ESPANARO

UK SOVEREIGN / UK OWNED / VETERAN OWNED

PRODUCT DATASHEET

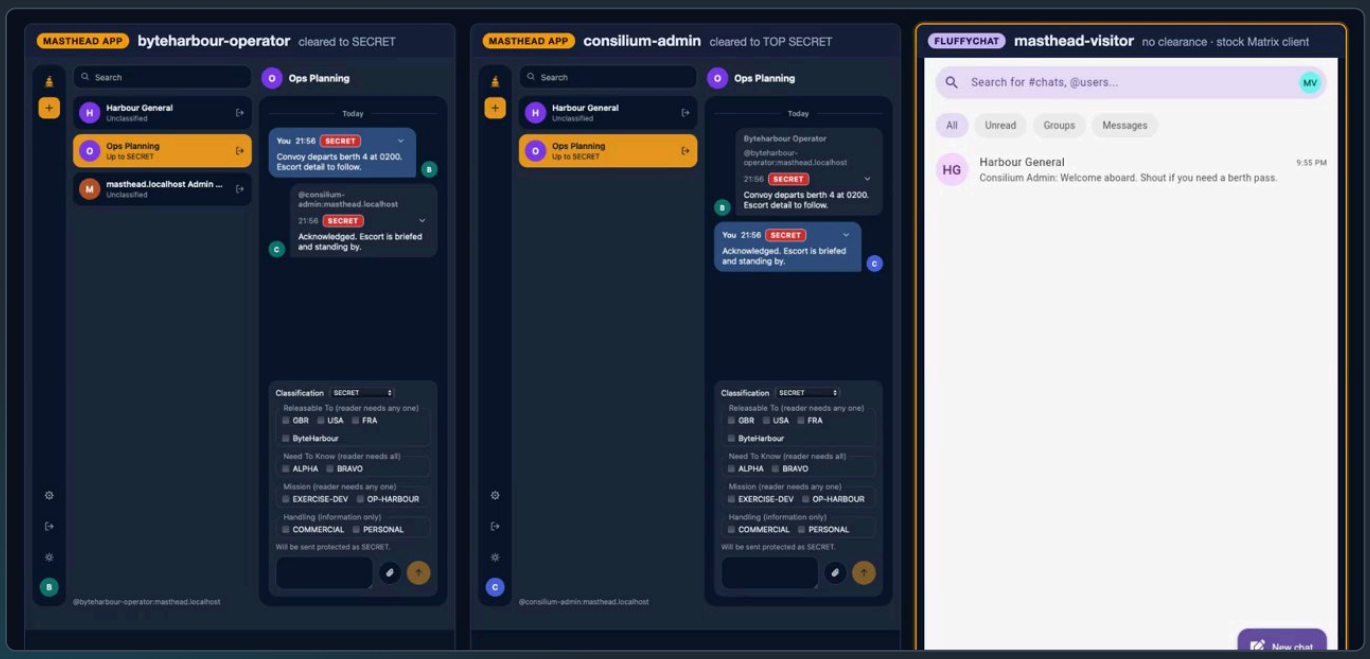
MASTHEAD

Labelled Secure Messaging

Secure messaging where policy decides who sees what.

MastHead is secure messaging built on the open Matrix standard. Users sign in through their organisation's own identity provider, **every room and message carries a sensitivity label, and HarbourGuard decides who may join**. Every decision is recorded, so teams and partners can talk in real time without losing control of who heard what.

Secure messaging | Labelled rooms | Policy-decided access | Built on Matrix | UK-Sovereign



Three users at different clearances, side by side. The visitor, on a standard Matrix client, sees no trace of the SECRET room. Demonstration environment, illustrative data. Interface screenshot, cropped.

