

fortyx security.

PRIVILEGED & CONFIDENTIAL

The next frontier in email security

80% of cyber attacks and data breaches stem from a lapse in email security. With Gen AI fuelling more targeted and more frequent attacks, it's time to reimagine email security.



PROBLEM

Email still remains the biggest open door

- Email remains the #1 attack vector, accounting for 80% of attacks [1]
- 376b emails sent out daily in 2024 (4.3% YoY growth) [2]
- Gen AI-powered attacks are increasing exponentially [3]

Existing solutions are falling short.



Phishing or social engineering attacks can paralyse the organisation, costing millions (\$) in financial and reputational damage

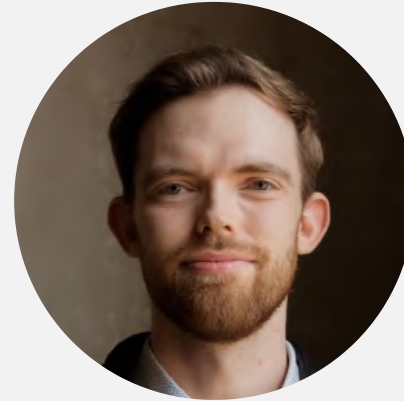


Misdirected emails can result in a data breach, risking a hefty fine from the Information Commissioner's Office (ICO)

OUR SENIOR MANAGEMENT

We get your cyber needs

We are IT and cybersecurity practitioners, and combine 80+ years of experience across world class organisations.



Tom Gilgan
Co-Founder + CTO



Parvez Alam Kazi
Co-Founder + CEO



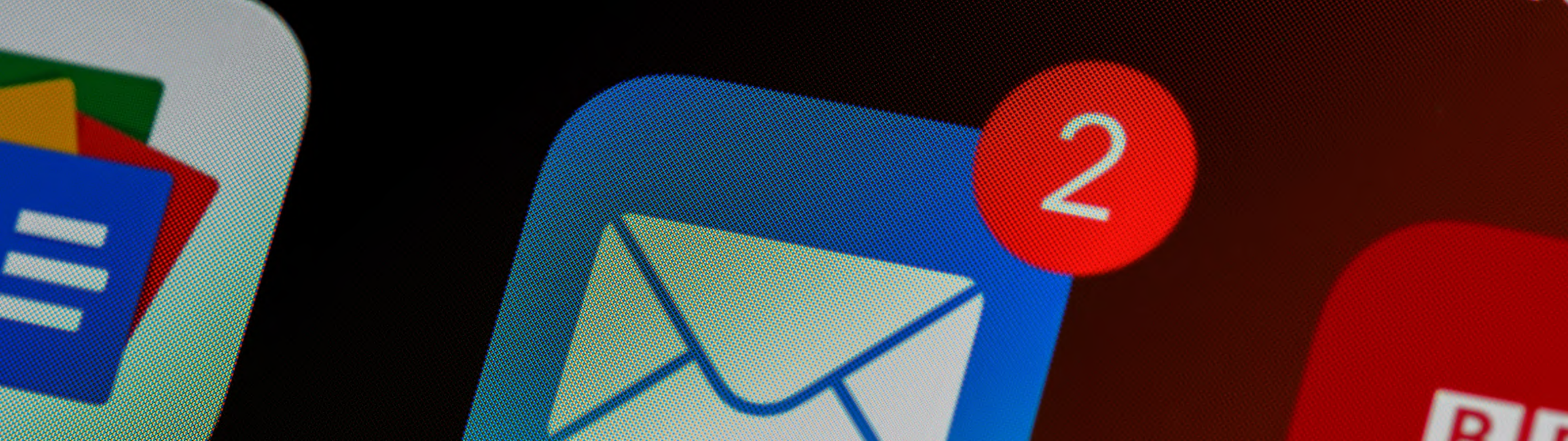
Nigel Moulton
Commercial Advisor



Adrien Pujol
Technical Advisor



Chris Hodson
Product Advisor



MISSION

We started this company to equip the human layer against cyber risks

Emails are the frontline. With the transformational power of large language models and agentic AI workflows, we are building the next generation of email security. One that safeguards organisations, without extra burden on users.

CURRENT GAPS

Why current solutions leave you exposed?



(1) API based approaches

These operate at your mailbox level, and leaves the door open.
Prioritises convenience over security



(2) Outbound protection neglected

Your outbound email etiquette matters, but other solutions over index on inbound email threats



(3) Static rule based detection

Ruled based detection doesn't adapt but attackers do, requiring manual reactive updates to these rules



(4) Difficult to get started

Demos, commercials, expensive professional services, manual setup – too many hurdles to get started and then stay on top

(1) Outbound & Inbound Protection

We provide holistic protection across your email flow

(2) Secure Email Gateway Based

More secure compared to API based approaches

(3) AI Native

LLMs for email analysis and agentic AI workflows for 5x faster email sec ops

(4) Adaptive natural language policies

Define policies using natural language that adapt over time

(5) Embedded Security Awareness

Not training that people hate, but set context with every flagged email

(6) Self Serve

AI workflows to make onboarding and operations seamless

OUR APPROACH

We are reimagining email security for the AI era

Sign up, set and forget. AI takes care of the rest like a team of security experts.

