



We Secure Your Content



Mail SQR Expert

全方位电子邮件内容安全管理系统

产品白皮书

目 录

1 背景概述	2
1.1 市场需求分析	2
2 Mail SQR Expert 产品介绍	3
2.1 产品概述	3
2.2 产品架构及工作模式	3
2.2.1 系统架构	3
2.2.2 工作模式	3
2.3 功能描述	4
2.3.1 功能特点	4
2.3.2 主要功能	4
2.4 产品功能及优势	6
2.4.1 产品功能	6
2.4.2 功能特色	7
3 典型应用	9
3.1 中小型企业	9
3.2 大型企业	10

1 背景概述

1.1 市场需求分析

随着计算机网络技术和数字通信技术飞速发展,计算机网络技术的应用不断深入到人们的日常工作、学习和生活中,应用领域也从传统的、小型的业务系统逐渐向大型、关键、综合的业务系统扩展,如电子政务、电子商务、CIMS、知识管理、电子金融、社会保障、GIS 系统等。在二十世纪末信息安全的课题就被提升到日常应用的高度,在解决了网络之间的安全问题后,电子邮件的管理和审计问题被信息系统管理员所关注。

电子邮件作为信息时代企业的生产工具,同样面临着适当监控、合理使用的问题。根据 Forrester Research 的调查:

- **25%** Outbound 邮件带有财务或法律性的管理风险
- **35%**企业怀疑 Email 泄露出机密重要资料
- **43%**企业将聘请专人稽核 Outbound 邮件的机密内容
- **33%**企业会进行 Outbound 邮件的内容稽核

随着中国加入 WTO,经济领域的国际竞争进一步加剧,国内的企业也需要认真考虑合理使用电子邮件,充分提高企业竞争力的问题,降低企业由于通过邮件泄露公司重要资料以及邮件丢失造成的损失。

而对资讯相对流通的邮件来说,更需要备份归档,来保存企业日常流通信息资产。Gartner 分析师 Ken Chin 说:"电子邮件数据存储需求的增长以及要求保留电子邮件记录以满足合规性要求和法律查找要求的规定为电子邮件有效归档工具开辟了一个巨大的市场。"Gartner 定义的电子邮件有效归档产品是指那些可以在一段确定的时间内提供电子邮件信息的可搜索归档的产品,过了那段时间之后可以将电子邮件信息清除。

尤其值得注意的是,在企业中广泛存在班工作时间内将公司帐号作为私用、收发娱乐邮件、通过 Email 泄露公司重要机密资料等现象,电子邮件的滥用给中国企业带来了巨大的损失。

因此,如何有效地解决这些问题,以便提高员工的工作效率,降低企业的安全风险,减少企业的损失,已经成为中国企业迫在眉睫的紧要任务。

2 Mail SQR Expert 产品介绍

2.1 产品概述

Mail SQR Expert- 以中文界面外观流畅、多元化邮件备份、简繁体邮件内容转换过滤、管理统计功能完整为产品特色，特重于安全审核管理及流量控管，提供完整的 E-Mail 管理功能，可以达到邮件备份、过滤、统计、增值管理(审核、流量调节)等多元化功能，以满足企业安管应用的需求，降低 E-Mail 不当使用所造成的企业风险。本系统为 Web 界面，方便管理员于任何时间、任何地点浏览与管理讯息。

