AN AI SECURITY PRODUCT BY Baseel

CUSTOMER CASE STUDY · NOVEMBER 2026

NON-PROFIT · GRANT-MAKING

Maulee Foundation

CUSTOMER

Maulee
Uniting Hearts, Transforming Lives

Cyprawall × Maulee

Enabling confident AI use across a grant-making foundation, without putting grant, partner or donor information at risk.

SECTOR	LOCATION	DEPLOYMENT	WEBSITE
Grant-making charity	London, England & Wales	Browser extension + SaaS control plane	maulee.org

> Cyprawall gave us visibility into which AI tools our teams were actually using, and stopped sensitive records from leaving without slowing anyone down.

Mrinmayee Nistane
Chief Operating Officer, Maulee Foundation

LIVE INSPECTION · ILLUSTRATIVE

PROGRAMME OFFICER → CHATGPT

```
Summarise this grant application from [NAME], contact [EMAIL], bank ref [ACCOUNT], and list any safeguarding concerns.
```

PII entities	3 redacted
Prompt injection	None found
Destination	Approved

REDACT Forwarded without personal data · decision logged

IN BRIEF

01
The challenge
Staff, trustees and volunteers were turning to AI to summarise applications and draft reports, with no view of which tools were receiving grant, partner and donor information.

02
Our approach
Cyprawall's browser extension and SaaS control plane: discovery of AI tools in use, inline redaction of personal data and prompt-injection checks on submitted documents.

03
The outcome
AI-assisted work continues, sensitive records stay inside approved tools, and trustees get a reviewable audit trail of every decision.

This case study describes how Cyprawall's capabilities align with Maulee Foundation's published grant-making model and governance commitments. It reflects the customer's own account above; quantified security outcomes have not been independently measured and are therefore not claimed.

Case Studies ↗

Maulee
Uniting Hearts, Transforming Lives

AT A GLANCE

Organisation
Registered charity, England & Wales

Sector
Grant-making charity

Location
London, England & Wales

Cyprawall deployment
Browser extension + SaaS control plane

Relationship
Baseel Partners LLP covers Maulee's operational and logistical expenses, as stated on maulee.org

CYPRAWALL MODULES

- Shadow AI discovery
- Inline inspection & redaction
- Prompt-injection detection
- AI-tool risk scoring
- Tamper-evident audit log

DATA PROTECTED

Applicant PII | Bank details | Safeguarding records | Partner accounts | Trustee papers | Donor data

CLIENT CONTACT
Mrinmayee Nistane
Chief Operating Officer
insights@maulee.org

01 Executive overview

Maulee Foundation is a grant-making charity registered in England and Wales. It funds registered charities whose work prevents or relieves poverty, relieves individuals in need, or advances education for disadvantaged people, and every grant follows a formal assessment against published criteria.

As AI assistants become part of everyday work, Maulee's staff, trustees and volunteers increasingly use them to summarise applications, draft correspondence and prepare reports. Cyprawall lets that continue, while making sure the information charities and donors entrust to Maulee stays where it belongs.

02 Operating context

Grant assessment is document-heavy: applications, governance and safeguarding evidence, accounts, impact reports and trustee papers. Much of it is supplied by partner charities in confidence, and some of it contains personal data.

Maulee publicly commits to transparency and rigorous vetting. Pasting that material into an unvetted AI tool would sit awkwardly with both, and with UK GDPR. The organisation needs proportionate controls that fit its operating model without adding infrastructure overhead.

03 AI risk & governance priorities

01
Know which AI tools are in use
See the assistants, plug-ins and connected apps staff and volunteers actually use, including personal accounts on work devices.

02
Keep applicant data private
Stop names, contact details, bank details and safeguarding information in grant files from reaching public AI services.

03
Protect partner confidence
Treat governance documents and accounts shared by charities during due diligence as confidential by default.

04
Resist manipulated documents
Detect hidden instructions in submitted documents before an AI summary is relied on in an assessment.

05
Stay lightweight
Deploy without new infrastructure, agents on every server or a full-time administrator.

06
Evidence for trustees
Give management and trustees a clear, reviewable record of how AI is governed.

04 Cyprawall solution alignment

Cyprawall sits between users and AI services. For Maulee, the browser extension and SaaS control plane provide coverage without network changes, and policies are written in plain terms: what is allowed, what is redacted and what is blocked.

