AMAROK
ULTIMATE PERIMETER SECURITY

From Cyber to Cargo: Closing Security Gaps at the Port Perimeter

PROUD MEMBER OF THE:

AAPA
ESSENTIAL. RESILIENT. UNITED.
SEAPORTS DELIVER

MEET AMAROK

The Ultimate Perimeter Security Company

AMAROK proudly provides perimeter security to over 8,500+ commercial and industrial businesses across North America. Our solar-powered, electric fence and other security solutions stop theft before it happens.

SOLUTIONS WE OFFER – TAILORED TO YOUR SECURITY NEEDS:

- Video Surveillance
- Electric Fencing
- Security Enhancements

Unlock **99%** **theft prevention** post installation with AMAROK

CONTACT US:

800.632.4391

sales@amarok.com

www.amarok.com

AAPA NEW MEMBERS

Meet Your Presenters

Keith Schoffstall
National Accounts Director – Vehicle Logistics & Port Authorities

John Armstrong
Vice President | Outside Sales

OUR PURPOSE

EDUCATIONAL

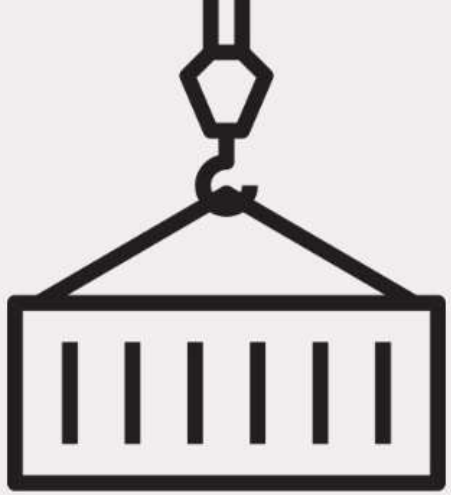
& Conversational

OUR COMMITMENT is to help ports build proactive, scalable security frameworks that protect continuity, safety, trust, and long-term operational confidence.

POLL 1

WHICH AREA REPRESENTS THE BIGGEST SECURITY GAP AT YOUR PORT TODAY?

- ❑ Perimeter protection
- ❑ Detection & verification
- ❑ Guard response coordination
- ❑ Cyber resilience
- ❑ Unsure / Haven’t assessed recently



Freight shipment theft costs the U.S. economy up to

$35 billion

per year.

Source - Freight Under Fire: The Explosive Rise of Cargo Theft, n.d. American Trucking Associations. https://www.trucking.org/

AMAROK
ULTIMATE PERIMETER SECURITY

THE AVERAGE LOSS VALUE ACROSS ALL INCIDENTS WAS

$115,230

WHICH IS

83%

HIGHER THAN THE FIRST HALF OF 2023 AVERAGE

30%

OF ALL CARGO THEFTS TAKE PLACE BETWEEN

12-6PM

37%

OF CARGO THEFTS TAKE PLACE ON

MONDAYS & FRIDAYS!

CARGO THEFTS UP 49% AT FREIGHT HUBS

POSITION

The Role of Safety in Port Security

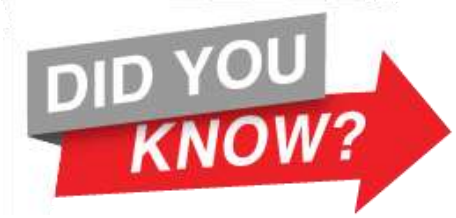
Security and safety are deeply connected. A secure perimeter reduces:

Confrontations between guards and intruders.

Liability exposure related to on-site harm.

Safety incidents tied to panic response and rushed shutdowns.

The emotional and psychological stress placed on personnel.



When safety and security are aligned, the port is not only harder to breach, but also a healthier, more predictable environment for the workforce.

