CROSS DOMAIN SOLUTION

ArrowLinx

Data Diode — Secure Information Gateway

Hardware-enforced one-way transfer that keeps mission-critical networks isolated.

ArrowLinx 5000 Series
High performance

ArrowLinx 1280
Compact

Cyber Resilience for Mission-Critical Networks

As systems become more interconnected, critical infrastructure faces growing exposure to data leakage, cyber intrusion and command injection — threats to national security, public safety and operational continuity.

ArrowLinx is a purpose-built data diode that secures one-way data flow between segregated networks. Its hardware-enforced transfer preserves the air gap and blocks unauthorised access, giving high-security environments protection they can rely on.

Air-Gapped Assurance for IT/OT Convergence

ArrowLinx is a high-assurance, hardware-enforced data diode built for the cybersecurity needs of governments, critical infrastructure and enterprises. It safeguards data integrity and operations while enabling secure IT/OT convergence, file transfer and real-time network monitoring.

01

Hardware-Enforced One-Way Security

Patented SFP+ modules physically enforce one-way transmission, so no data can travel in reverse. Unlike rule-based firewalls, there is no backflow risk even during system failure.

02

Easy Integration, Scalable Architecture

Broad protocol support and a self-service management portal speed up deployment. Stackable hardware integrates with file cleansing, video transcoding and threat detection tools.

03

Zero-Loss, High-Throughput File Transfer

Up to 1 + 1 Gbps and more than 10 TB of files a day, with zero file loss across over 5 million test transfers. Built-in loss detection and alerting keep data intact under heavy load.

04

Security Certification

Certified to Common Criteria EAL 4+ by the Cyber Security Agency of Singapore (CSA)*, independently validating the design for government, critical infrastructure and enterprise use.

**CC EAL 4+ certification by CSA Singapore applies to ArrowLinx models 5282, 5283, 5284 and 5285.*

© 2026 ArrowLinx. All rights reserved.

Safeguarding IT/OT Systems from Emerging Cyber Risks

As reliance on connected technology grows, critical infrastructure and government systems are increasingly targeted by sophisticated cyberattacks.

Operational Technology (OT) is now tied into IT networks to share data and improve efficiency. That convergence, combined with limited built-in security and wider exposure through remote access, external networks and cloud platforms, has made OT environments prime targets and put critical operations at risk.

Organisations face mounting pressure to secure IT/OT convergence against data breaches, operational sabotage and malicious command injection — threats that bring reputational damage, disruption to essential services and risks to national security.

As threats grow more advanced, firewalls and software-based controls alone are no longer enough:

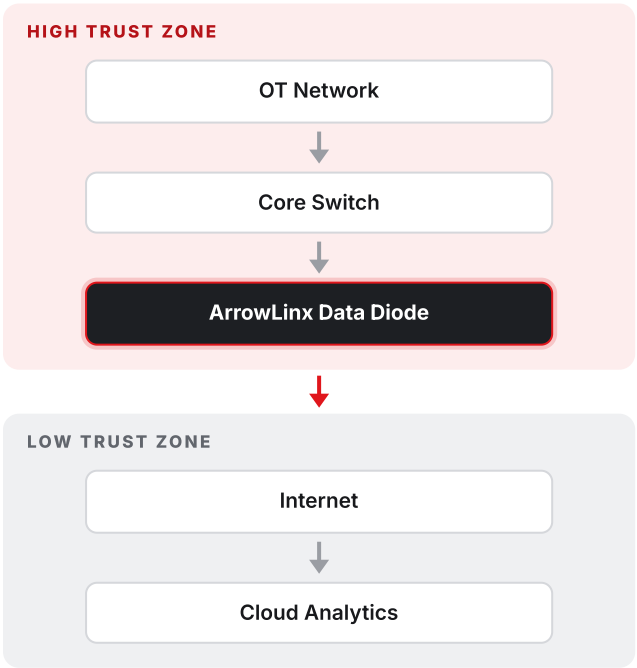
- **Data leakage:** confidential data can be exfiltrated through compromised endpoints or misconfigured systems. Rule-based firewalls can be bypassed or misconfigured, leaving critical gaps.
- **Cyber intrusion:** remote-access tools, phishing and malware are routinely used to breach isolated systems, often riding on legitimate traffic that a firewall lets through.
- **Command injection:** unauthorised commands sent to OT or SCADA systems can halt operations or cause real-world harm. Intrusion detection only flags such attempts; it does not stop them.