PRIORITY	CYPRAWALL CAPABILITY	CONTRIBUTION TO MAULEE
Shadow AI visibility	DISCOVER OAuth-grant discovery across Google Workspace or Microsoft Entra ID; usage seen through the browser extension.	A current inventory of AI tools in use and who connected them, instead of an annual questionnaire.
Applicant & donor data	REDACT Inline inspection of prompts to ChatGPT, Gemini, Claude and others; PII redacted before it leaves.	Staff still get a useful summary; personal identifiers never reach the provider.
Partner due diligence	BLOCK Policies for confidential documents and financial records sent to non-approved AI destinations.	Confidential partner material stays inside approved tools only.
Document integrity	Prompt-injection inspection of content pasted or uploaded for summarisation.	Reduces the chance that a manipulated submission skews an AI-assisted assessment.
Tool risk	Risk scoring of discovered AI tools; off-boarding checklists for retired tools.	A simple basis for deciding which tools to approve, restrict or decommission.
Governance	Tamper-evident, hash-chained audit log with export.	Reviewable evidence for trustee meetings, policy reviews and any data-protection enquiry.

05 Illustrative scenarios

A Summarising a grant application

A programme officer pastes an application into an AI assistant. Cyprawall REDACT removes applicant names, addresses and bank details; the assistant still returns a usable summary.

B Trustee papers in a free tool

A volunteer tries to upload board papers to an unapproved AI site from a personal account. Cyprawall BLOCK stops the upload and explains the approved alternative.

C Hidden instructions in a submission

An uploaded PDF contains concealed text telling the AI to rate the application highly. Prompt-injection inspection flags it for the assessor before the summary is used.

D A new AI plug-in appears

A staff member connects an AI note-taker to the shared mailbox. DISCOVER OAuth discovery surfaces the grant, its scopes and a risk score for review.

E Everyday drafting continues

A thank-you letter to a funded charity contains no sensitive data. Cyprawall ALLOW lets it through instantly and records the decision, so useful AI work is never slowed.

06 How Cyprawall fits Maulee's estate

1 **Discover**
Connect Google Workspace or Entra ID to inventory AI apps and grants.

2 **Classify**
Mark grant, partner, donor and safeguarding data as sensitive.

3 **Protect**
Roll out the browser extension to staff and volunteer devices.

4 **Review**
Tune policies with the team so legitimate drafting is not blocked.

5 **Report**
Share audit summaries with management and trustees.

07 Expected value

- Confidence that applicant, donor and partner information is not used to train or prompt public AI models.
- Clear visibility of the AI tools in use, including those adopted informally by volunteers.
- Productive AI use continues: most requests are allowed or redacted rather than blocked.
- A simple, evidence-based way to show trustees and regulators that AI use is governed.
- Lower risk of AI-assisted assessments being skewed by manipulated documents.

OUTCOME MEASUREMENT

Benefits should be confirmed against an agreed baseline.

Useful measures include the number of AI tools discovered and reviewed, the share of AI interactions inspected, redaction and block events by data type, prompt-injection detections, and completion of periodic policy reviews by management.

08 Implementation considerations

01
Identify where grant, donor, partner and safeguarding data lives and who may use it with AI.

02
Agree an approved list of AI tools and the policies for each data category.

03
Deploy the browser extension to staff and volunteer devices; connect identity for discovery.

04
Define who reviews blocked requests and approves exceptions.

05
Keep reporting proportionate: decision metadata, not raw sensitive content.

09 About Baseel & Cyprawall

Cypra.ai is the AI brand of Baseel Partners LLP, a global IT and cybersecurity services group founded in 2015, serving clients across the globe. The figures shown are company-published corporate profile figures, not Cyprawall-specific outcomes.

Cyprawall is an AI firewall and governance platform. It discovers AI tools in use, inspects prompts and responses inline, applies ALLOW, REDACT or BLOCK policies, risk-scores AI tools and keeps a tamper-evident audit log. It is available as a multi-tenant SaaS control plane or self-hosted.

100+
countries served

800+
clients

2,000+
projects

See how other teams govern AI with Cyprawall

Read more customer case studies, or book a walkthrough tailored to your environment.

CASE STUDIES

BOOK A DEMO