WHITE PAPER

A Solution Guide to Operational Technology Cybersecurity

Table of Contents

Executive Summary

With the acceleration of digital transformation (DX)—such as the transition to Industry 4.0—it has become critical for organizations to understand the similarities and differences between their information technology (IT) and operational technology (OT) networks, as well as what happens when the two intersect.

IT generally refers to computing, networking, and managing information in organizations. OT controls processes that have safety and physical impacts, guiding physical processes with equipment in manufacturing plants, power stations, pipelines, railways, and other infrastructure. While the impact of IT functions are typically restricted to an organization itself, many components of OT are critical to public safety and global economic health.

The air gap between OT and IT has evaporated and cyberthreats pose a real challenge to OT organizations: nearly three-quarters indicate they experienced a successful malware intrusion in the past year.[1]

IT and OT networks have traditionally been kept separate (even air gapped) but, motivated by the business advantages that are possible through DX, they are now being integrated.

Benefits of this convergence include the ability to reduce costs, boost productivity, and achieve a competitive advantage. The downside is that interconnecting the environments increases exposure to cyber intrusions, with cybercriminals taking advantage of targeting IT networks to gain access to OT systems. Attacks on power grids, shipping lines, manufacturing plants, and other facilities are steadily increasing.

In a global survey of OT security professionals, a staggering 93% of organizations admitted to experiencing an intrusion in the past 12 months, and 78% experienced more than three. Impacts included downtime, financial or data loss, brand degradation, and even reduced physical safety.[2]

The result is that companies in many industries are scrambling to provide security for vulnerable OT systems. Independent research for Fortinet by Westlands Advisory[2] finds that investment in IT/OT and OT-specific security technologies totaled $6.9 billion for all of 2022. And these investments are increasing more quickly than spending on IT-only cybersecurity, with a projected compound annual growth rate (CAGR) of 21% for OT security and 16% for IT/OT cybersecurity between now and 2027.

These investments are imperative in ensuring that organizations' IT and OT security postures are ready for the most sophisticated attacks. Today's cybersecurity solution must cover the entire attack surface, share threat intelligence between security products, and automate responses to threats. This comprehensive guide explains how Fortinet effectively provides security throughout the interconnected IT and OT infrastructure while fully enabling integration across Fortinet and partner security solutions and supporting security automation across the entire security ecosystem. It also explores how IT and OT are different yet increasingly interconnected, as well as ways to address increased security risks arising from such integrations.

This guide also reviews how elements of the Fortinet Security Fabric map to security controls in leading cybersecurity regulations, standards, and best practices. It outlines an architectural framework for securing OT—correlated to the Purdue Enterprise Reference Architecture (PERA)—and suggests actionable next steps in a journey to a desired state for cybersecurity. Finally, a helpful appendix maps existing OT security needs to Fortinet Security Fabric offerings.

Here is a review of the Fortinet cybersecurity platform—Fortinet Security Fabric for IT and OT—and a close look at the five things every organization must do to secure interconnected digital ecosystems:

1. Gain full visibility across digital assets, networks, and users
2. Segment the network into zones and implement security boundaries
3. Monitor and control access to digital assets
4. Implement proactive measures for threat detection and prevention
5. Streamline security operations across NOC and SOC

Digital Transformation: Opportunities, Challenges, and IT/OT Convergence

OT networks comprise industrial control systems (ICSs) that control equipment in industrial sectors such as manufacturing, energy and utilities, and transportation. ICSs were deployed decades before IT networks and were at first analog and proprietary, with little or no connectivity to IT or external networks. This led to the air gap practice of protection, that OT networks were "safe" because of their relative isolation.

As part of the larger drive towards digital transformation, organizations started unlocking the traditional boundaries between IT and OT to leverage digital technologies. The Internet of Things (IoT), Industrial Internet of Things (IIoT), cloud computing, artificial intelligence (AI), and other innovations that converge IT and OT networks can optimize operations, improve safety and reliability, and deliver a competitive edge.

All the improved agility and efficiency that comes from IT/OT convergence, however, also comes with increased risks to the business. The diminishing presence of the air gap between OT and IT networks means the OT infrastructure is subject to all the threats that IT systems have traditionally faced. Worse, an attack on OT systems can compromise industrial processes and equipment or critical infrastructure—potentially causing dire health and safety consequences if they are breached. For organizations looking to adapt the IT and OT infrastructure to account for convergence and DX, the security for the infrastructure must also transform to protect against evolving cyberthreats.

Information Technology vs. Operational Technology: Understanding the Two Ecosystems

Though IT and OT were designed to serve different purposes, they share the same binary notion at their foundation: “off” and “on,” zero and one, negative and positive. “Off” and “on” are the simplest operations in an industrial control system (ICS). At the most basic level:

- IT is composed of hardware and software that controls the ability to store, retrieve, transmit, and manipulate data or information.
- Operational technology (OT) is the use of hardware and software to monitor and control physical processes, devices, and infrastructure. Operational technology systems are found across a large range of asset-intensive sectors, performing a wide variety of tasks ranging from monitoring critical infrastructure (CI) to controlling robots on a manufacturing floor. OT is used in a variety of industries including manufacturing, oil and gas, electrical generation and distribution, aviation, maritime, rail, and utilities.[3]
- The IT/OT convergence zone, often considered part of OT, is actually a level of separation between IT and OT. This level is also referred to as the demilitarized zone (DMZ). Just below this level are OT dedicated systems oftentimes running the same operating system typically found in IT; thus, this level is comprised of IT-type systems in the OT environment.