Deploy for operations rooms, partner working and sensitive programmes, with the same policy layer as **ByteHarbour** and **Consilium**.

www.ESPANARO.com

WHAT IS MASTHEAD

Data-centric security for conversation

MastHead is Espanaro's secure messaging product. It is built on the open Matrix standard and adds what ordinary chat lacks: rooms and messages that carry their own sensitivity label, membership decided by policy rather than by hand, and a verifiable record of every decision. Users sign in with their organisation's identity provider, and the MastHead server enforces the policy, so a room cannot be opened to someone who is not entitled to it.

THREE PRINCIPLES

Labelled

Every room and message carries a sensitivity label, so the conversation knows how it must be handled.

Policy-decided

HarbourGuard decides who may join from each user's attributes, not from a hand-kept list.

Recorded

Every security decision is written to a verifiable audit trail on the server.

THE CHALLENGE AND THE OUTCOME

THE CHALLENGE

Teams coordinate operations in chat, but most chat tools have no idea how sensitive a conversation is.

Membership is managed by hand, so the wrong person can end up in the wrong room, and there is no reliable record of who could see what.

OPERATIONAL VALUE

MastHead delivers:

- → Rooms and messages carry a label
- → Access decided by policy, not by hand
- → Sign in with your own identity provider
- → Verifiable audit trail
- → Open Matrix standard, open client choice

THE APPROACH

MastHead moves teams from **chat that cannot tell a sensitive room from a social one** to **conversation governed by the same data-centric rules as documents, feeds and tracks**. The label travels with each message, and the server decides who is entitled.

WHERE IT SITS

MastHead uses **HarbourGuard** for access decisions and **ByteHarbour** labelling, so conversation follows the same data-centric security rules as documents and streams. **Consilium** alerts and playbooks can open the right room for the right people.

WHAT MASTHEAD DOES

Labelled rooms, policy-decided membership, every decision recorded

MastHead combines a Matrix server, a key service, the HarbourGuard policy layer and an audit console, with the MastHead desktop app for users.

- Secure messaging on the open Matrix standard
- Sign-in through the organisation's own identity provider
- A sensitivity label on every room and every message
- Room membership decided by HarbourGuard policy
- Access from user attributes such as clearance, role and organisation
- Invitations refused by the server when a user is not entitled
- Messages encrypted on the device, with the label bound and signed
- Keys released by policy
- Post-quantum ready key wrapping, hybrid X25519 and ML-KEM-768
- Audit console and activity view of every security decision
- Unclassified rooms open to standard Matrix clients
- Designed for multi-organisation and coalition teams

CORE CAPABILITIES

Three building blocks for governed conversation

01

Labels

Each room has a highest classification, and each message carries its own label, bound to it and signed.

02

Policy

HarbourGuard decides from each user's attributes who may join a room and who may receive the keys.

03

Audit

Every security decision is recorded on the server and visible in the audit console and activity view.

HOW A DECISION IS MADE

SIGN IN
Through your organisation's identity provider

LABEL
Each room and message carries a label

DECIDE
HarbourGuard checks the user's attributes

RECORD
Every decision is auditable

Open client choice

Unclassified rooms work with standard Matrix clients. A visitor on an unmodified client sees no trace of rooms they are not cleared for.

