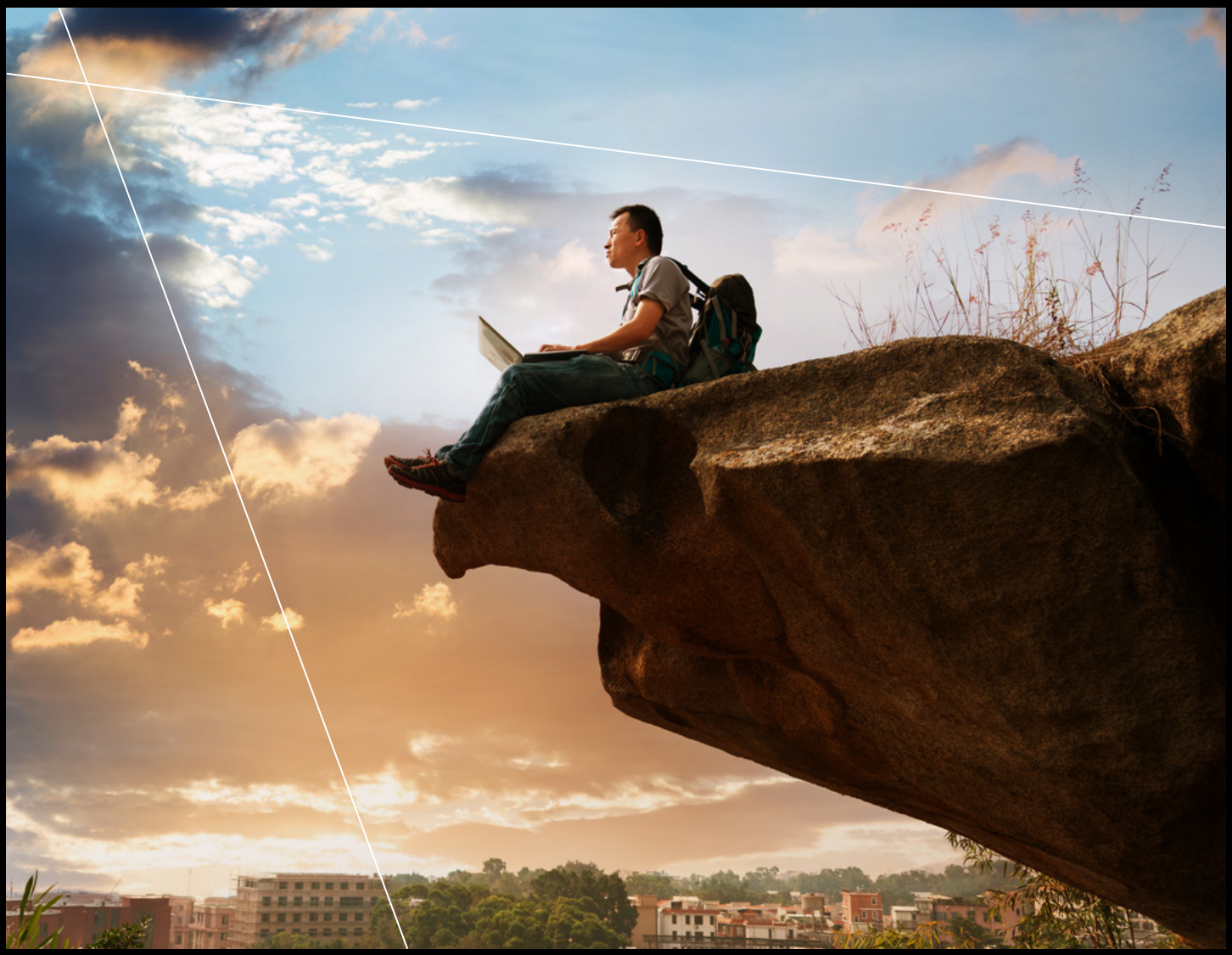
SES

STRATEGY GUIDE

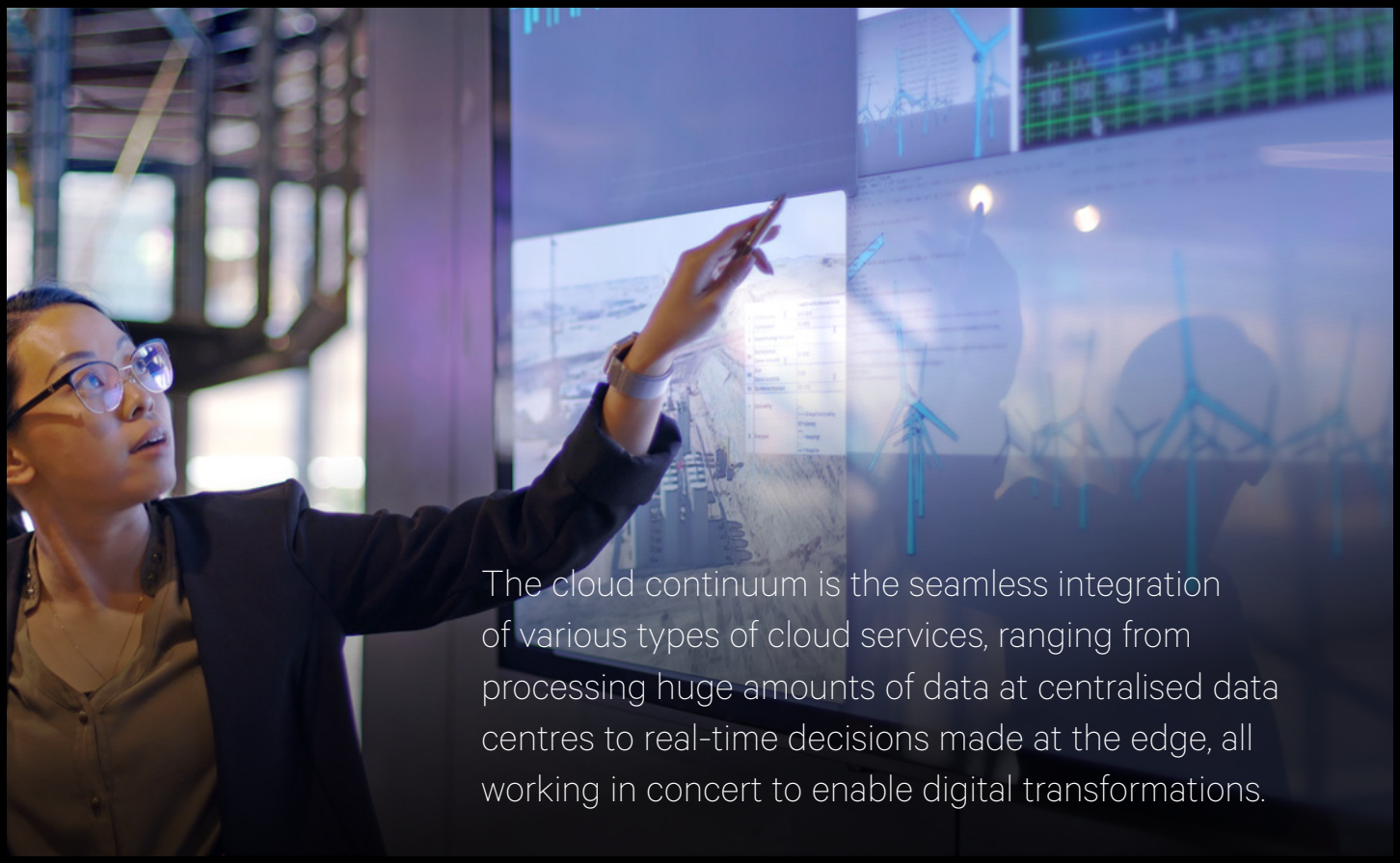
POWERING THE EDGE

Is your edge compute strategy robust enough to support your digitalisation goals?