However, IT and OT Have More in Common than You May Think

Similarities
• Operating systems: Microsoft Windows, Linux
• Database: Microsoft Excel, SQL
• Endpoints: servers and workstations
• Network equipment: network switches and routers
• Common protocols: FTP, HTTP, HTTPS, NTP, SNMP, Syslog, SSH, TCP/IP, Telnet

Distinction		
IT	Security Objective Priorites	OT
Medium	Availability requirement	Very high
Delays accepted	Real-time requirement	Critical
3-5 years	Component lifetime	20+ years
Scheduled	Application of patches	Rare
Mandatory	Security testing/audit	Occasional
High	Security awareness	Increasing
IT department	Design authority	OEM/SIs
Safety and availability are critically important in OT.		

Clarifying OT Terms

Air gap is a term that is used to describe the isolation of a computer or network. An air-gapped device or network is not physically connected to other devices or networks, nor can it connect wirelessly.

Convergence in terms of digital transformation means that OT components like control systems and industrial networks are being connected to IT systems and networks. With IT/OT integration, the data collected by physical equipment and IIoT devices can be used to identify problems more quickly, increase operational efficiency, and productivity.

Cyber-physical systems (CPS) are smart systems that include engineered interacting networks of physical and computational components. These highly interconnected and integrated systems provide new functionalities to improve quality of life and enable technological advances in critical areas, such as personalized health care, emergency response, traffic flow management, smart manufacturing, defense and homeland security, and energy supply and use. In addition to CPS, there are many words and phrases (Industrial Internet, Internet of Things (IoT), machine-to-machine (M2M), smart cities, and others) that describe similar or related systems and concepts. There is significant overlap between these concepts, in particular CPS and IoT, such that CPS and IoT are sometimes used interchangeably. Cyber-Physical Systems (CPS) are complex systems of computational, physical, and human components integrated to achieve some function over one or more networks.

Distributed control system (DCS) manage local controllers or devices of production systems in one particular location.

Engineering workstation (EWS) as defined by CISA, is usually a high-end, very reliable computing platform designed for configuration, maintenance, and diagnostics of the control system applications and other control system equipment. The system is usually made up of redundant hard disk drives, a high-speed network interface, reliable CPUs, performance graphics hardware, and applications that provide configuration and monitoring tools to perform control system application development, compilation, and distribution of system modifications.

Field sensors/actuators are diverse physical devices that are deployed on or near physical devices and processes. Sensors measure physical attributes such as temperature, voltage, current, rotations per minute, or wind direction. Actuators turn on and off equipment such as motors, pumps and breakers.

Historian server is a critical part of the industrial control system such as DCS or SCADA environment. It stores and logs data collected from various parts of the industrial network, enabling operators and stakeholders to view historical data for the plant.

Human machine interface (HMI) is the workstation for the human operator, displaying process data in real time. The operator monitors and controls the process through the HMI.

Industrial control systems (ICS) play a main role in OT and include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), remote terminal units (RTUs), and programmable logic controllers (PLCs).

Industrial Internet of Things (IIoT) devices do not typically control physical devices in industrial environments. Instead, IIoT devices are typically smart sensors that communicate directly to the cloud. These devices can either connect directly to the cloud or through an edge gateway that sends data to the cloud.

Internet of Things (IoT) are the user or industrial devices or network of devices that are connected to the internet and contain the hardware, software, firmware, and actuators that allow the devices to connect, interact, and freely exchange data and information. IoT devices include sensors, controllers, and household appliances.

Manufacturing executive system (MES) refers to the network that connects machines and work centers in a factory environment. These complex software systems monitor, track, document, and control the manufacturing process from start to finish. The data provided by an MES helps organizations increase plant efficiency and optimize production.

Operational technology (OT) is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and events in the industrial environment.

Operator workstation (OWS) refers to a computer terminal within the industrial network typically connected to DCS or SCADA servers. An OWS is typically considered a "client," as it requests and sends information to the central servers. The OWSs are used for monitoring all ICS operations, performing control actions, and parameter adjustments.

Programmable logic controller (PLC) is an industrial computer that has been adapted to control manufacturing processes. PLCs take sensor data, run some logic, and then based on that logic, send signals to actuators such as pumps, motors, and breakers to physically turn on or off. PLCs also receive commands from human machine interfaces (HMIs) and send time-series data to historian servers.

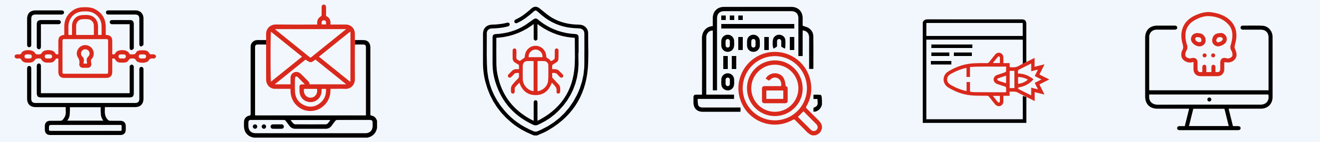
Safety instrumented system (SIS) are designed to override ICS, DCS, and SCADA systems as a fail-safe, last resort in the event that these systems begin to operate outside of safe limits. SISs are designed to provide corrective action if other elements of the control system fail or give faulty instructions.

