

SOLUTION BRIEF

Integrated, Broad Protection for Pharmaceutical Industrial Control Systems

Executive Summary

Pharmaceutical manufacturing leaders cannot risk operational technology (OT) systems failures due to a cyberattack, yet the attack surface is expanding rapidly. This requires pharmaceutical manufacturers to deploy a set of end-to-end security solutions, targeting specific areas of vulnerability in an automated and integrated way, helping to support growth and secure the digital journey in the widening ecosystem of connected medicine.

The Fortinet Security Fabric is designed to provide exactly this type of integration, tying together leading solutions ranging from next-generation firewalls (NGFWs) to endpoint protection solutions, access control technologies to sandboxing and threat intelligence. In combination, these solutions provide enhanced visibility into network threats. More importantly, their automated responses to threats are well-orchestrated, minimizing the risk that an attack will succeed.

Cybersecurity Failure Is Not an Option for OT

Pharmaceutical manufacturing and industrial process businesses simply cannot afford to fall victim to a cyberattack. A successful attack that shuts down a production line can damage both the bottom line, and in the case of a delayed product launch, brand reputation as well. This is a large and growing concern for pharmaceutical manufacturing leaders because the risk of cyberattacks is growing rapidly as the OT attack surface continues to expand.

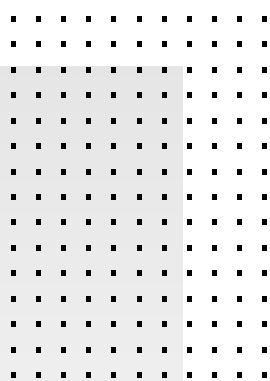
The proliferation of potential attack vectors is partly a result of the elimination of the “air gap” that traditionally existed between IT and OT systems; many businesses are linking industrial control systems (ICS) and supervisory control and data acquisition (SCADA) devices to network IT resources.

Fortinet offers an end-to-end yet incremental architectural approach to network security that addresses these new realities. The Fortinet Security Fabric provides broad and integrated coverage across both IT and OT infrastructures, delivering free, secure data flow within complex pharmaceutical ecosystems.

Security Fabric: Broad Visibility and Centralized Control

In the Fortinet Security Fabric, solutions across a wide spectrum of security capabilities share information in real time about threats they detect and coordinated response to those threats. This tight integration dramatically reduces the likelihood that a threat that is thwarted in one area of the network will have success at another network access point.

A key element in the Security Fabric is the FortiGate NGFW. In addition to their advanced security capabilities, FortiGate NGFWs come with management capabilities that are simple to use and provide visibility through a centralized console, whether the firewalls are deployed at the network edge, in the data center, or between segments of the internal network—such as between IT and OT segments.



A successful attack that shuts down a production line can damage both the bottom line, and in the case of a delayed product launch, brand reputation as well.

FortiGate NGFWs are easy to deploy, with centralized configuration that enables zero-touch deployment. FortiManager provides centralized and automated provisioning and management of up to 100,000 devices—including NGFWs, switches, and access points—facilitating faster configuration of device settings using provisioning templates, reducing the chance of human error, and streamlining security policy management.

Plant operations and manufacturing leaders who want to take a deeper dive into the organization's threat landscape can leverage FortiAnalyzer, which applies advanced analytics to data logs from both IT and OT solutions within the Security Fabric. Its comprehensive visibility of threats across the continuously expanding attack surface gives plant operations and manufacturing leaders confidence in the security of their devices, data, and applications. In addition, FortiAnalyzer provides vital network statistics, real-time monitoring of the threat landscape, and integrated reporting.

Another management tool that boosts the protections of the Security Fabric is FortiSIEM, Fortinet's multivendor security information and event management (SIEM) solution. FortiSIEM takes analytics that has traditionally been monitored in separate silos and brings the data together for a holistic view of security. Moreover, it offers machine learning (ML)-enabled user and entity behavior analytics (UEBA) to alert security staff when activities on the network raise suspicion.

Zero-Trust Access Across OT and IT Systems

A key component in thwarting attacks is preventing intruders from accessing the network in the first place. FortiAP access points and FortiSwitch switches, used in conjunction with FortiGate NGFWs, extend security controls down to where hosts first access the network. The ability to control network traffic by extending zero-trust architecture down to the end device reduces the avenues in which intruders can enter the network. FortiSwitch and FortiAP are available in ruggedized form factors that makes them suitable for deployment in the extreme conditions of OT field sites, manufacturing, and pharmaceutical production facilities.

FortiNAC is the Fortinet network access control (NAC) solution; it enhances the Security Fabric by providing visibility, control, and automated response for all devices that connect to the network. At the same time, plant operations and manufacturing organizations can use FortiAuthenticator to control which users and applications have access to applications and resources on the network.

By transparently identifying the appropriate level of access for every user attempting to connect to the network, FortiAuthenticator—in concert with FortiNAC and FortiToken—enables a company to employ a zero-trust network access policy. Instituting a zero-trust policy means users are permitted to access only those resources they need, which significantly lowers the risk of inappropriate lateral movement should an attacker gain access to the network.

Our next-generation endpoint protection solution, FortiEDR, provides endpoint detection and response (EDR) capabilities that secure endpoints companywide. FortiEDR responds to suspicious incidents through automated, policy-based actions that may quarantine a compromised endpoint, for example. The solution also automates protection against advanced threats, pre- and post-execution, with real-time incident response functionality.

