OCS - Real-time Monitoring

Leveraging 40+ years of communication and security experience, Viasat provides cost-effective, high-quality system monitoring and analysis services that expands your existing cyber security team`s effectiveness.

Viasat

Operational Cyber Services (OCS)

Operational Cyber Services (OCS) is an integration of cyber subject matter experts (SMEs), technology and processes tailored to improve data and system security for our customers by providing real-time threat detection, network visualization, and advanced investigative capabilities.

OCS enables customers to work with a single vendor to augment their existing cyber security personnel, which can substantially reduce their OPEX when compared with the cost of hiring cyber security professionals. Working in conjunction with our Security Operation Center (SOC), OCS employs advanced intrusion detection/prevention tools to continuously monitor cyber threats.

Among the tools OCS uses is a platform from artificial intelligence (AI) pioneer Darktrace, the world leader in cyber AI for cyber-threat detection and cyber-attack defense. These cyber-threat detection defense capabilities enables us to provide customers the most complete suite of Operational Cyber Services for the protection of their data and networks.

Key benefits

Centralized experts

A team of highly experienced cyber security analysts dedicated to preventing cyber security threats.

Reduce costs

The SOC assists your existing cyber security efforts and provides a force multiplier. Avoid costly training and employing staff will need to keep up with the latest vulnerabilities.

Protect your operations

We employ technologies including an arsenal of firewalls, probes, and event management systems that collect and monitor data as it moves across platforms. The SOC stays ahead of potential threats by analyzing active feeds, establishing rules, identifying exceptions, enhancing responses and keeping a close eye on possible vulnerabilities.

Providing our customers solutions to their cybersecurity vulnerabilities.

