

Sovereign software for defence, security and critical infrastructure.

Seven products that sense, govern, act and command, **designed to work with the systems you already have**. This catalogue summarises each product, shows it working, and sets out where it is used.

Modular

Open

Integration-led

Edge · On-Prem · Hybrid

UK-Sovereign



CONSILIUM



COGNISIGHT



PULSE SENTINEL



HARBOURGUARD



BYTEHARBOUR



WAYFORGE



RIBBONFLOW



Consilium common operational picture. Demonstration environment, illustrative data. Interface screenshot, cropped.

WHY ESPANARO

Practical capability for complex, controlled environments

Espanaro builds sovereign software for defence, national security and critical national infrastructure. The products in this catalogue address the questions operators ask most: what is happening, who can see it, what should we do, and how do our systems talk to each other.

UK sovereign, UK owned

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

Open and modular

Deploy only what you need and expand over time, through open interfaces.

Built to integrate

Connect new capability to existing sensors, systems and data, without wholesale replacement.

Operator-first

Designed around operator decisions and operational outcomes, not the technology trend.

THE PRODUCTS AT A GLANCE

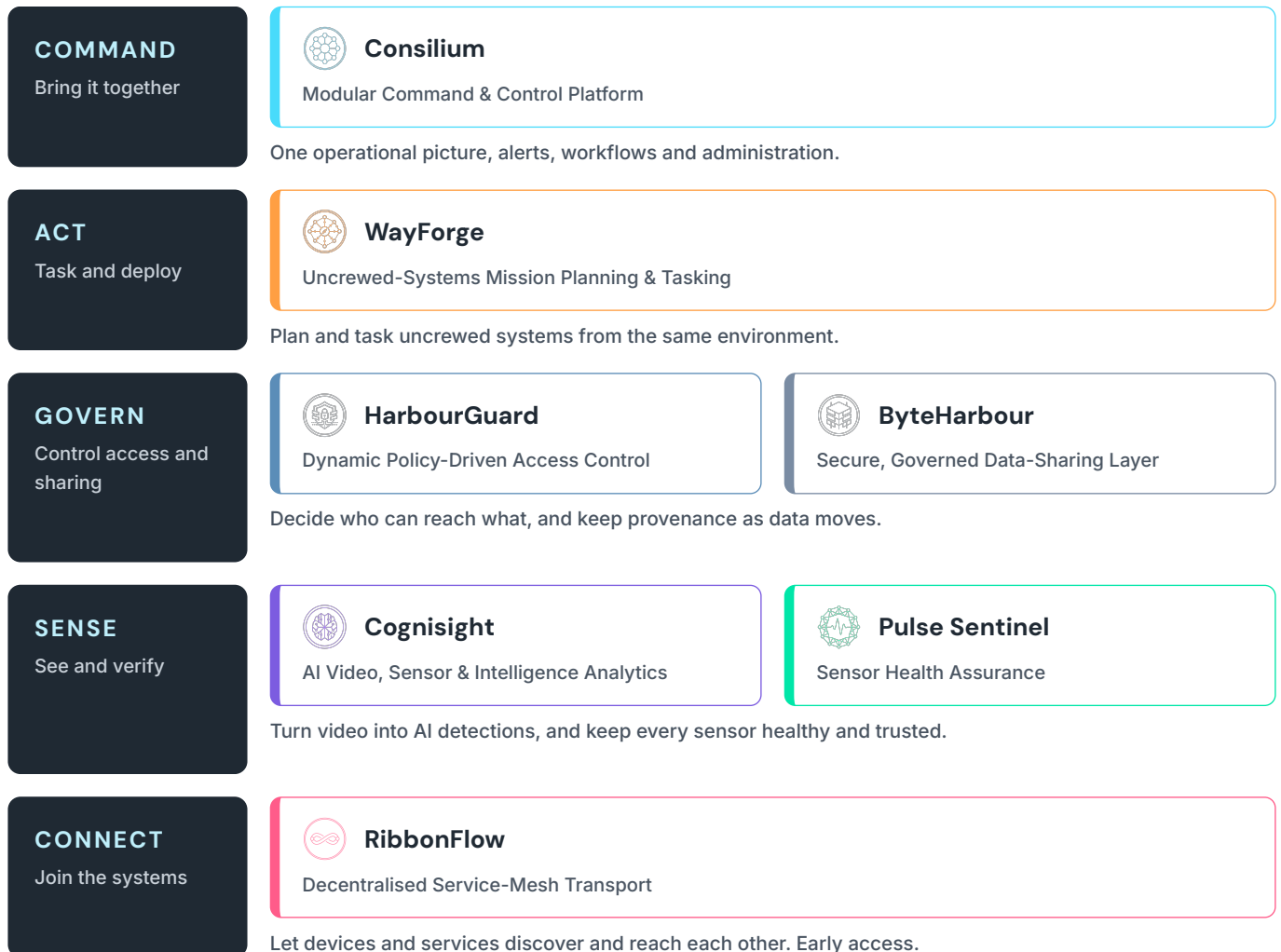
PRODUCT	STACK LAYER	WHAT IT DOES	DEPLOYMENT
 Consilium	Command	Modular Command & Control Platform	On-Prem · Cloud · Hybrid
 Cognisight	Sense	AI Video, Sensor & Intelligence Analytics	Edge · On-Prem · Hybrid
 Pulse Sentinel	Sense	Sensor Health Assurance	Edge · On-Prem · Hybrid
 HarbourGuard	Govern	Dynamic Policy-Driven Access Control	On-Prem · Private Cloud · Hybrid
 ByteHarbour	Govern	Secure, Governed Data-Sharing Layer	DCS Level 3
 WayForge	Act	Uncrewed-Systems Mission Planning & Tasking	Command Post · Vehicle · Distributed
 RibbonFlow	Connect Early access	Decentralised Service-Mesh Transport	Per host, with Consilium or at the edge

