Lark Mail Security White Paper

Foreword

With the development of the Internet, the use of business email has become more convenient and are applicable in various scenes. However, Internet businesses are constantly confronted with various risks today, such as hack attacks, sensitive information theft and misuse, malicious harassing messages, and so on. Lark Mail is secured with a robust information security system which is based on years of security capabilities and experience.

To help you understand the security capabilities of Lark Mail better, this white paper describes the information security capabilities of Lark Mail from aspects such as compliance, sensitive data protection, data retention, and anti-spam capabilities. Lark Mail maintains information security for organizations and users by coping with various Internet attacks and preventing user information from leaking.

Version change record

Date	Version	Description
June 1, 2023	V1.1	Version created

1 Compliance and privacy

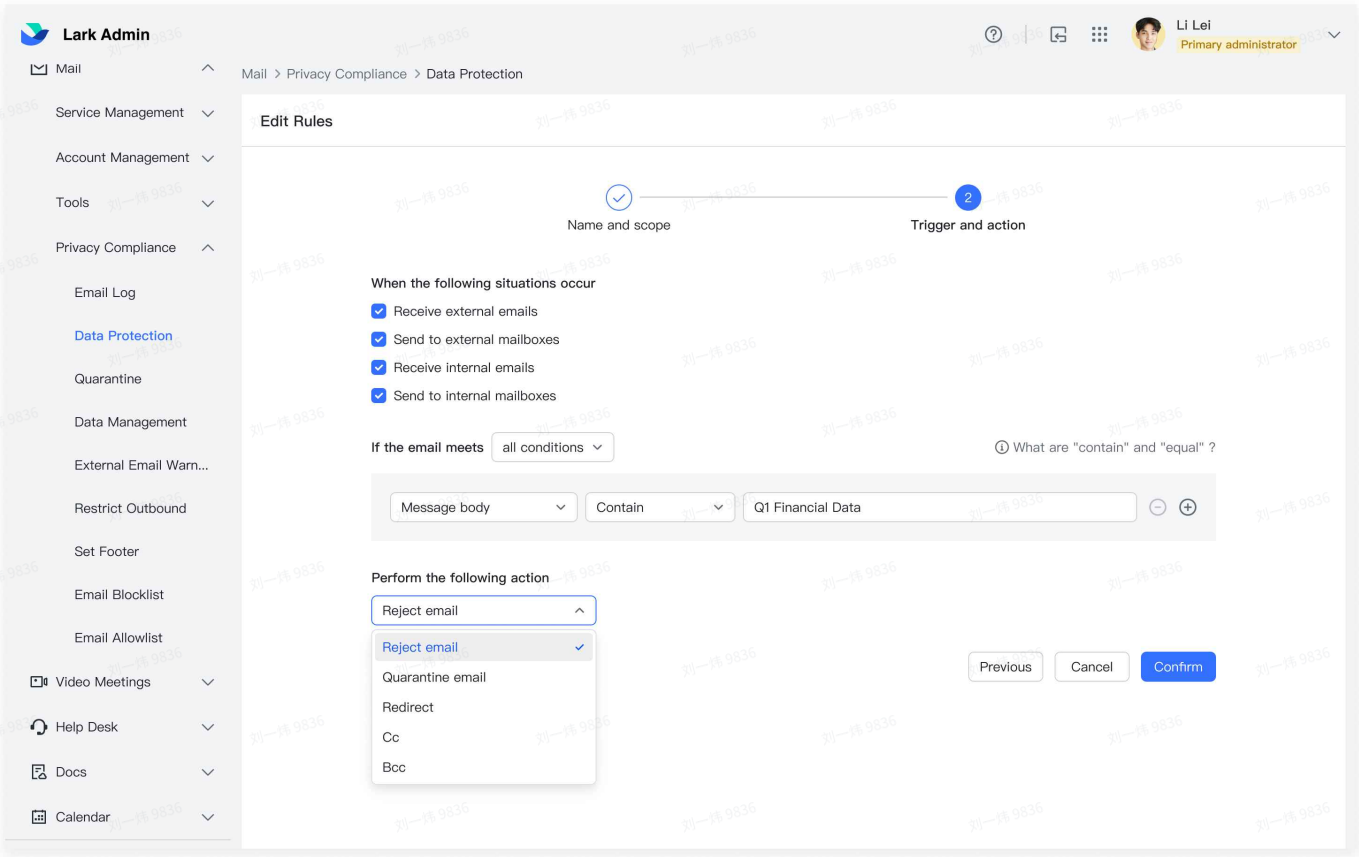
As a part of the Lark office suite, Lark Mail is consistent with Lark in terms of privacy compliance. Lark is committed to keeping data security, privacy, and security compliance for its users and has passed multiple international compliance certifications, such as ISO27001, ISO27017, ISO27018, ISO27701, CBPR&PRP, and DPTM, and has completed SOC 2 Type II and SOC 3 service certification reports.

For the complete introduction of Lark's compliance and privacy polices, see Lark Security and Compliance.

