

WHITE PAPER

Fortinet Cybersecurity Solutions for Pharmaceutical Manufacturing

Protecting IT and OT Resources Against Advanced Threats in Pharmaceutical Manufacturing with a Single Platform



Executive Summary

The growing need for competitive advantage and greater efficiency to reduce costs and improve time to market means pharmaceutical manufacturing organizations have had to rapidly digitize. Organizations need to meet the demand for accelerated research and production, introducing and managing an increasing amount of expensive and sophisticated equipment and technologies at their factories. Inevitably, as these organizations have digitally transformed, more and more systems and processes have become connected to the internet. The cybersecurity implications to the pharmaceutical manufacturing industry are significant, ranging from IP theft and supply chain disruption through to possible threats to physical safety, and in some cases, national security. Companies strive to secure their systems while maintaining business imperatives like operational efficiency, continuity of operations, product integrity, and compliance. The Fortinet Security Fabric provides a broad, integrated, and automated security architecture that covers all aspects of the manufacturing business—from the back office to the manufacturing floor, from air-gapped systems to connected ones, from internal users to third-party partners.

The story of today's manufacturing sector is a story of convergence. Pharmaceutical companies that previously produced products independently now work closely with a network of partners who perform different parts of the process. And the electronic systems that run factory operations, which were historically air-gapped, are increasingly being connected with IT systems—and therefore with the internet. As a result, these operational technology (OT) systems, including industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems, are exposed to an increasingly advanced threat landscape and are targets for hackers involved in terrorism, cyber warfare, and espionage.

As air gaps are removed around the world, OT systems are increasingly barraged with both recycled IT-based attacks and purpose-built OT exploits. Attacks on the pharmaceutical manufacturing sector's critical infrastructure can result in financial loss, compromised trials, contaminated drugs, delivery delays (a particular concern in a time where the mass rollout of vaccines is so important), a risk to brand reputation, and sometimes even loss of life or threats to national security.

Fortinet has protected OT environments in critical infrastructure sectors such as pharma, energy, defense, manufacturing, food, and transportation since 2005. By designing cybersecurity into these complex infrastructures via the Fortinet Security Fabric, organizations can integrate cybersecurity protection across OT and IT environments, from the lab to the manufacturing facility to the data center to multiple clouds.

Key Manufacturing Cybersecurity Challenges

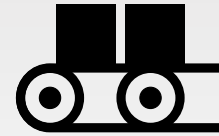
Plant, worker, and community safety

Manufacturing facilities contain machinery that can cause physical injury or death if it malfunctions or is not operated correctly. In the current threat landscape, adversaries aiming to disrupt operations with a cyber-physical attack can create safety risks for on-site employees and even nearby residents and passers-by. In addition, attacks can affect the safety of products produced at a factory, extending the risk over a wide geography.

At most pharmaceutical manufacturing organizations, siloed systems for IT, OT, and physical security is the default—and this does not help matters. Integrating just the IT security architecture between the data center, multiple clouds, and the edge is hard enough. But in an age when adversaries can coordinate cyber and physical attacks simultaneously, integrating all elements of security with centralized visibility may be the only viable way to protect human life.

Productivity and uptime

Any unplanned interruption in operations can incur significant costs to a pharmaceutical manufacturer, and the outage can create problems that cascade down distribution channels and up the supply chain. Unfortunately, many cyberattacks on manufacturers aim to cause just such a disruption. Others seek to move laterally within the network once they get in, but the attack can still have an impact on operations.



Any unplanned interruption in operations can incur significant costs to a pharmaceutical manufacturer, and the outage can create problems that cascade down distribution channels and up the supply chain.

Because they were historically air-gapped and system updates are less frequent, OT systems often have less sophisticated cybersecurity protection than IT systems. As a result, they are frequently targeted by cybercriminals on the premise that they are relatively easy to infiltrate. Even air-gapped OT systems can be infiltrated by infecting manufacturers' software updates before they are installed.

