CyberTransporter

Cross Domain Solutions

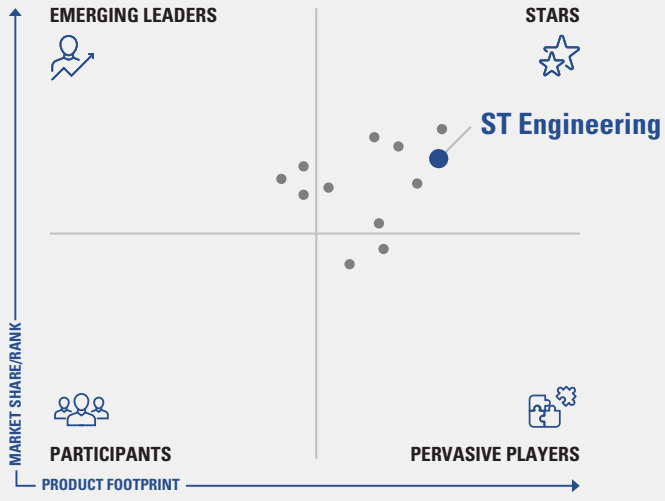
Cyber Resilience for Mission-Critical Networks

As systems grow increasingly interconnected, critical infrastructures face rising exposure to data leakage, cyber intrusion, and command injection, threats that jeopardise national security, public safety, and operational continuity.

CyberTransporter is a purpose-built data diode designed to secure unidirectional data flow between segregated networks. Its hardware-enforced one-way transfer maintains the air-gapped architecture and blocks unauthorised access, ensuring robust protection and delivering confidence in high-security environments.

CyberTransporter 5000 series

CyberTransporter 1000 series



Source: MarketsandMarkets. (2025, January). Data Diode Market Global Forecast to 2030.

MARKETSANDMARKETS™

CyberTransporter recognised as a STAR

in MarketsandMarkets' 360 Quadrant for the Data Diode Market

SECURE WHAT MATTERS

Safeguarding IT/OT Systems from Emerging Cyber Risks

As reliance on connected technologies grows across sectors, critical infrastructure and government systems are increasingly targeted by sophisticated cyberattacks. Between January 2023 and 2024, critical infrastructure worldwide faced over 420 million cyberattacks, averaging 13 attacks every second.[1]

Operational Technology (OT) systems are now increasingly integrated with IT networks to enable data sharing and improve operational efficiency. However, this convergence, combined with limited native cybersecurity and increased exposure through external networks, remote access, and cloud platforms, has introduced significant vulnerabilities. As a result, OT environments have become prime targets for cyberattacks, placing critical operations at heightened risk.

Organisations now face mounting pressure to secure IT/OT convergence against data breaches, operational sabotage, and malicious command injections, threats that can cause reputational damage, essential service disruption, and risks to national security.

As cyber threats grow more advanced, traditional firewalls and software-based controls are proving insufficient:

Data Leakage: Confidential data can be exfiltrated through compromised endpoints or misconfigured systems. Firewalls, reliant on software rules, can be bypassed or misconfigured, leaving critical gaps that enable data loss.

Cyber Intrusion: Remote access tools, phishing, and malware are commonly used to breach isolated systems. Firewalls may allow some legitimate traffic that attackers exploit, especially in complex, converged networks.

Command Injection: Unauthorised commands sent to OT or SCADA environments can halt operations or cause real-world harm. Intrusion detection systems only identify such attempts, they do not prevent them, leaving vulnerabilities unmitigated and systems exposed.

Cyber Realities

$10.5 Trillion

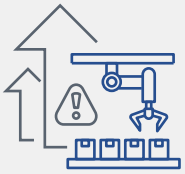
the projected annual global cost of cybercrime by 2025.[2]

$500,000

the average financial impact reported by critical infrastructure organisations hit by cyberattacks.[3]

>450

cyber incidents targeted state institutions and political systems in 2023, making them the second most attacked sector globally.[4]



87%

increase in ransomware attacks on industrial organisations, with manufacturing most affected.[5]

[1] Industrial Cyber. (2024, August 28). Critical infrastructure faces 30 percent surge in cyber attacks, KnowBe4 report highlight.

[2] World Economic Forum. (2023, January 2). Why we need global rules to crack down on cybercrime.

[3] SC Media. (2024, December 24). 5 critical infrastructure sectors hit hardest by cyberattacks in 2024.

[4] World Economic Forum. (2025, March 21). These sectors are top targets for cybercrime, and other cybersecurity news to know this month.

