



AnySecura

Email Control

Comprehensive email security and compliance solution

Monitor · Control · Secure · Audit · Manage





Module Overview

AnySecura Email Control integrates four core capabilities, providing enterprises with comprehensive email security, monitoring, and compliance management to prevent data leakage and ensure regulatory adherence.



Email Logs

Record complete details of all emails including senders, recipients, content, and attachments across various email platforms and protocols.



Email Outbound Control

Restrict email transmission based on sender, recipient, content, attachments, and size to prevent unauthorized data leakage.



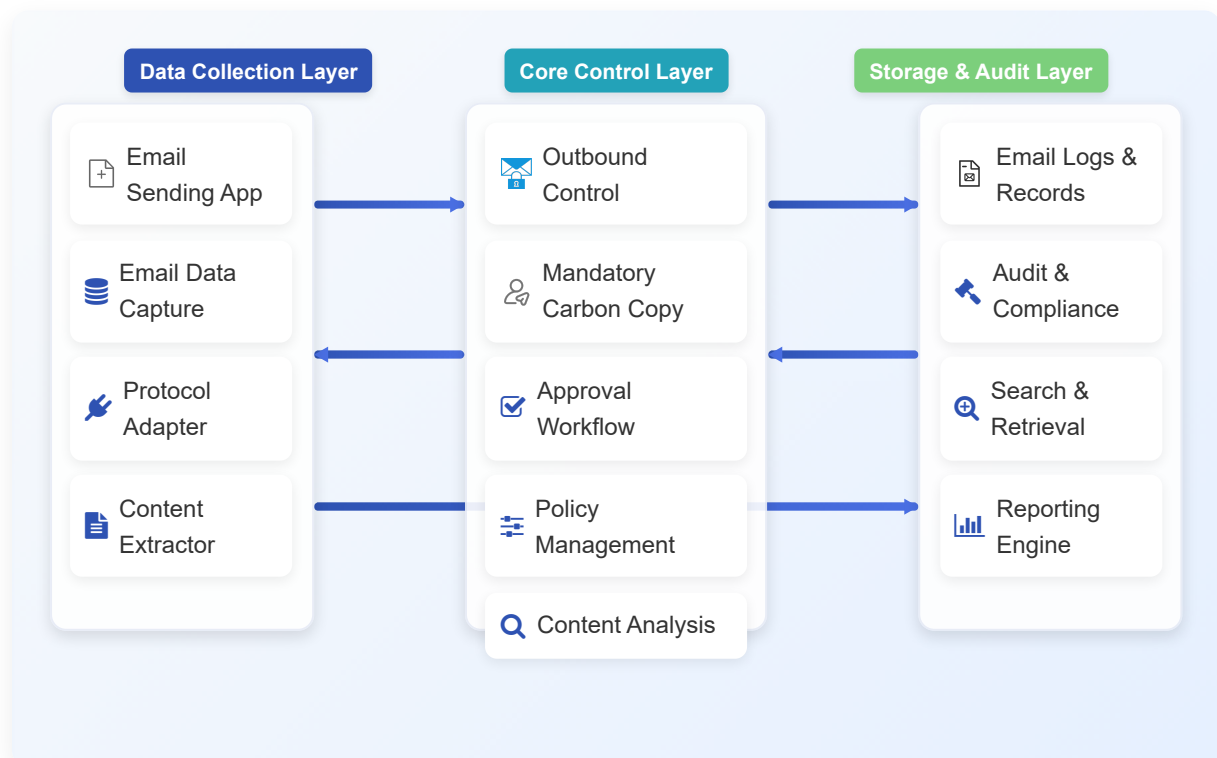
Mandatory Carbon Copy

Enforce copy requirements for external emails to ensure oversight and compliance with company policies.



Email Sending Application

Manage temporary permissions for email sending through approval workflows and self-filing processes.