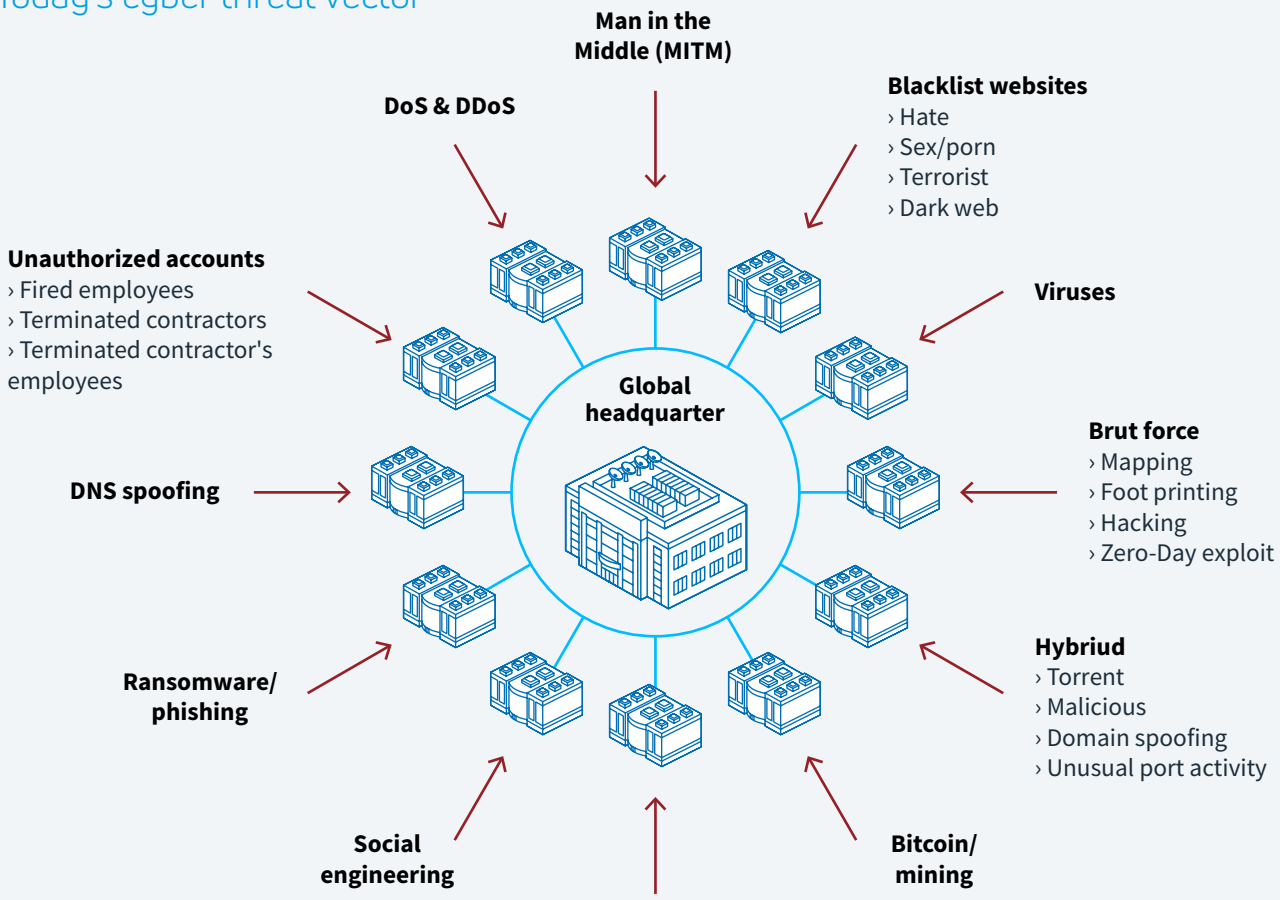
Taking **data**

Collaborating it into **information**

Operationalizing it into **knowledge**

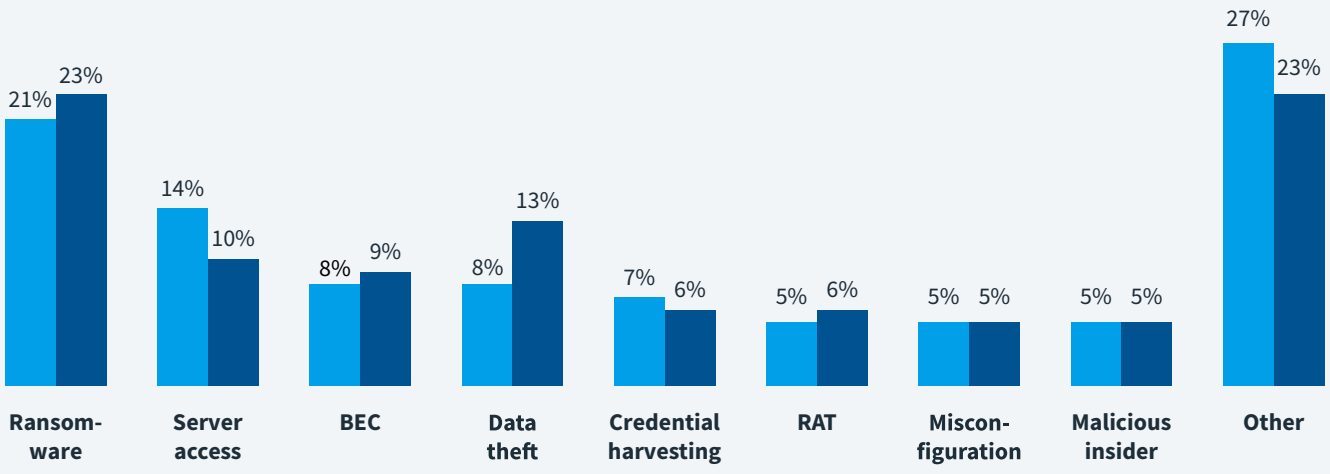
Providing **solutions**

Today's cyber threat vector



Top attack types, 2021 vs. 2020

Breakdown of top attack types, 2020-2021 (Source: IBM Security X-Force)[1]



[1]Other attacks include adware, banking trojans, botnets, cryptominers, defacements, fraud, DDoS, point of sale walware, spam, webscripts, webshells, and worms.

It takes an average of

207 days

to detect a breach.

An average

70 days

to contain a breach.

And an average cost of

USD$4.35 million.

