WATCHER – Datasheet

Watcher is a network monitoring and situational awareness platform that provides in-depth visibility and cyber resilience for Informational Technology (I.T.), Operational Technology (O.T.) / Industrial Control Systems (ICS) and Internet of Things (IoT).

Performs full deep packet capture and inspection (DPCI) allowing for detailed asset inventories across all domains (I.T., O.T., IoT, and IIOT) in addition to unparallel network situational awareness.

Automatically collects a wide range of asset information, logging all configuration changes for security analysis and storing on FIPS-140 compliant SSD for offline operational forensics.

Full pcap capture and storage

Asset Inventory and Network Map

- Automatic asset, communication and vulnerability inventory with full device fingerprinting
- Interactive visualizations of threats and risks
- Ability to ingest existing inventory lists for comparison and validation
- Geolocation and metadata

Network and Process Monitoring

- Complete network monitoring capture and monitoring
- Preconfigured network and process whitelists option
- Automatically passes alerts to operator display
- Hosts, Users, Applications, Protocols, Locations, Centers of Activity, Data Flow.
- it will look at FQDNs, URLs, IP Address, GEO Location, and Files to compare against known IOCs and GEO Location to detect any compromised devices that would be communicating outbound from the network.

Plug and Play & Customizable

- Connects via mirror / span port
- Ships preconfigured to immediately start capture right out of the box
- Temporary or permanent deployment

Logging & Investigation

- Logging and detailed network analysis of all communications and file operations
- Removable encrypted SSD

Threat Monitoring Integration

- Comprehensive monitoring for rogue communication indicators
- Partner threat intelligence ingestion
- SIEM agnostic

Dashboard and Reporting

- Dashboards for easy network visualization and asset threat visibility, including alert trends, asset charts etc.
- Sophisticated visualization engine that displays your network nodes and communication pathways.
- Detailed alert details to enable cross correlation for analysis and incident response.
- Ability to generate editable graphical reports.

Data Security Enclave Validation

- Instantly identify communication leaks in and between enclaves

Components and Architecture

Watcher provides the customer with an in-depth detailed device and network communication visibility allowing for detailed enhanced network situational awareness and cyber resilience for networks. By connecting to the SPAN/mirroring port of a network switch, it can passively and if required hybrid-actively establishes a highly granular device inventory and network baseline of normal communications. Watcher immediately alerts if there is a deviation, enabling real-time operational response and cyber risk management.

Available Configuration

System

Processor	Support for Intel Apollo Lake Atom Processors Atom x7-E3950 Atom x5-E3930
Processor Speed	1.3 ~ 1.6 GHz
Processor Cores	2 ~ 4
Integrated Graphics	Intel HD Graphics 500/505
Memory	Onboard LPDDR4 4 ~ 8 GB

Top I/O

Serial	2 RS-232/422/485 COM
Power	3-Pin Terminal Block Power Input (9 ~ 36 V) Intelligent Ignition Sensing

Front I/O

USB	4 USB 3.0
Other	3-pin CAN bus 8-bit Isolated Digital I/O (4-in, 4-out) Audio jack (Line-Out; Mic-In) Micro-SIM slot Power button

Bottom I/O

Ethernet	3 GbE LAN with Intel I210-IT controllers (2 PoE optional)
Video	2 DisplayPort

Expansion & Features

Expansion & Storage	1 M.2 2280 M-key (PCIe x4, SATA) 1 M.2 2230 E-key 1 mPCIe
Features	Onboard TPM 2.0

Mechanical

Dimensions (WxHxD)	56 x 154 x 119 mm (2.20 x 6.06 x 4.69 in)
Mounting Options	DIN-mount VESA-mount Wall-mount

Environmental & Regulatory

Operating Temperature	-25°C ~ 70°C
Storage Temperature	-40°C ~ 85°C
Shock	Tested according to IEC 60068-2-27 and MIL-STD-810G
Vibration	Tested according to IEC 60068-2-64 and MIL-STD-810G
Certifications	UL Listed configurations available CB Scheme FCC 47 CFR Part 15 Low-Voltage (2014/35/EU) Electromagnetic Compatibility (2014/30/EU) Radio Equipment (2014/53/EU) - Only applicable for configurations with wireless transmitters EN 55032 EN 55035 RoHS 3 (2015/863/EU) WEEE Directive (2012/19/EU) Power Immunity According to E-Mark 7637-2 & 16750-2 EN 50121 EN 62368-1 IEC 62368-1 UL 62368-1