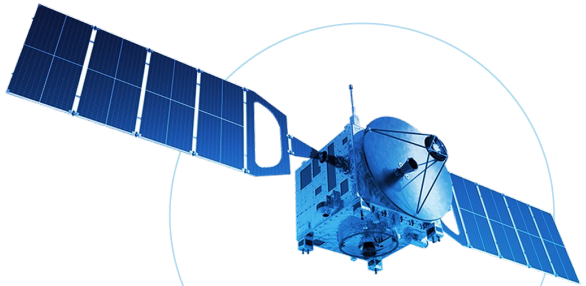
Ground Control

How Satellite IoT Connectivity Supports Data Security Measures



Introduction

Thales' 2024 Data Threat Report[1] found that **42% of Critical National Infrastructure (CNI) organizations have suffered a data breach.** Ransomware attacks are more common, with **28% of CNI organizations experiencing an attack in 2024.** External attackers were considered the greatest threat, overtaking human error, **and 93% of respondents reported an increase in attacks.**

In January 2025, we surveyed **506 American Adults to get their views on cybersecurity measures in CNI, with 82% of respondents stating that they believed organizations were not investing enough in cybersecurity.**

The Healthcare industry gave respondents the greatest concern, with **46% saying they had little to no confidence in their data security,** but no sector scored higher than **31% when it came to moderate or full confidence in their cybersecurity measures.**

62% of respondents said they would feel safer knowing that CNI organizations had backup satellite communications in case of cyber attacks or internet failures.

[1] Downloaded from https://cpl.thalesgroup.com/data-threat-report

Satellite connectivity has some inherent security advantages over cellular networks, but it's not universally more secure in all aspects. It's less susceptible to physical attacks, as most of its infrastructure is operated from space. Satellite signals are also harder to intercept.

Cellular data often passes through local Internet Service Providers (ISPs), which create potential vulnerabilities, including DDoS attacks, 'Man-in-the-Middle' Attacks, and DNS poisoning, whereas satellite communications typically bypass local ISPs, reducing their exposure to regional cyber threats.

But there are a growing number of satellite networks and service options, which in turn deliver varying levels of security. **While satellite networks are often considered to be airgapped because of their lack of dependence on physical infrastructure,** and the ability to transmit data directly from a device to the satellite, most do 'touch' the public internet once the data is returned to the ground station, and forwarded on to the data owner.

The varying levels of data security offered in this process, ranging from having an on-prem ground station to VPNs and firewalls, will be key topics of discussion in this report.

The State of **IoT Data Security** in **Critical Infrastructure**

We surveyed 506 American Adults in January 2025 to find out their level of confidence in the cybersecurity measures of CNI organizations.

Q1: How concerned are you about cyberattacks on critical infrastructure (power grids, water supply, fuel pipelines, etc.)?

On a scale of **'Not concerned'** to **'Very concerned',** the average response was **66/100,** indicating a medium to high level of concern.

Households in the **higher income brackets (>$175,000)** were more concerned **(73/100)** than households in **lower income brackets (<$24,999) (58/100).**

