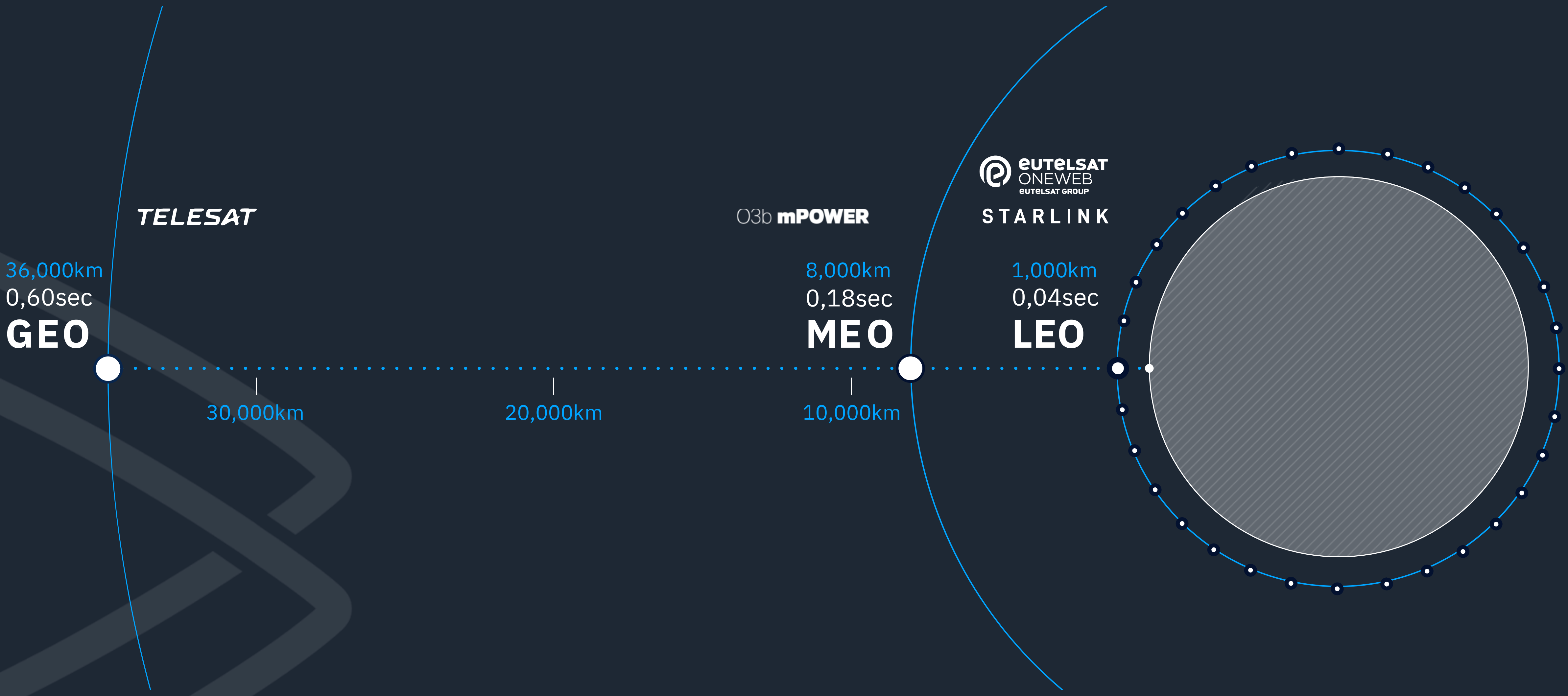
OMNIACCESS

27th ERVO

27th ERVO Meeting

Comms & Cyber Refresher

GEO / MEO / LEO


TELESAT
36,000km
0,60sec
GEO
O3b mPOWER
8,000km
0,18sec
MEO
eutelsat ONEWEB eutelsat group
STARLINK
1,000km
0,04sec
LEO
30,000km
20,000km
10,000km

Closer to Earth than ever before

New Orbit

Our satellites fly at Ultra Low Earth Orbits, 180 km above the Earth's surface, a third of the altitude of conventional Low Earth Orbit satellites.

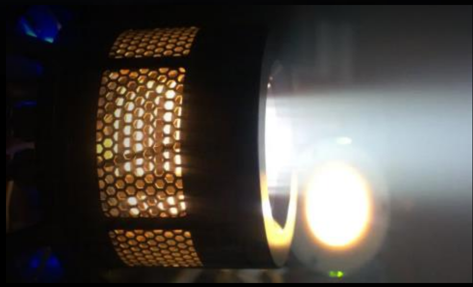
Metric	NEO1	Standard LEO
Altitude	180km	600km
Satellite lifetime	5 years	5 years
Native image resolution*	0.2m	0.72m
Direct-to-phone throughput	Web browsing & video streaming	Voice & message

70kg payload mass

300W payload power

1.1 Gbit/s downlink speed

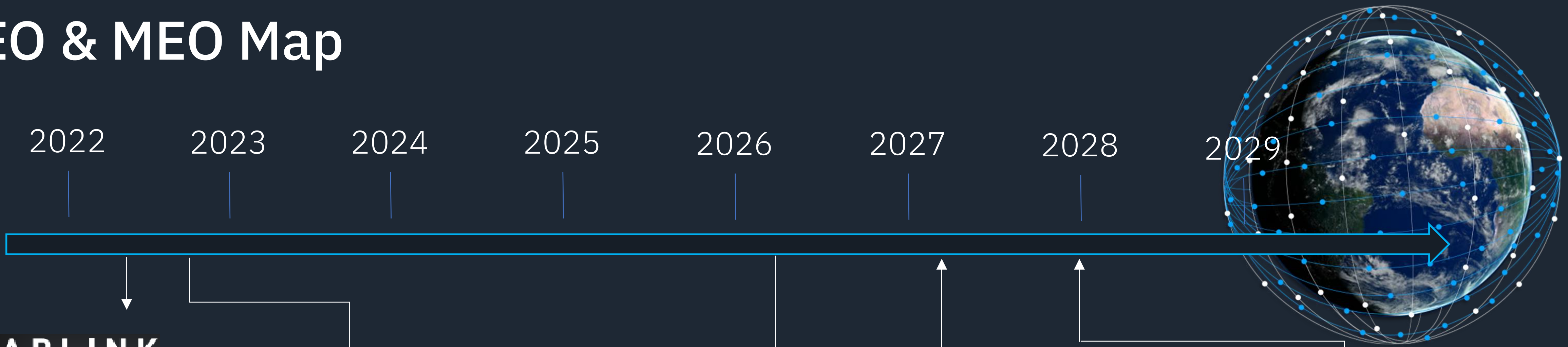
180-230km orbital altitude



Lower orbit. Higher performance.

OMNIACCESS

LEO & MEO Map



STARLINK

- › 8500 satellites launched
- ≈ 7200 operational
- Ku band to UT
- 550 km above Earth
- Best Effort

eutelsat ONEWEB eutelsat GROUP

- 654 launched (648 provisioned)
- Ku band to UT
- 1200 km above Earth
- MIR & CIR & SLAs

amazon Project Kuiper

- 27 Satellites launched
- 3236 satellites provisioned
- Ka band to UT
- 590-630 km

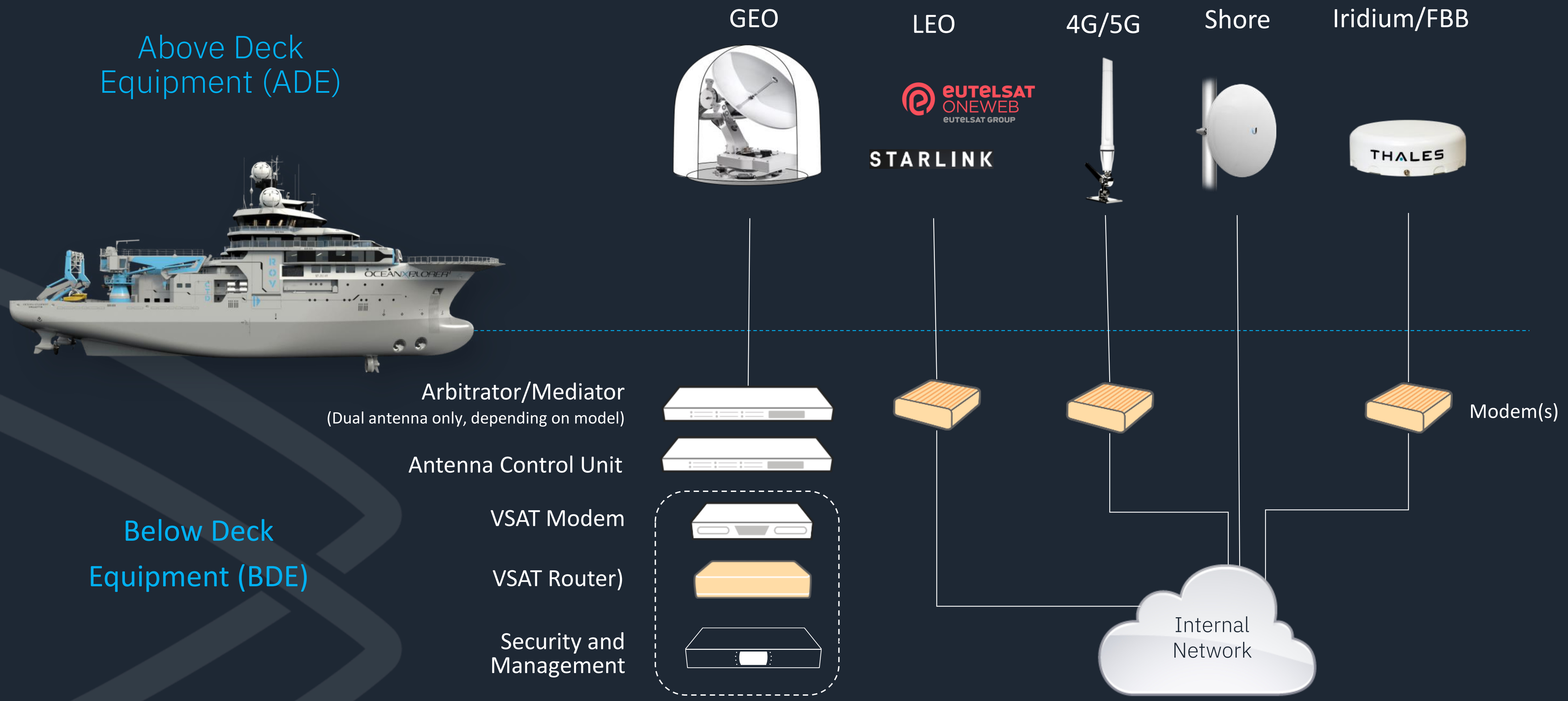
TELESAT LIGHTSPEED™

- 198 Satellites prov. (instead of 300)
- Ka band to UT
- CIR & MIR

O3b mPOWER

- 8 satellites launched
- 13 satellites provisioned
- Ka band to UT
- 8000 km above Earth
- Dedicated capacity

Communications equipment on a Research Vessel



Above Deck Equipment (ADE)

GEO

LEO

4G/5G

Shore

Iridium/FBB

Arbitrator/Mediator
(Dual antenna only, depending on model)

Antenna Control Unit

VSAT Modem

VSAT Router)