**(Cost of a Data Breach Report 2022 – IBM Security).*

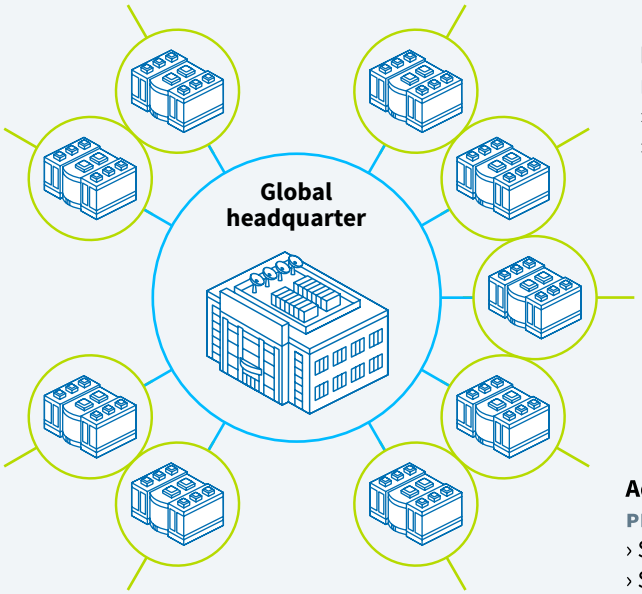
OCS provides a holistic solution that combines tools and services to counter each of these attack vectors.

OCS solutions

Risk Management Framework (RMF)
PROVIDING
› Controls assessment
› Risk awareness
› Policies
› Legal compliance
› Regulatory compliance
› Standardize processes

Employee training
PROTECTION COUNTERING
› Employee training
› Ransomware & phishing
› Social engineering
› Lack of security culture
› Incident response

Security Operations Center (SOC)
PROVIDING
› Continuous monitoring
› CyberSecurity engineering/architecture
› Rating score
PROTECTION COUNTERING
› Brut force
› Zero-day exploit
› DNS spoofing
› Viruses
› Bitcoin/mining
› Blacklist websites
› Hybrid
› Torrent
› Domain spoofing
› Secure setting



DDoS Protection
PROTECTION COUNTERING
› DoS
› DDoS

Asset management (IT/OT)
PROTECTION COUNTERING
› System secure setting
› System updates
› System default accounts
› System default passwords

Hardware encryption
PROTECTION COUNTERING
› Transmitting in the clear
› Man in the middle (MITM)
› Network analyzers
› Selling of encryption keys

Additional tools
PROTECTION COUNTERING
› System vulnerabilities
› System viruses

Conditional access control
PROTECTION COUNTERING
› Unauthorized accounts
› Terminated employees
› Terminated contractors
› Terminated contractor's employees
› Default accounts
› Default passwords
› Disgruntle employee

Email scanning
PROTECTION COUNTERING
› Viruses
› Ransomware
› Social engineering
› Disgruntled employee
› Lacking cybersecurity culture
› Forwarding CEO/CFO/CIO email accounts

OCS – Service overview

Operational Cyber Services (OCS) is an integrated suite of cyber offerings designed to improve data and system security by providing professional services, real-time threat detection, network visualization, and timely mitigating response.

Real-time monitoring

Visibility

Seeing on-net traffic, devices, and threat patterns enhances network security by mitigating threats in real-time.

Response

Identifying threats and taking corrective actions countering cyber attacks to the operations of any company.

Awareness

Running on your network and devices so, you can be aware of developing threats to them.

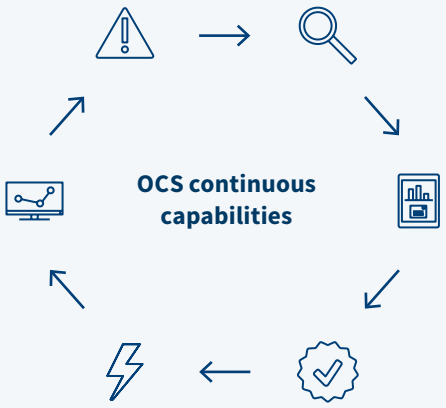
Monitoring

Threats attack around the clock and your network is continuously under siege from automated attacks or cybercriminals around the world. Monitoring security on your systems/networks for cyber attacks needs to be continuous so, you need cyber SMEs and timely tools in place.

