harbor

DATA SHEET

DISCOVERY:

Lighthouse

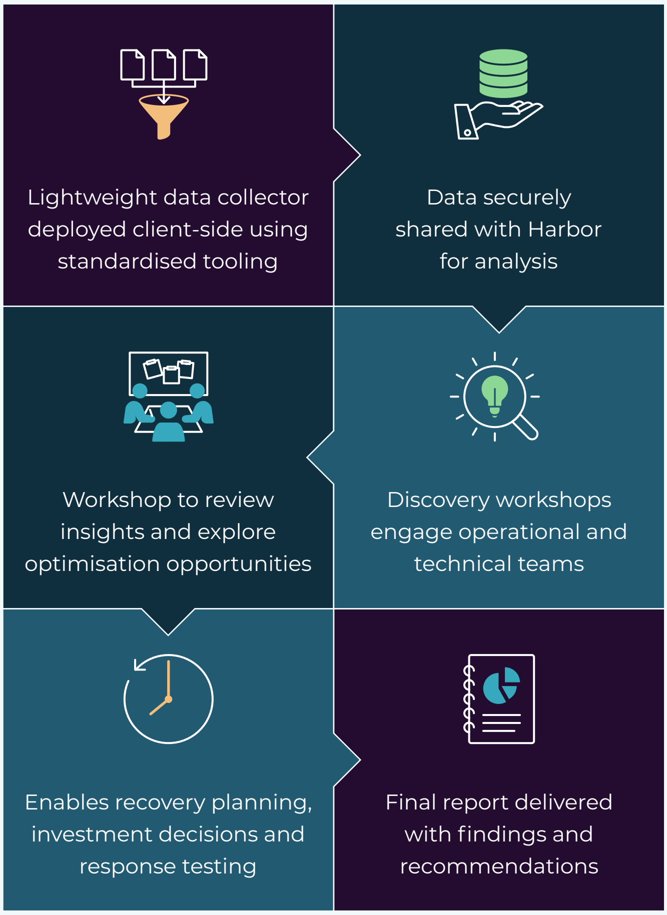
UNDERSTAND KEY RISKS.
FOCUS ON WHAT MATTERS.
RECOVER WITH PURPOSE.

What is Lighthouse Discovery?

A structured discovery engagement to help organisations understand their critical data, systems and services, and prioritise recovery in the event of a cyber attack.

- Identifies business-critical functions and prioritise recovery actions
- Clear current and future state data protection overview
- Side-by-side TCO and ROI analysis with Harbor
- Interactive dashboard highlights data volume, type and growth
- Operating systems benchmarked for next-gen data protection compatibility
- Compatible with LiveOptics, RVTools, Azure and AWS sizing scripts

How It Works



Lightweight data collector deployed client-side using standardised tooling

Data securely shared with Harbor for analysis

Discovery workshops engage operational and technical teams

Workshop to review insights and explore optimisation opportunities

Enables recovery planning, investment decisions and response testing

Final report delivered with findings and recommendations

Customer Benefits

Prioritise Recovery
Focus effort and resources on the systems and data that matter most.

Business & IT Alignment
Bridge operational and technical priorities with a shared understanding of recovery needs.

Risk Visibility
Identify recovery weaknesses and regulatory gaps before they become critical.

Preparedness Testing
Rehearse incident response and build team confidence under realistic conditions.

Tangible Outputs
Receive actionable deliverables including dashboards, runbooks and scenario reports.

We exist to do right by data.

Phased Engagement Approach

PHASE
1

Data Assessment

Free

Objective:

Feedback and clarify understanding of environment to client via data visualisation.

Outcomes:

- Data visualised for use across multiple stakeholders
- Clear understanding of As-Is before moving on to To-Be work

PHASE
2

Minimum Viable Company (MVC) Workshop

(Paid for engagement)

Objective:

Define the smallest set of systems needed to keep the business running during a crisis.

Outcomes:

- Service catalogue with application recovery tiers
- Recovery runbooks with estimated recovery times and cleansing durations

Audience:

Operational leads, CIO/CISO, application specialists, CTO, compliance officers

Pre-requisites:

Data assessment complete, list of applications to be mapped

PHASE
3

Cyber Recovery Assessment

(Paid for engagement)

Objective:

Evaluate cyber recovery readiness across systems and operations.

Outcomes:

- Cyber recovery report identifying weaknesses and remediation actions
- Review of alignment with regulatory frameworks such as NIST and DORA

Audience:

CIO/CISO, CTO, operational leads, compliance officers, business continuity leads

Pre-requisites:

Completion of Phase 2, visibility into existing recovery processes

PHASE
4

Disaster Recovery Scenario Planning (DR Drills)

(Paid for engagement)

Objective:

Validate response plans and improve readiness through scenario-based exercises.

Outcomes:

- Dynamic restore matrix showing which critical environments can be recovered, how quickly, and where gaps remain
- Detailed recovery scenario report capturing key decisions, risks, and actionable next steps from tabletop walkthroughs

Audience:

CIO/CISO, CTO, business continuity leads, operational leads, compliance officers

Pre-requisites:

Harbor provides 3 to 4 bespoke scenarios tailored to the customer’s environment

harborsolutions.com | sales@harborsolutions.com

We exist to do right by data.

© Copyright 2025 Harbor Solutions. All rights reserved.

harbor