Stack layers are explained on the next page. RibbonFlow is at early access.

HOW THE PRODUCTS FIT TOGETHER

Five layers, each usable on its own

Every product runs standalone. Used together, they cover the path from raw sensor data to a governed operational decision, with Consilium as the command layer on top.



Start with the product that solves the most urgent problem. Because each layer uses open interfaces, others can be added later without replacing what is already in place. The next page shows how the layers combine to put the right information in front of the right person or system.

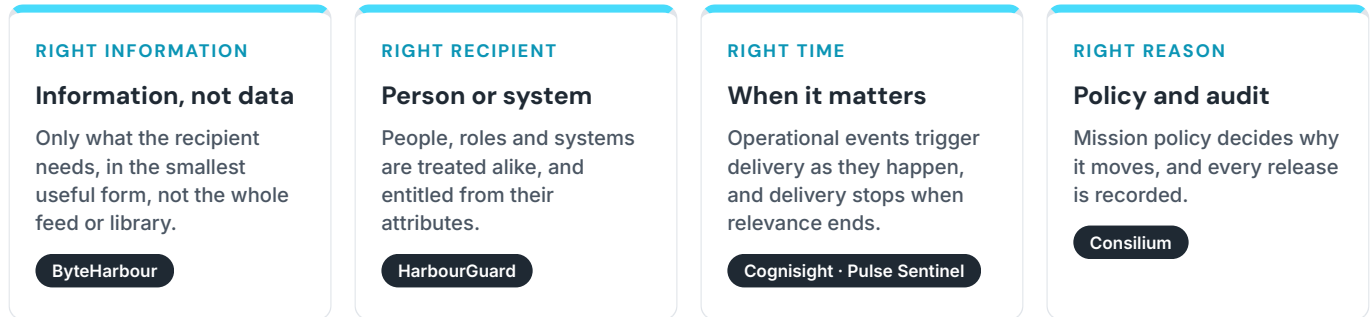
THE FLOW IN BRIEF



DECISION ADVANTAGE

The right information, to the right person or system, at the right time, for the right reason

Data is not the advantage. Information is. Used together, the products decide what matters, who needs it, how it travels and at what protection level, and move no more than the recipient needs.



FROM EVENT TO DELIVERY

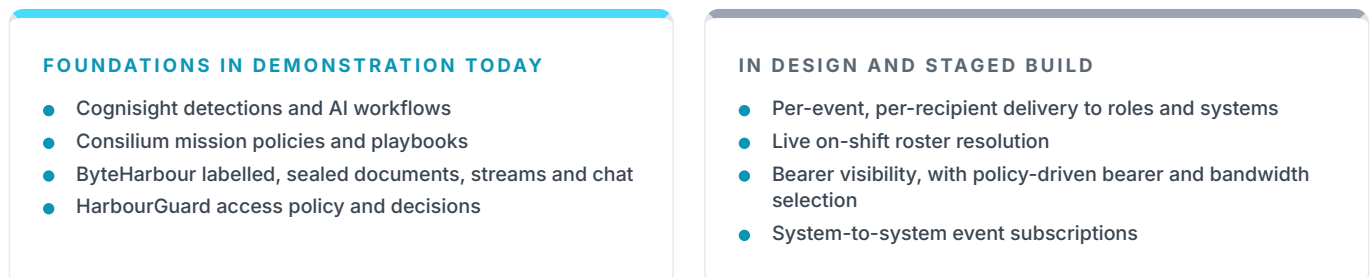


OPERATIONS DRIVING NETWORK POLICY

Consilium policies work with ByteHarbour to decide which data goes over which bearer, at which DCS level, and how much bandwidth the bearer needs. Operational triggers, such as a confirmed Cognisight detection, can drive technical network policy: request more bandwidth for the link carrying the responders' feed, then release it when the event closes.

