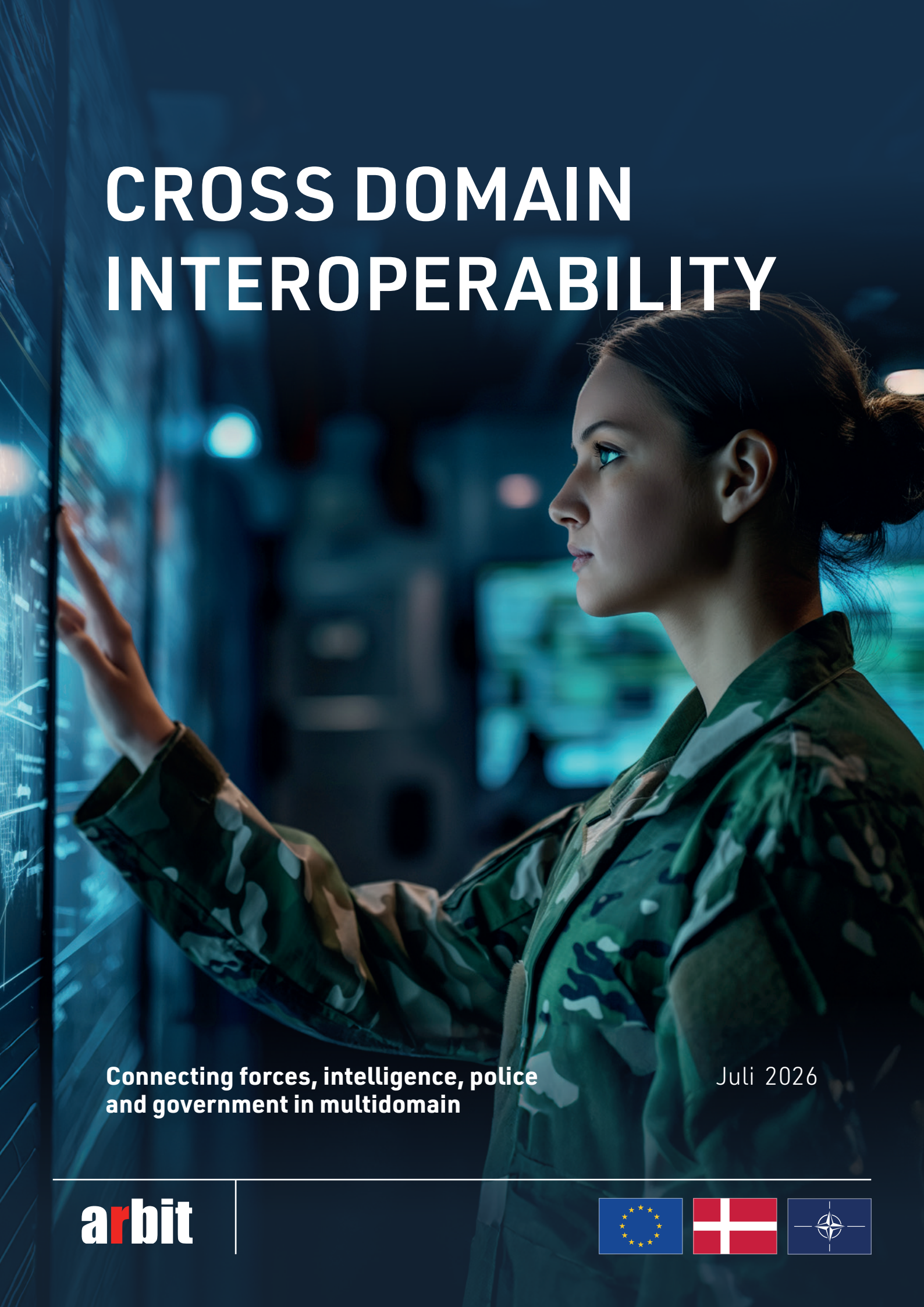
CROSS DOMAIN INTEROPERABILITY



Connecting forces, intelligence, police and government in multidomain

Juli 2026

arbit

20 Years of Connecting Forces

Arbit Cyber Defence Systems, based in Copenhagen, Denmark, was founded by Rasmus Borch and marked its 20th anniversary this summer, providing Cross Domain Solutions based on quantum technology tailored for organizations with stringent security and confidentiality requirements, such as intelligence agencies, police, defence, and infrastructure.

Our domain: Arbits' legacy and deep domain knowledge, originates from the intelligence community, focusing solely on Cross Domain Solutions designed to securely manage data transfers between networks of different security classifications and guarantee a unidirectional communication channel that enhances security while reducing costs, human error, and insider threats.

Arbit solutions are proven in Bold Quest from Georgia, US to Finland and are RUGGED ready to be deployed in challenging conditions on the battlefield, offering a Gateway (IEG) with reliable data management and C2 communication between security domains in military operations.

Certification: The company's most notable certification is the German Evaluation Assurance Level (EAL7+) for its Arbit Data Diode, a rare and high-level accreditation, NATO COSMIC TOP SECRET and EU TOP SECRET, which signifies the products compliance with the most rigorous security standards for information technology products. We are in the process of acquiring an EAL4 certification for the Arbit Trust Gateway

Clients: Arbit's expertise has attracted clients from all of Europe, the Middle East and Asia. Including the Danish Ministry of Defence Acquisition and Logistics Organisation (DALO) who has entered into a 20-year framework agreement with Arbit. This partnership is aimed at providing the Danish Armed Forces with advanced Cross Domain Solutions, underscoring a long-standing relationship between DALO and Arbit to enhance digital security and operational effectiveness.

Contribution: In recognition of our contributions to cybersecurity, Arbit became the first company in Europe to receive the "Cybersecurity Made in Europe" label from the European Cyber Security Organization (ECSO). And with our participation in international defence forums and projects, such as NATO EDGE, NATO CWIX, and European Defence Fund (SESIOP) we hope to demonstrate our commitment to advancing cybersecurity solutions that meet the needs of protecting and securing Governments or organizations around the world.

It's all about Trust: Arbit's success is shared through collaboration with clients, selected technological and strategic partners. Because for the founder, it is all about Trust. Let's Connect Forces.