POLL 2

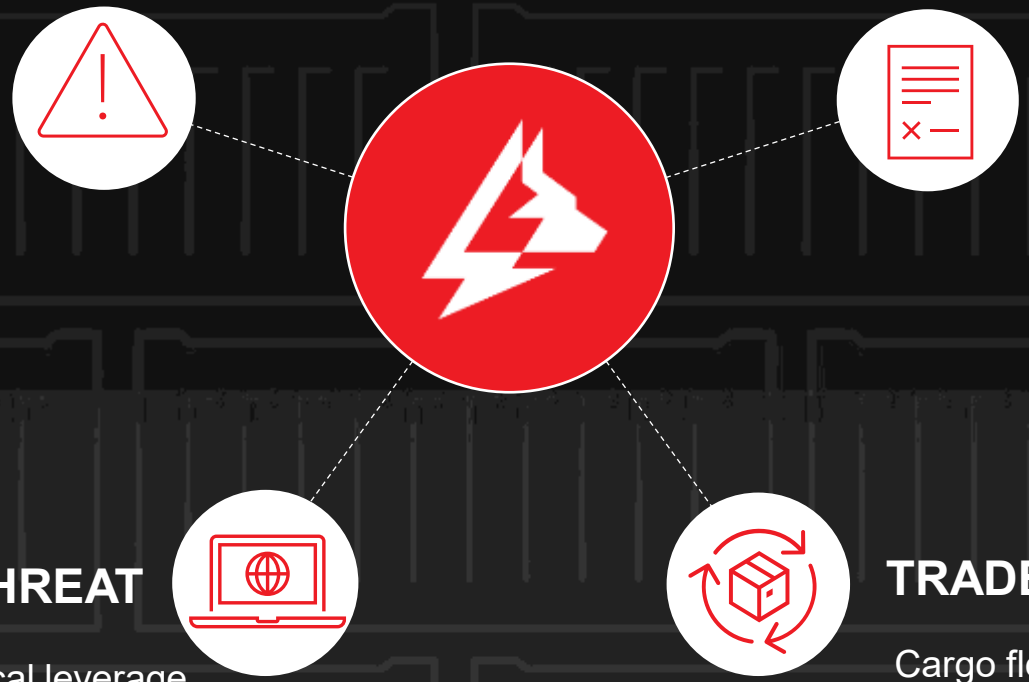
WHICH THREAT IS MOST CONCERNING FOR YOUR PORT OVER THE NEXT 12 MONTHS?

- ❑ Physical intrusion
- ❑ Cyber breach
- ❑ Regulatory pressure
- ❑ Workforce strain / safety events
- ❑ Throughput disruption

SITUATION

Current Risk Landscape

These risks are interconnected. A breach — whether physical or cyber — can disrupt throughput, slow vessel operations, delay transfers, impact OEM agreements, and trigger insurance scrutiny.



PHYSICAL THREAT

Organized theft groups and opportunistic intrusion attempts are increasing across multiple port regions.

REGULATORY PRESSURES

The U.S. Coast Guard cybersecurity rule requires incident reporting, cybersecurity plans, Cybersecurity Officers, and documented response protocols.

CYBER THREAT

Ports are now targeted due to the logistical leverage they hold. NATO has warned that state-linked actors are actively probing port infrastructure.

TRADE & TARIFF VOLATILITY

Cargo flow instability places pressure on ports to operate efficiently under changing conditions.

ASSESSING THE RISKS

Port Security Risk Analysis: A Proactive Approach

Ports are critical infrastructure with constant exposure to theft, breaches, and operational disruption. Even with existing security measures, vulnerabilities can exist due to location, layout, and asset concentration.

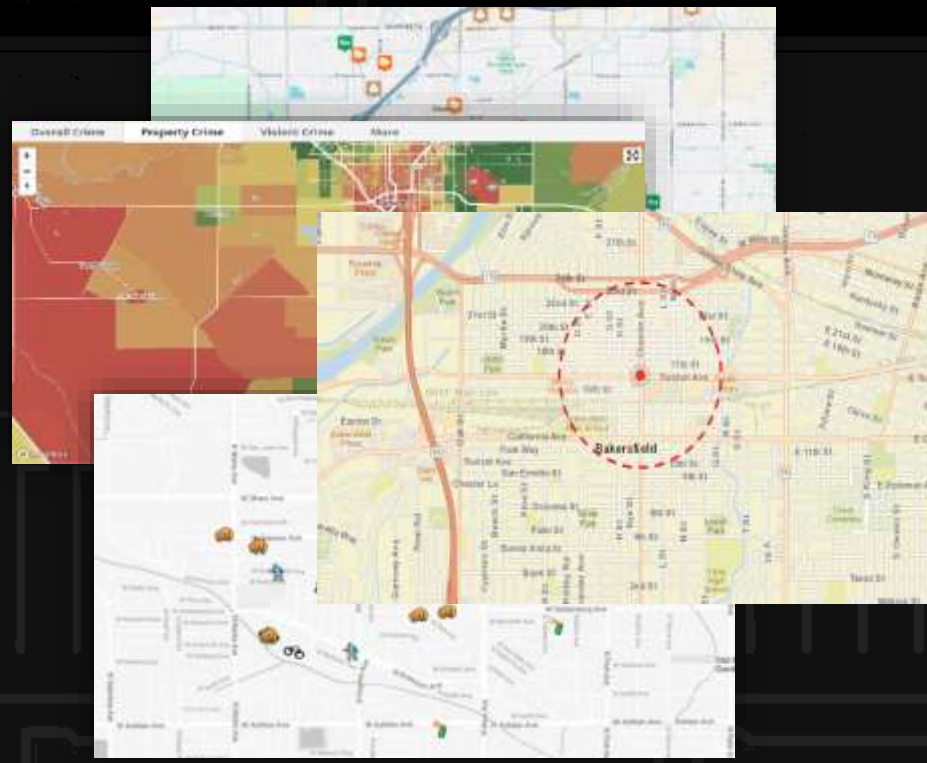
A Port Security Risk Analysis provides a clear understanding of perimeter risks and security gaps **before** incidents occur.

