

ArrowLinux: A Buyer's Guide to Hardware-Enforced, Common Criteria-Certified Cross-Domain Transfer

A global buyer's guide to one-way data transfer for OT, cross-domain and high-assurance network boundaries.

WHEN A FIREWALL IS NOT ENOUGH

There is a class of network boundary where a firewall, however well configured, is not considered enough: a nuclear plant's safety network, a power-grid control centre, a defence enclave, a bank's core settlement zone. In each case an auditor, a regulator or a tender requirement asks a hard question — can you prove that data cannot flow back into the protected network, not “is it configured not to” but “is it physically impossible?” A firewall cannot answer that question, because a firewall is software enforcing a policy, and policies can be misconfigured or exploited. A data diode can, because it removes the return path in hardware.

This guide is for the engineer, security architect or procurement lead evaluating one-way data transfer for a network boundary anywhere in the world. It explains what a data diode is and how it differs from a firewall, how ArrowLinux enforces one-way flow, what its Common Criteria certification actually means, where a diode fits in a real OT or cross-domain architecture, and how it compares with the alternatives.

ArrowLinux is powered by ST Engineering data diode technology, delivered globally under the ArrowLinux brand.

WHAT A DATA DIODE IS — AND WHY A FIREWALL IS NOT THE SAME THING

A data diode is a network device that allows data to travel in one direction only, enforced physically rather than by software. The principle borrows its name from the electronic diode, which permits current to flow one way. In a data diode the one-way property is implemented in the optical hardware: traffic is converted to light, sent across a link that has an emitter on one side and a detector on the other, and there is simply no physical component on the return path to carry a signal back. No packet, no acknowledgement, no covert channel — nothing electrical or optical can travel from the receiving side to the protected side.

That is the fundamental difference from a firewall. A firewall inspects two-way traffic and decides, by rule, what to allow. It is an excellent tool and every OT network should have one — but its assurance depends on the correctness of its configuration and the absence of exploitable flaws. A data diode changes the nature of the guarantee: there is no rule to get wrong, because the reverse direction does not exist as a path. For the highest-assurance segmentation — the boundary you must be able to defend in an audit — that distinction is the whole point.

HOW ARROWLINUX ENFORCES ONE-WAY FLOW

ArrowLinux implements the one-way guarantee with a deliberately simple physical design. The device is built from two physically separate boards: a Sender board that connects to the protected (sending) network, and a Receiver board that connects to the receiving network. The two boards are joined only by a pair of customised SFP+ optical modules. The module on the Sender side contains an optical transmitter and no means of receiving, while the module on the Receiver side contains an optical sensor and no transmitter. Data can therefore travel optically from sender to receiver and in no other direction — not because the firmware forbids it, but because the hardware to carry a return signal is not present.

Two further design choices matter to a security reviewer. First, each board has its own independent power supply, which mitigates side-channel attacks — there is no shared power rail through which information might leak between the two sides. Second, because the separation is structural, the device does not rely on a general-purpose operating system that must be patched on a schedule to stay secure; there is no requirement for regular OS updates. The current generation covers the 5000 series (Model 5282 / 5283, version 2.2.1055) and the compact 1280 model, superseding the earlier, now end-of-life 328X line.

WHAT THE COMMON CRITERIA CERTIFICATION ACTUALLY MEANS

“Certified” is a word used loosely in cybersecurity marketing, so it is worth being precise about what the ArrowLinx platform actually holds. The underlying 5282 and 5283 hardware (v2.2.1055) is certified under the Singapore Common Criteria Scheme, operated by the Cyber Security Agency of Singapore (CSA), at assurance level EAL4+ AVA_VAN.5. Common Criteria (ISO/IEC 15408) is recognised internationally under the Common Criteria Recognition Arrangement (CCRA), so the certification carries weight for buyers evaluating the product anywhere in the world, not only in the certifying jurisdiction.