For the human touch, when AI isn't enough, our trusted partners can help with detailed investigations and security reviews.


USER EXPERIENCE

Embedded security awareness


Every email flagged to the user or the SOC team comes with visual highlights and natural language context to help guide the user in real time.

Quarterly Financial Report – Confidential

15/04/2023, 09:32:00



 This email is addressed to 1 potentially incorrect recipient. Please verify each recipient carefully, especially External User.

Wrong Recipient **High Risk**

From: John Smith <john.smith@company.com>
To: Finance Team <finance@company.com>;
External User <wrong.person@competitor.com> 

Hello Team,
Attached is the quarterly financial report with detailed revenue projections for Q3. Please review and provide your feedback before our board meeting next week.
Key highlights:
Revenue is up 15% compared to last quarter
New product line is performing above expectations
Operating costs have been reduced by 7%
The **forecast suggests we'll exceed our annual targets by approximately 8.5%** if current trends continue.
Let me know if you have any questions or concerns about the data.
Best regards,
John

Attachments:

 Q3_Financial_Report_FY2023.xlsx (2.4 MB)  Executive_Summary_Q3.docx (1.2 MB)

Create policies using natural language.
Xander then scans for policy violations and changing communication patterns, and keep the policies up to date.

fortyx

- Security Operations
 - Dashboard
 - Outbound Email
 - Audit
- Administration
 - Users
 - Policies
- Theme

Policies > HR Data Handling

HR Data Handling

Human Resources department policy

Policy Description

Guidelines for handling sensitive salary and personnel information during recruitment

Policy Ruleset

- ✓ Share salary data with candidates during hiring process**

If <ul style="list-style-type: none">User is a member of HR departmentandCandidate has passed initial screeningandJob offer is in preparation phase	Then <ul style="list-style-type: none">Access to salary informationandCompensation informationandBenefits information
--	--
- ✗ Share employee salary information with external parties**

If <ul style="list-style-type: none">External party requests employee dataandNo written consent from employeeandNo legal requirement for disclosure	Then <ul style="list-style-type: none">Deny access to salary informationandLog access attemptsandNotify HR management
--	--
- ✗ Discuss compensation details outside recruitment context**

Xander HR Data Handling

I can help you modify and improve this policy on HR Data Handling. Tell me what changes you'd like to make to the rules and conditions.

Add a new rule HR can only share salary information with candidate during offer stage

I understand you want to create a new rule: "Add a new rule HR can only share salary information with candidate during offer stage". Would you like me to add this to the policy ruleset?

I've created the new rule: "Add a new rule HR can only share salary information with candidate during offer stage". It has been added to the policy ruleset.

Type your message...

John Doe
Security Analyst

fortyx ☰ **Audit & Event Log**
Track and analyze security decisions and system events 📄 Export Data

Security Operations
Dashboard
Outbound Email
Audit
Administration
Users
Policies
Theme

Event Log Analytics

🔍 Search events... 🏠 All Time

Timestamp	Event Type	Details	User/System	Status
07/05/2025, 09:23:45	Email Flagged	alice.smith@example.com To: bob.jones@example.com Risk: Wrong Recipient (high)	System	Pending
07/05/2025, 10:15:22	Email Approved	john.doe@example.com To: marketing-team@example.com Risk: Sensitive Content (medium)		
07/05/2025, 11:05:17	Email Rejected	sarah.williams@example.com To: external-partner@vendor.com, ceo@example.com Risk: Sensitive Content (high)		
06/05/2025, 14:22:38	Email Flagged	dev-team@example.com To: client@customer.com Risk: Wrong Attachment (high)		
06/05/2025, 15:47:01	Email Approved	finance@example.com To: vendors@supplier.com Risk: Wrong Recipient (low)		
06/05/2025, 16:35:29	Policy Update	HR Data Handling Added rule for salary information sharing		
05/05/2025, 09:12:55	Rule Created	Salary Information Sharing Policy: HR_Data_Handling		

John Doe
Security Analyst

Xander - AI Assistant

To help you with data analysis, email investigations and policy configurations

fortyx ☰ **Analytics**
Real-time insights into email security and potential risks

Security Operations
Dashboard
Outbound Email
Audit
Administration
Users
Policies
Theme

Total Alerts 🛡️

37 +6 from yesterday

Misdirected Recipients ⚠️

17 +2 from yesterday

Sensitive Conte

11

Pending Actions

Task	Status	Priority	Assi
Review suspicious login attempts	Needs Review	High	Sec
Update DLP policies	In Progress	Medium	Polic
Investigate data exfiltration alert	Pending	High	Inc
Review compliance reports	Completed	Low	Con

John Doe
Security Analyst

Xander ✕

Hello! I'm Xander, your AI security operations assistant. I can help you analyze emails, assess security risks, and provide insights about your security posture.

