



HARBOUR GUARD

Dynamic Policy-Driven Access Control

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

Harbour Guard provides dynamic, policy-driven access control for sensitive data, services and operational applications, **evaluating who is requesting access, what they are reaching, the context of the request and the applicable mission policy**. It operates independently or alongside ByteHarbour, Consilium and third-party systems.

Dynamic

Precise

Auditable

On-Prem · Private Cloud · Hybrid

UK-Sovereign

Deploy as a standalone access-control capability, or as the policy decision layer across the wider **Espanaro** product ecosystem.

www.ESPANARO.com

WHAT IS HARBOUR GUARD

Dynamic access control based on identity, context and mission

Harbour Guard provides dynamic, policy-driven access control for sensitive data, services and operational applications. It evaluates who is requesting access, what they are trying to reach, the context of the request and the applicable mission or organisational policy. It can operate independently or integrate with ByteHarbour, Consilium and third-party systems.

THREE PRINCIPLES

• Dynamic

Adapt access decisions as identity, mission and operating context change.

• Precise

Apply granular controls to data, services, functions and individual actions.

• Auditable

Record the policy, attributes and context behind each access decision.

THE CHALLENGE & THE OUTCOME

THE CHALLENGE

Defence, national security and critical-infrastructure organisations need to protect sensitive information without preventing authorised people from acting at pace.

Traditional role-based access controls are often **too static for operational environments**, where permissions must respond to changing identity, location, device posture, mission, classification and threat context.

OPERATIONAL VALUE

Harbour Guard delivers:

- Context-aware decisions
- Least-privilege access
- Reduced standing permissions
- Consistent policy enforcement
- Improved auditability

THE APPROACH

Harbour Guard provides a dynamic **policy decision and enforcement layer** that evaluates each access request against identity, attributes, environmental context and mission rules, letting organisations move beyond broad, permanent permissions to decisions that reflect **data sensitivity, current need and the operating situation**.

WHAT HARBOUR GUARD DOES

Evaluate every request, then decide and enforce

Harbour Guard weighs identity, attributes and operating context against mission policy, then applies a granular decision through the systems you already run.

- + Evaluates identity, role, clearance, organisation and other user attributes.
- + Considers device, network, location, time, mission and threat context.
- + Applies attribute-based and policy-based access-control decisions.
- + Supports allow, deny, restrict, mask, filter or time-bound outcomes.
- + Reduces dependence on broad, permanent role permissions.
- + Enforces policy consistently across connected applications and services.
- + Provides decision records for assurance, investigation and audit.
- + Integrates with identity providers, data platforms and operational systems.

CORE CAPABILITIES

Four building blocks for dynamic, policy-driven access

01

Policy Decision Engine

Evaluate each access request against identity, resource, context and mission policy.

02

Attribute-Based Access Control

Use user, device, data and environmental attributes to make granular decisions.

03

Policy Administration

Define, test, version and manage access policies through controlled workflows.

04

Enforcement & Audit Services

Apply decisions through connected systems and retain an auditable record of outcomes.

EVALUATE

Identity, attributes and context



DECIDE

Against mission policy



ENFORCE

Through connected systems



AUDIT

Record every decision

INTEGRATION BY DESIGN

A policy decision and enforcement layer across your estate

Harbour Guard evaluates each access request against identity, attributes, environmental context and mission rules, letting organisations move beyond broad, permanent permissions to decisions that reflect data sensitivity, current need and the operating situation.

INTEGRATION AREA	SUPPORTED APPROACH
Identity & directory services	Connect to existing identity providers, directories, roles, claims and authentication services.
Applications & APIs	Integrate policy decisions with web applications, services, APIs and operational workflows.
Data & information platforms	Apply controls to data access, sharing, querying, transformation and presentation.
Security & context sources	Consume device posture, network, location, classification, mission and threat attributes.
Espanaro product ecosystem	Integrate with ByteHarbour for governed exchange and Consilium for operational access control.

DEPLOYMENT OPTIONS

Deploy where the mission needs it

ON-PREMISES In your network For secure facilities, controlled networks and sovereign environments.	PRIVATE CLOUD Managed services For centrally managed policy services within approved cloud infrastructure.	HYBRID Best of both For consistent access decisions across local, central and partner environments.
--	--	---

BUILT FOR CONTROLLED ENVIRONMENTS

Assurance considerations

● Secure by design Attribute and policy-driven decisions, least-privilege access and granular enforcement.	● Data residency Decisions align to your network boundaries, classification model and operational governance.	● UK-sovereign Engineered in the UK with direct access to the product and delivery team.
---	--	---

REPRESENTATIVE USE CASES

Where Harbour Guard makes the difference

Mission-Based Access

Grant time-bound access according to operational task, location and mission need.

Sensitive Data Protection

Control access to classified, commercially sensitive or personally identifiable information.

Cross-Organisation Collaboration

Enable partners to access approved resources without inheriting broad internal permissions.

Application Modernisation

Add modern policy controls around legacy or specialist systems without replacing them.

Zero-Trust Architecture

Evaluate every request using current identity, device and environmental context.

Trials & Evaluation

Test policy models, attributes and enforcement patterns in controlled pilot environments.

WHY HARBOUR GUARD

Context-aware access control, built in the UK

- ✓ Moves access control beyond static roles and network location.
- ✓ Reduces standing privilege and excessive permissions.
- ✓ Applies policy consistently across systems and organisational boundaries.
- ✓ Can operate independently or as part of the wider Espanaro product stack.
- ✓ Works with existing identity, application and data estates.
- ✓ Improves traceability by explaining why access was allowed or denied.
- ✓ Supports granular, context-aware and time-bound decisions.
- ✓ UK-sovereign engineering with direct access to the product and delivery team.



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

Harbour Guard evaluates identity, attributes and operating context against mission policy, applying decisions that reflect data sensitivity and current need.

TECHNICAL SUMMARY

At a glance

Product type	Dynamic policy and attribute-based access-control software.
Primary function	Evaluate and enforce decisions using identity, resource, context and mission attributes.
Architecture	Modular policy decision, administration, information and enforcement services.
Deployment	On-premises, private cloud or hybrid.
Interfaces	APIs, identity claims, contextual attributes, policy integrations and enforcement points.
Users	Security teams, system owners, architects, administrators and application integrators.
Lifecycle	Suitable for policy discovery, zero-trust pilots, integration trials and operational deployment.

HOW TO ENGAGE

A straightforward path from first conversation to operations

STEP 01**Discovery**

Understand the access-control problem, environment and existing identity and data systems.

STEP 02**Policy Workshop**

Shape attributes, policies and enforcement options around your mission and constraints.

STEP 03**Pilot**

Evaluate Harbour Guard in a controlled deployment ahead of wider operational rollout.

**Give the right people access, for the right reason
and at the right time.**

Speak to Espanaro about a Harbour Guard policy workshop, access-control discovery or pilot deployment.

[Book a discovery session](#)

CALL

+44 1686 510 150

EMAIL

info@espanaro.com