Supervisory control and data acquisition (SCADA) refers to a system that collects data from various sensors at a factory, plant, site or in other remote locations and then processes this data in a central system which then manages and controls the field (e.g., factory or plant or site) operations.

Real Cyberthreats to OT

When controls for physical equipment connect to enterprise computer networks and the cloud, the digital attack surface expands, allowing cyberattackers to penetrate industrial organizations in new ways. As a result, the process of DX increases cyberthreat vectors through the interconnection with IT and the addition of cloud-based IIoT. This means that industrial breaches—by either attacking IT systems in the OT network or targeting OT-specific devices—are more frequent, with bad actors aggressively scouting their next targets. IBM Security X-Force reports that there has been a 2,204% increase in reconnaissance against OT.[4] Manufacturers have been a particularly enticing target, with a full 75% of all ransomware attacks in the first quarter of 2022 targeting the manufacturing sector. Future attacks are expected to continue the disruption by incorporating OT kill processes into new strains of ransomware.[5]

Common Attack Vectors



Ransomware

Phishing

Malware

Device Vulnerabilities

DDoS

Internal Threats

The fact is that there are no safe havens—today's targets (and threats) are global in scope. And while motivation for attacks varies from monetary to political and everything in between, the end result is nearly always crippling for the affected organization.

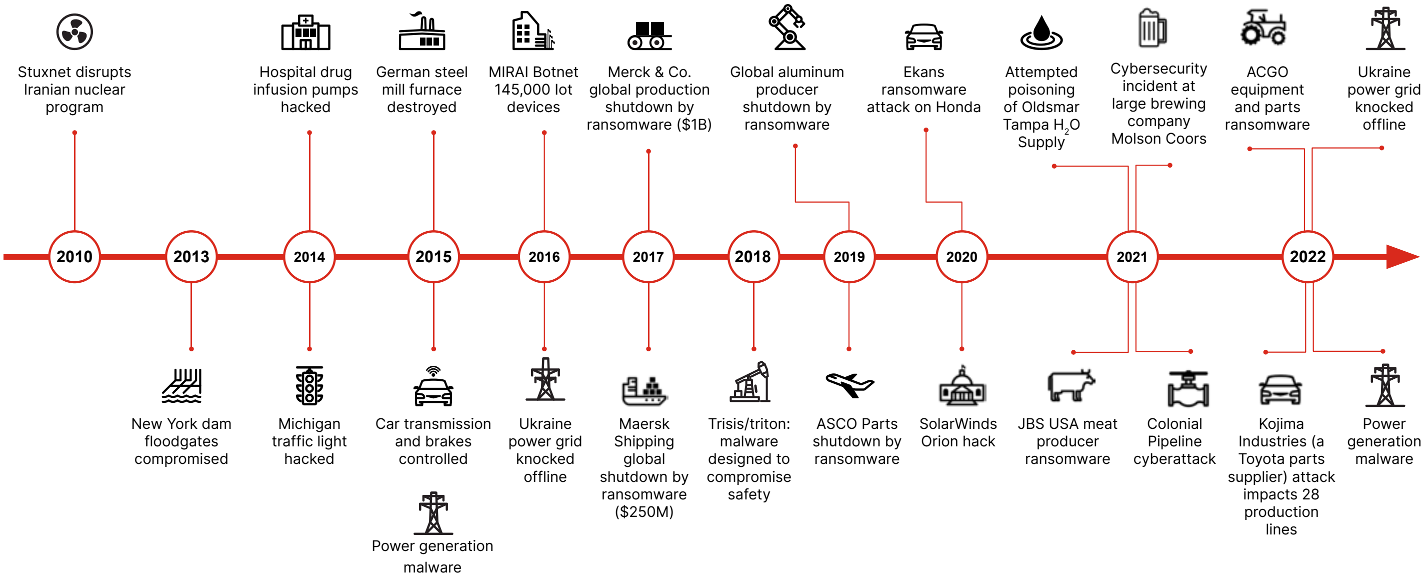

2010
Stuxnet disrupts Iranian nuclear program
2013
New York dam floodgates compromised
2014
Hospital drug infusion pumps hacked
Michigan traffic light hacked
2015
German steel mill furnace destroyed
Car transmission and brakes controlled
Power generation malware
2016
MIRAI Botnet 145,000 Iot devices
Ukraine power grid knocked offline
2017
Merck & Co. global production shutdown by ransomware ($1B)
Maersk Shipping global shutdown by ransomware ($250M)
2018
Trisis/triton: malware designed to compromise safety
2019
Global aluminum producer shutdown by ransomware
ASCO Parts shutdown by ransomware
2020
Ekans ransomware attack on Honda
SolarWinds Orion hack
2021
Attempted poisoning of Oldsmar Tampa H$_2$O Supply
Cybersecurity incident at large brewing company Molson Coors
JBS USA meat producer ransomware
Colonial Pipeline cyberattack
2022
ACGO equipment and parts ransomware
Ukraine power grid knocked offline
Kojima Industries (a Toyota parts supplier) attack impacts 28 production lines
Power generation malware

Figure 1: Cyberattacks are increasing in frequency and impact as noted in this timeline through 2022.