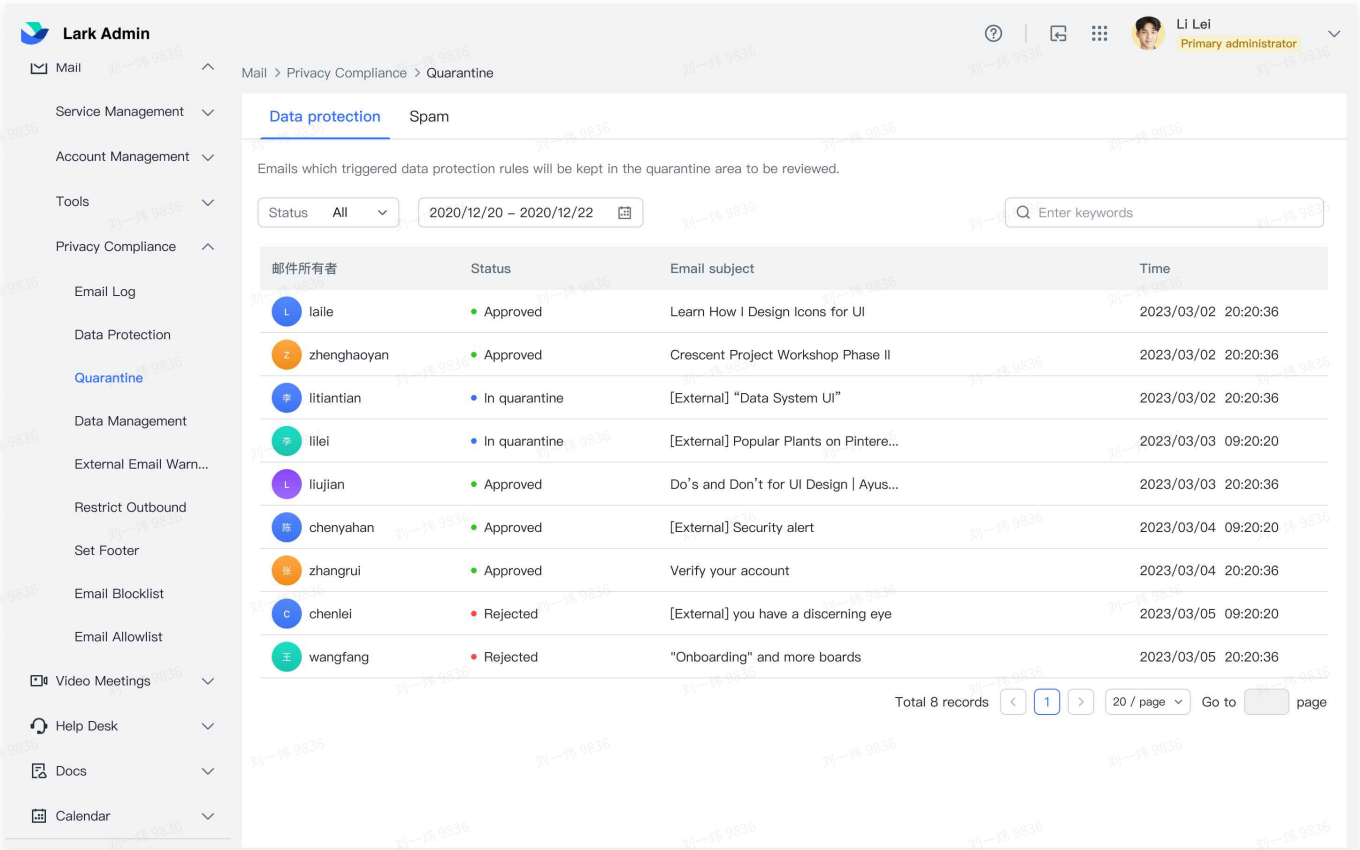
2 Sensitive data protection

2.1 Data loss prevention (DLP)

As sensitive organization data may be leaked when you sending or receiving business emails, Lark Mail offers data loss prevention. Organization administrators can configure data protection rules and define triggers and actions to be executed for the rules. After the rules come into effect, the system conducts content scans over the incoming and outgoing emails and automatically execute actions on once it detects that the email contents meets the rules. This ensures that sensitive and critical data of the organization will not be disclosed via emails.

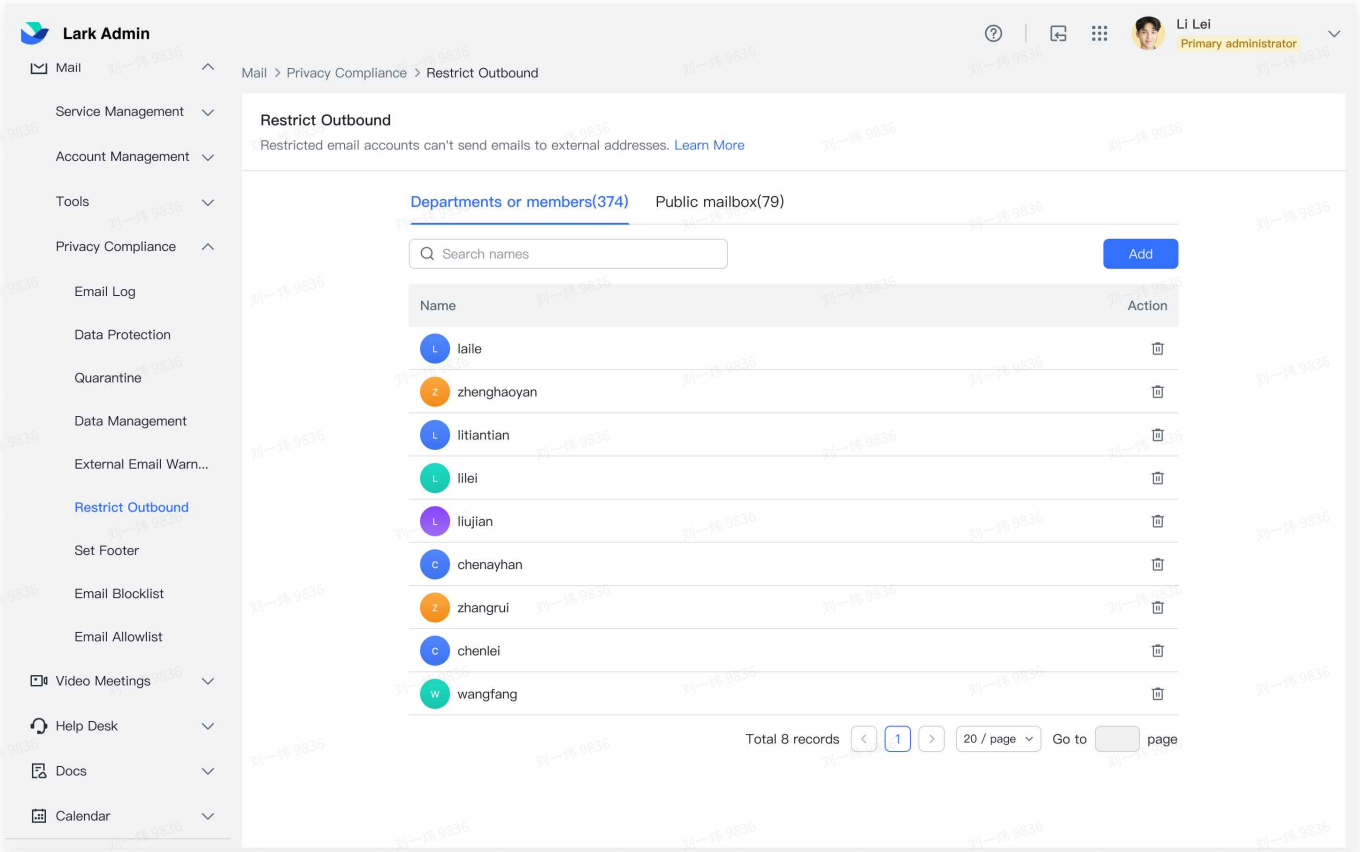


Emails declined to be sent and quarantined due to DLP rule triggering will be collectively placed in the quarantine. Organization administrators are allowed to review such emails in the quarantine and determine whether to release and resend these emails. This way, sensitive data of the organization are protected while normal email communications are ensured.



2.2 **Restriction on sending emails to users outside the organization**

Not all employees of an organization need to send emails to users outside the organization. Thus, to prevent leakage of sensitive organization data during email sending, you can configure settings to restrict certain employees from sending emails to external personnel. The restricted employees will not be able to send emails to external personnel, while internal email communications remain unaffected.