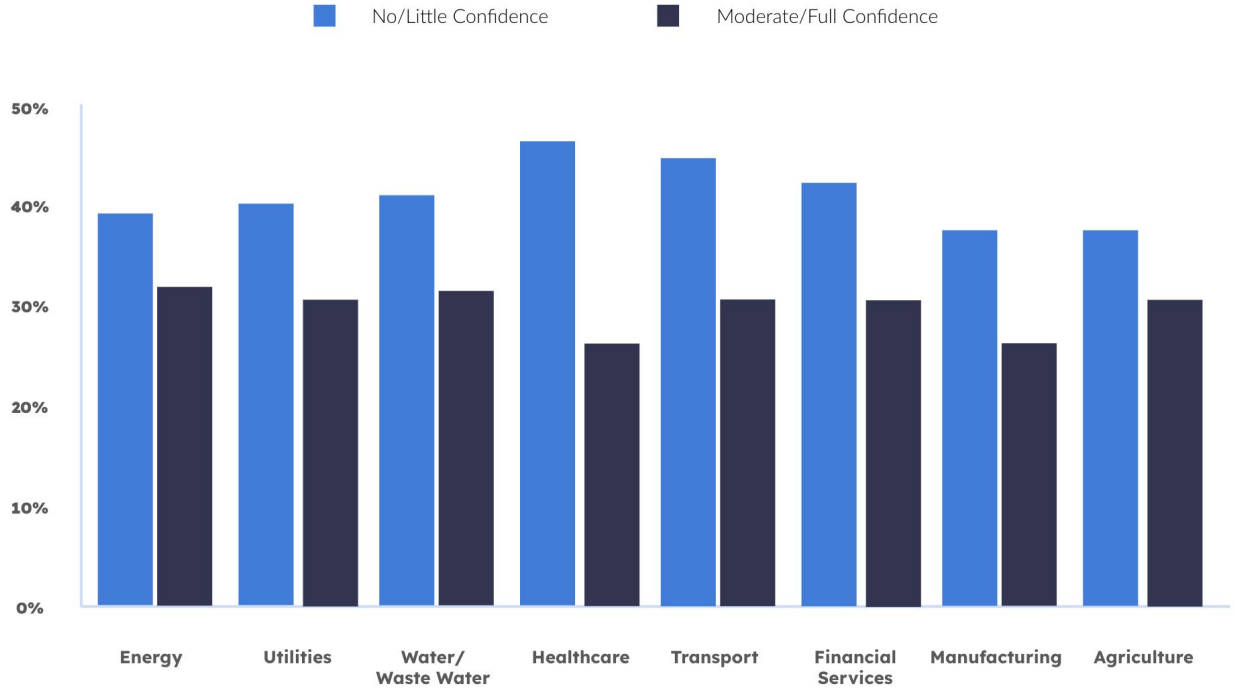
Older respondents **(>60 years old)** were also **more concerned; 75/100** vs. **57/100** for people aged 18-29.

Q2: How much confidence do you have that these essential services are protected from cyberattacks and other security threats?

This indicates that respondents place the **least amount of faith in Healthcare and Transport,** but no industry within the category has won the confidence of the US public.

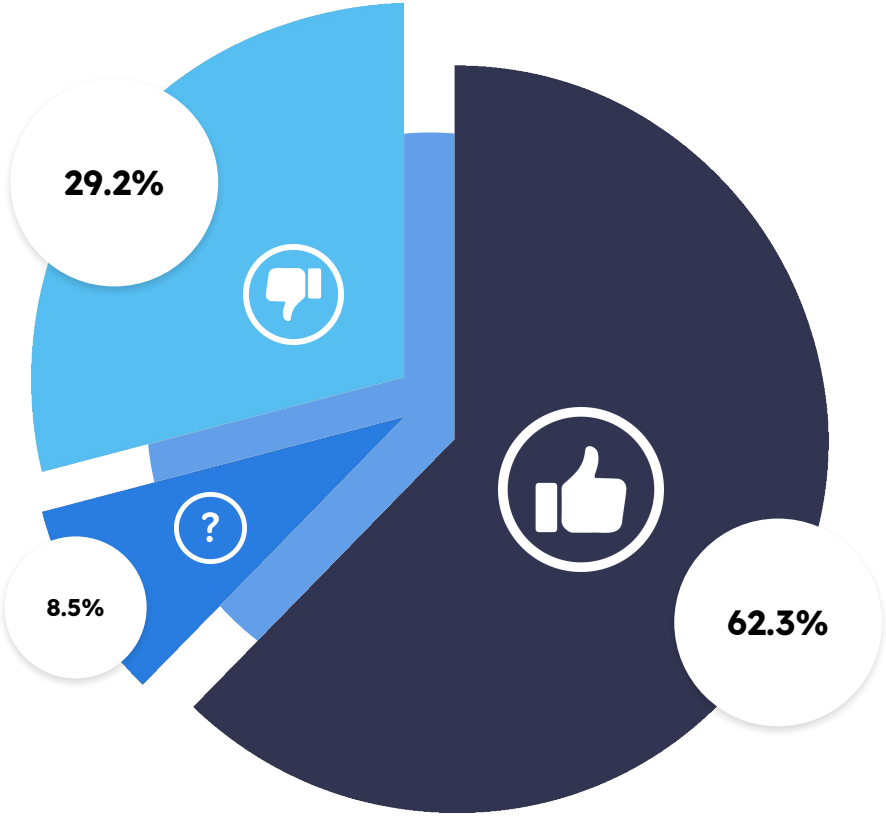
The public's concern is well-founded; **in 2023, the US healthcare sector was the most targeted by ransomware,** followed by Manufacturing and Utilities.[2]

