wurldtech

Solution Brief

Achilles Industrial Next Gen Firewall

As production systems become more interconnected, the exposure to network-based cyber incidents increases, putting production, reputation, and ultimately profits at risk. In particular, successful attacks on critical infrastructure such as oil and gas, utilities, smart grid and others can lead to devastating consequences in the economic, political, personal, public safety and privacy arenas. To mitigate these risks, Wurldtech protects system operators with the technical expertise and technology developed over many years as a leader in industrial security assessments, protection and certification.

Our solutions deliver the capabilities needed to defend your systems and address established industry standards and regulations. If it is important that you maintain the reliability, integrity and availability of your ICS/SCADA systems and networks, Wurldtech provides the security solutions you need.

Challenge

As operational technology (OT) leverages the benefits of the network, the threat of a successful cyber attack greatly increases. In fact, as reported by NSS Labs, there was a 600% increase in ICS vulnerability disclosures from 2010 to 2012. Therefore, system operators are under tremendous pressure to take the necessary actions and to ensure proper security precautions are in place to protect their critical infrastructure. System operators simply cannot respond to the growing number of security threats they face in today's environment. Specifically, system operators need a solution that addresses the following challenges when working through their security strategy:

- ICS/SCADA equipment is difficult or impossible to patch
- OT Protocols can easily be misused to disrupt critical systems
- Factory networks are very hard to rewire for proper segmentation
- Complete lack of visibility into attacks on the industrial network
- IT Security staff lacks experience with industrial equipment

BUSINESS CHALLENGE

Cyber attacks on critical infrastructure can result in significant downtime and productivity loss. System Operators need industrial-specific protections to ensure operational technology security and maximum uptime.

SOLUTION

The Achilles Industrial Next Gen Firewall is purpose-built to protect industrial and SCADA operations, offering comprehensive security, simplicity, and visibility. This network security solution monitors and blocks malicious activity and attacks to ensure highly available industrial operations for maximum uptime and secure productivity.

BENEFITS

- Protects unpatched system with strong perimeter and field defense
- Inspects and controls industrial protocol traffic with industry's leading threat intelligence
- Introduces breakthrough drag and drop virtual zoning for segmentation without re-wiring
- Displays graphical network-wide industrial security view and integrates with SIEM tools
- Simplifies security administration with easy to use graphical interfaces – no CLI required

Solution

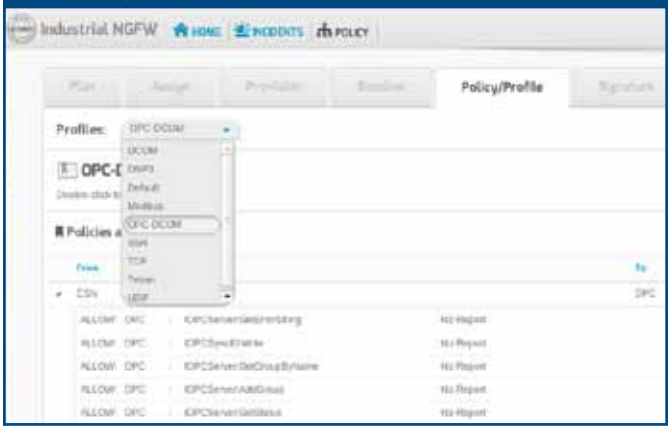
Achilles Industrial Next Gen Firewall is purpose-built to protect industrial and SCADA operations, offering comprehensive security, simplicity and visibility. This network security solution monitors and blocks malicious activity and attacks to ensure highly available industrial operations for maximum uptime and secure productivity.

The Achilles Industrial Next Gen Firewall combines the protection of a firewall, IPS and application visibility and control (AVC). These protections leverage Wurldtech's industrial security expertise and the industry's leading threat intelligence to secure critical infrastructure. To simplify security administration, the graphical user interface is designed for ease-of-use to efficiently manage security policy and protection profiles including breakthrough drag and drop virtual zoning for network segmentation without rewiring. This solution is made complete by offering full security visibility of the industrial network and integration with SIEM tools.

Features/Benefits

Security	**Protects unpatched system with strong perimeter and field defense** **Inspects and controls industrial protocol traffic with industry's leading threat intelligence**
Simplicity	**Introduces breakthrough drag and drop virtual zoning for segmentation without re-wiring** **Simplifies security administration with easy-to-use graphical interfaces – no CLI required**
Visibility	**Displays graphical network-wide industrial security view** **Monitors industrial protocols and delivers security alerts to the management console and 3rd party SIEM tools**

