ITW HARTNESS

Address:
50 Beechtree Blvd.
Greenville, SC 29605

Mailing:
P.O. Box 26509
Greenville, SC 29616

P: (864) 297-1200
F: (864) 297-4486
www.Hartness.com

HartnessCONNECT Cybersecurity

Table of Contents

Introduction

The HartnessCONNECT platform design includes cybersecurity, a top priority key component for ITW Hartness clients. The software protects the integrity of client networks while offering several options for configuration to meet the demands of the network and security professionals at customer sites.

The software solution employs a defense-in-depth methodology to leverage multiple tools and technologies to secure the platform from attackers. The built-in security technologies and testing methods protect and harden the environment from malicious activity.

Most importantly, the ITW Hartness team considers collaboration with customers about how the solution works and integrates into customer networks is imperative. ITW Hartness is committed to delivering a flexible solution that increases productivity without affecting the customer organization's security posture.

Overall Design

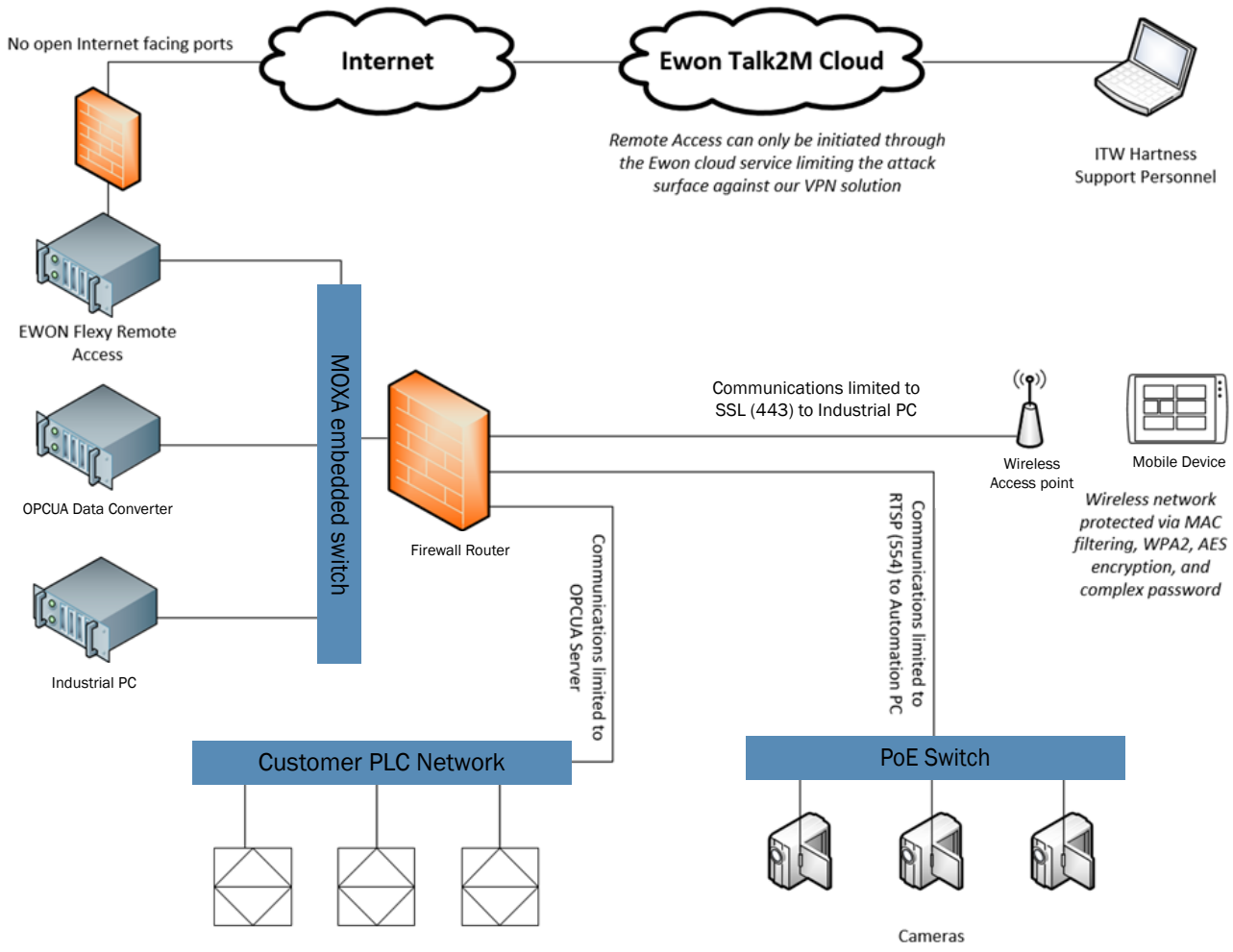
The HartnessCONNECT platform contains multiple components from disparate vendors that functionally coordinate in intuitive interface for controlling the equipment. The elements used in the solution are provided below along with a standard network diagram.
(Individual site configurations may vary based on client needs.)

