CYBERSECURITY™
MADE IN EUROPE

Arbit Data Diode 10 GbE

Whitepaper

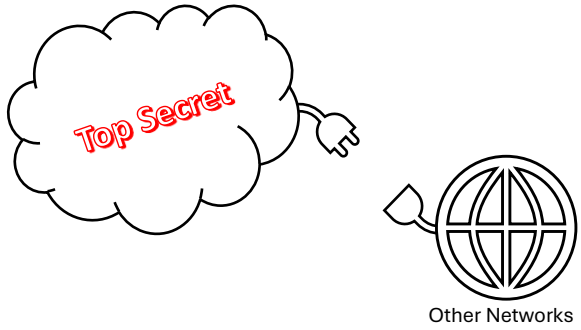
arbit

Table of contents

1. Concept 3
2. The Arbit Data Diode 4
3. Arbit Data Diode Configurations 4
4. Arbit Data Diode Hardware 6
4.1. Core Kit 10GbE 6
4.2. Dell COTS servers 7
4.2.1 Arbit Data Diode Device Configuration 7
4.2.2 Arbit Data Diode Unit Configuration 8
4.3. Ruggedized 9
5. Proxy Servers 10
6. Software 10
7. Filtering 11
8. Data Integrity 11

1. Concept

How do you keep the confidentiality and integrity of highly classified and top-secret networks, where data must always be guarded, and at the same time be able to transfer data across different network domains and classifications without worrying about cyber-attacks, espionage, hackers and data theft? And how do you enable operational efficiency and seamless communication with other networks, when the highly classified networks are air-gapped?



Huge effort is put into ensuring top-secret network separation, implementing strict security processes and perimeter control and deploying dedicated infrastructure and solutions for hardware sealing, filtered power supplies, RF-shielding of equipment / TEMPESTing and more.

That is why it is challenging to exchange data from highly classified networks and create interoperability using common IT tools and processes, as the security risks are simply too high.

Enter the Arbit Data Diode: Arguably the most secure method of transferring data across network domains.

Imagine a turnstile gate, that you exit through after a long and fun day at your favorite amusement park. However, once you exit through that turnstile, there is no way of entering again through that gate. The same concept applies to Arbits Data Diode, which is a network device relying on the laws of physics that provides superior network security over software firewalls as no ports are ever exposed.

The Arbit Data Diode solves the challenge by allowing secure connectivity and integration towards other networks, through Galvanic Separation, a fundamental security concept, whereby light is allowed to pass through unidirectionally (the turnstile), to allow data import from other networks into the air-gapped and top-secret network.

However, using any Data Diode is not necessarily a guarantee of high security and some Data Diodes are definitely more secure than others. To determine which Data Diode is most secure, you must look at its EAL, (Evaluation Assurance Level) certification, which is an international cyber security standard known as the Common Criteria, defined through ISO 15408, the international standard for evaluating the security properties of IT products and systems.

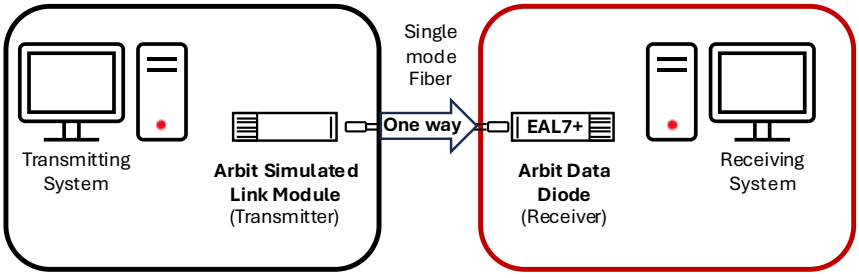
The Common Criteria has several components and concepts that standardize how security claims are made and validated, which are defined in 7 levels of confidence so to say. The higher the confidence level, the higher the extent of validation and verification performed. EAL7+ is the highest certification level achievable and certifies that a product, its design and its entire delivery process, from manufacturing to deployment, have been formally verified and tested providing maximum assurance.