Security and Management

Modem(s)

Internal Network

Below Deck Equipment (BDE)

Starlink Data-plans changes / Effective May 1, 2025

Starlink introduced/enforced a Terminal Access Charge (TAC):

TAC: → $150 / service line / month

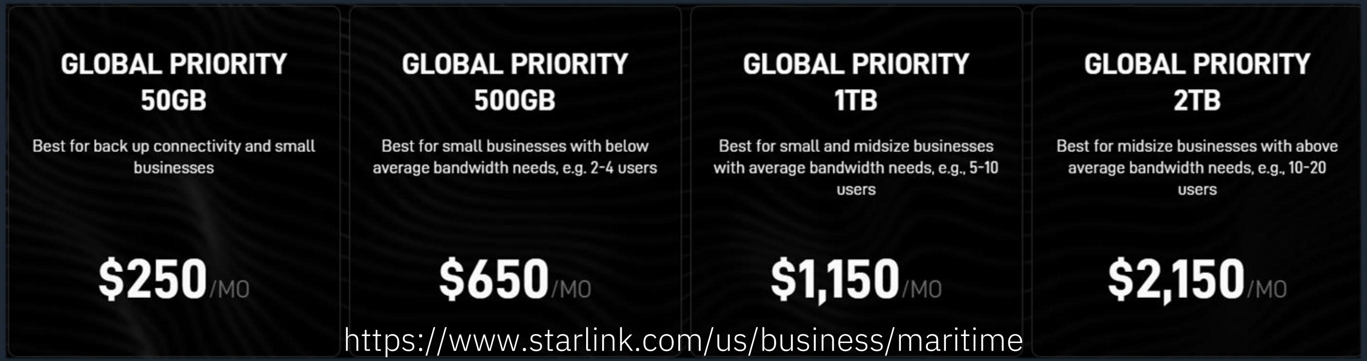
NB: Service line is up to 2 terminals

Data Blocks:

50 GB	→ $100 / month
500 GB	→ $500 / month

Terms:

- Expected consumption must be defined before the start of the billing cycle.
- Standard inland data (that was free of charge) disappeared
  - ➢ Now, once the quota is consumed, speeds throttle to 1/0,5Mbps but working everywhere (not only inland)
- Opt-in Overage is offered in blocks of 50GB @ $100.
- No upgrades or downgrades possible during the month.



GLOBAL PRIORITY 50GB	GLOBAL PRIORITY 500GB	GLOBAL PRIORITY 1TB	GLOBAL PRIORITY 2TB
Best for back up connectivity and small businesses	Best for small businesses with below average bandwidth needs, e.g. 2-4 users	Best for small and midsize businesses with average bandwidth needs, e.g., 5-10 users	Best for midsize businesses with above average bandwidth needs, e.g., 10-20 users
$250/MO	$650/MO	$1,150/MO	$2,150/MO

https://www.starlink.com/us/business/maritime

OmniAccess – Starlink Plans +

STARLINK

We offer all Starlink standard blocks, as well as below extended plans, where **we offer FOC (Free Of Charge) TAC on plans starting 3TB/m**

50 GB	→	$100 / month	+ TAC $150
500 GB	→	$500 / month	+ TAC $150
1 TB	→	$1,000 / month	+ TAC $150
2 TB	→	$2,000 / month	+ TAC $150
3 TB	→	$3,000 / month	(Incl. 1 X FOC TAC)
5 TB	→	$5,000 / month	(Incl. 1 X FOC TAC)
10TB	→	$10,000 / month	(Incl. 2 X FOC TAC)
15TB	→	$15,000 / month	(Incl. 2 X FOC TAC)
25TB	→	$25,000 / month	(Incl. 3 X FOC TAC)
Overage	→	$1.6 / GB	

*TAC for additional blocks of 2 antennas

EXCLUSIVE

With OmniAccess, all these plans can be pooled over n x antennas provided they are on the *same* vessel.

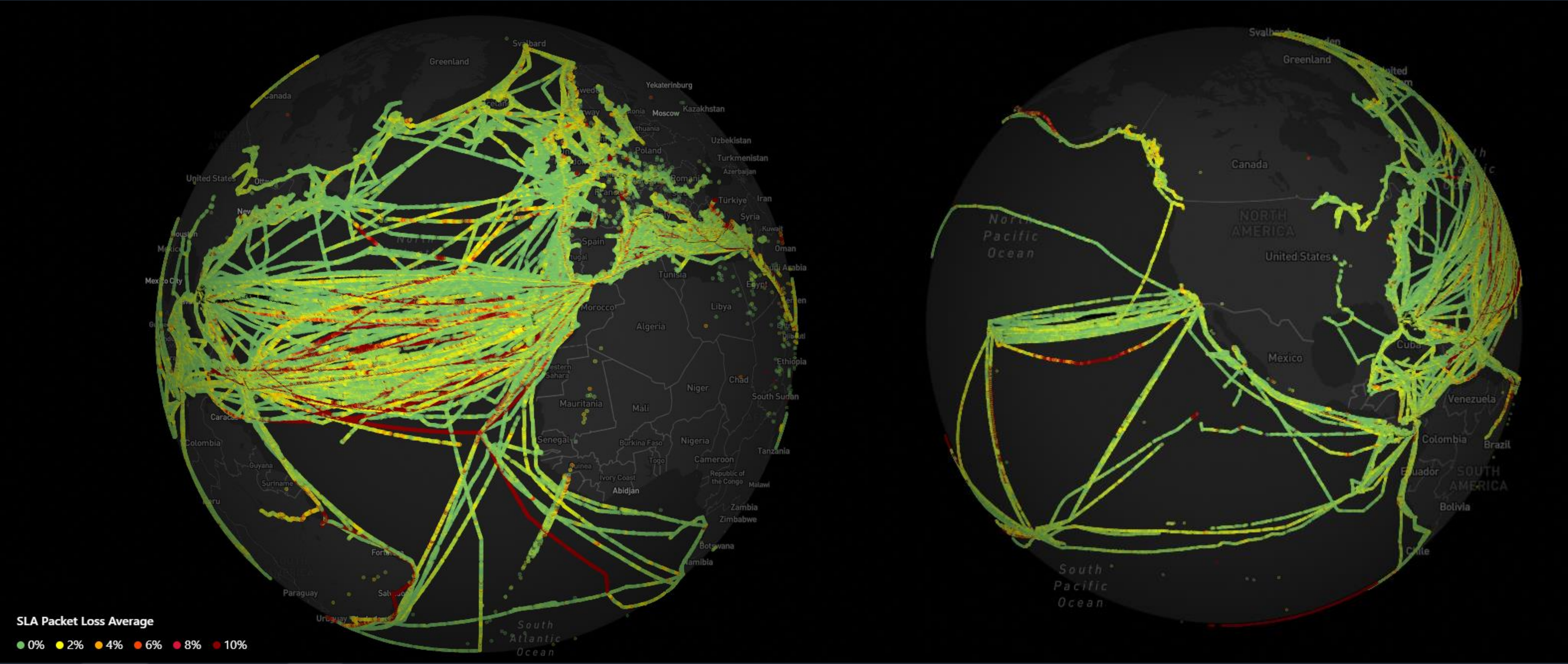
*Managed Service Fees as for now.

EXCLUSIVE	PAYG	→	$1.6 / GB
EXCLUSIVE	50GB Keep Alive (excl TAC)	→	Included with Unity Connectivity module
EXCLUSIVE	PAYG SL/5G Data Pivoting in Europe	→	$1.6 / GB
EXCLUSIVE	TOP UPs:		
	• 500GB	→	$750
	• 1TB	→	$1,400

Reach out to OmniAccess for customized pricing!

OMNIACCESS

OmniAccess Starlink heatmaps



OneWeb LEO Service plans

Product	Compatible UT	Plan	Monthly GB Allowance	Total MIR	Total CIR
Onboard	OW50M, OW70M, Peregrine, OW11FM	Onboard 20/4/100S	100	20/4	2/0.4
Onboard	OW50M, OW70M, Peregrine, OW11FM	Onboard 20/4/250S	250		
Bridge	OW10HM	HD Bridge 30/6/100S	100	30/6	2.4/1.2
Bridge	OW10HM	HD Bridge 30/6/1000S	1000		
Bridge	OW10HM	HD Bridge 30/6/US	Unlimited		
Bridge	OW50M, OW70M, Peregrine, OW11FM	FD Bridge 30/6/100S	100	30/6	3.2/1.6
Bridge	OW50M, OW70M, Peregrine, OW11FM	FD Bridge 30/6/1000S	1000		
Bridge	OW50M, OW70M, Peregrine, OW11FM	Bridge 30/6/US	Unlimited		
Master	OW50M, Peregrine, OW11FM	Master1 50/10/350S	350	50/10	6/3
Master	OW50M, Peregrine, OW11FM	Master1 50/10/500S	500		
Master	OW50M, Peregrine, OW11FM	Master1 50/10/900S	900		
Master	OW50M, Peregrine, OW11FM	Master1 50/10/US	Unlimited		
Master	OW70M	Master1 50/10/350S	350	50/10	8/4
Master	OW70M	Master1 50/10/500S	500		
Master	OW70M	Master1 50/10/900S	900		
Master	OW70M	Master1 50/10/US	Unlimited		
Ocean	OW70M	Ocean 75/15/1200S	1200	75/15	12/6
Ocean	OW70M	Ocean 75/15/2400S	2400		
Ocean	OW70M	Ocean 75/15/US	Unlimited		
Ocean Pro	OW70M	Ocean Pro 125/25/3000G	3000	125/25	25/9
Ocean Pro	OW70M	Ocean Pro 125/25/5000G	5000		
Ocean Pro	OW70M	Ocean Pro 125/25/UG	Unlimited		
Explorer	Peregrine, OW11FM	Explorer 100/20/1000B	1000	100/20	N/A
Explorer	Peregrine, OW11FM	Explorer 100/20/2500B	2500		
Explorer	2xPeregrine or 2xOW11FM	Explorer 200/40/1000B3	1000	200/40	N/A
Explorer	2xPeregrine or 2xOW11FM	Explorer 200/40/2500B3	2500		
Explorer	2xPeregrine or 2xOW11FM	Explorer 200/40/5000B3	5000		
Explorer	2xPeregrine or 2xOW11FM	Explorer 200/40/10000B3	10000		

Intellian OW10HM
(Half-duplex)

