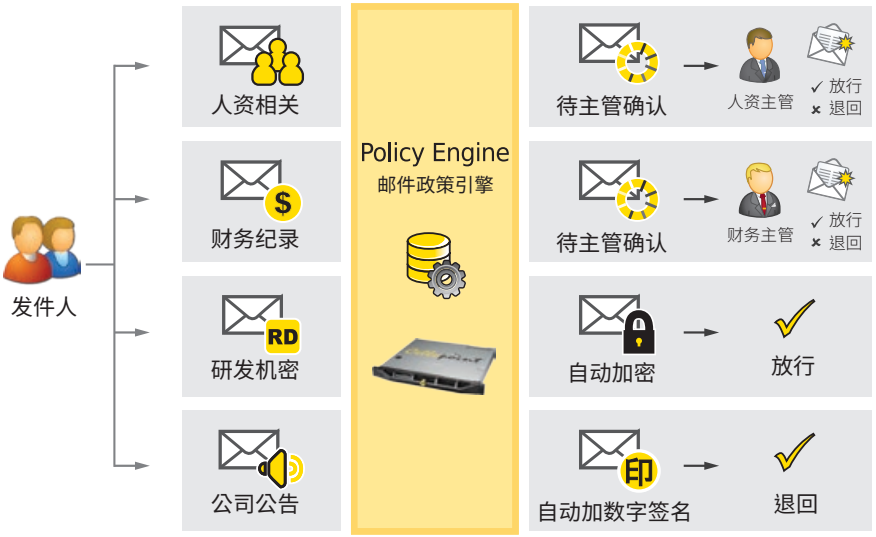
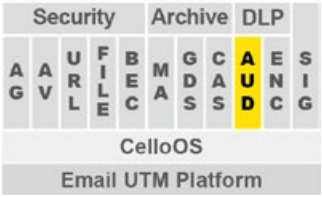
Provide comprehensive data loss prevention (DLP) to your messages.

电子邮件审核 (AUD)

Auditing Solution (AUD) 是整合式的邮件内容审核与数据外泄防御解决方案，协助监控电子邮件信息传递，减少数据外泄的风险。内建的 Policy Engine 提供弹性化的策略建立、执行及记录和回报能力，可简化管理和满足法规遵从的需求，同时大幅降低成本。





解决问题

- 快速发现组织风险
- 缩短审核响应时间
- 弹性的策略设定管理
- 高效搜集法律证据
- 依需求自定义报表

产品特色

- 防止数据外泄 (DLP)
- 遵从法规
- 组织策略执行
- 分层访问控制
- 整合 AD/LDAP 群组
- 提升邮件主机性能
- 节省审核人员管理时间
- 自动化审核作业

功能特点

识别敏感数据 (Identify Sensitive Data)

实时扫描与分析 – 提供深层的邮件数据检测，从邮件头、邮件正文到附件无一遗漏。支持压缩文件 (Zip) 与附件文档内容的扫描 (TXT, PDF, RTF, Word, Excel, Powerpoint)。

内容层级过滤 – 使用多维度的分类来过滤、识别敏感数据，包含内建的 ID 信息审核，或是组织自定义的词组或关键词过滤。

策略引擎 (Policy Engine) – 单一控制台管理邮件策略设定、编辑、部署与执行。

多种分类条件 – 提供结构化数据 (身份证号、信用卡号码) 等默认条件，及邮件的大小、附件、收件人等字段用于定义审核策略。

强大的策略设定 – 弹性且直观的过滤条件、执行动作设定，验证条件、整合组织策略，提供敏感邮件外泄保护 (Email DLP)。

事前审核—实时防止数据外泄

对传输中的邮件强制执行邮件策略，能主动阻挡敏感邮件传递，防止不慎或蓄意外泄数据的行为。当侦测到违规行为时，AUD 会提供多种回应动作，包括：进行阻挡、隔离、转发、删除、加密 (搭配 ENC 加密模块) 等。

事后审核—找出过去未发现的风险

了解历史邮件数据哪些是机密的、如何被传递、使用者是谁，以及最终的目的地。

当邮件经过扫描、分析与分类后，AUD 会将所有相关的信息存放在审核数据库中。通过直观的检索界面，审核人员可查询所有邮件行为，包含发送端、接收端、敏感内容关键词等。最后依据数据外泄情况采取对应的行动，如通知管理者或保存证据以供诉讼用途。

(需搭配邮件归档 - MA 模块)

功能特点

优点

- 打造一个更安全的 IT 环境，免除数据外泄 DLP (Data Loss Prevention) 风险
- 对于组织信息风险有更深入的了解，以协助未来组织策略的制定
- 改进智慧资产的管理及法规遵从
- 将信息安全策略转化为自动审核管理系统，以减少管理时间及人力
- 对往来邮件中的潜在风险及违反组织策略的行为进行实时监控和应对，让审核人员可以在第一时间收到通知并处理
- 自定义策略优先级，可以依照风险范围来调整处理的顺序

角色型访问权限

- 支持区分不同的角色：员工、管理者、群组管理员等
- 依照不同的角色定义不同的权限，可细化至任何群组层级
- 弹性制定群组安全策略

网页型控制台

无需安装任何软件就能在任何地点操作管理控制台，进行审核与设定

支持邮件系统

- Microsoft Exchange 2007/2010/2013/2016/Office 365/Exchange Online
- Lotus Domino
- Novell GroupWise
- Sendmail, Qmail, Postfix
- Zimbra
- Coremail

规格表

AUD 型号	50, 100, 250	500, 1000, 2000	5000, 10K, 20K	Service Provider
每日处理邮件数量	5~25 万封	50~200 万封	500~2000 万封	2,000 万封以上
硬件性能 (可承载人数)	50 ~ 250	500 ~ 2,000	5,000 ~ 20,000	20,000 ~ Unlimited
接收 / 外发邮件过滤	✓	✓	✓	✓
中继 (Relay) 模式部署	✓	✓	✓	✓
透明 (Transparent) 模式部署	✓	✓	✓	✓
以太网端口	GbE×2	GbE×2	GbE×2	GbE×2

※ 以上产品皆包含一年产品授权及标准保修，可依需求购买 1~N 年保修服务

※ 软件授权依电子邮件帐号数量计价