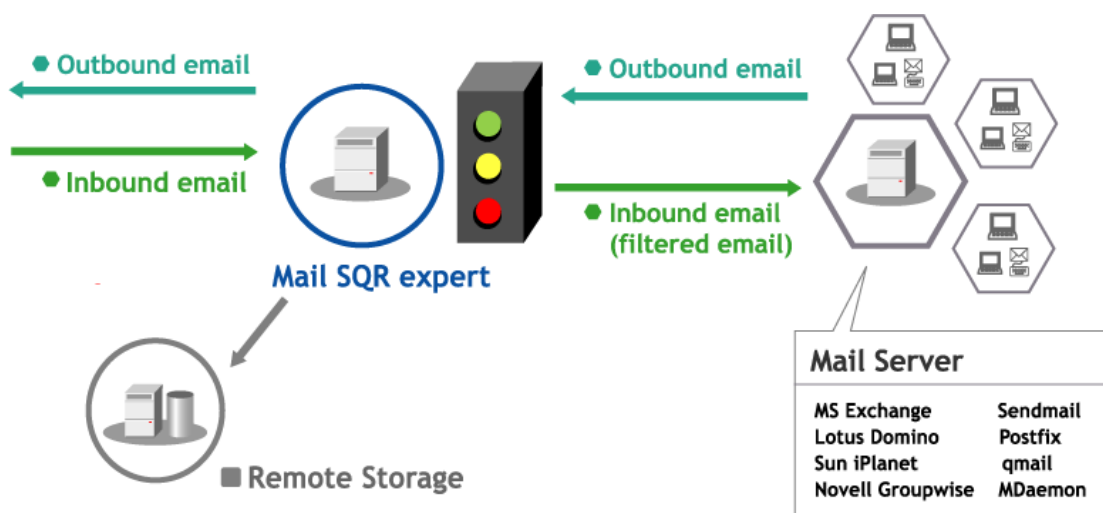
2.2 产品架构及工作模式

2.2.1 系统架构

Mail SQR Expert 主要由硬件平台、FreeBSD 操作系统、电子邮件管控审计软件等三个部分组成。硬件平台根据用户使用环境的不同，选取专用安全平台或基于高性能服务器架构进行设计；操作系统为运行稳定安全，性能表现突出的 FreeBSD 操作系统，并针对产品的设计和运行需要，对系统环境做了优化调整；电子邮件管控审计软件采用模块化设计，针对不同的应用环境和不同的安全策略，可以选购扩充的功能模块共同工作，以便提升产品工作运行的效率。

2.2.2 工作模式

Mail SQR Expert 是以 relay 的方式进行运作：



可在对现有网络架构影响最小的状况下快速部署。产品导入前请先考虑下列几项因素，并做好先期的规划与准备，以利产品快速且顺利的上线运作。

1、防火墙信息。

通常会将 Mail SQR Expert 放置于企业局域网内部，因此防火墙是否有 Port mapping 功能以及是否可以自行变更设定，将会影响到产品的上线。

2、是否有 Mail relay。Mail relay 的功能，以及是否可以改变 Mail relay 的邮件路由。

3、DNS 信息。外部 DNS 的管理方式，是否可自行管理。

2.3 功能描述

2.3.1 功能特点

- 完整的 Email 内容资产保存及复原服务
- 遵循科学规则及管理策略，提供完善的 Email 内容安全管理
- 分权以及弹性化的 Email 策略管理
- 调节流量 确保最佳化 Email 服务效能
- 提供完备统计报表，及时掌握邮件流通状况
- MyMail 个人化安全邮件服务，提供个人邮件复原及便利自主管理

2.3.2 主要功能

2.3.2.1 完整的 Email 内容备份和复原

● 邮件备份

提供本机空间管理 、 手动远程备份 、 自动远程备份等功能。

● 邮件记录及复原

将所有通过的邮件备份到数据库，提供快速查询功能，迅速查询到需要的邮件并可重送给原收件人。

2.3.1.2 Email 内容安全管理

● 邮件过滤

提供邮件过滤条件设定功能，过滤条件包含依据群组过滤、传送/接收型态、收件人类型、条件关联、发件人、收件人、主题、邮件及附件、附件名、附件类型、发送 IP、邮件大小、收件人数、加密附件、简繁体转换

