Operational Network Security Solution Brief

4 steps to address unique operational network security challenges

As the Internet of Things (IoT) promises powerful business outcomes from connected sensor-based solutions, the Operations Technology (OT) business challenge is that cyber attacks on operational environments threaten two key metrics: safety and productivity. Asset owners, system operators and system integrators need to protect against these threats to ensure operational safety and maximum uptime.

With production systems becoming more interconnected, the exposure to cyber incidents increases. Attacks and disruptions on critical infrastructure put reputation, production, people, and profits at risk.

This has left us with a new reality: if it's connected, it needs to be protected.

"But I already have IT security."

Operational security is different than Information security, just like your physical security is different than identity security. IT security protects information. OT security protects control of critical devices and equipment.

Traditional IT security vendors do not address OT-specific protocols, environments, or assets. Moreover, they don't have insight into the specific vulnerabilities found across device and software manufacturers' products.

Nor do they have Services personnel trained or qualified to safely go on site to perform security services. For example, securing OT networks requires deep packet inspection of MODBUS, DNNP3, and OPC protocols, to name a few. While common IT protocols like HTTP can sometimes be stopped by blocking a port, the same cannot always apply in OT, where protocols may be performing multiple functions (e.g. read, write, set points).

"But our existing firewalls already do this for us."

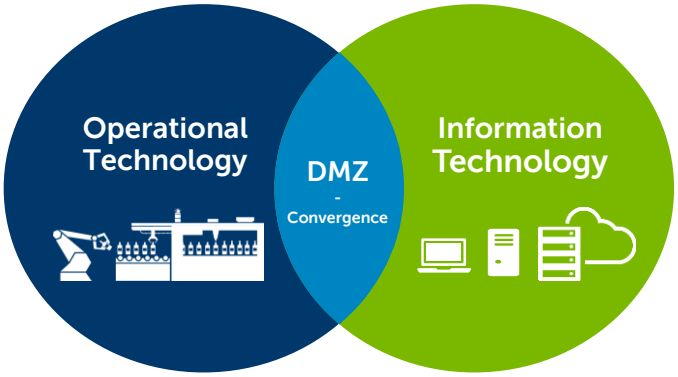
IT security is important and that activity should continue. OT-focused security solutions address critical network security needs in a broader IoT solution. OT-focused solutions are designed to see what firewalls can't: commands on a process control network.

Next-generation firewalls are designed to defend traditional IT traffic at the enterprise edge, but not in the OT environment itself. OT-focused solutions are different. They defend north/south (vertical) and east/west (lateral) traffic within the process control environment, all the way down to the application command and parameter level.

Although some firewalls can recognize OT protocols, they lack the command and parameter inspection capabilities required secure critical infrastructure.

1. Critical Infrastructure: Security Preparedness and Maturity (July 2014), Unisys and Ponemon
2. Verizon Data Breach Investigations Report 2015, Verizon

OT and IT Have Different Priorities for Cyber Security



		Operational Technology	Information Technology
Industrial Mindset	Security priorities:	AIC[1]	CIA[2]
	What's at risk:	Physical	Data
	Patching cycles:	Occasional to never	Frequent
Purpose-Built Technology	Strategy:	Protect process and safety	Protect data
	Protocols:	Often proprietary	Standardized
	Intelligence:	Vulnerability-based	Threat-based
Cyber Security Expertise	Cyber experience:	Industry-specific	IT-stack specific
	Certifications:	Domain-specific	IT-general

Key attributes of an OT-focused security solution

1 Availability, Integrity, Confidentiality
2 Confidentiality, Integrity, Availability

Your Industrial Internet security solution should include the following key precautions for your OT environment, in addition to your IT security protocols.

- Protocol inspection and whitelisting.
- Deep control over application layer communications, allowing the user to whitelist only the required functions and parameters for a given critical system.
- Flexible, deep-packet inspection (DPI) and signature-based protection for vulnerabilities. The deep packet inspection (DPI) engine was designed from the ground up for accuracy and flexibility. In OT, a deep protocol inspection engine is critical because unless you can see and validate each OT command and parameter in the intended context, there is simply too much risk for error or misuse.
- Reach into the protocol syntax and grammatical structure to parse and inspect the commands in the context of the impact they will have on the protected device.

When choosing an OT security solution, look for DPI engines that are purpose-built for OT to yield high accuracy and avoid false positives and blocks on evasion attempts, as compared to simpler, pattern-based engines. Also prioritize high flexibility to allow exploits to be detected even in niche or vendor-specific OT protocols. An optimized protocol inspection engine can parse and inspect OT network protocol packets and data flows, resulting in more control and confidence for operational availability.