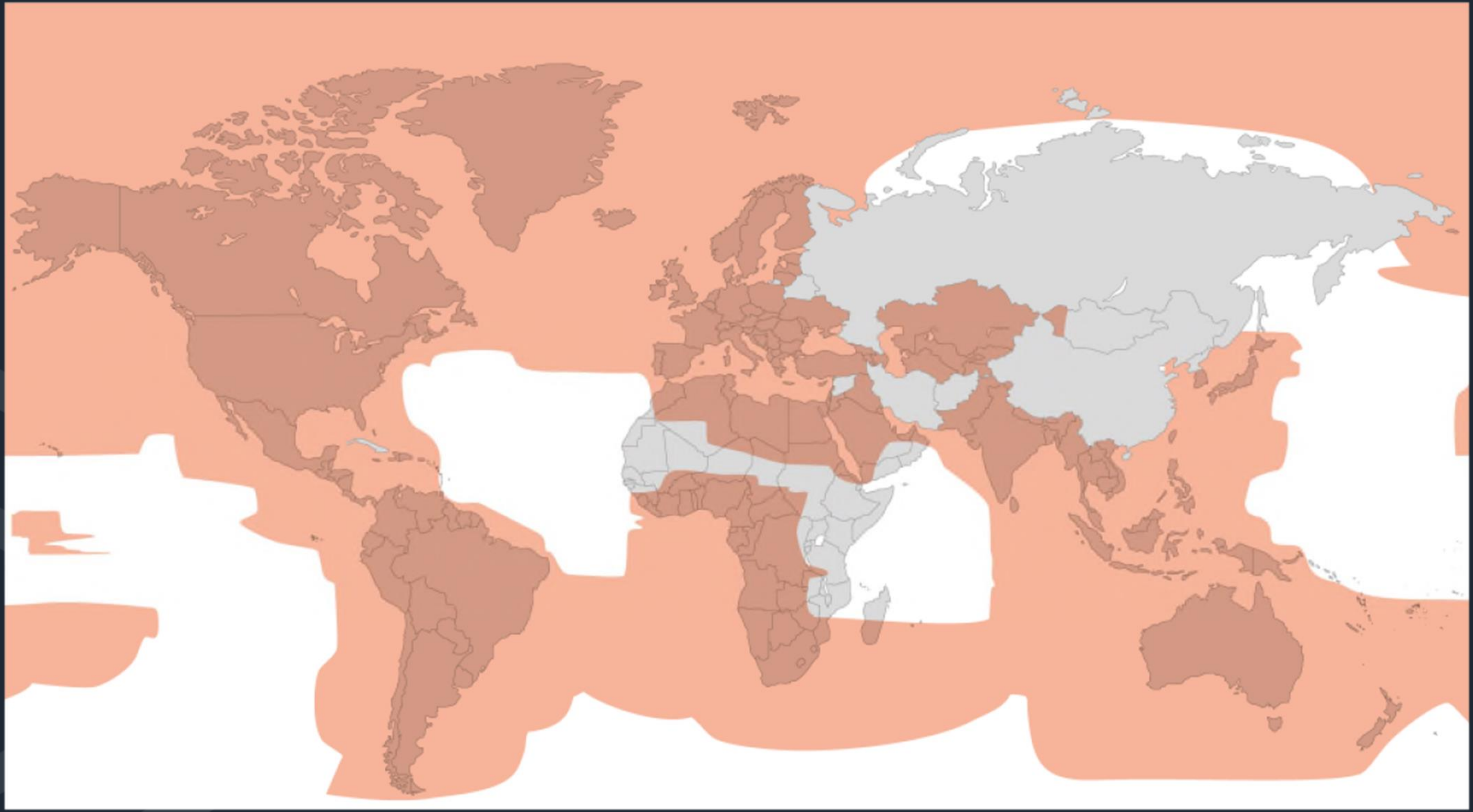
Intellian OW11FM
(Full-duplex)

Kymeta Peregrine u8

OW50M / OW 70M

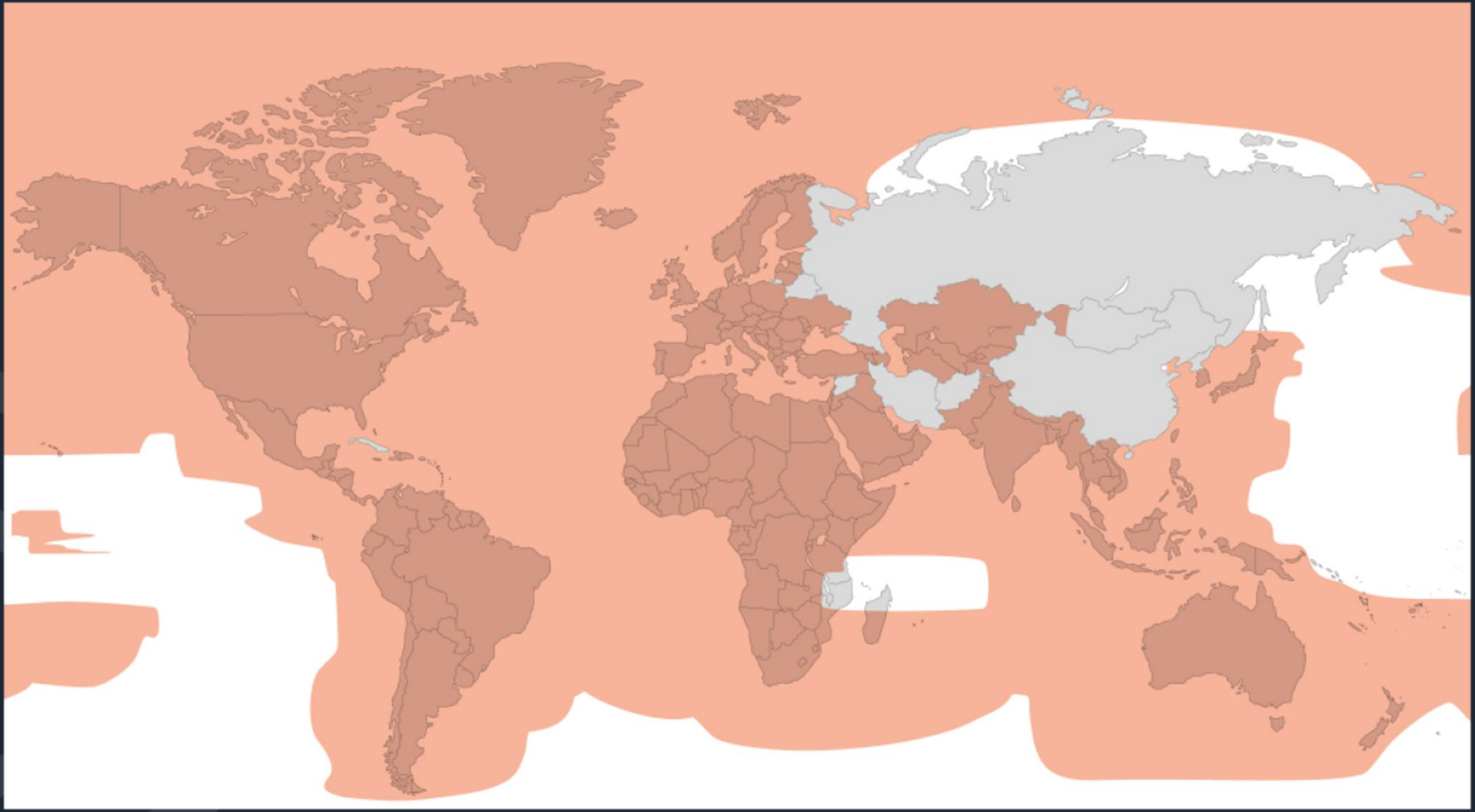
Reach out to OmniAccess for customized pricing!

LEO Network Coverage Forecast – June 2025



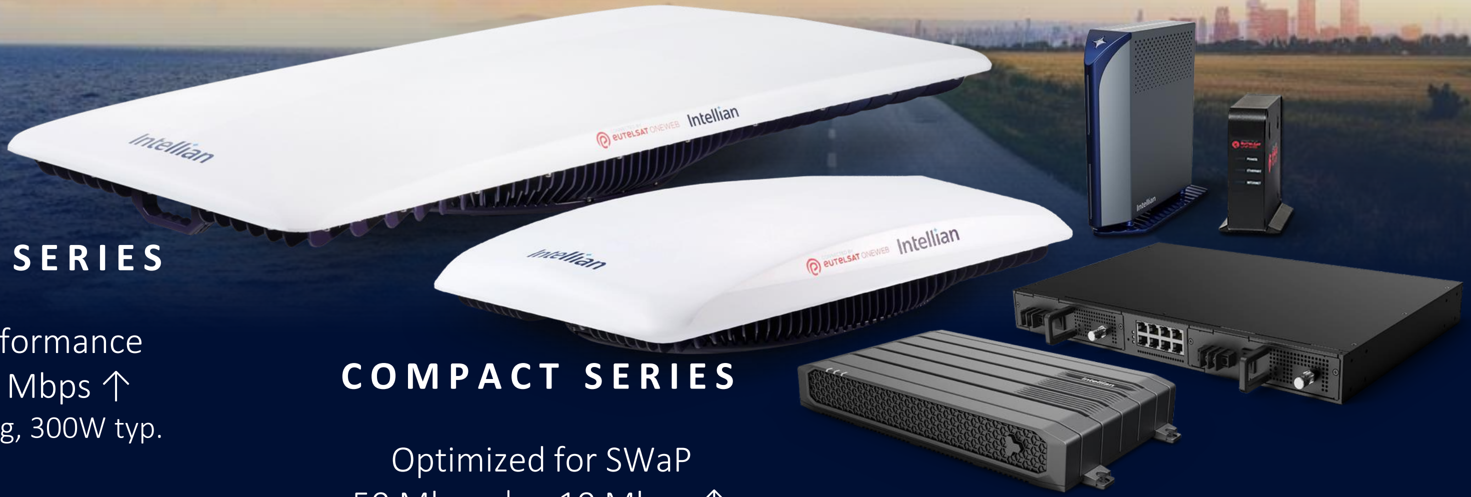
For representation purpose only

LEO Network Coverage Forecast – End of 2025



For representation purpose only

INTELLIAN FLAT PANEL SERIES



ENTERPRISE SERIES

Optimized for Performance
195 Mbps↓ x 32 Mbps ↑
97 x 50 x 13 cm, 20.5kg, 300W typ.

COMPACT SERIES

Optimized for SWaP
50 Mbps ↓ x 10 Mbps ↑
56 x 45 x 12cm, 12 kg, 165W Typ.