Alert
Your SOC security team is notified of potential threats to your system

Monitor
Active inspection of your cybersecurity security environments and event logs

Respond
Action is taken to prevent future attacks and remediate vulnerabilities



Identity
Logs and alerts are reviewed for legitimacy of access and activity

Analyze
Investigate vulnerabilities exposed by legitimate and unauthorized access

Validate
Authorize legitimate activity

SOC - Threat monitoring and detection – (Darktrace/Bitsight)

OCS's Threat Monitoring & Detection combines the benefits of the market leading machine learning intrusion detection technology offered by Darktrace with OCS's Security Operations Center (SOC) team to discover and deliver meaningful insight of your network's exposure to attacks.

The SOC team utilizes this advanced machine learning technology to identify network abnormalities and perform deep inspection and analyses to investigate the potential attack vector(s). This analysis includes identifying the vector origination, potential risk to data and/or devices, and developing and executing mitigation plans.

Key benefits of the machine learning systems:

- Self-learning – learns on the job
- Adaptive – evolves with your organization
- Probabilistic – understands the likelihood of a threat
- Fight back – autonomously responds to high-priority incidents
- Real-time – detects threats as they emerge
- Works from day one – delivers instant value
- No false positives – identifies subtle, weak indicators
- Data agnostic – ingests all data sources
- Highly accurate – models human, device, and enterprise activity
- Scalable – largest deployment has over 1 million users
- All networks & devices – works on physical and virtual networks, cloud, ICS

SOC Engagement & reporting

OCS's goal is to build trust with your cybersecurity team by providing real-time and meaningful data to advance the protection of your IT and OT networks. This is achieved through high frequency collaboration and knowledge sharing of network activity and concerns. Our SOC analysts will work with your team to design an engagement program to include metric and incident reporting and investigation, validation, and mitigation engagement practices.

Enhanced Cybersecurity Services (ECS)

Cyber threat protection with classified government intelligence for all US-based private and public sector enterprises - Combining classified threat intelligence with unique detection capabilities.

Viasat is only one of a few top commercial cybersecurity partners chosen by the Department of Homeland Security (DHS) to create an advanced level of cyber protection for national security and defense. Our Enhanced Cybersecurity Services combines DHS's sensitive and classified Cyber Threat Intelligence with our abilities to detect malicious traffic entering or exiting customer networks — creating 360 leading cyber coverage.

Leveraging 40+ years of communication and security experience. Our history of building communication and encryption products for national security and defense enables us to implement ECS and provide:

› Unique capabilities that use classified cyber threat information to protect networks

› Augmentation (not replacement) of your existing capabilities

› Early advanced warning against sophisticated cyber-attacks and nation state-sponsored attacks

Benefits

› **Operationalized classified intel**

ECS is the only way to operationalize sensitive and classified Government Furnished Information (GFI) in commercial and civilian environments to detect and stop advanced persistent threats capable of bypassing your existing security technology stack.

› **Early warning**

DHS CISA shares timely, actionable, and vetted GFI with qualified CSPs. ECS provides early warning of emerging threats. Indicators appear on average 6 months before they show up in premium commercial threat feeds.

› **Data privacy**

ECS leverages our Trusted Cyber Sensor (TCS) — a unique NSA-certified device that is installed within your network to inspect traffic for malicious activity. Data privacy and confidentiality is protectied, vs. solutions that require sending data to a third-party.

› **Low integration effort**

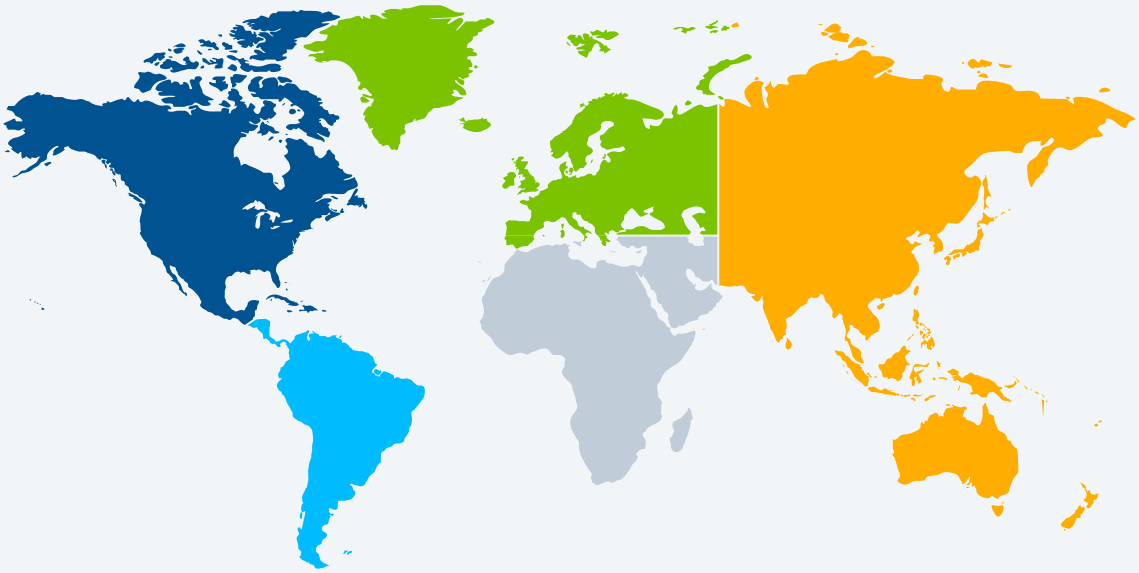
ECS with TCS is monitored, managed, maintained, and configured exclusively by our world class Cybersecurity Operations Center, giving you additional time and resources to meet your other business needs.