O3b mPOWER

PERFORMANCE ABOVE ALL



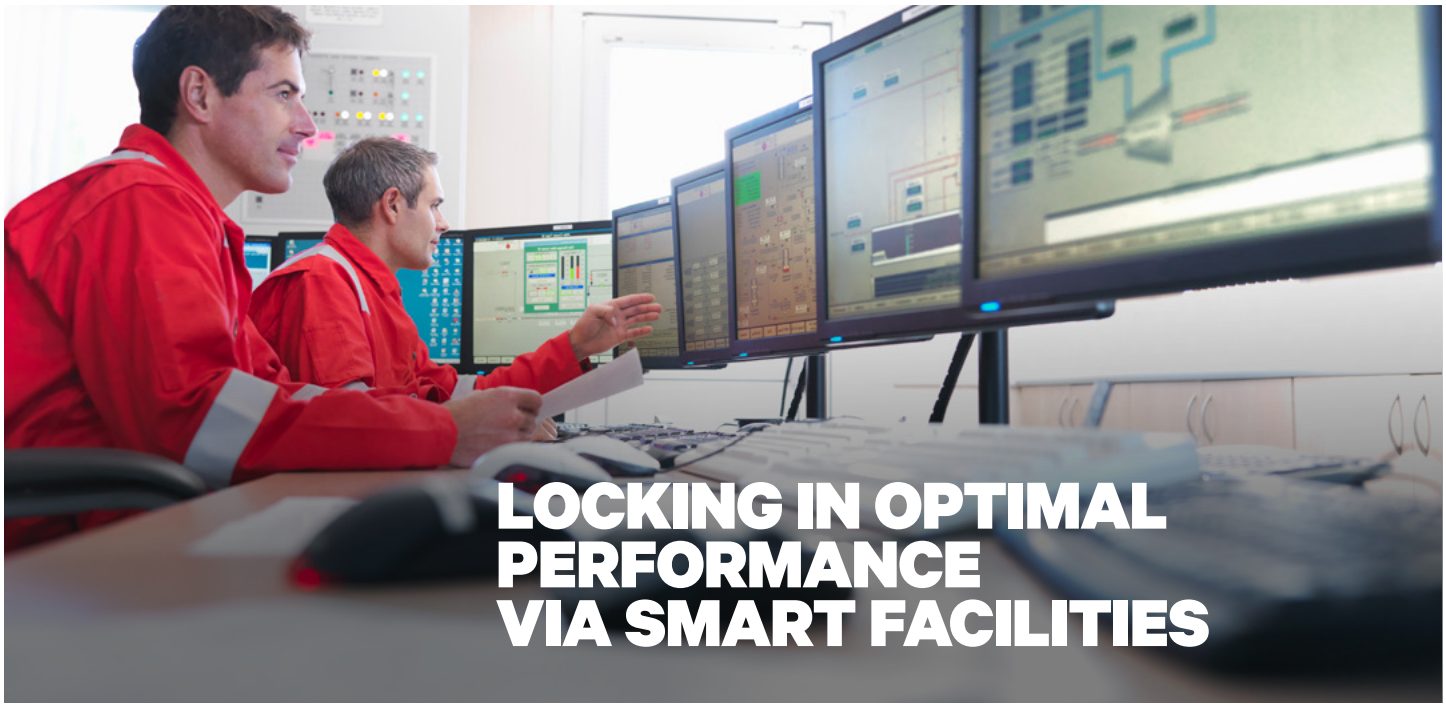
By 2030, the global edge computing market is expected to reach USD 155.9 billion, according to the Global Edge Computing Market Report.[1] This is driven by large scale adoption of Industry 4.0 technologies such as AI, machine learning, IoT, AR and VR, and 5G deployments.

While hyperscale data centres have the flexibility, scalability, and redundancy needed to process and store vast amounts of data, the last several years have seen computing power shift to the edge of the network, closer to the end user.

