

Lark邮箱安全白皮书

序言

随着互联网时代的发展，企业邮箱变得便捷，应用场景越来越多。然而，当前的互联网业务时刻面临着各类风险，如:黑客攻击、敏感信息被窃取与滥用、不良信息骚扰等。Lark邮箱积累多年安全防护能力和经验，目前已建立强大的信息安全体系。

本文将从合规性、敏感数据保护、数据留存、反垃圾等方面阐述Lark邮箱信息安全能力，以加强用户对Lark邮箱安全能力的了解。Lark邮箱能沉着应对互联网各类攻击，防范用户信息泄露，保护企业和用户信息安全。

版本变更记录

时间	版本	说明
2023年6月1日	V1.1	版本创建

1 合规与隐私性

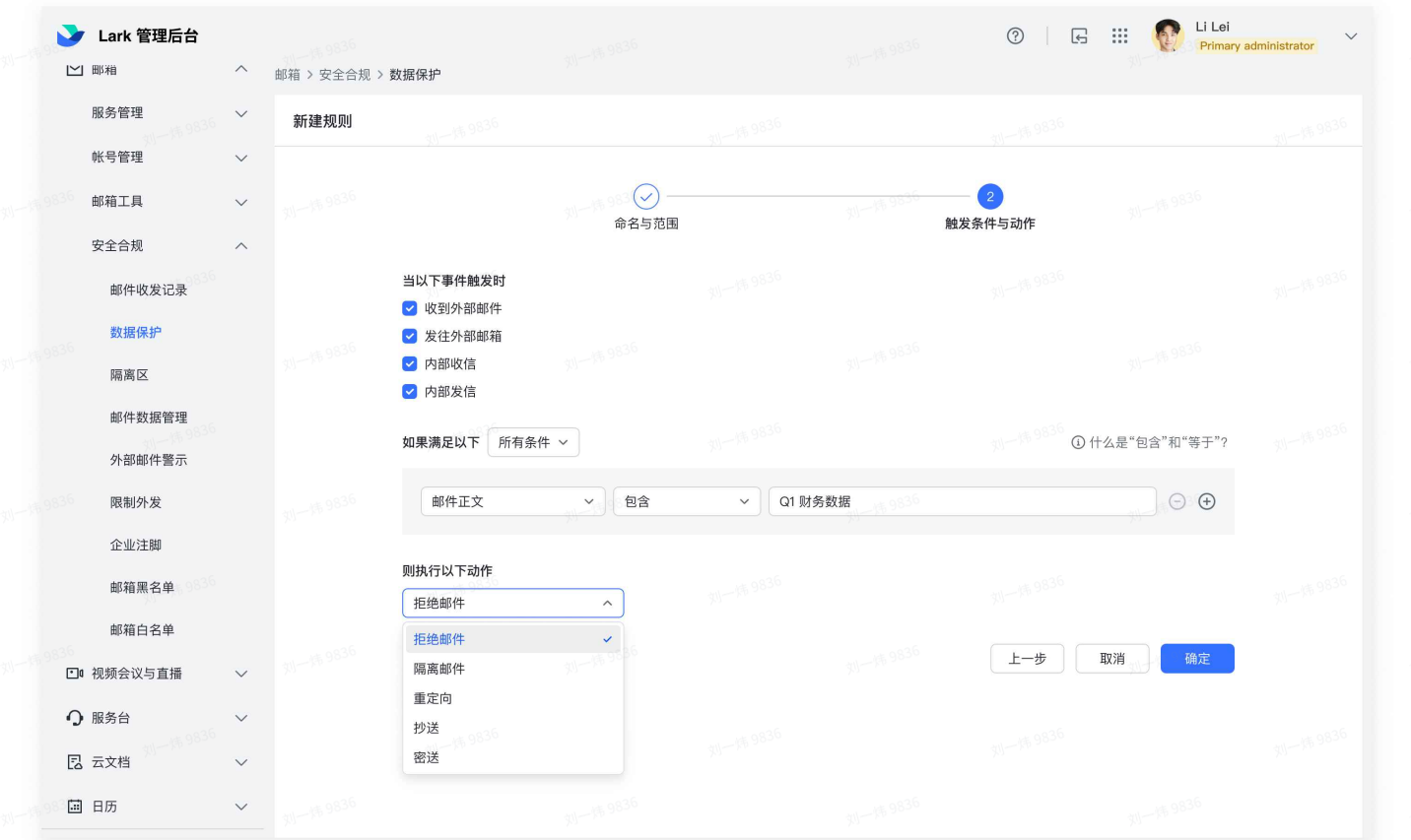
Lark邮箱属于Lark办公套件产品之一，在安全合规上与Lark保持一致。Lark持续致力于保障用户的数据安全、隐私及安全合规性，目前已通过多项国际合规性认证，包括ISO27001，ISO27017、ISO27018、ISO27701、CBPR&PRP、DPTM 等认证，并完成了SOC 2 Type II 以及SOC 3服务鉴证报告。

关于Lark合规与隐私性的完整介绍，可查看[Lark安全与合规](#)

