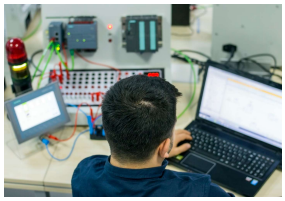
FORTIPHYD LOGIC

Fortified security for industrial networks

LogicWatch Pro

Controller endpoint detection




- Industrial controllers are still primarily “insecure by design”, allowing attackers to easily use legitimate functionality for catastrophic results
- Traditional endpoint detection and response (EDR) software cannot be installed on embedded industrial controllers like PLCs and RTUs
- Network sensors are too expensive and difficult to deploy for every controller in the network
- Performance and maintenance problems are difficult to diagnose, resulting in costly downtime
- Modifications to controllers made from insiders with physical access go unseen by traditional network monitoring systems

DETECT INTRUSIONS

Detect advanced cyberattacks and insider threats with patented machine learning anomaly detection

REDUCE DOWNTIME

Diagnose issues at least 3x faster with detailed logging of controller information and events all in one place

NO NEW HARDWARE

Gain visibility into your controllers with zero new hardware deployed on your network

Key Features and Benefits

Industrial controllers, like PLCs, RTACs, and RTUs, are a vital bridge in ICS networks, translating digital commands into physical actions. Unfortunately, they are often “insecure by design”, allowing attackers to use legitimate protocols and functionality to achieve their goals without having to find any zero-day vulnerabilities.

Traditional IT security solutions like endpoint detection and response (EDR) simply cannot be installed on the embedded, real-time systems. Network monitoring sensors are expensive and difficult to deploy thoroughly enough to monitor all controllers, and will still miss any activity by insiders with physical access to the controllers’ serial ports. Finally, performance and maintenance problems related to the controller configuration are often difficult to diagnose due to the lack of visibility.

LogicWatch Pro equips operators of critical infrastructure with unprecedented visibility into their controller operations to detect threats to their security, safety, and efficiency. The LogicWatch Pro “agent” uses native controller code (Ladder Logic e.g.) to extract key system diagnostic information without the need for any burdensome firmware modifications or hardware sensor deployment. The diagnostic information is fed into patented machine learning algorithms to alert operators when the controller is in an anomalous state that could indicate a nation-state level cyber attack, or deteriorating performance.

FORTIPHYD LOGIC
1345 Seaboard Industrial Blvd NW
Suite C7
Atlanta, GA 30318
info@fortiphyd.com

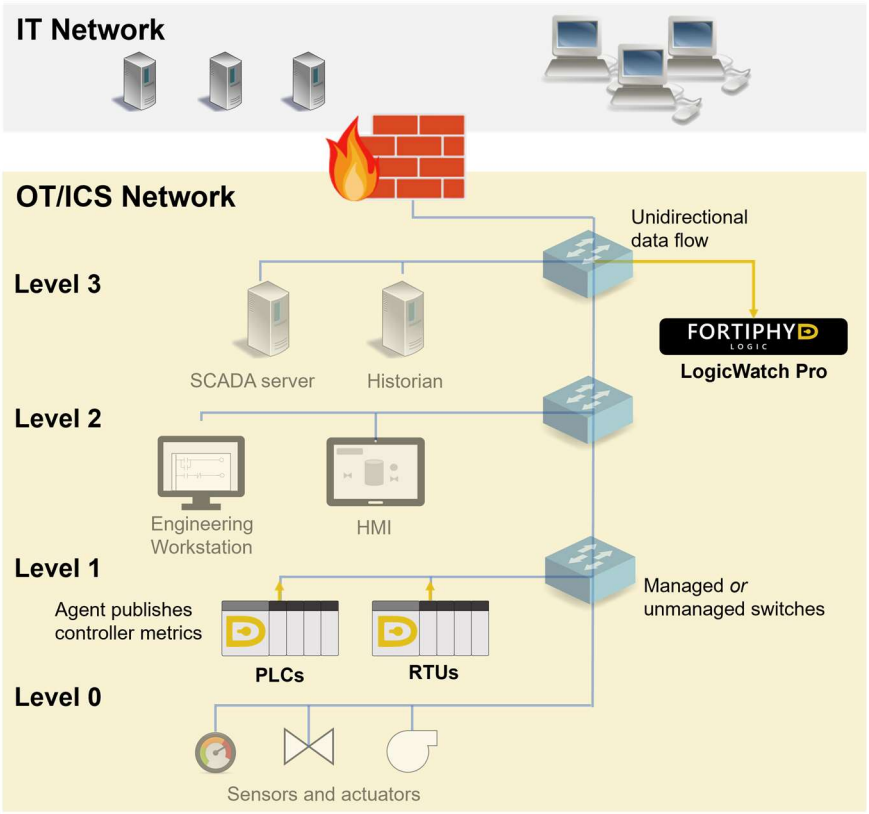
FORTIPHYD LOGIC

Fortified security for industrial networks

LogicWatch Pro

Controller endpoint detection

Deployment Architecture



Deployment Steps

LogicWatch Pro saves labor and money compared to network monitoring deployments at the PLC level by requiring **no hardware sensors** and **no mirror ports.** Deployments simply follow the following steps:

- Add the prebuilt LogicWatch Pro agent to the control logic of each controller being secured
- Deploy a single LogicWatch Pro server (physical or virtual) to collect all your controller metrics

OT NATIVE

The LogicWatch Pro agent uses native controller code, naturally integrating with your existing system with negligible overhead

OT FRIENDLY

Engineers are tired of having security forced on them to just check a compliance box. Choose a solution that adds as much value to operations as it does to security.

OT AFFORDABLE

Gain visibility into your controllers at 20% the cost of an equivalent network monitoring deployment

For more information on any of our products or services please visit: www.fortiphyd.com

FEATURES

Native

Hardware-Free

Affordable

FORTIPHYD LOGIC
1345 Seaboard Industrial Blvd NW
Suite C7
Atlanta, GA 30318
info@fortiphyd.com