[5] Industrial Cyber. (2025, February 25). Dragos finds ransomware attacks on industrial sector surge 87%, manufacturing hit hardest as OT targeting rises.

CyberTransporter - Air-Gapped Assurance for IT/OT Convergence

CyberTransporter is a high-assurance, hardware-enforced data diode that ensures unidirectional data flow between segmented networks. Designed to meet the cybersecurity needs of governments, critical infrastructure, and enterprises, it safeguards data integrity and system operations while enabling secure IT/OT convergence, file transfers, and real-time network monitoring.

Hardware-Enforced One-Way Security

CyberTransporter uses patented SFP+ modules to enforce physical, one-way data transmission, ensuring no data can flow in the reverse direction. Unlike firewalls that depend on software rules, CyberTransporter eliminates the risk of data backflow, even during system failure. This makes it ideal for mission-critical sectors requiring absolute assurance in air-gapped or network segregated environments.

Zero-Loss, High-Throughput File Transfer

Capable of achieving up to 1 Gbps throughput and handling over 10 TB of files daily, CyberTransporter delivers industry-leading performance with zero-loss transfer rate (tested with over 5 million file transfers). With built-in loss detection and automatic alerting, it ensures operational efficiency and maintaining data integrity across systems, even under high-volume loads or complex workloads.

Easy Integration and Scalable Architecture

CyberTransporter supports a wide range of protocols and features a self-service management portal for rapid deployment. Its modular, stackable hardware design enables seamless integration with third-party tools such as file cleansing, video transcoders, and threat detection systems, providing flexibility and scalability for both government and commercial use.

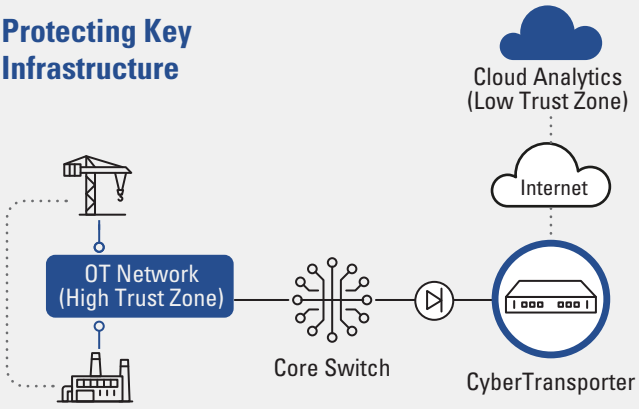
Security Certification

CyberTransporter has been certified at Common Criteria (CC) Evaluation Assurance Level 4+ (EAL 4+) by the Cyber Security Agency of Singapore (CSA), demonstrating compliance with rigorous cybersecurity standards. Attesting to its robust design and reliable operation in government, critical infrastructure, and enterprise environments.

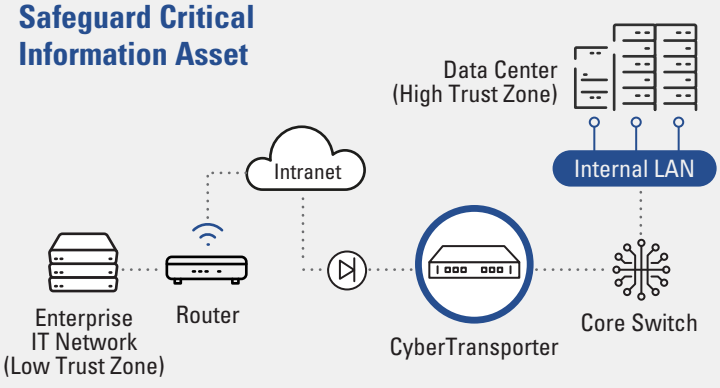
Establishing Trusted Cross Domain Security

CyberTransporter enforces unidirectional data flow to safeguard against configuration errors, insider threats, and firewall limitations, while enabling secure data exchange across high-assurance networks.

Protecting Key Infrastructure



Safeguard Critical Information Asset



CyberTransporter 5000 series

CyberTransporter 1000 series

Scalable Solutions for Every Operational Need

CyberTransporter 5000 Series

- **High-Throughput Operational Environments**
  Supports large-scale data flows of over 10 TB per day with zero-loss transfer and high-speed performance.
- **Critical Infrastructure and National Defence**
  Meets stringent certification standards (CC EAL 4+) for securing classified networks.
- **Multi-Zone Deployments with Redundancy**
  Stackable design supports high availability and load balancing across multiple network domains.

