FORTINET

SOLUTIONS OVERVIEW

Fortinet Manufacturing Cybersecurity Solutions

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

Executive Summary

Manufacturing organizations manage expensive and sophisticated equipment at their factories, and the systems running the machinery are increasingly connected to the internet. The cybersecurity implications of this trend are significant, including 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 covering all manufacturing business aspects. It covers everything from the back office to the manufacturing floor, from air-gapped systems to connected ones, and from internal users to third-party partners.

Exploits are increasing in volume and prevalence for almost every ICS/SCADA vendor.[1]

Today's market conditions have made adopting Industry 4.0 methodologies and technologies an "era of connectivity, advanced analytics, automation, and advanced-manufacturing technology" essential for manufacturers and organizations in other industries to remain competitive.[2] And the electronic systems that run factory operations, which were historically air gapped, are increasingly connected with IT systems and, therefore, 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.

Now that the infrastructures of IT and OT are almost universally integrated, the air gap that previously kept OT systems nearly invulnerable to cyberattacks is gone. The 2023 State of Operational Technology and Cybersecurity Report found that 32% of respondents indicated both IT and OT systems were impacted, an increase from 21% in 2022.[3]

Fortinet has protected OT environments in critical infrastructure sectors such as energy, defense, manufacturing, food, and transportation since 2005. Organizations can integrate cybersecurity protection across OT and IT environments by designing complex infrastructures using the Fortinet Security Fabric. With the Security Fabric, everything from the manufacturing floor to the data center to multiple clouds can be protected.

Key Manufacturing Cybersecurity Challenges

Manufacturers face a number of key cybersecurity challenges in their diverse OT and IT networks.

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. A successful cyber OT physical attack on connected ICS networks can disrupt or even deny critical services to society. In addition, attacks can affect the safety of products produced at a factory, extending the risk over a wide geography.

At most organizations, siloed systems for IT, OT, and physical security are the default, which 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 security elements 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 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 these types of disruptions. Other attackers seek to move laterally within the network once they get in, but the attack can still affect operations.

Because they were historically air gapped and system updates are less frequent, OT systems often have less sophisticated cybersecurity protection than IT systems. Because of their perceived vulnerability to infiltration, they often become prime targets for cybercriminals. Cybersecurity reports on industrial cybercrime often imply that these are fresh threats, but 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 among 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 them from more strategic work.

Architectural silos also create redundancies in the management of applications. A plethora of point products require already overworked cybersecurity teams to have a more comprehensive set of specific product skills. Having multiple products also leads to higher software and hardware licensing costs, along with the staff time to administer the multiple licenses. These factors can significantly increase overall operational expenses.

Impostors on social media present a real challenge for major brands, and the stakes are even higher for those who deal with personal or sensitive information.

Customer experience

Whether their products are for consumers or businesses, manufacturers routinely engage with customers in a highly targeted way, using social media and other engagement tools alongside their web presence. But these legitimate efforts can be countered by cybercriminals who manipulate social networks for profit. One study found that the major social media companies admit that a proportion of the profiles on their service are spam, fake, or duplicate, but the actual number of those accounts isn't clear.[4]

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 could devastate a company's reputation. Other factors, such as website downtime and temporary unavailability of products due to production outages, can have a negative impact on the customer experience.

Product integrity

Even a temporary degradation of product quality can be disastrous for a brand's reputation. For example, if a cyberattack affects a food processor's OT system in such a way that temperature is slightly changed or cooking time is slightly altered, spoilage or degraded product quality can occur. Depending on the product, this can also affect customers' physical health and safety.

Compliance

Depending on the goods they make, manufacturers are subject to a wide variety of regulations and standards. Penalties for noncompliance are sometimes high. In industries with historically poor reputations for data security and cybercrime, promoting a commitment to privacy and security can be a differentiating factor that appeals to customers and partners.

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

Use Cases

Manufacturers can solve the following use cases with Fortinet solutions.

Corporate infrastructure

Although the factory floor is the center of production, manufacturing companies have corporate IT needs similar to organizations in other industries. The corporate IT network houses important financial, intellectual property, human resources, product support, field support, and more data. Like various other sectors, manufacturers are becoming more dependent on cloud-based applications and infrastructure.

