InfoDiode PRO hardware and software solution

Information security of state information systems, financial industry organizations, Critical Infrastructure (CI) and Industrial Control Systems (ICS) imposes serious requirements to the implemented technical and organizational security measures. In some cases, complete isolation of information systems remains the best option. However, in today's world, absolute isolation does not allow to realize the full potential of IT technologies for solving the problems of process automation, building operational response centers and situational centers, building effective IT management systems. Statistics also show that complete isolation provokes violations of information security policies.

Uni-directional data transfer technologies can be used as a solution, providing electroplating of network segments and possibility of unidirectional data transport. Based on this technology AMT GROUP has created hardware and software solution InfoDiode PRO.

InfoDiode PRO guarantees protection against many information security threats and provides the highest level of isolation of information systems. The necessary functionality for interaction with related information systems is maintained.

InfoDiode PRO unique capabilities built into the solution of the industrial complex reveal the potential of using single-directional data transmission systems in a new way, which significantly increases the number of tasks solved with their help and possible application scenarios.

InfoDiode PRO is a 100% Russian solution: InfoDiode software implementation (AMT-Group) and Russian hardware platform. **InfoDiode PRO** provides one-way data transmission implementation. The main purpose - protection of critical segments (for example, LAN GIS, ICS), data unloading/loading with preservation of galvanic isolation and organization of protected interaction of remote Critical objects, ICS. The solution can be used to ensure data security in state organizations, including power agencies, industry, fuel and energy complex, as well as commercial enterprises of any industries using closed networks. The decision is based on the experience and development of AMT GROUP in the application of various systems of one-way data transmission.

InfoDiode PRO competitive advantages

InfoDiode PRO H&S solution is implemented on the Russian certified hardware platform, Russian software developed by AMT-GROUP. This allows **InfoDiode PRO** to be used in government information systems of any level of security and data privacy.

- **Import substitution:** domestic hardware and software platform.
- **Transmission Rate**: up to 1Gbps.

InfoDiode PRO

- Guarantee the protection of data, preserving its confidentiality and integrity, and prioritize data transmission;
- Organize remote access schemes with replicas of critical information resources (databases, virtual machines) outside the perimeter, guaranteeing the protection of critical infrastructure;
- Implement secure remote interaction of critical network segments of individual enterprises and organizations through untrusted networks;
- Ensure system fault tolerance through clustering;
- Provide data transfer on different protocols (transfer of files, email, etc.);
- Implement full monitoring of the state of transmission at the perimeter border, including data transmission to the external SIEM or DLP system;
- Integrate with Active Directory.

InfoDiode PRO - an efficient InfoSec solution easily integrated into existing infrastructure

Integration with other information security tools
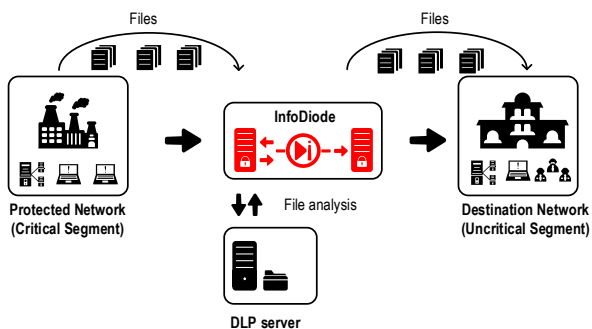
Integration with Data Loss Prevention (DLP) systems
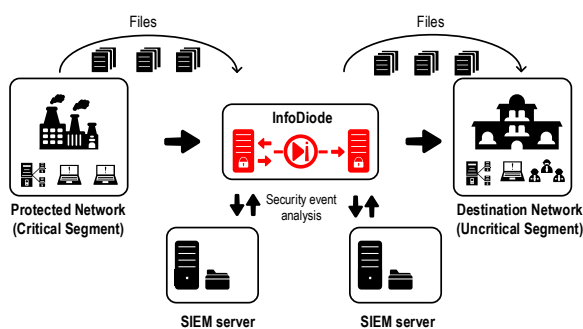
Integration with Security Information and Event Management (SIEM) systems

A fault-tolerant solution

InfoDiode PRO has a cluster implementation option, which allows building a fault-tolerant solution on the network perimeter. Data replication between cluster elements ensures continuity of data flow at the segment boundary.
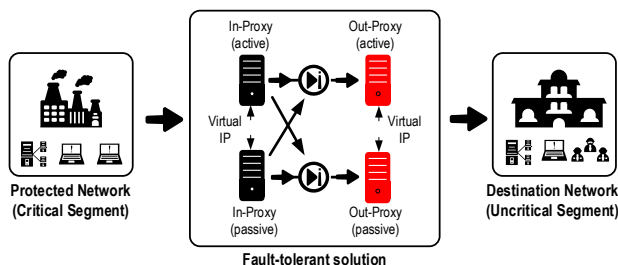
InfoDiode PRO Application Scenarios