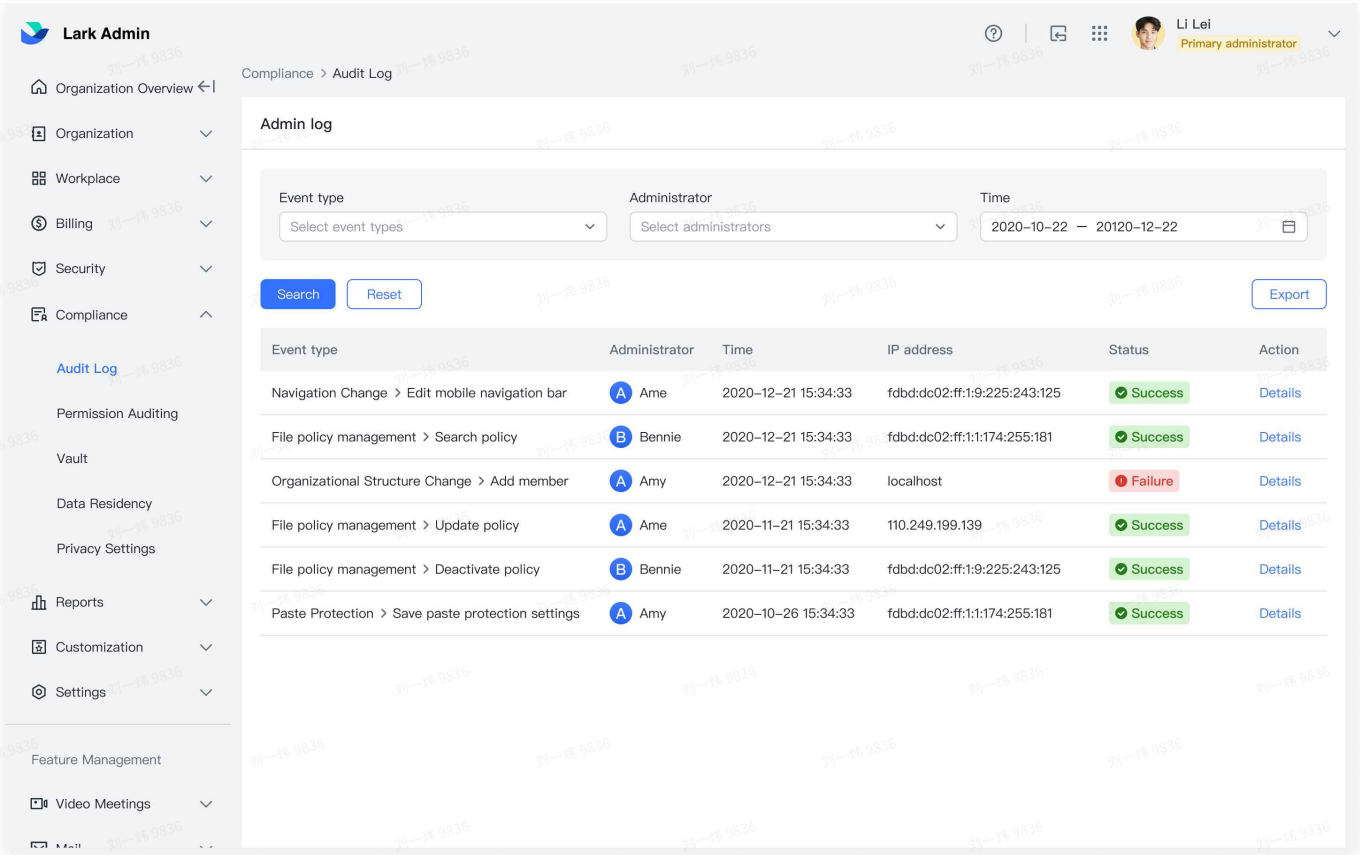


3 Data retention

With email data tracing/tracking and auto-retention of administrator action logs, Lark Mail makes compliance audit of organizations easy, meeting the organizations' requirements for compliance audits.

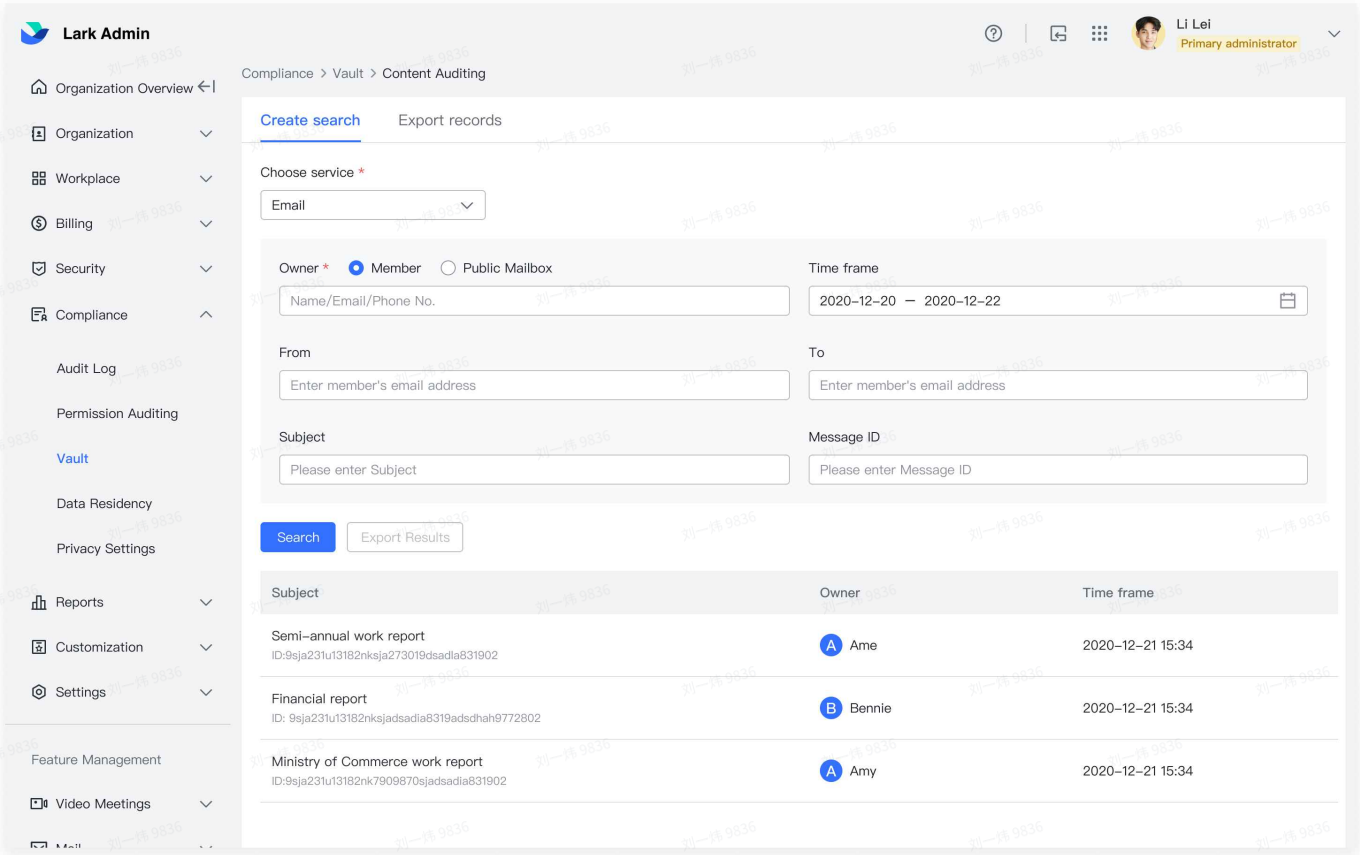
3.1 Action log retention

All actions of the administrators will be automatically logged and permanently kept. During the retention period, the data cannot be deleted. Log export is supported for retrieving and reviewing actions of the administrators.