› **Internal visibility**

ECS with TCS detects attacks inside your network such as ones that enter your supply chain and are hiding in plain sight, in addition to ingress and egress activity, and provides additional visibility to your internal networks.

Un-employment for Cybersecurity Professionals is **"0"**

Gap in cybersecurity professionals since 2019



Global ~ 2.72M	NA ~ 402,000	LATAM ~ 701,000	Europe ~199,000	APAC ~1.42M
Pandemic (2020): ~ 3.12M	**Pandemic (2020):** ~ 376,000	**Pandemic (2020):** ~ 527,000	**Pandemic (2020):** ~ 168,000	**Pandemic (2020):** ~ 2.045M
Pre-pandemic (2019): ~ 4.07M	**Pre-pandemic (2019):** ~ 561,000	**Pre-pandemic (2019):** ~ 600,000	**Pre-pandemic (2019):** ~ 291,000	**Pre-pandemic (2019):** ~ 2.6M

**Source: ISC² Cybersecurity Workforce Study, 2021*

Conditional Access Control

OCS's Conditional Access Control offering is a security platform that provides secure, efficient, and manageable access to critical industrial control systems. The Conditional Access Control service is an offering under the OCS's portfolio and is fully supported by our Security Operations Center (SOC).

Technology overview

OCS's Conditional Access Control integrates access control, threat monitoring, data inspection, and auditing services into a single control system to provide management and visibility to critical applications/systems and networks.

Key benefits:

- Web based management
- Deep monitoring with IPS and Splunk
- Malware and malicious code scanning
- Work Permit Engine with integration API
- Endpoint Control - Anti-virus and Windows updates verification on connecting client
- Secure File Transfer with threat emulation
- User authentication with two-factor and one-time password
- All traffic encrypted
- Access only with a valid work permit
- Map users' qualifications and skills
- Dynamic roles
- Easy overview for work permit planning
- Self-service for user administration, qualifications and systems
- All network and user activity is logged
- All changes to servers are logged
- SSL, Split-VPN and Full-VPN support

Architecture

The solution offered presents a security hub within the cloud that provides communications between the security hub, offshore rigs, and customers headquarters. The security hub is provided with redundancy in separate datacenters in Rogaland, Norway.

A remote access firewall is to be deployed at each offshore rig to terminate remote access traffic and provide an encrypted communication line. The remote access firewall can be an existing customer firewall or provided by OCS. Remote access firewalls are optional and not yet priced. Existing firewalls can be used, traffic routing can be done independent of communication barrier.

Cybersecurity Policies and Standard Operating Procedures

OCS's Cybersecurity Policies and Standard Operating Procedures (SOPs) development services include the creation of each policy or procedure. An example of those documents is presented in Table 1.

