Harbour Mastery®

i-Intermodal for NetSuite

Securing the Global Intermodal Supply Chain Future

How Oracle NetSuite + Harbour Mastery Are Redefining Surveillance, Crisis Prevention, and resilience for Ports and Multimodal Hubs

Walk into any modern seaport or intermodal terminal, and you can feel the tension between scale and fragility.

Global seaborne trade reached about **12.3 billion tons in 2023, growing 2.4% year over year**, and is expected to keep rising—though more slowly and with far more volatility than in the past.[1]

Yet the networks that move this cargo—ships, ports, rail, road, depots—are being stretched by geopolitics, cyber threats, and climate pressure.

900%

Increase in attacks targeting ships and port systems over a three year period.

In that environment, surveillance and crisis prevention can't be an afterthought or a patchwork of cameras and spreadsheets. They have to be built into the same digital backbone that runs port operations and multimodal logistics day to day. This has to be your Security Backbone as well.

That's the opportunity behind pairing Oracle NetSuite + Harbour Mastery Maritime for NetSuite— a maritime ERP built natively inside NetSuite that includes i-Seaports and i-Multimodal for NetSuite—with the AI capabilities emerging in NetSuite Next.[9]

A Risk Picture That's Getting Sharper—and Darker

The list of risks facing ports and intermodal corridors is now uncomfortably long: ransomware, GPS spoofing, insider threats, physical intrusion, extreme weather, labor disruption, and geopolitical chokepoints that can shift overnight.

Built for ORACLE NetSuite Native SuiteApp

> “Not since the closure of the Suez Canal in 1967 have we witnessed such sustained disruption to the arteries of global commerce.”[2]
>
> *Rebeca Grynspan – UNCTAD Secretary-General*

Several trends stand out:

- **Attacks are rising and getting more sophisticated.** An Atlantic Council study noted a **900% increase in attacks targeting ships and port systems over a three-year period,** highlighting how aggressively cyber actors are probing maritime infrastructure.[3]

- **Transport is now a prime target for ransomware.** ENISA’s work on the transport threat landscape shows that ransomware incidents reported in the transport sector nearly doubled in one year, jumping from **13% of reported cyber incidents in 2021 to 25% in 2022.**[4][6]

- **One port’s bad day can ripple globally.** In July 2023, a ransomware attack hit **Japan’s Port of Nagoya**, the country’s largest. Container operations were halted when the central terminal system went down, forcing a shutdown that lasted more than two days and even disrupting Toyota’s export packaging line.[5][7]

None of this is hypothetical anymore. A single compromised terminal operating system or gate-control platform can quickly become a **full-blown intermodal crisis**: ships idling at anchor, trains re-routed or delayed, trucks backed up onto city streets, and customers escalating all at once.

100%

Increase in ransomware attacks on transport in one year

Why Traditional “Security Systems” Aren’t Enough

Most ports and intermodal operators already have:

- CCTV and access control
- A patchwork of physical security procedures
- A terminal operating system (TOS)
- Separate finance, billing, contracts, and customer systems
- Stand-alone incident logs in email or spreadsheets

The problem isn’t a lack of tools—it’s the **lack of a coherent, shared picture.** The data that matters to security lives in different silos:

- Vessel calls, berths, and cargo services
- Trade contracts, guarantees, and leases
- Hazardous cargo and high-value shipments
- Gate moves, rail and truck handoffs, and yard operations
- Incident reports, mooring records, and patrol findings

When an incident hits, people scramble between systems and phone calls trying to piece together what’s really happening and who’s affected. That slows response and makes it harder to prevent a local disruption from becoming a bigger crisis.

The answer isn’t just more cameras or another monitoring screen. It’s **a new technology platform that treats operations, finance, and security as one connected environment.**

Oracle NetSuite + Harbour Mastery: A Maritime ERP Built for Intermodal Reality

This is where **Harbour Mastery Maritime for NetSuite** comes in—a suite of maritime industry applications built natively inside Oracle NetSuite, not bolted on as separate systems[8][9], eliminating another point of vulnerability.

