WL-630F-S

Industrial Core Firewall

Insights:

Cyberattacks on critical infrastructures & industrial environments are no longer a myth. Power generation facilities, metropolitan traffic control systems, water treatment systems, and factories are all at risk. Exploits freely available on the Internet make the Industrial Control Systems (ICS) of leading vendors easy targets for attackers.
These ICS environments can be harsh — exposing networking equipment to extreme temperatures, humidity, dust, and vibration. They require a rugged and reliable security gateway solution to detect threats and control access to critical components.

Solution:

The WitLinc WL-630F-S is a rugged appliance delivering Next Generation Threat Prevention for Critical Infrastructure and Industrial Control Systems. This solid-state appliance secures SCADA (supervisory control and data acquisition) protocols and OT(operational technology) equipment. The WL-630F-S includes Firewall, IPS, Application Control, Antivirus, Anti-Bot and Snort Zero-Day Protection.

Next Generation Firewall

WL-630F-S offers broad support for specialized SCADA and ICS protocols for over 5 SCADA specific commands. Additional protocol support is available on request.

- **PROTOCOL SUPPORT**: CIP | DNPNET | Modbus TCP/IP | OPC |S7-Net(Siemens)
- VPN **PROTOCOL SUPPORT**: IPsec, L2TP, WiVPN

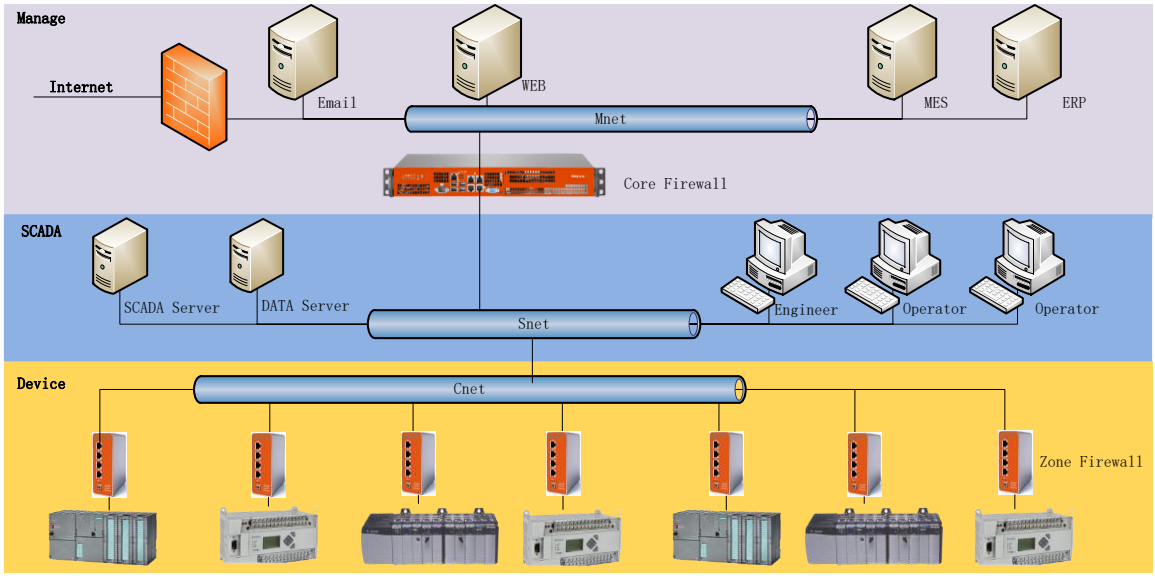
Integrated Threat Detection:

Detect and prevent targeted attacks against ICS/SCADA components in Operational Technology (OT) environments. With the best catch rate in the industry, our threat prevention technologies minimize the disruption of operational processes when deployed in detect-mode.

Best-in-Class Management:

Our unified, integrated management platform supports distributed IT and OT deployments, leading to operational consistency and efficiency of end-to-end (E2E) security. Administrators can define security policy for the entire network — including internal security, main sites, and remote sites — from a single, centrally located WitLinc Security.

With Web management approach designed for large-scale deployments, administrators can define a single security and device profile and apply it simultaneously to thousands of appliances — dramatically reducing deployment time and administrative overhead. With built-in compliance, meet and exceed emerging regulatory and other cyber security requirements. We constantly monitor the compliance status of the organization with hundreds of best practices, letting network security managers quickly assess the streng.



Technical Specifications

Network

LAN: 2 x 10/100/1000Base-T RJ45 ports | DMZ: 1 x 10/100/1000Base-T RJ45 or 1 x 1000BaseF port

WAN: 1 x 10/100/1000Base-T RJ45 or 1 x 1000BaseF port | USB: 2 x USB 2.0 2×USB3.0|VGA×1|SFP:4×1000BaseSFP（option）

Performance	2 Gbps firewall throughput, UDP 1518 bytes | 100 Mbps firewall & IPS 450 Mbps VPN throughput | 400,000 concurrent sessions
Network Connectivity	VLAN:1024 | 802.1X security | Layer 2 (transparent) and Layer 3 (routing) mode
Routing	OSPFv2 and v3 | BGP| RIP | Static routes | Multicast routes | Policy-based routing
High Availability	Active/Passive - L3 mode

Hardware Specifications

1x CPUs, 8x physical cores | 8 GB memory | 1x 128GB (SSD) drive

Size	(W x D x H): 160x120x42mm
Weight	1.2 kg (2.65 lbs.)
Enclosure	Rack mount 1U
Temperature	-40°to167°F / -40° to 75°C
Humidity	20%-90% (non-condensing)
Power	AC: 100-240V, 50 – 60 Hz Max power consumption: 200W
Certifications	Safety: UL, CB, CE, TUV GS Emissions: FCC, CE, VCCI, RCM/C-Tick Environmental: RoHS, REACH1, ISO140011