Therefore, organizations that accept no risks to their security profile and have highly sensitive information to guard, opt for EAL7+ certified solutions, like the Arbit Data Diode which is EAL7+ certified and offers a 100% guaranty that it only sends data in one direction!

On top of the EAL7+ certification, the Arbit Data Diode has received NATO COSMIC TOP SECRET and EU TOP SECRET accreditations allowing it to protect and safeguard Government, Military and Intelligence networks from espionage and cyber-attacks across Europe and NATO countries.

2. The Arbit Data Diode

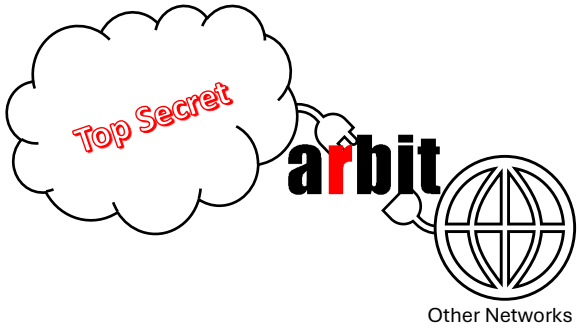
The fundamental components of the Arbit Data Diode consist of two SFP+ modules connected with a fiber optical cable. The sending SFP+ module is a unidirectional transmitter called an Arbit Simulated Link and the receiving SFP+ module, also unidirectional is the main Arbit Data Diode component. Connecting these two SFP+ modules with a single mode fiber cable creates a unidirectional connection between a transmitting system and a receiving system.



This guarantees that no data can be retrieved from the receiving system, as it is physically impossible to send any data back through the one-way fiber optical connection, making the Arbit Data Diode the perfect solution for Cross Domain information exchange offering network protection, preventing amongst other things:

- Data leakage
- Hacking
- Unauthorized access
- Unsafe data transfer
- Cyber attacks

This is the principle behind Arbit's strength, which has received the highest evaluation assurance level for IT products in the world, the Common Criteria EAL7+, certified by BSI the federal authority for cybersecurity in Germany. The Arbit Data Diode's security feature is enforced at the quantum level, hence the term Quantum Firewall. It is a physical data diode based on optics and semiconductors, without any software, microcode, or other processor logic involved.



This is why Government, Defence and Intelligence agencies rely on the Arbit Data Diode, part of a suite of solutions in the Arbit Cross Domain portfolio, for uncompromising cyber security to keep their networks isolated and protected against remote exploitation and data exfiltration yet allow them to be connected at the same time.

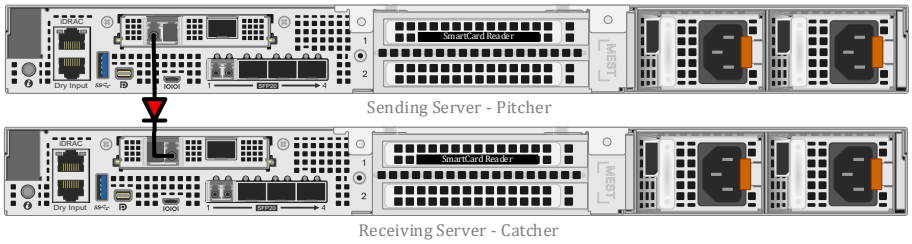
3. Arbit Data Diode Configurations

The Arbit Data Diode is a flexible and modular solution allowing several deployment options and configurations.

The basic solution can be delivered as 2 SFP+ modules and a fiber cable, called a Core Kit. This acts as a pure L2 device, that can be used as an example for streaming services relying purely on UDP protocol transfers.

For other types of services requiring file handling and other types of protocols, the solution consists of a Sending Server, called a Pitcher equipped with an Arbit Simulated Link SFP+ module that transmits data to a Receiving

Server called a Catcher equipped with the EAL7+ certified Arbit Data Diode 10GbE unidirectional SFP+ module. The Pitcher connects to the sending network, and the Catcher connects to the receiving network.