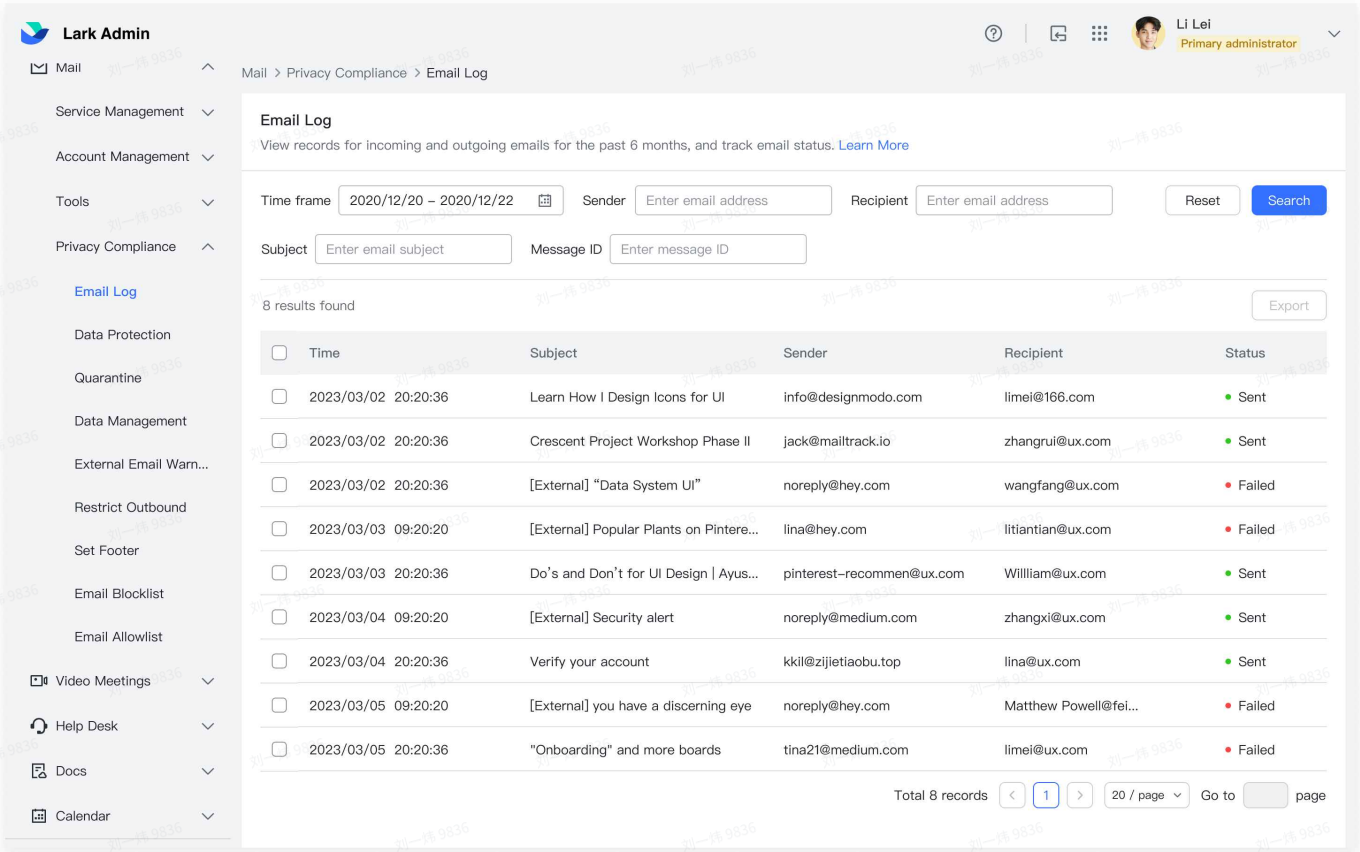
3.2 **Evidence preservation for data audit**

To meet the needs of our organization clients for compliance audits, we provide Data Vault in Lark Mail. All incoming and outgoing emails received and sent by organization members, including those deleted by the employees on the client side and emails of resigned employees, are automatically archived in Data Vault. This enables traceability, permanent storage through service period, real-time search, accessibility, and export of all emails, facilitating audits and judicial notarization of the organizations in the future.

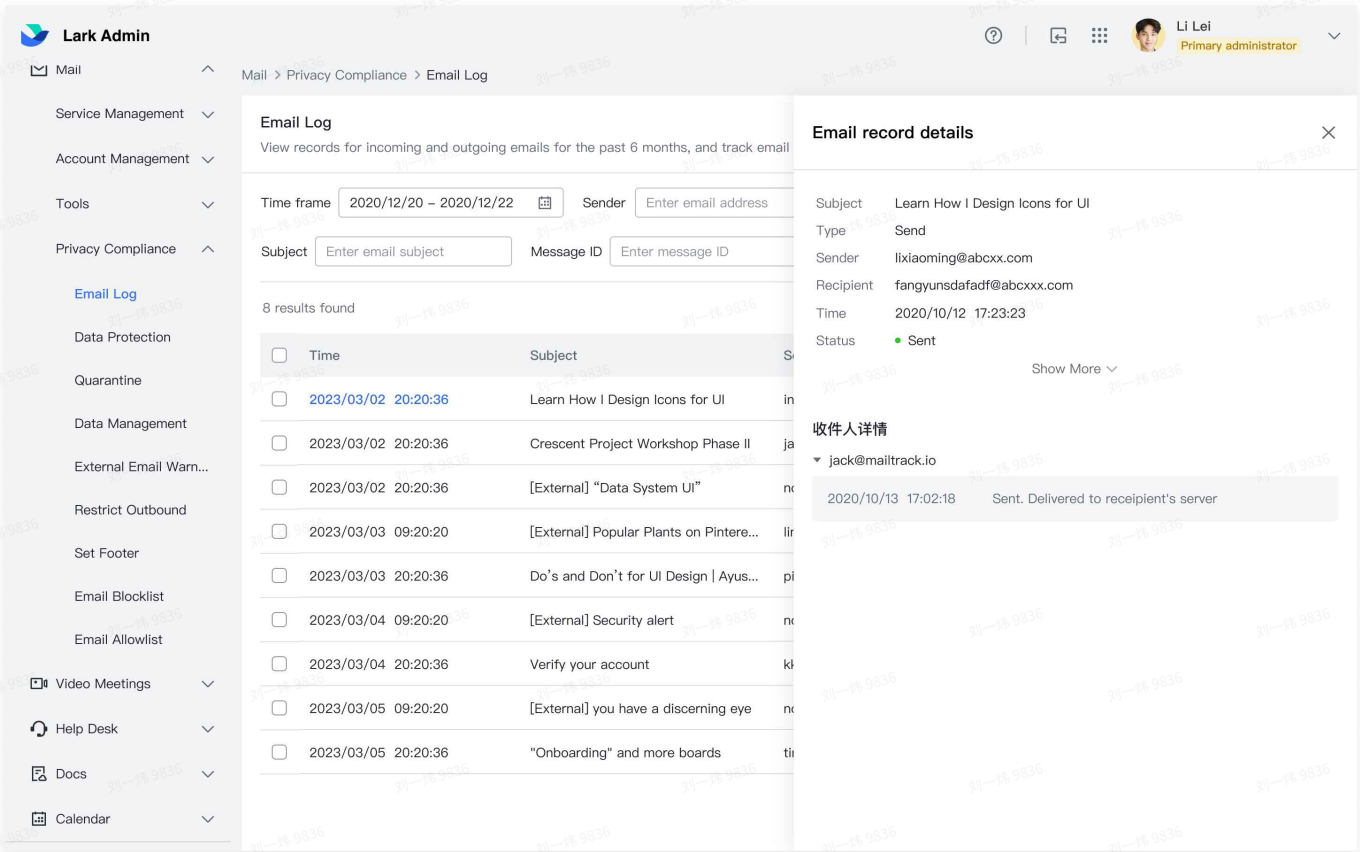


3.3 Data tracking

Lark Mail allows the administrators to inquire the incoming and outgoing email records in the last 6 months so that they can follow up the delivery status of the emails and keep tracks on the email data.