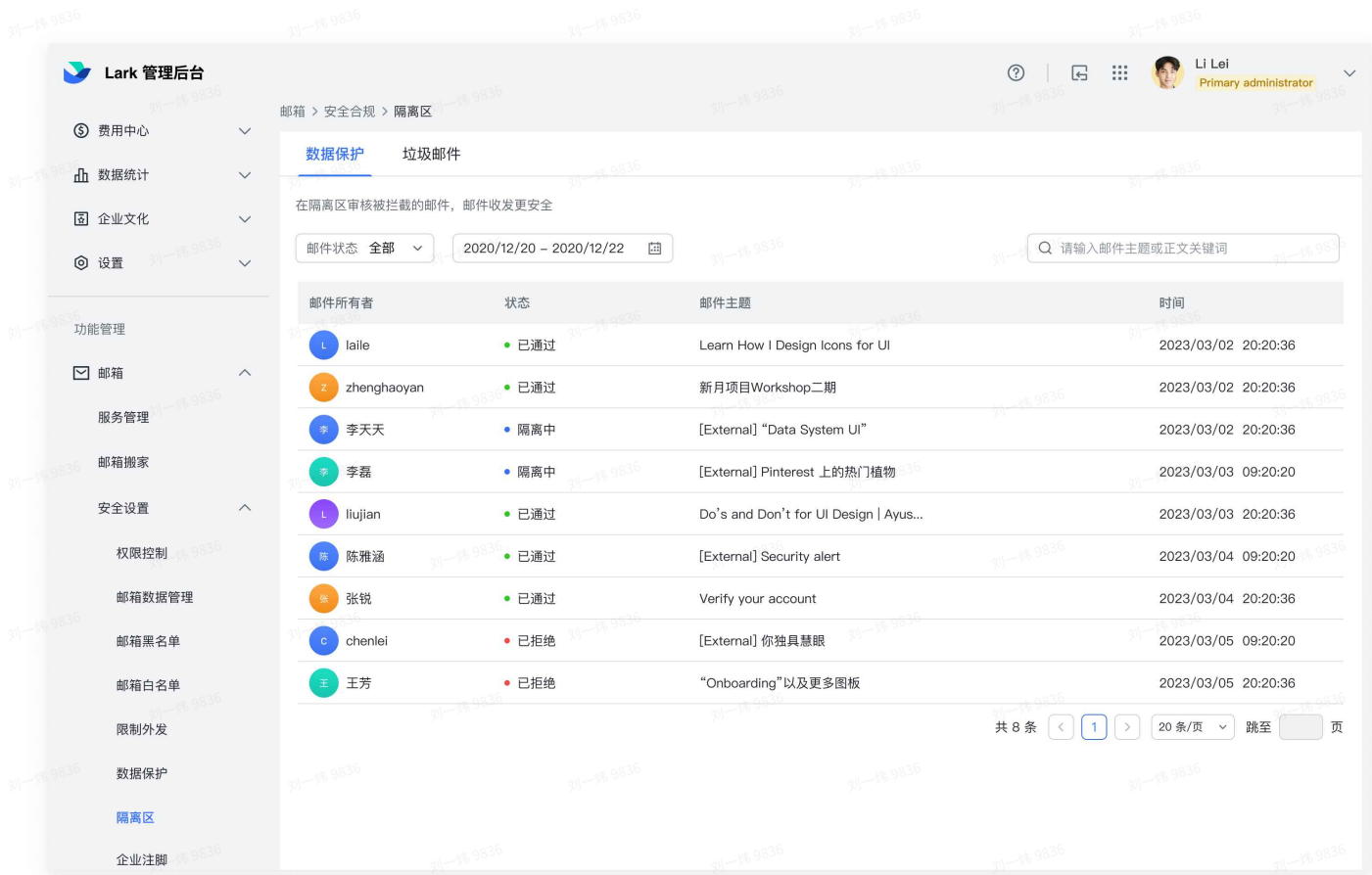
2 敏感数据保护

2.1 数据防丢失保护（DLP）

在企业邮件收发信过程中，可能存在泄露企业敏感数据的风险，Lark邮箱提供数据防丢失保护功能，企业管理员可设置数据保护规则，定义规则的触发条件和执行动作。规则生效后，系统将对出入站的邮件进行内容扫描，如发现邮件内容符合规则，则自动执行动作，确保企业的敏感数据、关键数据不会通过邮件泄露。

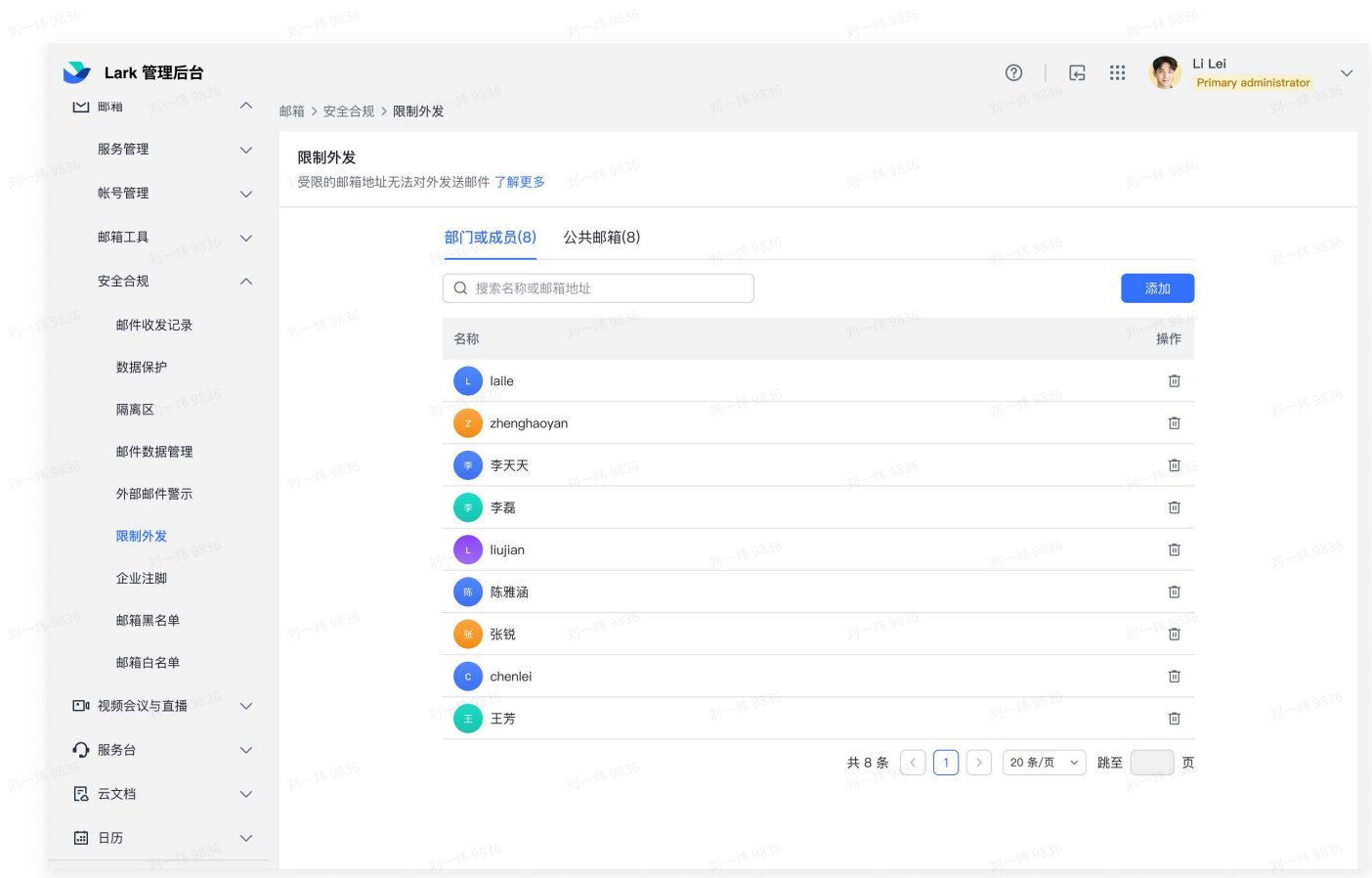


因触发数据防丢失保护规则，而被拒绝发送、隔离的邮件，将统一放置在隔离区，企业管理员可以在隔离区查看这些邮件的内容，对于隔离的邮件可以选择放行继续发送。确保企业在保护敏感数据的同时，不影响正常邮件的往来。



2.2 限制外发

在企业中并非所有员工都需要对外发信，为了防止企业敏感数据通过邮件对外泄露，对于无需对外发信的员工可以设置限制外发，受限制的员工无法对外发送邮件，对内部发送邮件不受影响。