INFORMATION	WHO RECEIVES IT	DCS HANDLING	BEARER AND BANDWIDTH
Weapon detection alert: snapshot and location	On-shift ops team and response units	Scoped to each recipient, highest handling for the site	Any permitted bearer. Small payload, sent first.
Live camera feed to responders	Named response units, for the duration of the event	Sealed stream. Access ends when the event closes.	Wideband bearer. Bandwidth raised on the trigger, released at close.
Sensor health summary	Duty officer	Standard handling	Low-rate bearer is enough.
Planning document or imagery	Cleared partner system	Release per recipient	Held until a suitable bearer is available.

Illustrative policy. Rules, levels and bearers are configured for each deployment.



Items in design and staged build are design intent, scoped for each programme, and are not delivered capabilities.



CONSILIUM

Modular Command & Control Platform · Command layer

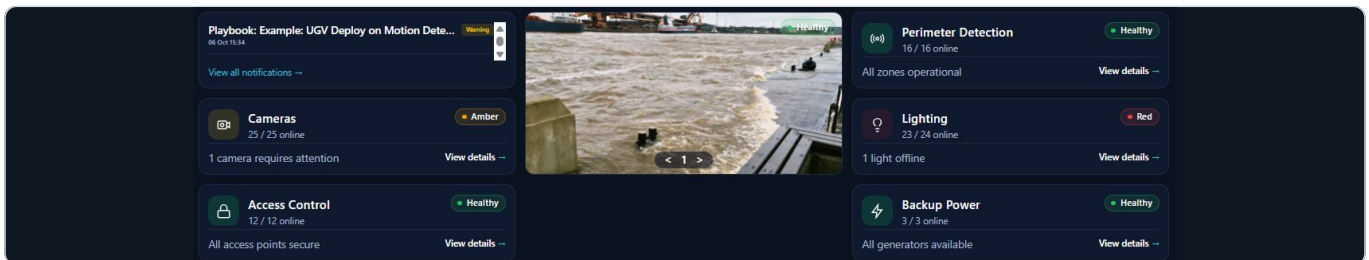
One operational picture, from the systems you already have.

A modular command-and-control platform that connects sensors, platforms and operational systems into one governed view, with alerts, workflows and reporting.



Common operational picture. Live map with camera feeds and sensor markers in one place.

Demonstration environment, illustrative data. Interface screenshot, cropped.



Site and system health. Connected systems and feed status at a glance.

Demonstration environment, illustrative data. Interface screenshot, cropped.

One coherent picture

Cameras, sensors, alerts and maps in a single configurable view.

Integrate, do not replace

Open interfaces and adaptors connect the systems you already run.

Deploy where you need it

On-premises, cloud or hybrid, built for controlled environments.

TYPICAL USE CASES

- Secure site operations
- Command and control across distributed assets
- Multi-system integration for trials and pilots

WORKS WITH

Cognisight

Pulse Sentinel

WayForge

HarbourGuard

ByteHarbour

SAPIENT, ONVIF, RTSP, MQTT, DDS



COGNISIGHT

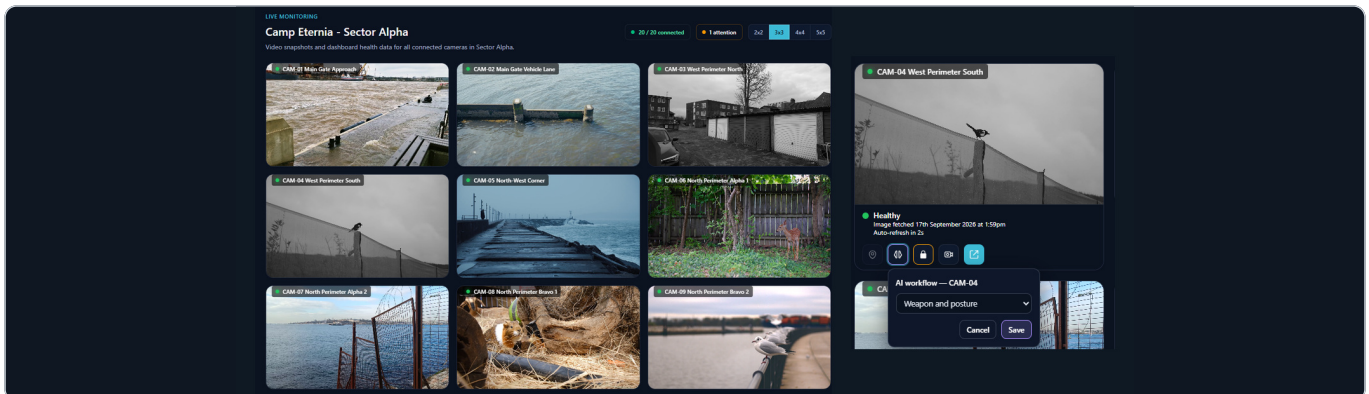
AI Video, Sensor & Intelligence Analytics · **Sense layer**

See what matters, the moment it happens.

