cyberhive

Securing satellite communications

Extend your zero trust networks into IoT, OT and remote off-grid locations

Overcoming the combined challenges of high latency and weak security

Businesses strive to increase growth and profitability, and those with Internet of Things (IoT) and Operational Technology (OT) also require secure connectivity between IT systems and industrial networks.

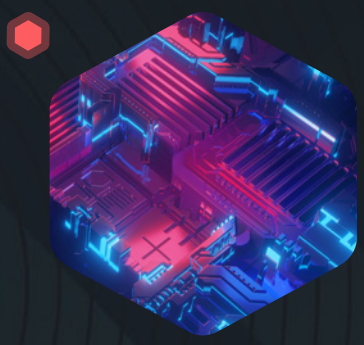
Organisations also need to meet legislative and regulatory compliance, while reducing the risk of a cyber-attack. Traditional solutions that secure data centres, Internet traffic and data communications were designed to operate in a world of very low data latency and lack the reliability needed for remote operations.

Industrial settings that rely upon remote satellite communications require a different approach. Traditional VPNs are simply not reliable enough for satellite use. This is because any interruption of signal can cause network dropouts. Satellite links are also challenging for secure communications, as encryption requires increased network bandwidth.

How can you secure connections between Enterprise IT, IoT and OT to ensure that operations are reliable in remote and rural areas, or where communications on the move are required?

91%

of businesses surveyed by **Inmarsat** believe satellite connectivity is key to improving the effectiveness of IoT solutions



Delivering zero trust network access (ZTNA) across the divide between IT, IoT and OT

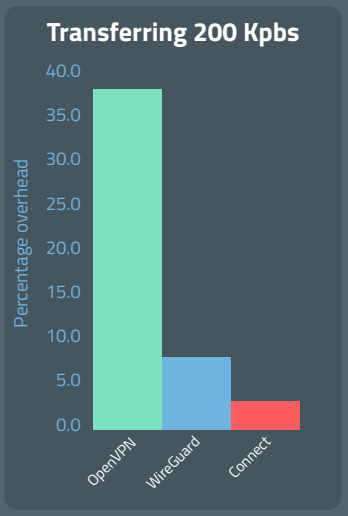
CyberHive has developed Connect, a software-defined mesh network, certified to operate over satellite links and provide a stable and high performing VPN that employs quantum-safe cryptography.

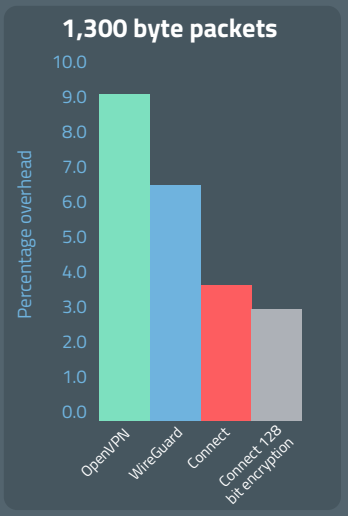
CyberHive Connect implements a zero trust overlay network with extremely low overheads. Performance is maintained, even with high levels of latency or packet loss due to network drop-outs. It further protects the confidentiality and integrity of session traffic with layered quantum-safe cryptography.

The challenge for satellite communications is that NIST standards are difficult to implement in a way that is performant and achieves high levels of cyber security.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CyberHive Connect implements quantum-safe symmetric key cryptography which exceeds the strength of AES-256 and offers faster execution with improved operational efficiency. Connect also adds NIST-approved quantum-safe resistant cryptography for the key exchange.





Key benefits:

- Reduces risk of compromise to IoT installations.
- Low data overheads to keep operating costs down.
- Simple and easy to use, setup and manage.
- Future-proofed against attack by quantum computers.

Certified results:

- Packet overhead is less than 2%, excluding configuration or handshake traffic.
- Added latency is circa 0.4 milliseconds.
- Jitter is less than 0.06 milliseconds.
- Performance over satellite links is not affected at transfer speeds of 200 Kbps even with lost packets.