This shift makes edge computing a critical part of the cloud continuum. Processing data at the edge enables real-time control loops that gather data, apply insights, and implement actions. It can also optimise the use of core network resources by limiting the amount of data being transported to the centralized cloud for handling. The edge can serve as a platform for deploying virtualised network functions which can be "chained" to flexibly deploy value-added capabilities such as firewalls, load balancers and SD-WAN. Finally, edge computing can host mobile functions such as private 5G and applications like IoT, allowing a single stack of equipment to support functionality that extends beyond compute infrastructure and networking capability.

These capabilities all contribute to making edge computing an important tool in any digitalisation strategy, enabling use cases that improve network security, boost operational efficiency, and create enhanced customer experiences.

1. Research and Markets, 2022



LOCKING IN OPTIMAL PERFORMANCE VIA SMART FACILITIES

91%

of industrial companies are investing in digital factories[2]

$2-3M

cost savings over the lifetime of each vessel from maritime digitalisation[3]

20-25%

cost savings per barrel for offshore oil and gas operators using digital tools and analytics[4]

Digital transformation in industries such as maritime, manufacturing, and resource extraction depend on new tools that leverage IoT, big data, and AI to better manage assets, boost productivity, and improve the customer experience. These technologies depend on cloud and edge compute resources underpinned by new networking architectures, including 5G.

Digital redundancy
Creating digital twins of production assets or the final product itself provides the opportunity for early simulation and testing that can streamline product development.

Early detection
Analysing machines' sensor data at the edge enables early identification of any defects, lowering maintenance costs and production delays related to equipment failure.

Seamless inventory management
Automated materials tracking monitors the location of all components of a product so inventory can be continuously managed.

Automation
Fully autonomous robots handle high-volume repetitive processes where accuracy and speed are critical.

Greater collaboration
Augmented reality enables collaboration between on-site technicians and off-site experts.

Processing data at the edge allows 5G networks to support these use cases, providing the latency, responsiveness and enhanced application performance needed for industrial facilities to operate more efficiently and profitably—particularly when deployed in conjunction with private 5G for added flexibility and security.

2. PWC, 2020
3. Oliver Wyman, n.d.
4. McKinsey, 2020

EXTENDING NETWORK SECURITY TO THE EDGE

77%

of CISOs reported seeing an increase in disruptive network attacks in 2021

New digital technologies, multi-cloud strategies, distributed workers, and third-party applications were essential to the survival of many enterprises over the last few years. However, these capabilities often came with a price.

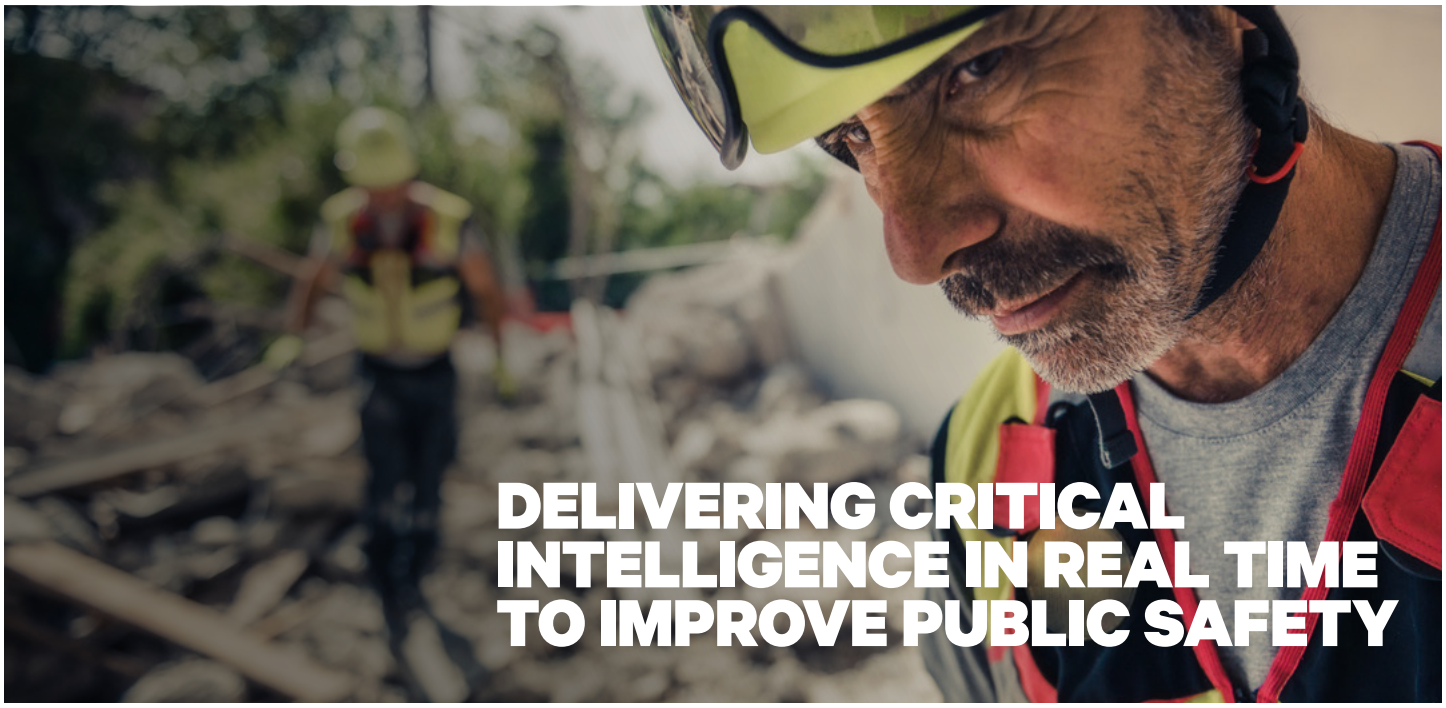
The strategic integration of edge resources with the centralised cloud adds additional safeguards to data generated and stored at the edge, enforcing organisational security policies across all devices, data, and users.

