



HexaView
TRUST CONSOLE

IN PARTNERSHIP
WITH



**Cyber
Dockside.ai**

WHITE PAPER · OCTOBER 2026

The control layer above your security tools

Why cybersecurity mesh architecture needs a bidirectional single pane of glass, and how HexaView delivers one across IT and OT

Most organisations do not lack security tools. They lack one place to see what those tools are telling them, act on it, and prove that their controls work. This paper explains the architecture that closes that gap, and where HexaView fits.

EXECUTIVE SUMMARY

One pane to see, act and prove

Security teams have spent a decade adding point solutions, each one justified on its own. Endpoint, identity, cloud, email, vulnerability, operational technology and compliance tools now sit side by side, often from different vendors, each with its own console and its own version of the truth.

Cybersecurity mesh architecture (CSMA) is the industry's answer: let those tools work together, rather than adding more. This paper sets out what CSMA asks for, how it complements defence in depth and zero trust, and how HexaView provides the control layer above your tools.

Key takeaways

**Tool sprawl is a control problem, not a spending problem.**

Each tool works. Together they leave teams switching screens, leaders without one picture and auditors without a clear line from policy to evidence.

**Mesh architecture is the right idea.**

Cybersecurity mesh architecture asks for tools that work together through shared analytics, identity, policy and a consolidated view. It is an approach, not a product.

**The missing piece is a pane that acts, not just displays.**

Read-only dashboards stop at visibility. HexaView is designed to be bidirectional: see across every tool, then push approved, audited actions back.

**Keep the tools you have.**

HexaView sits above your existing stack across IT and OT. Nothing is ripped out; each new integration adds to one shared picture.

CONTENTS

- 01 The problem: more tools, less control
- 02 Cybersecurity mesh architecture in brief
- 03 Defence in depth and mesh: additive, not either-or
- 04 Introducing HexaView
- 05 What HexaView does
- 06 HexaView and the mesh layers
- 07 Closing the loop from policy to proof
- 08 HexaView and zero trust
- 09 Vendor-agnostic by design
- 10 Built for IT, OT and maritime
- 11 Getting started
- 12 Where HexaView does not help, and conclusion

WHO THIS IS FOR

CISOs, heads of security operations and GRC leaders in organisations running a multi-vendor estate across IT and, increasingly, OT. Particularly relevant to ports, terminals, shipping and other critical infrastructure.

SECTION 01

The problem: more tools, less control

**Every tool is an island**

Each product has its own console, data model and alerts. Analysts switch between screens to piece together one incident.

**Visibility without action**

Most consolidation tools only read. When something needs to change, the work still happens tool by tool, by hand.

**The loop is never closed**

A policy, the control that implements it, the evidence, the detection and the test all live in different places. Proving the control works is a project, not a click.

**Cost rises, confidence does not**

More tools bring more licences, more integrations and more specialists, yet leadership still lacks one clear view of resilience.

How the estate got here

Defence in depth taught organisations to layer protection, and rightly so. Each new threat, regulation or business change brought a new specialist product. Cloud adoption, remote working and connected operational technology accelerated the pattern. The result is an estate where every individual control may be sound, but the whole is hard to see, slow to act on and difficult to evidence.

The symptoms are familiar: duplicated alerts across products, gaps between tools that no single team owns, manual evidence gathering before every audit, and board reporting assembled by hand from screenshots. None of these is fixed by buying another point solution.

The question is no longer which tool to add. It is how to make the tools you already own work as one.

SECTION 02

Cybersecurity mesh architecture in brief

Cybersecurity mesh architecture is an approach first described by the analyst firm Gartner in 2021. Its central idea is composability: instead of each security product working alone, products contribute to a shared set of foundational layers, so that they can be managed, analysed and acted on together. Protection can then follow assets, users and workloads wherever they are, rather than depending on a single network perimeter.

CSMA is an architecture, not a product. No single vendor delivers all of it, and no organisation needs to replace its estate to adopt it. In practice it is described through four supporting layers:



Security analytics and intelligence

Bring signals from many tools together, correlate them and add context, so that decisions are based on the whole picture rather than one product's view.