Besides, to meet the requirements of organizations for preventing sensitive data leakage and core data retention, Lark Mail allows the administrators to recall or recover emails sent or deleted by the employees.

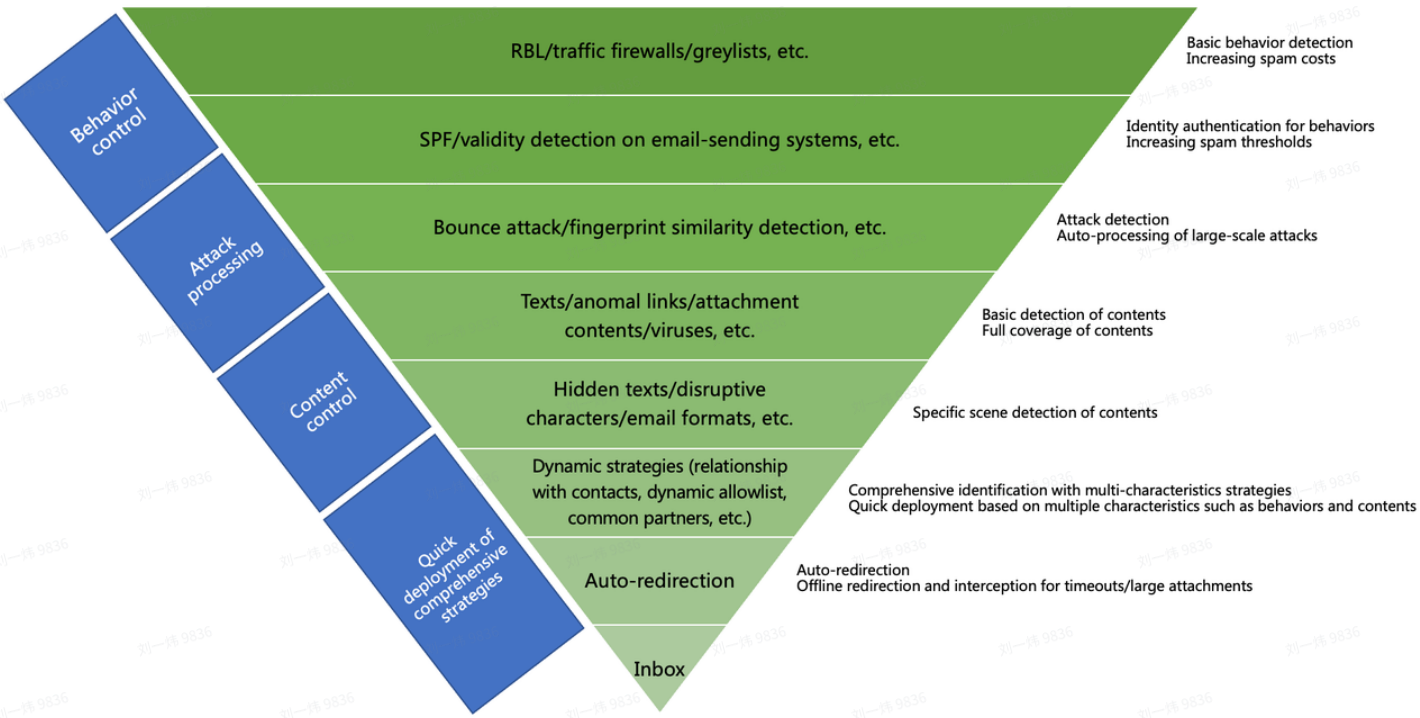


4 Anti-spam

The anti-spam system of Lark Mail is a comprehensive system that maintains environmental security during email delivery. With powerful algorithmic capability, the system can effectively identify different types of phishing emails, viruses, ads, spams, and malicious attachments. This reduces email security risks and ensures information and production security of the organizations.

4.1 Anti-spam filtering capability

The anti-spam function of Lark Mail fulfills a 7-layer filtering mechanism with multi-system collaboration. With a spam identification rate higher than 99%, it efficiently prevents spams from spreading.



Basic behavior detection: Spam senders usually send a large number of emails to a targeted system within a short period. Lark Mail implements effective measures, such as multi-dimensional frequency monitoring, traffic firewall, DNS inquiry about blocklists from multiple international anti-spam organizations, and dynamic greylist, to intercept abnormal traffics and behaviors to reduce the risks of email attacks.

Identity authentication: Globally advanced anti-spam protocols such as SPF/DKIM are fully supported to further inhibit spoofing and phishing and to improve email security.

Anti-attack association detection: Smart analysis of sending-receiving relationship is conducted to efficiently intercept bounce attacks. Fingerprint algorithm is used to check similarity among emails and associate spams from different senders. This expands the identification scope and facilitates automated processing.

Content detection: Comprehensive spam detection is carried out for email subject, body text, attachment contents, attachment viruses, attachment type, links, headers, and other information. Multiple advanced algorithmic models are used for content filtering and can effectively prevent malicious contents from entering the inboxes of the users.

Specific scene detection: For special scenes, such as those using hidden texts or disruptive characters, and those in abnormal email formats, which aim at escaping from anti-spam detection, we timely add spam characteristics and adopt multiple measures to enhance the cheating threshold of hack attacks.