CyberTransporter 1000 Series

- **Compact for Smaller Operations**
  Space-saving and cost-effective for SMEs, branch offices, remote sites, or decentralised facilities with limited IT infrastructure.
- **Air-Gapped Compliance for Essential Services**
  Provides baseline unidirectional data protection for enterprise networks.
- **Network Segregation in Constrained Environments**
  Enforces hardware-level one-way data transfer without complex configuration, ideal for edge or embedded deployments.

Key Features

- **Patented SFP+ technology** delivers hardware-enforced, unidirectional data flow for secure one-way communication.
- **Certified for high assurance** with CC EAL 4+ certification and NITES accreditation from the Cyber Security Agency of Singapore (CSA).
- **Supports up to 1 Gbps daily throughput** with built-in loss detection and automatic alerting.
- **Broad protocol compatibility** ensures seamless integration across diverse systems and environments.
- **Integrated management portal** streamlines configuration, monitoring, and operational deployment.
- **Stackable architecture** enables scalable throughput and redundancy to meet growing operational demands.

Key Benefits

- **Enhances cyber resilience** through air-gapped architectures.
- **Safeguards critical systems** by physically preventing data leakage, manipulation, and unauthorised access, delivering end-to-end confidentiality.
- **Maintains operational continuity with** high-availability design that ensures uninterrupted data flow.
- **Secures IT/OT convergence** by safely transferring real-time data between segmented networks.
- **Future-proofs against quantum-era threats** with hardware-based isolation that blocks advanced network exploits.
- **Enables fast deployment and simplified management** by operating independently of software stacks.

Use Cases for CyberTransporter

CyberTransporter delivers a suite of solutions for secure, unidirectional data flow across segregated networks, ensuring safe information exchange, operational continuity, and compliance in mission-critical and enterprise environments.

	Government	Critical Infrastructure	Enterprise
Secure Network Monitoring Gateway Enables one-way transmission of OT network telemetry to IT monitoring systems, ensuring real-time visibility while preventing inbound threats.	●●●	●●●	●●○
Secure File Transfer Gateway Transfers files safely by applying cleansing, antivirus (AV) scanning, and Content Disarm and Reconstruction (CDR) to remove malware and enforce policies.	●●●	●●●	●○○
Secure e-Application Gateway Protects real-time HTTP(S) services by scanning payloads at the application and network layers, supporting safe bidirectional transactions.	●●●	●●○	●○○
Real-Time Messaging Gateway Delivers low-latency alerts and system events across domains through unidirectional communication, ensuring isolation is maintained.	●●●	●●●	●○○
Secure Email Relay Gateway Protects internal network from cyber threats from email by applying cleansing, antivirus (AV) scanning, and Content Disarm and Reconstruction (CDR) to remove malware originating in untrusted networks.	●●●	●○○	●○○
High-Bandwidth Zero-Loss Gateway Transfers large volumes of files with zero loss using patented retransmission technology, ensuring resilient, high-throughput operations.	●●●	●●●	●○○
Secure Exchange Gateway Synchronises Exchange Servers across disconnected domains to maintain communication while preventing unauthorised access.	●●●	●●○	●●○
Secure Video Streaming Gateway Streams video securely by transcoding and sanitising feeds, removing embedded malware and exploits in real time.	●●●	●●○	●○○
Enterprise Download Gateway Automates secure software patching by downloading, cleansing, and distributing updates across segregated zones, ensuring malware-free transfers.	●●●	●●○	●○○

Recommended Implementation of Cross-Domain Solution:

- ●●● Anchor – Foundational to enforcing cross-domain security controls
- ●●○ Enhancer – Improves security posture and risk mitigation
- ●○○ Complement – Adds value to security but not essential for enforcement

SECURE WHAT MATTERS

ST Engineering Cybersecurity

With over two decades of cybersecurity expertise, ST Engineering's Cyber business has evolved from a focus on cryptography to leading in end-to-end cybersecurity solutions. We protect government entities, critical infrastructure, and enterprises against evolving threats. Our capabilities include operating over 20 global Cybersecurity Operation Centres (SOCs), training 2,500 professionals, and driving innovation through R&D. Leveraging deep engineering expertise, we integrate advanced cybersecurity into communications and industrial systems, empowering organisations to achieve cyber resilience through a comprehensive approach encompassing people, processes, and technology. We secure what matters.

www.stengg.com/en/cybersecurity sg.linkedin.com/showcase/st-engineering-cybersecurity/

ST Engineering