The number of data violation cases in **Manufacturing and Utilities in the United States increased by 270% between 2020 and 2023,** with the cases registered in 2022 alone impacting **23.9 million people.**[3]



[2] Source: https://www.statista.com/statistics/1323599/us-most-targeted-industries-by-ransomware-attacks/
[3] https://www.statista.com/statistics/1367262/us-annual-number-of-data-compromises-in-manufacturing/

Q3: Would you feel safer knowing critical infrastructure had backup satellite communications in case of cyberattacks or internet failures?



Awareness of satellite's role in supporting infrastructure has been raised by the war in Ukraine, in which **Starlink's satellite internet service replaced terrestrial networks degraded or destroyed by Russia.**[4]

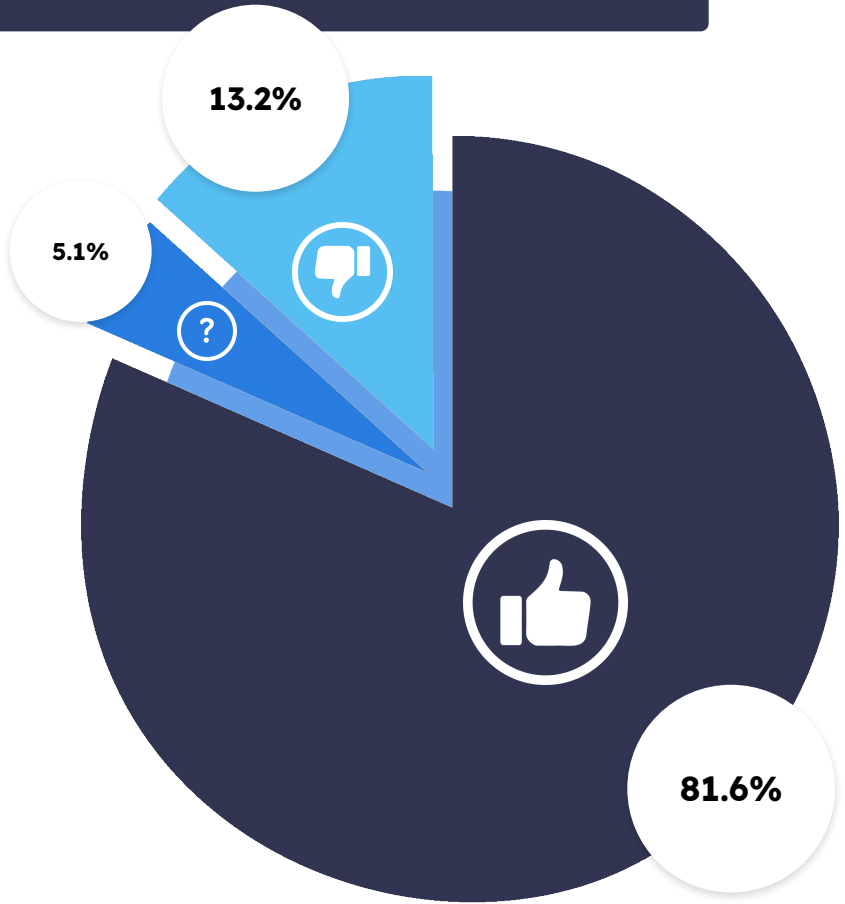
In a similar vein, **Taiwan has contracted Eutelsat OneWeb to deliver low earth orbit satellite internet,** in a bid to address its "technological vulnerabilities" as it comes under repeated cyber attacks from China, who views Taiwan as a breakaway province.[5]