Unpack that string, because each part carries weight:

- **Common Criteria (ISO/IEC 15408)** is the international standard for evaluating the security properties of IT products. A CC certificate means an accredited, independent laboratory — not the vendor — tested the product against a formal Security Target and a defined evaluation methodology.
- **EAL4** is the Evaluation Assurance Level: the depth and rigour of the evaluation. EAL4 is the highest level routinely recognised for commercial products and is the practical ceiling most buyers will see outside of bespoke government evaluations.
- **AVA_VAN.5** is the part that genuinely distinguishes this product. It is the vulnerability-analysis assurance component, and level 5 — the highest — means the product was assessed to resist an attacker with High attack potential, a level chosen for government-grade applications.

For a buyer, the certification does two jobs. It is independent evidence that the one-way property holds under serious scrutiny — the evaluated security requirements (FDP_IFC.2 and FDP_IFF.1 in CC terms) are precisely the information-flow-control properties that make a diode a diode. And it is a procurement asset: when a tender or a regulator anywhere asks for evidence of assurance, an internationally recognised CC certificate valid through 2027 is exactly the artefact that satisfies the requirement, rather than a vendor data sheet.

DATA DIODE VS FIREWALL VS UNIDIRECTIONAL SECURITY GATEWAY

Buyers new to this space often hit a confusing distinction between a “data diode” and a “unidirectional security gateway.” They are related, and the difference is practical rather than marketing.

Property	Firewall	Pure Optical Diode	ArrowLinx (Unidirectional Gateway)
Enforcement	Software rule / policy	Physical hardware	Physical hardware
Direction	Bidirectional, rule-based	One-way only	One-way only
Supports TCP/IP apps (file transfer, OPC, historian)	Yes	No (connectionless traffic only)	Yes, via protocol break and re-origination
Misconfiguration risk	Present	Minimal	Minimal
Independent assurance level	Varies by product	Varies by product	Common Criteria EAL4+ AVA_VAN.5

A pure optical diode guarantees one-way flow at the physical layer, but on its own it cannot participate in a normal TCP/IP conversation. TCP needs a handshake and acknowledgements travelling in both directions; a diode, by design, blocks the return half. So a bare diode reliably carries only connectionless traffic — UDP streams such as syslog, for instance — where nothing needs to come back.

A unidirectional security gateway solves that by adding software on top of the hardware diode. The gateway terminates the protocol on the send side, ships the payload across the one-way optical link, and re-originates the protocol on the receive side — so applications that normally expect a two-way connection (file transfer, OPC, historian replication, SFTP, database replication) work across the diode without ever opening a real return path. ArrowLinx belongs in this category: it is a hardware-enforced unidirectional gateway, pairing the physically one-way SFP+ link with software that moves files and multiple OT and IT protocols natively. Its ZeroLoss capability — built on a patented file-lost-detection mechanism — answers the obvious worry about one-way transfer: if nothing can acknowledge receipt, how do you know a file arrived? The published reliability figure is fewer than one file lost for every five million transferred, at rates exceeding 200 small files per second, with throughput options of 500 Mbps, 1 Gbps and 1+1 Gbps and higher-bandwidth options across the range.

None of this replaces your firewall. The three technologies are complementary: keep the firewall for routine, policy-based segmentation, and add a diode or unidirectional gateway specifically on the flows that must be provably one-way. A robust OT architecture usually has both.

WHERE A DATA DIODE FITS: COMMON DEPLOYMENT PATTERNS

Across the industrial and government networks ArrowLinux serves worldwide, the same handful of patterns come up again and again.

OT-to-IT Data Extraction

Historian, telemetry, alarm and event data has to leave a segmented OT network so the IT or cloud side can run analytics, dashboards and reports. A diode lets that data flow out continuously while guaranteeing the OT zone gains no inbound exposure in return — the analytics platform, however compromised it might one day be, has no path back to the controllers.

Security Log Aggregation

The same shape, pointed at your defenders. Syslog and security events stream one-way from OT and IT systems into a central SOC or SIEM. Because the path is one-way, the monitoring platform — a high-value target precisely because it sees everything — can never become the route by which an attacker pivots back into the systems it monitors.

