InboxTidy.ai

Security and Architecture Whitepaper

Title:	Security and Architecture Whitepaper
Document Version:	1.0
Document Type:	Whitepaper
Company:	InboxTidy Ltd.
Document Number	IT-WP-001

1. Revision History

Revision	Change Description	Date (DD-MMM-YYYY)
1.0	Initial Draft	16-04-2026

2. Sign-Off

Version	Signed off by	Position	Date (DD-MMM-YYYY)
1.0	Steven Brown	CEO and Chief Architect	16-04-2026

3. Executive Summary

InboxTidy is an AI-assisted email categorisation and drafting solution designed with a tenant-contained architecture**.**

The core security principle is simple:

All customer data always remains within the customer's Microsoft 365 tenant.

InboxTidy does not extract, store, or process email content outside of the customer environment. This eliminates traditional risks associated with external AI services, data transfer, and third-party processing.

4. Design Principles

InboxTidy is built on the following foundational principles:

2.1 Tenant Containment

- No email data leaves the Microsoft 365 tenant
- Processing occurs entirely within customer-controlled services

2.2 Zero External Data Dependency

- No reliance on external AI APIs
- No transmission of email content to third-party platforms

2.3 Least Privilege Access

- Permissions scoped strictly to required mailbox operations
- No broad or unnecessary data access

2.4 Microsoft-Native Security Alignment

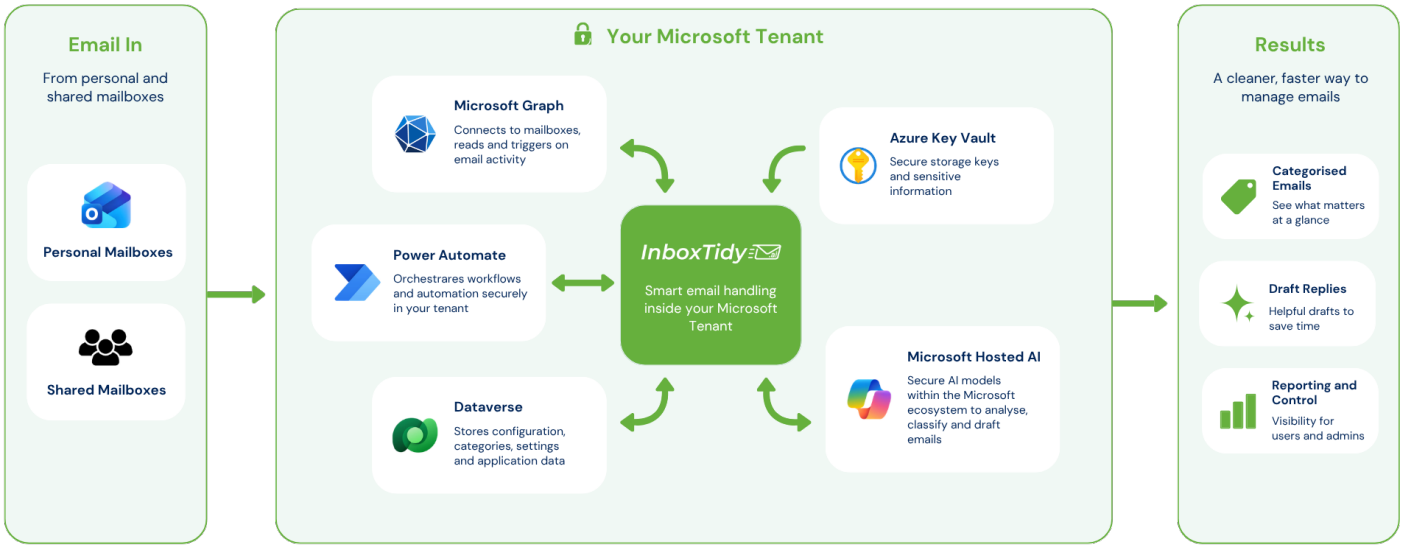
- Leverages existing Microsoft 365 identity, compliance, and security controls

5. High-Level Architecture

5.1. Logical Overview

InboxTidy operates as an application deployed within the customer's Microsoft 365 tenant, interacting with:

- Exchange Online (email data source).
- Microsoft Power Platform (Automation, App & Database).
- Microsoft Graph API (secure data access layer).
- Azure services such as Key Vault to keep secrets secure.