CNX-BB

Smallest Form Factor
13 x 12 x 4 cm
1-port GigE RJ45
**Compact Series Only*

CNX-WIFI

Wi-Fi & Networking
21 x 17 x 8 cm
4-port GigE RJ45

CNX-Mobility

Wi-Fi & Networking, Ruggedized
30 x 20 x 4 cm
4-port GigE RJ45

CNX-Rack

Rack Mount, Enables Primary-Primary
44 x 25 x 4 cm
8-port GigE RJ45

WHAT’S IN THE BOX – Enterprise / Maritime Series

Intellian’s Flat Panel Series For The Eutelsat OneWeb Network

OUTDOOR UNIT PACKAGE

Enterprise / Maritime Series

Coax Cable, RG6 (5m)

RF Sticker

Hardware

Grounding Strap
(L Variants only)

Adjustable
Mount Adapter
(L Variants only)

QIG

INDOOR UNIT PACKAGE

CNX

CNX-WIFI
w/ Wall Mount

OR

CNX-Mobility

OR

CNX-Rack
w/ NA & EU Power Cables
(AC Variant)

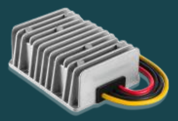
Power
Adapter*

(N/A for
CNX-Rack)

AC PSA, 250w

NA & EU
Power Cable

OR



DC-DC Converter

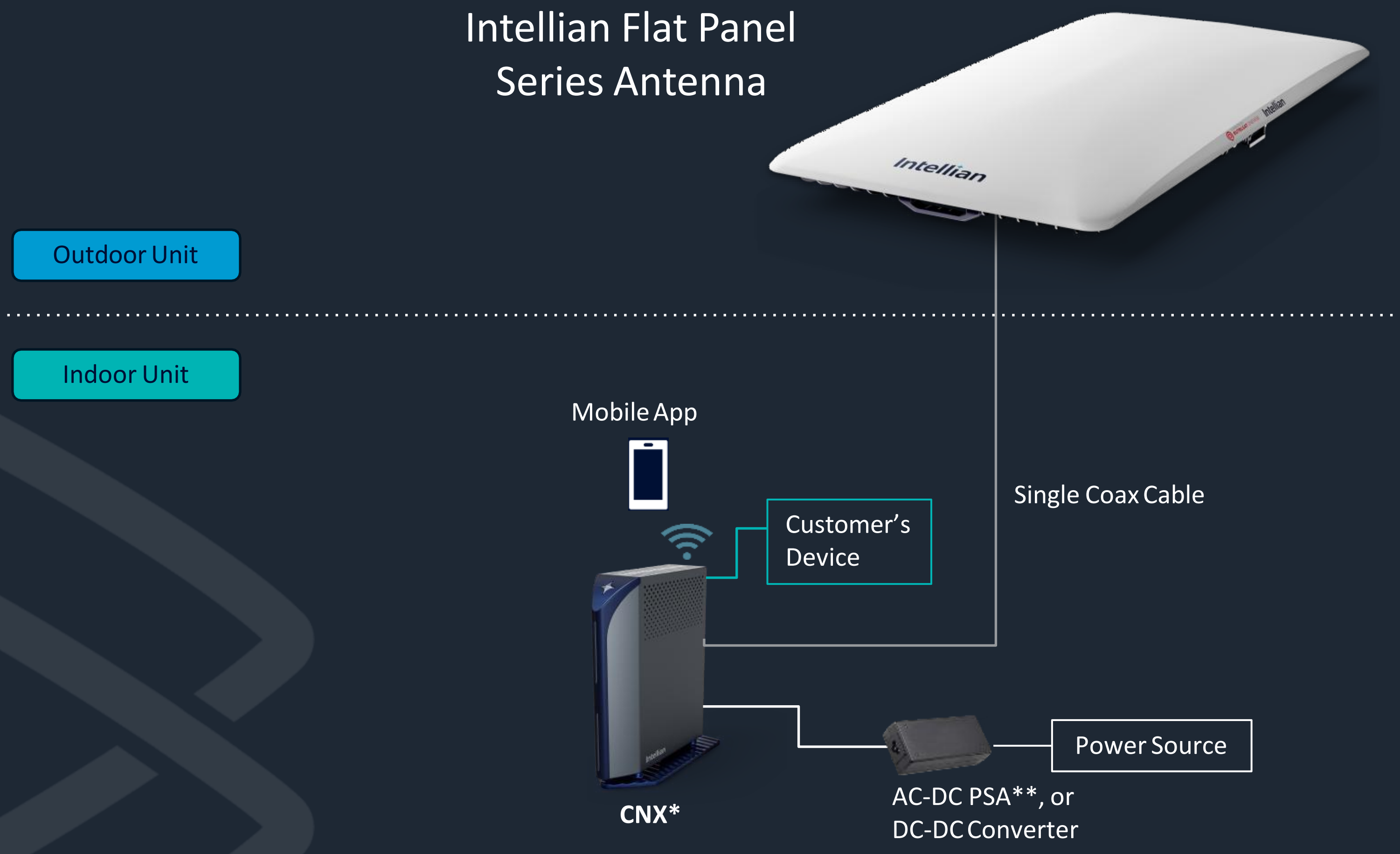
QIG

Ethernet Cable
(1m)

*CNX-Mobility utilizes a different power connector

SYSTEM CONFIGURATION

Intellian's Flat Panel Series For The Eutelsat OneWeb Network



* Can utilize alternative CNX
** 250W PSA for Compact.
450W PSA for Enterprise

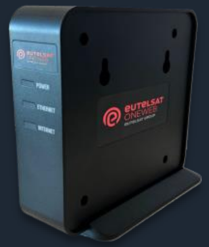
CNX's Portfolio

CNX-Rack

Maritime, Telco, Enterprise

CNX-Mobility

Land Mobility, Military, Maritime



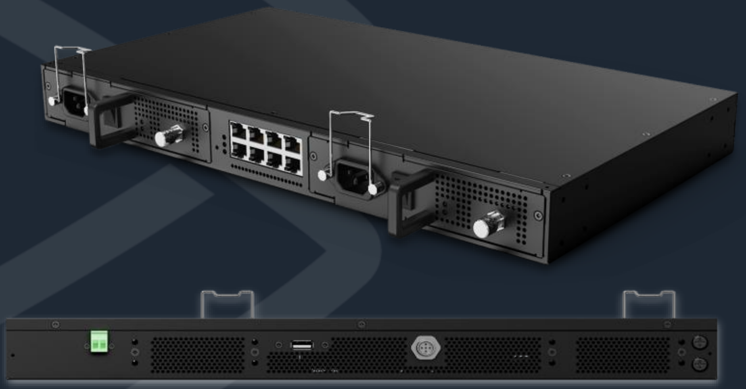
CNX-BB

Land Mobility

CNX-WIFI

Enterprise

CNX-Rack Specs:



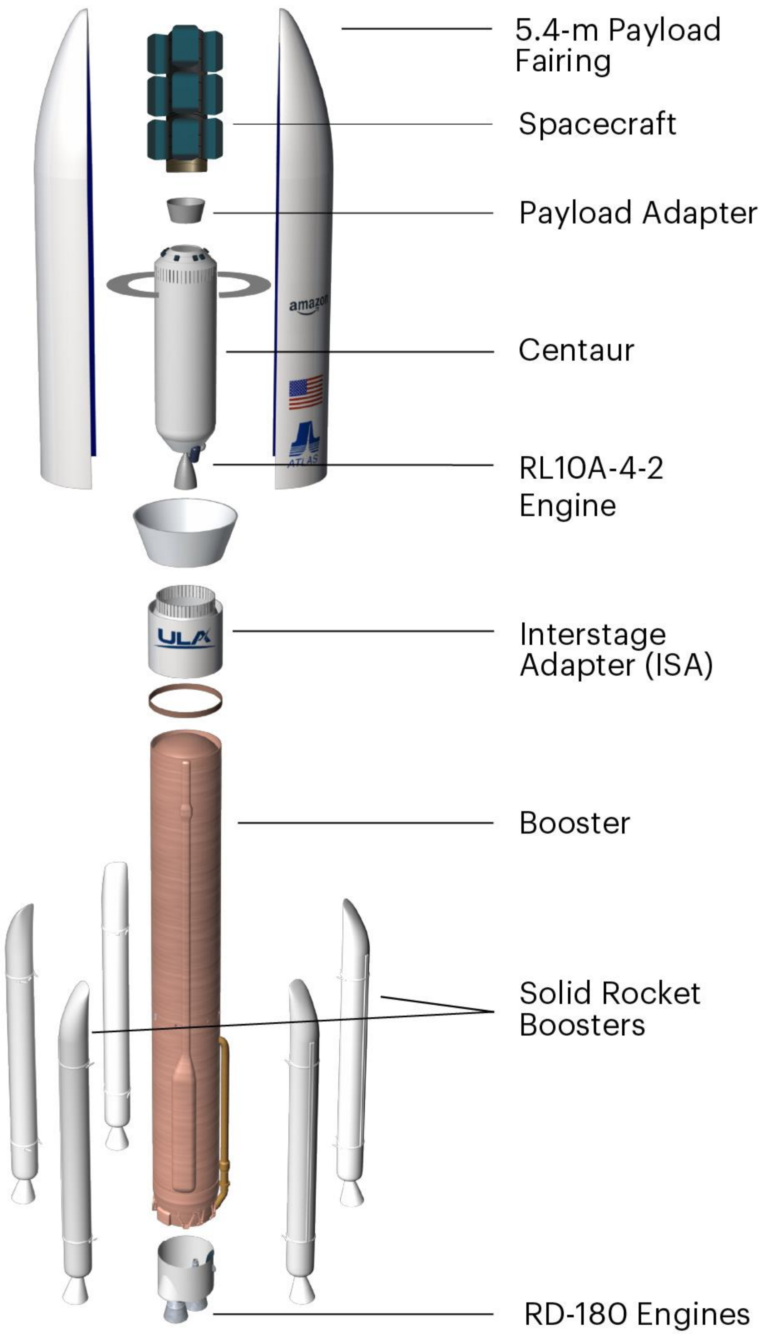
Specifications	
Dimensions	44.2cm x 25cm x 4.4cm (19 inch x 1 RU chassis)
Weight	6.3kg
Operating Temp	-25º to +55º C
Ingress	IP31
Data Interfaces	8-port GigE RJ45 1x USB (Type-A)
Power Distribution Modules	Dual 450W PDM AC: 110V- 200VAC DC: -48VDC
Interface	+56VDC, F-Type conn (one per power module)

Amazon Kuiper updates

KA-01, Kuiper-1 mission / April 28, 2025

Amazon's Project Kuiper used a United Launch Alliance **(ULA) Atlas V** rocket to deliver the first **27 satellites** of the constellation into low Earth orbit (LEO).

https://youtu.be/ZATwTLIbQu8



Kuiper satellite images In Orbit

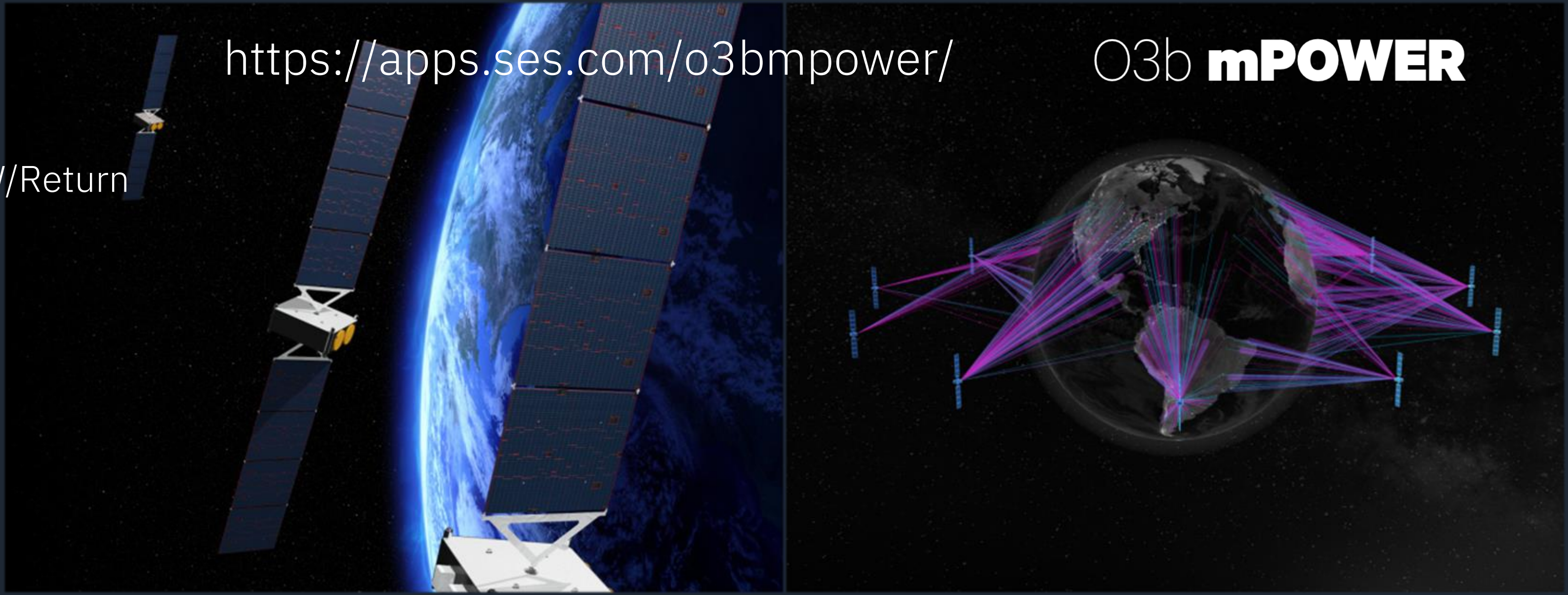
- Rectangular, solar-array-topped satellites with visible electronics and vent-like structures, unlike SpaceX’s cylindrical Starlink craft.
- Ka-band phased-array antennas to UT
- Up to 400 Mbps