Operational efficiency

Siloed security operations resulting from a lack of integration between different security tools inevitably increase operational inefficiencies. Without integration, manual tasks such as correlating log reports from different systems and assembling compliance reports waste the time of highly paid cybersecurity professionals and distract from more strategic work.

Architectural silos also create redundancies in the management of applications. A plethora of point products requires a bigger set of specific product skills to be represented on an overworked cybersecurity team. They can also result in higher software and hardware licensing costs—and the staff time to administer the multiple licenses. These factors can significantly increase overall operational expenses.

Customer experience

Pharmaceutical manufacturers now routinely engage with customers in a highly targeted way, using social media and other engagement tools alongside web presence. But these legitimate efforts can be countered by cybercriminals who manipulate social networks for profit, or spread dangerous misinformation about medicines. One study found that more than half of the world's social media accounts are fraudulent.*

Securing web properties and social media interactions is paramount for manufacturers, as the loss of data from potential customers in the early stages of the buying cycle, or sensitive personal data and medical records could be devastating to a company's reputation. Other factors such as website downtime, temporary unavailability of product due to production outages, and the like can negatively impact customer experience.

Product integrity

Degradation of product quality—even if temporary—can be disastrous for a brand's reputation. For example, if a cyberattack affects a drug manufacturing's OT system in such a way that temperature is slightly changed or altered, spoilage or degraded product quality can occur. In the case of drugs and other medicine, this has the potential for serious effects to customers' physical health and safety.

Compliance

In a heavily regulated industry like pharma, manufacturers are subject to a wide variety of guidelines and standards. Penalties for noncompliance are sometimes high, but an even higher cost often comes from diminished brand reputation in the event of a breach.

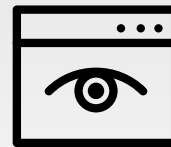
Organizations must be able to demonstrate compliance with multiple regulations and standards without redeploying staff, from strategic initiatives to preparing audit reports—which wastes valuable staff time and opens the possibility of human error in the reporting. Manual correlation of data for audit reports is almost always necessary with a disaggregated cybersecurity infrastructure.

Use Cases

Following are the key use cases Fortinet solutions enable manufacturers to solve:

Corporate infrastructure

While the factory floor is the center of production, manufacturing companies have similar corporate IT needs to organizations in other industries. This corporate IT network houses important data related to finance, intellectual property, HR, product support, field support, and more. As with other industries, manufacturers are increasingly reliant on cloud-based applications



Cybersecurity teams must have centralized visibility into all systems, the ability to segment the network according to business need, and centralized control of both wired and wireless networks.

and infrastructure, and Internet-of-Things (IoT) devices are growing in number at the network edge.

More recently, the massive surge in remote work is of particular concern to an industry susceptible to cyberattacks. The increased use of personal devices and collaboration tools, combined with the vulnerability of home networks compared to their corporate or R&D equivalents is of serious concern to pharmaceutical manufacturing organizations handling vast amounts of confidential information and valuable intellectual property.

Whatever sensitive data is housed there, the corporate infrastructure needs a broad, integrated, and automated cybersecurity solution with end-to-end integration. The Fortinet Security Fabric provides just such a solution, built on the foundation of FortiGate next-generation firewalls (NGFWs) and artificial intelligence (AI)-powered threat intelligence from FortiGuard Labs. A wide array of Fortinet cybersecurity tools integrates seamlessly into the Security Fabric, along with dozens of third-party solutions delivered by Fabric Partners. And an open ecosystem and extensive application programming interface (API) tools make the integration of other third-party tools possible.

Air-gapped manufacturing systems

While the majority of OT systems are now connected to IT systems, a number of OT systems are still air-gapped—that is, not connected to any other network. While one might assume that such systems are safe from cyberattacks, they still use IP-based control systems and administrators still install software updates provided by the manufacturer. This gives adversaries an opening to penetrate a system by infecting the updates through the vendor's network. And while air-gapped systems may not contain sensitive data, infiltrations can cause costly disruptions and safety issues.