Supplier Breach Shuts Down Toyota Plant Operations

Kojima Industries is a key Toyota parts supplier, providing the automotive giant with parts for seats and other vehicle components. When Kojima was hit by a cyberattack in March 2022, it forced Toyota to shut down 28 production lines at 14 of its Japanese plants.[6]

The attack is thought to be the result of Emotet malware, possibly entering the Kojima system using authentication information stolen from infected devices of Toyota employees.[7] The virus—and a threatening message—were discovered through a file server error and confirmed after a server reboot. An ominous fact is that 80% of Kojima's staff had undergone in-house training on information security.[8]

With the lack of parts disrupting Toyota's just-in-time manufacturing model, the breach is said to have caused a serious 5% dip in the company's monthly production capability.[9]

Attempted Poisoning of Tampa-Area Water Supply

Public acknowledgement of a cyber intrusion aimed at compromising critical municipal infrastructure is rare, but in February 2021, a bad actor gained confirmed access to the water supply in Oldsmar, FL, just outside Tampa.

An alert plant operator noticed that his mouse cursor was moving while not under his control. As the horrified employee watched, the intruder reset the level of sodium hydroxide, also known as lye, from a safe level to one that would severely damage human tissue.

While the dangerous action was quickly reversed, law enforcement officers—from locals to the FBI and Secret Service—are still seeking answers. The exact cause of the breach and the identity of the attackers remain unknown, but in an interview with Wired,[10] investigating officials conceded that, "OT systems were externally accessible, and that all evidence points to the attacker accessing them from the internet." In warning others, the Oldsmar sheriff says, "There is merit to the point that critical infrastructure components shouldn't be connected. If you're connected, you're vulnerable."

Pipeline Shutdown Puts Company in Senate Hot Seat

A single stolen password—that's all it took for hackers to launch a ransomware attack against Colonial Pipeline and disrupt fuel supplies to the entire southeastern U.S. In a Senate committee hearing following the attack, Colonial's CEO admitted that the attacker gained access through a legacy virtual private network (VPN) that did not require multi-factor authentication.[11]

The breach's impact was widespread. A jet fuel shortage caused airport disruptions, while fears of a gas shortage caused panic buying, increased prices, and long lines at the pumps. It was also expensive, as the company paid a ransom in Bitcoin worth appropriately $4.4 million to stop the attack.[12]

For Colonial, however, the costs went far beyond the ransom. Following the hearings, security experts roundly criticized the company for "poor cybersecurity hygiene", and the Transportation Safety Agency (TSA) created new pipeline regulatory directives that will increase compliance costs for the entire industry.[13]

Global Attack on Farming Equipment Manufacturer

Hacker group Black Basta spared no locations in their attack on agricultural equipment and parts producer, ACGO. On May 5, 2022, a ransomware attack shut down sites in the U.S., Germany, China, and France.[14]

The attack, which occurred just weeks after an FBI warning about agriculture-related attacks, took the company a long and costly 15 days to fully restore their factories and parts operations. In addition to the loss of production capabilities, company data was also stolen during the attack.

With production stopped, line workers in France were forced to go home and take paid leave, while U.S. farmers found themselves without key equipment during the critical planting season.

Some Key Learnings from OT Cyberattacks

- Because OT has been traditionally isolated, security is not top of mind, thus basic security hygiene is not implemented within many OT environments. Safety and security must be systemic within an organization to help best practice adoption.
- Nation-states are the biggest threat actors and have demonstrated an ability to inflict global damage.
- Spear phishing, compromised endpoints, and stolen credentials are common attack vectors. This underscores the necessity of two-factor authentication, employee security education, and continuous system monitoring for indicators of compromise (IOCs).
- Attackers are gaining expertise in OT sabotage. They are developing, selling, and buying specialized tool sets designed to penetrate OT protocols and equipment.
- The cultural gap between IT and OT generates safety and security risks within organizations. Organizations where IT and OT are divided are especially susceptible to successful cyberattacks.
- Segmentation is not commonplace within OT environments and thus the lack of segmentation is the most exploited vulnerability—in particular, inadequate segmentation between IT and OT networks. In addition, IT malware like ransomware and worms are making their way into OT networks and traversing laterally, because there is no real network segmentation in place to slow them down.

The Fortinet Cybersecurity Solution for IT/OT

Securing an OT environment can seem daunting at first—but mitigating risks can be accomplished incrementally. Securing any environment is a journey, and it is important to have a destination in mind. In this case, that is an environment optimized to respond to all manner of threats across both IT and OT.

It is common practice to deploy best-in-class point security solutions to solve different security challenges. However, point security solutions are not integrated and work in silos. As a result, security can become complex, difficult to manage, and introduces security gaps. Furthermore, point solutions leave asset owners saddled with the technical debt—they have to make sure their integrations continue to perform as expected as vendors release upgrades. A unified platform-based solution can simplify management and reduce complexity.