4 steps to better OT network resilience

1 | Select an advanced OT-focused ICS vulnerability protection suite

Select a security vendor that offers an extensive set of ICS-specific vulnerability signatures, designed to thwart exploits and exploit variants. These should be more powerful than traditional IT threat signatures. The proper OT-focused security solution should be able to defend against unknown threats--including zero-day attacks--that exploit a root vulnerability.

2 | Establish baseline network communications

Observe and record all OT network communications to establish traffic patterns to determine "what's normal." This becomes the baseline for OT network communications whitelisting, the strongest form of cyber security policy creation. Having a baseline allows system operators to make informed decisions about communications integrity across their controls networks.

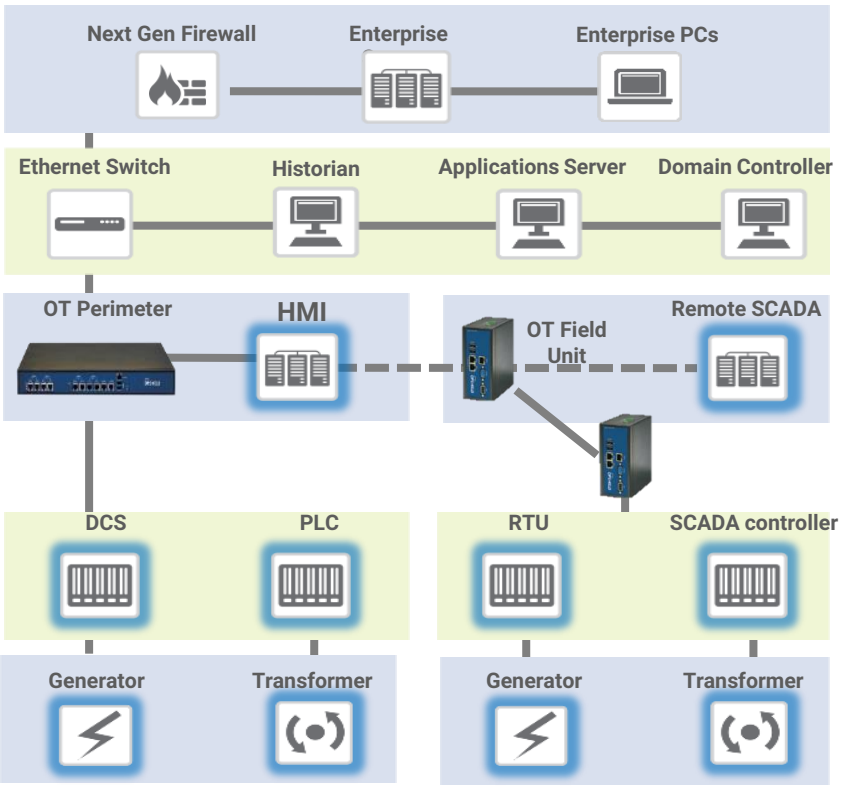
3 | Conduct network communications whitelisting

Building on the baseline, leverage OT network communications whitelisting to enable operators to block, allow or simply alert on all traffic that isn't match an established policy. Operators gain more control and reduce complexity associated with unnecessary traffic. This approach prevents attackers from misusing protocol commands, such as "shutdown," "scan," or "factory reset," as well as parameters such as "set point."

4 | Segment the OT network

The OT-security solution should utilize a drag-and-drop interface that allows an operator to quickly segment an OT network, without the need to reconfigure or reengineer. Zone-specific whitelist policies also help minimize unexpected downtime by preventing lateral movement of ICS infections.