"Homeland Security in every country must focus on ports of entry which involves the same basics down through History – to get the most accurate information and intelligence possible and then direct the resources they have to help their allies, and STOP by whatever means necessary, their enemies, be they criminal or terrorists. Harbour Mastery's internet-based solutions' goal is early and accurate information to aid legitimate commerce and help security forces to stop illegal threats." [11]

Walt Viglienzone – Captain USCG (Ret) and former Dean of the USCG Academy

Key components include:

- **i-Seaports for NetSuite** – A comprehensive ERP layer for vessel and cargo logistics, agent services, cruise and passenger flows, trade contracts, and real estate/terminal leasing, all built inside NetSuite.[8]
- **i-Multimodal for NetSuite** – A maritime module that extends the platform across terminals, freight forwarding, and intermodal cargo logistics—covering reservations, service requests, terminal operating functions, and associated financials, all natively within NetSuite.[8]

Because everything is **built into NetSuite's data model**, you get **one native environment** that ties together:

- Vessel calls, berths, and services
- Cargo and terminal operations
- Contracts, tariffs, leases, and guarantees
- Invoices, revenue, and collections
- Intermodal moves—rail, road, and storage

That single source of truth isn't just an accounting advantage. It's the foundation for real intermodal surveillance and crisis prevention:

- Security teams can see which high-risk vessels, cargoes, and customers are on the water, in berth, in yard, or in transit.
- Incident alerts can be tied directly to affected vessels, terminals, contracts, and financial exposure.
- Harbour police, port operations, and finance are working from the same facts, not competing spreadsheets.

Ports already using this stack are seeing the impact. A Port Tampa Bay testimonial sums it up:

"Port Tampa Bay is growing 5–10% per year – without adding employees, and we are now getting much more done with greater accuracy, ROI, and customer satisfaction using NetSuite and Harbour Mastery's i-Seaports Management."[8]

And for the Port of Lake Charles, one of the U.S.'s busiest port districts, the decision to move to Harbour Mastery + NetSuite was explicitly about building a platform for the future.

That same platform is precisely what's needed for smarter surveillance and crisis prevention.

What NetSuite Next Adds—and Where AI Actually Helps

Oracle's NetSuite Next initiative adds AI-native capabilities onto this built-in ERP backbone, centered around a conversational assistant called Ask Oracle. NetSuite describes Ask Oracle as a natural-language layer that lets users search, navigate, analyze, and act across the entire NetSuite dataset using everyday language.[9]

Evan Goldberg, Founder and EVP of Oracle NetSuite, says it this way:

"NetSuite Next puts AI to work for businesses by making it a natural extension of the way they already work."[9]

For ports and intermodal operators running i-Seaports and i-Multimodal, that opens up efficient possibilities without turning security over to a black box:

- **Faster anomaly spotting.** Ask Oracle can help surface unusual vessel calls, cargo patterns, or gate activity compared to historical norms—flagging potential fraud, smuggling risk, or operational issues for human review.[9]
- **Richer incident context.** When something goes wrong—a cyber alert on the TOS, a suspicious mooring event, a hazardous spill—AI-driven workflows can automatically assemble affected vessels, cargoes, contracts, and customers from the shared data model.
- **Predictive risk and resilience.** Combining operational data from i-Seaports and i-Multimodal with AI models enables forecasting of congestion, equipment stress, or staffing bottlenecks so issues are prevented rather than merely reacted to.[3][6]

> “By combining Harbour Mastery’s maritime expertise and functionality, and NetSuite’s integrated cloud business system, the port will be able to achieve new levels of efficiency and innovation – helping to set the stage for a smarter, more agile future.”[8]
>
> *George Walters – CEO of Harbour Mastery*

The point isn’t to shout “AI” in every sentence. It’s to quietly **reduce noise, surface the right signals, and give people better information** when it matters.

Keeping It Human: Technology as an Enabler, Not a Replacement

For all the technology, security, and crisis prevention, it still comes down to people: harbor masters, terminal managers, marine pilots, tug operators, operations personnel, security officers, customs officials, and local emergency services.