● 邮件过滤处理方式

过滤条件处理功能包含自动回复、密件副本、邮件审核、延迟发送、退回邮件、丢弃邮件、允许传送、主动通知、通知 email 设定。

2.3.1.3 分权管理

● 管理帐号

供依公司组织及管理政策来设定管理群组、账号

● 登入权限设定

包含所控管之群组与系统功能，如：邮件记录、分类查询、邮件过滤、邮件审核、政策管理、统计报表、病毒隔离、延迟发送、系统设定

2.3.1.4 流量监控和调节

● 延迟发送

将档案大或收件人多的批量邮件(非紧急或重要的邮件),排在频宽充裕的流量离峰时段,运用本功能可妥善分配公司的频宽资源。

● 流量监控

管理员可自定流量监控，当监控条件满足时，可设置通知管理员或相关人员。

2.3.1.5 统计报表

● 统计报表类型

分为流量状况、流量报表、连接统计、邮件处理状态统计、群组排名、人员排名

● 报表自订发送

统计报表可以设置排程发送，以利相关人员掌控所有邮件状况。

2.3.1.6 MyMail 个人化邮件服务

● 个人化功能的权限设置

可依照个人或群组给予个人化功能的权限，亦可自订默认值

2.4 产品功能及优势

2.4.1 产品功能

标准功能	说明
MyMail 个人化安全邮件服务	提供个人 Email 收发明细的通知寄送，符合个人的使用认知。用户登录个人的管理界面，可使用个人邮件夹、分类邮件夹、个人统计..等功能。
邮件记录及查询	记录公司所有收发的电子邮件，并提供条件查询、分类查询以及全文检索查询等功能，协助管理员更深入了解公司电子邮件的流量、或邮件使用状况。查询结果将提供详细邮件记录列表、统计模式报表以及统计图表。
策略管理	可遵循法规或管理策略进行 Email 内容过滤的管理设置，提供全公司各群组的邮件过滤设置总表，可调整设置条件或优先顺序，利于企业管理策略的实施与调整效率。也提供策略导出、导入，协助企业快速复制到其他经营据点。
邮件审核	依据管理策略进行邮件的审核处理(如寄出、退回、删除)，以加强邮件内控的管制效果，提供群组分权审核管理，以达成部门差异化管理的需要。
延迟寄送	可将档案大或收件人多的批量邮件(非紧急或不重要的邮件)，排在频宽充裕的流量离峰时段，运用本功能可妥善分配公司的频宽资源。
邮件备份	提供邮件记录、邮件内容(含附件)、及系统设置档三部份的备份文件。将每日邮件备份成一个资料夹，并能逐月寻找某日期的邮件备份资料。
邮件还原	用户若发生邮件资料毁损，可通过分类查询或 MyMail 个人化安全邮件服务，能将邮件记录及内容进行还原寄送。
帐号管理	可依管理策略提供主管帐号并给予部份权限，进行其所管辖群组的信件管理。能依群组内成员的管理需要，进行个人化功能开关的权限设置。
统计报告	包含个人邮件分析报表、邮件使用排名统计(依整体、群组、个人)、流量分析、连线统计、邮件处理状态统计、策略管理报表、流量监控报告、防毒统计报告(选购功能)..等多类图形化统计报表。
系统设置	提供系统记录、使用记录..以检视系统状态，并可进行邮件备份设置、数据库维护、系统设置、环境设置..等相关设置。

标准 LDAP 帐号整合	可整合标准 LDAP 服务器，自动同步 Email 群组帐号资料以及分权管理员帐号，并支援 AD 阶层式群组架构，以进行分群管理的效益；并可搭配不合法收件人过滤设置，强化字典档攻击的防御效果。
SMTP 代理认证	可使邮件服务器不直接暴露于外部，以避免绕信攻击及遭受垃圾邮件的轰炸，且不影响内部人员于外部发信。
选购功能	说明
Multi-Way 模块	双机以上在线热备，可在原本有一台系统的前题下，增购第二台以上可提高稳定度，应付大流量客户，可达成冗余效果。
防毒模块	可选购加载杀毒系统，杀毒可选用 NOD32 或 Sophos / ClamAV。
邮件归档管理(A)-Archiving 模块(简称:归档模块)	在 MSE 架构(Relay)基础下,可选购归档模块,可支持多个存储位置挂载,可设定依条件存放的周期与管理,实现邮件生命管理周期。
内部邮件记录(I)-Internal 模块(简称: 内部邮件模块)	在 MSE 架构(Relay)基础下,因同域内相互发送邮件并不会转抄送至外端中继设备,因此需要此模块备份同域内互发的邮件,实现内部所有人员邮件保存,并在此进行内部去重覆化的动作。
邮件稽核模块-Audit	提供完整的邮件事件稽核流程,从初始阶段到调查>审核阶段>产生分析报告,方便审核人员对邮件进行审核注解的操作。
双帐号认证模块-Double Auth	可在查阅邮件时,强制要求第二帐号通过认证,才得以查看邮件内文。
SSL(TLS)邮件传输加密模块	邮件传输过程中默认为 128 bits TLS 加密传输,可避免封包被截取后的数据外泄,该模块也可在界面上导入证书,满足加密传输需求。

2.4.2 功能特色

● **提供强大的邮件管理功能：**企业订立电子邮件的安全管理策略后，Mail SQR Expert 可提供策略管理、内容过滤、邮件审核、延迟发送..等服务。可依据公司的策略来进行管理设定，以便发现是否有违反公司的管理规定的行为发生，以达到邮件安全管理的目的。

a) 提供丰富的邮件过滤条件设置：过滤条件包含依据群组过滤、形态、收件人类型、条件关联、发件人、收件人、主题、正文及附件内容、附件文件名、附件类型、发送 IP、大小、收件人数、包含加密附件、启用简/繁转换检查功能。

b) 提供多种邮件过滤条件处理功能：过滤条件处理功能包含自动回复、密件抄送、邮件审核、延迟发送、退回邮件、丢弃邮件、允许传送、主动通知、通知 Email 设定、建立此过滤条件的分类查询。