AI-enabled analytics for video, sensor and intelligence data. Operators build detection workflows in Consilium, assign them to cameras and surface the events that need attention.



AI workflow builder. A camera feed linked to posture and weapon detection, then to log and alert actions. Demonstration environment, illustrative data. Interface screenshot, cropped. Shown within Consilium.



Camera wall and workflow assignment. A camera wall, and the selector that assigns an AI workflow to a camera. Demonstration environment, illustrative data. Interface screenshot, cropped. Shown within Consilium.

Less manual monitoring

Routine activity is filtered so operators focus on what matters.

Build your own workflows

Chain posture, weapon, aggression and fall detection to alerts and logs.

Assign per camera

Choose which AI workflow each camera runs, from the camera view.

TYPICAL USE CASES

- Perimeter and site security
- Rapid video review
- Incident investigation

WORKS WITH

ONVIF and RTSP cameras

Consilium

MQTT and DDS event streams

APIs in JSON and XML

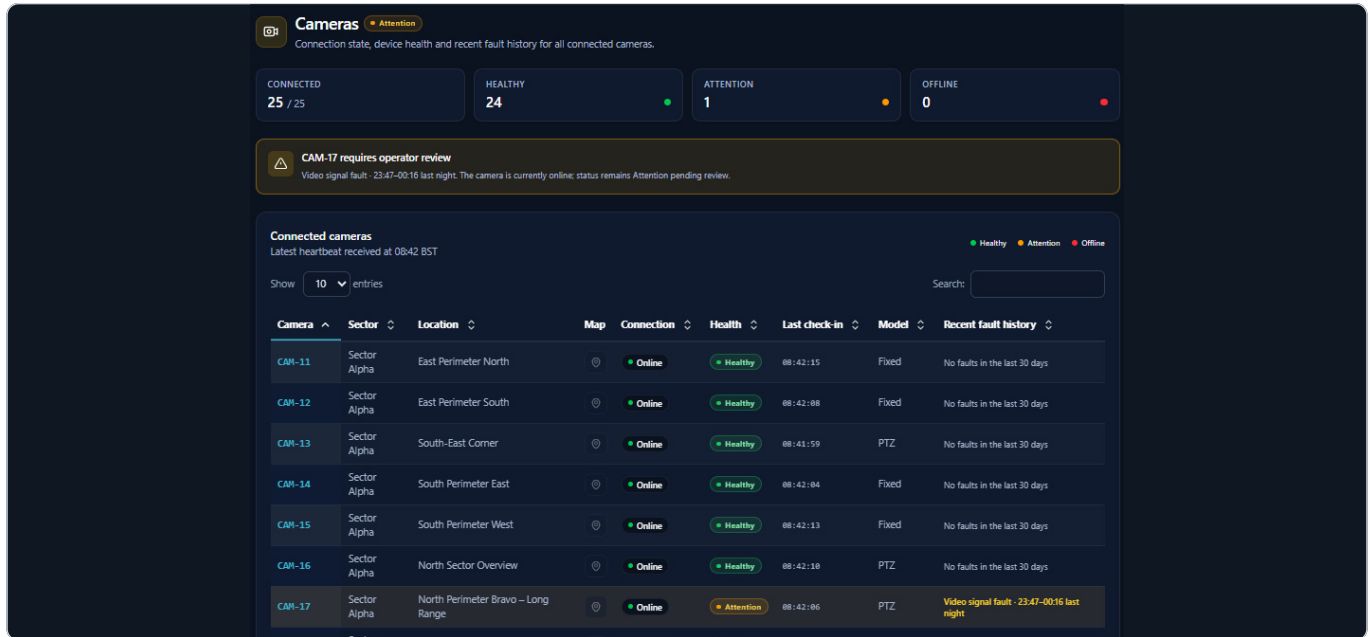


PULSE SENTINEL

Sensor Health Assurance · Sense layer

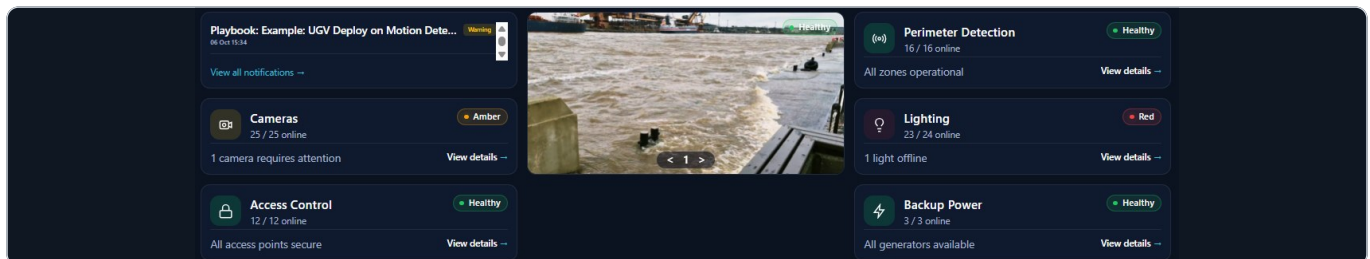
Know your sensors work, and how far to trust them.