Distributed identity fabric

Make identity the consistent reference point across tools and environments, so access decisions and investigations follow the user, device or workload wherever it is.



Consolidated policy and posture management

Define policy once, translate it into the configuration each tool needs, and measure posture against it continuously.



Consolidated dashboards

Give every team, from analysts to the board, a single, composite view of the security estate and its effectiveness.

Our reading. Most estates already contain good tools for analytics and identity. What is usually missing is the layer that ties policy, posture and visibility together across vendors, and lets teams act from one place. That is where HexaView is focused.

SECTION 03

Defence in depth and mesh: additive, not either-or

Mesh architecture does not replace defence in depth. Layered protection is still how individual threats are stopped. Mesh adds the connective layer that makes those protections visible, consistent and provable as one estate.

ASPECT	DEFENCE IN DEPTH ON ITS OWN	DEFENCE IN DEPTH WITH A MESH LAYER
Starting point	Layers of protection around assets and networks	A shared fabric that connects the tools protecting each asset
Where control sits	In each product, configured separately	Defined once, applied through each product
Visibility	Per tool, per team	Composite view across tools and teams
Context	Limited to what one product can see	Correlated across products and environments
Response	Tool by tool, often manual	Coordinated, with approved actions across tools
Evidence for audit	Gathered by hand before each review	Captured continuously as controls run
Adding new technology	Another console to learn and run	Another source in the same shared picture
Best at	Depth of protection for specific threats	Coherence, coordination and proof across the estate

What stays the same

Your endpoint, identity, network, cloud, email and OT protections keep doing their jobs. Their owners keep their tools.

What changes

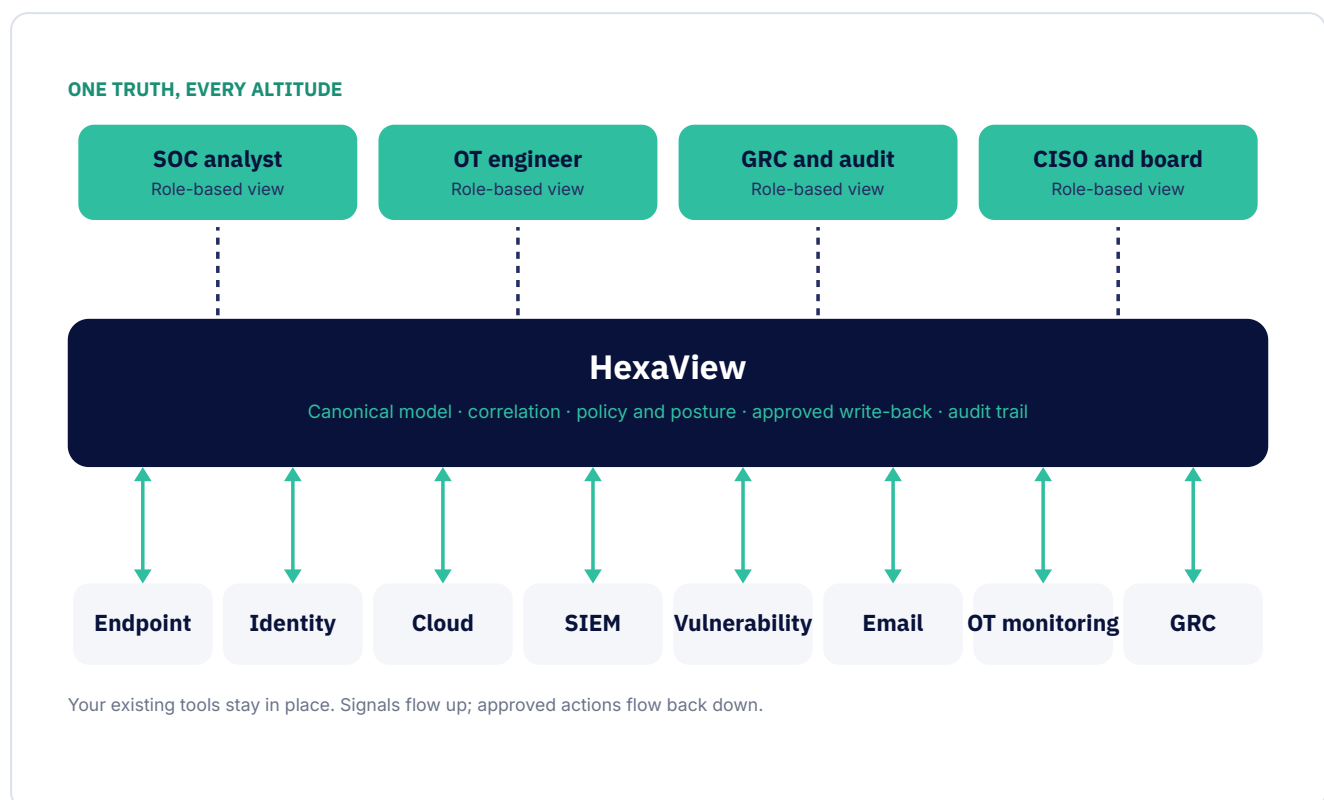
Policy, posture, visibility and coordinated response move into one shared layer, so that the estate can be run and evidenced as a whole.