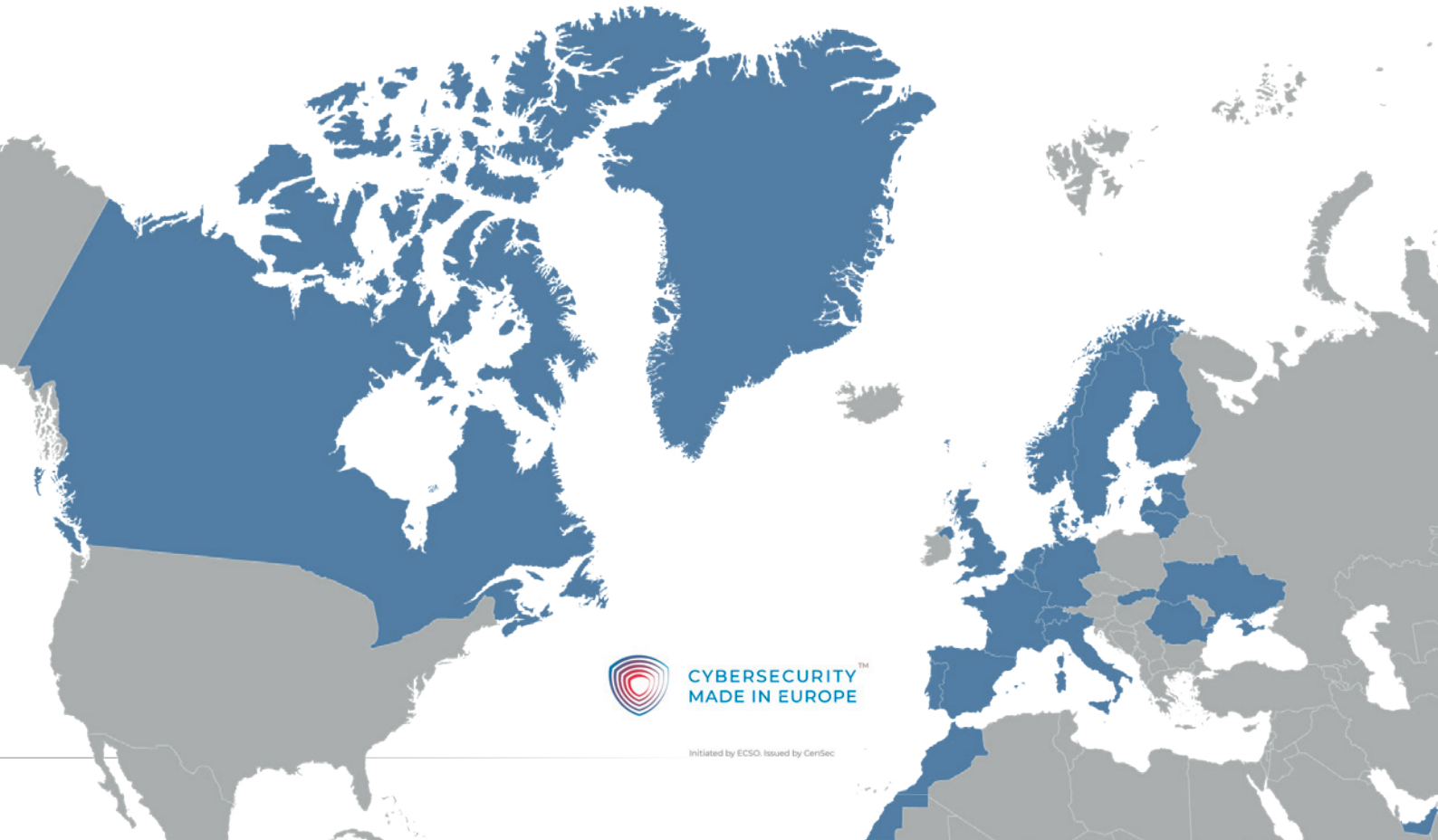
Content

"Digia are proud to announce that Finnish NCSA has assessed the Digia Linja gateway product and issued a statement on the fulfillment of requirements. Digia Linja gateway product (includes the Arbit Cyber Defence Systems data diode) meets the Finnish national criteria for SECRET (TLII SALAINEN).

– LEAD SOLUTION ARCHITECT, AKI MARTTI, DIGIA PLC

"KONGSBERG DEFENCE & AEROSPACE has implemented the Cross Domain Solutions developed by Arbit, which has improved our network security without impairing work process efficiency. Both the Arbit Data Diode and the Arbit Trust Gateway meet all of KONGSBERG's strict requirements for speed, security, stability and manageability."

– CIO, JAN HELGE STRØM, KONGSBERG



Arbit secures the Danish EU Presidency with secure information release and data sharing

Arbit in Goverment, and Serverrooms

Together with Statens IT, Arbit has tailored a solution based on the Arbit Data Diode Hardware technology providing hard segmentation and boundary protection for ministries, along with advanced anti-malware platforms in a redundant and resilient architecture.

Friends and partners

CYBERS — ESTONIA

DELL Technologies — DENMARK

digia — FINLAND

EUROTEMPEST — NETHERLAND

MILDEF — SWEDEN

necas OEM ELECTRONIC SOLUTIONS — DENMARK

OPSWAT. — USA

secunet — GERMANY

Videnca — SWEDEN

LEONARDO — ITALY

Member of

CenSec CENTER FOR DEFENCE, SPACE & SECURITY — DENMARK

DANSK ERHVERV Danish Chamber of Commerce — DENMARK

DI Danish Defence and Security Industries — DENMARK

ECSO EUROPEAN CYBER SECURITY ORGANISATION — BELGIUM

Reference customers

DANISH MINISTRY OF DEFENCE ACQUISITION AND LOGISTICS ORGANISATION

DANISH MINISTRY OF DEFENCE ACQUISITION AND LOGISTICS ORGANISATION
WWW.FMI.DK/ENG

KONGSBERG

KONGSBERG
WWW.KONGSBERG.COM

STATENS IT

THE AGENCY FOR GOVERNMENTAL IT SERVICES
WWW.STATENS-IT.DK/ENGLISH

TERMA

TERMA
WWW.TERMA.COM

CYBERSECURITY MADE IN EUROPE

Initiated by ECSO. Issued by CenSec

DATADIODE

Galvanic Separation at its best

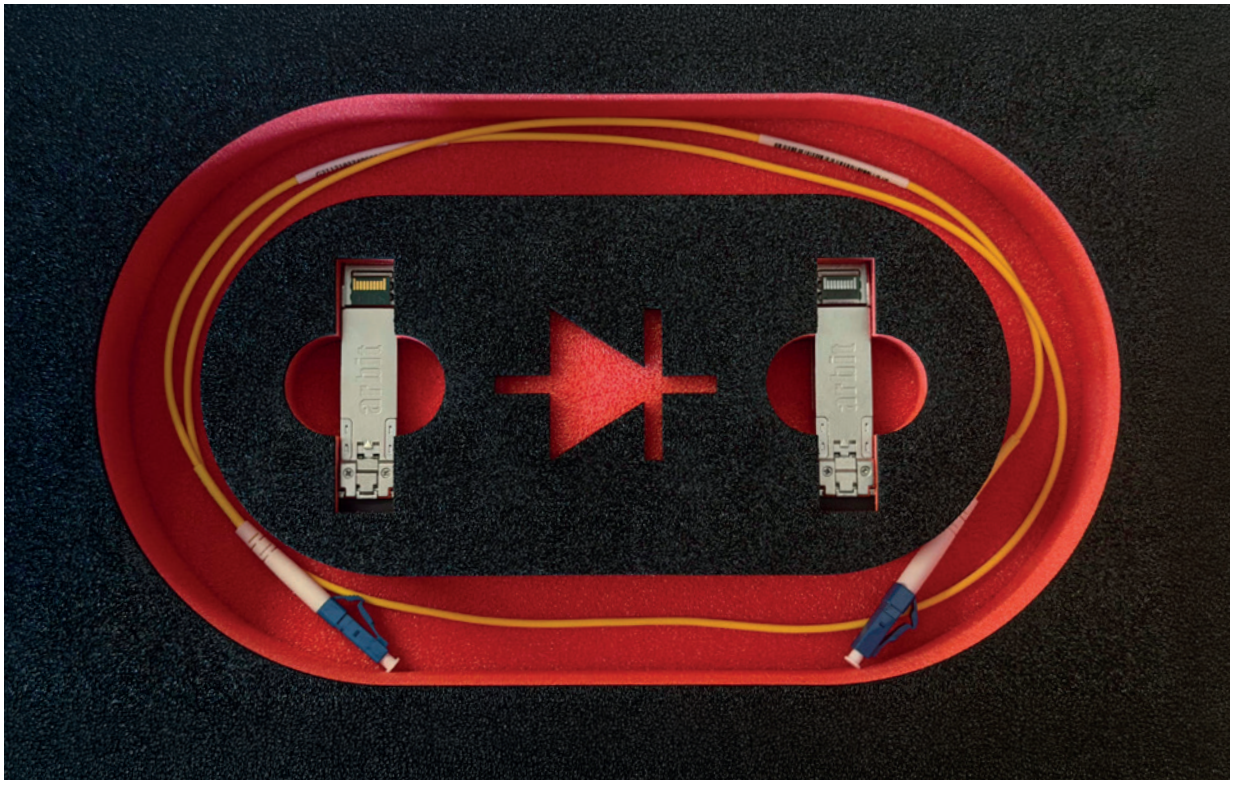
The Foundation of Arbits strength!