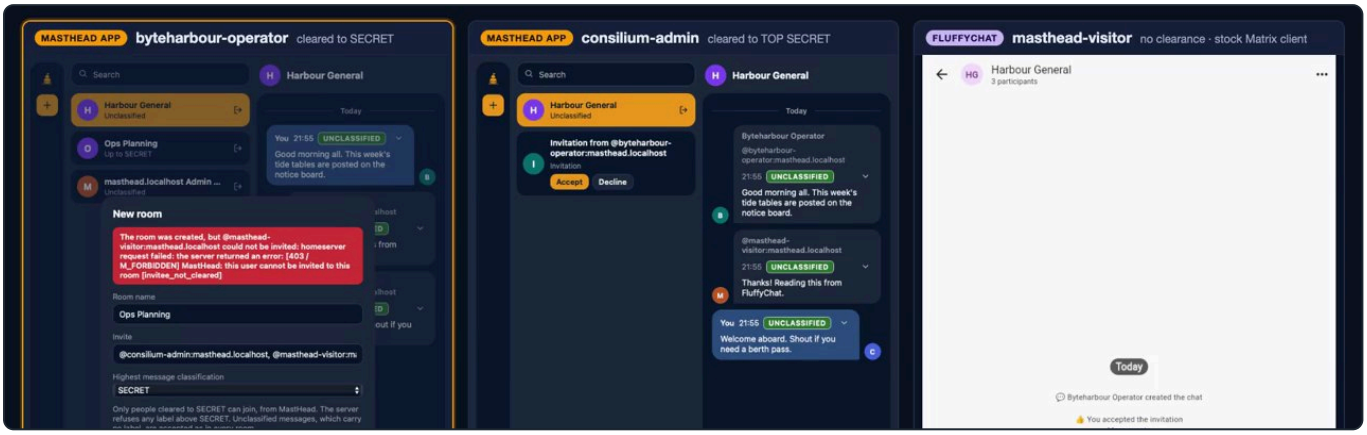
Built to implement the standards

Message labelling and binding are built to implement ACP 240 and STANAG 4774 and 4778.

PRODUCT IN ACTION

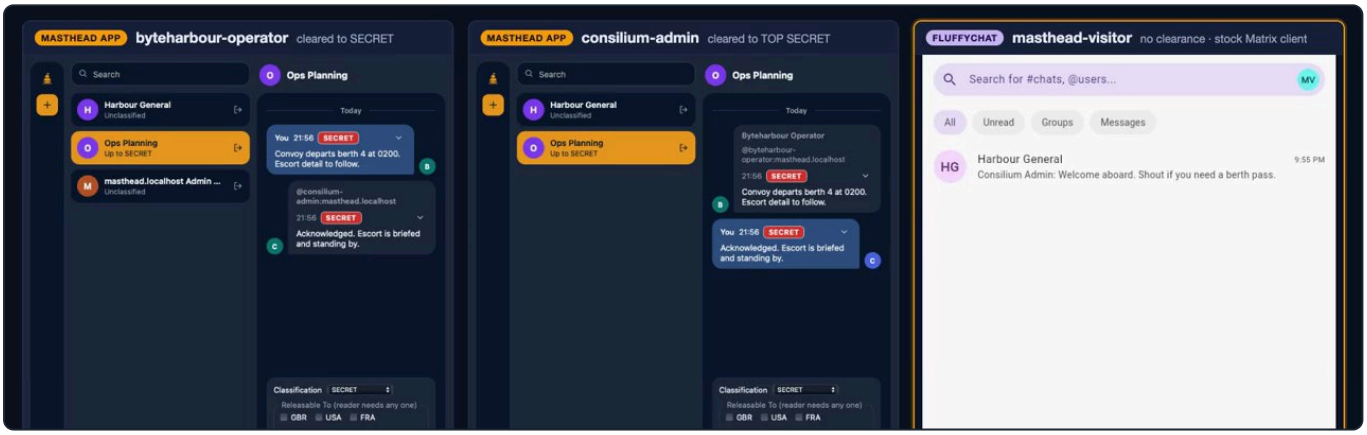
See MastHead working

These screens are from a MastHead demonstration with three people at different clearances: an operator cleared to SECRET, an administrator cleared to TOP SECRET and an uncleared visitor on a standard Matrix client.