SECTION 04

Introducing HexaView

HexaView is one bidirectional single pane of glass for every security tool you run, across IT and OT. Software first, with expert services when you want them.

HexaView sits above your existing tools. It brings their signals into one canonical model, presents them in role-based views, and is designed to let authorised users push approved, audited actions back into those tools from the same place. It is the layer that turns a collection of products into an estate you can run and prove.



Illustrative architecture. Connector coverage for your estate is confirmed during scoping.

SECTION 05

What HexaView does

Eight capabilities, one console. Each is designed to work with the tools you already run, and each improves as more of your estate is connected.

**One role-based view**

Every function in one place, with depth for analysts and a clear summary for leadership.

**Bidirectional by design**

Not just dashboards: enter data and push gated actions back into your tools, with approval and a full audit trail.

**The closed loop**

Policy to control, evidence, detection and validation, tracked end to end and provable in one place.

**IT and OT together**

One picture across corporate IT and operational technology, with safe, passive collection for OT.

**AI assistant**

Ask questions in plain language across your estate, with answers that cite their sources so they can be checked.

**Continuous compliance**

Controls monitored against your chosen frameworks, with evidence captured as you go rather than before each audit.

**Resilience Index**

An explainable, versioned score for the board, with the detail one click away.

**Your tools stay**

HexaView ingests their signal and adds the layer above. No rip-and-replace.

Availability. HexaView is under active development. The capabilities available for your organisation, and their timing, are confirmed during scoping. Compliance frameworks and regulatory requirements change over time; the specific frameworks in scope, and their current requirements, are confirmed and verified for your jurisdiction during onboarding.

SECTION 06

HexaView and the mesh layers

HexaView does not claim to be the whole mesh. It provides the consolidated policy, posture and dashboard layers, and connects to the analytics and identity tools you already own so that they contribute to one picture.

MESH LAYER	WHAT IT ASKS FOR	HOW HEXAVIEW SUPPORTS IT	WHAT STAYS WITH YOUR TOOLS
Security analytics and intelligence	Correlated view of signals across tools	Normalises and correlates signals from connected tools into one canonical model, with an AI assistant that cites its sources	Your SIEM, EDR and analytics engines keep detecting
Distributed identity fabric	Identity as the common reference point	Uses identity from your identity provider as a key that links users, devices and events across tools	Your identity provider and access controls keep enforcing
Consolidated policy and posture	Policy defined once, posture measured continuously	Maps policies and controls to frameworks, monitors posture and tracks each control through to evidence and validation	Each tool keeps its own configuration engine
Consolidated dashboards	One composite view for every audience	Role-based views from analyst to board, plus approved write-back so that teams can act from the same place	Tool consoles remain available for deep specialist work