Sensor health assurance. It shows whether each sensor is working as it should and how much to trust its output, and reports faults into Consilium.



Sensor and device health. Connected, healthy and attention counts, with fault history for each camera.

Demonstration environment, illustrative data. Interface screenshot, cropped. Shown within Consilium.



Estate health in Consilium. Cameras, perimeter, lighting, access control and power by health state.

Demonstration environment, illustrative data. Interface screenshot, cropped. Shown within Consilium.

Early warning

Faults, drift and degradation are flagged before they mislead operators.

Trust state per sensor

A clear view of how far each sensor output can be relied on.

Visible in Consilium

Trust faults reach operators and workflows in the same operating view.

TYPICAL USE CASES

- CCTV and camera estates
- Detection sensor assurance
- Position and timing sources

WORKS WITH

Consilium

Sensor and device data

MQTT and DDS event streams

ONVIF video systems



HARBOURGUARD

Dynamic Policy-Driven Access Control · **Govern layer**

The right access, for the right reason, at the right time.

Dynamic, policy-driven access control with its own login and administration. It is linked to Consilium, where its policies are enforced inside the C2 platform.

Access policies. Named policies set classification, vetting, releasability and need to know.

Demonstration environment, illustrative data. Interface screenshot, cropped.

Authorisation activity. Requests, allowed and denied decisions and active policies.

Demonstration environment, illustrative data. Interface screenshot, cropped.

Context-aware decisions

Access reflects identity, device, location, time and mission.

Least privilege

Reduces standing permissions with granular, time-bound outcomes.

Auditable

Records the policy and attributes behind each decision.