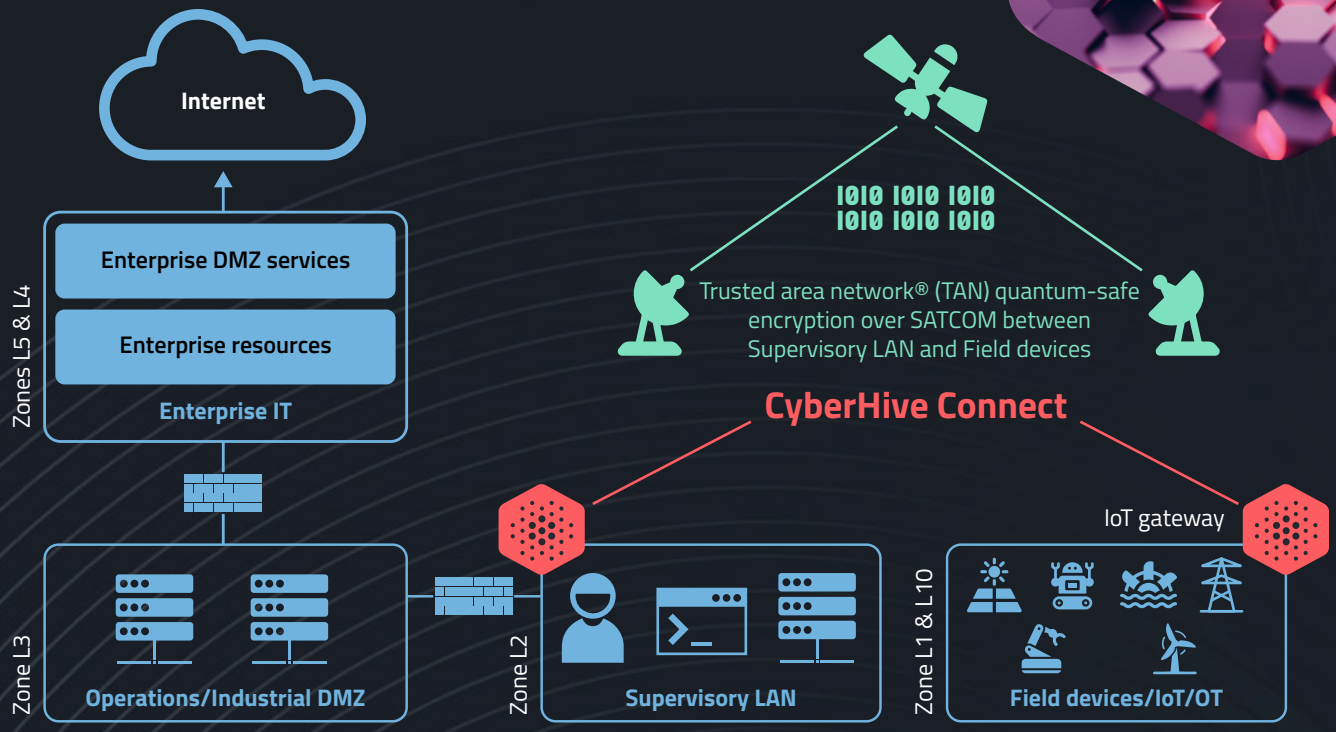
User scenarios

- Predictive maintenance and proactive alerting
- Remote inspections of utilities and energy operations
- Over-the-air (OTA), diagnostics, maintenance and updates
- Aviation
  - more efficient maintenance operations
  - secure communications and redundancy
- Smart farming and precision agriculture
  - autonomous farm machinery and equipment
  - livestock tracking and geofencing
  - sustainable food production and transportation
- Mining and maritime
  - monitoring and transferring data between remote stations/vessels
  - maintenance and updates
  - new configurations and routes
- Government and defence
  - secure communications; intelligence, surveillance and reconnaissance

ISA-99/IEC 62443 set of standards

The ISA-99/IEC 62443 set of standards facilitate simple deployments to a router or IoT gateway from mobile, satellite or any IP based network.

Figure below shows CyberHive Connect in a representative hybrid enterprise and industrial architecture, providing a satellite link between Supervisory LAN and Field devices.



Implementing CyberHive Connect between the Supervisory LAN and Field devices zones

Simple

CyberHive Connect simplifies device management and onboarding when compared to traditional VPN solutions, reducing administrative overhead and the chances of introducing security weakness as the result of human error.

Secure

Quantum-safe forms of encryption are justified due to the threat of 'record and replay' attacks against high value data assets. Furthermore, quantum-safe cryptography should be deployed now to future-proof longer life assets.

Performant

CyberHive Connect excels at creating a highly reliable and performant communications tunnel between enterprise IT infrastructure and the industrial network.

About CyberHive

We build innovative and trusted products, that protect our clients from constantly evolving digital threats.

CyberHive protects the most valued organisations, their people, data and assets, with patented technology that is simple, secure and performant.

Deployed in minutes, we enable our customers to focus on their growth, profitability and innovation.

ISO 27001 CERTIFIED

HM Government G-Cloud Supplier

inmarsat ELEVATE CERTIFIED PARTNER

01635 881881

info@cyberhive.com

www.cyberhive.com

CyberHive
2nd Floor, Newmarket House
Market Street,
Newbury,
Berkshire RG14 5DP