

New! Canary Uni-Directional Data Security Diodes

Featuring:

- **One-Way, Air-Gapped Data Forwarding** ▪ **Reversed Transmissions Blocked** ▪
- **Simple Host Connections with RJ-45 Auto-Negotiation & Auto-Cross** ▪
- **"We Deliver Data Assurance and Increased Customer Confidence!"** ▪

Canary Uni-Directional Data Security Diodes help defend against a broad range of external, Cross-Domain and insider cyber threats that can escape common security applications to reveal or corrupt sensitive information & make mission-critical Data Services non-available.

Protect secure servers and sensitive data from compromise. Data Security Diodes stand guard between domains where un-restricted, two-way communications increases risk of penetration, malicious attack and data loss.

Application 1: Canary 100 Megabit **CT-20SD** and Gigabit **GT-10SD** Data Security Diodes forward information originating from an *un-secured* open source to a restricted High-Security destination. Simultaneously, they *optically isolate* the data path to stop all return-path transmissions and completely block the reverse transmission of sensitive information.

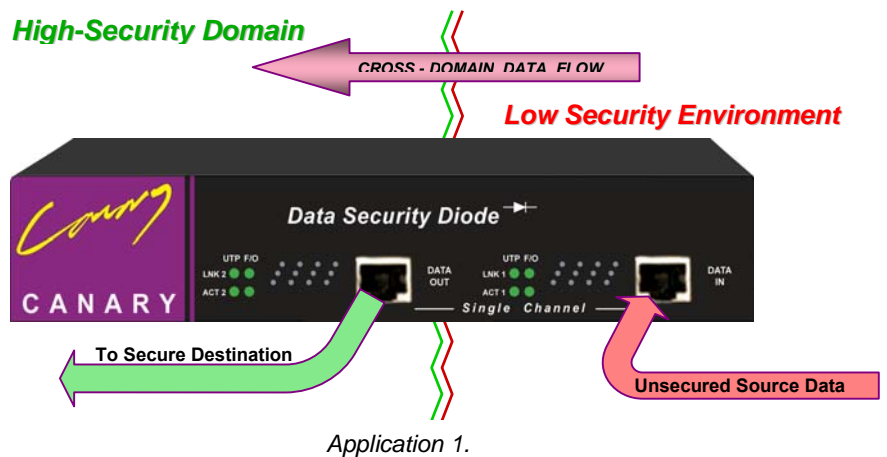
Application 2: Position a Canary Data Security Diode to optically isolate a secured, trusted, information source and *selectively forward* authorized data to weakly protected *insecure* lower domain destinations.

The partitioned data path *shields the* Secure Source from hidden viruses, Trojans, malicious programs or other intrusion attempts and prevents the corruption or unintended release of critical data, or its loss and non-availability.

Local Data Diode/Host UTP connections are negotiated to pseudo full-duplex mode but bi-directional full-duplex traffic is not internally forwarded between Data Diode input and output ports. Data handling functions including IP acknowledgement, Flow-Control and CRC error notification are completely disabled and no internal or external means are available to defeat the Diode Uni-Directional function.

As another defensive layer for your critical data, Canary Data Security Diodes "*Deliver increased confidence and peace of mind!*"

CT-20SD & GT-10SD: UTP to UTP Single-Point Data Diodes



▪ Plug-and-Go UTP Connections:

Configure your application to run via UDP. Connect the *un-secure* device to the **CT-20SD** or **GT-10SD** Security Diode "Data-In" port; then simply connect the Security Diode "Data-Out" port to the Secure Domain Host for restricted, optically isolated, one-way data transmission (*Application 1*). Reverse the connection scheme for *Application 2*.

▪ Flexible, Secure Network/Host Configurations:

Low to High: Forward information to a Higher Security domain while blocking the un-authorized release of sensitive data in the reverse direction;

High to Low: Restrict authorized user access. Maintain System and Data Security, Integrity and Availability while allowing the limited export of selected information to lower security-level destinations.

▪ Hardwired Immunity from External Software threats:

Canary **CT-20SD** or **GT-10SD** Data Security Diodes execute their key functions in hardware. With tamper-resistant cases, there is no vulnerable software, firmware, memory or buffers that can be exploited to attack and surreptitiously alter or disable Diode Uni-Directional operation.

Using UDP or similar protocol over a point-to-point link eliminates the need for normal transmission acknowledgments.