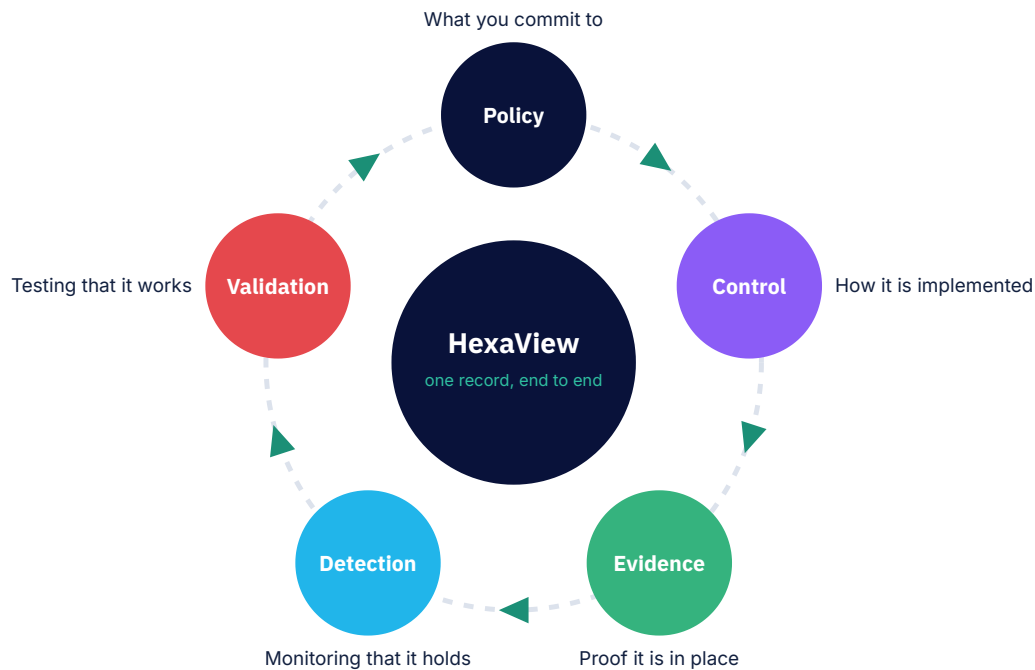
Why the dashboard layer has to be bidirectional

A consolidated dashboard that only reads is useful for reporting, but it leaves the work where it was: in each tool, done by hand. The value of the mesh comes when the shared layer can also coordinate action. HexaView is designed so that an authorised user can raise a change, route it for approval and push it to the right tool, with every step recorded. Humans own every consequential action; the platform makes it faster and auditable.

SECTION 07

Closing the loop from policy to proof

The hardest question a CISO is asked is also the simplest: does this control actually work? Answering it today usually means gathering a policy from one system, configuration from another, evidence from a third and test results from a fourth. HexaView is designed to keep that chain in one record.

**For the auditor**

Evidence on demand, linked to the control and framework it supports.

For the SOC

Detections tied to the controls they protect, so that a gap in one is visible in the other.

For the board

A resilience view built from the same record, not from a separate report.

SECTION 08

HexaView and zero trust

Zero trust and mesh architecture are often presented as rivals. They are better understood as partners. Zero trust sets the principle for access: no implicit trust, continuous verification, least privilege. Mesh architecture provides the connective layer that lets the tools enforcing that principle be managed and evidenced together.

ASPECT	ZERO TRUST	MESH LAYER (HEXAVIEW)
Philosophy	Never trust, always verify, at every access request	Connect the tools so that policy, posture and response work as one
Where it acts	Identity, device and access decisions	Across all security tools and teams
Typical tools	Identity provider, ZTNA, device management, micro-segmentation	The consolidated layer above those tools
Main question answered	Should this request be allowed?	Is our estate configured, monitored and working as intended?

How HexaView supports a zero trust programme

- ◆ **Visibility of enforcement.** See identity, device and access posture across the tools that enforce zero trust, in one view.
- ◆ **Policy to evidence.** Track each zero trust control from policy through to the evidence that it is in place and the detection that it holds.
- ◆ **Coordinated response.** When something needs to change, raise it once and route it, with approval, to the tool that enforces it.
- ◆ **Progress the board can follow.** Report zero trust maturity from the same record the operational teams use.