[4] Source: https://www.economist.com/briefing/2023/01/05/how-elon-musks-satellites-have-saved-ukraine-and-changed-warfare
[5] https://www.theguardian.com/world/2024/oct/15/taiwan-to-have-satellite-internet-service-as-protection-in-case-of-chinese-attack

Q4: Do you believe organizations should invest more in cybersecurity for critical infrastructure?

Again, the public's concerns are borne out by the data. In the UK, a recent assessment of **58 critical government IT systems revealed significant gaps in cyber-resilience, with an additional 228 legacy systems potentially at risk.** The National Audit Office (NAO) criticized senior civil servants for not prioritizing cyber-resilience, leading to inadequate investment and staffing.[6]

AI has also helped rapidly advance cyber threats, with **BT reporting a 1,200% increase in bot-driven scanning of systems for vulnerabilities over the past year.**[7] Despite this, the World Economic Forum latest Global Risks Report found that just **11% of respondents were concerned about financial losses, and 12% concerned about reputational damage.**[8]



[6] Source: https://www.theguardian.com/technology/2025/jan/29/cyber-attack-threat-uk-government-departments-whitehall-nao
[7] https://www.theguardian.com/business/2024/sep/12/hackers-weaponising-ai-for-cybercrime-bt-warns
[8] https://www.reuters.com/sustainability/sustainable-finance-reporting/esg-watch-companies-complacent-about-cybercrime-despite-rise-risk-ai-2025-02-03/

The Role of Satellite IoT in Enhancing Security

How Satellite Connectivity Reduces Security Risks

Less Physical Attack Surface

While this isn't a frequently reported issue outside of war zones, the fact remains that cellular infrastructure can be targeted more readily than satellite infrastructure. Notoriously, the 2020 Nashville AT&T data center bombing knocked out cellular, internet and emergency communications across multiple U.S. states,[9] highlighting the vulnerability of centralized telecommunication facilities to physical attacks. **In contrast, satellites are out of reach of most malicious activity, with only the ground stations presenting a target.**

