Terafence

IoT Cyber Security

Terafence Vsecure 20|50

Technical Brief

Designed to protect CCTV equipment, Terafence Vsecure uses Air-Gap to segmentize and isolate CCTV 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 Vsecure not only protects CCTV from cyber-attacks but also can protect other network assets by blocking any malicious attempts by an already infected CCTV devices to infiltrate and infect devices with malicious code or cause other kind of damage.

Terafence installation and configuration are done using automatic tools such as Onvif camera detector and WEB based GUI on the Secure side (Side_A).

.

Security Features

- Protects IoT/NoT devices from TCP/IP-based attacks (IP cameras on segmented networks)
- Terafence Proprietary FPGA hardware-based Data flow direction control enforcement at the physical and logical layers 1/2
- Complete block of information flow, either physical or logical
- Hardware based Uni-directional return channel for protocol commands to end-devices, without potential cyber risks.
- Strong solution utilizing multiple independent security layers: Hardware at layers 1&2, Linux system at 3&4 and Software at application levels (5,6,7)
- Timed, event or logic decision-driven centrally controlled camera hardware power cycling*
- Prevents non-authorized viewing of video streams controlled by the Vsecure data-flow direction control unit.**

Device Management

- Provides camera-operational alarms, information and statistics such as down time, bit rate per camera, upper or lower bit rate, thresholds and more statistics
- Provides a centralized tool for management and camera control *
- Warns against vandalism or camera alteration, such as turning the camera from a preselected angle. *
- Provides the ability to promptly disconnect a suspiciously infected device/network from the company infrastructure**
- High throughput per unit – 1Gpbs.
- Load balancing **
- High availability via unit clustering **

* Future release
** Optional