Security

PROTECTING AGAINST CYBER THREATS

The number, sophistication, and severity of cybersecurity threats continue to rise. Cyberattacks have evolved into a threat with global impact.

Government agencies and businesses around the globe are expanding their efforts to protect highly valuable information assets, and mitigate a broad range of risks threatening confidentiality, integrity, and availability of their data. Working with industry partners who recognise that effective cybersecurity is a joint effort is key to remaining ahead of the race, and keeping an edge over adversaries.

At SES, many of our customers have identified cybersecurity as a key area of focus and development. We share this understanding, and address cybersecurity as a priority across all key areas of our business—from customer hand-off points, where we receive data through our secure network and ground infrastructure, up to the satellite, and back down to the customer application at a remote site. We take a holistic view to applying best practices and processes in cybersecurity. This enables us to support our customers in effectively complying with the latest government and industry standards, while meeting mission objectives and maintaining cost effectiveness at the same time.

We take a highly consultative approach to customer engagement, enabling us to understand the challenges you face. Building on these insights, we tailor market-leading network solutions powered by our MEO and GEO satellite fleet and extensive ground infrastructure to your specific needs. This reduces the complexity of operating secure and effective networks, so you can remain focused on driving maximum value from your network solutions.

SES

SATELLITE / IN-ORBIT SECURITY

- Diversified security offering, up to latest generation encrypted control technology
- Anti-jamming capability or jamming resistance by design
- Tailored security for customer services, including traffic encryption
- Unique capability of hybrid GEO/MEO services, enabling high performance and service resilience
- World-class interference mitigation system

CUSTOMER APPLICATION / REMOTE SITE

- Next-generation customer terminals, supporting state-of-the-art security
- Customer Service Portal, offering self-service monitoring capabilities

SES GROUND INFRASTRUCTURE

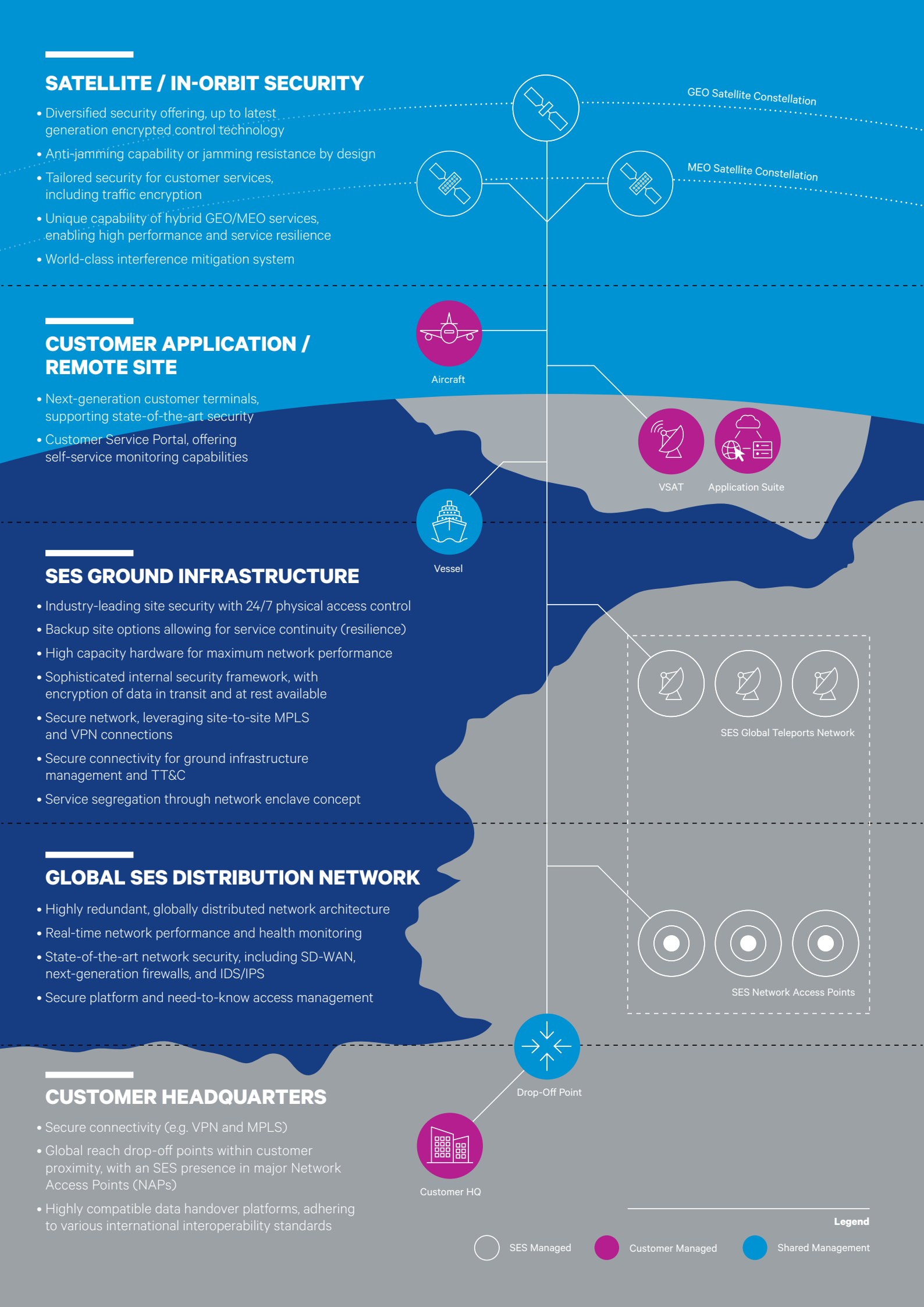
- Industry-leading site security with 24/7 physical access control
- Backup site options allowing for service continuity (resilience)
- High capacity hardware for maximum network performance
- Sophisticated internal security framework, with encryption of data in transit and at rest available
- Secure network, leveraging site-to-site MPLS and VPN connections
- Secure connectivity for ground infrastructure management and TT&C
- Service segregation through network enclave concept