Establishing Trusted Cross-Domain Security

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

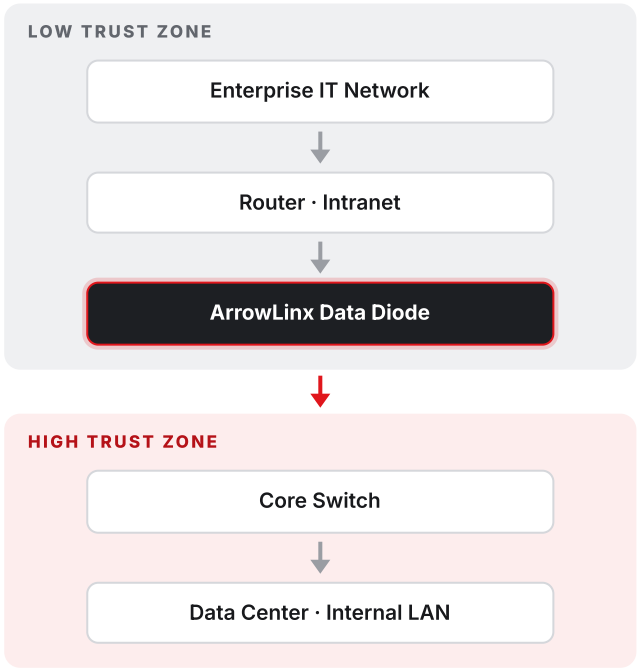
Protecting Key Infrastructure

Data leaves the OT network — nothing can return.



Safeguarding Critical Information Assets

Data enters the data center — nothing can leak out.



© 2026 ArrowLinx. All rights reserved.

Scalable Solutions for Every Operational Need

The ArrowLinx portfolio covers diverse deployment environments, from standard cross-domain sites to high-throughput critical networks.

ARROWLINX 5000 SERIES

High performance

- High-throughput secure data transfer
- High-availability, redundant deployment
- Mission-critical networks and operations

ARROWLINX 1280

Compact

- Standard cross-domain deployments
- Flexible IT and OT environments
- Enterprise and critical infrastructure sites

10 + 10 Gbps
Unidirectional transfer (model 5283)

1 + 1 Gbps
File throughput (model 5283)

1 in 5M
Maximum file loss rate, all models

EAL 4+
Common Criteria, certified by CSA*

KEY FEATURES

- **Patented SFP+ technology** delivers hardware-enforced, unidirectional data flow for secure one-way communication.
- **Certified for high assurance** with Common Criteria EAL 4+ from the Cyber Security Agency of Singapore (CSA).*
- **Up to 10 + 10 Gbps** unidirectional transfer, with built-in loss detection and automatic alerting.
- **Broad protocol compatibility,** including HTTP(S), OPC UA, MODBUS, IEC 104 and MQTT, for integration across diverse systems.
- **Integrated management portal** streamlines configuration, monitoring and operational deployment.
- **Stackable architecture** scales throughput and redundancy as operational demands grow.

KEY BENEFITS

- **Enhances cyber resilience** through air-gapped architectures.
- **Safeguards critical systems** by physically preventing data leakage, manipulation and unauthorised access.
- **Maintains operational continuity** with a high-availability design for uninterrupted data flow.
- **Secures IT/OT convergence** by safely moving 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 simple management** by operating independently of software stacks.

**CC EAL 4+ certification by CSA Singapore applies to ArrowLinx models 5282, 5283, 5284 and 5285. Protocols listed are for the 5000 Series.*

© 2026 ArrowLinx. All rights reserved.

Use Cases for Cross-Domain Solutions

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

Gateway	Government	Critical Infrastructure	Enterprise
Secure Network Monitoring Gateway Sends OT telemetry one way to IT monitoring for real-time visibility, with no path for inbound threats.	●●●	●●●	●●○
Secure File Transfer Gateway Moves files safely with cleansing, antivirus (AV) scanning and Content Disarm and Reconstruction (CDR).	●●●	●●●	●○○
Secure e-Application Gateway Protects real-time HTTP(S) services by scanning payloads at the application and network layers.	●●●	●●○	●○○
Real-Time Messaging Gateway Delivers low-latency alerts and system events across domains while isolation stays intact.	●●●	●●●	●○○
Secure Email Relay Gateway Cleanses, AV-scans and applies CDR to email from untrusted networks before it reaches the inside.	●●●	●○○	●○○
High Bandwidth Zero Loss Gateway Transfers large volumes of files with zero loss using patented retransmission technology.	●●●	●●●	●○○
Secure Exchange Gateway Synchronises Exchange servers across disconnected domains while preventing unauthorised access.	●●●	●●○	●●○
Secure Video Streaming Gateway Transcodes and sanitises video feeds in real time, removing embedded malware and exploits.	●●●	●●○	●○○
Enterprise Download Gateway Downloads, cleanses and distributes software updates across segregated zones, malware-free.	●●●	●●○	●○○

RECOMMENDED IMPLEMENTATION

- ●●● **Anchor** — foundational to enforcing cross-domain security controls
- ●●○ **Enhancer** — improves security posture and risk mitigation
- ●○○ **Complement** — adds value but is not essential for enforcement

Plan your cross-domain deployment

Talk to the ArrowLinx team about the right model for your network.

www.arrowlinx.com
sales@arrowlinx.com

© 2026 ArrowLinx. All rights reserved.