pMon-751
Product Overview

PFP Cybersecurity's pMon-751 supports simultaneous standalone integrity assessment of connected devices while addressing both hardware and software security threats. pMon-751 allows the user to monitor target devices directly EMI, or via DC using an inductive current probe.

No threat intelligence required
pMon detects abnormal execution behavior and alerts instantly, so it only needs to know what is "normal" activity. Anything outside of the learned normal behavior is flagged.

No performance or operational impact
While traditional cybersecurity approaches involve installing software or monitoring network communications, pMon analyzes side channel signals emitted during software execution which represent power consumption.

Cannot be detected by the hackers/Impossible to evade
Since pMon has no communication with the target device, attackers have no way of knowing they are under observation, and the technology is nearly impossible to evade.

Real-time malware detection - Malicious or Accidental
Continuous 24x7 real-time monitoring with malware detection time in milliseconds. Our PFP Analytic software detects any firmware/software change, including both active and dormant attacks.

Simple Human Dashboard and Standard Interfaces
At the user level, you want to know, "Am I good?" Our red-light/green-light dashboard provides status at a glance. But when things go wrong, you need information in depth, situational analysis. PFP integrates and communicates with industry standard Security Information and Event Management (SIEM) tools.

Easy Install
pMon installs quickly without modifications to the target system.

Broad Application
pMon supports a wide variety of targets, from chips, to boards, to devices, and to systems. pMon is rated for operation in industrial environments.

No Impact on Certifications plus Quality Assurance
No software modification on the target means existing safety certifications do not need to be recertified. The dedicated pMon also warns of hardware changes, faults and failures instantly.

About Us

PFP Cybersecurity provides an IoT platform for security, safety, and quality.

Contact Us

www.pfpcyber.com
540 - 200 - 8344
1577 Spring Hill Road # 405
Vienna, VA 22182

Specifications

Mechanical

- Dimensions
  6"H x 2.1"W x 4"D
- Weight
  TBD
- Mounting
  35mm DIN rail
- Protection Class
  IP30 (>2.5mm Tools, thick wires, etc.)

Certifications

- Safety of Industrial Control Equipment
  UL E145483

Environmental

- Operating Temperature
  0˚C to +50˚C (commercial)
- Storage Temperature
  -40˚C to +85˚C
- Relative Humidity
  5% - 95% (non-condensing)
- Vibration
  IEC60068-2-64

Reliability

- Standard Warranty on Hardware
  1 year
- MTBF
  TBD

LED Indicators

- Power
  On
- PFP Monitoring
  Blink per cycle
- Fault
  Malware Detected
- Network
  Link Status, Activity

Interfaces

- Ethernet
  10/100/1000 BaseT
- Serial
  RS232

Specifications (model specific)

Model	Power Sensor	Sensor Input	Power Input	Advantages
pMon-751	EMI Probe	SMA	2 sensors & 2 triggers	Localization of tamper to specific component or standoff monitoring
pMon-751	DC Current	Screw Terminal	2 sensors & 2 triggers	Chip, board and device level detection via external power connection