https://youtu.be/EsmtGZBKfx8

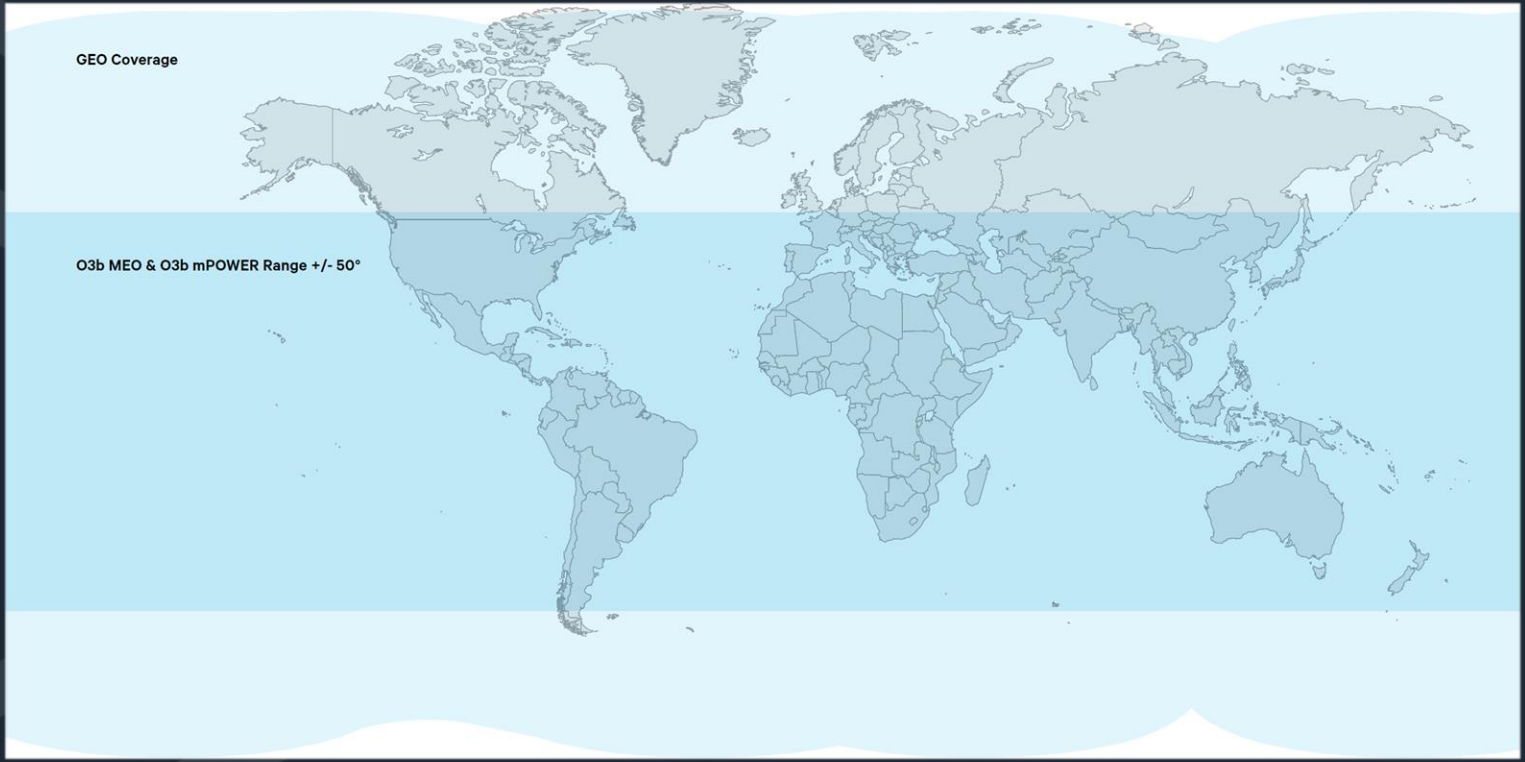
Amazon is required to have at least half of its planned 3,236 satellites in orbit by July 2026

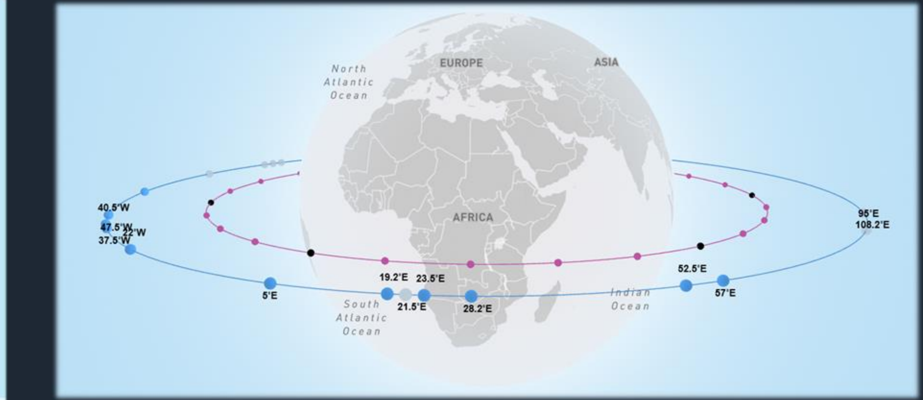
SES – O3b mPower

- 8 satellites launched
  - HTS → Distance → Scale → Symmetrical FW/Return
- 13 satellites provisioned
- Ka band to UT
- 8000 km above Earth
- 5Mbps to 300Mbps (Cruise service)
- 150ms latency
- 99.5% availability
- Coverage between ±50° latitude
  - MEO belt



https://apps.ses.com/o3bmpower/





Cyber Security drivers

Principally either Regulation or Cyber attacks
+ [Cyber] Insurance costs ?

accelerated by LEO and Digitalisation

Cybersecurity Regulations & Compliance

INTERNATIONAL MARITIME ORGANIZATION

IMO

MSC.428(98)

NIS2

1. Management accountability
2. Reporting to authorities
3. Risk Management
4. Business Continuity

UR E26

For the ship as a collective entity for cyber resilience

UR E27

for third-party equipment suppliers

OT - Sample Maritime Cybersecurity Incident!

- **April 6, 2024**, a **cyber attack targeted several key maritime ports and Vessels**
- Sophisticated ransomware & malicious software were used
  - ➢ Affect port operations and manipulate Automatic Identification Systems (AIS)
- Several ships reported unauthorized changes to their navigation routes!
- Attack exploited vulnerabilities in the **outdated AIS**

System that enables ships to broadcast their identity, position, speed, and other navigational data to nearby vessels and coastal authorities.

Monetary Losses:

- Estimates exceeding $500 million.
  - Halted port activities and shipping delays
  - Insurance claims, ransom payments, and losses from perishable goods.
  - Average ransom demand around $3.2 million per affected entity.

Operational Disruption:

- Ports across Europe, Asia, and North America reported extensive delays.
- Major shipping companies like Maersk and CMA CGM had to reroute vessels and suspend certain operations temporarily.
- The Port of Rotterdam experienced a near-complete shutdown of its automated systems, leading to massive backlogs and delays.

Cyber is not just an IT problem anymore!

UR E26 ? → Cyber resilience of Ships

- UR E26 (a Unified Requirement) is a technical standard (class notation) that is developed and agreed upon by all IACS (International Association of Classification Societies) members to ensure uniformity and consistency in the application of safety and technical requirements across the maritime industry.
- What UR E26 is about is to prove that the vessel is 'cyber resilient' at any time.
- Needs to be demonstrated in the lifetime of a vessel
- Applies to new ships > 500GT and contracted from July 1, 2024

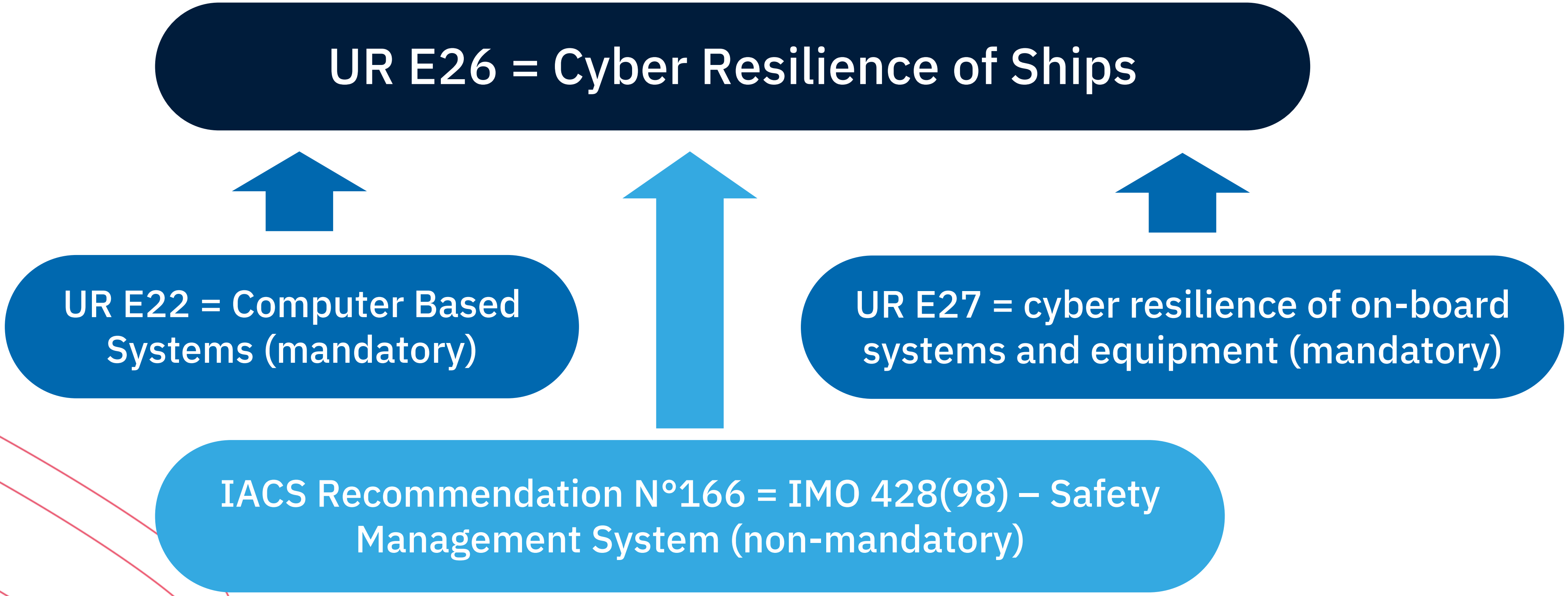
- None of the suppliers are UR E26 compliant as such. They may propose systems that are UR E27 compliant (like OmniAccess does with their UNITY)
- UR E27 provides the assurance to the customers that the type-approved systems will by nature meet the necessary UR E26 requirements.