Our customers go to great lengths to uphold confidentiality and integrity of their highly classified networks, where their data must always be guarded. Huge effort is put into ensuring airgap separation between multiple classified domains, implementing strict security processes and perimeter control and deploying solutions such as filtered power supplies, shielding/TEMPESTing equipment, and more.

It is therefore essential that the selected Cross Domain Solution supports and maintains this high level of protection.

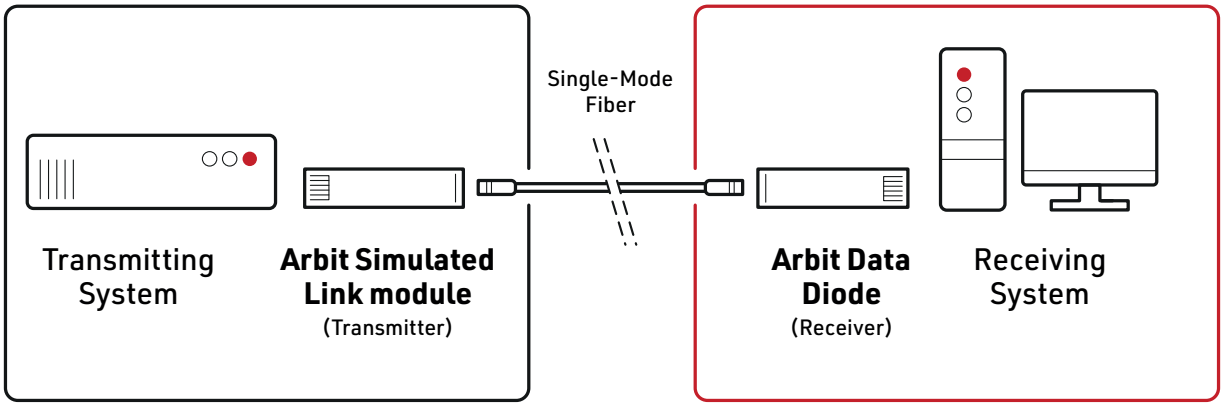
The Arbit Data Diode provides Galvanic Separation, a fundamental security concept, relying on the laws of physics whereby light is allowed to pass through unidirectionally. This is the principle behind Arbit's strength, which has received the highest evaluation assurance level for IT products in the 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.



Technical Specifications

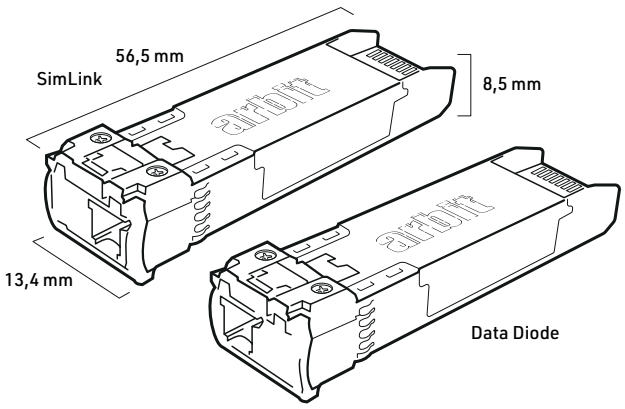
Data Rate	10GbE (SimLink & Diode)
Connector Type	LC (single)
Wavelength	1310 nm
Transmission Distance	Up to 20 km (SimLink), source-dependent (Diode)
Power Consumption	Max. 0.3W at 3.3V
Operating Temp	-20°C to 85°C (Extended support down to -40°C possible with preheating in ruggedized configuration)
Storage Temp	-40°C to 85°C
Compliance	CE, SFF-8431 4.1
Certification (Data Diode only)	EAL7+ (Certified by BSI Germany), NATO COSMIC TOP SECRET and EU TOP SECRET accredited



Use cases

The Core Kit ensures absolute unidirectional communication, making it ideal for:

- Command and control (C2) infrastructure
- Secure update channels for intelligence or case-sensitive systems
- Boundary protection between high-side and low-side networks
- Hard-segmented air-gapped networks in classified environments
- Transfer of digital evidence (incl. video streams) to protected networks



With NATO COSMIC TOP SECRET and EU TOP SECRET certification (Data Diode), no software logic, and instant SFP+ integration, the Arbit Core Kit is ideal for any environment where data confidentiality and integrity are mission critical.

DATADIODE EAL 7+

Fast, hardware-based network security

Unilateral data transfer between networks without the risk of unauthorized remote access.

The Arbit Data Diode, a Common Criteria EAL7+ certified solution, physically separates high security networks from lower classified networks, allowing one-way data transfer without compromising the confidentiality and integrity of the highly classified network.

Government and Public sectors along with Military and Defence agencies deal with critical and highly sensitive information. The Arbit Data Diode provides 100% guarantee that no data flows in the wrong direction providing network protection and allowing highly classified networks to import data while guarding against cyber attacks, espionage, hackers and data theft.

The Arbit Data Diode consist 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.

Software vs. hardware solution

	FIREWALL	SOFTWARE DATA DIODE	ARBIT DATA DIODE
100% protection against data theft	No	No	Yes
100% protection against hackers	No	No	Yes
Secure one-way connection	No	No	Yes
Protected by laws of physics	No	No	Yes

Sending Server – Pitcher

Receiving Server – Catcher

Contrary to software solutions that ensure only the logical separation of networks, optical data diodes enforce physical separation of networks without any return channel. The Arbit Data Diode having the highest evaluation and certification in the world (EAL7+), fulfills advanced needs for stability, scalability, throughput and low latency, together with a competitive total cost of ownership. The best official client case is 24 files per. sec. nonstop for 14 days without any data loss.

DESCRIPTION	RESULT
File-based throughput	7 Gbps
UDP throughput	9,8 Gbps
Transactions per second	18,0 (52 KB files)
Transaction failure rate	0 (out of 5 mio files)

Arbit Data Diode Fact Sheet

BENEFITS

- 100% secure hardware data diode
- Full galvanic separation
- High throughput and transfer rate
- High stability and low TCO and maintenance
- Proven track record for 15 years
- User-friendly web interface
- Powerful add-ons to control content moving through the data diode
- Full integration with OPSWAT advanced anti-malware platform
- Easy and secure configuration management
- Combine with TEMPEST level A
- Mix Tempest level A protection with EAL7+ cyber security in one device to protect and manage CLASSIFIED DATA
- Smartcard configuration management for added integrity and hardening.