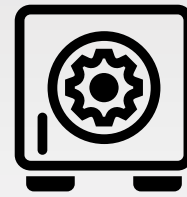
As a result, NGFW protection is required even for air-gapped systems, and this must be accompanied with comprehensive cybersecurity tracking and reporting. FortiGate NGFWs provide robust protection and industry-leading performance when inspecting both encrypted and unencrypted traffic. FortiManager provides single-pane-of-glass management and a variety of reporting tools. FortiAnalyzer delivers analytics-powered cybersecurity and log management for maximum visibility and better detection of breaches. The FortiSIEM cybersecurity information and event management tool enables a coordinated and automated response to attacks.

Connected manufacturing systems

Digital transformation and the need for business agility are creating increasing co-dependence between IT and OT. From industrial IoT sensors that monitor manufacturing operations to systems that pull publicly available data from the internet to facilitate decision-making, OT systems are less and less isolated. From a cybersecurity perspective, the main result of this convergence is a greatly expanded attack surface. And since OT systems often are not patched consistently, weakening cybersecurity protection, this presents risk to an organization in the short term.

But if cybersecurity issues can be resolved, the potential is great for combining IT and automation networks into a single, secure, manageable, and converged environment. Cybersecurity teams must have centralized visibility into all systems, the ability to segment the network according to business need, and centralized control of both wired and wireless networks.

The Fortinet Security Fabric covers the entire attack surface, giving broad visibility into who is on the network and what they are doing. It also provides integrated control over each system to ensure that it does what it is supposed to do. Additionally, the Security Fabric enables intelligent segmentation to provide greater control, and automated awareness of known and unknown threats. Built on the foundation of FortiGate NGFWs and AI-powered threat intelligence from FortiGuard Labs, the Security Fabric provides seamless integration with dozens of cybersecurity tools from Fortinet and its Fabric Partners.



Cybersecurity teams must have centralized visibility into all systems, the ability to segment the network according to business need, and centralized control of both wired and wireless networks.

