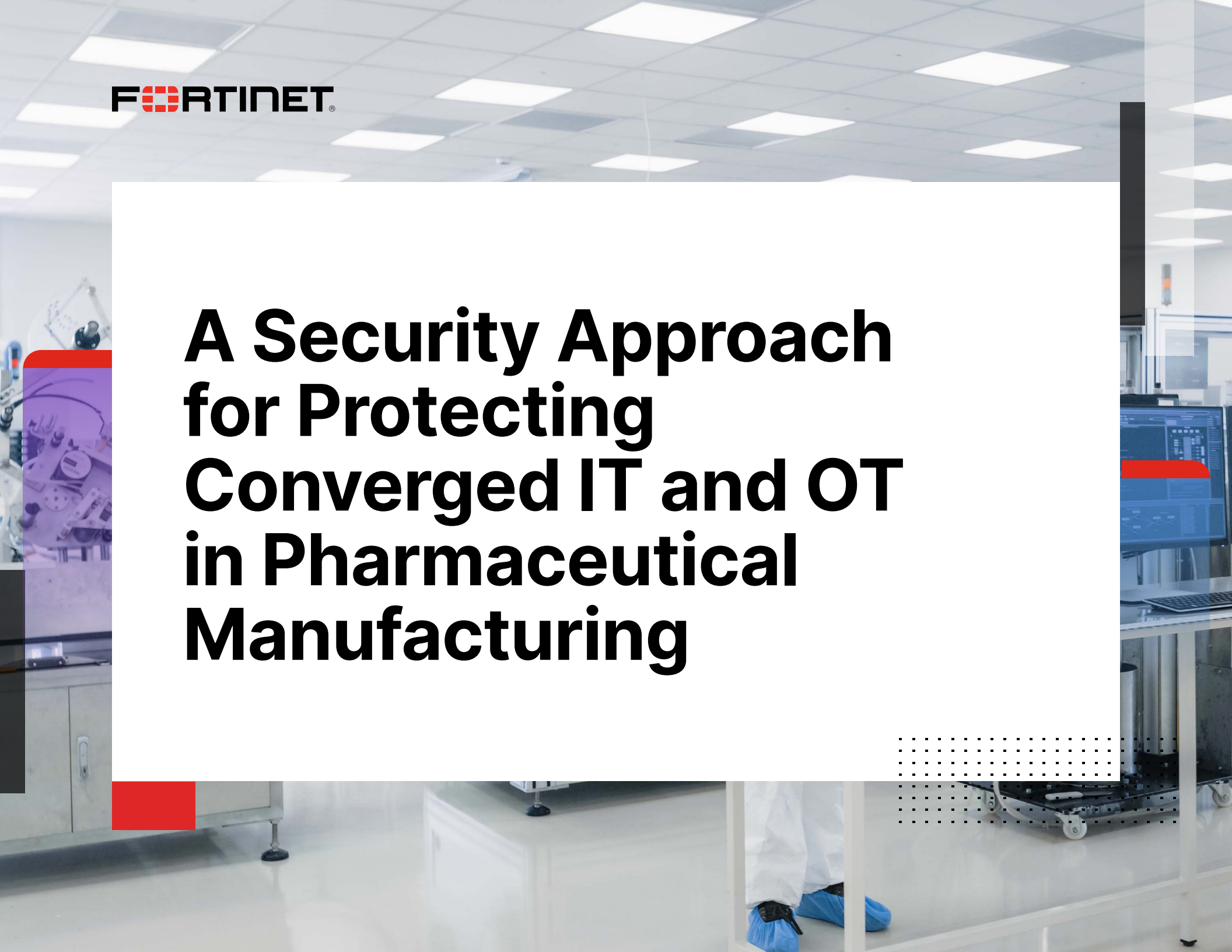

# A Security Approach for Protecting Converged IT and OT in Pharmaceutical Manufacturing

# Table of Contents

# Executive Summary

Operational technology (OT) networks, which control equipment in critical infrastructure such as manufacturing assembly lines and transportation, and distribution and logistics have traditionally been kept separate from information technology (IT) networks, which control data in all organizations. In recent years, pharmaceutical manufacturing has benefited from a number of compelling innovations in IT such as artificial intelligence (AI) and big data analytics, which promise to bring improved outcomes to OT networks as well. As a result, the integration of OT and IT networks is accelerating, supply chain and process management are becoming increasingly digitized, and this expands the digital attack surface, exposing OT networks to attacks coming from IT networks.