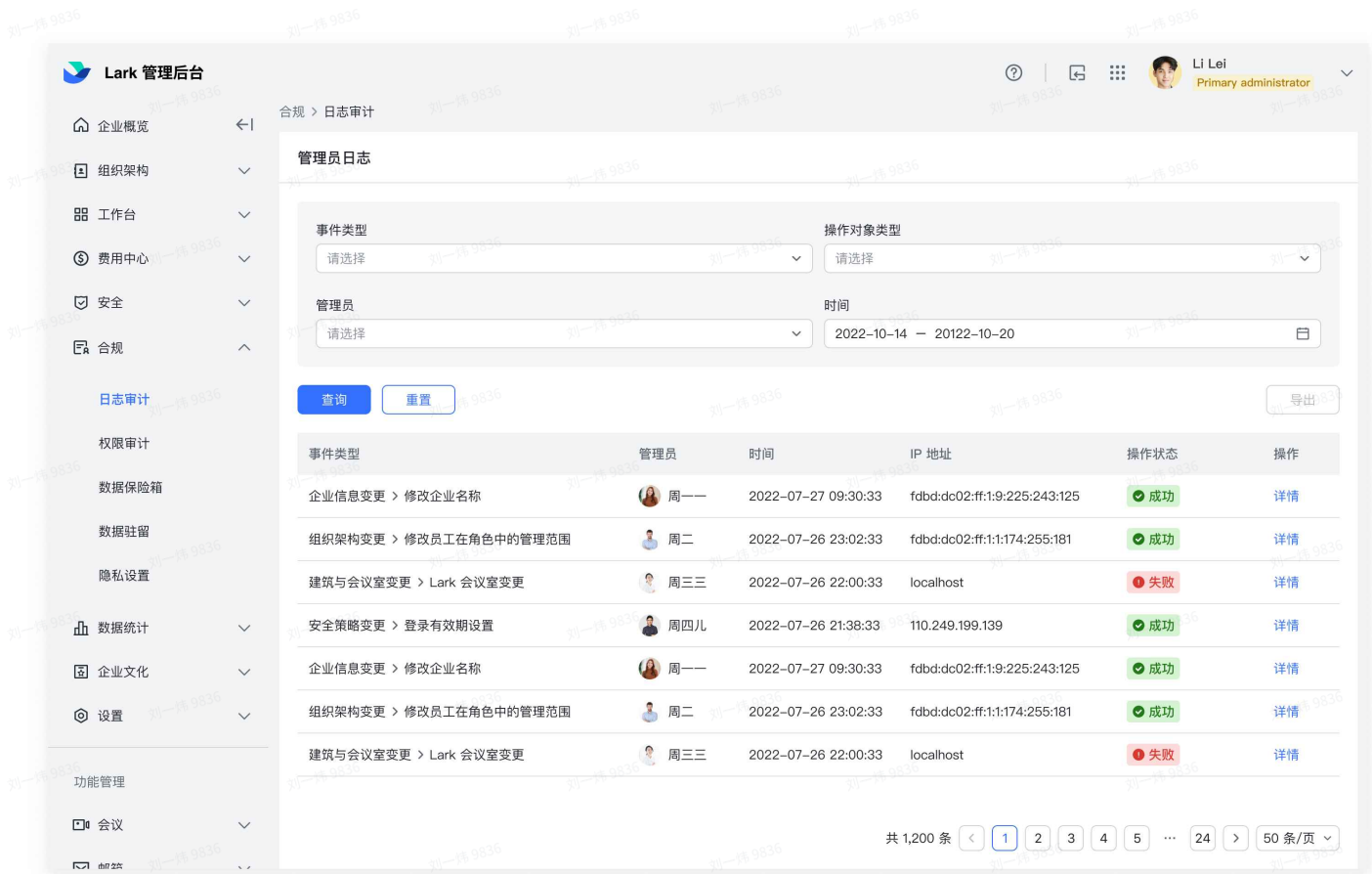


3 数据留存

Lark邮箱对企业的合规审计有很好的支持，邮件数据可追溯可跟踪，管理员操作日志自动留存，以满足企业合规审计的要求。

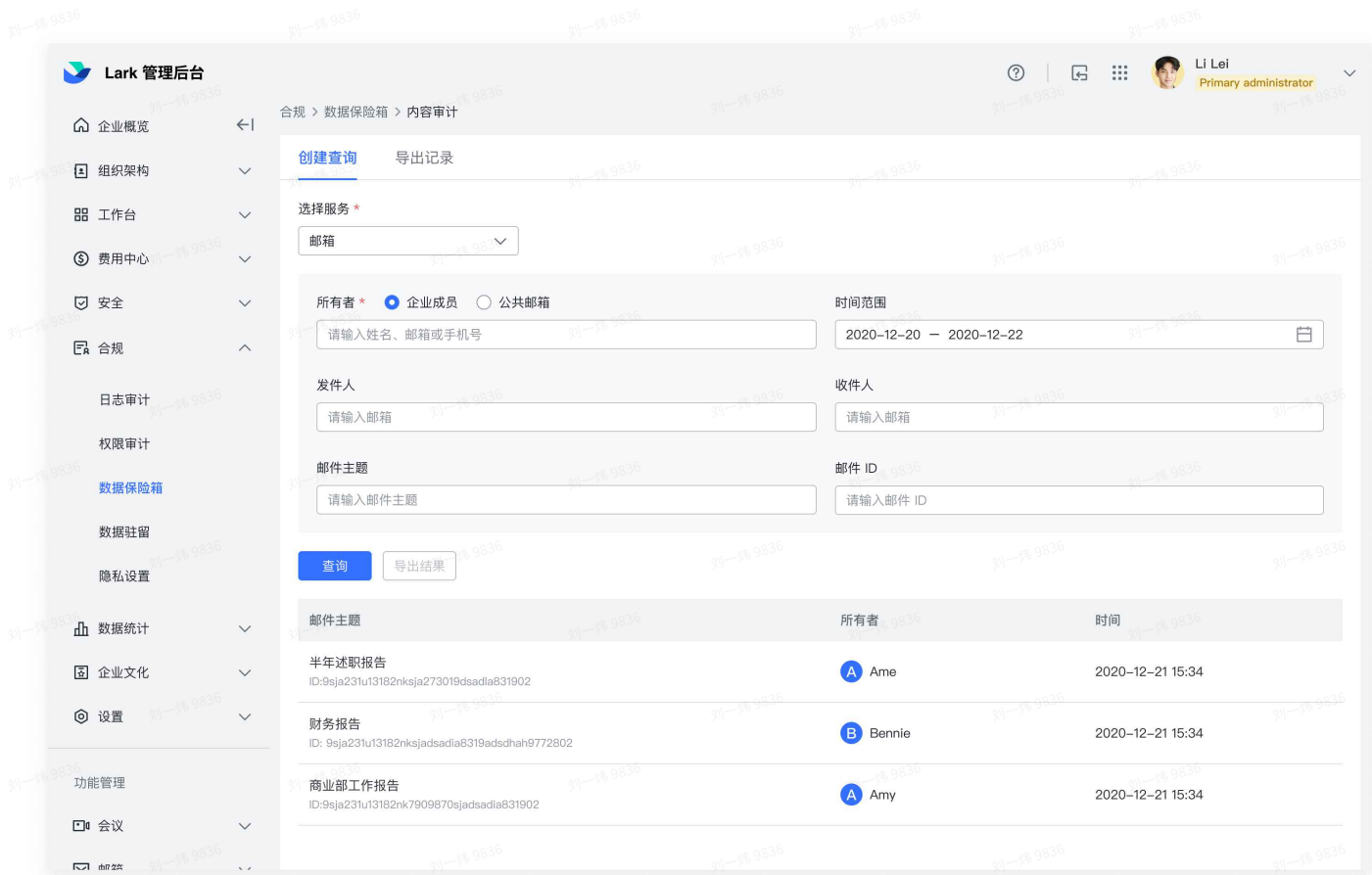
3.1 操作日志留存

管理员所有操作将会被自动记录到日志，且永久保留，保留期间数据无法删除。日志记录支持导出，便于公司调取查看管理员任何操作。