Fortinet Protects IT and OT

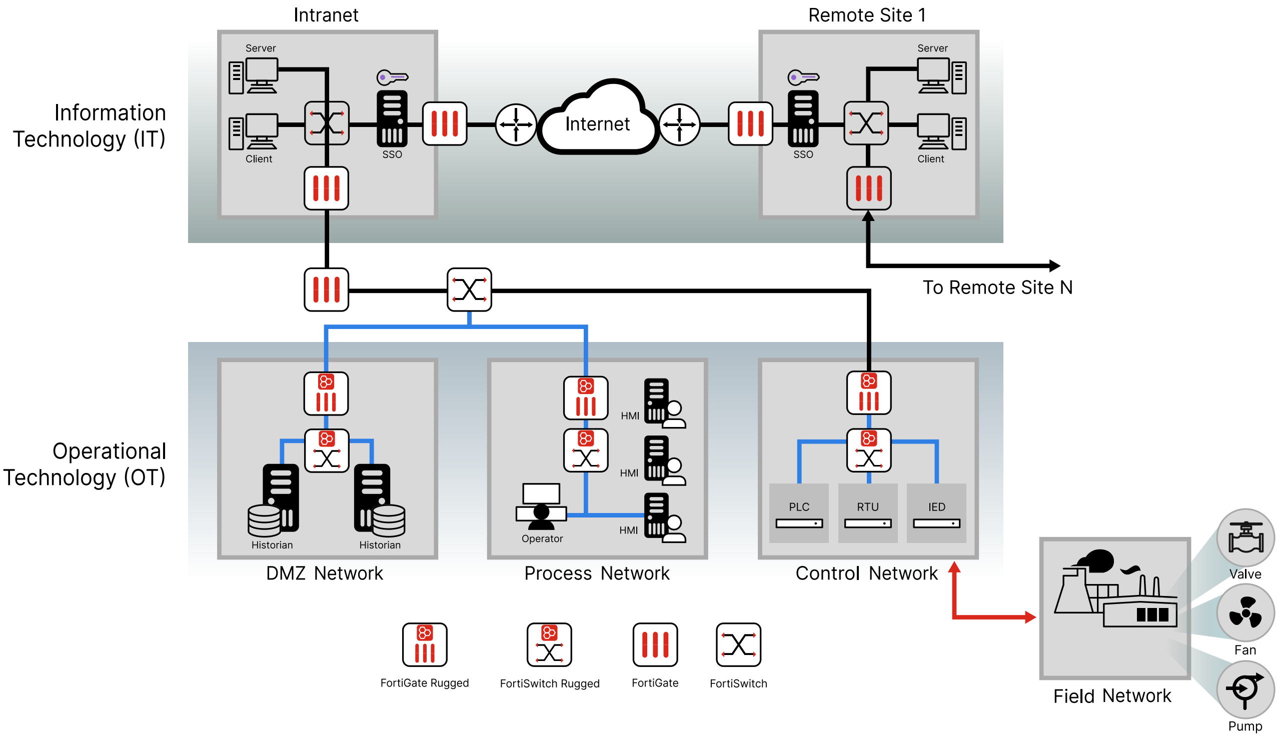


Figure 2: Common IT and OT Network illustrating the need for comprehensive cybersecurity for all users, devices, and applications across all network edges.

Fortinet Security Fabric, comprising FortiGate and FortiSwitch, as shown in Figure 2, brings together the concepts of convergence and consolidation to provide comprehensive cybersecurity protection for all users, devices, and applications—across all network edges. It provides:

- **Broad visibility and protection** of the entire digital attack surface to better manage risk
- **Integrated solutions** that reduce management complexity and share threat intelligence
- **Automated self-healing networks** with AI-driven FortiGuard security services for fast and efficient operations
- **Simplified management** from a single pane of glass

The resulting security architecture provides continuous trust assessment of devices and workloads, which dynamically adapts as network configurations change (see Figure 3).

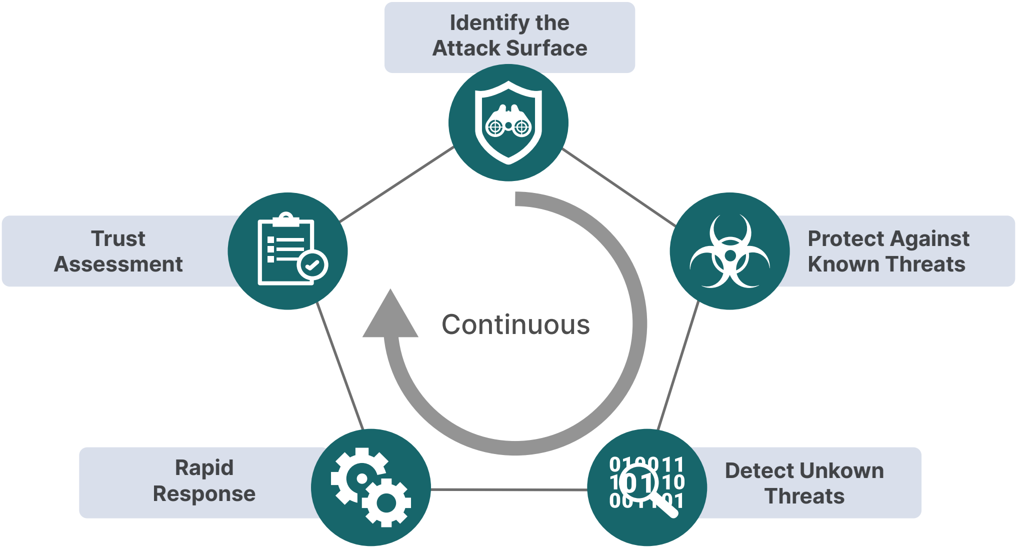


Figure 3: Framework for Digital Transformation Security. Continuous trust assessment from multiple points in the network enables faster detection and automated responses, minimizing mitigation time.

