

Secure Inbox in Salesforce

Controlling Email Visibility Where It Actually Matters

The Problem Nobody Talks About

In Salesforce today, email visibility is controlled at the **record level - not the conversation level**.

That means:

If a user can access a record, they can see every email attached to it - regardless of sensitivity.

There is no native way to:

- Separate internal vs external communication
 - Restrict sensitive conversations
 - Control access at the email thread level
-

Why This Becomes a Real Risk

On a single record (Case, Account, Opportunity), teams handle:

- Customer communication
- Internal discussions
- Legal or compliance conversations
- Partner or vendor coordination

All of this gets stored together.

The result:

- Sensitive emails are exposed to unintended users
- Attachments follow the same visibility
- Compliance depends on user discipline, not system enforcement

Organizations are forced to rely on process instead of control.
And process breaks.

Why Current Workarounds Fail

Teams try to compensate with:

- Separate cases or records
- Manual email forwarding
- Naming conventions or “do not open” rules
- User training and internal guidelines

But in reality:

- These approaches increase complexity
- They are easy to bypass
- They introduce inconsistency across teams
- They create operational friction

Security becomes a human responsibility - not a system capability.

The Core Issue

The limitation is not email.

It's the lack of conversation-level control.

Salesforce handles:

- Record access very well

But:

- **Email conversations inherit record visibility automatically**
 - There is no native separation inside the same record
-

Introducing Secure Inbox

Secure Inbox introduces a new control layer inside Salesforce:

Conversation-level (thread-level) visibility

Instead of treating all emails on a record equally, it allows:

- Multiple independent email threads on the same record
- Each thread to have its own access rules
- Attachments to inherit thread-level security
- Clear separation between different types of communication

How It Works (Conceptually)

Within a single record:

- Emails are grouped into **threads (conversations)**
- Each thread has:
 - Its own visibility rules
 - Its own participants
- Only authorized users can access:
 - The thread
 - Its messages
 - Its attachments

What This Enables

True Separation of Communication

- Customer vs internal vs legal vs partner conversations
- All on the same record - without exposure

Predictable Security

- No reliance on manual behavior
- Enforced access rules

Cleaner Operations

- No need for duplicate records
- No workarounds or hidden communication

Better Compliance & Auditability

- Controlled visibility of sensitive data
- Reduced risk of accidental exposure

User Experience Impact

From a user perspective:

- They only see conversations relevant to them
- Sensitive threads are invisible if not authorized
- No additional steps or manual classification required
- The system enforces rules quietly - without changing how users work.

Business Impact

Secure Inbox delivers:

- Reduced compliance and data exposure risk
 - Clear ownership of communication
 - Improved trust in Salesforce as a system of record
 - Better collaboration across teams without compromising security
-

What Secure Inbox Does NOT Do

It does **not**:

- Replace Salesforce Email-to-Case
- Introduce a new email client
- Change how users send or receive emails
- Require retraining of teams

It extends Salesforce's email model where it is weakest.

Typical Rollout Approach

Most organizations adopt Secure Inbox in phases:

1. Enable thread-level visibility
2. Apply to sensitive or high-risk teams
3. Validate behavior and impact
4. Expand across the organization
5. Refine access rules over time

Low risk. High impact.

Key Takeaway

Salesforce controls access at the record level.

Secure Inbox adds control at the conversation level.

This closes a critical gap in how email is managed inside enterprise Service Cloud environments.