When combined with an intent-based approach to network segmentation—which can limit traffic between IT and OT network segments to only those users and applications that require such access—FortiEDR can contain incidents and prevent outbreaks from spreading across IT and OT systems.

Proactive Advanced Threat Detection and Prevention

Automation options in the Fortinet Security Fabric mean solutions do not require human intervention before responding to every detected threat. FortiSOAR, a standalone security orchestration, automation, and response (SOAR) solution, integrates natively with the Fortinet Security Fabric and includes connectors to hundreds of security solutions from both Fortinet and third-party providers.

One key component in thwarting attacks is preventing intruders from accessing the network in the first place. This is another area in which Fortinet provides leading solutions for plant operations and manufacturing leaders.



Tight integration of endpoint and network security across both OT and IT networks streamlines management activities and accelerates response when a threat is detected. With our adaptive and businesswide Security Fabric, we can support requirements for an ecosystemwide approach to security, compliance, and continuous validation with a broad, integrated, and automated security platform. FortiSOAR also helps reduce alert fatigue, and its enterprise case management and easy-to-use playbooks support faster response to legitimate threats for security operations center (SOC) staff. Tight integration also helps ensure that automated response by solutions in the Fortinet Security Fabric to detected threats is coordinated, providing a better-orchestrated defense against attackers networkwide.

These benefits are further enhanced by the integration of leading-edge threat intelligence from FortiGuard Labs, one of the largest security research and analyst teams in the industry. FortiGuard threat intelligence utilizes data gathered from millions of Fortinet sensors deployed worldwide. Artificial intelligence (AI) and ML technologies automate the analysis of more than 100 billion security events every day. The FortiGuard Industrial Security Service specifically targets OT attackers, continuously searching for and updating signatures to identify threats to the common ICS/SCADA protocols. FortiGuard Industrial Security Service incorporates additional vulnerability protection provided by the major ICS manufacturers. This combination of human and automated intelligence provides the best available protection against zero-day threats.

When a FortiGate NGFW or other core Security Fabric solution detects a threat, the suspicious code is quarantined in FortiSandbox for testing before it is released to business-critical OT and IT resources. Organizations that rely on OT may also utilize FortiDeceptor to proactively root out problematic users or applications; acting as a honeypot, the solution lures, exposes, and then eliminates advanced attacks that get through the edge NGFWs. Both solutions are designed specifically to target threats to OT security. For example, FortiSandbox is designed to run open files specific to OT operating systems, such as a Siemens programmable logic controller (PLC) or a Schneider remote terminal unit (RTU).

Customer Care That Meets the Needs of Pharmaceutical Organizations

Highly available technical support is an essential component of any security solution deployed in OT environments. A gap in security caused by delayed customer support could lead to downtime of a production line, which might equate to millions of dollars in lost revenue, as well as damage to customer service and brand reputation. And it is vital to support and meet compliance for the likes of GDPR, NIST, FDA, OECD, and more, with continuous validation to ensure operations meet auditor requirements. This means tangible scores against relevant standards and against peer organizations, and actionable information about how to prioritize and resolve compliance issues.

FortiCare Support Services provide 24×7 support for ICS environments. One service option delivers replacement hardware to pharmaceutical manufacturing sites within four hours, along with an engineer to install the device, update firmware, and provide other services as necessary.

The FortiCare 360 Protection Bundle adds to this package by providing operational services via cloud-based, real-time management and analytics. The 360 Protection Bundle gives pharmaceutical manufacturing leaders a comprehensive toolset, without adding security staff.

An additional option for organizations utilizing the Fortinet Security Fabric is a customized engagement from expert engineers on the Fortinet Professional Services team. A resident engineer can provide security solution design, transition assistance, and operational services for Fortinet solutions, for faster time to value of Security Fabric components.

When a FortiGate NGFW or other core Security Fabric solution detects a threat, the suspicious code is quarantined in FortiSandbox for testing before it is released to business-critical OT and IT resources.



Conclusion

As possible security vulnerabilities mount at pharmaceutical manufacturing businesses, Fortinet solutions protect both OT and IT networks. This provides pharmaceutical manufacturers with cross-vendor interoperability and visibility, with wider control and monitoring of data—crucial in this age of connected medicine and the expanding attack surface and sophistication of threats this unlocks.

Fortinet solutions are also specifically designed to support OT environments—from the rugged form factor on FortiGate NGFWs, FortiAP, and FortiSwitch to the ability of FortiSandbox to open files specific to OT operating systems. FortiGuard Labs OT-focused Industrial Security Service likewise boosts protections for ICS/SCADA devices. The Fortinet Security Fabric offers additional integrations for third-party security.

Pharmaceutical manufacturing leaders need a comprehensive strategy for blocking known and unknown threats, as well as for responding appropriately when security solutions detect an attack that has successfully breached the network perimeter. Those who cannot afford downtime of their OT systems should consider the breadth of functionality and OT-specific capabilities that Fortinet solutions bring to market—with the Security Fabric to overcome the challenges of maintaining data integrity and visibility, increasing operational efficiency, cost control, and compliance reporting across even the most complex pharmaceutical infrastructures. With a single platform for consistent, complete risk mitigation and total assurance, as well as visibility of the entire security ecosystem, Fortinet supports the growth and security of the digital journey.



www.fortinet.com

Copyright © 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.