arbit

CROSS
DOMAIN
SOLUTIONS

GATEWAY

Data release from secure networks

Secure release of approved data from highly secure or air-gapped networks

Moving data into a secure network is easily handled by a data diode. However, when data is required to leave a secure network, this is often accomplished using USB-sticks or other portable devices, along with all the inherent security risks.

The Arbit TRUST Gateway (ATG) eliminates the need for manual data transfer and ensures that only approved data is allowed to leave the secure network, making this critical communication as safe as possible. The ATG platform also supports browse down and remote desktop access set up from high to low.

The ATG uses signing technology to securely identify the source of the released data. Only approved source systems and authorized individuals are able to sign data, which is then allowed to pass through the gateway. Adding the Arbit release portal, a number of organizational security requirements can be added such as two factor release.

The ATG is based on Common Criteria EAL7+ certified Arbit Data Diode technology. This protects against attacks from the receiving side as well as the transmitting side. In addition, the system is based on hardened Linux installations.

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

The Arbit TRUST Gateway (ATG) ensures that data released from a protected network is both source and content checked according to company standards, and that no rogue process or system can send data through or even piggyback information on approved transactions.

The ATG acts like a secure platform where several COTS or custom checks can be performed. The ATG is based on the robust Arbit Data Diode technology and consists of two Arbit Data Diodes that are connected in serial.

This creates an isolated VOID network which is not accessible from neither the high side nor low. Therefore the isolated VOID is the perfect area for final filtering and checks as it cannot be manipulated.

All configuration and program code is stored read-only so that it is impossible for an attack to change the system in any way. Rebooting the system is guaranteed to restore the approved configuration and the Arbit program code.

Certified Common Criteria EAL 7+ Accredited SECRET Built on Data Diode technology ✓ Content Verification arbit

BENEFITS

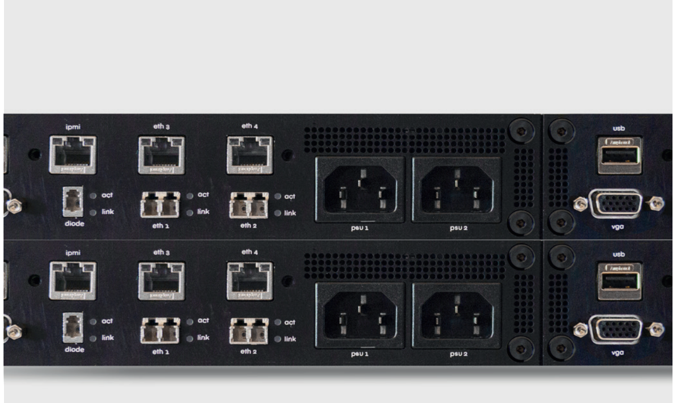
- Replaces non-secure manual data transfer
- Proven transmission stability using Arbit Data Diode technology
- Integrates with existing company infrastructure
- Open API for building custom content verifiers (C++ and Java)
- Supports 'Releasing and Drafting Officer' function using the Arbit Trusted Information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

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 SECRET by CFCS, DK

INTEGRATES WITH

- SYSTEMATIC SitaWare (Command and control software)
- Arbit Trusted Information Release platform (Two factor release of data)
- Arbit Desk Top Gateway (Browse down)
- Arbit WEB Gateway (WEB access)



COMPARE WITH OTHER METHODS FOR DATA EXPORT	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

REFERENCE CUSTOMERS

The Agency for
Governmental IT Services
www.statens-it.dk/english

Danish Ministry of Defence Acquisition
and Logistics Organisation
www.fmi.dk/eng

ARBIT CYBER DEFENCE SYSTEMS APS