What HexaView is not. HexaView does not replace your identity provider, ZTNA service or access controls, and it does not make access decisions itself. It makes the tools that do visible, coordinated and provable.

SECTION 09

Vendor-agnostic by design

Organisations choose the best product for each job, and they should keep that freedom. HexaView is vendor-agnostic: it works with the tools you have chosen rather than steering you towards one supplier's ecosystem. When a tool is replaced or a new one added, it becomes another source in the same picture, without retraining every team on another console.

Your tools stay. HexaView adds the layer above.

Architecture principles

**Credentials do not centralise**

Tool credentials stay close to the tools, so a compromise of the control plane does not hand over every connected product.

**Data where you need it**

Designed so that data can stay in your jurisdiction and your cloud, for regulated and sovereign organisations.

**Processing at the edge**

Heavy ingestion and normalisation run near the data, rather than in one central bill.

Deployment options

Hosted

Fastest to start. We host and run it; you sign in.

Dedicated

Your own single-tenant instance for stronger isolation.

Customer cloud

The data plane runs in your cloud. Credentials and raw data stay with you.

Isolated

For the most sensitive OT and sovereign environments.

Deployment availability and timing are confirmed for each organisation during scoping.

SECTION 10

Built for IT, OT and maritime

Critical infrastructure estates are not just corporate IT. Ports, terminals and fleets run operational technology that cannot be scanned aggressively or taken offline, alongside shore systems that face the same threats as any enterprise. HexaView is designed to give one picture across both, so that a risk crossing from shore to ship, or from IT to OT, is visible to everyone who needs to act.

**Vessel**

Bridge, engine and cargo systems, and ship-to-shore links

**Terminal**

Quay and yard equipment, gate and access, terminal power

**Shore**

Corporate IT, fleet IT, identity and the ISMS

Site by site and vessel by vessel, in one pane. OT collection is passive and safe-by-design.

The right depth for every role

ROLE	WHAT HEXAVIEW GIVES THEM
SOC analyst	Full case depth and live investigation. One console instead of many.
OT engineer	Asset and continuity view. Safe and passive, no disruption to operations.
GRC and audit	Controls, evidence and reporting on demand, mapped to your frameworks.
CISO and board	A resilience score and a summary they can read, with detail one click away.

**CyberDockside.ai**

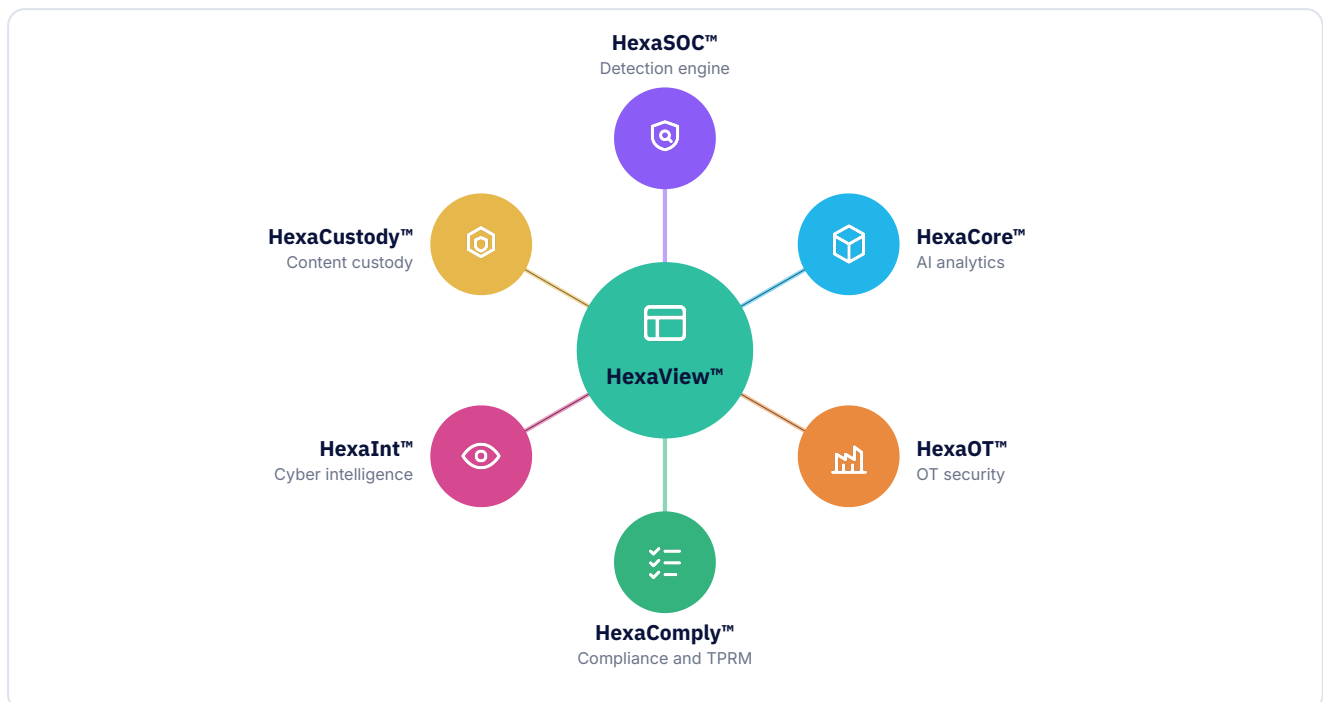
Why CyberDockside.ai. CyberDockside.ai brings maritime and port-sector context to every HexaView engagement, so that what is configured reflects how vessels, terminals and shore teams actually operate.