Secure File and Patch Import

Runs the other direction: updates, patches, anti-virus definitions and engineering files must get into the OT zone, but you do not want a general-purpose inbound connection to carry them. A diode (or unidirectional gateway with ZeroLoss file transfer) imports them one-way, with no reverse channel. This pattern pairs naturally with file-sanitisation at the boundary.

Cross-Domain Transfer

The defence and government use case: moving data from a higher-classification enclave to a lower one, where hardware-rooted separation between domains is a hard requirement rather than a preference. This is the application for which AVA_VAN.5-level assurance was designed.

The industries served map closely onto ArrowLinux's global customer base: government and public security, financial services, high-tech manufacturing, energy and utilities, transport, and healthcare.

THE INDEPENDENT-ASSURANCE ANGLE — WHY ORIGIN AND CERTIFICATION ARE ON THE TENDER

One factor is increasingly explicit in procurement worldwide: vendor origin and the independence of the certifying authority. Procurement gates for critical infrastructure now sometimes screen suppliers for exposure to a single country's jurisdiction. For buyers who need a high-assurance security product while managing that constraint, ArrowLinux offers something distinctive: a platform certified under a national Common Criteria scheme recognised internationally under the CCRA. When a requirement asks for a rigorously and independently certified, non-aligned option, that combination is a credible answer. It is not a claim that other vendors are insecure — it is that origin and certifying authority are themselves selection criteria on many tenders, and on those criteria ArrowLinux scores well.

COMPLIANCE FOUNDATION: COMMON CRITERIA EAL4+ AVA_VAN.5

For buyers anywhere, the compliance anchor is the certification itself. ArrowLinux is built on ST Engineering data diode technology — the same 5282 / 5283 hardware platform (version 2.2.1055) independently evaluated and certified, which gives ArrowLinux a single, internationally recognised piece of evidence to present against almost any framework a regulator or auditor names, rather than a different justification for each one:

- **Independent laboratory evaluation.** The certification was carried out under the Singapore Common Criteria Scheme, administered by the Cyber Security Agency of Singapore (CSA) — an accredited, independent laboratory tested the ST Engineering hardware against a formal Security Target, not a vendor self-assessment.
- **EAL4 — the assurance ceiling for commercial products.** Evaluation Assurance Level 4 is the highest level routinely achieved outside bespoke government evaluations, covering the depth and rigour with which the design and implementation were examined.
- **AVA_VAN.5 — resistance to a High attack potential adversary.** This is the vulnerability-analysis component that most products never reach; it was chosen specifically for government-grade applications and is the detail that distinguishes genuine hardware assurance from a marketing claim of “certified.”
- **Certificate validity.** Issued 8 July 2022 and valid through 8 July 2027, covering the ST Engineering 5282 and 5283 hardware (v2.2.1055) that underpins the ArrowLinux platform.
- **Evaluated security functions.** The certification specifically tested FDP_IFC.2 and FDP_IFF.1 — the formal information-flow-control properties that prove data can move in one direction only. These are exactly the properties an auditor is checking for, whatever the name of the framework governing the deployment.

Because the certification is evaluated against the underlying security property — provable one-way information flow — rather than against any single national standard, it transfers cleanly into the documentation for IEC 62443 zones-and-conduits, ISO/IEC 27001 controls, sector-specific technology-risk rules, or a bespoke government cross-domain

requirement. ArrowLinX works with buyers to map the ST Engineering Common Criteria certificate directly into whichever audit or tender documentation applies.