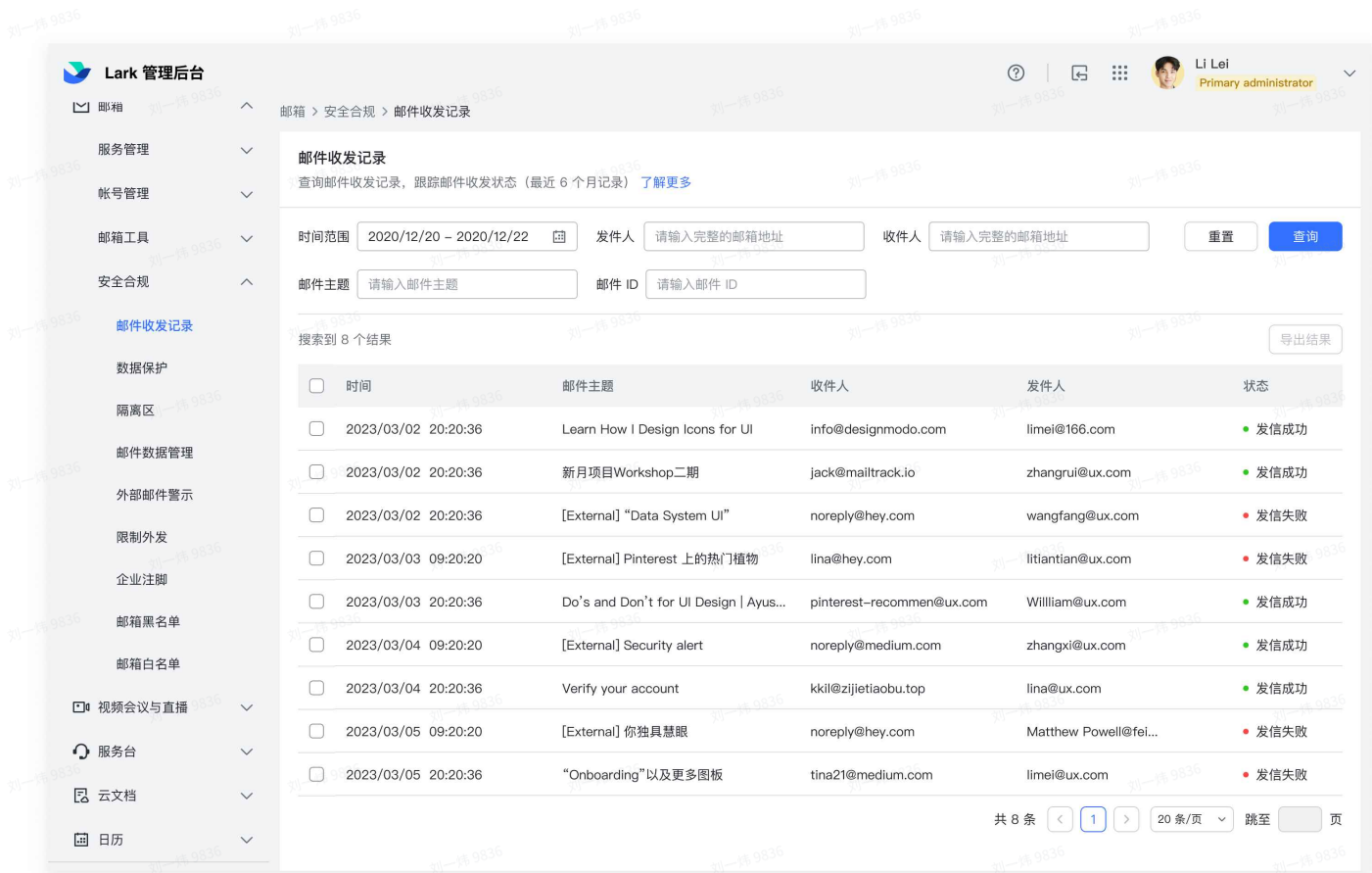
3.2 数据审计存证

Lark邮箱为满足企业客户合规审计需求，提供数据保险箱功能。企业内所有成员的收发邮件将自动归档到数据保险箱中，包括员工在客户端删除的邮件、离职员工的历史邮件，实现了所有历史邮件可追溯、服务期内永久保留、支持实时搜索、访问及导出，方便企业客户日后用于审计、司法公证。

