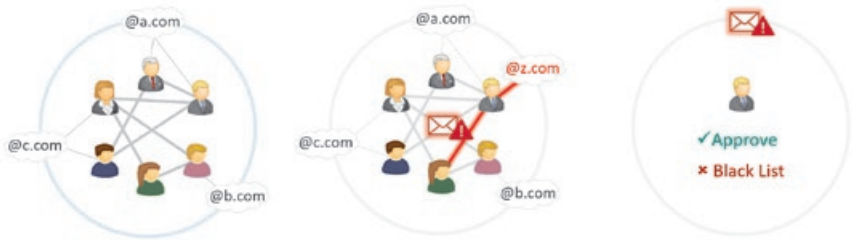
" 王大明 " <WangDM@cellopoint.com> 窜改为 " 王天明 " <WangDM@cellopoint.com>

- 发件账号异常侦测，例如：

" 王大明 " <WangDM@cellopoint.com> 窜改为 " 王大明 " <Wang_DM@cellopoint.com>

- 发件网域 (Cousin domain) 混淆侦测，例如：

" 王大明 " <WangDM@cellopoint.com> 窜改为 " 王大明 " <WangDM@cellop0int.com>



AI for Modeling | **Warning or Blocking** | **Identify**

根据使用者行为分析 UBA(User Behavior Analytics) 的特色，Anti-BEC 模块将其应用在欺诈邮件分析上，将每一个邮件账号收发信的特征及行为做统计分析，并通过 AI 算法辨识哪些属正常，哪些属异常，并通过人机互动，再进化成更精准的辨识欺诈模型。

AI for Modeling

将个人邮件往来行为进行建模，通过人工智能算法，找出正常通联模型与正常发件人，及异常的陌生发件人或伪冒发件人。

Warning or Blocking

系统将可疑邮件暂时隔离，并发出通知邮件给收件人做告警，再由收件人做确认是否为欺诈邮件。

系统可直接将异常的欺诈邮件做隔离。

Identify

可疑邮件经由收件人确认后，可与机器学习系统交互建模，进而演化更精准的辨识欺诈引擎。