c) 提供多种附件内容过滤的格式：包含 PDF (*.pdf)、 Word(*.doc)、 Excel(*.xls)、

PowerPoint(*.ppt)、MDB(*.mdb)、RTF(*.rtf)、ZIP(*.zip)、RAR(*.rar)、BMP(*.bmp)、GIF(*.gif)、JPG(*.jpg)、PNG(*.png)、MP3(*.mp3)、AVI(*.avi)、RM(*.rm)、MPG(*.mpg)、RA(*.ra)、WMV(*.wmv)、ASF(*.asf) 等格式。

d) 提供以群组检视过滤策略：以群组检视所设置之内收、外送邮件过滤策略列表；并提供立即修改功能。

● 分权管理和群组设置

a) 弹性化分权管理：可依公司组织及管理政策来设置管理帐号，然后设置该管理站帐号的权限。提供登入权限设置，包含所控管之群组与系统功能，如：邮件记录、分类查询、邮件过滤、邮件审核、策略管理、统计报表、延迟发送、系统设置

b) 群组、群组成员与电子邮件帐号：可通过手工、导入和 LDAP 自动同步三种方式设置群组及成员。

● 多样化、全面的图表分析：Mail SQR Expert 提供操作简便的 Web 管理界面，通过群组排名、人员排名、流量报表、连接统计等报表，无论是群组或个人的使用统计均能一目了然。

● MyMail 个人邮件服务：提供的个人功能包括：分类收件箱、统计报表及个人化设置

a) 个人邮件复原：提供个人邮件记录浏览和查询功能，查询到所需要的邮件点选【取回】就会将该邮件重新发送到用户的邮箱中。

b) 个人化统计报表：按邮件处理状态(包括：正常传送、退信、审核后退回等)统计个人收发邮件的封数和流量。

3 典型应用

◆ 概述

随着国内计算机和网络技术的迅猛发展和广泛普及，企业经营活动的各种业务系统都立足于 Internet/Intranet 环境中，越来越多企业业务对于信息技术的依赖程度较之以往有了显著的提高。电子邮件在公司的运作过程中起到了巨大的作用，企业对于电子邮件的依赖性也越来越高，但同时员工在收发邮件时给公司带来了风险。

因此，在企业中广泛存在上班工作时间里将公司帐号作为私用、收发娱乐邮件、将个人隐私及重要信息寄给人事部门、通过 Email 泄露公司重要机密资料等现象，对于邮件的审核和管理迫在眉睫。

同时，对于邮件的备份也越来越重要，各国相继出台了有关电子邮件记录保全和管理的相关法规。邮件的备份可以防止内部重要邮件流失--提高公司竞争力、符合政府法案，以免受罚、保留公司黄金数字资产。

3.1 中小型企业

◆ 部署

通过使用 Mail SQR Expert 的 relay 模式部署，部署拓扑见下图。所有用户收发的邮件均通过 Mail SQR Expert 进行备份和过滤后转发，从而实现对用户电子邮件的管控和审计。



◆ 效果

通过式部署 Mail SQR Expert ，可以对企业网络应用达到审计和管控的作用。

- ✓ 了解群组或个人的使用邮件的次数和流量
- ✓ 查询相关邮件的详细资料

- ✓ 对于涉及公司机密的邮件进行审核，可以对邮件允许、退回或者直接删除
- ✓ 对于非工作性质的娱乐邮件或者非重要邮件延迟发送，节约公司资源
- ✓ 分权管理，将不同部门员工的管理权限分配给各部门领导或指定人员
- ✓ 针对丢失邮件进行复原
- ✓ 提供丰富的统计报告，支针对邮件流量进行监控

3.2 大型企业

部署

在大型的企业中用户数量巨大，对机器的可靠性、稳定性要求极高，Mail SQR Expert 的部署采用 Multi-way 模式，部署拓扑见下图。所有用户收发的邮件均通过 Mail SQR Expert 进行备份和过滤后转发，从而实现对用户电子邮件的管控和审计。



◆ 效果

通过 Multi-way 方式部署 Mail SQR Expert ，两台 Mail SQR Expert 都是 Active，增强了运行的可靠性和稳定性。可以对企业网络应用达到审计和管控的作用。

- ✓ 了解群组或个人的使用邮件的次数和流量
- ✓ 查询相关邮件的详细资料
- ✓ 对于涉及公司机密的邮件进行审核，可以对邮件允许、退回或者直接删除
- ✓ 对于非工作性质的娱乐邮件或者非重要邮件延迟发送，节约公司资源
- ✓ 分权管理，将不同部门员工的管理权限分配给各部门领导或指定人员
- ✓ 针对丢失邮件进行复原
- ✓ 提供丰富的统计报告，支针对邮件流量进行监控