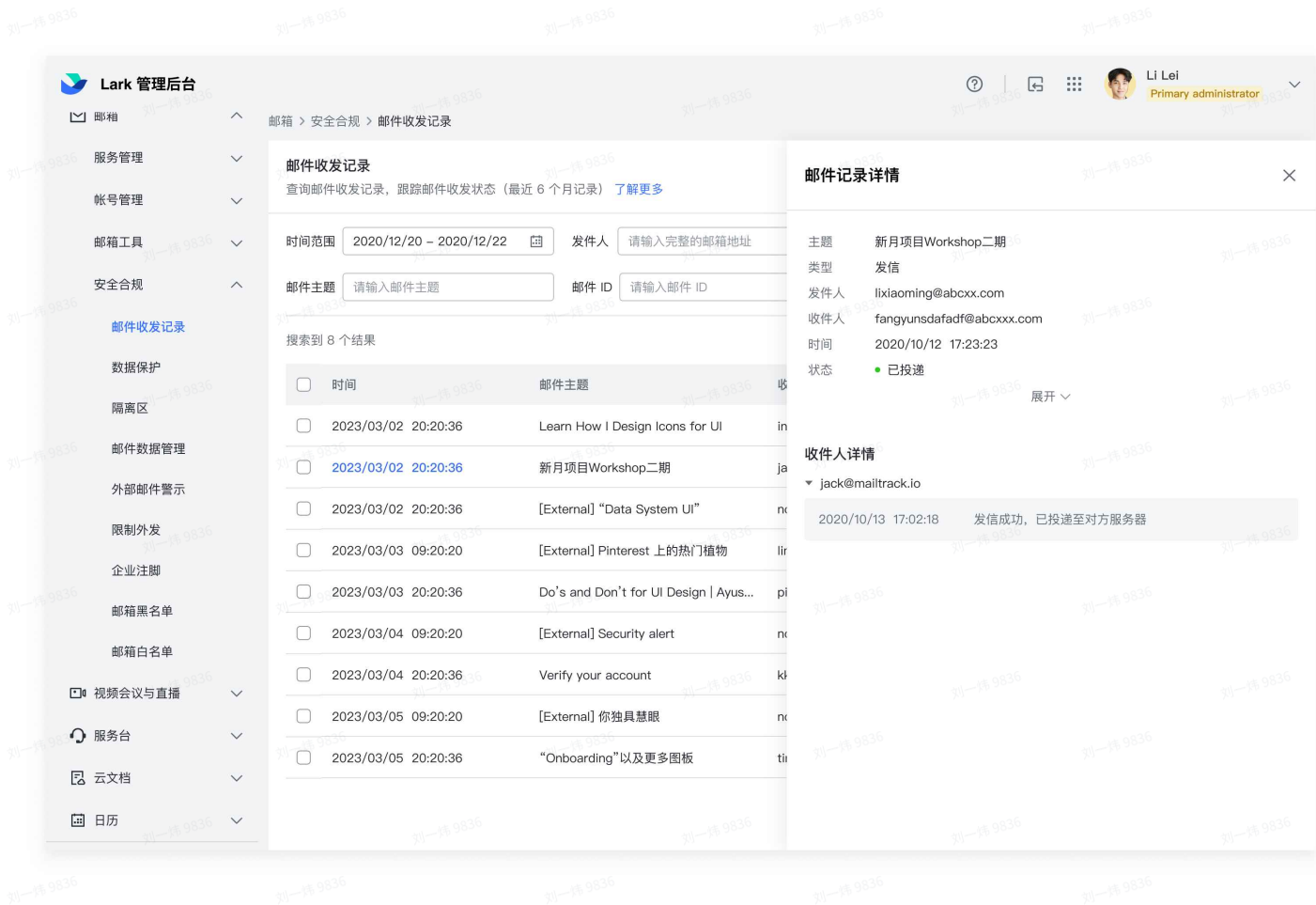


3.3 数据跟踪

在Lark邮箱，邮箱管理员可查询 6 个月内所有邮件的收发记录，跟踪邮件收发状态，让管理员掌握邮件数据的动向。



在Lark邮箱，邮箱管理员对员工已发送的邮件可执行撤回，对员工已删除的邮件可执行恢复，满足企业对于敏感数据防泄露、核心数据留存的需要。



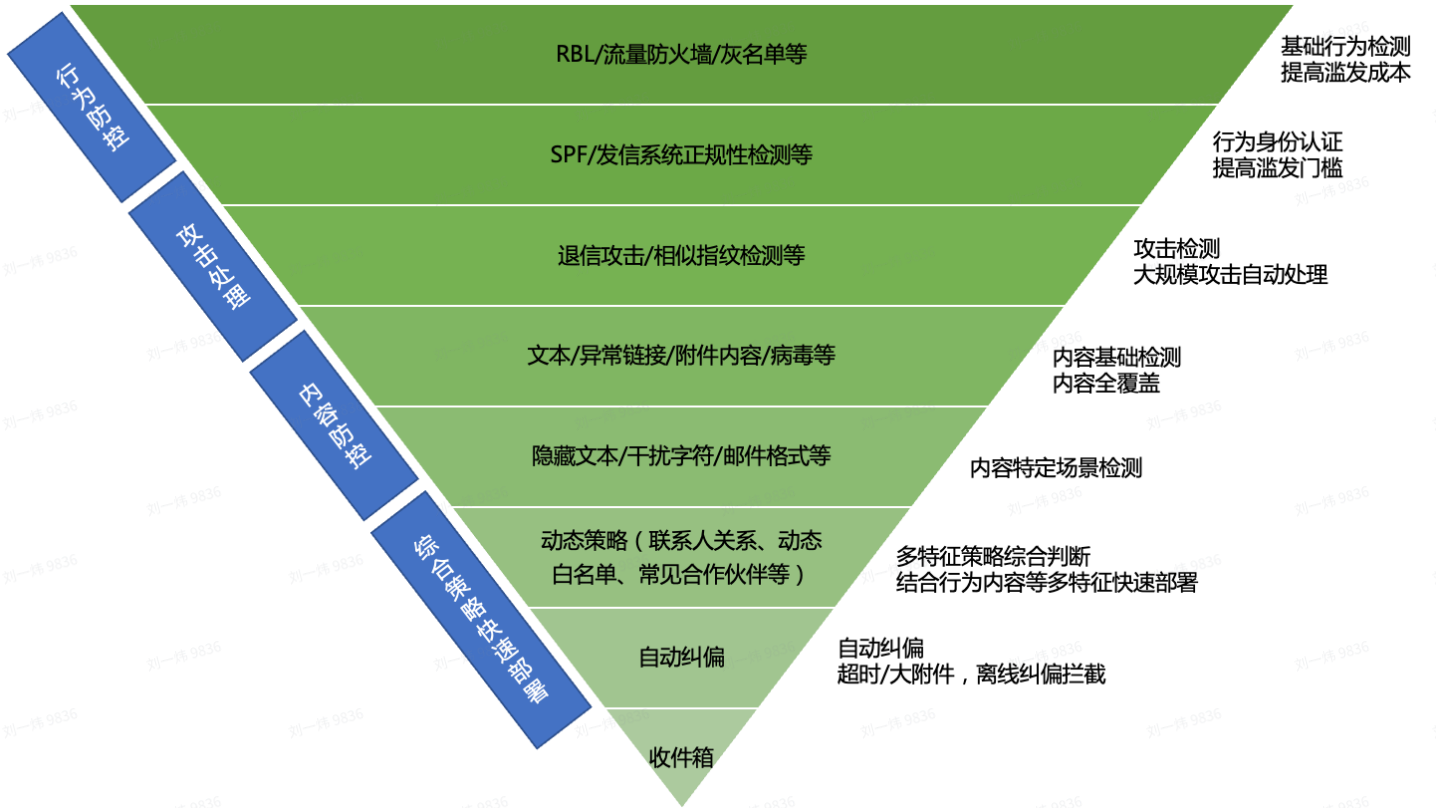
4 邮箱反垃圾

Lark邮箱反垃圾系统是一套用于维护收发信环境安全的综合系统，基于强大的算法能力，能够针对不同类型的钓鱼、病毒、广告、垃圾邮件、附件进行有效识别，降低企业邮件安全风险，保障企业的信息

和生产安全。

4.1 反垃圾过滤能力

Lark邮箱反垃圾通过多系统协同实现7层过滤机制，垃圾邮件识别率大于99%，有效防止垃圾邮件扩散。



基础行为检测：垃圾邮件发送者通常会在短期内向目标系统大量发送邮件，通过多维度频率监控及流量防火墙、DNS查询多个国际反垃圾组织黑名单结果、动态灰名单等对异常流量及行为进行拦截，减少邮箱遭受攻击的风险。