SECTION 11

One pane for the wider HexaShield ecosystem, and getting started

HexaView works with your own tools on its own. When you also use HexaShield services, each one feeds the same pane, so the intelligence compounds rather than arriving as another report.

Attach any service to your HexaView licence: managed detection and response, OT security, compliance as a service and third-party risk, cyber intelligence and content custody.



Getting started

1

Discover

Your estate, your obligations and what you need to evidence

2

Scope

Connectors, roles
and outcomes
agreed for a
defined scope

3

Prove

A time-boxed proof
of value on your
own estate, before
any wider
commitment

4

Roll out

Site by site and, for maritime, vessel by vessel, in one pane

SECTION 12

Where HexaView does not help, and conclusion

Naming the limits

- ◆ HexaView does not replace your detection, identity, endpoint or OT monitoring tools. It depends on them, and its value grows with the number of tools connected.
- ◆ It does not fix a misconfigured tool on its own. It makes the misconfiguration visible and routes the change, with approval, to the people who own it.
- ◆ Connector coverage varies by product and version. Coverage for your estate is confirmed during scoping, not assumed.
- ◆ It is not a substitute for skilled people. Humans own every consequential action; HexaView makes their work faster, coordinated and auditable.

Conclusion

Security estates will keep growing, and they should: new risks need new protections. What has to change is how those protections are run. Cybersecurity mesh architecture points the way, and its value depends on a shared layer that can see across every tool, act through them with control, and prove the result.

HexaView is built to be that layer: one bidirectional single pane of glass across IT and OT, above the tools you already trust, delivered with HexaShield's services when you want them and with CyberDockside.ai's maritime insight where it matters.

See it. Prove it. Secure it.

Book a working session on your own estate: we map your tools, your obligations and the views each team needs.

[REQUEST AN EXECUTIVE BRIEFING](#)[TALK TO A SPECIALIST](#)

HexaShield

hexashield.io · hello@hexashield.io
+44 7445 033229

CyberDockside.ai

cyber.dockside.ai ·
remie.kalloe@cyber.dockside.ai
+316 55943820

Notes. Cybersecurity mesh architecture is described here in HexaShield's own words; the term was introduced by Gartner, Inc. in 2021, and this paper is not endorsed by Gartner. Product capabilities describe HexaView's design; availability and timing are confirmed for each organisation during scoping. Interface and architecture visuals are illustrative. HexaView™, HexaSOC™, HexaCore™, HexaOT™, HexaComply™, HexaInt™ and HexaCustody™ are trademarks of HexaShield. Other names may be trademarks of their owners.