Key Risk Factors Evaluated:

- Local and regional cargo theft and crime trends
- Facility layout, acreage, and access points
- Adjacent land use, rail lines, and roadways
- Lighting, visibility, and line-of-sight conditions
- History of theft or attempted breaches
- Type and value of cargo and equipment
- Existing security investments (guards, cameras, alarms)
- Condition and effectiveness of perimeter fencing

☑ KNOW YOUR CRIME RATE

AMAROK Example:



Other Local Crime Risk Tools:

- CrimeGrade.org
- SpotCrime.com
- CommunityCrimeMap.com
- CrimeMapping.com

EXAMPLE

Reflect and Act

A widely recognized waterfront in the Pacific Northwest demonstrated something critical. **Layered security cannot merely exist** — it must function as an integrated system.

In that case:

→ Cameras were recording but **not actively detecting**.
→ Guards were present, but **stretched and reactive**.
→ Perimeter controls existed, but **coverage was inconsistent**.

SECURITY CANNOT BE REACTIVE. IT MUST BE PROACTIVE, MONITORED AND SCALABLE.

Increased Delays

Insurance Escalation

Workforce Concerns

Public Attention

OEM Pressure

WAKE UP CALL

Once trust and operational confidence are shaken, they take **YEARS** to rebuild.

RECOMMENDATION

A layered approach **protects** people, cargo, and continuity by **reinforcing** each stage of detection and response.

LAYERED SECURITY

1. **Perimeter Deterrence & Delay**
2. **Detection & Verification**
3. **Response Coordination & Documentation**
4. **Cyber Resilience & Network Integrity**

When these layers reinforce each other, ports gain:

Faster detection, lower guard strain, fewer safety confrontations, reduced operational downtime, stronger compliance, and insurance posture.

REAL-LIFE EXAMPLES

Case-Based Outcomes

A vehicle processing environment achieved a 38% reduction in guard patrol dependency, freeing staff to focus on high-value response and safety compliance checks.

A multi-terminal operator improved incident verification speed, reducing false dispatch and improving response coordination accuracy.

A port operator documented layered security improvements that strengthened insurance positioning and satisfied OEM risk standards.

These are not hardware achievements—**they are operational and safety gains.**

WHAT'S NEXT?

Get Ahead Of The "What If's"

What If?

- **What if** your port could reduce guard patrol strain and reassign staff to strategic safety oversight?
- **What if** one intrusion disrupted operations for 24 hours – what is the real cost in continuity and trust?
- **What if** layered security reduced your insurance and liability exposure?
- **What if** proactive protection prevented incidents before they reached critical operational zones?

POLL 3

HOW OFTEN DOES YOUR PORT EVALUATE OR UPDATE PERIMETER SECURITY PROTOCOLS?

- ❑ Quarterly
- ❑ Annually
- ❑ Only after an incident
- ❑ Not sure

NEXT STEPS

Practical Playbook – How Ports Begin

STEP 1

Identify perimeter pressure points; especially low-visibility or rail-adjacent zones.

STEP 2

Evaluate how guard resources are allocated, look for patrol roles that could shift into high-value response readiness.

STEP 3

Conduct Risk/Threat Evaluations

This approach is actionable *without* procurement or equipment decisions.

NEXT STEPS

Practical Playbook – How Ports Begin -

STEP 4

Use Compliance Guidelines like MARSEC

STEP 5

Leverage PSGP Funding

STEP 6

Align security success metrics to operational KPIs: Throughput protection, safety conditions, risk score improvement, downtime avoidance

This approach is actionable *without* procurement or equipment decisions.

OUR POSITION

AMAROK is not here to replace your guard forces.

We are here to strengthen operational resilience, layered awareness, and safety coordination across ports.

We recognize the unique complexity of port environments. Safety, logistics, throughput, workforce, and regulatory stability are all interdependent.

OUR COMMITMENT is to help ports build proactive, scalable security frameworks that protect continuity, safety, trust, and long-term operational confidence.

THANK YOU!

Q & A

AMAROK
ULTIMATE PERIMETER SECURITY

Contact Us For Your FREE Port Security Risk Analysis

sales@amarok.com

amarok.com/threat-assessment

AAPA NEW MEMBERS

Connect With Us!

Keith Schoffstall
kschoffstall@amarok.com
443.257.3527
Connect with me

John Armstron
jarmstrong@amarok.com
916.201.728
Connect with m