Our role:

- As OmniAccess (supplier, but also cyber experts/advisors) we offer solutions as well as services to help our customer to get their UR E26 class notation.
- Our solutions help meeting the 'functional elements' following the NIST principles (identify, protect, detection, respond and recover).
- Our teams of experts can work with our customers to assess, design, deliver and operate their IT / OT environments and guarantee maintenance of the ship cyber resilience over time.

Cyber is not just an IT problem anymore!
If OT gets compromised, consequences could be catastrophic

Dependencies



UR E26 = Cyber Resilience of Ships

UR E22 = Computer Based Systems (mandatory)

UR E27 = cyber resilience of on-board systems and equipment (mandatory)

IACS Recommendation N°166 = IMO 428(98) – Safety Management System (non-mandatory)

In **UR E26** (Cyber Resilience of Ships), the other two Unified Requirements, **UR E22** and **UR E27**, are referred to as complementary and connected standards, each addressing related but distinct aspects of cyber systems on board ships.

In **UR E26**, the **IACS Recommendation No. 166** is referenced as a **guiding document** that supports the implementation of cyber resilience requirements.

UR E26 vs. IMO MSC.428(98)

UR E26 is mandatory for **new ships** that **require class approval**. It's system-level, technical, and includes strict requirements and documentation (like SHM and CDRs).

IMO MSC.428(98) is broader but more general—it's about incorporating cyber risk into operational procedures, like the ISM Code, and applies to **all existing and new ships**.

	UR E26	IMO MSC.428(98)
Issued by	IACS (International Association of Classification Societies)	IMO (International Maritime Organization)
Type of Document	Unified Requirement (technical standard)	Maritime Safety Committee Resolution (guidance)
Entry into Force	Applies to **new ships** contracted from **July 1, 2024**	In force since **January 1, 2021**
Scope of Application	Newbuild ships **with digital systems onboard**	**All ships** (new and existing)
Focus	Technical **cyber resilience of onboard systems** (IT & OT)	**Cyber risk management** in the company's Safety Management System (SMS)
Level of Detail	Highly detailed – includes 3 lifecycle stages: Development, Integration, Operation	High-level guidance – refers to best practices and risk-based approach
Key Requirements	- Secure-by-design system development	- Identify cyber risks
	- System Hardening Measures (SHM)	- Incorporate mitigation into the ISM Code
	- Documentation (CDR)	- Crew awareness and training
	- Testing & lifecycle support	

Company Type	Applies To	Relevant Regulation(s)
Shipowners / Operators	All ships	IMO MSC.428(98), UR E26 (for new builds)
Shipyards	New ships being built	UR E26
System Integrators / Vendors	Systems onboard new ships	UR E26
Fleet Managers	Existing fleets	IMO MSC.428(98)

NIS2 DIRECTIVE

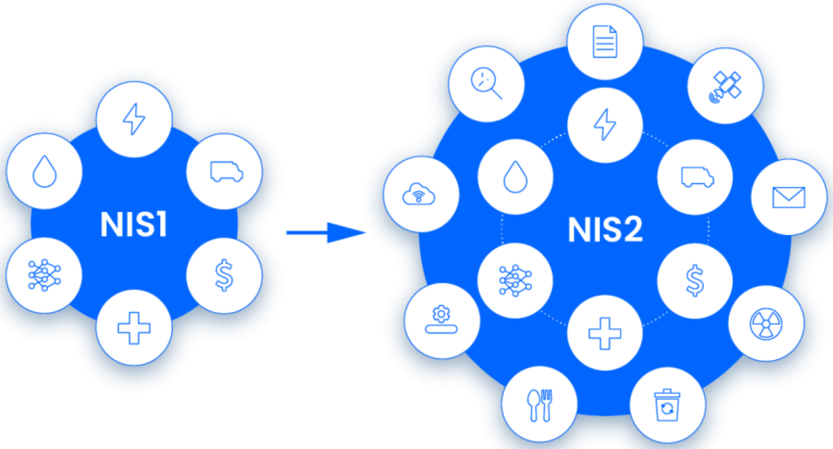
What’s NIS 2
Network and Information Security Directive

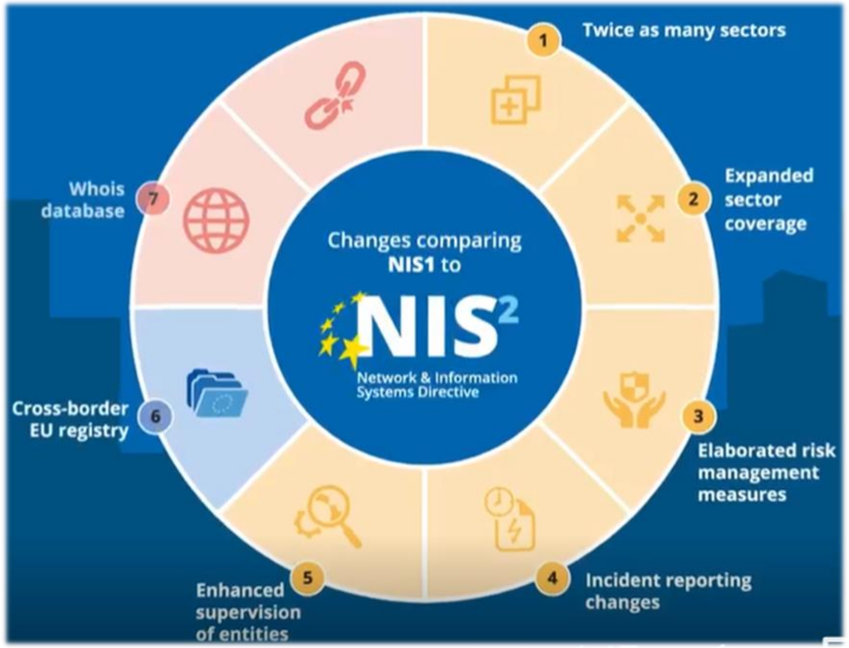
NIS2: Europe’s Most Extensive Cybersecurity Directive To Date

Is the latest regulatory framework the European Union (EU) introduced to strengthen the Cybersecurity of critical infrastructure and digital services.

Aims to address emerging cyber threats, promote cross-border cooperation, and enhance resilience of EU’s digital economy.

By October 2024, non-compliance will result fines of “at least” €10 million or 2% of the global annual revenue, whichever is higher.

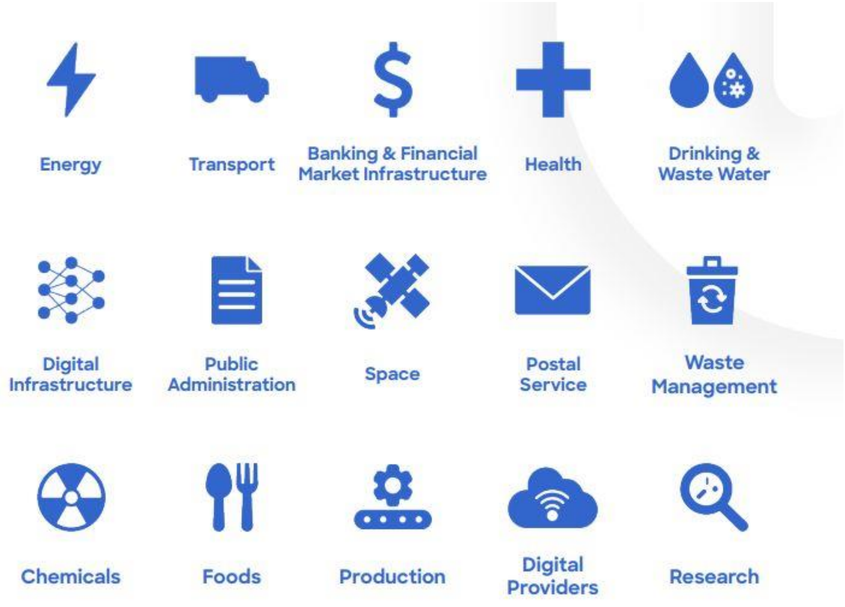



Changes comparing NIS1 to
NIS2
Network & Information Systems Directive
1 Twice as many sectors
2 Expanded sector coverage
3 Elaborated risk management measures
4 Incident reporting changes
5 Enhanced supervision of entities
6 Cross-border EU registry
7 Whois database

Organizations Affected By NIS2

NIS2 DIRECTIVE

NIS2 affects all entities that provide **essential** or **important** services to the European economy and society, including companies and suppliers.



NIS2 Entity Categories

Essential Entities (EE)

Size threshold: varies by sector, but generally 250 employees, annual turnover of € 50 million or balance sheet of € 43 million

Energy
Transport
Finance
Public Administration
Health
Space
Water supply (drinking & wastewater)
Digital Infrastructure

e.g. cloud computing service providers and ICT management

Important Entities (IE)

Size threshold: varies by sector, but generally 50 employees, annual turnover of € 10 million or balance sheet of € 10 million

Postal Services
Waste Management
Chemicals
Research
Foods
Manufactoring

e.g. medical devices and other equipment

Digital Providers

e.g. social networks, search engines, online marketplaces

Plus all sectors under "essential entities" and within the size threshold for "important entities"

Note:
An entity may still be considered "essential" or "important" even if it does not meet the size criteria, in specific cases such as when it is the sole provider of a critical service for societal or economic activity in a Member State.

https://nis2directive.eu/who-are-affected-by-nis2/

Key Requirements and Obligations of NIS2 Directive

Objective A: Managing Security Risk

- Governance
- Risk Management
- Asset Management
- Supply Chain

Objective B: Protecting Against Cyber Attack

- Protection Policies & Processes
- Identity & Access Control
- Data Security
- System Security
- Resilient Network & Systems
- Staff Awareness & Training