Table 1: Cybersecurity Policies and Standard Operating Procedures (SOPs)

Cybersecurity Policies		
Document No.	***Document Code***	***Document Name***
1	AC	Access Control Policy
2	AT	Security Awareness and Training Policy
3	AU	Audit and Accountability Policy
4	CA	Security Assessment and Authorization Policy
5	CM	Configuration Management Policy
6	CP	Contingency Planning Policy
7	IA	Identification and Authentication Policy
8	IR	Incident Response Policy
9	MA	Maintenance Policy
10	MP	Media Protection Policy
11	PE	Physical and Environmental Protection Policy
12	PL	Security Planning Policy
13	PS	Personnel Security Policy
14		Risk Assessment Policy
15	SA	System and Services Acquisition Policy
16	SC	System and Communication Protection Policy
17	SI	System and Information Integrity Policy
Standard Operating Procedures (SOP)		
18	SOP	Firewall Policy
19	SOP	Patch Management Procedures
20	SOP	Privacy Policy

Email protection & training

Email-based cybersecurity attacks remain the top vulnerability for individuals and corporations. Currently more than 90% of cyberattacks have been launched through email and the existence of new attack methods are developing at an alarming rate.

To combat these vulnerabilities, OCS offers the global leading suite of email protection technology and services designed by Mimecast.

Comprehensive defense email security

Mimecast's Comprehensive Defense plan is purpose built to provide perimeter protection to safeguard against internal and external email-based threats and to change behavior and lower organizational risk with persistent, engaging security awareness training.

Key benefits:

- Adds protection for inside your network and organization
- Prevents the lateral and external spread of threats
- Makes end-users security assets, not liabilities
- Reduces cyber risk with targeted training for the employees who need it most

Cyber Orchestration

OCS's Cyber Orchestration offering is built on the Splunk Cloud platform which is uniquely designed to capture and orchestrate machine data from wherever it is generated, including physical, virtual and cloud environments. It enables all data to be searched, monitored, and analyzed, in real-time, from one place.

Key benefits:

- **Visibility:** allows the collection of non-security and security data across organizational silos and multi-cloud environments for better investigations and incident response.
- **Efficiency and context:** allows to de-duplicate, collect, aggregate, and prioritize the threat intelligence from different sources improving the security investigations and efficiency as security operations are streamlined.
- **Flexibility:** it is a modern platform of big data that allows you to solve and scale security use cases for your security operations center, compliance, and security operations. It is quite flexible and can be deployed on the cloud, on-premises, or hybrid environment.
- **Behavioral analytics:** optimizes the security operations and speed up the investigation, reduces complexity, and responds to attacks and threats.

Cyber training - Culture development services

Preventing ransomware and phishing attacks training

In an effort to assist our customers, OCS provides Culture Development Services that provides organization employee training in Ransomware and Phishing in an effort to fight off these Social Engineering Attacks. This training is customized for the customer's employees to a personal basis. This philosophy teaches the lesson to the employee on a personal level. Noting that employees that make the connection with the training and make it a habit at home with family will take those habits to work.

The following services are intended to continually educate employees on the importance of the cybersecurity for personal and company protection and to measure the effectiveness of your cybersecurity program.

Monthly phishing exercise/training

Phishing attacks are the most frequent attack vector and are used to spread ransomware and steal user data, including login credentials and credit card. Phishing Exercises are designed to alter employee behavior via real-world phishing simulations to provide a safe, hands-on experience and learning opportunities.

Monthly cybersecurity bulletin

This emailed bulletin informs the company employees of recent cybersecurity information, results of the latest monthly ransomware exercise/training results and provides company policy updates.

Periodic FYI news

This emailed newsletter informs the company employees of recent cybercrime events that could affect them personally.