FEATURES

- 10 GbE (Common Criteria EAL7+ certified)
- Accredited NATO COSMIC TOP SECRET and EU TOP SECRET
- No maximum file size (only limited by disk space on proxy servers)
- 64 data channels per diode
- Data channel priority (on transaction basis)
- Supports up to 24 streaming channels (logging, video, audio via UDP)
- High availability with peer-to-peer recovery
- Syslog and notifications by email
- Software runs on hardened Linux

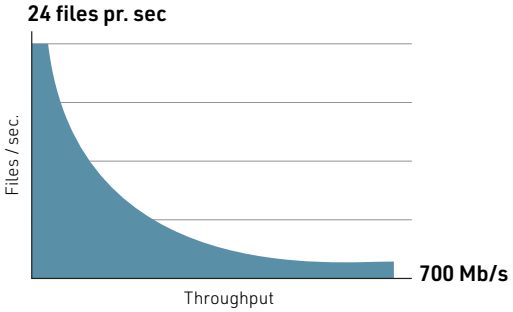
SUPPORTED PROTOCOLS

- Mail (SMTP)
- Simple File Transfer (FTP, SFTP)
- Windows share forwarding (SMB)
- Windows share mirroring (SMB)
- Network File System share
- forwarding (NFS)
- Network File System share
- mirroring (NFS)
- Time synchronization (NTP)
- Streaming UDP, TCP via UDP
- REST API Forwarder (HTTP, HTTPS)
- Telemetry via MQTT
- OPSWAT Integrations

KEEP YOUR SYSTEMS SECURELY UPDATED

- WSUS
- Linux repository
- Anti Virus updates

RELATION BETWEEN FILE SIZE AND BANDWIDTH



HARDWARE SPECIFICATIONS		
Configuration Type	Arbit Data Diode Standalone	Arbit Data Diode with Proxy server
Supported server	Dell PowerEdge R360	Dell PowerEdge XR5610
Memory and Storage	32 GB RAM / 8 x 480GB SSD (3.84 TB)	32 GB RAM / 16 GB Read Only SSD
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	1x 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	

GATEWAY

Data Release from Secure Networks

Safe release of approved data from highly secure and air-gapped networks.

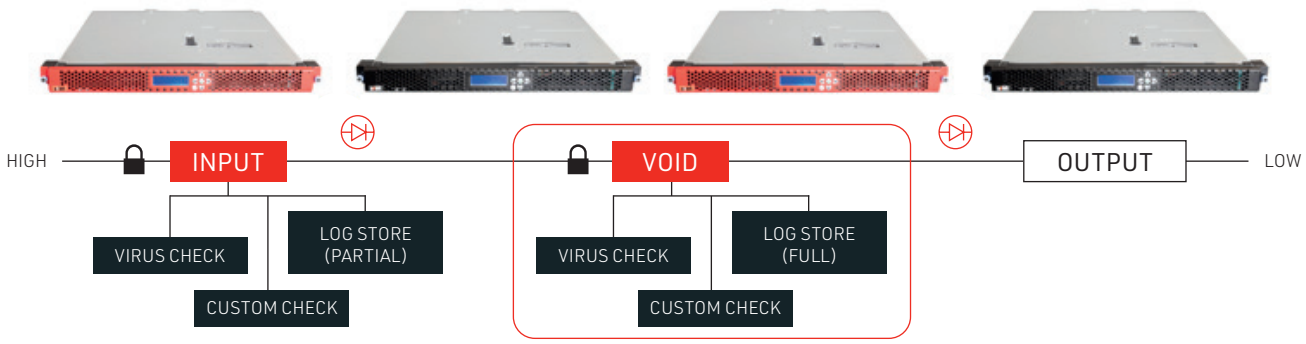
Moving data into a secure network is easily handled by an Arbit Data Diode. However, when data needs to leave a secure network, it is of utmost importance that no secrets or other guarded information is released without prior consent and approval. The Arbit Trust Gateway (ATG) ensures that only approved and releasable data is allowed to leave the secure network in a controlled and secure manner, making the process of data release as safe as possible.

Using USB-sticks or other media devices to release data from highly secure networks, comes with inherent risks. Risks that must be avoided at all times, to safeguard secrets and eliminate leakage of unwanted information release. The Arbit TRUST Gateway (ATG) eliminates those risks and ensures that data released from a protected network is both source and content checked according to security policies.

The ATG uses signing technology to identify the source of the released data. Only approved sources and authorized individuals can sign data, that can pass through the gateway after successful evaluation, ensuring that no rogue process or system sends data through or piggybacks information on approved transactions.

The ATG can perform several content checks, including filters developed by Arbit as well as third parties like multi scanning products using the Arbit Open API.

ARBIT TRUST GATEWAY ARCHITECTURE



Based on the Common Criteria EAL7+ certified Arbit Data Diode the Arbit Trust Gateway consists of two Arbit Data Diodes connected in series. This creates an isolated VOID (Verification of Identity and Data) network between the two Arbit Data Diodes, which is not accessible from neither the high nor low side. This makes the isolated VOID network the perfect place for final filtering and checks, before releasing data, as its verification mechanisms cannot be manipulated.

Arbit Trust Gateway Fact Sheet

BENEFITS

- Replaces non-secure manual data transfer
- Proven transmission stability using Arbit Data Diode technology
- Integrates with existing company infrastructure Open API for building custom content verifiers (C++ and Java)
- Supports 'Releasing and Drafting Officer' function using the Arbit Trusted Information Release portal
- Full integration with OPSWAT advanced anti-malware platform
- Optional external content verifiers and AD-lookup verifying sender or content
- Smartcard configuration management for added integrity and hardening.

FEATURES

- Built on Data Diode technology
- Based on 1U rack-mountable units
- All zones with galvanic separation
- Fiber or copper connectors to external networks
- Read-only boot device
- Low power consumption
- Low latency
- Accredited NATO SECRET and EU SECRET

INTEGRATES WITH

- SYSTEMATIC SitaWare (C2 software)
- Arbit Trusted Information Release Portal (Two factor release of data)
- Arbit Desktop Gateway (Browse down)
- Arbit Web Gateway (Web access)

COMPARISON BETWEEN DATA EXPORT METHODS	USB	CD-ROM	Arbit Trust Gateway
Avoids two-way connection when releasing data	NO	YES	YES
Verifies source of released data	NO	NO	YES
Verifies data content according to security policy	NO	NO	YES
Ensures release work-flow policy is upheld 24x7	NO	NO	YES
Low latency in release of data	NO	NO	YES
Automatic threat & content scanning using OPSWAT MetaDefender™	NO	NO	YES

HARDWARE SPECIFICATIONS	
Support Servers	Dell PowerEdge XR5610
Memory and Storage	32 GB RAM / 2.5" SATA 16 GB Read Only SSD
Diode principle	Hardware based (optical)
Backflow	None (secured by the laws of physics)
Certification	Based on the Arbit Data Diode Common Criteria EAL 7+. Pending Common Criteria EAL4+
Fiber technology	Single mode 1310 nm
Diode NIC speed	10 Gigabit
Server Size	1U, 19" (4 units required for a complete trust gateway: 1 Input Guard, 1 VOID Proxy, 1 VOID Guard, and 1 Output Proxy)
Server Weight	Max .11 kg
Power supply	2 x 100-240 VAC 50/60 Hz (Hot swap redundant per server)
Dimensions (W x H x D)	19" x 1U x 463 mm

Arbit Open API

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

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 (CDS).