A recent survey conducted by consulting firm EY found that 77% of Chief Information Security Officers (CISOs) reported seeing an increase in disruptive network attacks in 2021, with enterprises often overlooking security best practices in favour of accelerating their digital transformation.[5]

The risk of a security breach is intensified when computing is pushed out to the edge, away from centralised security defences. That risk is compounded as the number of edge-compute deployments, the amount of data produced at the edge, and the number of remote users exponentially increase. Integrating security into edge computing mitigates that risk, protecting data and resources at the farthest reaches of the enterprise network. While ensuring devices are properly configured, tested, and patched is the first step toward securing the network, leveraging edge-based analytics and machine learning provides a powerful second layer of security, enabling enterprises to quickly detect threats and act immediately.

The strategic integration of edge resources with the centralised cloud adds additional safeguards to data generated and stored at the edge, enforcing organisational security policies across all devices, data, and users. Processing data at the edge enables companies to make real-time decisions that improve their operations and the customer experience, as well as facilitating compliance with regional regulations around the management of personal data. By maintaining the access control and encryption policies associated with that data in the cloud, enterprises capitalise on data generated at the edge without compromising its security.

5. EY Global Information Security Survey, 2021.



DELIVERING CRITICAL INTELLIGENCE IN REAL TIME TO IMPROVE PUBLIC SAFETY

Taiwan is one of the world's most beautiful countries, but also prone to natural disasters. This drove the Taiwanese government to seek access to critical cloud services in the event of a sustained network disruption.

SES and Microsoft responded to the request, combining their respective connectivity and computing capabilities with an open Radio Access Netowrk (RAN) solution from **Pegatron** that delivers resilient private 5G services, including communications among first responders, and 4K video transmission for command and control purposes.

When disaster strikes, edge computing plays an invaluable role in restoring operations and saving lives. Collecting and processing data from a wide range of devices—from mobile phones to smart vehicles to traffic sensors—provides first responders with situational awareness during an emergency, including continuous monitoring of the environment to safely expedite rescue efforts. As a foundation for 5G, edge computing becomes even more powerful in a crisis. Virtual network "slices" deployed at the edge deliver the latency and performance needed to support the varying requirements of emergency services personnel, enabling new digital technologies that are well suited for disaster management:

Augmented Reality
Augmented Reality (AR) glasses allow first responders to share information with doctors to ensure appropriate care and treat patients in real time.