OT breaches are now commonplace in pharmaceutical manufacturing, and the repercussions are serious. Attacks can, for example, cause production shutdown, disrupt supply chains, or focus on systems that are critical to industrial safety processes. To thwart attacks and minimize OT risk, implement five best practices:

1. Increase network visibility
2. Segment networks
3. Analyze traffic for threats
4. Enforce identity and access management
5. Secure both wired and wireless access

These practices are presented as a foundation for enhancing OT security posture for pharmaceutical manufacturers.

## Why IT and OT Are Converging

Accelerated by the events of the COVID-19 pandemic, pharmaceutical manufacturing is embracing new levels of digitalization, automation, and innovation. For example, machine learning (ML) for preliminary drug discovery and augmented reality (AR) for remote technical advice and aid procedures, to the Internet of Things (IoT)-enabled supply chain management and predictive equipment maintenance. These new developments in IT are remaking processes and improving outcomes for pharmaceutical organizations around the world, and this is typically referred to as digital transformation (DX).

In OT networks, which control critical infrastructures such as pipelines, electric grids, transportation systems, and manufacturing plants, change is coming more slowly.

Pharmaceutical manufacturing OT environments are vital to public health and global economic well-being. They were developed decades before IT networks and have different vendors and proprietary protocols. There was little reason to connect OT and IT networks at first, especially because doing so increases the risk of cyberattacks.

The challenge when integrating IT and OT is that the bigger digital attack surface increases the risk of cyberattacks.

# Recommended OT Cybersecurity Best Practices

So, how can risks be minimized while enabling gains to be maximized? The following are five areas pharmaceutical manufacturing OT leaders need to have checked in order to protect against malicious cyberattacks.

## 1. Identify assets, classify, and prioritize value

Improving security posture starts with visibility: You cannot protect what you cannot see. Lack of visibility is a critical security gap at many organizations. Security teams need an up-to-date inventory of devices and applications running on the network. One challenge is that many OT networks cannot be actively scanned with the methods used for an IT network.

Security teams should consider contacting a vendor or technology partner to conduct a threat assessment. This assessment sometimes uses a system such as a next-generation firewall (NGFW) that can recognize OT application protocols and passively observe network traffic, including encrypted traffic. The system uses the information it collects to profile and categorize devices on your network based on their characteristics and behavior.

The result is a report that:

- Provides an inventory of connected devices
- Notes high-risk applications
- Detects and identifies top exploits of application vulnerabilities
- Assesses the risk value of each asset
- Identifies indications of malware, botnets, and devices that may be compromised
- Categorizes applications and analyzes their network usage

This information serves as a good foundation for prioritizing risks and optimizing a security plan.

## 2. Segment the network

Network segmentation is one of the most effective architectural concepts for protecting OT environments. The idea is to divide the network into a series of functional segments or "zones" (which may include subzones, or microsegments), and make each zone accessible only by authorized devices, applications, and users. A firewall defines and enforces the zones, and it also defines conduits, which are channels that enable essential data and applications to cross from one zone to another.

The architectural model of zones and conduits greatly reduces the risk of intrusion. It restricts an attacker's ability to move in an east-west or lateral direction. Users or devices authorized for a specific activity in a specific zone are limited to functioning properly within that zone. Segmentation is a fundamental best practice for securing OT. Each zone is assigned a security level from 0 to 4, with 0 representing the lowest level of security and 4 the highest. Strict access controls limit access to each zone and conduit based on the authenticated identity of the user or device.

Security teams should consider a firewall with purpose-built security processors, designed to accelerate specific parts of the packet processing and content scanning functions, compared to the general central processing units (CPUs) found in many firewalls. Purpose-built security processors enable high-speed cryptography and content inspection services without degrading network performance. This is important in keeping zones and conduits from becoming bottlenecks.