A modern platform should:

- Give each role a clear, role-based view of the same underlying reality
- Eliminate double entry and manual reconciliations that waste time and hides risk
- Make it easy to share critical situational awareness quickly when incidents occur

That’s ultimately what Oracle NetSuite + Harbour Mastery Maritime for NetSuite offers: a maritime-native ERP built inside NetSuite that unifies the supply chain comprised of seaports, marinas, and multimodal truck and rail operations, and is ready to take advantage of the AI capabilities emerging in NetSuite Next—without losing human judgment at the center.[8][9]

In a world where a single cyber incident or chokepoint disruption can ripple through the global economy, the question for port and intermodal leaders is no longer whether to modernize their surveillance and crisis-prevention capabilities.

The real question is how quickly they can move to a platform that treats security as part of the core business—not an afterthought on the edge of the network.

For more about Harbour Mastery visit https://harbourmastery.com/

References

1. **UNCTAD** – Global trade volumes (2023/24) United Nations Conference on Trade and Development. Review of Maritime Transport 2024: Navigating Maritime Chokepoints. UNCTAD, 22 Oct. 2024, unctad.org/publication/review-maritime-transport-2024.
2. **UNCTAD** – Ongoing disruption & Suez-level comparison United Nations Conference on Trade and Development. Review of Maritime Transport 2025: Staying the Course in Turbulent Waters. UNCTAD, 24 Sept. 2025, unctad.org/publication/review-maritime-transport-2025.
3. **Atlantic Council** – Maritime cyber risk growth Loomis, William, et al. Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity. Atlantic Council, Oct. 2021, www.atlanticcouncil.org/in-depth-research-reports/report/raising-the-colors-signaling-for-cooperation-on-maritime-cybersecurity/.
4. **ENISA** – Ransomware rising from 13% to 25% in transport European Union Agency for Cybersecurity. “Understanding Cyber Threats in Transport.” ENISA, 21 Mar. 2023, www.enisa.europa.eu/news/understanding-cyber-threats-in-transport.
5. **Nagoya port ransomware incident** “Toyota to Suspend Packaging Line after Cyberattack on Japan Port.” Reuters, 6 July 2023, www.reuters.com/business/autos-transportation/japans-biggest-port-plans-resume-operations-thursday-after-cyberattack-2023-07-06/.
6. **ENISA** – Transport Threat Landscape (deeper stats on transport cyber) European Union Agency for Cybersecurity. Transport Threat Landscape. ENISA, 2023, www.enisa.europa.eu/publications/transport-threat-landscape.
7. **Technical analysis of Nagoya cyber incident** (replacement for Harbour Mastery datasheet) Dragos, Inc. “OT Cybersecurity Breach Disrupts Operations at the Port of Nagoya, Japan.” Dragos, 2023, www.dragos.com/blog/ot-cybersecurity-breach-disrupts-operations-at-the-port-of-nagoya-japan/.
8. **Port of Lake Charles selects Harbour Mastery + NetSuite** (Walters quote) “Port of Lake Charles Selects Harbour Mastery and NetSuite to Transform Its Maritime Operations.” PR Newswire, 29 Jan. 2025, www.prnewswire.com/news-releases/port-of-lake-charles-selects-harbour-mastery-and-netsuite-to-transform-its-maritime-operations-302363026.html.
9. **NetSuite Next & Ask Oracle** (Evan Goldberg quote, AI description) Oracle NetSuite. “NetSuite Next: ERP with AI Capabilities.” NetSuite, 2025, www.netsuite.com/portal/products/netsuite-next.shtml.
10. **Global maritime system quote** (Horizon Lines CEO) Raymond, Charles G. “World Trade Security Is Imperative and Attainable: Cooperative Effort, U.S. Leadership Are Necessary.” TR News, no. 246, Sept.–Oct. 2006, pp. 18–19, onlinepubs.trb.org/onlinepubs/trnews/trnews246.pdf
11. **Walt Viglienzone Captain USCG (Ret), Pensacola, FL** – Harbour Mastery Inc. Advisor on security functionality of its products, 2004 to date.