Additionally, the proliferation of Internet-of-Things (IoT) devices at the network edge is on the rise. No matter what sensitive data may be housed there, the corporate infrastructure needs a broad, integrated, and automated cybersecurity solution with end-to-end integration. The Fortinet Security Fabric is 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 solutions integrate seamlessly into the Security Fabric and dozens of third-party solutions delivered by Fabric Partners. The open ecosystem and extensive application programming interface (API) tools make the integration of other third-party tools possible.

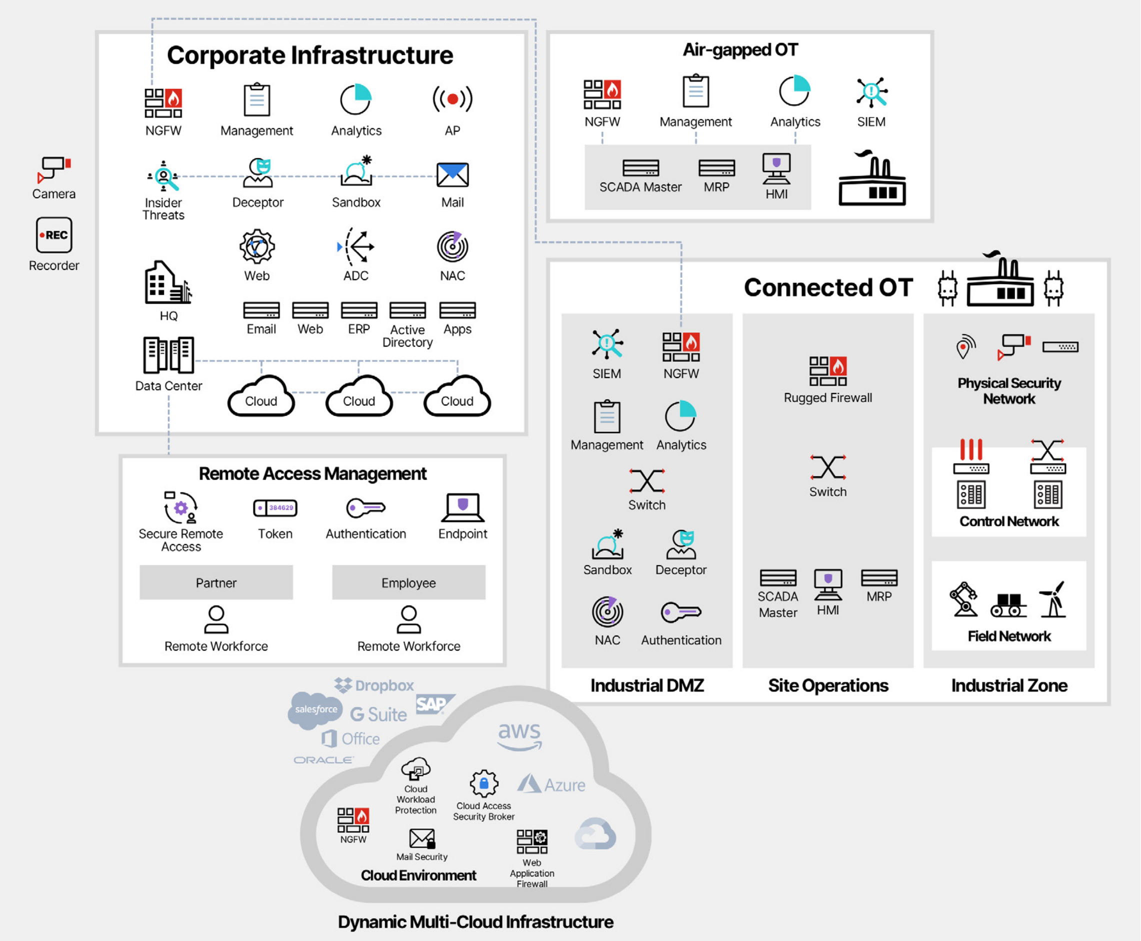
Air-gapped manufacturing systems

As industrial systems become more complex, interconnected, and interdependent, protecting the OT environment with a simple air gap is no longer feasible. Increased connectivity with IT systems, the cloud, third-party vendors, and 5G networks opens an entirely new set of risks to OT networks. Although it's easy to assume these systems are safe from cyberattacks, they still use IP-based control systems. Administrators also install software updates provided by the manufacturer, which gives adversaries an opening to penetrate a system by infecting the updates through the vendor's network. Even though air-gapped systems may not contain sensitive data, infiltrations can cause costly disruptions and safety issues.