DEPLOYMENT CONSIDERATIONS BEFORE YOU BUY

- **Confirm the application is genuinely one-way.** The cleanest diode deployments are flows that never legitimately need a return path. If an application expects two-way acknowledgements, you need the unidirectional-gateway protocol software (which ArrowLinX provides) rather than a bare diode — identify this early.
- **Size the throughput to the data, not the headline number.** Historian and event extraction rarely needs the top bandwidth; bulk file or video transfer might. Certified models offer 500 Mbps, 1 Gbps and 1+1 Gbps, with higher options in the range — size this against your real flow.
- **Plan the protocol break.** Each one-way application (syslog, OPC, file transfer, historian replication) has its own configuration on the gateway. Listing the exact flows up front turns deployment into a checklist.
- **Keep the firewall.** The diode handles the must-be-one-way boundary; the firewall continues to do routine segmentation. Defence-in-depth means both.
- **Budget for the certificate's lifecycle.** The current certification runs to 8 July 2027; for long-life infrastructure, factor the product roadmap and re-certification into your plan.

HOW ARROWLINX DELIVERS IT, GLOBALLY

ArrowLinX is delivered in three layers, wherever in the world a deployment is required:

- **Architecture review and sizing.** Engineers map the data flows you need to protect, confirm which of them must be one-way, and determine whether the right answer is a data diode, a unidirectional gateway configuration, an encryptor, or a combination — then size the model and throughput to your actual traffic.
- **Deployment and integration.** Deploy and commission the device on site, configure the one-way applications (historian, syslog, file transfer and the rest), and integrate with your existing OT, IT and SOC systems and your firewall estate.
- **Compliance support and ongoing service.** Help translate the platform's Common Criteria certification into the language of your audit — IEC 62443, NIST, NERC CIP, NIS2, ISO 27001 or a local equivalent — and support the deployment through its lifecycle.

FREQUENTLY ASKED QUESTIONS

What is a data diode, in one sentence?

A data diode is a network device that lets data travel in only one direction, enforced by hardware — an optical link with a transmitter on one side and a sensor on the other, with no physical return path — so a protected network can send data out (or receive it in) without ever exposing an inbound connection that could be attacked.

How is a data diode different from a firewall?

A firewall inspects two-way traffic and allows or blocks it by software rule; its security depends on that configuration being correct. A data diode removes the reverse direction physically, so there is no rule to misconfigure and no return path to exploit. They are complementary — keep the firewall for routine segmentation and add a diode where a flow must be provably one-way.

What certification does ArrowLinX have?

The underlying platform (5282 and 5283, version 2.2.1055) is certified under the Singapore Common Criteria Scheme by the Cyber Security Agency of Singapore at EAL4+ AVA_VAN.5, issued on 8 July 2022 and valid through 8 July 2027. Common Criteria is recognised internationally under the CCRA. The AVA_VAN.5 component means the product was assessed to resist an attacker with High attack potential, an assurance level chosen for government-grade applications.

Can a data diode transfer files, or only simple data streams?

A bare optical diode reliably carries only connectionless traffic such as syslog. ArrowLinX is a hardware-enforced unidirectional gateway, so it adds protocol software that moves files and OT/IT protocols across the one-way link. Its ZeroLoss capability, built on patented file-lost detection, transfers files reliably — the published figure is fewer than one file lost per five million transferred — despite the absence of a return acknowledgement path.

Does a data diode replace my firewall?

No. A diode secures the specific boundary where a flow must be one-way; your firewall continues to handle routine, policy-based segmentation everywhere else. A sound OT architecture uses both, as part of defence-in-depth.

Is ArrowLinx available outside a single region?

Yes. ArrowLinx is a global brand, and the underlying certification is recognised internationally. The segmentation logic — IEC 62443 zones and conduits, IT/OT separation for critical infrastructure — applies equally across regions, and ArrowLinx supports deployments worldwide, working with local partners to map the architecture to whichever regional compliance framework applies.

Talk to Us

If a firewall is no longer enough for one of your network boundaries — if an auditor, a regulator or a tender is asking you to prove a flow is one-way — ArrowLinx is a credible, certified answer, wherever you operate.

Talk to ArrowLinx

www.arrowlinx.com
info@arrowlinx.com

ArrowLinx is a global data diode brand powered by ST Engineering data diode technology. Common Criteria certification details, model numbers and specifications follow the underlying manufacturer's published documentation and the Cyber Security Agency of Singapore's certified-product listing, and may change between product revisions; confirm current details for your procurement.