TYPICAL USE CASES

- Mission-based access
- Sensitive data protection
- Zero-trust architecture

WORKS WITH

Identity providers and directories

ByteHarbour

Consilium

Applications and APIs

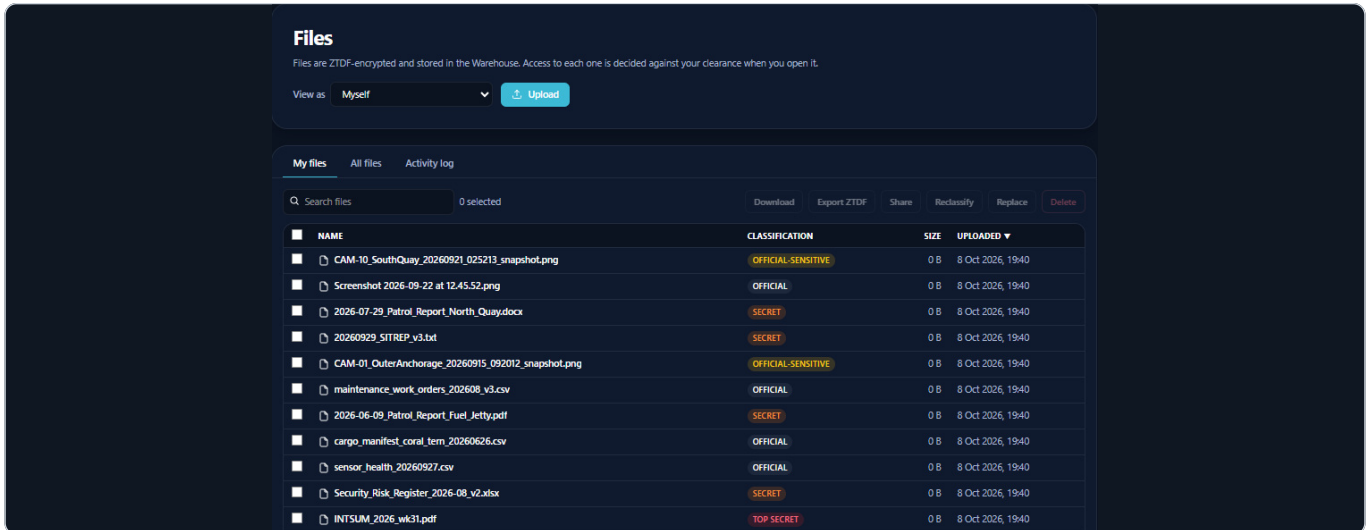


BYTEHARBOUR

Secure, Governed Data-Sharing Layer · Govern layer

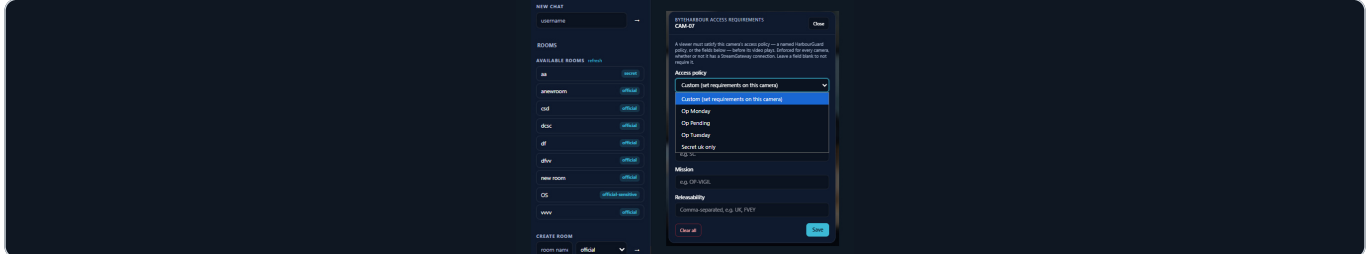
Share data securely, without losing control of it.

A secure, governed data-sharing layer. It protects documents, camera feeds and chat with classification and access control, and preserves provenance as data moves. Reported at DCS Level 3 for document and stream sharing.



Protected documents. Encrypted files, each with a classification label, decided at open time.

Demonstration environment, illustrative data. Interface screenshot, cropped. Shown within Consilium.



Secure chat and camera access. Classified chat rooms, and a camera tied to a named HarbourGuard policy.

Demonstration environment, illustrative data. Interface screenshot, cropped. Shown within Consilium.

Controlled exchange

Policy-aligned workflows govern how data is shared and consumed.

Provenance preserved

Source, classification and handling context travel with the data.

Less integration friction

Modular adaptors connect legacy and modern systems without replacement.

TYPICAL USE CASES

- Cross-organisation data sharing
- Legacy system integration
- Operational data fusion