Control physical access to your Canary Data Security Diodes and their cable connections to thwart unauthorized access and safely deliver critical data where needed – *Easy, Secure, Information Availability!*

Canary Communications

Main Features:

Interfaces – Local Connections:

- CT-20SD or CT-20SD-V: Two 100BASE-TX (RJ-45) Ports *
- GT-10SD or GT-10SD-V: Two 1000BASE-T (RJ-45) Ports *
- * (plus Internal Fiber Optic Link between physically isolated PCBs)

Networking – Local User Connections:

- 100BASE-TX & 1000BASE-T: Auto-negotiation and Auto-crossover enable half/full duplex Ethernet Diode Links with *local* Source and separately, with *remote* Destination equipment.



Management;

- No management reporting or access to internal functions
- No provision for error handling/reporting

Mechanical & Environmental:

- Inside, Desktop locations or 19" rack-enclosures
- Two units can be mounted side-by-side on a standard 19"-wide shelf (available from Canary)

Please contact Canary for technical details on additional models.



Specifications:

| | | |
|-------------------|--------------|-----------------------------|
| Standards: | IEEE 802.3u | 100BASE-TX * |
| | IEEE 802.3ab | 1000BASE-T * |
| | IEEE 802.1d | Spanning Tree: None |
| | IEEE 802.1q | VLAN: Limited Functionality |
| | IEEE 802.3x | Flow Control Not Supported |

Throughput: 100 Mbps (One-way transmission Max.) or; 1000 Mbps (One-way transmission Max.)

Max Distances: RJ-45/UTP : 100 meters
* See *Data Rates* Note above *

Max. Altitude: 2000 meters

Enclosure: NEMA 1 and International Protection: IPX0

Power: 100 ~ 240 VAC Auto-ranging wall-mount, typical (-V): 9 - 48 VDC input + Terminal Block option (-V) versions use external DC Power sources

Temperature: Operating: 0° C to 50° C
Storage: -20° C to 70° C

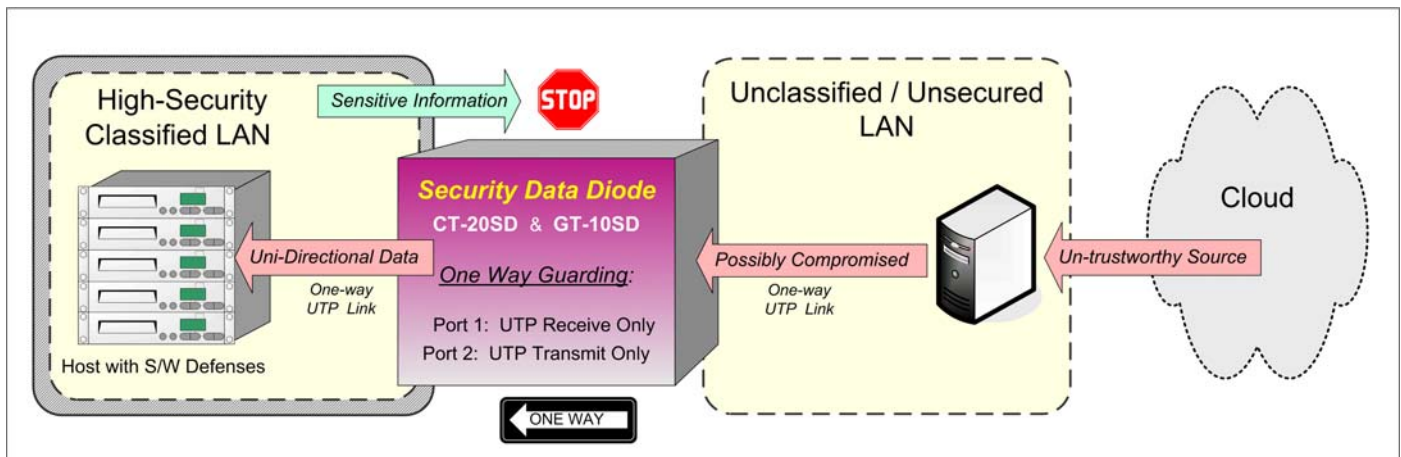
Humidity: Operating: 10% to 80% RH
Storage: 5% to 90% RH

Emissions: CE Mark EN60950 & EN55022 and FCC Part 15 of Class A

Safety: US 21 CFR (J) & EN 60825-1 standards and UL 1950 applications, EN 60950, CE, TUV

Dimensions: 5.21 in. x 8.43 in. x 1.64 in. (D x W x H)
[12.7 cm x 20.3 cm x 4.4 cm] (D x W x H)

Weight: 5.5 lb. (2.5 Kg) (shipping wt.)



JM 04.10.17

For more information please visit us at:
www.canarycom.com
info@canarycom.com

Canary Communications is an
ISO 9001 : 2008 Registered Company

