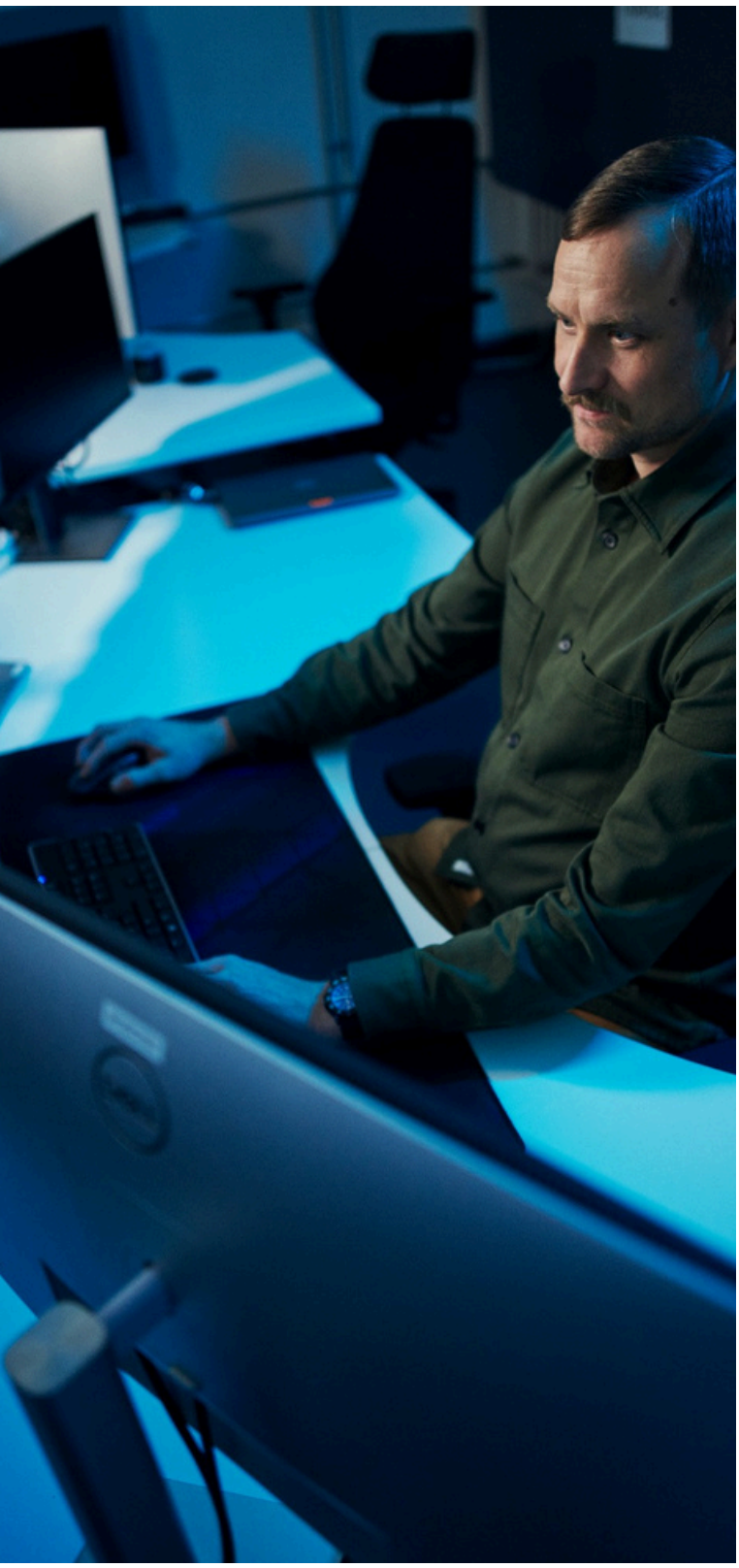
INSTA

Insta Cross Domain Guard

Protection of your Critical Systems and Data

insta.fi/en//crossdomainguard

Insta Cross Domain Guard – Protection of your Critical Systems and Data



Insta Cross Domain Guard protects critical systems and data from cyber threats. It enables controlled and secure data transfer between networks and security levels of different classifications, up to security level SECRET.