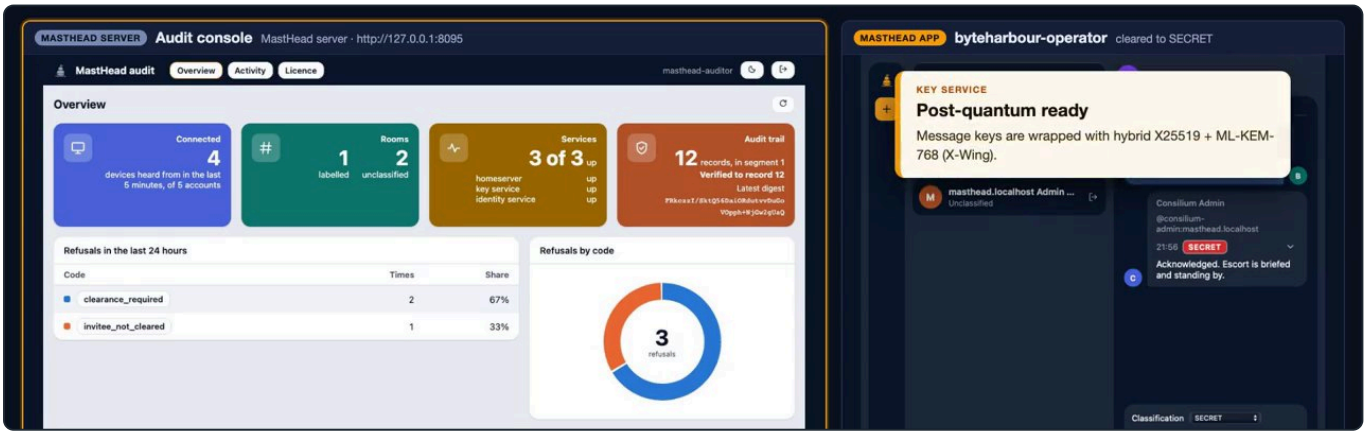
Invitation refused. The operator creates a room with SECRET as its highest classification. The server checks clearance first and refuses to invite the uncleared visitor.

Demonstration environment, illustrative data. Interface screenshot, cropped.



No trace for the uncleared. While the cleared users work in the SECRET room, the visitor on a standard Matrix client sees no sign that the room exists.

Demonstration environment, illustrative data. Interface screenshot, cropped.



Every decision recorded. The audit console shows each security decision on the MastHead server. It is open only to the auditor role.

Demonstration environment, illustrative data. Interface screenshot, cropped.

Screens are from a demonstration environment with illustrative users and data, cropped for layout.

INTEGRATION BY DESIGN

Open standards and the Espanaro policy layer

MastHead is built on open standards, so it fits the identity, network and client choices an organisation has already made.

INTEGRATION AREA	SUPPORTED APPROACH
Matrix	Built on the open Matrix messaging standard. Unclassified rooms work with standard Matrix clients.
Identity	Users sign in through their organisation's identity provider.
HarbourGuard	Decides who may join each labelled room and who may receive keys, from user attributes.
ByteHarbour	Uses ByteHarbour labelling, so messages follow the same rules as documents and streams.
Consilium	Alerts and playbooks can open the right room for the right people.
Audit	Every security decision is recorded and can be reviewed in the audit console.

DEPLOYMENT OPTIONS

Deploy where the mission needs it

ON-PREMISES

In your network

A MastHead server on a secure site or controlled network.

PRIVATE CLOUD

Managed hosting

Hosted in approved cloud infrastructure, run by your team or ours.

FEDERATED

Across organisations

Partner organisations each sign in with their own identity provider.

BUILT FOR CONTROLLED ENVIRONMENTS

Assurance considerations

Server-enforced policy

The server refuses access that policy does not allow, whatever client is used.

Verifiable audit

Each decision is recorded as it was made, for review and investigation.

UK sovereign, UK owned

Veteran owned and engineered in the UK, with direct access to the product team.

REPRESENTATIVE USE CASES

Where MastHead makes the difference

Operations rooms

Coordinate an incident with only the people entitled to take part, with a room opened by a Consilium playbook.

Partner and coalition working

Share a room with another organisation under a common label, each signing in with their own identity provider.

Counter-drone and site security

Give the guard force a labelled room for each incident, linked to the operational picture.

Sensitive programmes

Keep programme conversations to the right cleared team, with a record of every decision.

WHY MASTHEAD

Secure messaging, built in the UK

- Labels on every room and message
- Membership decided by policy
- Sign in with your own identity provider
- Server-enforced, whatever the client
- Verifiable audit trail
- Built on the open Matrix standard
- Same policy layer as ByteHarbour and Consilium
- UK-sovereign engineering with direct access to the team

Talk in real time, keep control of who heard what.