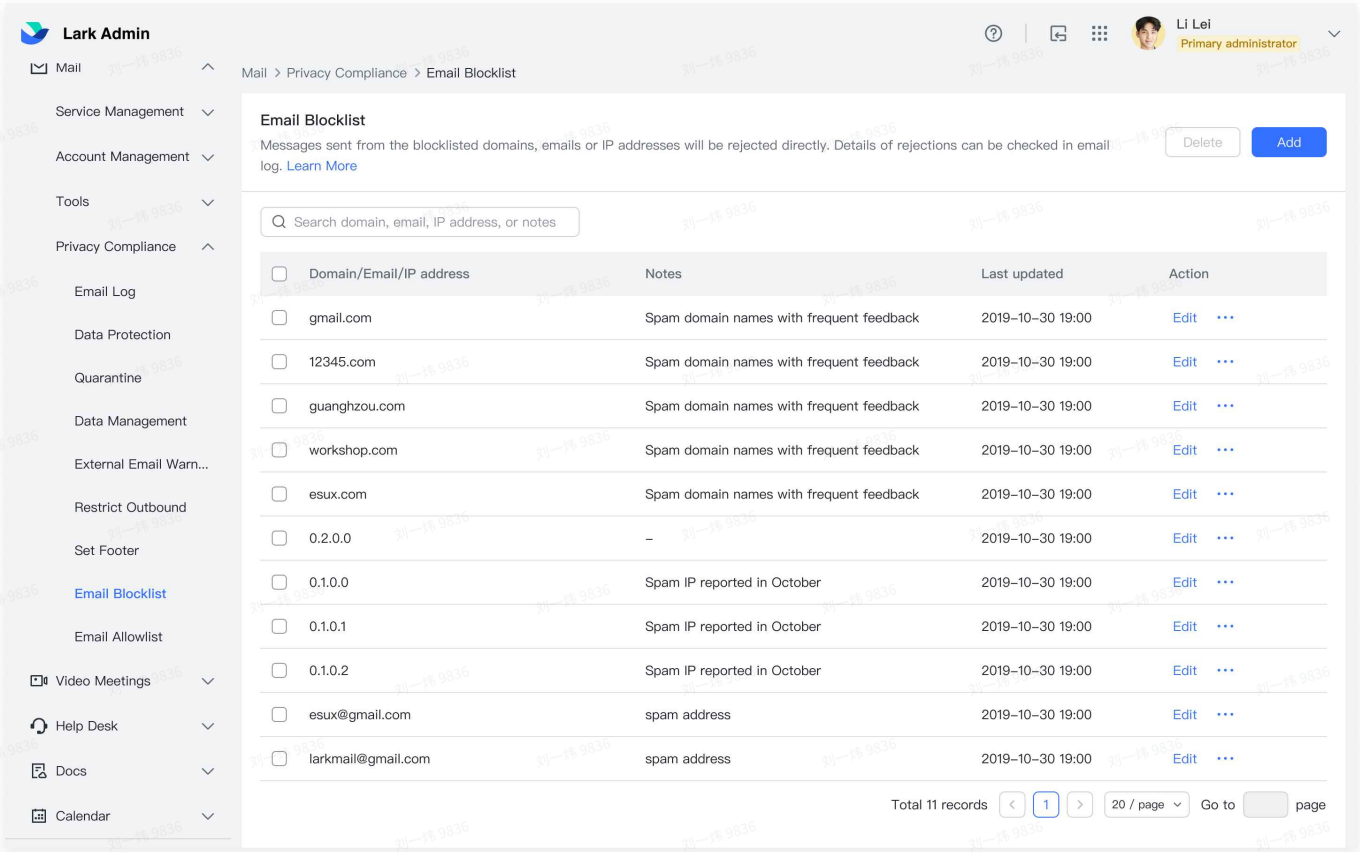
Comprehensive detection with multi-characteristics strategy: Multi-characteristics configuration portfolio strategies that integrate characteristics such as identity authentication, email sending behavior, and email contents are used for comprehensive identification. The strategies support quick deployment.

Auto-redirection: When system times out or virus scanning for large attachments takes a long time, offline email scans are carried out instead. In case of any anomalies, the system will automatically redirect such emails at question from inbox to the Spam folder.

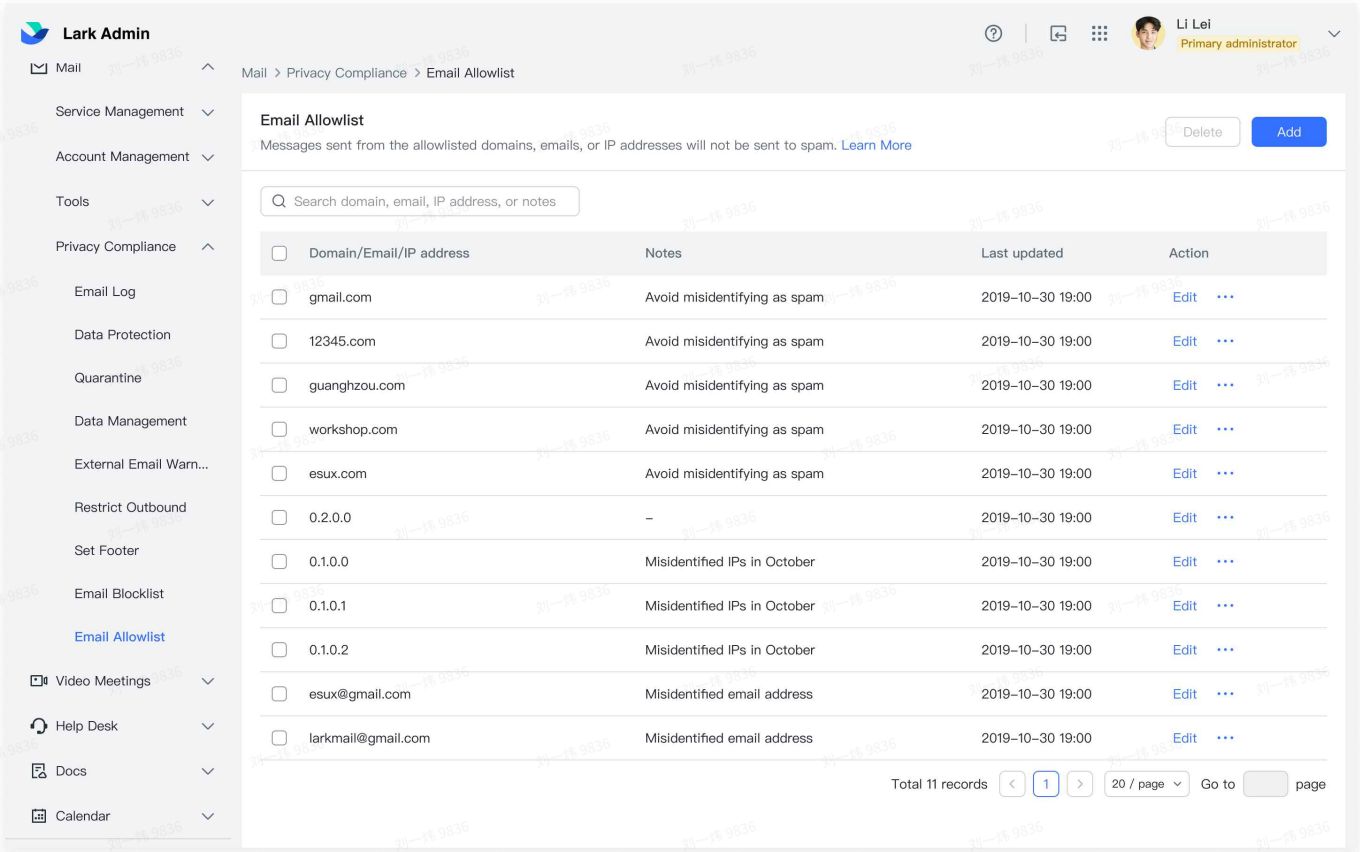
4.2 Anti-spam function of Lark Mail product

4.2.1 Administrator-side blocklist/allowlist mechanism

In case of constant harassment from a certain domain or email address, the organization can add such domain name or email address to its email blocklist. Mails sent from the domains or email addresses on the blocklist will be directly rejected.