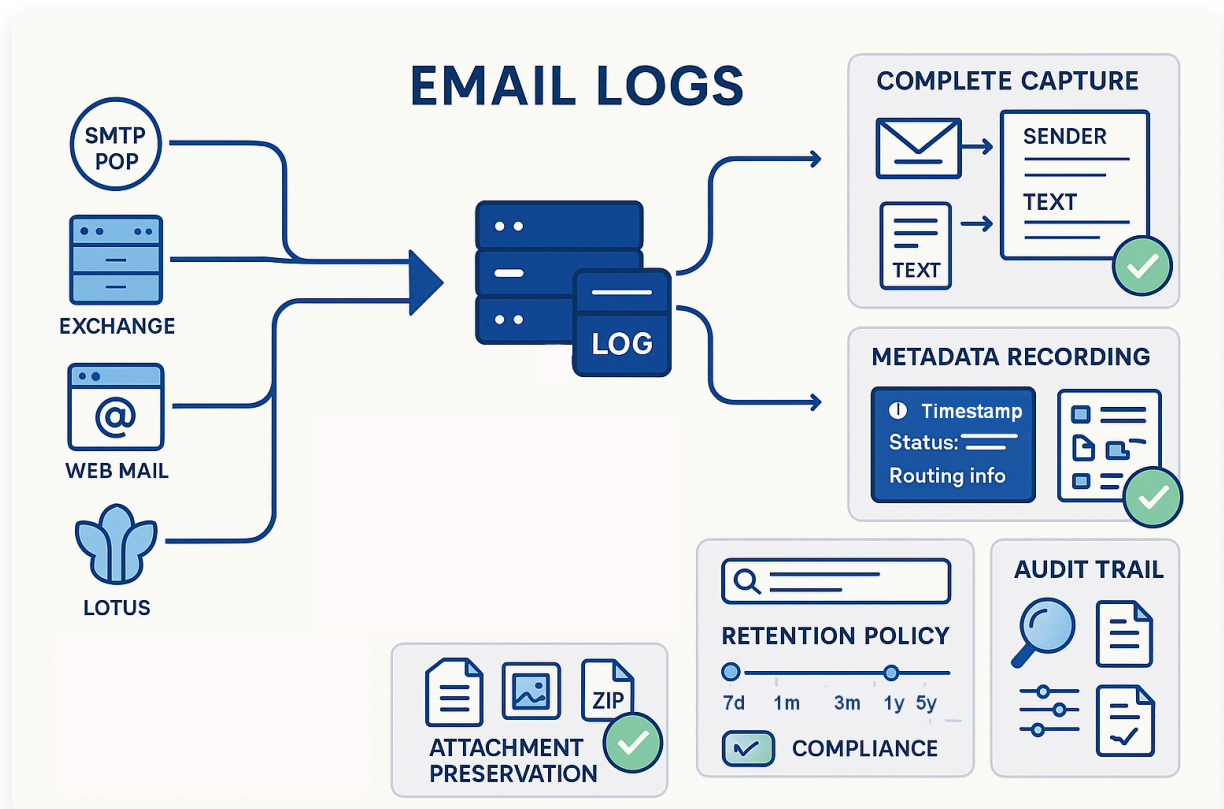




Email Logs

Comprehensive recording and archiving of all email communications across various platforms to ensure compliance, enable audits, and support investigations.

- ✓ **Complete Capture:** Record recipients, senders, body text, and full attachments for emails sent through standard protocols and Exchange.
- ✓ **Multi-platform Support:** Capture web emails and Lotus emails with complete metadata and content.
- ✓ **Detailed Metadata:** Record timestamps, delivery status, and routing information for comprehensive audit trails.
- ✓ **Attachment Preservation:** Store complete copies of all email attachments in their original format.
- ✓ **Searchable Archive:** Indexed storage enabling quick retrieval by sender, recipient, date, subject, or content.
- ✓ **Retention Policies:** Configurable storage periods to meet regulatory requirements and business needs.