## 3. Analyze traffic for threats and vulnerabilities

Once NGFWs divide an OT network into segments and conduits, it is valuable to analyze network traffic for known and unknown threats. Security teams should seek to integrate an NGFW capable of inspecting encrypted application traffic. Additionally, the NGFW should be integrated with a live-feed service to provide updates on the most common OT protocols and OT application vulnerabilities. A service of this type enables the NGFW to inspect OT application traffic and spot exploits. Real-time global intelligence alerts update the firewall so it can identify even new and sophisticated threats. When integrated with a compatible endpoint security solution, the NGFW can monitor endpoints for indicators of compromise (IOCs) gleaned from a variety of sources around the globe.

The firewall can also learn from traffic on a network and establish a baseline or understanding of what is normal or abnormal across IT and OT systems. It can quarantine, block, or send alerts when it detects abnormal activity or IOCs. Integrated as part of the NGFWs, AI capabilities, which are delivered as part of a self-evolving threat intelligence system, develop signatures to catch zero-day threats before they are even written.

To make threat hunting and compliance reporting easier, security teams should add a security information and event manager (SIEM) that can correlate data from point security solutions and device logs across IT and OT networks.

The optimal approach is integrating a SIEM that can map a real-time topology of the network and track and record security events. Such an approach yields correlation of information from different solutions to deliver context, minimize response time, and simplify reporting.

## 4. Control identity and access management

Stolen credentials are an element of many OT cyberattacks. Spear phishing used to steal credentials is a key part of such attacks. A first layer of defense in controlling identity and access management (IAM) exploits should be a secure email gateway with signature- and reputation-based prevention.

Security teams should seek an IAM solution that:

- Enforces role-based access for each user, limiting access through integration with the firewall to only appropriate resources and network microsegment
- Validates identity with zero-trust and multi-factor authentication, combining something the user knows (such as username and password) with something the user has (such as a phone, laptop certificate, or physical security key) or something the user is (such as a fingerprint or other biometric)
- Enables single sign-on (SSO), saving time by enforcing enterprise user identity-based security without requiring additional sign-on screens
- Authenticates devices attached to the network by observing their characteristics and behavior, and where appropriate, noting the need for software updates to patch vulnerabilities
- Restricts access to only authenticated devices, locking down all other ports

## 5. Secure both wired and wireless access

In an OT environment, two attractive targets for cyberattacks are network switches and wireless access points (APs). Both should have security by design, administered from one central interface, instead of being protected by add-on point security solutions, managed through multiple interfaces. Security management that is centralized not only reduces risk but also improves visibility and minimizes administration time for security and operations teams.

Another distinct feature to consider in firewalls, switches, and wireless APs is a ruggedized form factor, enabling deployment in the extreme conditions of field sites found in OT, such as the refrigeration of chemicals, or the temperature-regulated storage of medicines. They should support centrally created security policies at the far edges of the network, where threat actors are likely to attack because they expect less security. A failure of equipment at the network edge is not just an annoyance; it can mean costly critical downtime and time-sensitive deployment to resolve the equipment failure.

# Conclusion: Proactively Limit Risk in OT Networks

For pharmaceutical manufacturers to stay competitive and accelerate ahead of their peers, organizations need to connect OT environments to their IT networks. In most instances, IT and OT network convergence is planned and strategic to an organization. It is also possible that integration exists that was not planned or even known.

IT and OT integration is a strategic initiative that is reshaping the pharmaceutical manufacturing industry, enabling organizations to become more resilient, more flexible, and more efficient. However, while being able to unlock the potential of data in this way is driving business excellence, it is also increasing the likelihood of OT breaches. While breaches cannot be stopped 100% of the time, they can be limited through network segmentation, detected faster through traffic analysis, and minimized in frequency through identity and access management, as well as wired and wireless access control. Following these best practices can greatly reduce the cost and potential downtime if an attacker is able to get a foothold in an OT network.

Enabling rapid progress with an adaptive, businesswide security fabric that delivers free data flow within complex pharmaceutical ecosystems means Fortinet is able to support the growth of pharmaceutical manufacturers, while delivering actionable security across IT and OT environments from a single platform to secure your digital journey as a modern life sciences organization.

FORTINET

www.fortinet.com



May 15, 2021 2:42 AM

eb-protecting-it-and-ot-in-pharma-manufacturing-V1-5142021

1033701-0-0-EN