Communication security

CyphreLink

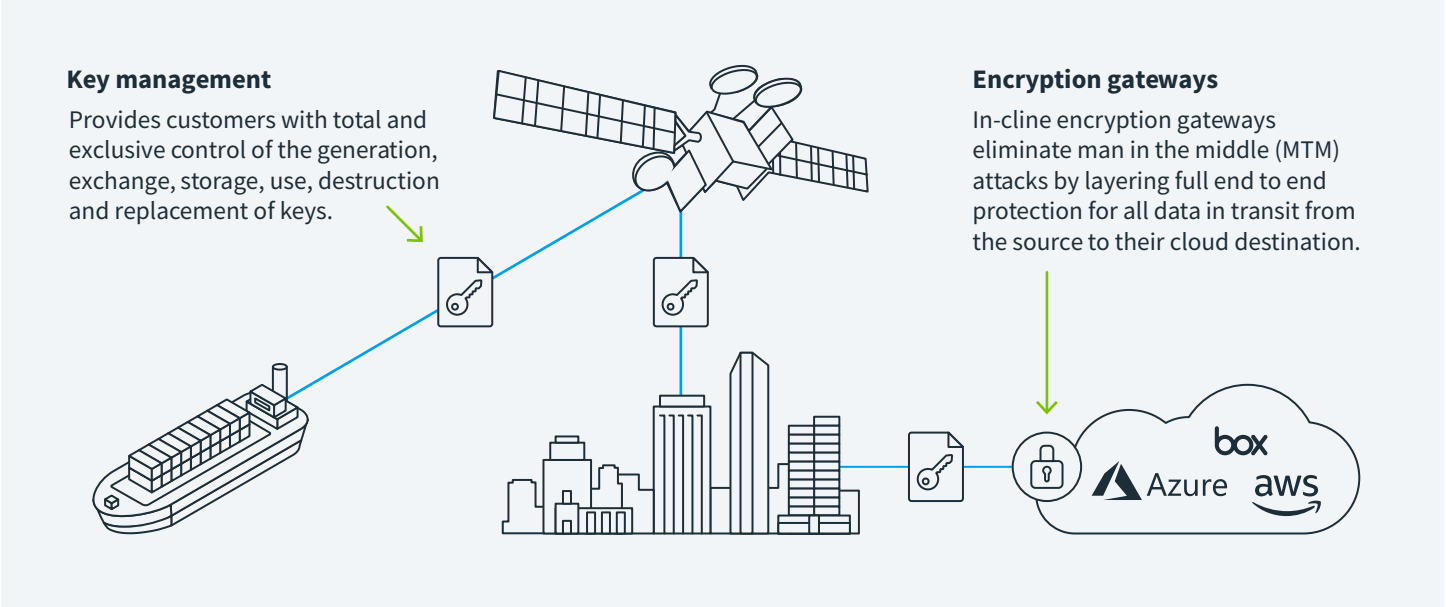
CyphreLink is an advanced data-in-transit solution that provides unassailable encryption for data in-transit, digital certificates, and encryption keys by establishing a highly secure connection between trusted end points.

CyphreLink is an over-the-top solution that interoperates with any type of connectivity including Viasat and other network service providers' existing networks. It is designed to scale and operate at carrier and cloud grade to strengthen the movement of data across a heterogeneous mix of secure private network links, mobile network carrier segments and cost-advantaged open networks. With CyphreLink, enterprises can be ensured that the secure connection across satellite, fixed, or wireless networks can be done with greater flexibility and agility than traditional connections.

CyphreLink is easily incorporated into an enterprise's existing data protection technologies. By serving as a unifying management solution, CyphreLink offers hardened security that reduces man-in-the-middle (MITM) attacks and unauthorized eavesdropping, while expanding the abilities of an organization to leverage virtually any network efficiently and cost-effectively.

CyphreLink key features:

- Seamless access, transmission, and retrieval of data across networks, in the cloud, and with trusted third-party connections.
- End-to-end encryption tunneling maintains data integrity and ensures operational uptime.
- Offloads cryptographic operations outside of accessible host CPU and system memory.



Professional Service Options

Managed Implementation Service

The Managed Implementation service provides customers with an experienced Mimecast Implementation Engineer who will help ensure Mimecast Services are implemented according to Mimecast best practice, whilst helping to ensure that any requirements unique to the customer's current environment or needs are accounted for in full.

Splunk Implementation Services

The Splunk Implementation service improves the implementation, adoption, and care of the Splunk Cloud platform. The service is an annual service that connects customers with Splunk SME's to implement and improve the following areas:

- Tuning Reports & Alerts
- Developing Use Cases
- Developing SPL Queries
- Improving the Efficiency of Splunk SPL
- Admin training
- Dashboard and report creation
- Discovery of additional technology integrations
- Executive dashboard development
- Assistance with ongoing Splunk care
- Awareness Training Implementation Service
- Implementation of the Awareness Training Program.

Global headquarters
6155 El Camino Real, Carlsbad, CA 92009-1699, USA

TEL 703-980-3555 **WEB** viasat.com/cybersecurity **EMAIL** cybersecurity@viasat.com