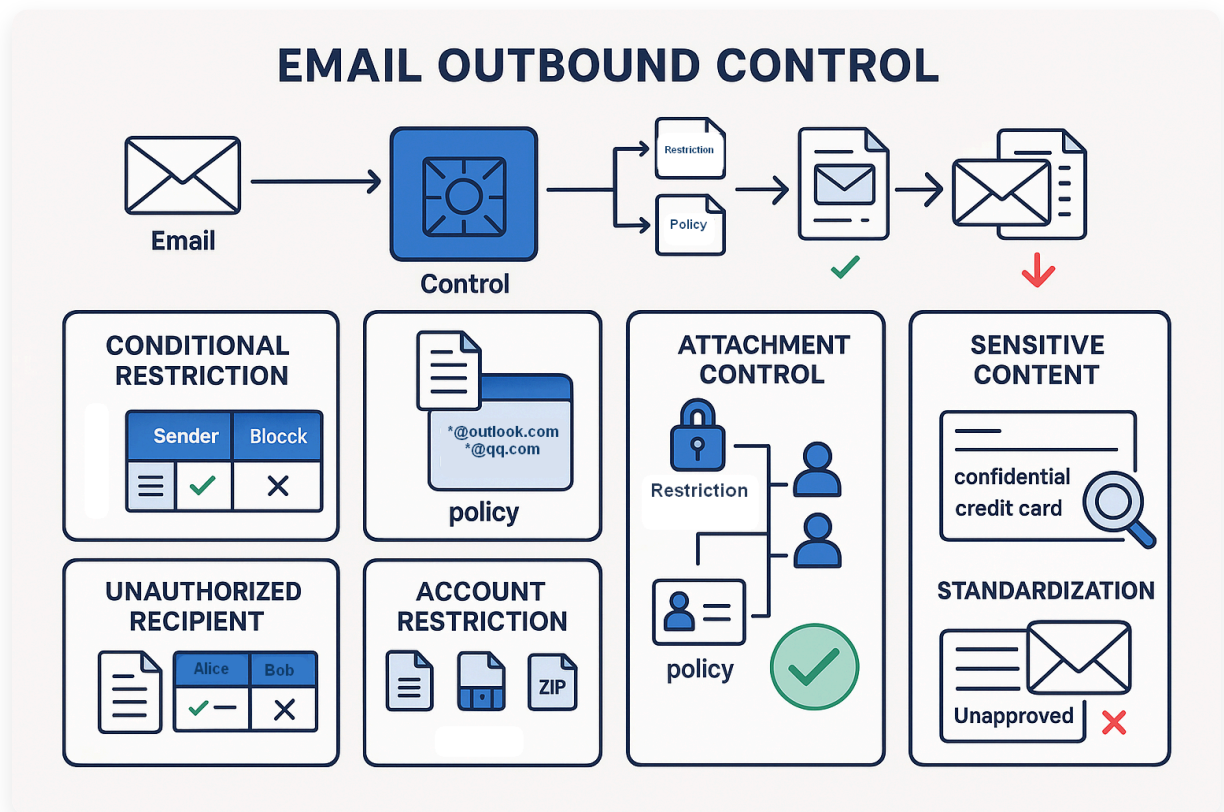




Email Outbound Control

Granular control over outgoing emails to prevent unauthorized data leakage while allowing legitimate business communications.

- 📌 **Conditional Restrictions:** Control email-sending based on sender, recipient, subject, attachments, and size.
- 🚫 **Unauthorized Recipient Blocking:** Prevent sending emails to specific individuals or domains not approved by policy.
- 📎 **Attachment Controls:** Block attachments with specific names, extensions, or those exceeding size limits.
- 🔑 **Account Restrictions:** Limit which accounts can send external emails based on role or department.
- 🔍 **Sensitive Content Detection:** Identify emails containing predefined sensitive keywords in subject, body, or attachments.
- 🏢 **Standardization:** Restrict email sending to only approved enterprise email accounts.