NGFW protection is required even for air-gapped systems, and it must be accompanied by comprehensive cybersecurity tracking and reporting. Fortinet 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

The need for business agility and reporting creates increasing co-dependence between IT and OT networks. OT systems are less and less isolated, whether from industrial IoT sensors that monitor manufacturing operations or systems that pull publicly available data from the internet to facilitate decision-making. From a cybersecurity perspective, the main result of this IT/OT convergence is a greatly expanded attack surface. OT systems often are not patched consistently, which weakens cybersecurity protection and 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 needs, and centralized control of wired and wireless networks.



The Fortinet Security Fabric covers the entire attack surface and provides broad visibility into who is on the network and what they are doing. The integrated control it provides over each system helps ensure that the system 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.

Fortinet manufacturing cybersecurity solutions enable companies to build an end-to-end, integrated security architecture that spans IT, OT, and physical security from headquarters to the manufacturing plant while covering internal users and third-party partners.

The CEO and senior management teams all agree that strategies to accelerate time to market, enhance product quality, and listen to customers are yielding positive results.

Third-party vendor management

As industries transition toward adopting a Manufacturing-as-a-Service (MaaS) framework, third parties have more access to corporate networks and OT systems. This access can complicate the notion of the "trusted user." It forces organizations to continually assess their protection against insider threats, including third-party threats. Keeping track of each partner's cybersecurity posture through regular vetting is critical. Organizations need robust protection against insider threats, whether those threats are accidental or malicious and whether they come from within the company or from a member of the partner network.

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

Multi-cloud cybersecurity

Manufacturers are quickly embracing cloud-based services. Many 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 the customer experience. Protecting cybersecurity for these assets is critical. 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. It helps ensure consistent policy management, 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 threat intelligence powered by AI.

The FortiCASB cloud access security broker (CASB) service has comprehensive reporting tools to provide insights into resources, users, behaviors, and data stored in the cloud. FortiCASB enables advanced policy controls to be extended to Infrastructure-as-a-Service (IaaS) resources and Software-as-a-Service (SaaS) applications. FortiCNP cloud-native protection enables cybersecurity and DevOps teams to evaluate their cloud configuration cybersecurity posture and identify potential threats that result from misconfiguration.

Fortinet Differentiators for Manufacturing Cybersecurity

Manufacturers can protect everything across their diverse OT and IT networks using Fortinet solutions. For manufacturing cybersecurity, the Fortinet solutions offer a number of key differentiators:

Integration

Fortinet technology provides an end-to-end, integrated cybersecurity architecture covering IT and OT, cyber and physical security, factory and headquarters, data centers, and multiple clouds. This integrated approach 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, using a single pane of glass. This visibility 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 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, deception technology, and UEBA.

OT-specific threat intelligence

FortiGuard Labs provides robust threat intelligence that is specific to OT systems to help manufacturers make better strategic decisions. Fortinet has worked closely with manufacturing customers for 17 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 integration helps streamline data into a single view for informed decision-making.

Protect IT, OT, and Physical Security

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 with broad visibility and integrated control. Learn more about how Fortinet can help you plan or continue your cybersecurity journey.

[1] Top five OT security threats, Nomios, May 10, 2022.

[2] What are Industry 4.0, the Fourth Industrial Revolution, and 4IR?, McKinsey and Company, August 17, 2022.

[3] 2023 State of Operational Technology and Cybersecurity Report, Fortinet, May 24, 2023.

[4] Fake Accounts on Social Media, Epistemic Uncertainty and the Need for an Independent Auditing of Accounts, Internet Policy Review, February 7, 2023.

FORTINET

www.fortinet.com

November 20, 2023 7:01 PM

517972-B-0-EN