MastHead brings data-centric security to conversation. Rooms carry a label, HarbourGuard decides who may join, and every decision is recorded.

Use cases are representative and are configured to each customer.

WHERE IT FITS

Part of one software family, useful on its own

MastHead runs standalone or with the other Espanaro products. Each layer uses open interfaces, so capability can be added without replacing what is already in place.

COMMAND Bring it together	**Consilium** Orchestration and C2		
SENSE See and verify	**Cognisight** AI video and sensor analytics	**Pulse Sentinel** Sensor health assurance	**Watchkeeper** Multi-sensor fusion
GOVERN Control access and sharing	**HarbourGuard** Policy-driven access	**ByteHarbour** Governed data sharing	
ACT Task and deploy	**WayForge** Uncrewed-systems tasking		
CONNECT Join the systems	**RibbonFlow** Service mesh, early access	**MastHead** Labelled secure messaging	

MATURITY AND PROOF POINTS

MastHead today

Demonstrated

Working end to end

Labelled rooms, server-enforced invitations and an audit console, demonstrated with users at three clearances.

Label travels

Each message is encrypted on the device, with its label bound and signed.

Open client choice

Unclassified rooms work with standard Matrix clients, with no trace of rooms a user is not cleared for.

DEPLOYMENT FORMS

FORM	MASTHEAD
Embedded in a platform Runs on a compute module inside a UGV, UAV, vehicle or sensor node, within the platform's own power, comms and update cycle.	Not applicable
Edge node beside a platform A forward node, such as the Espanaro DATE Box (Decision Advantage Tactical Edge), serving several platforms and sensors on a local network.	Scoped per platform
Site and on-premises Secure sites and controlled networks, hosted locally and run by your team or ours.	Supported
Hub, cloud and federated Central or accredited hosting, private cloud or hybrid, federating several sites and partners.	Supported

STANDARDS AND INTERFACES

Built on the open Matrix standard. Organisation identity providers. Built to implement ACP 240 and STANAG 4774 and 4778 for labelling.

SUPPORT AND COMMERCIAL

Licensed per deployment, with integration services scoped to each programme. Supported by Espanaro's UK product and engineering team. Available direct or through prime and integrator partners, embedded in their systems or connected by API. All IP is owned by Espanaro Ltd.

Status describes Espanaro's own deployments, trials and demonstrations. It is not an independent certification or a technology readiness level. Capabilities are configured for each customer.

TECHNICAL SUMMARY

At a glance

Product type	Secure messaging software.
Primary function	Labelled rooms and messages with policy-decided membership.
Components	MastHead server with Matrix server, key service, policy and audit. MastHead desktop app. Standard Matrix clients for unclassified rooms.
Identity	Organisation identity providers.
Access control	HarbourGuard policy from user attributes such as clearance, role and organisation.
Protection	Messages encrypted on the device, label bound and signed. Built to implement ACP 240 and STANAG 4774 and 4778. Post-quantum ready key wrapping.
Deployment	On-premises, private cloud or federated.
Status	Demonstrated end to end, with server-enforced policy and audit. Ready to deploy with your teams.

HOW TO ENGAGE

A straightforward path from first conversation to operations

STEP 01

Discovery

Understand who needs to talk, across which organisations and at what sensitivity.

STEP 02

Integration workshop

Shape labels, policies and identity integration around your teams.

STEP 03

Deploy

Run MastHead with your teams and move into operational use, with UK support.

Talk freely. Share safely.

Speak to Espanaro about a discovery session, an integration workshop or a demonstration.

Book a demonstration

CALL
+44 1686 510 150

EMAIL
info@espanaro.com

MASTHEAD · an **ESPANARO** product · www.espanaro.com

MastHead is built on the open Matrix standard. Standards wording describes Espanaro's design, not an independent certification. Screens are from a demonstration environment with illustrative data.