Mandatory Carbon Copy

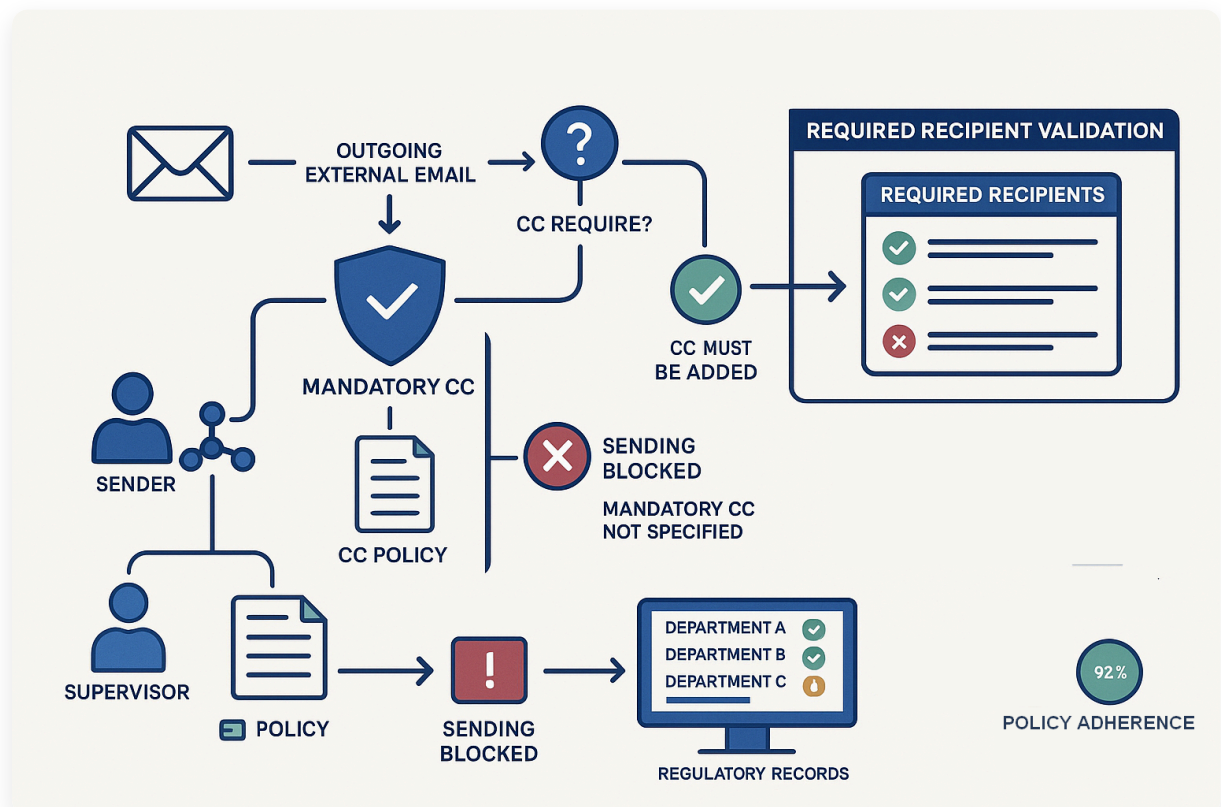
Enforce oversight of external communications through required carbon copies to designated recipients, ensuring transparency and compliance.

CC Enforcement

- ✅ **Required Recipients:** Emails can only be sent externally if a designated recipient is copied.
- 👤 **Organizational Hierarchy:** Configure CC requirements based on department, role, or email content.
- 👤 **Supervisor Oversight:** Ensure external emails are copied to department supervisors for review.
- ⚠️ **Enforcement Mechanism:** Block emails that don't meet the mandatory CC requirements.

Compliance & Benefits

- ✅ **Audit Trail:** Maintain evidence of oversight for compliance and regulatory requirements.
- 🛡️ **Data Leak Prevention:** Additional layer of review before information leaves the organization.
- ⚖️ **Policy Adherence:** Ensure consistent application of communication policies across the organization.
- 🕒 **Historical Review:** Enable retrospective analysis of communications for investigations or audits.













Email Sending Application

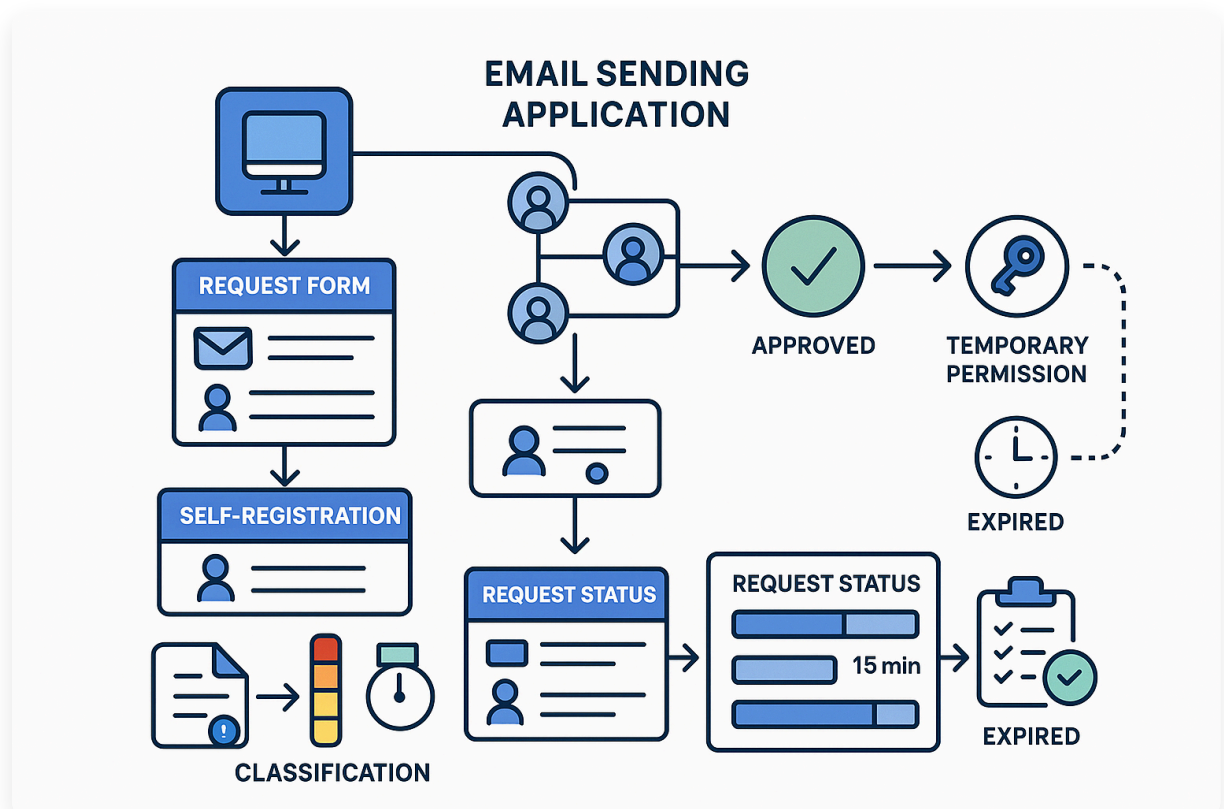
Flexible workflows for requesting temporary permission to send emails when prohibited by policy, balancing security with business needs.