Try asking me:

- Can you analyze this flagged email for potential threats?
- What are the current security trends in my organization?
- Help me understand this policy violation
- Show me a summary of today's security incidents

Type your message... 📤

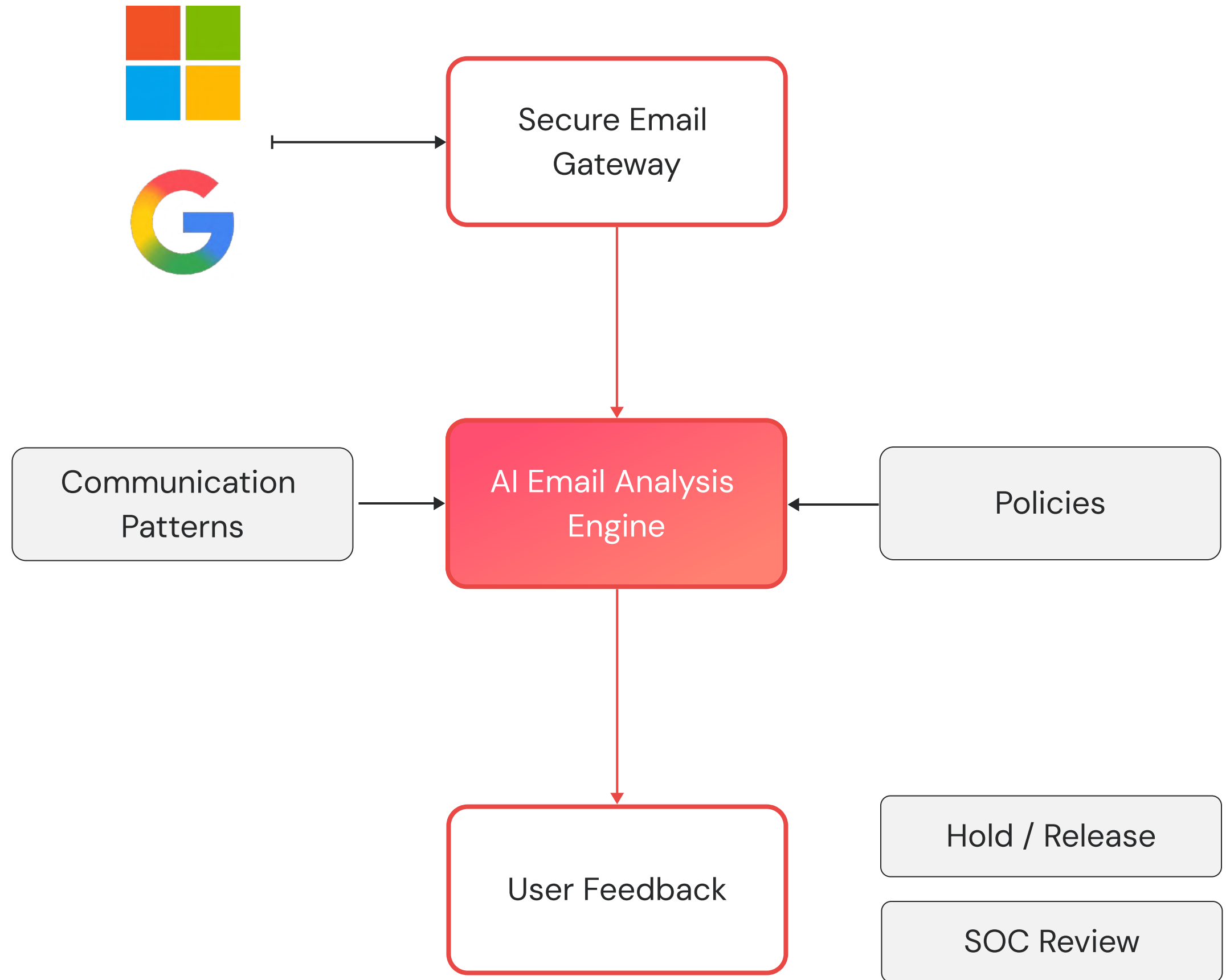
Detailed audit logs

All AI based decisions, policy updates are captured for audit and reporting purposes

HOW IT WORKS

AI at the core

- We route your email flow through our secure email gateway.
- Emails are analysed by our AI engine, with context about your organisation's communication patterns and policies.
- The user receives context with every flagged email. If the AI is unsure, it goes to your SOC team for review.





This helps prevent the near misses recently in terms ICO-reportable offenses

CHIEF INFORMATION OFFICER

GLOBAL CYBERSECURITY COMPANY (300 EMPLOYEES)

//

Microsoft E5 only flags the obvious, mailing externally, missing an attachment. I like that Fortyx spots real-world scenarios like sending sensitive data with the wrong classification and stops it before it leaves the building.

CHIEF TECHNOLOGY OFFICER

FRAUD INVESTIGATION SOFTWARE COMPANY (100 EMPLOYEES)

GET IN TOUCH

We are running limited pilot slots for our early customers

For a demo and to book your pilot slot, get in touch soon.

[Book a meeting](#)

Or email us at contact@fortyx.co (we respond within 24 hours)

fortyx security.

PRIVILEGED & CONFIDENTIAL

Take your email security
to the next level