Security Fabric Safeguards for OT

In an OT environment, the Fortinet Security Fabric provides network visibility by authenticating and classifying IT, OT, and IIoT devices. Unlike other security solutions, it does this passively via deep packet inspection (DPI) without active scanning—a critical factor as many OT networks are particularly sensitive, and scanning can have a negative effect.

Instead, the Security Fabric discovers and classifies devices in real time to build risk profiles based on their behavior. Then it dynamically assigns devices to device groups, along with distributing appropriate policies to security devices and network segments. By making the environment visible, the Security Fabric also enables intent-based segmentation into secured network zones. It protects zones by enforcing customized policies, dynamically updated by continuous trust assessment. This allows the network to automatically grant and enforce baseline privileges for each OT device risk profile, enabling the critical distribution and collection of data without compromising the integrity of critical systems .

In addition, an integrated approach enables the centralized correlation of intelligence between security devices and segments. The Fortinet Security Fabric is able to quickly identify anomalous behavior and send an alert, as specified, to the network operations center (NOC) or security operations center (SOC). That level of responsiveness is possible only if devices are able to see and share information with each other. The Security Fabric can automatically wall-off potentially compromised devices to contain incidents and respond in a coordinated way. In an OT environment, it can be configured to monitor, detect, and alert, without affecting production.

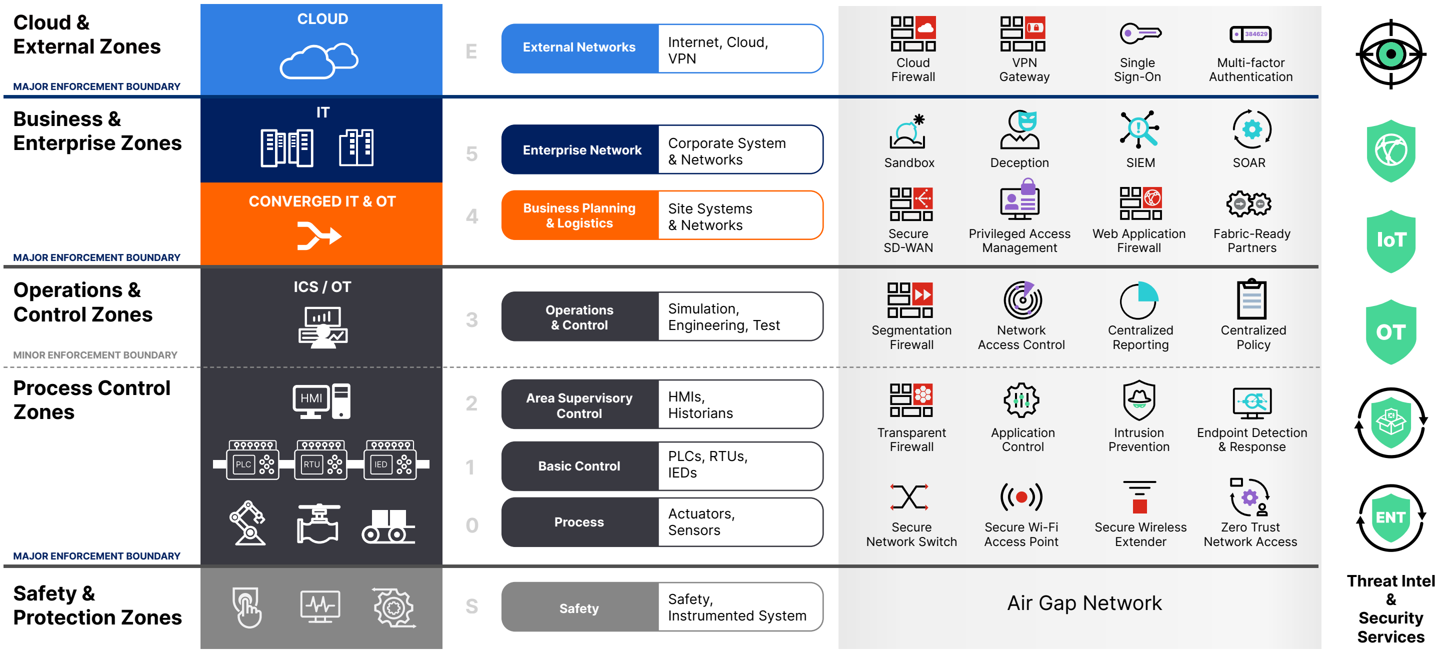


Figure 4: The Fortinet Security Fabric Realized for the Converged IT and OT Organization. Broad visibility from integrated security solutions, which also share local and global threat intelligence, provides a security foundation for organizations with IT and OT environments. For a list of OT security needs matched to Fortinet offerings, see the Appendix.

Fortinet OT Expertise

For nearly two decades, Fortinet has been protecting OT and critical infrastructure customers in sectors such as energy, defense, manufacturing, food, and transportation. A line of Fortinet security appliances has been ruggedized to serve indoors or outdoors at sites with extreme heat, cold, vibration, and electrical interference.

