Terafence
IoT Cyber Security

Technical Brief

Designed to protect IoT and IIoT equipment, Terafence TFG-1URP uses Air-Gap to segmentize and isolate industrial end-devices from any harmful, or abusive, malware attacks and thus secure them from any form of cyber-attacks.

Terafence's proprietary hardware chip (FPGA), developed and manufactured in Israel, creates a fully controlled data-path between two network segments and while allowing normal protocol data to flow from one side to the other, the return path simply does not exist, hence Air-Gapped.

Terafence is acting as a Protocol Proxy, terminating TCP/IP sessions on both ends and only moving raw data between the two unidirectional gateway sides. RAW data is not stored within the unit thus eliminating the requirement to safeguard such data by encryption or other methods. As nothing is stored, no such tools are used (like data encryption, compression or alike). Terafence technology and network mechanisms do not use cryptology to secure data exchange but instead denies network access.

Terafence TFG-1URP not only protects IoT/IIoT end-devices from cyber-attacks but also can protect other network assets by blocking any malicious attempts by an already infected end-devices to infiltrate and infect devices with malicious code or cause other kind of damage.

Terafence TFG-1URP supports multiple, simultaneous protocols:

- SFTP/FTP/SMB- File transfer
- SMTP – Email Relay
- SYSLOG Forwarding
- RTSP – CCTV live streaming
- HTTP/S – File / data upload to web servers / cloud
- Local SYSLOG forwarding
- Modbus – Multiple PLC's to multiple HMI's
- IEC-104 – Power utilities
- MQTT – Data Broker and Publisher

Key Features:

- Total galvanic network separation
- Terafence proprietary hardware chip (FPGA)
- HTTPS WEB GUI for configuration (from secure side only)
- Two accompanying CPUs for protocol support

Security features:

- Hardened Linux operating system on accompanying CPUs
- Core security hardware has no OS, no MAC/IP
- Secure unit access (HTTPS) to GUI

Technical Specification:

- 1Gbps data throughput
- Dual Input Voltage: 100 – 240 VAC 50/60Hz internal fully redundant hot-swapable AC power supplies
- Network Ports - 2xRG-45 CAT5E ports
- No moving mechanical parts
- Measurements: W440 x H44 x D260(mm) (1U)
- 19" 1U rackmount, desktop mounting
- Operating temperature – (-40) ~ (+70)OC
- In-door use only
- FCC Part 15, Subpart B, Class A

Solution Highlights:

- Total Galvanic, physical network separation, hardware based on Terafence's proprietary FPGA CHIP.
- Solution includes two accompanying CPUs for protocol support and termination (none transparent proxy).
- Simple, easy configuration using HTTPS GUI
- 1Gbps backplane
- IEC62443-4-2 – SL2
- MIL-STD-810F Method 516.5
- 20 Year MTBF

Terafence’s Partner Details:

www.hennsol.com.au
Info@hennsol.com.au

TERAFENCE COMPRISES
PROFESSIONALS TO MAKE IoT & NoT
SECURE FROM MALICIOUS ATTACKS

Terafence Ltd. specialises in the development of advanced firmware/microchip solution for cyber security connectivity and additional mechanical waves based solution to control medical implants and wearable devices. Established in 2015, Their patent pending TFence™ technology uniquely offers total protection from tampering or hacking IoT devices by completely blocking data entry – while maintaining data outflow and control. And relevant patent describing secure way to control implants and wearable based on ultra sound waves. Their pioneering company comprises seasoned professionals sharing a common goal – to make IoT and NoT safe and secure from malicious attacks.

www.terafence
info@terafence.com