The Arbit Data Diode is designed to function in three different configurations:

Configuration	Features
Core Kit (L2 Device)	The Pitcher and Catcher offer simple UDP-forwarding with no further functionality.
Unit	The Pitcher and Catcher offer the following protocols for transporting data: **Protocol** / **Application examples** UDP – Video/audio streaming, SPLUNK integration, syslog TCP via UDP – System integration using TCP (one way) NTP – Time synchronization In this configuration the Pitcher and the Catcher rely on external applications, such as the Arbit Web Gateway, the Arbit Desktop Gateway or other customized applications to provide file handling and protocol conversions, running on proxy servers. The systems run with read-only disks storing the OS and the Pitcher / Catcher SW and configuration can be saved on Smartcards for added security hardening. Configuration Management is done through the Arbit Configurator. Filters can be applied for additional content screening. Proxy servers can be virtualized.
Device	The Pitcher and Catcher offer the following protocols for transporting data: **Protocol** / **Application examples** UDP – Video/audio streaming, SPLUNK integration, syslog TCP via UDP – System integration using TCP (one way) NTP – Time synchronization SMTP – E-Mail transfer FTP/SFTP – File transfer, Centos/Ubuntu offline repository, WSUS SMB Forward – Windows share forwarding SMB Mirror – Windows share mirroring Localhost/NFS Forward – Network File System share forwarding Localhost/NFS Mirror – Network File System share mirroring HTTP/HTTPS – REST API forwarding, Server-Side Events, Command and Control, WSUS, Web Services MQTT – Telemetry OPSWAT Vault – OPSWAT Kiosk-to-Vault and Vault-to-Vault OPSWAT CDR – OPSWAT data sanitization (Content Disarm and Reconstruction) In this configuration, file handling is supported directly on the Pitcher and Catcher. Configuration Management is done through the inbuilt browser-based User Interface.

4. Arbit Data Diode Hardware

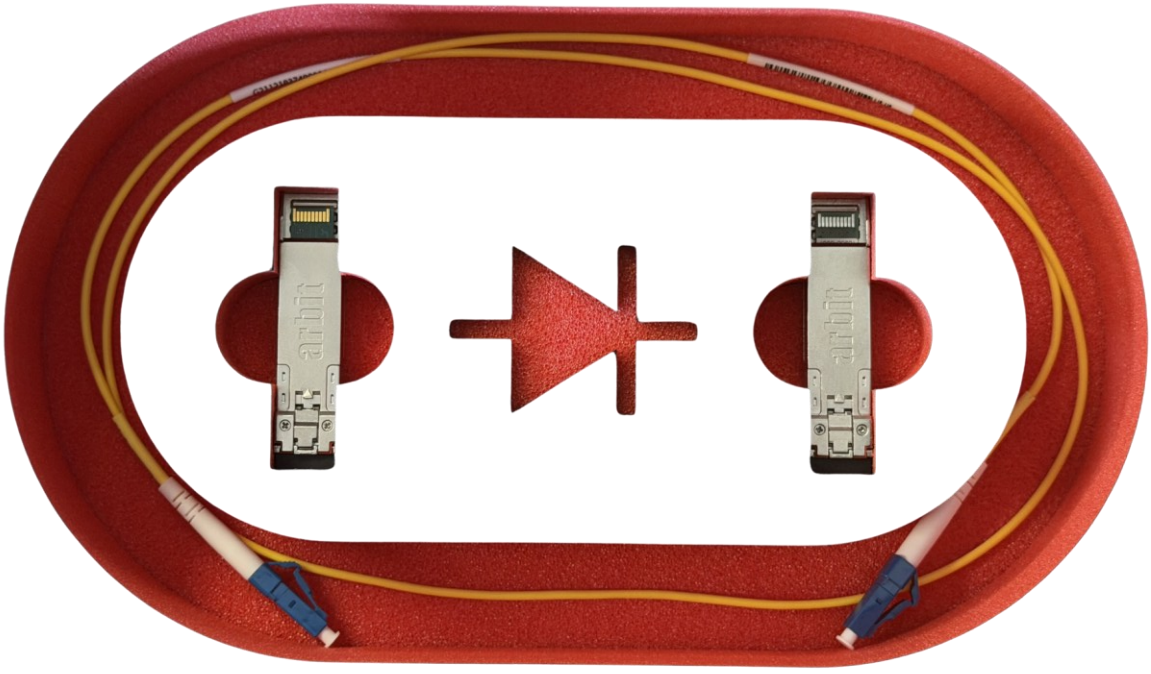
The Arbit Data Diode is available in three form factors:

- Core Kit (10GbE): This deployment option corresponds to the L2 Device configuration described in the table above and consists of 2 SFP+ modules and a single-mode fiber cable.
- Dell COTS servers (10GbE): This deployment option corresponds to the Unit or Device configuration above and the hardware is designed for server room usage.
- Ruggedized (1GbE): This deployment option corresponds to the Unit or Device configuration above and the hardware is designed for battlefield usage and is limited to 1GbE.

4.1. Core Kit 10GbE

The Core Kit consists of the following components:

- Arbit Simulated Link Module 10GbE
  Transmitter-only SFP+ module with TOSA, 10GbE
- Arbit Data Diode Module 10GbE
  Receiver-only SFP+ module with ROSA, 10GbE, EAL7+ certified
- Fiber Cable
  LC-LC single-mode fiber, 1310 nm, up to 20 km



The Core Kit is ideal for deployments where a minimal footprint is required, and simple UDP forwarding use cases, such as video streaming. Simply plug-in the SFP+ modules in existing network equipment and you can achieve a unidirectional flow of data while ensuring 100% galvanic separation and network protection.

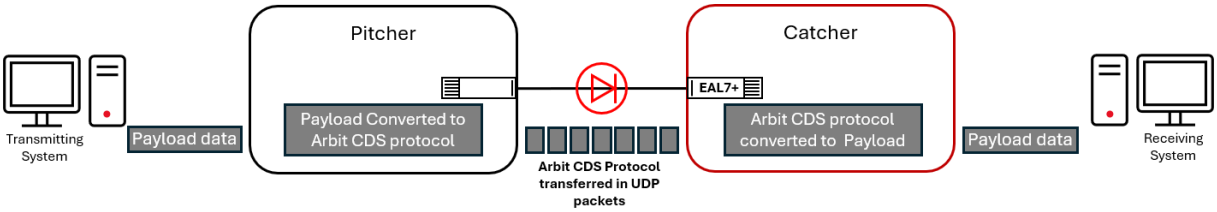
4.2. Dell COTS servers

This hardware configuration designed for data center deployments relies on two Dell COTS servers comprising of a Sending Server, called a Pitcher, equipped with an Arbit SimLink SFP+ module that transmits data to a Receiving Server, called a Catcher, equipped with the EAL7+ certified Arbit Data Diode 10GbE unidirectional SFP+ module. The Pitcher connects to the sending network, and the Catcher connects to the receiving network.

4.2.1 Arbit Data Diode Device Configuration

When deployed as a Standalone Arbit Data Diode Device, the supported server configuration is the Dell PowerEdge R360 and is delivered with 3.84 TB of storage and 32 GB of RAM.

In this Device configuration, the Pitcher and Catcher perform file handling and protocol conversion on their own, while also ensuring galvanic separation and unidirectional transfer of data from the sending side to the receiving side. Files are stored on the disks to allow the file handling and protocol conversion processes to happen.



The main mode of operation of the Arbit Data Diode Device is to monitor a certain folder for data and ensure that it is transferred to the receiving side, while performing the necessary protocol conversions for that operation to happen. This configuration also supports Filters, which may perform a wide variety of custom-made actions and content checks, for additional verification. Refer to section 7. Filtering for more information.

Pitcher

Catcher

Configuration of the Devices is performed using an inbuilt browser-based User Interface.