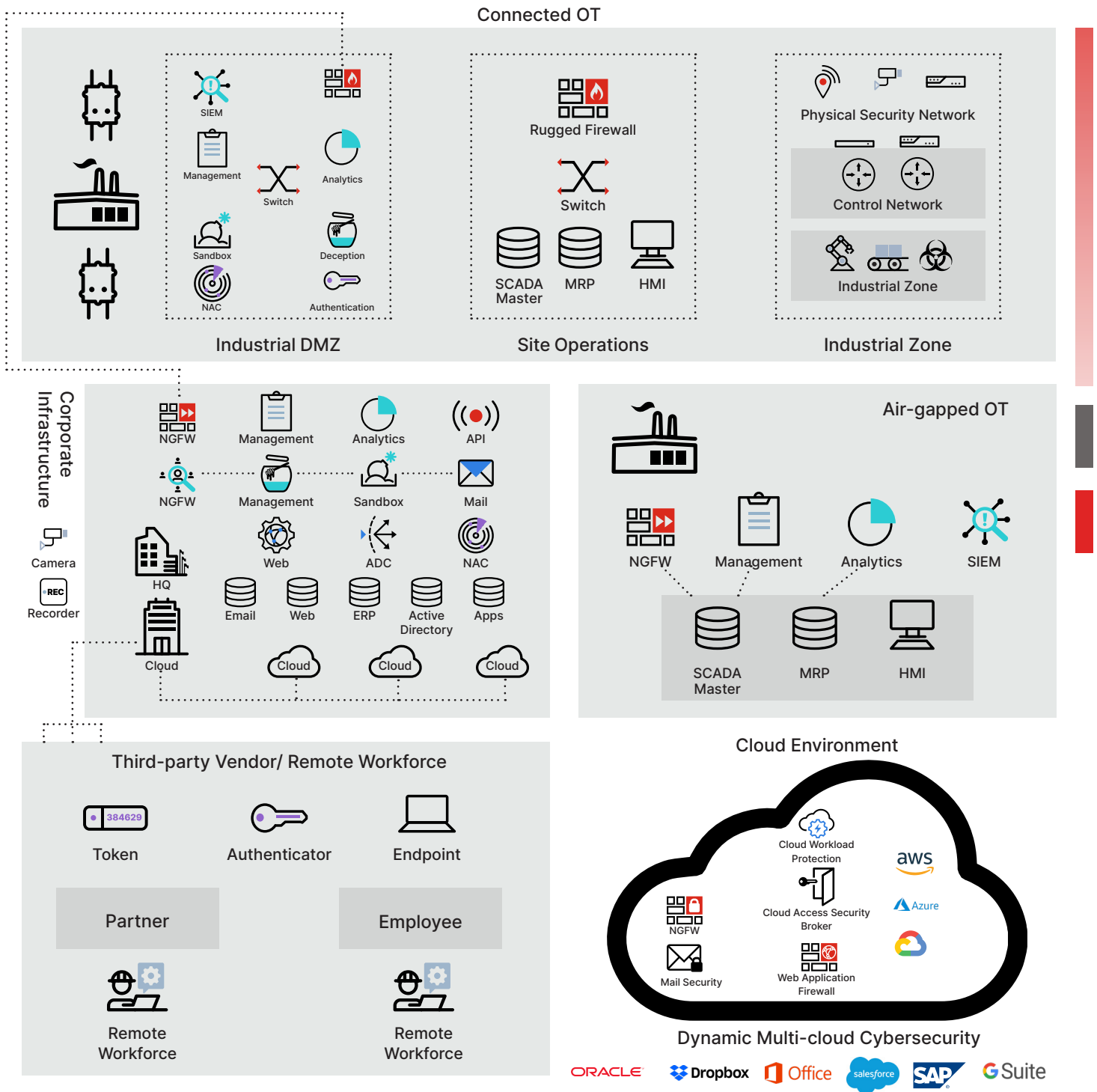


Figure 1: Fortinet manufacturing cybersecurity solutions enable companies to build an end-to-end, integrated security architecture spanning IT, OT, and physical security, extending from headquarters to the manufacturing plant while covering internal users and those from third-party partners.

Third-party vendor management

As the industry moves in the direction of a Manufacturing-as-a-Service (MaaS) model, third parties have more access than ever before to corporate networks and OT systems. This complicates the notion of the trusted user and forces organizations to continually assess their protection against insider threats—including from third parties. Keeping track of each partner's cybersecurity posture through regular vetting is critical. Organizations also need robust protection against insider threats, whether those threats are accidental or malicious, and whether they come from within the company or from an element of the partner network.



The integrated solutions of the Fortinet Security Fabric provide a multilayered defense against these threats. Intent-based segmentation capabilities in FortiGate NGFWs allow organizations to segment their network intelligently in a world of dynamic trust. The FortiAuthenticator identity and access management solution and FortiToken tokens leverage that segmentation in granting access to users on a need-to-know basis. FortiInsight uses user and entity behavior analytics (UEBA) to identify anomalies in the expected behavior of trusted users and entities that might indicate a compromised account. And FortiDeceptor uses deception technology to deceive, expose, and eliminate attacks originating from internal and external sources.

Multi-cloud cybersecurity

Many organizations now have cloud-based manufacturing resource planning (MRP) and enterprise resource planning (ERP) systems. These systems often pull data from both IT and OT systems for quick and effective decision-making, a process called “digital twinning.” Cloud-based solutions are also routinely used for services that impact customer experience. Protecting cybersecurity for these assets is critical, so an organization’s integrated cybersecurity architecture must extend from the data center to OT systems to multiple clouds.