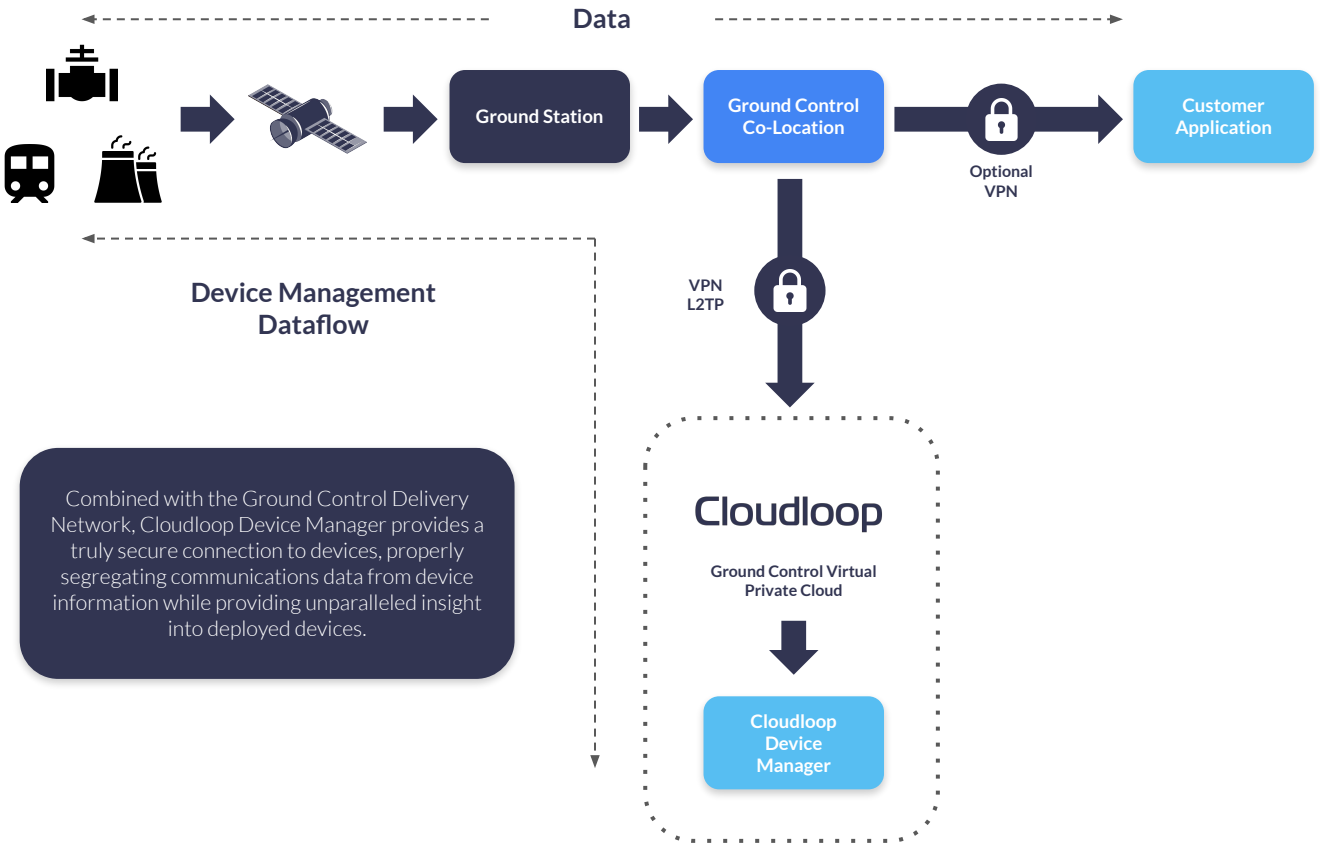
Ground stations are typically located in elevated and remote locations, for improved visibility to their satellite(s).[10] For example, Iridium's ground stations are located in Fairbanks, Alaska; Svalbard, Norway; Tempe, Arizona, and Punta Arenas, Chile. **They need robust security measures - access control, perimeter security, surveillance etc.** - but as the ground stations are limited in number, and often removed from population centers, this is much easier to achieve than with cellular infrastructure.

[9] Source: https://urgentcomm.com/911/tennessee-board-reports-nashville-bombing-impact-on-911-future-plans
[10] https://geoawesome.com/eo-hub/ground-stations-explained-how-does-satellite-data-travel-from-space-to-earth/

Bypassing Local ISPs

It's very common for cellular infrastructure to leverage local ISPs; mostly for backhaul connectivity, but also for roaming agreements. The problem with this is that local ISPs can introduce vulnerabilities including DDoS attacks, BGP hijacking, and DNS poisoning.[11]

Satellite connectivity bypasses this. As the diagram illustrates, data travels from your application to the satellite, then to a ground station. It is then usually moved via a VPN to the customer's application. Service providers like Ground Control shore up the security in this process by co-locating a data center in the same premises as the ground station, providing greater control and flexibility over security measures.