WORKS WITH

Legacy and operational systems

Consilium, Cognisight and Pulse Sentinel

HarbourGuard

MQTT, DDS and APIs

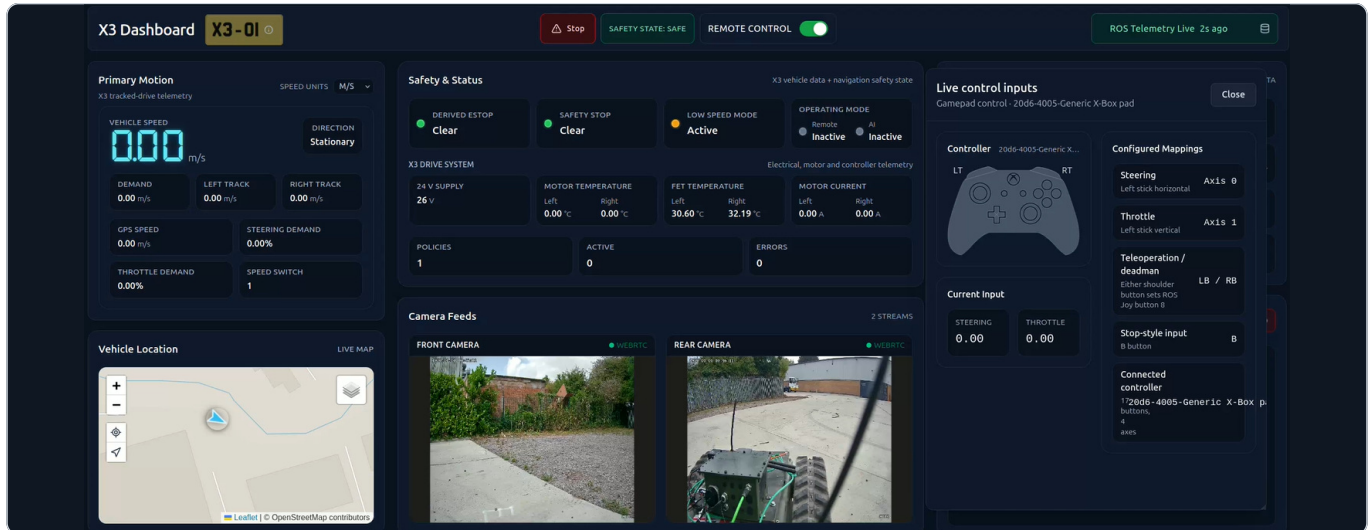


WAYFORGE

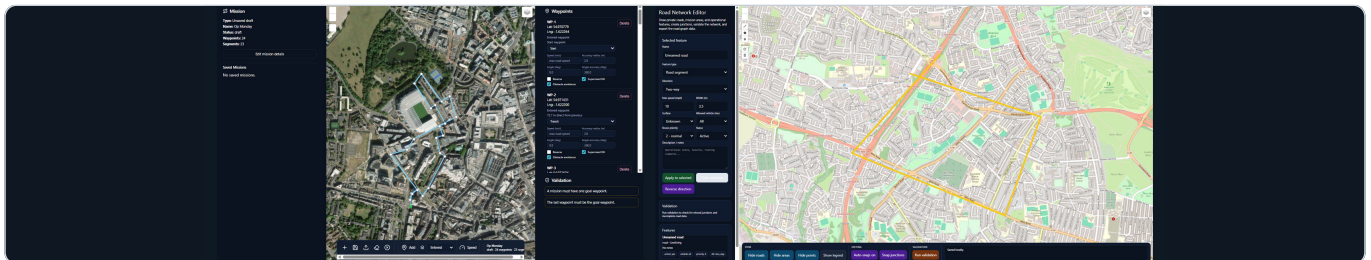
Uncrewed-Systems Mission Planning & Tasking · Act layer

Plan, task and deploy uncrewed systems, as one workflow.

Mission planning, road-network planning and vehicle control for uncrewed systems, inside Consilium. A hardware-agnostic layer that connects platforms to the wider picture.



Live X3 vehicle, driven through WayForge. Telemetry, safety state, camera feeds and gamepad control for the X3 tracked UGV. Live test environment. Interface screenshot, cropped. Shown within Consilium.



Mission planner and road network editor. Place waypoints on a map, and draw and validate private road networks and mission areas. Demonstration environment, illustrative data. Interface screenshot, cropped. Shown within Consilium.

One mission workflow

Plan routes, tasks and constraints once, across platform types.

Repeatable deployment

Rehearse, repeat and evaluate missions consistently.

Connected to the picture

Platform activity feeds Consilium and wider command systems.

TYPICAL USE CASES

- Secure-site patrol
- Hazardous-area operations
- Mission rehearsal and trials

WORKS WITH

UGVs, UAVs and USVs

Sensors and payloads

Consilium

Platform APIs and adaptors



RIBBONFLOW

EARLY ACCESS

Decentralised Service-Mesh Transport · Connect layer

Let services find each other, and connect without a central hub.

A decentralised service-mesh transport. Nodes announce services, discover what they need and exchange messages. Early access, with hardening in progress.

```

two-node mesh verification (transcript condensed)

$ ribbonnode -socket=/tmp/ribbon-a.sock -listen=0.0.0.0:0
[INIT] ribbon node starting, self_uuid=9d97065f... version=0.2.0
$ ribbonnode -socket=/tmp/ribbon-b.sock -listen=0.0.0.0:0
[INIT] ribbon node starting, self_uuid=298fe7d1... version=0.2.0
[HANDSHAKE] mutual trust established with 9d97065f...

[1] Baseline push/ack round trip over the live mesh (node A to node B)
    PASS : hub acknowledged playbook (device identity verified, not revoked)
[2] Disconnect: node B stopped, push sent while it is down
    PASS : no ack received while node B is down, as expected
[3] Reconnect: node B back up under a NEW peer id (d8abadfa...)
    PASS : mesh re-established, same device identity, no re-pairing needed
[4] Revoked-certificate case on the live mesh
    PASS : hub rejected the validly signed batch from the revoked device

Phase 1 and 2 complete: all checks PASSED against the live two-node mesh.

```

Live two-node mesh verification. Baseline sync, node-down, reconnect and revoked-device checks on a live two-node mesh. Terminal transcript condensed from an engineering record.

```

verification summary (from engineering records)

RibbonFlow, verification summary (engineering record)

Consilium RibbonFlow plug-in      23 tests (adaptor, API permissions, listener)
Full Consilium test suite         489 passed, 0 failures, 0 regressions
Sensor discovery (Request/Announce) 18 passed over real loopback UDP
Edge sync transport tests         17 / 17 pass

Behaviours exercised
timeout with no responder         falls back to static config
malformed or empty-token reply    falls back to static config
plug-in disabled (default)        every call audited, no network traffic
revoked device certificate         message rejected at the Espanaro layer

```

Verification summary. Test counts and behaviours exercised across three integrations. Condensed from an engineering record.

Self-enrolling sensors

Sensors ask where to enrol and fall back to static configuration.

Reconnect without re-pairing

Restarted nodes return under the same device identity.

Identity checked per message

Signatures, certificates and revocation are enforced at the Espanaro layer.