The Fortinet Security Fabric enables comprehensive protection for the multi-cloud environment, ensuring consistent policy and configuration management, and threat detection and response across the entire attack surface. FortiGate VM brings the NGFW to a virtual machine that works well for cloud environments, and the FortiWeb web application firewall (WAF), which is available in several form factors, protects the application layer with in-line, AI-powered threat intelligence.

The FortiCASB cloud access security broker (CASB) service provides insights into resources, users, behaviors, and data stored in the cloud with comprehensive reporting tools. This enables advanced policy controls to be extended to Infrastructure-as-a-Service (IaaS) resources and Software-as-a-Service (SaaS) applications. The FortiCWP cloud workload protection (CWP) tool enables cybersecurity and DevOps teams to evaluate their cloud configuration cybersecurity postures and identify potential threats resulting from misconfigurations.

Fortinet Differentiators

Fortinet differentiators for manufacturing cybersecurity

Fortinet solutions offer manufacturers the ability to protect everything across their diverse OT and IT networks. Key differentiators include:

- **Security for modern and legacy equipment**

The Fortinet Security Fabric offers the ability to secure both modern and legacy equipment, even when the equipment runs on aging or end-of-life operating systems, without disrupting production processes.

- **Integration**

Fortinet technology provides manufacturers with an end-to-end, integrated cybersecurity architecture that covers IT and OT, cyber- and physical security, factory and headquarters, data center, and multiple clouds. This makes true security automation possible, and enables coordinated workflows from protection to detection to response.

- **Monitoring and management**

Fortinet enables manufacturers to consolidate networking, cybersecurity, and surveillance functions into a single system, with full visibility and control on a single pane of glass. This helps prevent cyber-physical attacks and breaks down silos between different teams.

- **Ruggedized hardware**

Hardware can often take a beating in a manufacturing setting, and physical damage to a firewall appliance can often result in a shutdown of factory operations. Fortinet offers a broad selection of ruggedized appliances to fit all environmental needs, and to support business continuity.



- **Proactive protection against insider threats**

Managing risk around insider threats gets more complex as more third-party suppliers and partners have access to the network. Fortinet offers a comprehensive solution to guard against insider threats, including intent-based segmentation, deceptor technology, and UEBA.

- **Continuity for R&D and manufacturing**

Fortinet can protect anyone, anywhere, regardless of device or network, through the visibility of data, and the control of credentials plus multi-factor authentication (MFA) alongside actionable intelligence. Next-generation endpoint security provides real-time automated endpoint protection, detection, and response. Fortinet's platform and firewall capacity enable safe throughput and processing of IP and publicly identifiable information.

- **Cross-vendor interoperability and visibility**

Where our firewalls and switches are deployed alongside those from other vendors, our integrations enable control and monitoring of data, in some cases integrating better with other vendors' products than they do with their own portfolio. We provide the network access control visibility and device recognition needed in pharmaceutical operational technology.

- **OT-specific threat intelligence**

FortiGuard Labs provides robust threat intelligence specific to OT systems, helping manufacturers make better strategic decisions. Fortinet has worked closely with manufacturing customers for 15 years.

- **Security Fabric ecosystem**

In addition to the broad portfolio of Fortinet security tools, specialized OT solutions can be integrated seamlessly with the Fortinet Security Fabric through the ecosystem of Fortinet Fabric Partners. This helps to streamline data into a single view for informed decision-making.

Conclusion

In a rapidly evolving marketplace that demands just-in-time production, manufacturers cannot afford to be slowed down by cybersecurity events—or by efforts to prevent them. The Fortinet Security Fabric provides a unified platform that can protect IT, OT, and physical security—enabling rapid progress with an adaptive, business-wide Security Fabric that delivers free data flow within complex pharmaceutical ecosystems. With broad visibility and integrated control from a single pane of glass, Fortinet can support your growth, and secure your journey.

* ["Q3 Fraud and Abuse Report,"](#) Arkose Labs, September 18, 2019.



www.fortinet.com

Copyright © 2021 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. 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.