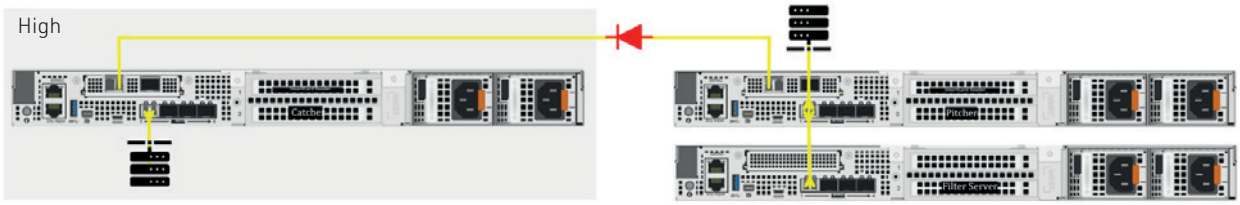
The Arbit Open API provides users total control over their data that passes through the Arbit CDS, simplifying integration towards for example Command and Control systems, Battle Management Systems or any other SW application. It allows customers to flexibly control and shape their security profile as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

Easy Intergration

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.

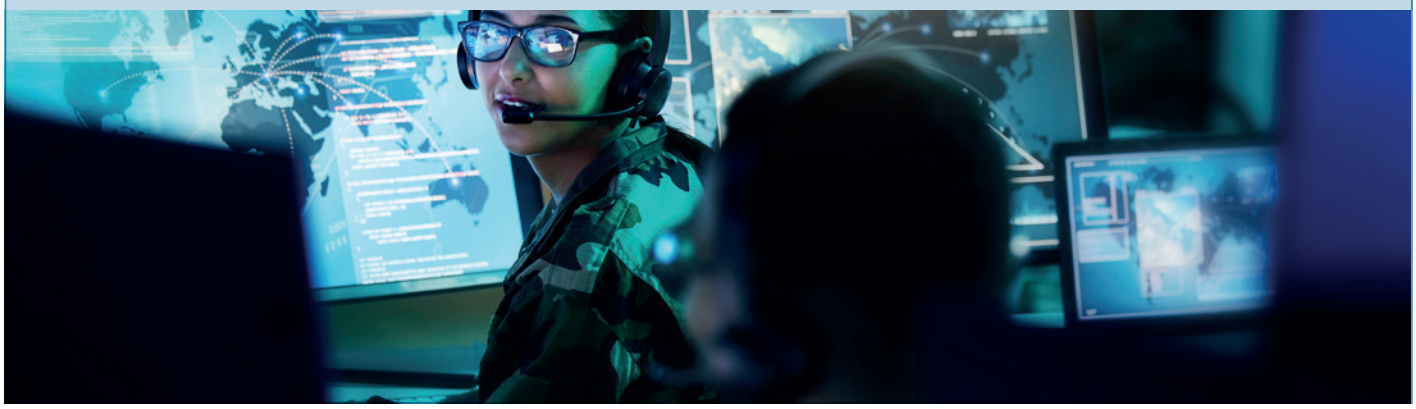
The Arbit Open API can be used for creating filters or labelling services and the like that verify and check data against certain standards, such as STANG 4774 / 4778.2 which then gives a go/no-go decision to determine if that data should be allowed to pass through the Arbit CDS or not.

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.



Additionally, the Arbit Open API can be called in the outgoing direction of traffic as well as the incoming direction, giving flexibility to have various types of verification depending on the traffic type and the network classifications involved.

Arbit provides several predefined filters, such as certain STANAG standards out of the box and can also customize filters on behalf of our customers through the Arbit SDK or allow customers to build and design their own security filters, giving them full ownership of their data flow.



Working Behind Closed Doors

Ensuring operational efficiency in highly classified office environments, such as government and intelligence agencies and military headquarters, is crucial. The same goes for operational efficiency on the battlefield. Yet how efficient are such office environments if they are air-gapped and isolated for security purposes?

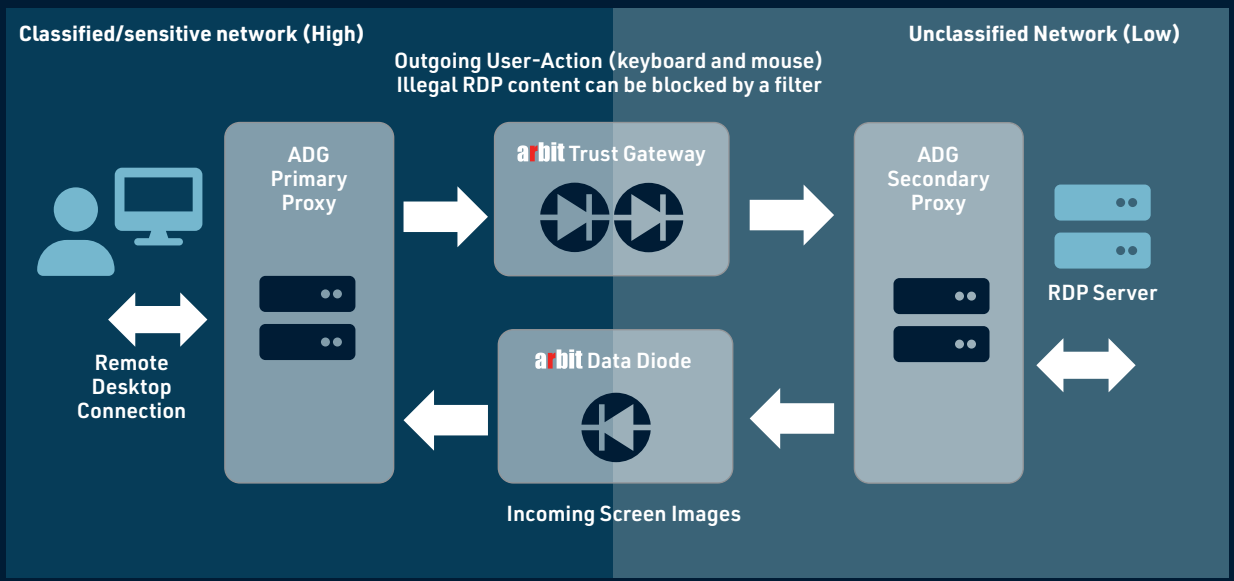
Like any other office environment relying on IT, highly classified office environments and their networks are used for communication, HR, CRM, and ERP systems and at times need connectivity to other networks for cross-domain information exchanges.

Using Arbit's Cross Domain Solutions provides the operational efficiency needed to exchange emails and documents and share C2 information between headquarters and the battlefield, and vice versa.

Arbits Applications can add to the operational efficiency and boost productivity in the following ways.