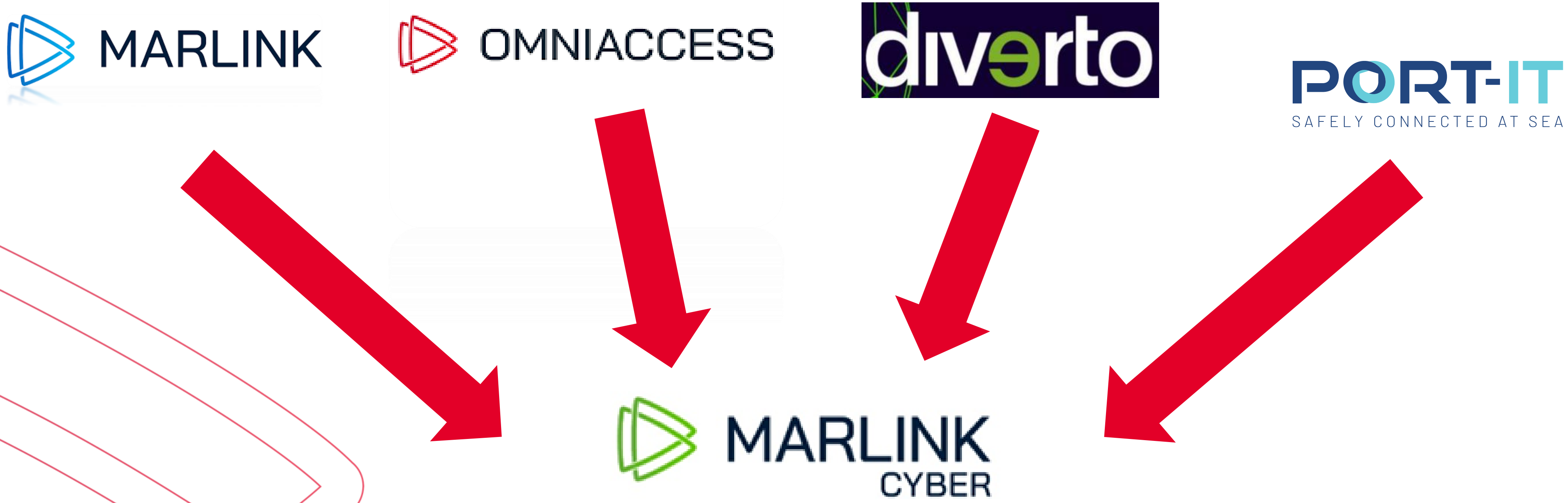
Objective C: Detecting Cyber Security Events

- Security Monitoring
- Proactive Security Event Discovery

Objective D: Minimising the Impact of Cyber Security Incidents

- Response & Recovery Planning
- Improvements

A Dedicated Cybersecurity entity and brand within the Marlink Group



180+ cybersecurity experts in 11 countries

Expertise, Trust, Reliability and Confidentiality

Market leader for maritime cyber security

The Marlink group has been positioned as **market leader for maritime cyber security** share in Valour Consultancy's new report: ‘The Future of Maritime Cybersecurity – 2025’.

Press Release: Subscriptions to Maritime Cybersecurity Services Reached Over 60,000 in 2024 | Valour Consultancy

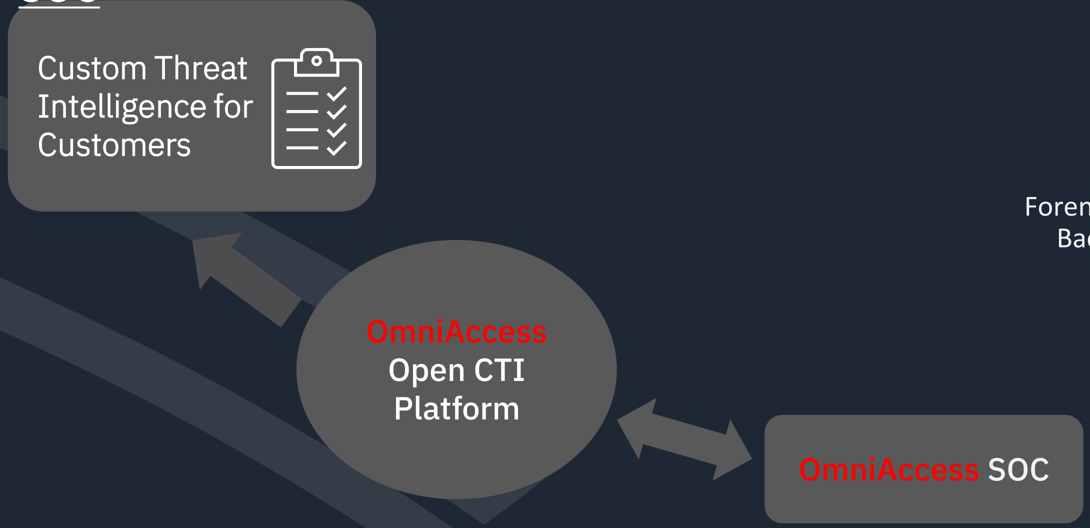
Marlink positioned as market leader for maritime cyber security

Credit: Valour Consultancy

OmniAccess / Marlink Cyber

Services around the NIST Framework

OmniAccess has the industries largest database for Maritime Threats, thanks to +1800 Vessels currently monitored by our SOC

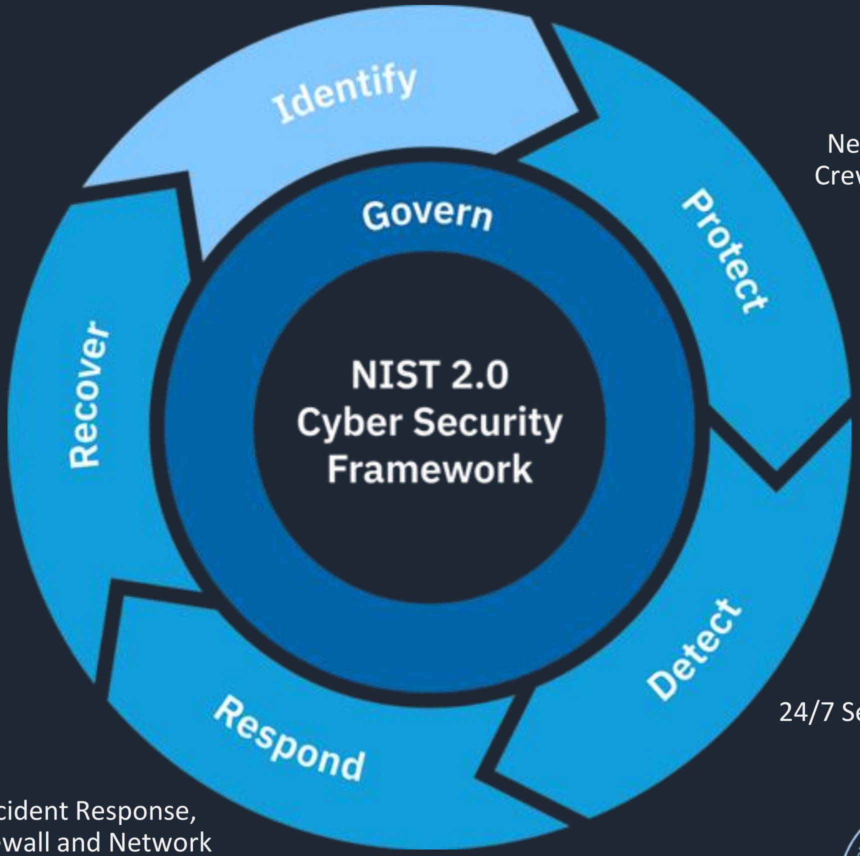


Custom Threat Intelligence for Customers
OmniAccess Open CTI Platform
OmniAccess SOC

Threat Detection, Risk Assessment, Vulnerability Scan, Penetration Test, OSINT report

Policies, Antivirus, EDR/XDR, IDS/IPS, Network Segmentation, Crew Awareness Training, MFA, zero trust

Forensic Analysis, Backup, etc.



SOC
24/7 Security Operations Center

Incident Response, Firewall and Network Reconfiguration, Access and Authentication Review

FORTINET splunk> AVANAN THE CLOUD SECURITY PLATFORM cisco

CROWDSTRIKE paloalto NETWORKS tenable Microsoft

Information Security Management System ISO 27001 Certified

MARLINK CYBER OMNIACCESS

Cyber Services expertise

Governance, Risk and Compliance

Profesional Services

vCISO
BIA & RISK MANAGEMENT
EDUCATION AND AWARENESS
INFORMATION AND CYBER SEC STRATEGY
MANAGEMENT SYSTEM DEVELOPMENT
SUPPLY CHAIN SECURITY MANAGEMENT
BUSINESS CONTINUITY MANAGEMENT
CYBER WAR SIMULATIONS

Defense Services (SOC teams)

Profesional Services

SOC/T1/T2/T3
SECURITY INTELLIGENCE
THREAT HUNTING
EARLY ALERTING
DECEPTION HONEYPOT SOLUTION
DDOS PROTECTION
INCIDENT MANAGEMENT
FORENSIC SERVICES

Offense Services

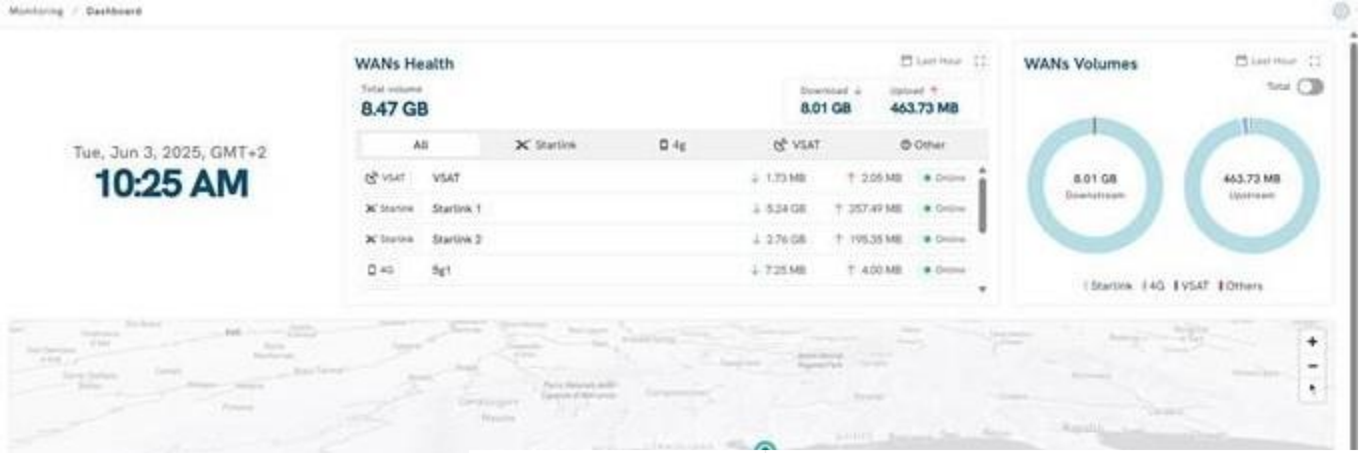
Profesional Services

VULNERABILITY ASSESSMENTS (IT/OT)
SOCIAL ENGINEERING TESTS
PENETRATION TESTS (IT/OT)
RED TEAMING EXERCISES
PURPLE TEAMING EXERCISES
APPLICATION AND PRODUCT TESTING
THREAT LED PENETRATION TEST (TLPT)

