AN AI SECURITY PRODUCT BY Baseel

CUSTOMER CASE STUDY · NOVEMBER 2026

TECHNOLOGY · CYBERSECURITY SERVICES

# Deeshaa Limited

CUSTOMER

Cyprawall × Deeshaa

Governing AI across a global technology and cybersecurity services business where every prompt can carry client data.

| SECTOR | HEADQUARTERS | DEPLOYMENT | WEBSITE |
|---|---|---|---|
| IT, cybersecurity & technology consulting | Gibraltar; clients in 50+ countries | Gateway, desktop agent & API gateway | deeshaa.biz |

> “Redaction happens inline and every decision lands in the audit trail — our compliance reviews went from weeks of data pulls to a single export.”
>
> **Seema Shintre**
> Managing Director, Deeshaa Limited

LIVE INSPECTION · ILLUSTRATIVE

DEVOPS CONSULTANT → AI CODING ASSISTANT

```
Why does this deploy step fail?
AWS_SECRET_ACCESS_KEY=wJalr…  aws s3
sync ./build s3://[CLIENT-BUCKET]
```

| | |
|---|---|
| Secrets | **1 cloud key** |
| Client identifiers | **1 redacted** |
| Destination | **Approved** |

BLOCK Stopped before leaving the network · user told why

## IN BRIEF

01

### The challenge

Consultants across ten-plus practices use AI every day, and their prompts carry client code, configuration, credentials and data from many environments at once.

02

### Our approach

Cyprawall in three traffic paths: gateway or ICAP for office traffic, desktop agents for consultants on client sites, and the API gateway for ML and agent workloads.

03

### The outcome

Secrets and client data are stopped or redacted inline, and compliance reviews run from a single audit export instead of weeks of data pulls.

This case study describes how Cyprawall’s capabilities align with Deeshaa Limited’s published technology, cybersecurity and managed-services portfolio. It reflects the customer’s own account above; quantified outcomes have not been independently verified and are therefore not claimed.

Case Studies ↗

DEESHAA
The Right Direction

AT A GLANCE

Organisation
**International technology and cybersecurity services**

Sector
**IT, cybersecurity & technology consulting**

Headquarters
**Gibraltar; clients in 50+ countries**

Cyprawall deployment
**Gateway, desktop agent & API gateway**

CYPRAWALL MODULES

- Shadow AI & OAuth discovery
- Secrets & source-code detection
- Inline redaction
- API-gateway inspection
- SIEM export & audit log

DATA PROTECTED

- Client source code
- API keys & secrets
- SAP extracts
- Infrastructure config
- Client PII
- Vulnerability findings

CLIENT CONTACT
**Seema Shintre**
Managing Director
seema@deeshaa.biz

## 01 Executive overview

Deeshaa Limited is an international technology and consulting organisation headquartered in Gibraltar. Its portfolio spans Microsoft Dynamics 365, SAP S/4HANA, DevOps, big data, data-centre services, artificial intelligence and machine learning, and a cybersecurity practice covering Cyber Essentials audits, infrastructure security, IoT security and GDPR.

Consultants across those practices use AI daily: to debug pipelines, interpret ERP configurations, draft audit findings and prototype ML solutions. Cyprawall gives Deeshaa the controls to make that safe for its clients, and the evidence to prove it.

## 02 Operating context

For a technology services provider, prompts are rarely about the business itself. They contain client source code, infrastructure configuration, SAP data extracts, firewall rules, vulnerability findings and credentials, often from several client environments in the same week.

As a firm that advises others on GDPR and Cyber Essentials, Deeshaa must hold itself to the same standard. Its partners (Microsoft, AWS, AT&T, IASME, Tenable, SonicWall) mean a mixed estate, so AI governance has to fit existing gateways rather than replace them.

## 03 AI risk & governance priorities

01
### Client data segregation
Keep one client's code, configuration and data out of AI tools that are not approved for that engagement.

02
### Secrets never leave
Catch API keys, connection strings and credentials in debugging prompts before they reach an AI provider.

03
### Protect source & IP
Govern proprietary and client source code shared with coding assistants.

04
### Secure AI delivery
Inspect traffic from the ML and agent solutions Deeshaa builds, not just staff chat.