身份认证：全面支持 SPF/DKIM 等全球先进的反垃圾协议，能进一步防止冒用及钓鱼，提升邮件安全能力。

防攻击关联检测：智能分析收发信关系，有效拦截退信攻击；利用指纹算法检测邮件相似性，关联不同发件人的垃圾邮件，扩大识别范围并自动化处理。

内容检测：对邮件主题、正文、附件内容、附件病毒、附件类型、链接、信头等进行全面垃圾检测，多套先进的算法模型用于内容过滤，有效减少不良内容进入用户收件箱。

特定场景检测：针对利用隐藏文本、干扰字符、异常邮件格式等躲避反垃圾检测的特殊场景，及时扩充垃圾特征，多手段检测提升黑产作弊门槛。

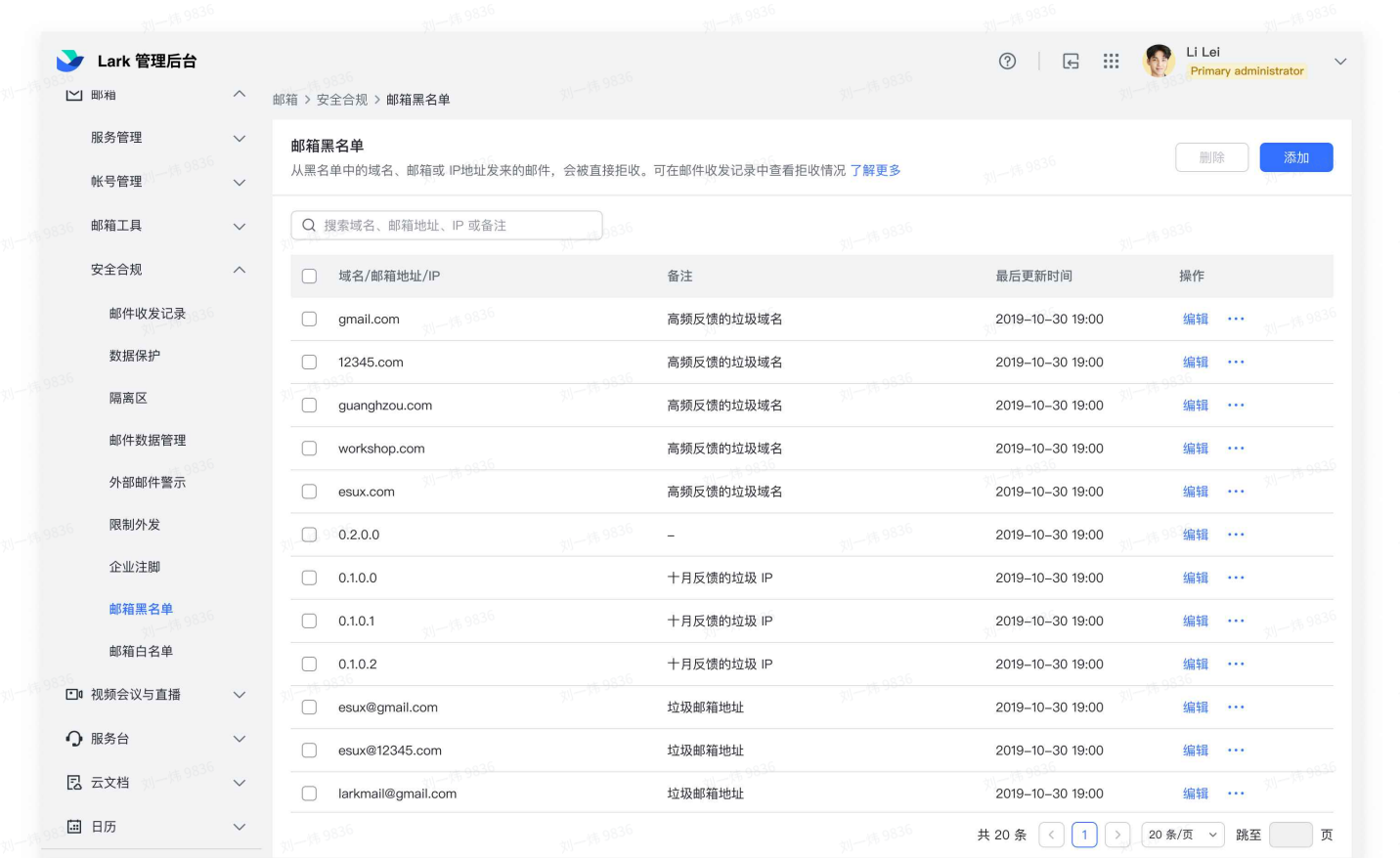
多特征策略综合检测：结合身份认证、发信行为、邮件内容等多特征配置组合策略进行综合判定，策略可快速部署。

自动纠偏：当遇到系统超时或者超大附件病毒扫描耗时较长时，会对邮件进行离线扫描，若离线扫描有问题，系统会自动将问题邮件从收件箱纠偏至垃圾箱。

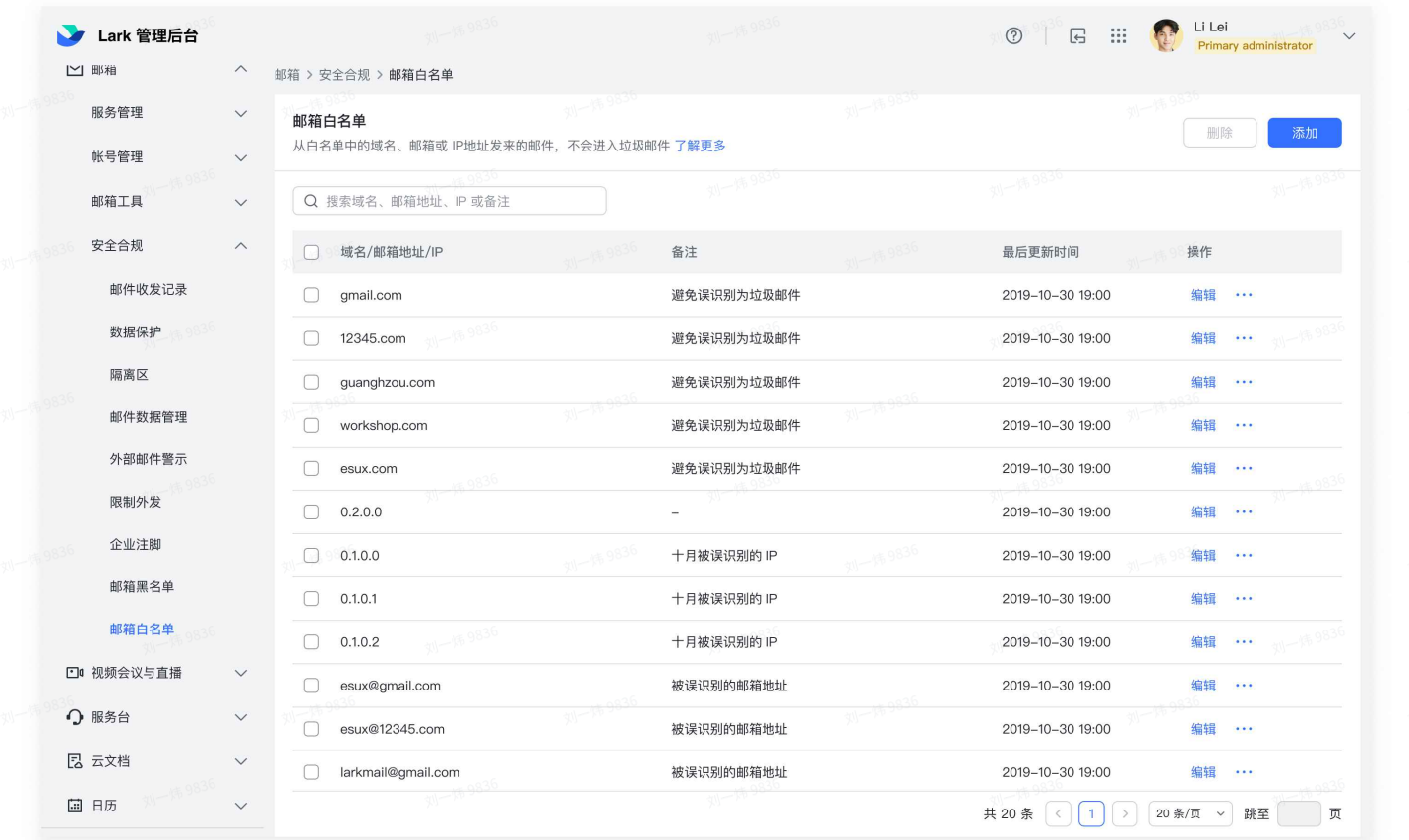
4.2 反垃圾产品功能

4.2.1 管理员侧 黑/白名单机制

企业如果频繁遭到某个域名或者某个邮箱地址的骚扰，可以将域名或邮箱地址添加到邮箱黑名单内，来自黑名单中域名或邮件地址的邮件，将会被直接拒收。



企业可以将需要一直收到邮件的域名或邮件地址，添加到邮件白名单中，以确保能正常接收来自白名单内的域名和邮件地址的邮件，避免遗漏和错过重要的邮件。在大多数情况下，企业无需配置白名单，Lark邮箱会准确判断区分垃圾邮件和正常邮件。