TYPICAL USE CASES

- Sensor self-enrolment
- Edge sync transport
- Service-to-service messaging

WORKS WITH

Consilium plug-in

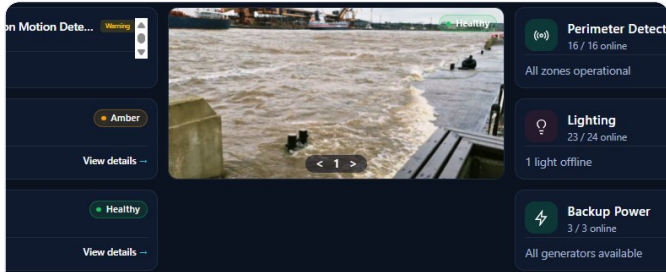
Edge Runtime sync

Sensor enrolment adaptors

USE CASES

Where the products work together

Every scenario runs the same decision-advantage flow: an event, a policy decision, an entitlement check, a sealed release and delivery over the right bearer, as set out on page 4. Each can start with a single product and grow as needs change.



Secure site operations

See, correlate and respond across a site

A detection reaches the on-shift team and response units as a sealed, scoped alert, not as standing access to every feed. Policy decides the route, and can ask for more bandwidth while the event is live.

Cognisight

Pulse Sentinel

Consilium

HarbourGuard



Uncrewed-systems missions

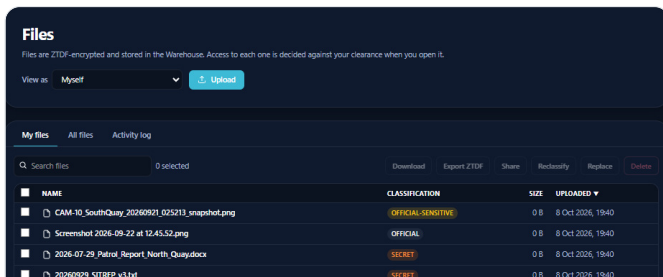
Plan, task and supervise platforms

Missions and road networks are planned in one workflow, and vehicles are driven with live telemetry and camera feeds. Mission events can set the policy for the vehicle link.

WayForge

Consilium

Cognisight



Controlled data sharing

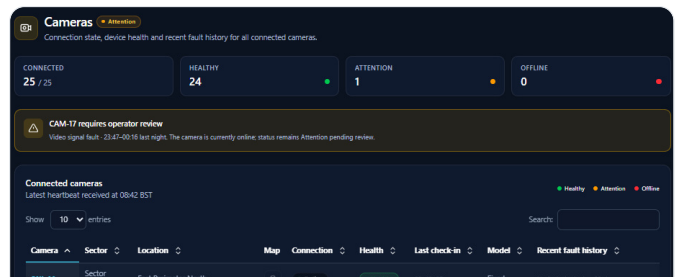
Share what you must, keep control

Documents, camera feeds and chat carry classification labels. Each release is made per recipient, at the DCS level required, and decided against clearance and recorded.

ByteHarbour

HarbourGuard

Consilium



Sensor assurance

Trust the sensors you rely on

A silent or degraded sensor raises an alert to the right owner, and policy decides how the report travels. Sensors can enrol and sync across a mesh. RibbonFlow is at early access.

Pulse Sentinel

RibbonFlow (early access)

Consilium

Screens are from Espanaro demonstration and test environments. Scenarios are representative and are configured to each customer. Per-recipient delivery and policy-driven bearer selection are in design and staged build.

DEPLOYMENT, ASSURANCE AND ENGAGEMENT

Deploy where the mission needs it

ON-PREMISES

In your network

Secure sites, controlled networks and locally hosted operations.

PRIVATE CLOUD / CLOUD

Managed hosting

Centrally managed services in approved cloud infrastructure.

HYBRID

Best of both

Distributed operations across edge, site and central services.

EDGE / SITE

Close to the source

Analytics and reasoning near cameras and sensors.

ASSURANCE CONSIDERATIONS

Secure by design

Role and policy-driven access, Zero Trust principles and governed information sharing.

Data residency

Deployment aligns to your network boundaries, security model and governance.

UK sovereign, UK owned

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

STANDARDS AND INTERFACES

Products connect through open interfaces including SAPIENT, ONVIF, RTSP, MQTT, DDS, Modbus and APIs in JSON and XML. ByteHarbour metadata handling is aligned to ACP240, guided by STANAG 4774 and 4778, and ByteHarbour is reported at DCS Level 3 for document and stream sharing. This is Espanaro's capability statement, not an independent certification.

HOW TO ENGAGE

STEP 01

Discovery

Understand the operational problem, environment and existing systems.

STEP 02

Workshop

Shape modules, integration and deployment options around your mission.

STEP 03

Pilot

Evaluate in a controlled deployment ahead of wider rollout.

Screens in this catalogue are from Espanaro demonstration environments with illustrative data, cropped for layout. The WayForge X3 screen is from live vehicle testing. RibbonFlow is at early access and its images are condensed engineering records.

ESPANARO



UK SOVEREIGN / UK OWNED / VETERAN OWNED

Start with the problem, not the technology trend.

Speak to Espanaro about a discovery session, an integration workshop or a pilot deployment of any product in this catalogue.

Book a discovery session

CALL

+44 1686 510 150

EMAIL

info@espanaro.com

WEB

www.espanaro.com