OMNIACCESS

UNITY

Cybersecurity dashboard



Tue, Jun 3, 2025, GMT+2
10:25 AM

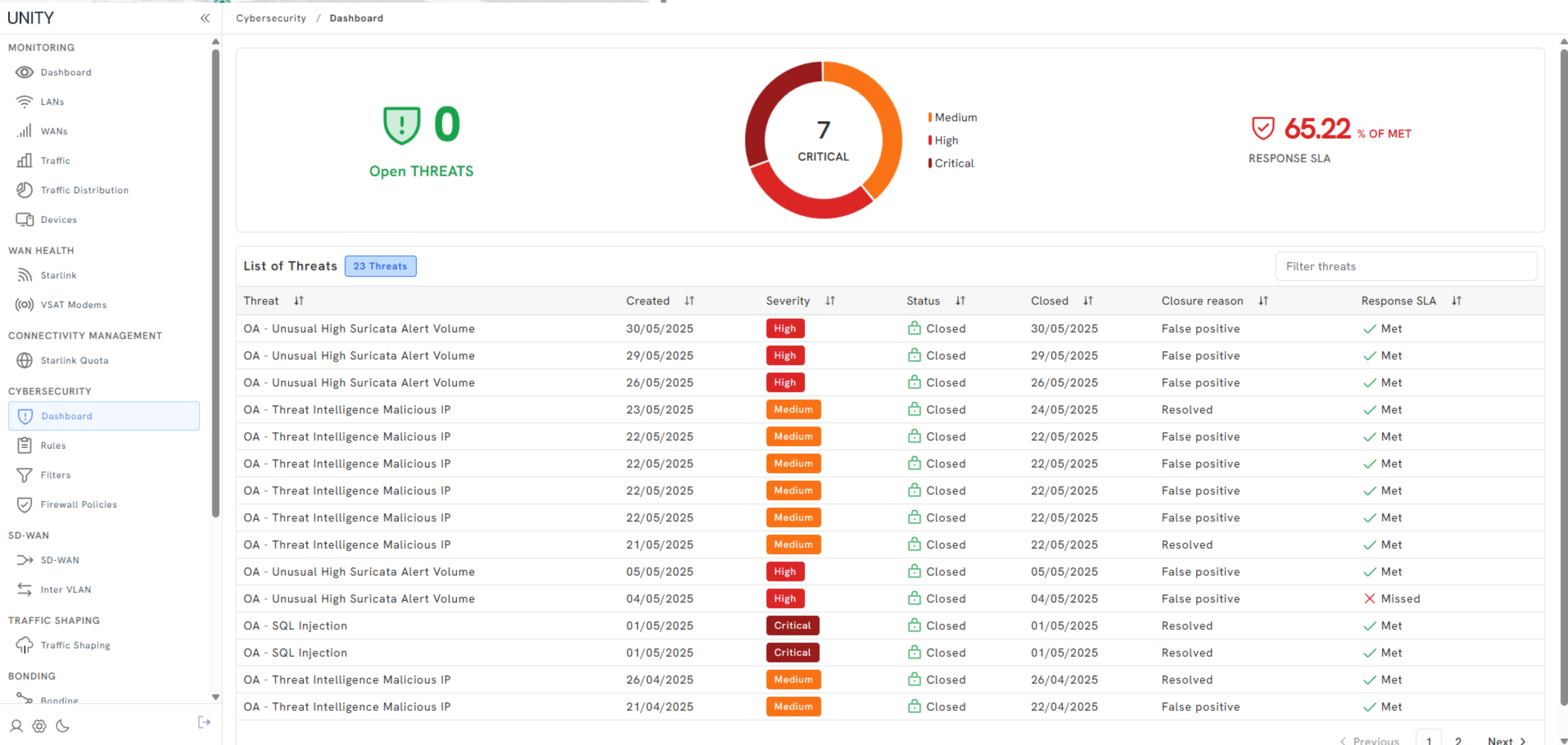
WANs Health
Total volume
8.47 GB
Download ↓ 8.01 GB
Upload ↑ 463.73 MB

VSAT	VSAT	↓ 1.73 MB	↑ 2.05 MB	Online
Starlink	Starlink 1	↓ 5.24 GB	↑ 257.49 MB	Online
Starlink	Starlink 2	↓ 2.76 GB	↑ 195.35 MB	Online
4G	5g1	↓ 7.25 MB	↑ 4.00 MB	Online

WANs Volumes

Logs
Empty logs
No security events

Network Status
Total volume
8.38 GB



0
Open THREATS

7
CRITICAL

65.22 % OF MET
RESPONSE SLA

List of Threats 23 Threats

Threat	Created	Severity	Status	Closed	Closure reason	Response SLA
OA - Unusual High Suricata Alert Volume	30/05/2025	High	Closed	30/05/2025	False positive	✓ Met
OA - Unusual High Suricata Alert Volume	29/05/2025	High	Closed	29/05/2025	False positive	✓ Met
OA - Unusual High Suricata Alert Volume	26/05/2025	High	Closed	26/05/2025	False positive	✓ Met
OA - Threat Intelligence Malicious IP	23/05/2025	Medium	Closed	24/05/2025	Resolved	✓ Met
OA - Threat Intelligence Malicious IP	22/05/2025	Medium	Closed	22/05/2025	False positive	✓ Met
OA - Threat Intelligence Malicious IP	22/05/2025	Medium	Closed	22/05/2025	False positive	✓ Met
OA - Threat Intelligence Malicious IP	22/05/2025	Medium	Closed	22/05/2025	False positive	✓ Met
OA - Threat Intelligence Malicious IP	22/05/2025	Medium	Closed	22/05/2025	False positive	✓ Met
OA - Threat Intelligence Malicious IP	21/05/2025	Medium	Closed	22/05/2025	Resolved	✓ Met
OA - Unusual High Suricata Alert Volume	05/05/2025	High	Closed	05/05/2025	False positive	✓ Met
OA - Unusual High Suricata Alert Volume	04/05/2025	High	Closed	04/05/2025	False positive	✗ Missed
OA - SQL Injection	01/05/2025	Critical	Closed	01/05/2025	Resolved	✓ Met
OA - SQL Injection	01/05/2025	Critical	Closed	01/05/2025	Resolved	✓ Met
OA - Threat Intelligence Malicious IP	26/04/2025	Medium	Closed	26/04/2025	Resolved	✓ Met
OA - Threat Intelligence Malicious IP	21/04/2025	Medium	Closed	22/04/2025	False positive	✓ Met

Network Security

Where do you stand today?

IMPLEMENT
Advanced Network Management

- Do your devices need to communicate across LANs? (**Inter-LAN**)
- Do you plan a **connected OT programme**? Have you **segmented** your OT devices?

ENFORCE
your IT Policy

- Have you implemented **an IT policy**?
- Do you wish to restrict business machines to **productive use** only?

STOP
Malware in your network

- How do you secure **private crew devices** and prevent them from infecting business PCs?
- In addition to endpoints, what are your other layers of **malware detection**?

DETECT & PROTECT
from Intrusions (IPS)

- Have you implemented protection mechanisms against onboard **network intrusions**?

Global Maritime Cyber Threat Report 2025

https://www.omniaccess.com/cyber-report/

1,998 Vessels Monitored

1,974 Firewalls Managed

22,921 EDR Devices Protected

9,923 Mailboxes Protected

30 Billion Security Events

700,000 Alerts

53 Major Incidents Managed

Key Threats in the Maritime Industry

Torpig/Mebroot

A banking Trojan with deep rootkit capabilities. In maritime operations, this poses a threat to payment systems and credential theft from crew, suppliers, or booking platforms — increasing the risk of financial fraud and regulatory non-compliance.

SystemBC

A sophisticated backdoor used by ransomware operators for encrypted C2 traffic and persistence. In maritime environments, it could facilitate lateral movement from IT into OT networks (via misconfigured firewalls or weak segmentation), threatening critical functions like cargo systems or engine diagnostics.

Mozi & Mirai

A banking Trojan with deep rootkit These IoT-based botnets exploit exposed devices common in shipboard systems, such as satellite routers, bridge-connected systems, or crew network IoT devices. They are frequently used for DDoS attacks, propagation, and botnet expansion — threatening **navigation reliability and ship-shore communication integrity.**

Prometei

A modular botnet often seen in **cryptojacking and credential theft,** exploiting weak RDP/SMB protocols — commonly observed in maritime companies with **poorly segmented crew or vendor access.**

Top Tools Abused by Threat Actors

PowerShell

Command-line tool and scripting language used for automating tasks and managing Windows systems, widely adopted by administrators and security experts to streamline processes, oversee system operations, and respond to security threats. Cybercriminals have exploited it to gain unauthorized access and execute harmful code, specifically to deliver stealthy "fileless" malware attacks.

AnyDesk

Remote desktop tool that enables users to access devices remotely and receive technical support while ensuring encrypted connections and secure file transfers. Although it is legitimate software, cybercriminals have exploited it for command-and-control (C2) operations and data theft. (I.e.: Akira ransomware group).

ScreenConnect

Remote desktop tool, that allows users to access and control devices remotely, facilitating IT support, encrypted connections, and secure file transfers. While it is a legitimate tool, threat actors have abused it to establish unauthorized access, deploy malware, and maintain persistent control over compromised systems for espionage and cybercriminal activities. (I.e.: Black Basta ransomware group).

WinSCP

Free, open-source client for SFTP, FTP, WebDAV, and SCP protocols, specifically built for Microsoft Windows. Cybercriminals exploited WinSCP to transfer large amounts of stolen data, upload malicious files to targeted servers to facilitate deeper system breaches, and establish remote access to execute commands or deploy further malware, ensuring prolonged control over compromised systems.

Metasploit

Open-source penetration testing framework that has been misused by threat actors to exploit vulnerabilities. (I.e.: LockBit ransomware group).

Cobalt Strike

Adversary simulation tool designed to mimic the continuous presence of cyber threats within network environments designed as a legitimate resource for penetration testers and red teams to evaluate network security. Cybercriminals have also misused it for malicious activities, and instances of its code being leaked online have accelerated its adoption by a wide range of threat actors, boosting its weaponization.

Most Detected Threats

MITRE Stage	Technique (ID & Name)	Threat level	Description
Initial Access	T1078 - Valid Accounts	🔥🔥🔥	Most common - stolen credentials used over VPN, SSH, or remote portals
	T1133 - External Remote Services	🔥🔥🔥	Attackers using poorly secured remote services (RDP, SHH)
	T1190 - Exploit Public-Facing Application	🔥🔥	Know software vulnerabilities in firewall, UI, or management ports
Execution/Persistence	T1059 - Command and Scripting Interpreter	🔥🔥	Running scripts or commands post-access (PowerShell, bash)
	T1543 - Create or Modify System Process	🔥	Creating services to remain active on the sytem
Lateral Movement	T1021.001 - Remote Desktop Protocol	🔥🔥	Moving laterally between guest/crew and operational networks
	T1071.001 - Web Protocols	🔥	Using standard web traffic for internal movement
Command & Control	T1095 - Non-Application Layer Protocol	🔥	Using non-standard communication (e.g., ICMP, TCP) to avoid detection
	T1573 - Encrypted Channel	🔥	Secure channels (e.g., HTTPS) to hide attacker communication
Impact	T1499 - Endpoint Denial of Service	🔥	Crashing or overloading onboard systems
	T1496 - Resource Hijacking (e.g., cryptojacking)	🔥	Using the ship's processing power for mining crypto

🔥 = Low 🔥🔥 = Moderate 🔥🔥🔥 = High

Critical Detected Attacks

Botnet	Detection Frequency
Torpig/Mebroot	31%
Mozi	19%
Mirai	14%
SystemBC	13%
Prometei	10%
UDPoS	8%
Bladabindi	2%

OMNIACCESS

OMNIACCESS

THANK YOU!

marwan.chartouny@omniaccess.com

+34 672 61 70 22