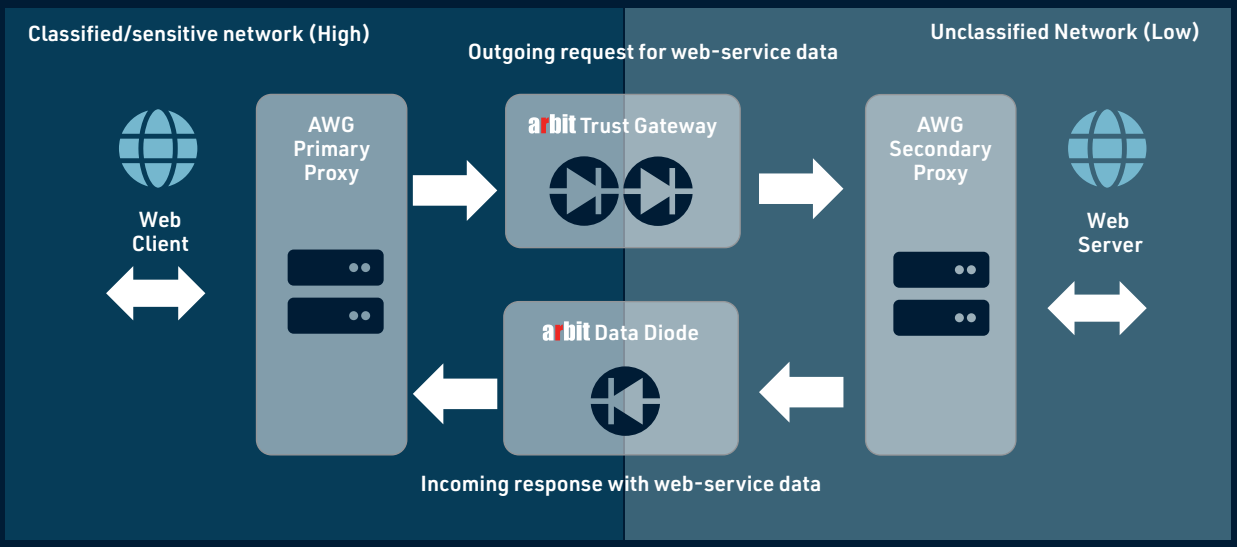
Simplify Remote Work with Secure Remote Desktop Access

The Arbit Desktop Gateway allows you to securely connect to and use remote desktop applications on remote servers in other network domains from the convenience of a terminal located in your highly classified and protected network. Eliminating the need for several terminals and network connections, saving cost and cumbersome connectivity solutions.



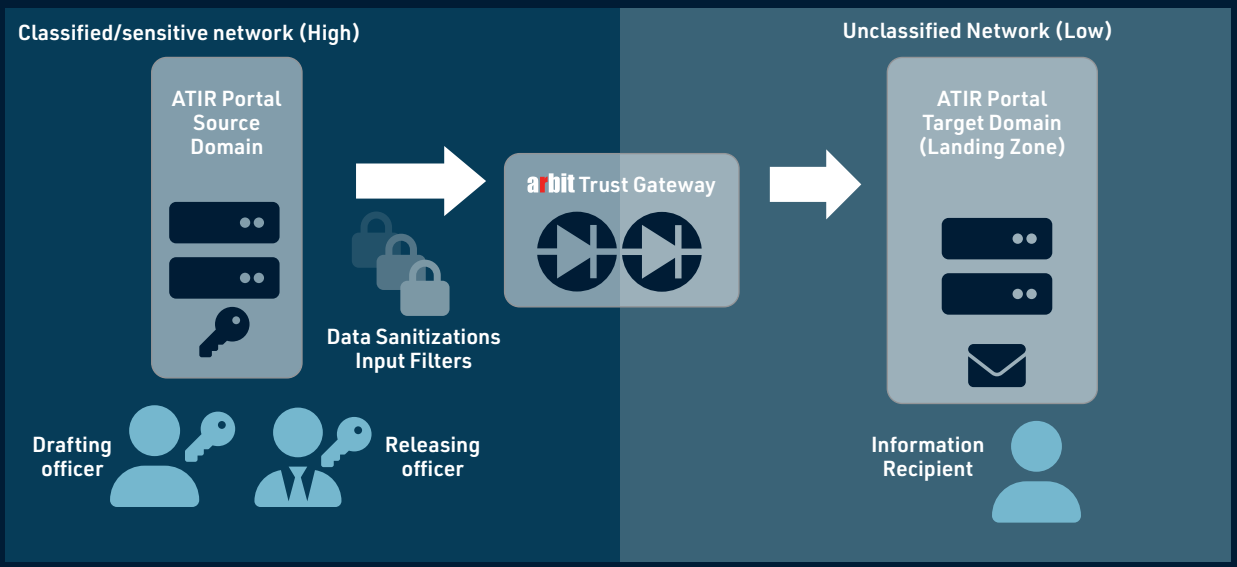
Seamless web service integration

Integrate external web services with your applications running in your classified network. The Arbit Web Gateway allows you to build controlled and seamless dataflows using the ubiquitous HTTPS protocol. It's a convenient, secure, and efficient way to integrate cross-domain capabilities into your existing systems.



Fulfilling the "Trust, but Verify" principle in Cross Domain Exchange

With The Arbit Trusted Information Release (ATIR), a two factor release process is used to verify and control that the information you release is indeed, what is allowed to pass through. The release must be performed by two individuals: a drafting officer preparing the release, and a releasing officer approving it.



For Armed Forces

Ruggedized Data Diode and Trust Gateway for Harsh Environments

Picture by the courtesy of General Dynamic.

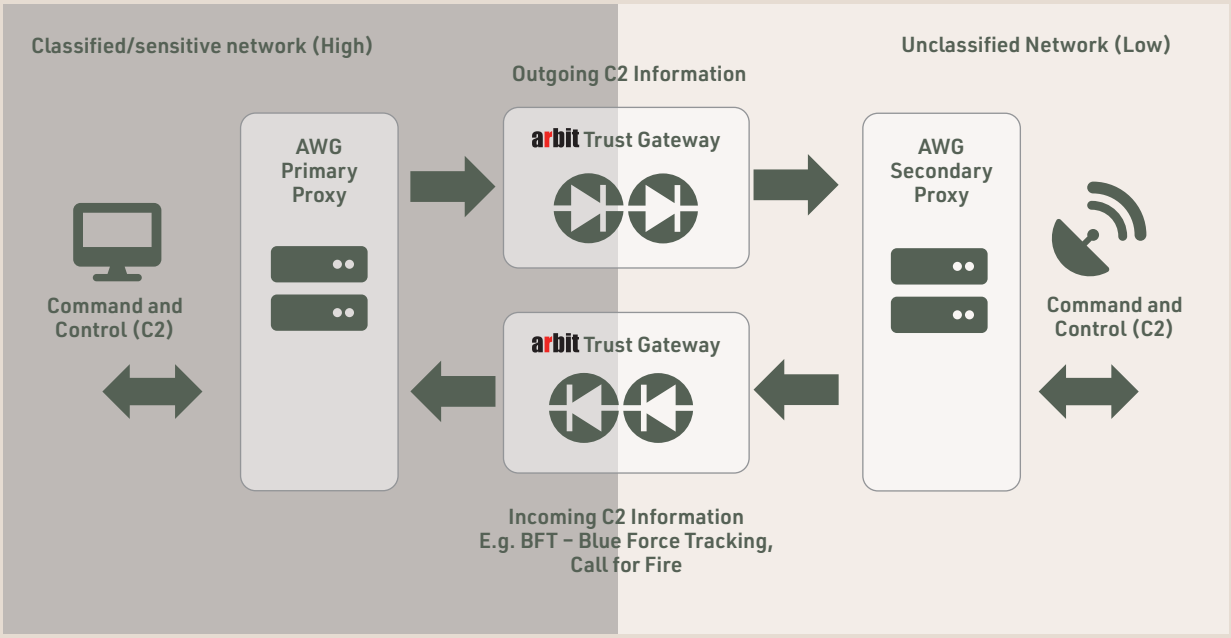
Arbit Cyber Defence has a 20-year agreement with The Danish Ministry of Defence Acquisition and Logistics Organisation (DALO), focusing on digital Cross Domain Solutions for the Danish Defence.