Drones
Drones deliver critical supplies and gather intelligence from areas that cannot be safely accessed.

Emergency sensors
5G-connected sensors in emergency vehicles coordinate response efforts.

Mapping tools
Situational awareness tools use sensors and AR to create 3D maps.

HD video
High-definition video transmission enables tighter command and control.

Communication platforms
Cloud-hosted, satellite-enabled collaboration platforms enable continuous communication among emergency personnel.

5G technology has the potential to bring public safety organisations a new range of tools and capabilities that shorten response times, reduce the risk to first responders, and improve outcomes for impacted areas. Edge computing makes 5G networks even more powerful in public safety scenarios, bringing compute resources closer to the end user to deliver the latency and responsiveness needed for restoration and recovery efforts.

THE REALITY OF CONNECTING TO THE EDGE

Pushing compute power out to the edge of the network opens the door to a wide range of new use cases and has the potential to add complexity to end-user operations.

A "toolkit" approach, in which cloud-optimised connectivity is combined with edge compute resources and value-added solutions, addresses those challenges, eliminating complexity and adding business value to the edge.

Edge devices can be difficult to manage and monitor—both physically and virtually—opening the door to security breaches that could expose critical data. Managing edge deployments across multiple sites is also a challenge, particularly in a multi-cloud environment where an organisation may already be struggling with secure and reliable connectivity between cloud providers. A successful edge compute strategy depends on edge nodes being securely and reliably connected to the centralised cloud data centre or data centres, which may prove challenging for remote sites such as maritime vessels, offshore facilities such as oil rigs or windfarms, and mining facilities.

A "toolkit" approach, in which cloud-optimised connectivity is combined with edge compute resources and value-added solutions, addresses those challenges, eliminating complexity and adding business value to the edge. For example, a private 5G network that pre-integrates the edge compute platform with the 5G core, RAN, and connectivity to the central cloud provides enterprises with control and security without the hassle of procuring, deploying, and managing the individual components. An offshore oil platform can better capitalise on the terabyte of data it generates each day by deploying an edge node that integrates machine learning for real-time insights and immediate action, then transfers a subset of that data to the cloud for further processing and storage. Leveraging SD-WAN as part of an edge node improves network security and delivers better visibility into network performance and traffic patterns.

Enabling these edge "stacks" to be consumed as a managed service reduces complexity even further. An OPEX model eliminates the need for capital investments or up-front payments and provides enterprises with an end-to-end service level agreement and a single point of contact for the edge infrastructure—allowing them to focus on their core business.

COMPREHENSIVE EDGE COMPUTE SOLUTIONS FROM SES

Edge compute plays a critical role in the cloud continuum, but its success depends on the existence of a reliable, secure network infrastructure.

O3b mPOWER gateways are co-located with major cloud providers, reducing latency, and simplifying the routing of edge traffic to the cloud.

SES delivers that infrastructure, bringing flexibility and security to end users located at the edge, in locations that lack reliable and consistent terrestrial connectivity. Through our partnerships with the world's leading cloud service providers, we provide the underlying network fabric needed for enterprises to seamlessly access the cloud, wherever they operate.

Our next-generation O3b mPOWER network delivers private, dedicated connectivity to the cloud, with low-latency, multi-gigabit symmetric rates that adapt dynamically to network demand from the edge.

We are innovating with our partners to develop a suite of managed edge and managed 5G solutions to deliver intelligence to the edge and drive new revenue-generating use cases for end users. These solutions combine connectivity with next-generation technologies such as private 5G, distributed SD-WAN, and advanced analytics, to deliver intelligence to the edge and drive new revenue-generating use cases for end users.

Talk with us about how we can power your edge compute strategy.
www.ses.com

SES HEADQUARTERS

Château de Betzdorf
L-6815 Betzdorf
Luxembourg

Published in May 2023.

For more information about SES, visit www.ses.com

O3b mPOWER

PERFORMANCE ABOVE ALL