GLOBAL SES DISTRIBUTION NETWORK

- Highly redundant, globally distributed network architecture
- Real-time network performance and health monitoring
- State-of-the-art network security, including SD-WAN, next-generation firewalls, and IDS/IPS
- Secure platform and need-to-know access management

CUSTOMER HEADQUARTERS

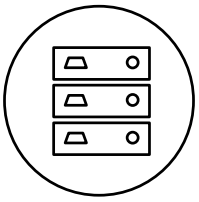
- Secure connectivity (e.g. VPN and MPLS)
- Global reach drop-off points within customer proximity, with an SES presence in major Network Access Points (NAPs)
- Highly compatible data handover platforms, adhering to various international interoperability standards



OUR SECURITY MANAGEMENT FRAMEWORK

A solid and thorough Information Security Management Framework is the key to establishing a trust-based customer relationship.

Our Security Management Framework is based on international standards, including ISO/IEC 27001 and NIST SP800-53, and we work continuously to maintain and improve the framework. It covers the diverse aspects, locations, and teams of our internal operations, so customers can trust that our security controls and processes will ensure efficient and effective management of Information Security risks.



Data Management

We recognise the value and importance of your data, and so we treat it as if it were our own. One of our key security processes is the SES Data Management Framework, which supports the identification, classification, and appropriate handling of information. The framework has been implemented to systematically identify protection requirements for information assets in terms of confidentiality, integrity, and availability. This facilitates our risk-based approach to protecting information assets in a way that's aligned to their classification.

As part of our data management framework, we have established a risk-based control framework, including an effective combination of ISO/IEC 27002 and NIST SP800-53 controls. This ensures information assets are adequately protected in accordance with their classification. We use the same control framework to assess and ensure that adequate security controls are in place across SES systems, applications, and outsourced IT services.

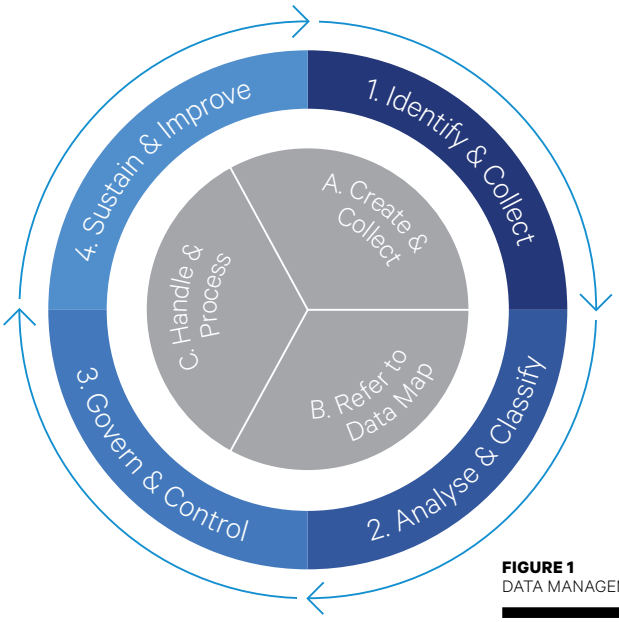


FIGURE 1
DATA MANAGEMENT FRAMEWORK

Network Security

Our networks are managed and controlled to protect information systems and applications, ensuring the security of information transferred over our internal networks, and protecting our services from unauthorised access and interruption.