5.2. Data Flow Summary

- InboxTidy reads email metadata and content via Microsoft Graph
- Microsoft hosted AI (GPT) processes the email content within the tenant boundary
- Output actions are written back:
  - Categories applied
  - Draft responses created
  - Metadata updated

Key Point:
At no stage is email content transmitted outside the tenant, or readable to users or administrators.

6. Identity and Access Management

InboxTidy relies entirely on Microsoft Entra ID (Azure AD):

- OAuth 2.0 / OpenID Connect authentication
- Application registration within the customer tenant
- Admin consent model for permissions

6.1. Permission Model

Typical permissions include:

- Mail.Read
- Mail.ReadWrite
- Mail.Send (for draft handling only, where enabled)

All permissions are:

- Explicitly consented by the customer
- Visible and auditable within Microsoft 365
- The Enterprise App (Graph) is only allowed to access mailboxes that belong to a specific mail enabled security group, via an Exchange Online application access policy.
- All Microsoft Graph webhook notifications are validated using a shared clientState value to confirm they relate to a known subscription before they are processed.

7. Data Security

7.1. Data at Rest

- Managed entirely by Microsoft 365
- Protected via Microsoft encryption standards

7.2. Data in Transit

- Secured via HTTPS / TLS 1.2+
- All communication remains within Microsoft-controlled endpoints

7.3. Data in Processing

- Processing occurs within the tenant environment
- No external compute environments handle email content
- All Power Platform automations use secure inputs and outputs, ensuring email content is masked during processing and not exposed afterwards.

8. AI Processing Model

InboxTidy's AI capabilities are designed to operate:

- Within the tenant boundary
- Without sending data to external AI providers

8.1. Key Characteristics

- No training on customer data outside the tenant
- No shared models across customers using their data
- Deterministic and auditable processing flows where possible

9. Logging and Telemetry

InboxTidy generates minimal operational telemetry.

9.1. Included

- Performance metrics
- Error states (non-content)
- System health indicators

9.2. Explicitly Excluded

- Email body content
- Attachments
- Sensitive personal data

Telemetry is designed to:

- Support reliability
- Avoid data privacy risks

10. Network and Boundary Security

InboxTidy does not introduce new external data pathways.

Key Controls

- All data access via Microsoft Graph API
- No inbound public endpoints required for email processing
- No data egress of email content outside Microsoft 365

11. Customer Security Responsibilities

InboxTidy inherits the customer's Microsoft security posture.

Customers are responsible for:

- Identity governance (MFA, Conditional Access)
- Mailbox permissions and access policies
- Data Loss Prevention (DLP) configuration
- Retention and compliance policies
- Monitoring and alerting within Microsoft 365

12. Compliance Alignment

InboxTidy is designed to support compliance with:

- UK GDPR
- EU GDPR

Key Compliance Advantages

- No cross-border data transfer introduced
- No subprocessors handling email content
- Clear data controllership (remains with customer)
- Simplified DPIA outcomes due to contained architecture

13. Threat Model Overview

13.1. Reduced Risk Areas

- Data exfiltration (no external transfer)
- Third-party exposure
- AI model leakage

13.2. Primary Risk Domains

- Misconfigured permissions
- Compromised user accounts
- Microsoft tenant-level security weaknesses

14. Deployment Model

InboxTidy is deployed:

- As a registered managed application within the customer's tenant
- With controlled permissions via admin consent
- Without requiring infrastructure outside Microsoft 365

15. Business Continuity and Resilience

InboxTidy:

- Relies on Microsoft 365 availability and resilience
- Does not introduce separate critical infrastructure dependencies

Failure scenarios:

- InboxTidy unavailable → no impact on email availability
- Core email services remain unaffected

16. Limitations and Transparency

InboxTidy does not:

- Provide independent data storage
- Act as a security monitoring tool
- Replace Microsoft-native compliance tooling

It is a productivity enhancement layer, not a control system.

17. Conclusion

InboxTidy's architecture is intentionally simple:

- **No data leaves the tenant**
- **No external AI dependency**
- **No additional data risk introduced**

This positions InboxTidy as a **low-risk, high-value AI solution** suitable for:

- Regulated industries
- Security-conscious enterprises
- Organisations with strict data governance requirements