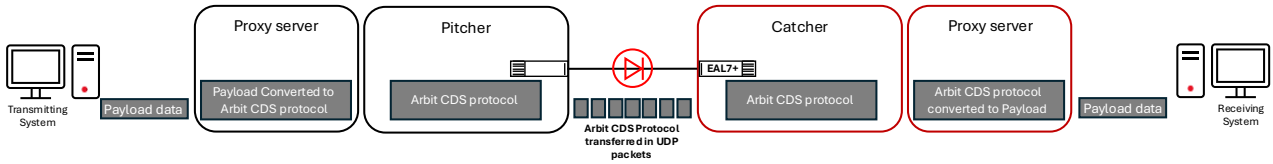
4.2.2 Arbit Data Diode Unit Configuration

When deployed as an Arbit Data Diode Unit, the supported server configuration is the Dell PowerEdge XR5610 and is delivered with 16GB read-only SSD storage and 32 GB of RAM.

Pitcher

Catcher

In Unit configuration, the Pitcher and Catcher rely on external applications for file handling and protocol conversion, and the main job of the Arbit Data Diode in this case is to provide galvanic separation and unidirectional transfer of data from the sending side to the receiving side. No files are stored as the disks installed in these Units are read only and contain the OS and the Pitcher/Catcher SW only.



The Arbit Web Gateway and the Arbit Desktop Gateway are amongst the applications that transport data through this type of setup. The Arbit SDK allows for development of own applications, providing freedom of choice for customers to tailor solutions according to their needs. Proxy servers may also be used to support higher capacities of storage, and these proxy servers can also be virtualized.

Configuration of the Units is performed using the Arbit Configurator and the configuration are stored on Smartcards for enhanced security hardening. This ensures added security against tampering and unwanted and unlawful configuration changes. This configuration also supports Filters, which may perform a wide variety of custom-made actions and content checks, for additional verification. Refer to section 7. Filtering for more information.

Dell COTS Pitcher and Catcher Server Specifications

HW Specifications	Value	
Configuration Type	Arbit Data Diode (Unit Configuration)	Arbit Data Diode (Device Configuration)
Supported server	Dell PowerEdge XR5610	Dell PowerEdge R360
Memory and Storage	32 GB RAM / 16 GB Read Only SSD	32 GB RAM / 8 x 480GB SSD (3.84 TB)
Diode principle	Hardware based (optical)	
Backflow	None (secured by the laws of physics)	
Certification	Common Criteria EAL 7+	
Fiber technology	Single mode 1310 nm	
Diode NIC speed	10 Gigabit	
Server Size	1U, 19” (two units required for a complete diode: 1 Pitcher and 1 Catcher)	
Server Weight	Max. 11 kg	
Power supply	2 x 100-240 VAC 50/60 Hz (Hot swap redundant)	
Dimensions (W x H x D)	19” x 1U x 463 mm	

4.3. Ruggedized

For battlefield and other harsh environments, the Ruggedized Arbit Data Diode is engineered and tested to international standards. It delivers unparalleled operational reliability, flexibility, and environmental resistance in mobile and stationary installations. Designed to support a range of military standards, to withstand the extreme environments it can be deployed in.

It is based on the same Arbit Data Diode for unidirectional communication, Common Criteria EAL7+ certified by BSI with a ruggedized form factor. The main difference between the Dell COTS server version and the ruggedized version, besides the physical casing, is the throughput value which is 1GbE for the ruggedized version.

The ruggedized Arbit Data Diode enhances operational efficiency on the Battlefield allowing for seamless C2 Integration.