A key differentiator of Fortinet in the OT security solutions marketplace is its focus on—and continually growing OT services for—the FortiGate next-generation firewall (NGFW) provided by FortiGuard Labs. FortiGuard Labs delivers specialized security services for OT though an OT-specific IPS package. In addition to a vast library of IT device vulnerabilities, the IPS inspects and polices network traffic for OT-specific applications and protocols. It also identifies vulnerabilities in various OT-specific devices and systems and protects them from exploitation—It also known as virtual patching—discussed further in this paper.

The IPS also offers deep packet inspection (DPI) for OT protocols to support implementation of granular security policies. The IPS database is continuously updated via a connection to the FortiGuard Labs servers or it can be updated manually if a direct connection to the FortiGuard Labs servers is not possible, such as for isolated industrial networks. The combination of FortiGate NGFW with OT-specific IPS and continual updates from FortiGuard Labs provides more sophisticated application control of the traffic between zones on an OT network. It also enables the FortiGate NGFW to detect attempted exploits of known vulnerabilities. Because OT environments often operate with minimal or periodic patching, being able to detect and block attacks on known vulnerabilities is especially important.

The intelligence delivered through FortiGuard Labs comes from its global development team, with very experienced threat hunters, researchers, analysts, engineers, and data scientists working to provide real-time protection against advanced threats found in the network, endpoint, emails, applications, and web threat vectors (see Figure 5).[15] This award-winning team combs through a constant stream of data from nearly 5.6 million devices deployed globally. The network combines the latest threat intelligence and original research from strategic global security agencies, key technology partners, and cybersecurity alliances around the world. All this information is fed back into every Fortinet appliance to provide up-to-the-minute protection from zero-day threats, botnets, viruses, and other malicious exploits.

FortiGuard Labs Overview

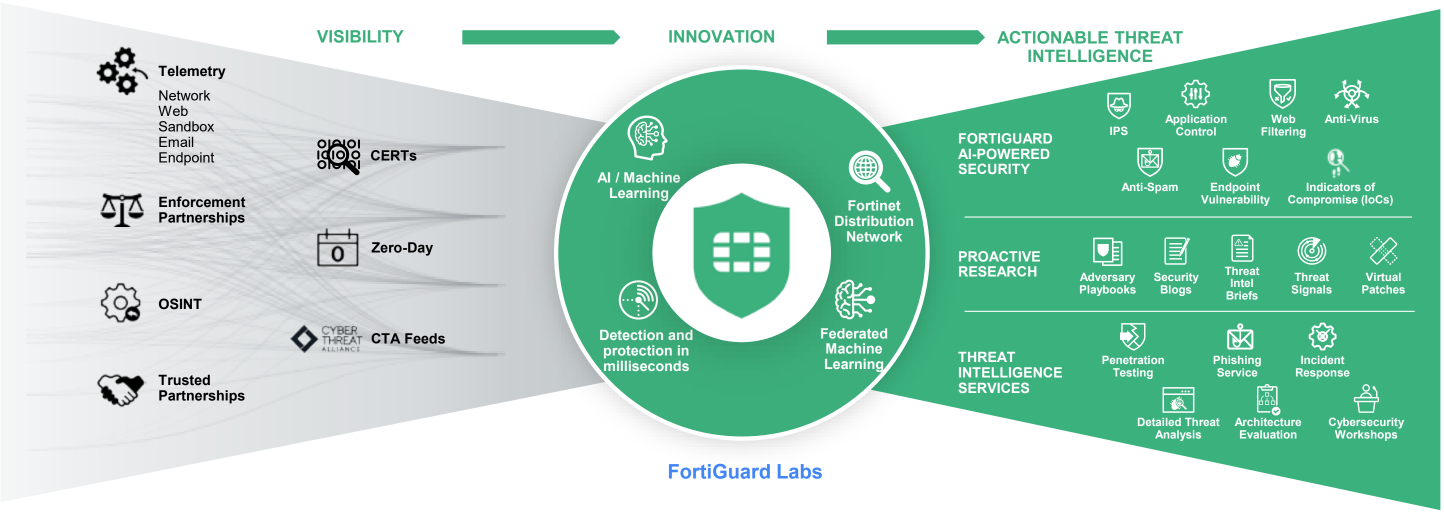


Figure 5: FortiGuard Labs Security Services. FortiGuard Labs includes 500+ experts using in-house and patented technologies to provide real-time security services.

Your OT Security Plan

As organizations plan their OT security transformation, they should assume that their OT systems have already been compromised. The wisest organizations plan for the possibility that hidden malware is present, simply waiting to wake up, in an environment where an attacker has little constraint, the opportunity for lateral movement, and the ability to elevate privilege.

These assumptions enable OT security teams to implement a more thorough approach to identifying and neutralizing access to critical and highly valued OT assets. They also encourage processes that enable quick recognition of actions that are beyond normal. The fact is that proactive security needs to be engineered directly into the environment, not added on at scattered points after the fact. Let's take a closer look at five things every organization must do to protect itself.