05
### Fit the existing stack
Integrate with secure web gateways, SIEM and identity platforms already in place.

06
### Client assurance
Produce audit-ready evidence for client reviews, GDPR and Cyber Essentials work.

## 04 Cyprawall solution alignment

Cyprawall is deployed in the paths Deeshaa's teams already use: the network gateway (or ICAP alongside an existing secure web gateway) for office traffic, desktop agents for consultants on client sites, and the API gateway for AI applications under development.

| PRIORITY | CYPRAWALL CAPABILITY | CONTRIBUTION TO DEESHAA |
|---|---|---|
| **Shadow AI & connected apps** | DISCOVER OAuth-grant discovery across Microsoft Entra ID, GitHub, GitLab and Slack. | A live view of AI tools and coding assistants connected to company and repository accounts. |
| **Credentials & secrets** | BLOCK Inline detection of keys, tokens and connection strings in prompts and uploads. | Secrets are stopped at the point of use, before they reach a third-party model. |
| **Client & personal data** | REDACT PII and client identifiers redacted from prompts to ChatGPT, Gemini, Claude and others. | Consultants get AI help on the problem without exposing the client behind it. |
| **Source code & IP** | Source-code detection with per-destination policy for approved coding assistants. | Code flows only to tools approved for that client or internal project. |
| **AI/ML delivery** | API-gateway inspection of model calls, including prompt-injection detection. | Agent and ML solutions inherit the same guardrails as human users. |
| **Assurance & SOC** | Hash-chained audit log, AI-tool risk scoring and SIEM export. | One export for compliance reviews; incidents flow into existing security operations. |

## 05 Illustrative scenarios

### A Debugging a client pipeline

A DevOps consultant pastes a failing deployment script that includes a cloud access key. Cyprawall BLOCK stops the prompt, names the secret type and suggests resending with it removed.

### B Interpreting an SAP extract

An ERP consultant asks an assistant to explain a data extract containing customer names. Cyprawall REDACT masks the personal fields and the question is answered.

### C A coding assistant on a new repo

A developer authorises an AI coding app on a GitHub organisation. DISCOVER OAuth discovery records the grant and its scopes, and the tool is risk-scored for approval.

### D Injected instructions in retrieved content

An ML agent built by Deeshaa retrieves a web page containing hidden instructions. API-gateway inspection flags the injection before the model acts on it.

### E A client asks for evidence

During a Cyber Essentials or GDPR review, a client asks how AI is controlled. Deeshaa exports the audit trail of policy decisions ALLOW REDACT BLOCK for the period in question.

## 06 How Cyprawall fits Deeshaa's estate

1 **Discover**
Connect Entra ID, GitHub and GitLab to inventory AI apps and grants.

2 **Route**
Gateway or ICAP for office traffic; desktop agents for consultants.

3 **Protect**
Policies for secrets, code, PII and client identifiers by destination.

4 **Extend**
Put the API gateway in front of ML and agent workloads.

5 **Assure**
Stream decisions to SIEM; export evidence for client reviews.

## 07 Expected value

- Clients' code, configuration and data are protected even when consultants use AI to work faster.
- Credentials are stopped at the moment they would leave, not discovered weeks later.
- AI governance fits alongside existing gateways, SIEM and identity platforms.
- The same guardrails cover the AI and ML solutions Deeshaa builds for clients.
- Compliance and client-assurance requests are answered with an export rather than a data-gathering exercise.

OUTCOME MEASUREMENT

### Turn expected value into verified results with an agreed baseline.

Suggested measures: share of AI traffic routed through Cyprawall, AI tools discovered and reviewed, secrets blocked, redaction events by data type, prompt-injection detections, and time taken to answer a client or auditor evidence request.

## 08 Implementation considerations

**01**
Confirm in-scope practices, client engagements and the AI tools approved for each.

**02**
Choose the traffic path per team: gateway/ICAP, desktop agent or API gateway.

**03**
Define policies for secrets, source code, PII and client identifiers, then test with consultants.

**04**
Agree who reviews blocks and approves exceptions, including out-of-hours.

**05**
Integrate audit export with SIEM and set retention to meet client contracts.

## 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