DDoS: Distributed Denial of Service
DNS: Domain Name System
BGP: Border Gateway Protocol

[11] Source: https://medium.com/%40ian_25476/the-imperative-of-cybersecurity-in-telecommunications-are-our-isps-keeping-up-5c06b60dba9a

Harder to Intercept Compared to Cellular Networks

Cellular signals are broadcast from towers and travel in multiple directions, covering large areas. This makes them easier to intercept using relatively simple equipment like IMSI catchers (stingrays) or signal sniffers.[12] **Conversely, satellite signals travel in a focused beam, between the satellite and the ground station; the adversary would need to be within the transmission path to intercept.**

Further, elements of cellular networks still operate on frequencies such as 2G and 3G with known vulnerabilities,[13] whereas satellite networks use multiple frequency bands and proprietary modulation schemes and encryption protocols, making unauthorized interception more difficult.

Satellite signals are also relatively weak by the time they reach Earth's surface, so specialized and highly sensitive receivers would need to be used to pick up the signal; not off-the-shelf radio equipment.

[12] Source: https://sls.eff.org/technologies/cell-site-simulators-imsi-catchers
[13] https://www.p1sec.com/blog/the-phasing-out-of-2g-and-3g-networks-what-it-means-for-telecom-security

Security Considerations: Advantages & Limitations

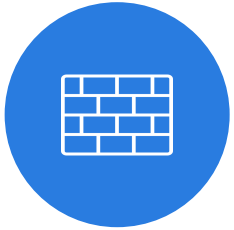
High Encryption Standards by Default

Professionally operated, mature satellite networks such as those operated by Iridium and Viasat encrypt data using AES-256, a symmetric block cipher algorithm recognized for its security and efficiency.

Avoids Man-in-the-Middle Attacks

Satellite networks are much harder to compromise via MitM attacks due to their direct transmission methods, reduced ISP reliance, high-altitude signal paths, and strong encryption.

However, they're not completely immune. As the earlier diagram illustrated, the means by which data is routed from the ground station to the user's application needs consideration. There are several options here with varying degrees of security.



VPNs / Firewalls

The most commonly deployed method for securing data being moved from a ground station is to utilize a combination of firewalls and VPNs.

Feature	Firewalls	VPNs
Main Purpose	Filters and blocks unauthorized traffic	Encrypts and secures data in transit
Protection Level	Defends against cyberattacks & unauthorized access	Prevents eavesdropping & data interception
Where Used?	At ground stations & customer networks	Between the ground station and customer application

Private Wire

Private wire connections create a direct, secure link between a satellite ground station and a customer's network, bypassing the public internet entirely. This can be achieved through dedicated leased lines or private Layer 2 circuits (such as MPLS or SD-WAN). This results in a closed, high-security data path that prevents exposure to cyber threats like DDoS attacks or data interception.

This is a more expensive option but provides CNI, defense and industrial IoT applications with higher security, reliability and compliance.

Private Satellite Network

In this option, your data is returned to a ground station on your premises. It's a service provided by TSAT, a Ground Control partner, whose services we implement. In their words, this segregation provides significant mitigation against typical attacks against terrestrial telecom infrastructure. **Due to the private network implementation, the satellite bandwidth (frequency spectrum) is also not shared by other users.**

TSAT's services are widely adopted in CNI because of the greater physical security afforded by having the ground station physically located within the organization's premises, **and the fact that the data never touches shared channels.**

How Different Satellite Networks Approach Security

When it comes to ground station security, both physical and digital, here's what some key satellite network operators and service providers offer in terms of data security measures.

Viasat | Security Measures

Viasat stands out for its deep-rooted defense expertise, applying security measures from military and government contracts to its commercial IoT and critical infrastructure networks.

Their Cybersecurity Operations Center provides 24/7 threat monitoring, leveraging petabytes of proprietary cyber threat intelligence gathered over 30+ years as a defense contractor. This gives them unique insight into nation-state-level attacks and advanced cyber threats.