This long-term framework is to increase network security across various military units, from HQ server rooms to frontline units.

RUGGED GATEWAY

Cross Domain Solution (CDS) in Multi Domain Operations

Enhance Operational Efficiency on the Battlefield with Seamless C2 Integration

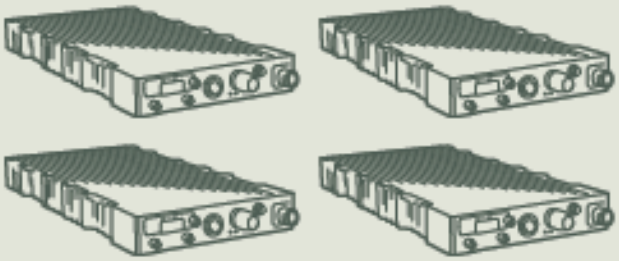


The Arbit Cross Domain Solution (CDS) integrates seamlessly with BMS and C2 systems, such as SitaWare from Systematic, providing situational awareness across multiple security domains, making communication between headquarters and the battlefield secure and efficient. It functions with two Arbit Trust Gateways (ATG), one for data import and one for data export, while maintaining galvanic separation. Can be deployed on Ruggedized Hardware to withstand even the harshest of

RUGGED GATEWAY

Cross Domain Solution (CDS) in Multi Domain Operations

The Arbit Cross Domain Solution, supporting C4ISTAR, allows you to securely exchange C2 information between coalition forces on the battlefield, supporting both automated and manual release as well as import of data.



SECURE AND TIMELY DATA EXCHANGE

Smaller or larger military formations that have deployed Cross Domain solutions to obtain the highest security, still have the essential need to exchange timely C2 Information between subordinate units and/or coalition forces. The Arbit CDS supports safe and fast data exchange, supporting both automated and manual release and import of data. The Gateway is accredited NATO SECRET and EU SECRET.

Since the import and export of data are subject to many security procedures and regulations, the Gateway supports a full set of security procedures that can be required for data exchanges. Typically, classifications, markings, release ability, formats, and origin of data must always be verified and checked before data can be released or exchanged. In addition, some types of information exchanges are extremely time-sensitive, such as blue force tracking and Cross Domain calls for fire. The Arbit CDS allows you to set validations and checks to meet your security profile, including release procedures (two-factor release), data content validation, validation of signing, classification, and other filters such as multiple virus scanning. Arbit CDS is built on Arbit's hardware-based Data Diode technology and therefore offers a continued network separation with no backflow possible.

The Arbit CDS is designed and built to operate on the battlefield under the most challenging conditions. All units are 1U 19"/2 and a full gateway is only 2U (UPS and power supply excluded) equipped with NATO standard connectors and designed for vehicle mount.

FEATURES AND FORMFACTOR (reduced weight and size)

Developed for Arbit by MilDef, to meet rugged military standards ((MIL-STD-810) and flexible mounting the new hardware can be deployed in several configurations reducing the size to 1/3 of the previous version.

Data Centric security and Cross Domain solutions for multidomain operations

Cross Domain Solutions and Data Centric security for multidomain operations

Building a multi-Domain Operations network naturally includes discussions of Data Centric Security and information exchange between different security domains. Cross-Domain Security and Cross-Domain Solutions (CDS), such as gateways, are essential components of NATO's data-centric security framework.

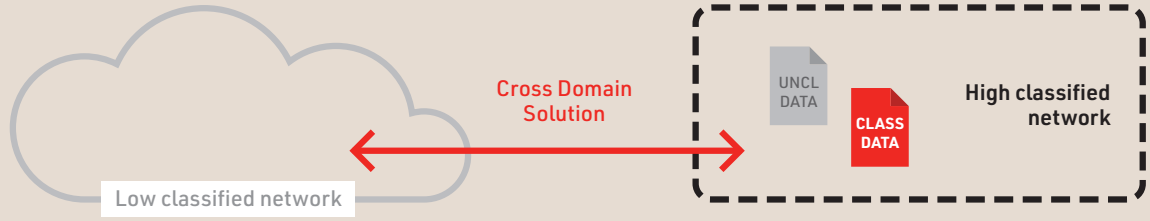
- Cross-Domain Solutions (CDS) like data diodes and gateways, or IEGs, are specialized security systems. They control and monitor the transfer of information between different networks and security domains to prevent data leaks and ensure that only appropriately sanitized and approved data crosses domain boundaries.
- Data Centric security (DCS) protects the representation of information directly and ensures that data retains its integrity and confidentiality when moving across domains and that only users with the precisely correct user rights can access (and decrypt) specific data within that network and security domain.

The challenge designing DCS

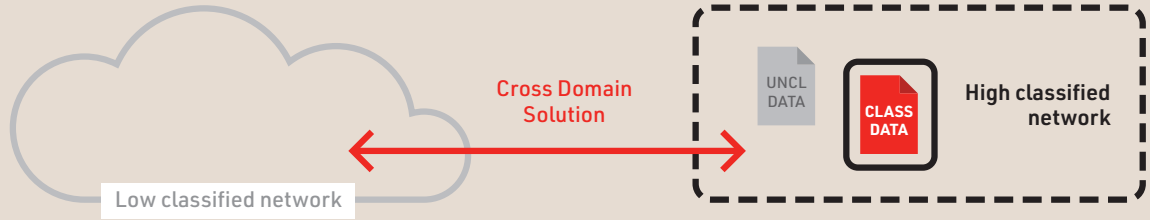
Data-centric security is designed to address the evolving threats in cyberspace, ensuring the integrity, confidentiality, and availability of mission-critical data across its operations and among its member nations.
The challenge with the Data Centric security approach, from a classification security perspective, however, is that the specific network that stores a HIGHLY CLASSIFIED file, automatically gets the same HIGH classification if that data is available unencrypted – even for a short while.
This means that if a user accesses and opens a file (and thereby decrypts it) that is NATIONAL TOP SECRET on a network, the network will automatically become NATIONAL TOP SECRET with all compliances, regulations, rules concerning interconnections, information sharing across nations, etc.

So, if a piece of classified data is sufficiently encrypted, the encrypted data is no longer classified and could be stored or transmitted on networks with a lower classification. However, as soon as the data is unencrypted (even in memory on a user's computer), the network connected to the computer must have the appropriate classification level. E.g. secret information cannot be decrypted on the internet.

Type 1: Classical border protection – both classified and unclassified data are accessible inside the network



Type 2: Classical border protection AND Data Centric Security – Classified data inside the network is stored encrypted



Type 3: Classical border protection AND Data Centric Security – EXPORTED classified data is not accessible

From PINK to GREEN at NATO CWIX26

A successful test and proof of interoperability

At NATO CWIX26 Arbit once again participated in one of NATO's most important interoperability exercises, supporting secure information exchange across multiple environments.

During CWIX26, Arbit again participated as a mediator between sender and receiver, contributing to secure and controlled Cross Domain communication through Arbit's Cross Domain solution. By using the Arbit Trust Gateway (CC-686) and the Arbit Data Diode (CC-736), Arbit supported interoperability testing and secure information exchange across multiple operational environments.

CWIX26 gathered more than 3000 participants from NATO allied nation and industry partners. All covering different operational focus areas such as AIR, Maritime, Land, Cyber, CBRN and Friendly Force Tracking (FFT). By participating in CWIX 26, Arbit continues to support NATO interoperability efforts and international collaboration within secure and mission critical environments.