To prevent breaches, detect attacks, and limit the potential impact of cybersecurity incidents, our network security zones are segregated and protected by an effective combination of complementary security controls. These include:

- Multiple layers of firewalls
- Application gateways, including email and web gateways with multiple anti-virus checks and dynamic content analysis
- Network intrusion detection and prevention systems
- Multiple layers of anti-virus scanning
- Strong, multi-factor authentication for remote access

System Security

As a core control to prevent unauthorised processing activities on our information systems, we have implemented access controls using a role-based access control (RBAC) model. We also operate state-of-the-art, centrally managed anti-malware and intrusion detection/prevention solutions by major security brands across different layers of the system.

Vulnerability Management and Security Monitoring

Our systems are continually scanned for vulnerabilities, and our highly trained security monitoring personnel perform regular proactive threat watch activities using cyber threat intelligence feeds that include the latest information on new vulnerabilities, zero days, indicators of compromise, and other factors.

We take significant efforts to reduce the likelihood and impact of information security incidents, including security orchestration and automation, extensive security monitoring, and the operation of a centralised, state-of-the-art Security Information and Event Management (SIEM) platform. SES is a founding member of the international Space Information Sharing and Analysis Center (ISAC), where industry leaders join forces to defend against advanced cyber threats. This ensures we can detect unauthorised access or potential security incidents in a timely manner. This also helps us to benefit from our internal threat intelligence and learn lessons from our internal security monitoring and incident response team, so that we can continuously adapt and improve our security infrastructure and control framework to stay ahead of the rapidly changing cyber-threat landscape.

Awareness and Education

We understand that any cyber defence is only as good as its weakest link. Our comprehensive Security Awareness and Training programme aims to provide employees and contractors with the security education they need to continuously improve our information security culture.

Physical Security

The SES sites and buildings are protected based on our comprehensive global physical security policy and standards. We have adopted the physical security principles established in ISO/IEC 27002, supported by more detailed guidance provided by NIST SP800-53.

Our sites are secured in alignment with the risk level and services offered. Critical sites implement the highest level of physical IT security controls that address topics including:

The inventory of authorised individuals	On-site guards and alarm systems
Electronic access control system for IT area or site access	Layered fences and barriers
Managed access credentials and audit logs	State-of-the-art environmental controls (for example, fire and water damage protection, emergency power)
CCTV system monitoring of sensitive areas	Access control for the transmission medium, and cabling protection

Controls Review and Management Ownership

Our dedicated information security committee is comprised of key SES stakeholders who oversee relevant aspects of governance over how we manage and protect information—both physical and electronic—created internally or received via third parties. The committee meets regularly, and reports directly to our Senior Leadership Team. It also oversees how information is classified, transferred, stored, and protected, as well as guiding our compliance with related laws, regulations, policies, and customer requirements.

We take significant efforts to reduce the likelihood and impact of information security incidents, including security orchestration and automation, extensive security monitoring, and the operation of a centralised, state-of-the-art Security Information and Event Management (SIEM) platform.

WANT TO KNOW MORE ABOUT OUR SECURITY MANAGEMENT FRAMEWORK?

Contact us at
getconnected@ses.com

SES HEADQUARTERS

Château de Betzdorf
L-6815 Betzdorf
Luxembourg

SES NETWORKS GLOBAL GOVERNMENT SALES OFFICES

Accra | Ghana
Addis Ababa | Ethiopia
Bogota | Colombia
Bucharest | Romania
Dubai | United Arab Emirates
Tampa Bay | USA
The Hague | The Netherlands
Istanbul | Turkey
Kiev | Ukraine
Lagos | Nigeria
London | UK
Miami | USA
Mexico City | Mexico
Munich | Germany
Nairobi | Kenya
Paris | France
Princeton | USA
Reston | USA
Riga | Latvia
Rio de Janeiro | Brazil
São Paulo | Brazil
Sydney | Australia
Singapore | Singapore
Stockholm | Sweden
Warsaw | Poland
Washington DC | USA

Published in September 2019.

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

SES