For high-throughput industrial IoT applications, Viasat ensures secure data transmission in remote, distributed locations using encrypted VPNs and specialized monitoring solutions designed for energy and utilities.

Their approach integrates IT and OT system security, addressing one of the sector's biggest vulnerabilities. Unlike many providers, they also implement advanced log management and correlation systems, ensuring end-to-end visibility across complex, geographically dispersed infrastructures.

Security Measures

Iridium operates a unique Low Earth Orbit (LEO) satellite constellation, providing global, low-latency, and weather-resilient connectivity. Each satellite is cross-linked to up to four others, creating a redundant mesh network that ensures data can be rerouted efficiently, maintaining communication even if individual satellites encounter issues.

For security, Iridium employs FIPS-140-2 and ASC22FO encryption standards, ensuring that voice and data transmissions remain uncompromised. This level of security is particularly beneficial for U.S. government customers, providing them with secure control of their operations.

Additionally, Iridium's network is independent of local infrastructure, making it largely unaffected by terrestrial safety and security threats. This independence ensures that users have reliable communication capabilities even in remote or disaster-affected areas where ground-based networks may be compromised.

tsat | Security Measures

TSAT offers a fully private satellite network designed specifically for critical national infrastructure. Unlike shared satellite services, TSAT's on-premises gateway eliminates reliance on public telecom networks or the internet, significantly reducing exposure to cyber threats. Its dedicated satellite bandwidth prevents interference from other users, ensuring consistent and secure connectivity.

To counter jamming, spoofing, and cyber intrusions, TSAT employs AES-256 encryption, secure boot processes, and encrypted file systems. Unlike many networks, TSAT does not rely on GPS timing, making it immune to GPS jamming. Its geo-redundant hubs and frequency diversity allow terminals to automatically switch frequencies if interference occurs, ensuring uninterrupted communication.

For resilience against major cyberattacks or satellite failures, TSAT enables multi-satellite diversity. Networks can be split across two independent satellites, ensuring that if one fails, the other remains operational. Organizations can also quickly repoint antennas to restore connectivity.

Since TSAT is a fully private network deployed on-premises, customers maintain complete control over cybersecurity policies to meet compliance standards like NIST, IEC 62443, and GDPR.

Conclusions & Recommendations

As the demand for secure and reliable satellite connectivity grows, particularly in the realm of IoT for critical infrastructure, understanding the limitations and security measures of satellite networks becomes crucial. **While satellite communications offer many advantages, such as global coverage and resilience against physical attacks,** they are not immune to emerging threats like cyberattacks, jamming, and spoofing.

However, with the right mitigation strategies - e.g. encryption, redundancy, and private satellite networks - satellite systems can offer a secure foundation for mission-critical applications. The evolution of these technologies, combined with a strong cybersecurity culture and best practices, will continue to enhance the security of satellite networks, **making them a reliable choice for IoT applications in industries like energy, healthcare, and transport.**

When navigating the complexities of satellite IoT connectivity, it's essential to work with a partner who understands both the technological and security aspects of satellite communication. **Ground Control offers decades of experience in providing satellite solutions that prioritize reliability, security, and flexibility.**

Our expertise in satellite technology, combined with a deep understanding of mission-critical applications, allows us to tailor solutions to meet your specific needs. **By partnering with Ground Control, you gain access to a team that is not only well-versed in the latest satellite technologies but also dedicated to helping you secure your communications, mitigate risks, and ensure that your operations stay connected no matter the challenges.**

Ground Control

We work with CNI organizations in 140 different countries, helping to move data securely and reliably. Please get in touch if you'd like to learn more.

- 20 years' experience
- Unbiased network recommendations
- Great airtime rates
- Future-ready IoT insights
- Satellite IoT platform
- Design and build own hardware

Email: hello@groundcontrol.com

Call: UK: +44 (0) 1452 751940
USA: +1.805.783.4600

Visit: www.groundcontrol.com