In the Navy – Zero Unit

With a minimal footprint, the Arbit Data Diode protects information and systems on Naval Vessels.

Arbit is deployed within several Naval Installations and ensures that critical information doesn't fall into the wrong hands, and systems are not destroyed by cyber-attacks.

A use case involves requirements for unidirectional UDP communication between different security domains on a Naval vessel, demanding a Cross-Domain Solution that can perform in harsh environments and adhere to the highest security standards, all with a minimal physical footprint. In this case, the Arbit Data Diode fulfills all three requirements: ruggedized for military use, certified, accredited, and without taking up any rackspace.

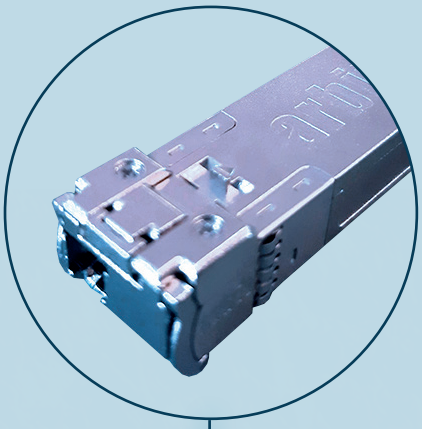


Photo: Danish Patrol Vessel Ejner Mikkelsen, captured in the arctic by Captain Troels Sundwall.

Arbit Hardware Deployment Options

Based on customer needs, the Arbit Data Diode and the Arbit Trust Gateway can be deployed in several configurations depending on the security requirements of our customers and the use cases to be served, all with Interchangeable Modular Hardware. All our software runs on all our hardware platforms.

Example Use Cases and Protocols

- Video and Audio Streaming (UDP, TCP via UDP)
- E-mail (SMTP)
- Simple File Transfer (FTP, SFTP)
- Windows share forwarding (SMB)
- Windows share mirroring (SMB)
- Network File System share forwarding (NFS)
- Network File System share mirroring (NFS)
- Time synchronization (NTP)
- REST API Forwarder (HTTP, HTTPS)
- WSUS (HTTP, HTTPS)
- Server-Side Events (HTTP, HTTPS)
- Command and Control (HTTP, HTTPS)
- Web services (HTTP, HTTPS)
- Remote Desktop File handling (RDP)

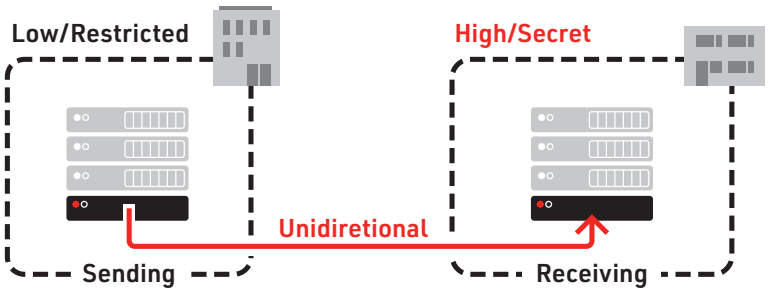
Example Use Cases and Protocols

- 10GbE SFP+ modules supporting UDP protocol
- 1U COTS Server HW for data center deployment supporting all protocols
- 1U 19"/2 Ruggedized HW for battlefield deployment supporting all protocols

Interchangeable modular hardware:
All our software runs on all our hardware platforms.

Galvanic Separation in Cross Domain High Security Networks

Our solution's architecture ensures galvanic separation of hardware of different classification levels. It adheres to clearance distances, so that no microprocessor operates with more than one network CLASSIFICATION. This design also enables our hardware to meet TEMPEST standards, as only one network CLASSIFICATION exists inside each physical box.



Sending and Receiving units can be separated into a single rack, different racks,or different locations. Connected only with a single fiber.

secunet – protecting digital infrastructures

secunet is Germany's leading cybersecurity company. In an increasingly connected world, the company's combination of products and consulting assures resilient digital infrastructures and the utmost protection for data (up to EU and NATO SECRET), applications and digital identities. secunet specialises in areas with unique security requirements – such as cloud, IIoT, eGovernment and eHealth. With security solutions from secunet, companies can maintain the highest security standards in digitisation projects and advance their digital transformation.

Over 1,000 experts strengthen the digital sovereignty of governments, businesses and society. secunet's customers include federal ministries, more than 20 DAX-listed corporations as well as other national and international organisations. The company was established in 1997, is listed at the German Stock Exchange and generated revenues of 393,7 million euros in 2023.

secunet is an IT security partner to the Federal Republic of Germany and a partner of the German Alliance for Cyber Security

LEONARDO – strategic partnership

Leonardo and Arbit have signed a strategic agreement to co-design, co-develop and certify a cross-domain solution aimed at meeting cybersecurity requirements for highly complex, multi-national and multi-domain programs featured by a high level of interoperability. The advanced solution, based on Arbit's NATO certified "Data Diode" technology, will allow a secure and rapid transfer of information across networks with multiple classification levels for both critical infrastructures and Defence, enabling the latter to conduct multi-domain operations.

Leonardo is an international industrial group, among the main global companies in Aerospace, Defence, and Security (AD&S). With 53,000 employees worldwide, the company approaches global security through the Helicopters, Electronics, Aircraft, Cyber & Security and Space sectors, and is a partner on the most important international programs within these sectors, such as Eurofighter, NH-90, FREMM, GCAP, and Eurodrone.

OPSWAT. – Perimeter protection Cross Domain, on the HIGH side

OPSWAT's motto is "Trust no File. Trust no Device." The Arbit/OPSWAT partnership excels at managing the challenges of impex 'Ing files between one domain to another. Addressing malware and viruses is complex and should be handled at the network perimeter to avoid over-reliance on endpoint protection. OPSWAT uses the world's leading multi-scanning technology, with up to 33 anti-malware engines, to detect and remove up to 99.6% of the world's top 10,000 threats. OPSWAT's Content Disarm and Reconstruction (CDR) technology, disarms and de-weaponizes over 180 file types, stopping zero-day threats. For files that can't be processed by CDR, OPSWAT's emulation-based sandbox performs a final check at near wire-speed, ensuring files are clean before import.

EUROTEMPEST

Eurotempest develops high-assurance IT products and systems for defence- and government use. Their products are used by national- as well as central authorities, throughout EU and NATO in more than 20 countries.

Eurotempest customers can select TEMPEST versions of the latest IT products technology with confidence that formal requirements and standards are met.

Eurotempest employees have years of experience from various high-assurance projects involving TEMPEST, crypto and secure systems development. They work directly with most of the major manufacturers of IT equipment and are technology partners to companies like Panasonic, HP, DELL, Fujitsu, NEC/Sharp and Allied Telesis.

Arbit supports

CYKEL NERVEN
FOR EN VERDEN UDEN SCLEROSE

SIF

DM

Idrætsforeningen Flyvestation Karup
- medlem af Dansk Militært Idrætsforbund

InterForce

OFFICERSTIDNINGEN

OPERATORS

VETERANPROJEKT GRØNLAND

2606425 · 2026-07

Want to know more about our solutions?

Scan the QR-code to download all our product information.

https://arbitcds.com/products/

arbit

Immerkaer 54 | 2650 Hvidovre | Denmark | Email: info@arbitcds.com | VAT DK38991469 | www.arbitcds.com