4.2.2 用户侧 黑/白名单机制

如果用户在收件箱中收到垃圾邮件，可以将该邮件标记为垃圾邮件或移至“垃圾邮件”文件夹，今后来自该发件人的邮件都将被自动移至“垃圾邮件”文件夹。

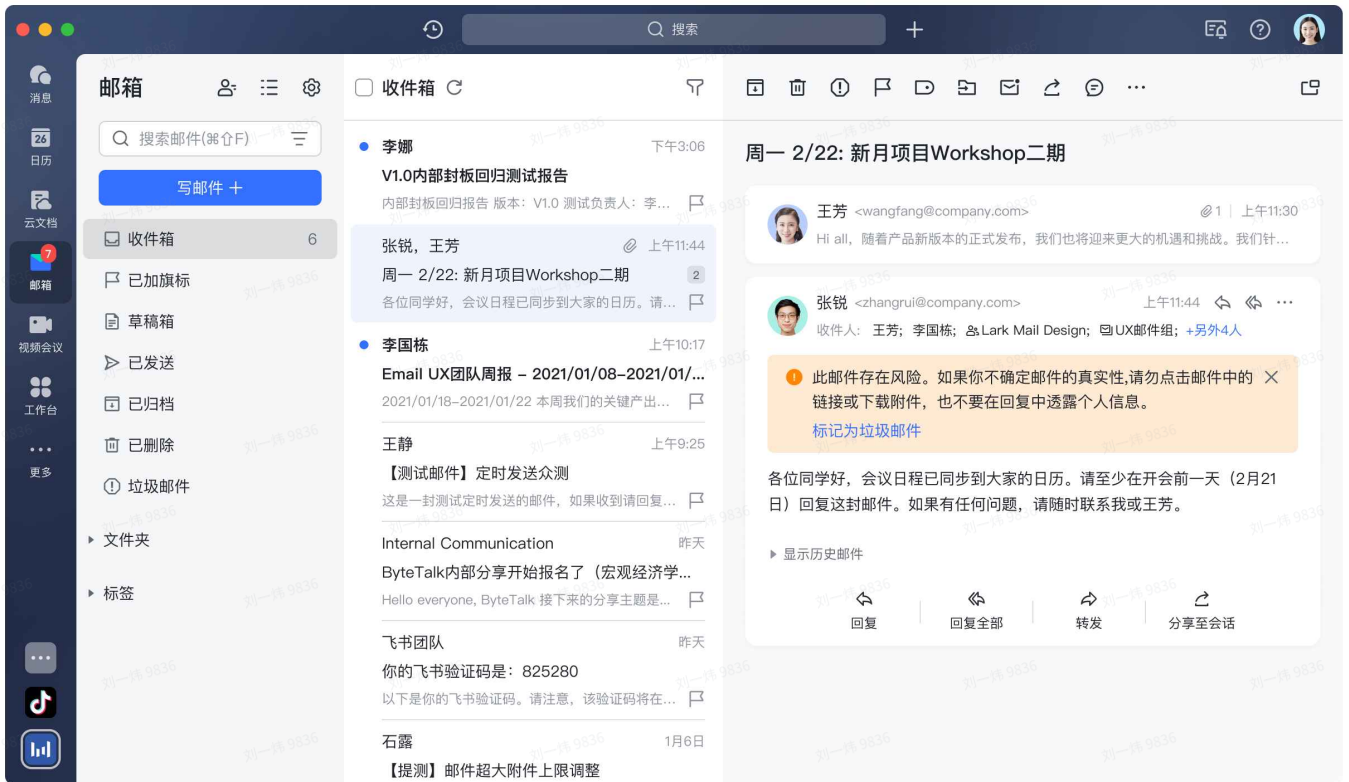
如果Lark邮箱中的垃圾邮件归类不正确，或者用户自己将邮件错误地标记为垃圾邮件，用户可以点击邮件上方的“这不是垃圾邮件”按钮，今后来自该发件人的邮件将会正常进入收件箱，而不会被自动移至“垃圾邮件”文件夹。

关于用户侧黑/白名单机制完整介绍，可查看[垃圾邮件处理指南](#)

4.2.3 风险提醒

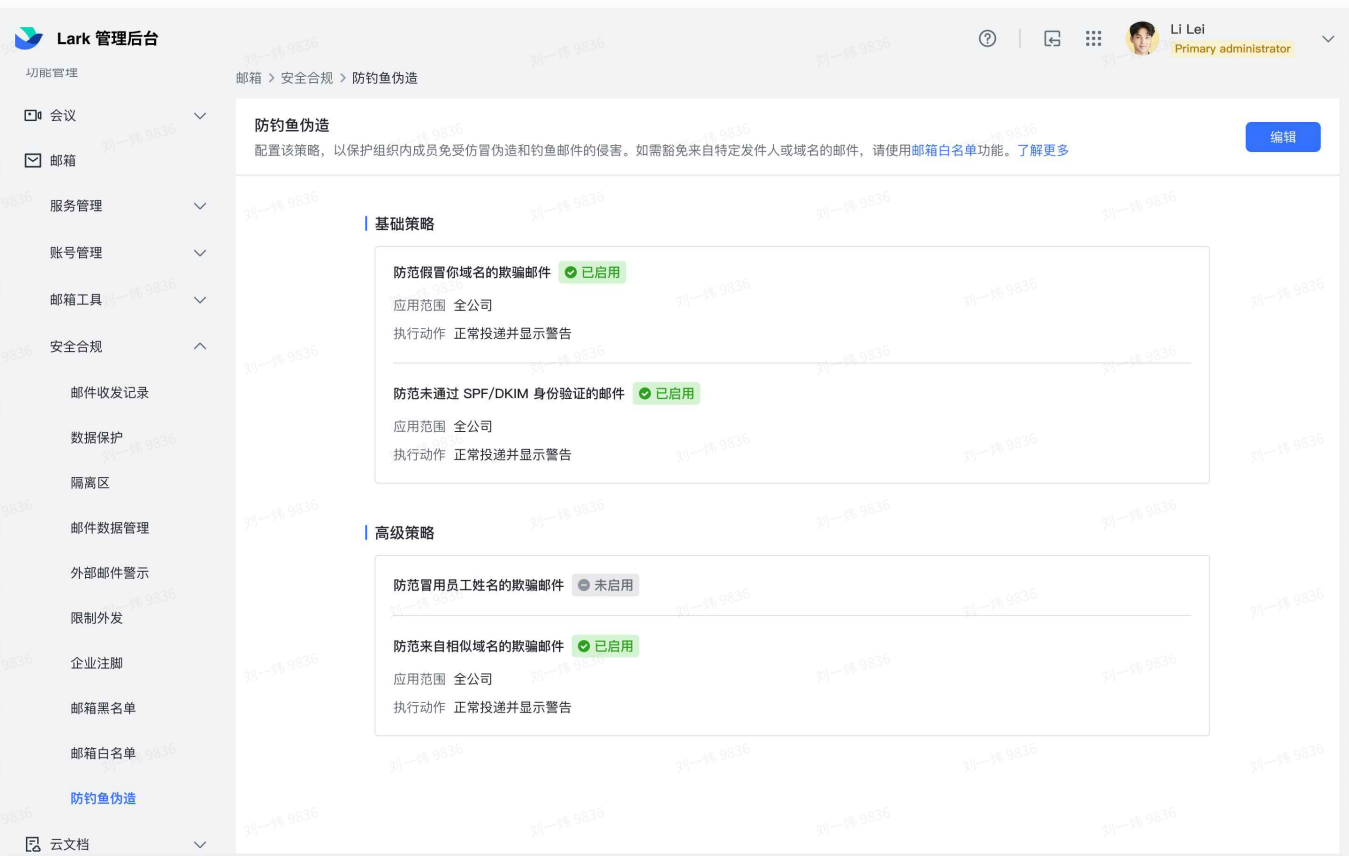
Lark邮箱对无法确认邮件发件人真实身份的邮件以及钓鱼、病毒等高风险邮件，会在邮件上方弹出风险提示，提醒用户谨慎处理，保护好个人信息。