Ruggedized Server Specifications

HW Specifications	Value
Processor	3× Intel Atom® x7835RE (each with 8 cores)
Power	Input 12–36 VDC
Operating Temperature	-40°C to +60°C
Storage Temperature	-40°C to +71°C
Humidity	95 ± 4% RH (MIL-STD-810H)
IP Protection	IP65 (Solid: 6X, Water: X5)
Shock Resistance	40 g / 11 ms (MIL-STD-810H)
Vibration	Wheeled (20), tracked (20), helicopter (14) (MIL-STD-810H)
EMI/EMC Compliance	MIL-STD-461F (RE102, CE102, CS114)

Dimensions	(WxH) 220 × 43.4 mm
Rack Depth Compatibility	400 mm including cable clearance
Weight	3,5 kg

5. Proxy Servers

Proxy Servers can be used together with the Arbit Data Diode, when it is deployed in the Unit configuration. Proxy servers must fulfill the following minimum requirements in case of physical HW:

Feature	**Minimum requirement (industrial)**
CPU	4 (not counting hyper-threading)
CPU architecture	x86 64 bit (AMD or Intel)
RAM	32 GB
Disk type	SSD Mixed Use
Disk configuration	JBOD
RAID controller	Linux OS compatible
Disk space	*<daily amount of traffic>* multiplied by *<days to store traffic for retransmission>* multiplied by 2
Network interfaces	2 (one of which must be either: 1000BASE-T, 10GBASE-T or 10GBASE-LR)

Proxy Servers can also be deployed virtually, giving more freedom of choice.

Arbit provides appropriate server configurations according to the specific use case.

6. Software

The Arbit Data Diode software has the following features:

Feature	**Value**
Network speed	10 GbE (Dell COTS HW) or 1GbE (Ruggedized HW)
Supported protocols	Please refer to section 3. Arbit Data Diode Configurations.
Custom protocols/services	Yes, either developed by Arbit, end customer or third party.
Transmission error detection	Yes
Automatic error correction	Yes, on all services except raw UDP steaming.
MTBF	< 3,75 *10^{-10} packets
Maximum file size	Half free disk space on proxy server (or 2^{64}-1 bytes)
Management interface	Web interface or Arbit Configurator
Retransmission	Manual by web-interface on Pitcher
Traffic overload protection	Back pressure and safe points on Pitcher
Data channels	No fixed boundary on the number of data channels through the diode
Data channel priority	Yes, transaction based
Regular maintenance	None (the system runs unattended)
Operating System (Unit)	Hardened SUSE Linux
Operating System (Device)	Latest Red Hat or Ubuntu Server

7. Filtering

The Arbit Open API for added Security and Content Filtering is an inherent part of the secure by design philosophy and architecture of the Arbit Cross Domain Solutions.

The Arbit Open API provides users total control over their data that passes through the Arbit Data Diode, simplifying integration towards for example Command and Control systems, Battle Management Systems or any other SW application. It allows customers to flexibly control and shape their security profile as they see fit, as it provides an added layer of verification when importing data through the Arbit Data Diode.

Arbit CDS solutions deployed in Multi Domain Operation scenarios, require integration between several classifications, physical domains and even across borders, where multiple protocols and standards are in play. The Arbit Open API enables secure integration of connectivity and communication when dealing with for example Federated Mission Networks using the Tactical Assault Kit platform with the Cursor on Target protocol.

The Arbit Open API can be used for creating filters or labelling services and the like that verify and check data against certain standards, such as STANG 4774 / 4778.2 which then gives a go/no-go decision to determine if that data should be allowed to pass through the Arbit Data Diode or not.

The Arbit Open API also enables easy integration towards external applications, such as virus scanners like ClamAV or MetaDefender from our partner OPSWAT, to ensure malicious code doesn't get imported, into a secure network.

8. Data Integrity

The Arbit Data Diode utilizes several layers of data integrity:

1. The unidirectional transport is based on UDP which includes a checksum ensuring that the individual packages are not corrupted.
2. On top of the UDP transport the data diode maintains strict transaction control, which is able to detect any lost packets, which ensures that all packages are processed in the correct order.
3. When transporting files and supporting TCP-like streams, the data diode uses a forward error correction algorithm which prevents almost all network transmission errors.
4. All files are verified by checksum after arrival on the Catcher.
5. A retransmit cache on the Pitcher ensures that any transmission errors due to hardware or power failures can be retransmitted manually.