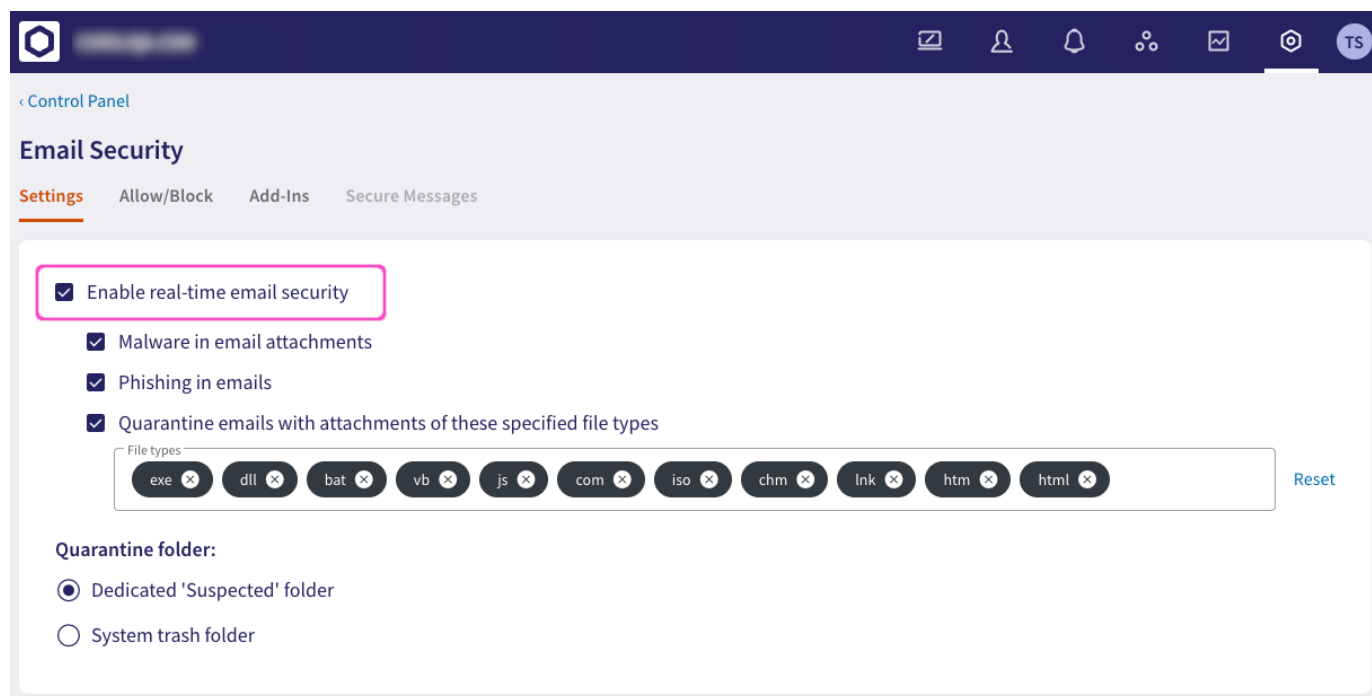


Settings

The **Settings** tab is used to manage Coro's email security settings. To enable email security, select **Enable real-time email security**:



This provides access to the following options:

- **Malware in email attachments**
- **Phishing in emails**
- **Quarantine emails with attachments of these specified file types**
- **Specify the default email quarantine folder**

Malware in email attachments

All incoming emails are immediately scanned for attachment files that might be malicious. Suspicious files are deleted for all recipients to prevent possible damage and a ticket is raised to record the event. As Coro has already enacted remediation, no further Admin intervention is required and the ticket is marked closed.

Admin users can review closed malware tickets to examine the details, including performing actions such as downloading the suspicious email for analysis or adding sender details to an Allowlist or Blocklist.

To learn more, see **Malware in email attachments**.