未通过身份验证的邮件不一定是垃圾邮件，可以在 **收件箱** 或 **垃圾邮件** 看到未通过身份验证的邮件，根据情况选择是否标记为垃圾邮件。



4.2.4 管理员防钓鱼伪造功能

管理员可以为企业设置防钓鱼伪造策略，保护组织内成员免受仿冒伪造邮件和钓鱼邮件的侵害。



目前防钓鱼伪造功能提供了以下四种策略：

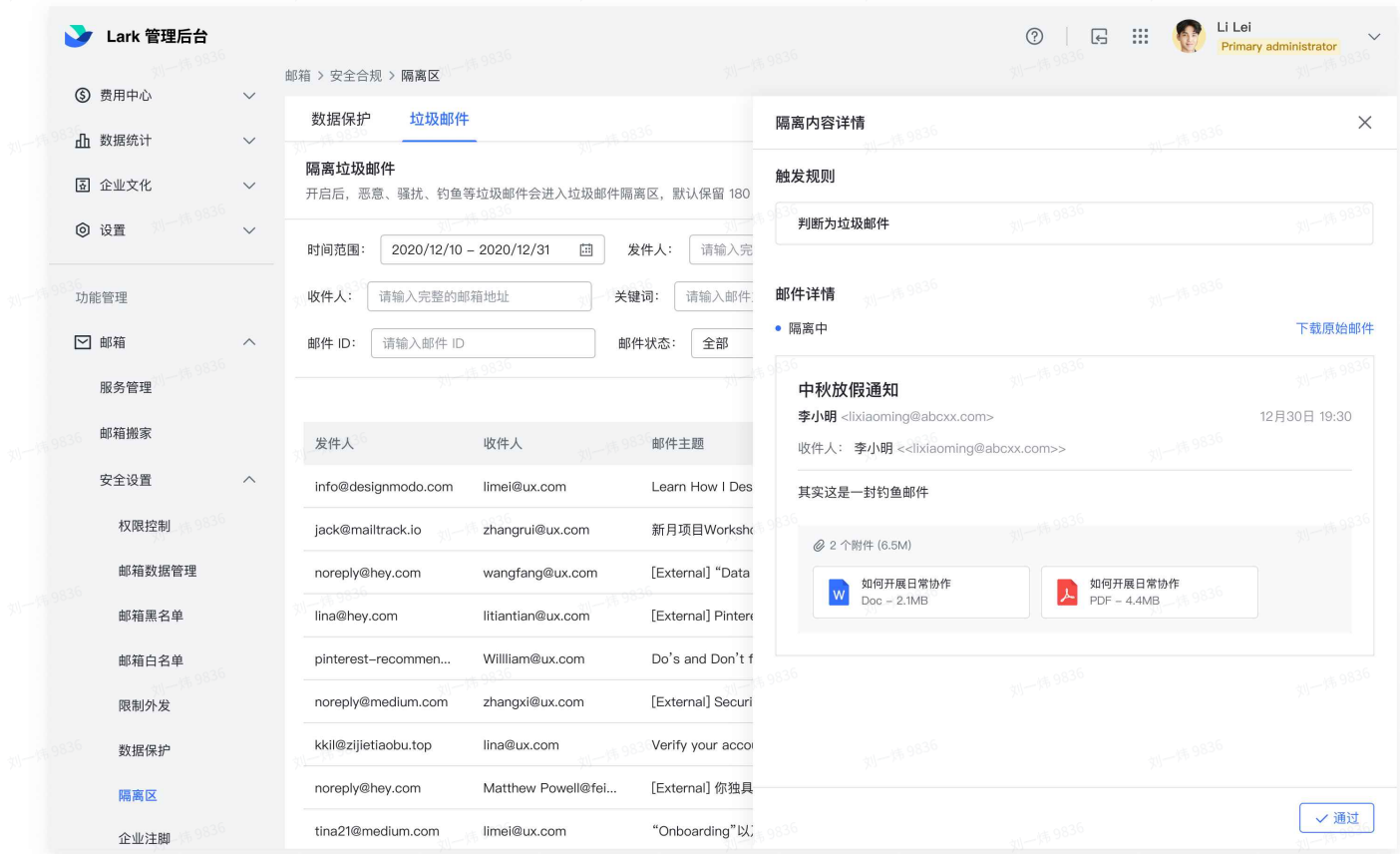
策略名称	说明
防范假冒你域名的欺骗邮件	防范假冒来自于公司域名，但实际未通过 SPF 或 DKIM 身份验证的邮件
防范未通过 SPF/DKIM 身份验证的邮件	防范未通过 SPF 或 DKIM 身份验证的邮件
防范冒用员工姓名的欺骗邮件	防范来自公司外部，发件人名称与防冒用姓名（包括默认名称、英文名和别名）相同的邮件
防范来自相似域名的欺骗邮件	防范外部使用与公司域名相似的域名发来的邮件，例如："examplee.com" 和 "eaxmple.com" 可能会被视为"example.com"的相似域名

关于管理员防钓鱼伪造功能完整介绍，可查看[管理员如何开启防钓鱼伪造功能](#)

4.2.5 隔离区邮件审核

触发数据保护规则或者被系统判定为垃圾邮件的邮件会进入隔离区，管理员可以在隔离区管理被拦截的邮件。

管理后台可见"数据保护"和"垃圾邮件"两类隔离区，按照邮件所在隔离区、时间范围、发件人、收件人、邮件主题、邮件 ID等进行检索后，在列表中点击邮件，能够查看该邮件被递送至隔离区的原因和具体内容；对邮件选择通过或拒绝，点击通过则邮件正常收发，点击拒绝则该邮件不会进入收件人的收件箱。



关于邮箱隔离区完整介绍，可查看[Lark邮箱隔离区](#)

5 应急响应策略

事故处理流程：

1. 前置监控系统检测到相关指标到达阈值后，启动事故障影响面分析并通知值班群；
2. 值班同事开始进行话术及客户预案准备与事故预警，待确认事故后第一时间知会客户；
3. 事故处理完毕或指标正常后，值班同事再次知会客户，并启动后续事故复盘相关事宜。