Revolutionizing the Data Diode

Data diodes are no longer the complex, expensive solutions of the past. DiOTa provides a low cost, easy-to-use, minimal overhead data diode cybersecurity solution designed to protect digital assets and provide secure data transfers with low throughput requirements. This hassle-free device combines the unhackable security and minimal maintenance of hardware-enforced data diodes with an all new user interface and easy setup, all at a lower total cost of ownership than firewalls.

Built for the IIoT

As endpoints are rapidly multiplying and new connections proliferate, DiOTa provides a fit-for-purpose solution to secure the new landscape of IIoT devices, including distributed and remote OT assets, and cloud connectivity. It can be deployed at the edge the operational technology (OT) environments or right at endpoints for 1:1 secure one-way transfer of SCADA, SIEM, files, and other data to external users or platforms. Even traditionally off-limits devices, such as safety systems, can be safely connected directly to the cloud.

No Expertise or Updates Required

Take control of your OT security. Unlike competing solutions, including software-based firewalls, DiOTa requires little to no specialized resources for setup, ongoing configuration management, or software updates. It can be set up in minutes with no security expertise required. Unlike IT security solutions, DiOTa is designed to last over 10 years to secure OT digital assets for their entire lifetime with a single, easy configuration. There simply is no other solution available that combines this level of security at a lower TCO or higher ease of use.

Mass Deployments at a Fraction of the Cost

With affordable pricing that scales with deployment, get up and running quickly and stay secure for years with zero training and little to no upkeep costs.
Simple, Compact, and Lightweight

DiOTA is specifically designed for the requirements of modern OT environments and micro-segmentation (1:1 protection) of digital assets within the IIoT. Its extremely low SWaP (size, weight, and power) requirements are ideally suited for the security and data collection from edge, remote, and distributed assets without adding significant overhead. Built on an ARM-based, secure hardware platform, DiOTA allows for optional DIN rail mounts, taking up minimal space after installation.

Unhackable Security

Sophisticated threats can use coordinated, persistent tactics to overcome firewalls, advanced RBAC, passwords, multi-factor authentication, and even biometrics, but jumping the physical gap in a data diode with electronic tools remains impossible. While firewalls are enforced by configurable code and policy, DiOTA is physically enforced with a hardware-based security mechanism and provides 100% confidentiality and segmentation between networks.

DiOTA is also not vulnerable to the software bugs, zero-day exploits, or misconfiguration that plague firewall solutions, and provides something firewalls simply cannot: protection from the unknown. The device does not need regular patching or maintenance to stay secure, and the enforcement mechanism never becomes less effective over time.
Intuitive UI for an Effortless User Experience

DiOTA’s user interface features an intuitive, browser-based administration tool that’s extremely easy to set up and manage. No specialized skillset or security experience is required. Sit back and watch the data flow across DiOTA in real-time via the built-in dashboard visualization tool.

No Special Skills Required
Easy to Use Setup Wizard
Zero Ongoing Maintenance

Do Less, Secure More

While software firewalls often lure in customers with low upfront costs, they tend to conceal their biggest financial burden - the resources required for ongoing, long-term maintenance. For OT/IoT environments with limited security resources, DiOTA provides far greater security without any of the burden and stress of onerous configuration, patching and updates, and policy management. It can be maintained on a shoestring budget or left completely alone – no misconfiguration or unpatched vulnerabilities to worry about.

While most competing solutions can take hours or days to install and configure, DiOTA can be up and running in less time than your last coffee break.
Get Started Immediately

Quickly and easily begin setting up your DiOTa with the Quick Start Guide provided with your device. The Quick Start Guide provides guidance on how to set up the DiOTa hardware in your environment and how to configure the source and destination sides on DiOTa’s user interface.

Quick Start Instructions

1. To set up DiOTa, run the setup wizard on both the Send and Receive sides. You will need a computer.

Setup Wizard

Quickly set up and configure DiOTa in minutes with the user interface Setup Wizard. Select your protocol and fill in the network addresses for your source and destination. Because each side is independently administrated for additional security, users configure the send side of the DiOTa and then follow the same steps for the receive side. It’s as simple as that. Most users are up and running in less than 20 minutes.

Built-In Help Guides

Any time you need support with configuring your DiOTa, visit the Help tab on the user interface and access product documentation at your disposal. Whether you need guidance with changing your password or enabling protocol adapters, help is available on-demand, whenever you need it – no calling, no waiting.
Two-Way in a One-Way World

A successful one-way data transfer requires meeting the expectations of a two-way world. A majority of network traffic involves some sort of acknowledgement or two-way connection in order to function (an obvious exception is UDP). The “secret sauce” of DiOTa is in providing a one-way transfer, with a true separation between source and destination networks, while maintaining simultaneous two-way communications with both the source network and the destination network to avoid disruption. This is accomplished through using proxies that run on each side of DiOTa.

The send side proxy communicates with the source network, acknowledging the receipt of packets before extracting the payload, and then sending it across DiOTa. On the receive side, the proxy receives the payload, builds a new packet around it using the original protocol, and sends the data on its way over the two-way protocol. In this way, DiOTa achieves a one-way transfer in the middle of two two-way exchanges.

Supported Protocols

- TCP
- UDP (Unicast & Multicast)
- File Transfer
- Modbus
- Syslog
- OPC DA
- OPC A&E
- SNMP Traps (UDP, TCP)

Loopback Test

Validate that the DiOTa hardware is functioning within factory specifications by continuously sending data packets from the Send side to the Receive side within a specified time length.
Securely Enable Cloud Connectivity

Securely connect devices to the cloud in minutes with zero risk. DiOTA’s hardware-enforced security means users no longer have to worry about adding firewall rules in the DMZ and Enterprise zones of a traditional Purdue Model each time a device is added. In addition, the unhackable nature of the device means data from even previously untouchable devices such as safety instrumented systems can be securely connected directly to cloud platforms or monitoring centers for analysis.

Technical Specifications

**OPERATING CONDITIONS**
• -4°F to +113°F / -20°C to +45°C
• 5% to 90% humidity non-condensing

**POWER SUPPLY**
• Input: 9-25V DC
• Estimated normal operating usage: 10W total
• Connector Options
  + Option 1: AC power brick with barrel connector (included)
  + Option 2: DC power phoenix connector (DIN rail clip included)

**MOUNTING SYSTEMS**
• Tabletop
• DIN rail (DiOTA DC only)

**APPROVALS**
• FCC Class B compliance
• CE mark
• IEC/EN 62368-1
• CAN/CSA-C22.2 62368-1:2014
• VCCI
• Based on EAL certified technology

**ISO**
• Manufactured using ISO9001: 2015 certified quality program

**THROUGHPUT**
• Maximum of 5 Mbps

**CHASSIS SIZE & WEIGHT**
• 1.75” W × 6.75” H × 5.75” D
• 4.44 cm × 17.15 cm × 14.48 cm
• 1 lb / 0.45 kg

**SUPPORTED PROTOCOLS**
• TCP, UDP (Unicast, Multicast), File & Directory Transfer,
  Modbus, OPC DA/A&E, SNMP Traps (UDP, TCP), or Syslog

**MEAN TIME BETWEEN FAILURES (MTBF)**
• 10 years

**NETWORK CONNECTIVITY**
• Separate ethernet connections for network data and administrative functions
• Physical connectors: 8PBC (RJ45)
• Supports 10BASE-T, 100BASE-TX