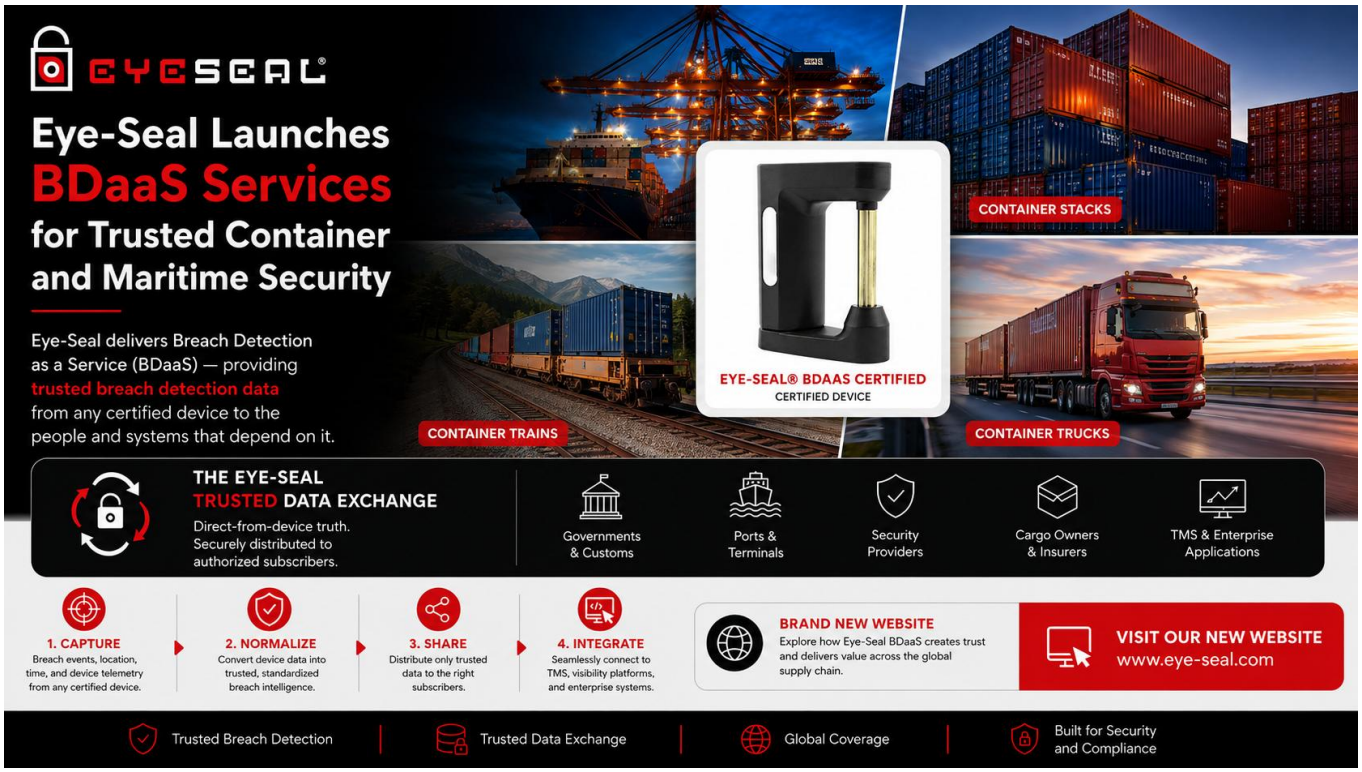
EYESEAL®

— BREACH DETECTION AS A SERVICE

Building a Trusted Global Breach Detection Service

How Eye-Seal BDaaS turns cargo tampering, theft and unauthorized access into trusted, actionable events for cargo owners and the global trade ecosystem.



The core idea

A breach alert becomes more valuable when every authorized party can trust what happened, when it happened, where it happened, and which cargo movement was affected.

Trusted Breach Detection. Trusted Data Exchange. Trusted Supply Chains.

EYESEAL®

— WHY TRUSTED BREACH DETECTION MATTERS

From device alert to trusted evidence

Global cargo moves across carriers, ports, terminals, borders, warehouses, rail corridors and roads. Security evidence is often fragmented across devices, vendors and applications. Eye-Seal BDaaS creates a common trust layer: ingest breach and tamper signals from certified devices, normalize them into a consistent event record, and securely deliver that record to authorized subscribers and systems.

A raw device message is not yet a trusted business event. It becomes operationally valuable when the receiving organization can understand its source, timing, location, context and delivery path.

1. CAPTURE	2. NORMALIZE	3. TRUST	4. SHARE
Receive breach, tamper, unauthorized opening, location and device telemetry from an Eye-Seal Certified device.	Convert different device messages into a common event model with time, location, device identity and shipment/container context.	Apply controlled device onboarding, secure routing, event integrity and auditable delivery so the event can be relied upon.	Deliver the event in parallel to authorized cargo owners, logistics providers, customs, ports, security teams and applications of record.

Why “trusted” changes the value proposition

Confidence in the event. The recipient is not simply consuming an alert; it is receiving a standardized breach record tied to an approved device identity and controlled data path.

Confidence in the timing and location. A trusted event anchors the breach to when and where it occurred, improving investigation, exception management and chain-of-custody decisions.

Confidence in distribution. The same event can be delivered to multiple authorized subscribers without relying on manual forwarding, screenshots or disconnected integrations.

Confidence across borders and systems. A common trust model reduces the need for every port, government agency, TMS or cargo owner to create a separate proprietary integration to every device vendor.

A global trust layer

The strategic value of BDaaS is not only breach detection. It is the ability to establish a repeatable, device-agnostic way to trust and exchange breach evidence across the cargo journey.