Organizations can also add valid domain names or email addresses to its email allowlist. This ensures normal reception of emails from such domains and email addresses and avoids omitting or missing important emails. In most cases, allowlist configuration is not required because Lark Mail is able to identify and differentiate valid emails from spams.



4.2.2 User-side automatic blocklist/allowlist mechanism

You can mark any unwanted email in the inbox as a spam or remove it to the "Spam" folder. Future emails from the same sender will be **automatically** moved to the "Spam" folder.

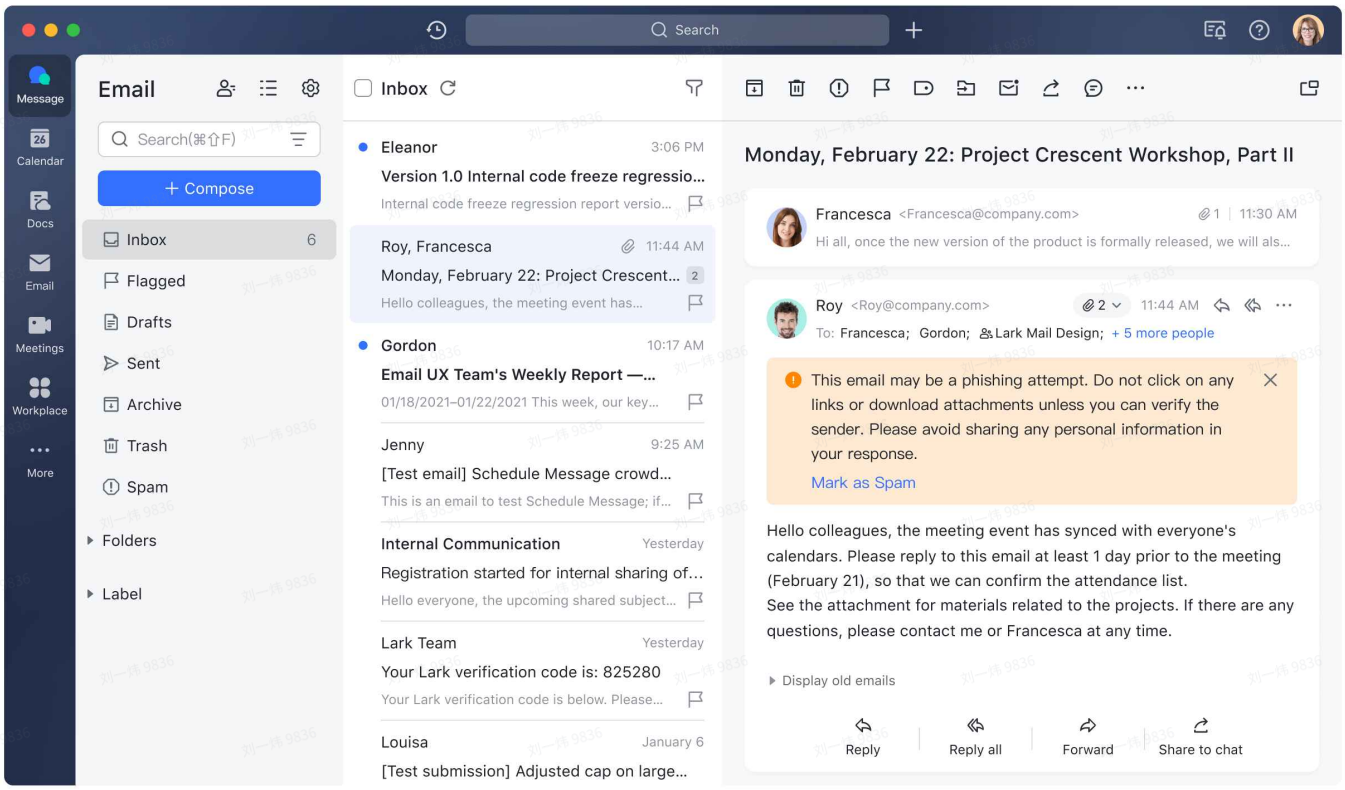
If an email is classified as spam by Lark Mail or you by mistake, you can click the **"This is not a spam"** button at the top of the email. Then, future emails from this sender will be placed in the inbox, not being automatically moved to the "Spam" folder.

For the complete introduction of the user-side automatic blocklist/allowlist mechanism, see Guide to handling spam emails.

4.2.3 Risk reminder

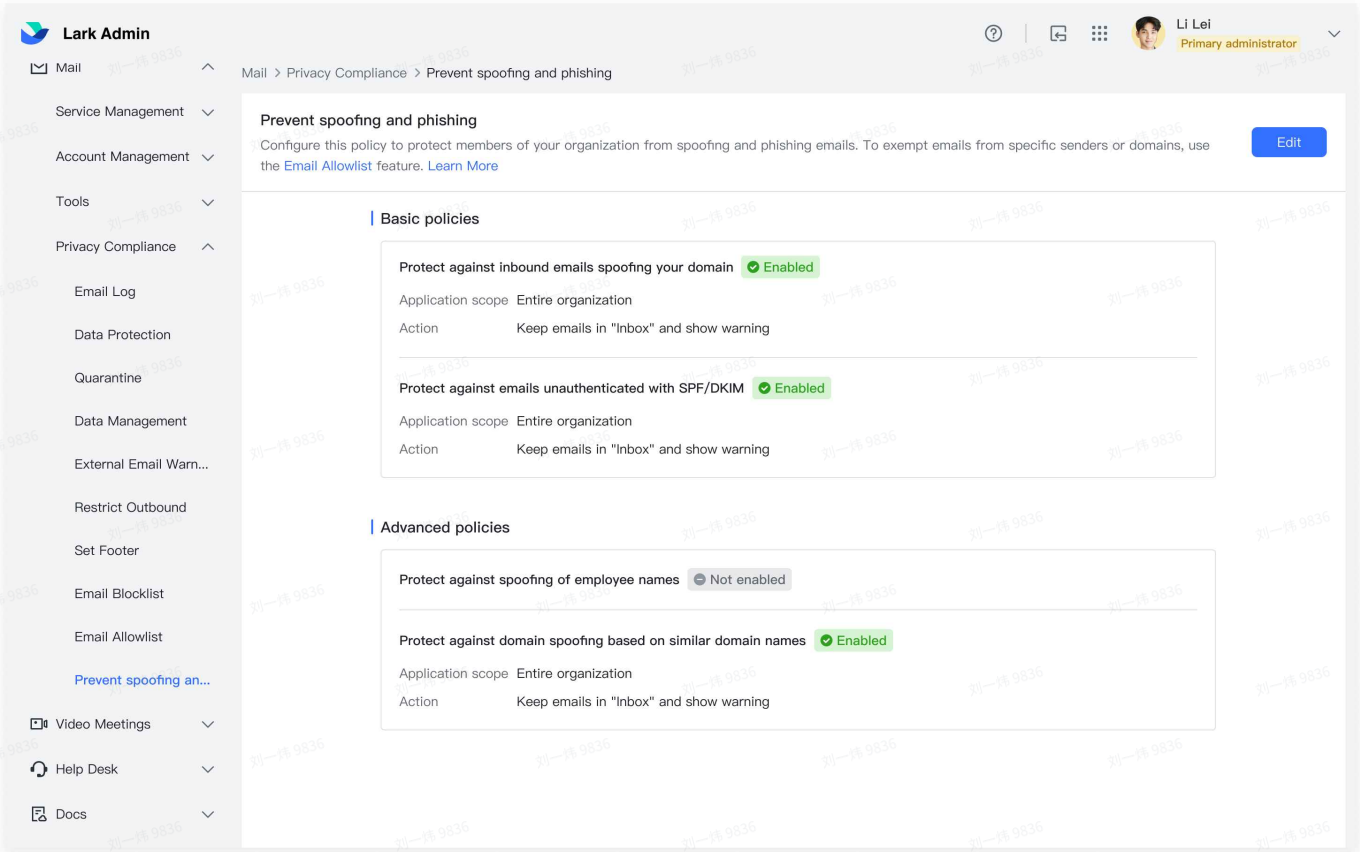
For emails whose senders cannot be identified and emails of high risks of phishing, viruses, or other attacks, Lark Mail provides pop-up risk reminders at the top of such emails. Users are reminded to handle those emails with caution for protecting their personal data.