Scenario 1. Data export

Scope of application: government, enterprises of the defense-industrial complex, critical facilities, commercial organizations using closed networks.
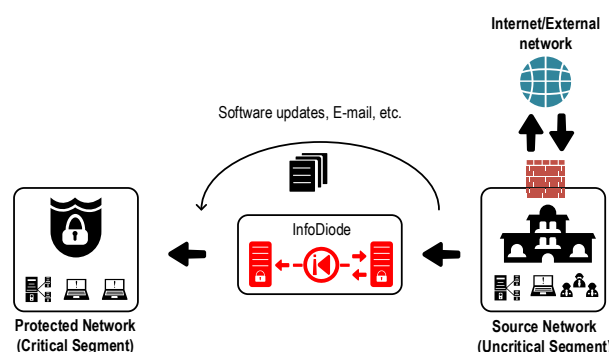
In this scenario, the integrity of the data transmitted is guaranteed.
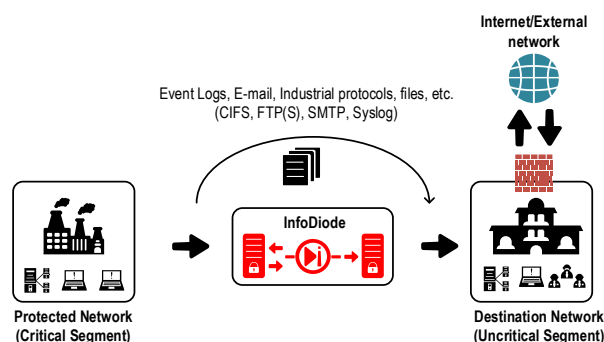
Scenario 2. Data import from external sources

Scope of application: government, enterprises of the defense-industrial complex, critical facilities, commercial organizations using closed networks.

This scenario guarantees confidentiality of the protected data.

Scenario 3. Simultaneous data uploading and loading

Scope of application: any organizations using closed network segments.

This scenario provides a bidirectional but asynchronous interaction between segments. This makes it possible to achieve a high level of protection and insulation of segments with the possibility of both unloading and loading data. Given the impossibility of establishing connections (exclusion of feedback for the attacker for most protocols), this scenario significantly exceeds the level of security of traditional firewall schemes on the perimeter.
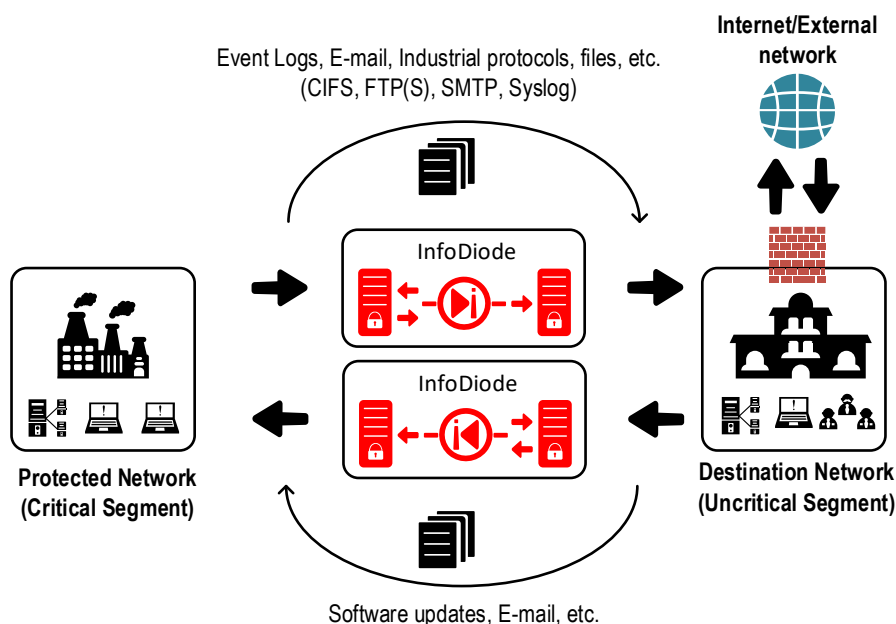
Scenario 4. Secure remote interactions between critical network segments (Site-to-Site)

Scope: Any organization using geographically separated closed network segments.

The scheme provides a high level of protection against external threats (similar to Scenario 3) and effective isolation, while maintaining full-fledged two-way secure interaction of remote nodes.
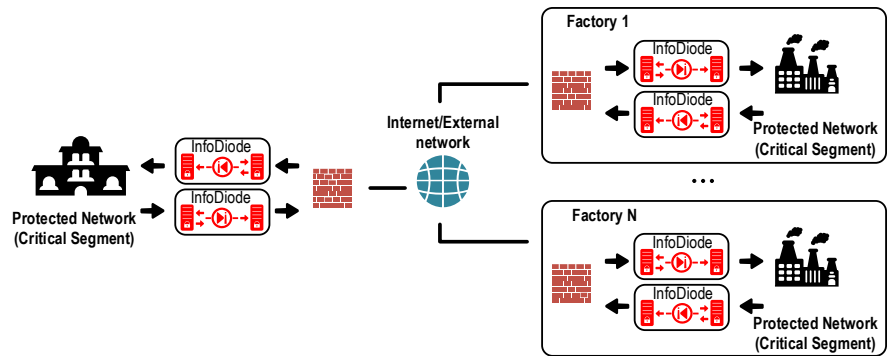
Scenario 5. Creation of an isolated demilitarized zone

Scope: any organization that needs secure remote access.