Request & Approval Process

-  **Formal Application:** Users can submit requests for temporary permission to send restricted emails.
-  **Multi-level Approval:** Configurable workflows with role-based approvers based on email sensitivity.
-  **Time-bound Permissions:** Grant temporary access for specific periods with automatic expiration.
-  **User-friendly Interface:** Simple portal for submitting and tracking application status.

Alternative Options & Tracking

-  **Self-filing Option:** Enable email sending through self-registration for lower-risk scenarios.
-  **Purpose Documentation:** Require business justification for sending restricted emails.
-  **Classification-based Processes:** Different approval workflows based on content sensitivity.
-  **Activity Tracking:** Monitor all emails sent under temporary permissions with detailed logs.



Application Scenarios



1. Financial Services Compliance

The Challenge

A financial institution needs to comply with regulations requiring oversight of all external communications. They struggle to prevent unauthorized information disclosure while allowing necessary business correspondence.

The Solution with AnySecura

Implementing **Mandatory Carbon Copy** and **Email Outbound Control**:

1. Configure rules requiring all external emails to be copied to compliance officers
2. Set up content scanning for sensitive financial data and client information
3. Implement restrictions on sending attachments containing financial records
4. Create audit trails for all external communications

Results Achieved

- ✓ 100% compliance with financial regulations
- ✓ 95% reduction in unauthorized information disclosure
- ✓ 60% faster audit preparation and reporting



2. Intellectual Property Protection

The Challenge

A manufacturing company with proprietary designs and formulas needs to prevent intellectual property leakage through email while maintaining operational efficiency.

The Solution with AnySecura

Deploying **Email Logs** and **Email Sending Application** workflows:

1. Implement content detection for intellectual property keywords and patterns
2. Restrict external sending of design files and technical documents by default
3. Create approval workflows for legitimate external sharing needs
4. Maintain comprehensive logs of all intellectual property-related communications

Results Achieved

- ✓ Eliminated unauthorized sharing of proprietary information
- ✓ 80% reduction in IP-related security incidents
- ✓ Streamlined legitimate information sharing with 30% faster approvals

Core Values & Benefits



Data Loss Prevention

Prevent unauthorized disclosure of sensitive information through email with comprehensive control mechanisms and content monitoring.



Regulatory Compliance

Meet industry regulations and internal policies with complete audit trails, mandatory oversight, and configurable controls.



Balanced Security

Maintain security without hindering business operations through flexible workflows and temporary access provisions.



Complete Visibility

Full visibility into all email communications with searchable archives and comprehensive monitoring capabilities.

Ready to Secure Your Data from Email Leakage?

 [Learn More About Solutions](#)

 [Contact Our Experts](#)



www.anysecura.com



support@anysecura.com

© 2025 AnySecura SOFTWARE PTE. LTD. All rights reserved. Enterprise-grade security solutions.