EYESEAL®

— CARGO OWNER USE CASES AND VALUE

Protect the shipment - and improve the response

Cargo owners ultimately bear much of the financial and operational impact of theft, contamination, unauthorized access, pilferage, diversion and cargo integrity failures. BDaaS gives the cargo owner a direct, trusted signal that can be used to drive decisions rather than simply add another tracking dashboard.

Use Case	BDaaS Role	Cargo Owner Value
Unauthorized container opening	Detect an unexpected opening or seal breach and immediately establish time and location evidence.	Faster response; clearer accountability; improved claims and investigation evidence.
Theft and pilferage	Flag container access during vulnerable dwell, transfer or inland movement.	Reduce time-to-awareness and support targeted intervention.
Cargo contamination / illicit insertion	Identify access to a secured container after packing or during transit.	Support supply-chain integrity programs and create evidence for security and customs review.
High-value / sensitive cargo	Add independent breach intelligence to existing visibility and security controls.	Strengthen risk management without replacing the cargo owner's existing TMS or visibility platform.
Trade-lane exception management	Compare breach events with planned route, port, terminal and handoff context.	Focus teams on meaningful exceptions rather than continuously watching location dots.
Claims, insurance and audit	Preserve a time- and location-aware breach record for post-event review.	Improve evidence quality and reduce ambiguity around where a security exception occurred.

The cargo owner value proposition

- Independent breach evidence that can complement carrier and visibility data.
- One normalized security event model across certified device types.
- Alerts can flow directly to the cargo owner while also being shared with authorized ecosystem partners.
- No requirement to replace the cargo owner's application of record; BDaaS can feed TMS, visibility, risk and trade platforms in parallel.
- A foundation for risk scoring, security analytics and lane-level performance over time.

— VALUE ACROSS THE CARGO ECOSYSTEM

One trusted event - many authorized beneficiaries

Cargo security is inherently multi-party. A single breach may matter simultaneously to the shipper, logistics provider, port, customs authority, insurer and security team. A trusted global service becomes more valuable as more authorized stakeholders can consume the same objective event without duplicating device integrations.

Cargo owners / shippers	Direct awareness of breach and tamper events; stronger chain-of-custody evidence; faster exception decisions.
Freight forwarders / logistics providers	A differentiated security service for customers and a normalized security feed across modes and trade lanes.
Ports / terminals	Earlier knowledge of security exceptions entering or occurring within controlled facilities; improved coordination with cargo owners and agencies.
Customs / government	A trusted external breach signal that can support risk assessment, inspection prioritization, authorized-trader programs, customs fast-lane concepts, VAT-loss reduction initiatives and next-generation digital cargo systems.
Security providers / law enforcement	Time- and location-specific events that can accelerate triage and focus investigative resources.
Insurers / risk providers	More objective event evidence and the potential to support improved risk segmentation, claims analysis and loss-prevention services.
TMS / visibility / trade applications	A standardized breach event feed that enriches existing operational data without forcing the application to certify and integrate every device independently.
Certified device partners	A neutral certification and trust path to global markets. Eye-Seal does not pick device winners or dictate use cases; manufacturers of one-time connected bolt seals, multi-use smart locks, smart labels and other breach-detection devices can certify to a common trust model and participate in the BDaaS ecosystem.

Network effect of trust

The more organizations that recognize a common breach event, the more useful the service becomes. Cargo owners gain broader protection, applications gain a simpler integration model, and government stakeholders can consume consistent evidence without being tied to a single hardware vendor.

EYESEAL®

— THE CASE FOR A TRUSTED GLOBAL BREACH DETECTION SERVICE

From fragmented alerts to global cargo trust

The long-term opportunity is a trusted breach-detection layer for global trade: device-agnostic at the edge, standardized at the event layer, secure in transit, and governed by subscriber authorization. Trust also means working with trusted industry partners. Through Eye-Seal's collaboration agreement with Deloitte Global Tax & Trade in Brussels, Eye-Seal is helping advance Port and Custom Fast Lanes, Government VAT-loss reduction, and enhancing next-generation digital trade platforms.

CERTIFIED DEVICE	TRUSTED INGESTION	NORMALIZED EVENT	AUTHORIZED EXCHANGE	SUBSCRIBERS & APPS
Breach / tamper / access	Known identity + controlled route	Time + location + context	Policy-based distribution	Action + record + analytics

What "global trusted" should mean in practice

Device trust: Eye-Seal is not a device company. It certifies qualified third-party technologies to a common trust framework - from trusted one-time bolt seals, to trusted multi-use smart locks, trusted smart labels and emerging breach-detection devices. Certification addresses device identity, firmware/security, telemetry and data routing.

Data-path trust: Events use controlled connectivity and routing into the Eye-Seal platform rather than uncontrolled device-to-recipient paths.

Event trust: Different device messages are converted into a common, auditable breach event model.

Subscriber trust: Only approved parties receive the information they are authorized to consume.

Application trust: Enterprise and government systems can consume one normalized service interface instead of a growing number of untrusted point integrations.

Operational trust: The service produces evidence that can be used consistently across security, claims, compliance, risk and operational workflows.

Strategic outcome

A trusted global breach detection service can become a neutral security layer across trade lanes - allowing cargo owners to protect shipments, technology providers to simplify integration, and authorized public-sector stakeholders to consume consistent breach evidence at scale.

Conclusion

Eye-Seal BDaaS turns physical breach signals into trusted, shareable evidence. Certified third-party devices detect events; Eye-Seal provides the trust layer; and trusted global partners extend that evidence into cargo security, customs, tax, risk and digital-trade workflows.

Trusted Breach Detection. Trusted Data Exchange. Trusted Supply Chains.