Security



Deep Packet Inspection support for a broad range of industrial protocols

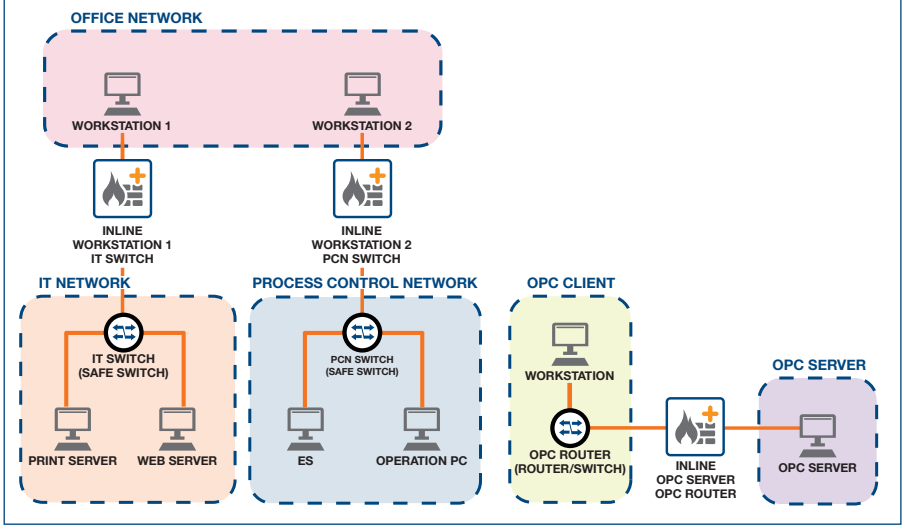
TESTIMONIAL

"We are very pleased to be working with Wurldtech to protect our critical systems around the world. They have unmatched expertise and experience in this domain and are a true solutions provider advocating a functional methodology and approach instead of a single product... Wurldtech's products and services are trusted and integrated throughout our global operations."

Ted Angevaare
Global DACA Manager

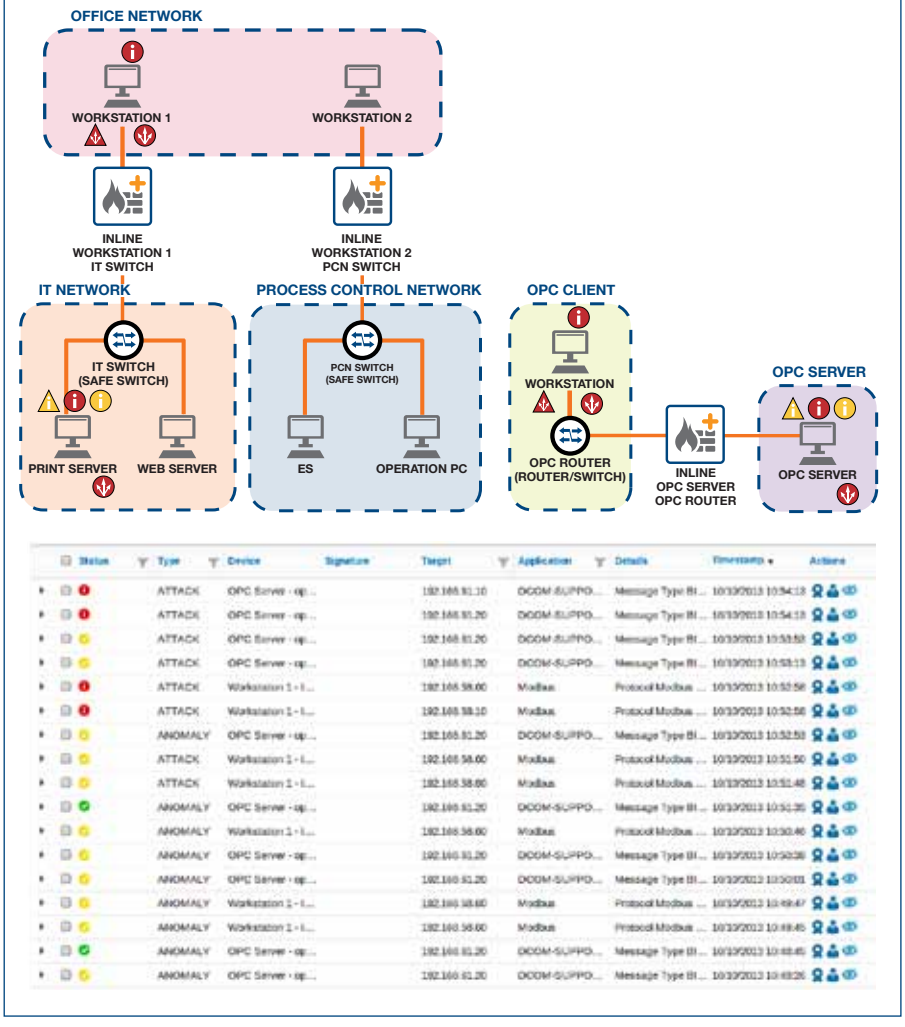
Shell

Simplicity



Easy drag and drop network segmentation and zoning

Visibility



Graphical network-wide industrial security view

Defining an Industrial Next Gen Firewall

Firewall offers stateful inspection to track the state of network connections and information to ensure that sent and received packets are expected and allowed. Only legitimate traffic is allowed through the network. In addition, the firewall maintains the network zoning and segmentation to control traffic flows.

Intrusion Prevention System/Intrusion Detetection System (IPS/IDS) accurately detects and prevents cyber attacks to the industrial network. By leveraging Wurldtech's OT and IT signature set, the Achilles Industrial Next Gen Firewall offers specific and customized, industrial protection for ICS/SCADA systems and industrial networks. The deep packet inspection engine is built from the ground up to work effectively with the growing list of industrial protocols. In addition, the architecture is built to easily support new and proprietary protocols.

Application Visibility & Control (AVC) identifies applications on the industrial network and enforces application allow/deny rules. Even finer details can be included. For example, Achilles Next Gen Firewall can detect whether commands are coming directly from the local management console (and if not, then it can ignore the command, which is a potential attack). Also, control can be programmed with a specific set point and if a command is sent for a point outside of the appropriate range, then again, the firewall can stop the potential attack. AVC offers System Operators protection and visibility into the network traffic and applications used across the connected production systems.

Centralized Management delivers the single graphical interface to build and deploy security policy and protection profiles. It also offers a network-wide view of alerts and attacks on the industrial network.

NEXT STEPS

For more information or a product trial, please call Wurldtech sales toll free at 1 877 369 6674,
email: sales@wurldtech.com
or visit our website at
wurldtech.com