Emails failing identity authentication are not always spams. You can check the unauthenticated emails in **Inbox** or **Spam** and determine whether to mark them as spams.



4.2.4 Anti-phishing/anti-spoofing function for administrators

Administrators are allowed to set up anti-phishing and anti-spoofing strategies for their organizations to protect organization members from infringement of spoofing or phishing emails.



Currently, the following four anti-phishing/anti-spoofing strategies are provided:

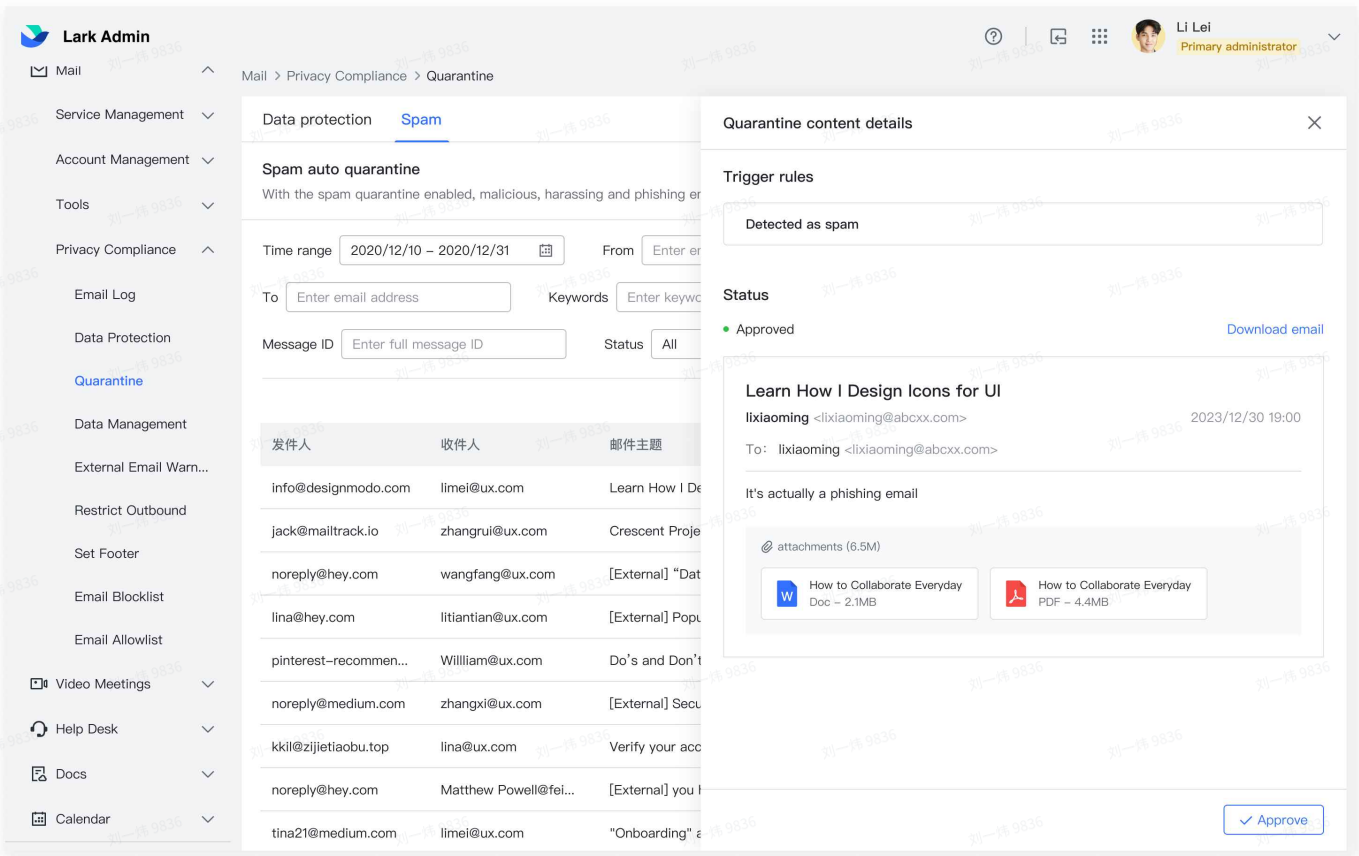
Strategy name	Description
Protection against deceptive emails with fake domain names as yours	Guards against emails sent from your company domain but failing to pass SPF or DKIM identity authentication
Protection against emails failing to pass SPF/DKIM identity authentication	Guards against emails failing to pass SPF or DKIM identity authentication
Protection against deceptive emails under employee names	Guards against external emails from senders whose names (including default names, English names, and aliases) are same as the ones under the anti-spoofing strategy
Protection against deceptive emails from domains with similar names as your organization	Guards against external emails from domains with similar names as your organization. E.g.: "examplee.com" and "eaxmple.com" may be deemed as similar domains to "example.com."

For the complete introduction of the anti-phishing/anti-spoofing function for administrators, see Admin | Prevent spoofing and phishing.

4.2.5 Verification of emails in quarantines

Emails triggering data protection rules or identified as spams by the system will be moved to a quarantine where administrators can manage such intercepted emails.

Two quarantines, namely "Data protection" and "Spam," can be found in Admin Console. Administrators can search an email based on information (such as the specific quarantine, time range, sender, receiver, email subject, and email ID) and click the email to check the reason why the email is transferred to the quarantine and the details. Administrators can click Pass or Reject. If Pass is clicked, this email enters the inbox; If Reject is clicked, this email does not enter the receiver's inbox.



For the complete introduction of the quarantine, see Lark Mail quarantine area.

5 Emergency response strategy

Accident response flow:

1. Pre-monitoring system detects that a metric has reached the threshold, initiates an accident impact analysis, and notifies the on-duty group.

2. The on-duty members prepare scripts and emergency plans for clients, send accident warnings, and inform the clients once the accident is confirmed.
3. Once the accident is under control or the metric is normal, the on-duty members notify the clients again, and make preparations for a subsequent accident review.