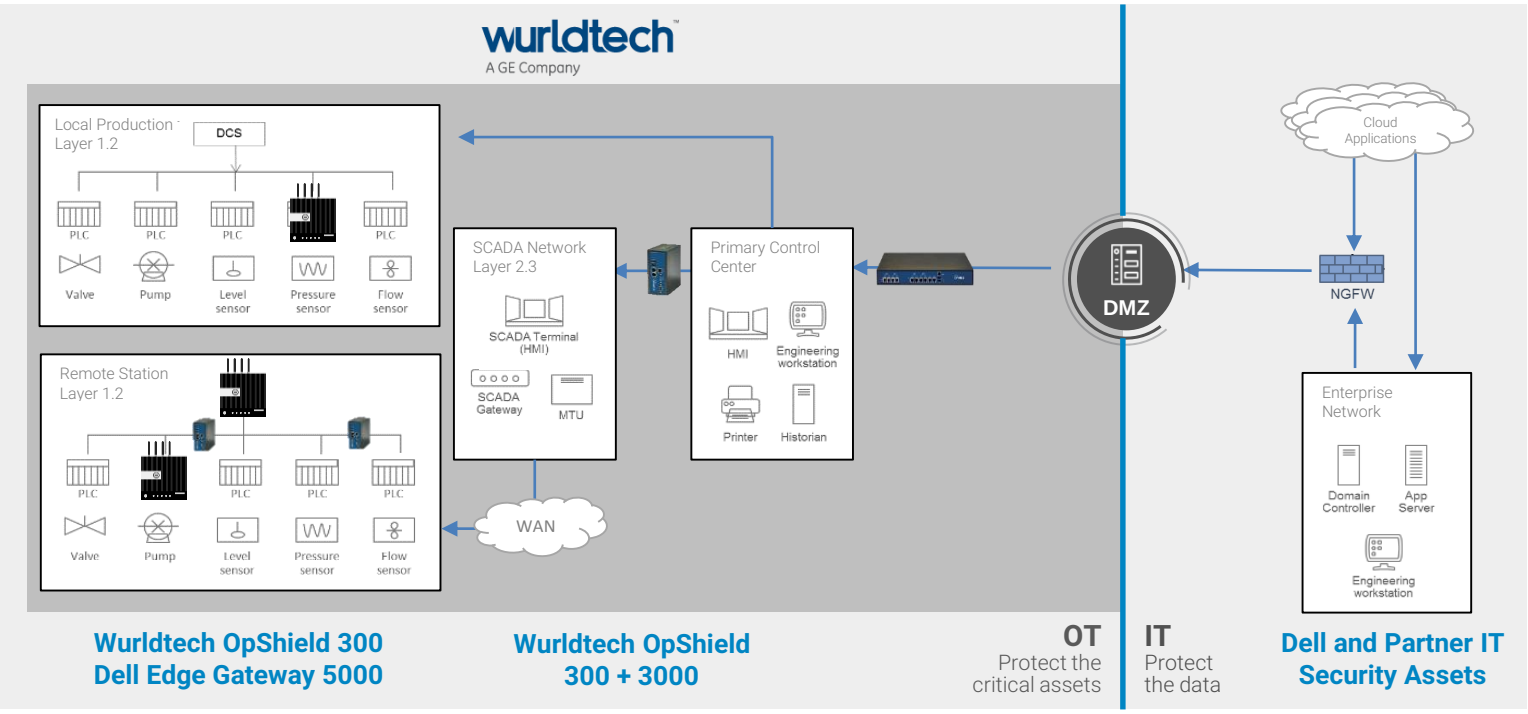
This methodology is unlike traditional VLANs or other segmentation techniques.



Solution Example: Leveraging Wurldtech OpShield for OT Security together with Dell Edge Gateways

This Industrial IoT Security Solution Brief represents a single solution provided by the industry leading partner below as a reference. Your specific security needs may involve a combination of this and other technology providers within our IoT Partner ecosystem.

To provide a baseline for you to build scalable IoT solutions while protecting your people, processes and equipment on the plant floor, Dell has developed a flexible architecture centered around the Edge Gateway 5000 and Wurldtech OpShield IPS appliances. Dell believes OpShield from Wurldtech in an excellent choice to meet your overall OT network security needs. Wurldtech, a GE company, has performed over 200 security assessments specific to operational environments since 2006 and has services personnel with certifications specific to industrial environments. Through their extensive experience, they know about, and can help mitigate, many issues and concerns that are not made public. The Dell Edge Gateway 5000 enables you to collect, analyze, relay, and act on real-time data from machine I/O and sensors in a variety of use cases by leveraging your own software or any number of offerings from our partners. An edge gateway can be inserted upstream of a PLC to perform localized real-time analytics or be directly connected to sensors for data aggregation and normalization. Deploying Wurldtech's OpShield 300 appliances at various points immediately upstream of Dell Edge Gateways and your existing PLCs provides protection as close as possible to individual assets and production cells. The OpShield 3000 appliance offers more throughput and is designed to sit at the boundary of the OT-IT DMZ to monitor and protect entire operations networks. On the IT side of the DMZ, Dell and its partners have a broad portfolio of assets and expertise to satisfy IT security needs as well as connecting to enterprise and cloud applications through a next generation firewall (NGFW). This distributed architecture provides maximum flexibility for you to tap into data from your existing capital assets along with net new sensors for increased visibility into your operations through analytics, all while protecting your overall network and preserving valuable production time.



Along with our IoT Solutions Partners, we provide technology you can trust to help you get started quickly and efficiently.

Dell takes a pragmatic approach to the Internet of Things (IoT) by building on the equipment and data you already have, and leveraging your current technology investments, to quickly and securely enable analytics-driven action.

The Dell IoT Solutions Partner Program is a multi-tiered partner ecosystem of technology providers and domain experts to complement Dell's broad portfolio of IoT-enabling technologies.

To learn more visit us online at: www.delliotpartners.com

Contact Dell Sales to learn more about the Dell Edge Gateway 5000, our ecosystem of qualified partners, and to deploy this flexible IoT security solution today.

IoT Solutions
Partner Program

Dell IoT Solutions
One Dell Way
Round Rock, TX 78664
www.dell.com/iot
1-800-438-9973