Overall Design

Typical Equipment List

- Platform Switch/Firewall
- OPCUA
- Remote Access
- Industrial Control PC
- Wireless Controller
- iPad for Platform Control
- Onsite Cameras
- PoE Switch for Cameras

Architectural Design



Cyber Protection

Segmentation

The HartnessCONNECT platform is segmented to limit the exposure to the Automation PC and to prevent lateral movement throughout the network in the event a cybersecurity occurs. Figure 1 shows the logical separation of devices in the HartnessCONNECT panel along with the specific ports permitted to each device or segment. Limiting the ports and protocols allowed to connect to each device improves the overall security of the entire platform. Logging of failed connection attempts is stored for review if malicious activity occurs or is suspected.

An enterprise firewall separates the segments to permit only authorized traffic between them. Camera, PLC, and wireless networks are separated from the HartnessCONNECT platform.

Logging

The ability review system logs are required in the event of an error or cybersecurity encroachment. The HartnessCONNECT platform logs events from key systems to inform regarding system failures or cybersecurity issues.

The HartnessCONNECT platform stores the logs from devices in a centralized logging location, which may also function as a tool for troubleshooting and forensic review in the event an issue occurs at the client site. ITW Hartness uses Kiwi Syslog to store syslog messages, which are maintained on the Automation PC.

PLC Network

The design of the HartnessCONNECT solution allows for granular control of communication within the client industrial-control network. All communications between HartnessCONNECT and the industrial-control network pass through a firewall and are logged for review and analysis. The ITW Hartness team works closely with onsite personnel to ensure the solution meets the client's compliance requirements.

Backups and Recovery

The HartnessCONNECT platform stores multiple versions of its configuration on nearline storage and can be recovered quickly in the event of an attack or hardware failure. The configuration necessary to restore operations is also maintained in an offsite location and may be restored by an onsite technician in the event of a catastrophic failure.

Wireless

Operators have wireless access to the HartnessCONNECT platform for connecting via iPad to the Automation 3100 computer to operate the equipment, review metrics, etc. The wireless network has strict access controls that permit only HTTPS traffic to traverse the firewall to the Automation 3100 computer.

HartnessCONNECT utilizes an Anybus HMS AWB2030 wireless controller protected by WPA/PSK security. The wireless network is configured to use AES 256-bit encryption to transmit data. This network has also been segmented to limit access to other devices in the HartnessCONNECT platform.

Cyber Protection

Password Management

Basic password controls are often overlooked in Industrial Control System environments. ITW Hartness changes all default passwords on equipment and uses randomly generated passwords for each location. The password key for each site is a unique, sixteen-character, randomly generated password, making deciphering sufficiently extreme to thwart a would-be attack in the event a wireless handshake is captured. Passwords are not shared between locations.

Patching

The majority of cybersecurity incidents are caused by missing patches on equipment. The ITW Hartness team closely monitors the Internet for vulnerability and patching announcements from the vendors used in the HartnessCONNECT platform and works to patch equipment as soon as possible to eliminate known vulnerabilities as a risk to customers.

Remote Access

Remote access to the HartnessCONNECT platform allows the ITW Hartness team to monitor equipment and provide support when necessary. It also affords the ability to apply patches and updates to systems for security. The remote access is provided by Ewon, Talk2M to provide secure remote connectivity to our engineers without compromising the security of the client network. Its solution provides true multifactor authentication in order to access the connection portal. The system is accessible only by HartnessCONNECT support team members and is invisible to outside attackers.

The Talk2M solution requires no open inbound ports on the client firewall and does not respond to scanning or exploitation attempts from external sources. The Talk2M solution builds an outbound connection to a Talk2M server using UDP or TCP/HTTPS port. This connection may be coordinated with local onsite IT if requested and may be turned off by customer IT to be enabled when necessary.

HartnessCONNECT support personnel who wish to connect to a remote device at a customer site initiate a connection to the Talk2M cloud. Once authenticated via two-factor authentication, they have access to only the remote networks they have permission to support. All remote access is logged. This solution provides a robust connection that does not open additional attack vectors at our customer locations.

Multiple deployment models are offered for a wide range of environments:

- Leveraging an existing Internet connection provided by our clients
  The Ewon remote access solution is firewall friendly, operating over a single outbound port on the customer firewall (TCP 443 or UDP 1194). Instructions are available on how to enable and disable access to the remote VPN service through the client's corporate firewall for granular control of access.
- Implementing a cellular or broadband Internet connection for support
  The remote-access technology works over a wide range of Internet connectivity solutions. If an existing connection is not available, or preferred, a connection to be used strictly for monitoring the HartnessCONNECT platform may be implemented. This connection is secured by the Ewon remote-access device that has been penetration tested by a third-party service provider.

Cyber Protection

Pentration Testing

ITW Hartness has contracted with a third-party firm that provides penetration-testing services to test the HartnessCONNECT platform. This testing simulates real-world attacks attempting to move laterally through the platform. The testing has verified the implemented security controls have hardened the HartnessCONNECT platform, making lateral movement difficult if not impossible.

Conclusion

The HartnessCONNECT platform has been designed with the security of ITW Hartness customers in mind. The implemented defense-in-depth strategy prevents and detects malicious activity. The solution is customizable, and the ITW Hartness team can work with network and security teams at customer sites to ensure the solution makes each organization more productive without compromising security posture.

ITW HARTNESS

Proven innovation. Powerful commitment.