In some cases it is necessary to provide secure remote access to the company's resources both internal users and partners, suppliers and contractors. Scenario 5 implies the creation of an isolated demilitarized zone to which only permissible for remote users and contractors/partners data. This ensures the privacy and integrity of critical data within the information system: it prevents remote users from accessing internal resources through VPN connections.
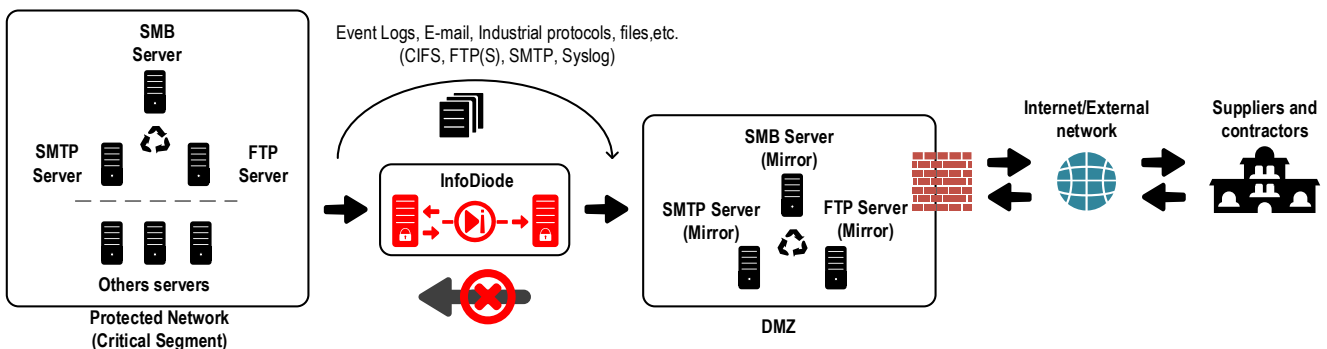

Scenario 6. Broadcasting from an automated workstation application in a closed segment

Scope: contractors, external support services, vendor support services, remote monitoring.

In the case of interfacing networks with different levels of criticality, it is required to provide external monitoring of the state of indicators of technological equipment, network, etc. in accordance with what is observed on the screen of the operator's monitor, right down to controlling mouse and/or manipulator movement. Scenario 6 allows you to organize streaming desktop information «as it is» beyond the critical segment. This ensures the privacy and integrity of data within the information system: it eliminates the ability of remote users to access and influence operator computer and the

network within the critical segment through VPN connections, RDP connections to internal resources.

09.12.22
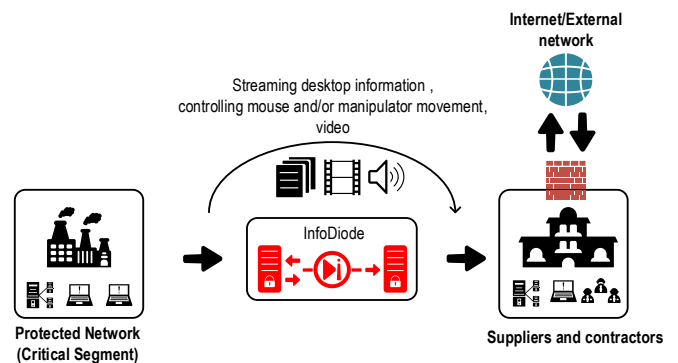
InfoDiode PRO technical specifications

Characteristics	Specifications
Transmission rate	Up to 900 Mbps
Fault-tolerant solution	Yes
Supported protocols	FTP/FTPS, CIFS, SMTP, SFTP, StartTls, IPSec, UDP, SNMP, Syslog, NTP, Active Directory
Interfaces	4 x 1000Base-T
Switching interfaces within the InfoDiode PRO between the hardware component and servers	1000Base-SX
Mounting	
InfoDiode PRO base	3 rack units
InfoDiode PRO cluster	6 rack units
Power supply	100 – 240 V (AC)
Operating conditions	10 – 35 C, humidity 5 - 95 %

Ordering information

P/N	Description	Detailed description
InfoDiode PRO base		
AMTID-IDK-1000-SCFM	InfoDiode PRO base, including InfoDiode PRO software	2 proxy servers, InfoDiode RACK single (AMTID-HW-BK), 3RU form factor, InfoDiode PRO software
InfoDiode PRO cluster		
AMTID-IDK-2000-SCFMHA	InfoDiode PRO cluster, including InfoDiode PRO software	4 proxy servers, 2 ACC InfoDiode RACK double (AMTID-HW-HA-BK), 6RU form factor, InfoDiode PRO software