Insta Cross Domain Guard is a unidirectional data transfer and filtering solution that enforces one-way communication at the physical layer of the OSI model. Our product is based on a data diode solution, an implementation model approved by the authority (Traficom) for secure data transfer:

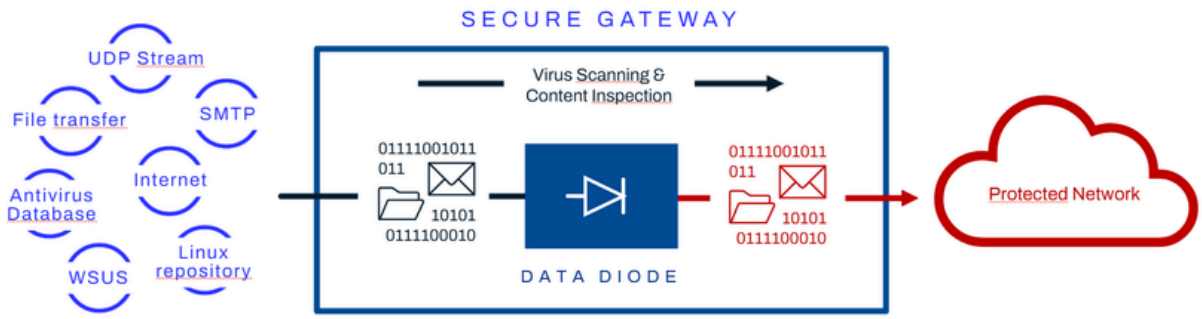
1) Between networks/systems of different security classifications

2) Between different organizations

Insta Cross Domain Guard enables data transfer across one or more security levels and consists of a data diode and Insta's gateway software.

As a data diode solution, Insta uses products supplied by partners that have undergone international certification processes. One such partner is the Dutch company Sentyron, whose data diode is EAL7+ certified and approved up to the NATO Cosmic Top Secret level.

Sarankulmankatu 20 | P.O. Box 80 | FI-33901 Tampere, Finland | +358 20 771 7111



Protocols

The solution supports, among others, the following protocols:

- UDP/IP and TCP/IP
- File transfer (FTP, SFTP)
- Email (SMTP)
- Syslog
- SNMP Trap
- Time service (NTP)

Additional functionalities

- Automatic journaling of transferred data
- Automated reporting
- Advanced content inspection
- Integration with logging, SIEM, or SOC systems
- RESTful Forwarder to exchange information between two systems securely
- User-specific file transfer
  - Single sign-on (SSO)
  - Integrable as part of the customer's web portal
  - Enables a bidirectional implementation without the need to allow USB devices to be connected to systems in the secure network

Performance options

- 1 Gbps
- 10 Gbps

Reliability and Maintenance

The solution leverages a data diode from the Dutch company Sentyron, approved up to NATO Cosmic Top Secret level and Common Criteria EAL7+. High availability can be ensured through redundant components and a hot standby implementation, ensuring that a single hardware failure does not cause service interruption or degrade performance.

Data transfer reliability is enhanced by mechanisms for detecting and correcting transmission errors. In addition, journaling of transferred data is supported, enabling verification of transmitted information through reports.

Continuous development, updates, and new features are provided in accordance with the agreement. Support and maintenance services cover updates, deployment, hardware warranty, and hardware replacement services.

USE CASES

Insta Cross Domain Guard enables the implementation of customer-specific use cases in scenarios where secure data transfer is required. It supports, among others, the following use cases:

Updates in classified environments

The solution provides update procedures for classified environments. Maintaining up-to-date updates is essential for secure operation. The integrity and origin of update packages are verified.

User-specific file transfer

A web-based user interface can be used to replace USB devices in file transfer and to enable file transfers in accordance with the security policy.

Files

Files and directory structures can be replicated between

different security classifications. The files undergo the necessary content inspection and journaling.

Sensor Data

Data from various sensor sources can be transmitted to a higher security classification environment. This enables, for example, the real-time transfer of video feeds from surveillance cameras.

Monitoring Data

Enables remote monitoring of high-security environments and services.

Bidirectional Cross Domain Guard

A REST interface enables data retrieval from higher security classification environments.

Email

Email transmission between networks of different security classifications includes validation of message structure (RFC 7504) and attachment file types. Messages are journaled according to configuration, and invalid messages are routed to quarantine.

Insta Cross Domain Guard

Protection of your Critical Systems and Data

insta.fi//crossdomainguard | cybersec.sales@insta.fi

INSTA

Sarankulmankatu 20 | P.O. Box 80 | FI-33901 Tampere, Finland | +358 20 771 7111