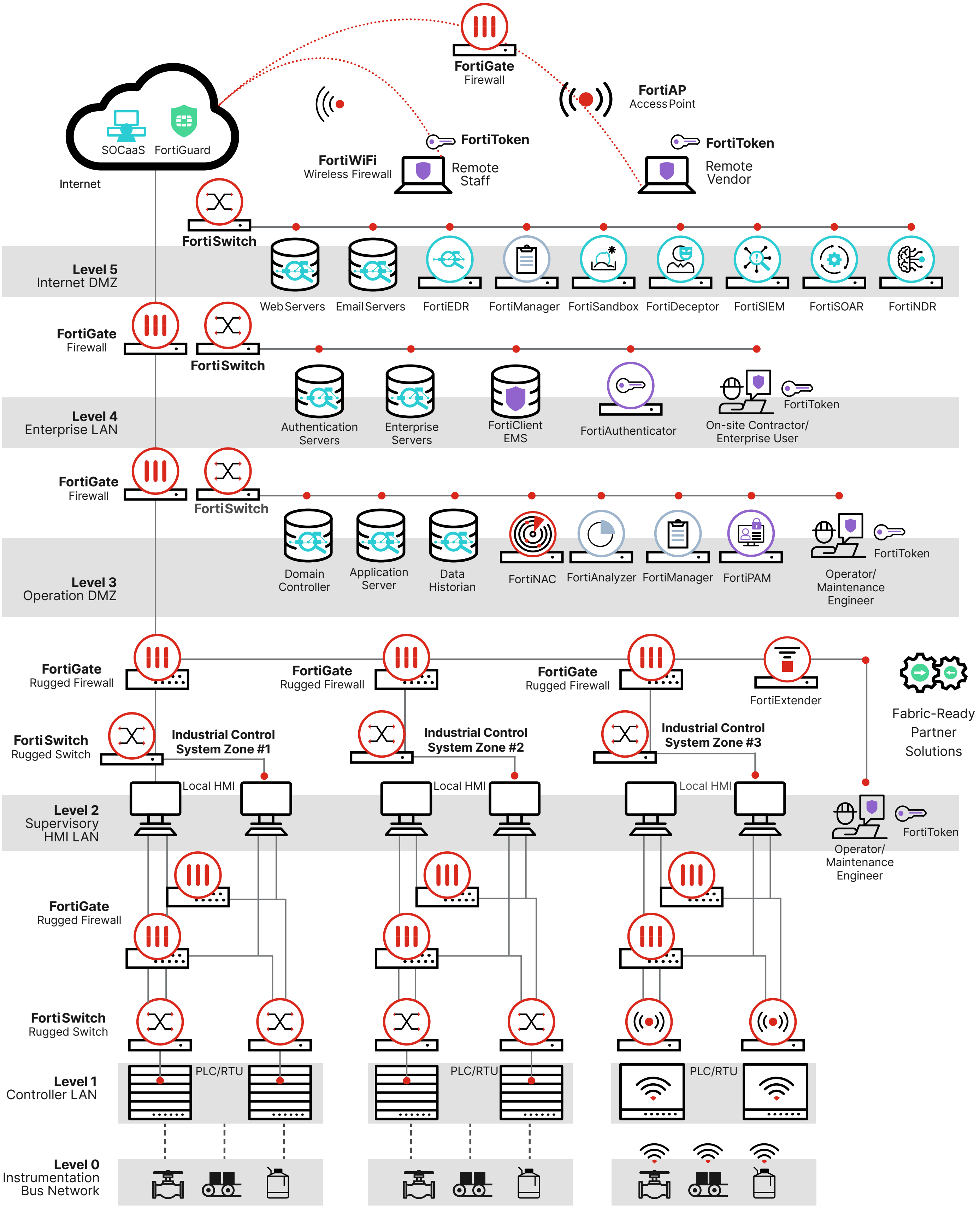


Figure 6: Securing all layers of the Purdue Model using Fortinet solutions across a connected IT and OT infrastructure.

Must-Do #1: Gain Full Visibility Across Digital Assets and Networks

A security team requires detailed and specific knowledge of all the digital assets to implement the desired level of security protection. Digital assets may include users, applications, devices, and systems spread across IT and OT environments. In addition to the IT assets, it is imperative to develop a thorough asset model of all the relevant digital assets deployed in OT, including PLCs, RTUs, HMIs, historians, and so forth. A lack of awareness, or a blind spot, as to what is critical vs. non-critical because you don't know its existence means you can't apply the desired level of security protection for it. Such blind spots represent a huge security gap in OT.

The first step in improving OT security posture is to have an up-to-date inventory of assets, such as devices and applications running on a network, as well as the users accessing or operating those assets. This can serve as a strong foundation for planning security architecture. It also helps with determining what best practices should be deployed based on the organization's particular needs.

A comprehensive security risk assessment should be able to provide a list of assets, applicable threats, and vulnerabilities found.

Visibility into the OT assets and networks can be achieved by leveraging FortiGate—with or without the integration of FortiSwitch—plus solutions from the Fortinet partnership portfolio such as Nozomi Networks, Dragos, Claroty, and more. Fortinet's FortiGuard Labs offering includes an OT-specific security service that can be leveraged for visibility and control over OT applications and protocols. Combined with FortiSwitch and FortiGate, you can achieve comprehensive visibility into the OT assets and networks. This can be expanded further for industrial wireless networks with the integration of FortiAP or FortiExtender with FortiGate.

- **FortiGate NGFW** is for security control and policy enforcement.
- **FortiAnalyzer** provides centralized monitoring, logging, and reporting for FortiGate appliances deployed across IT and OT.
- **FortiManager** provides centralized device management and security policy implementation for FortiGate appliances across IT and OT. It enables consistent security policy enforcement and software updates across all FortiGate appliances from a single and streamlined user interface.

- **FortiSIEM** delivers the ability to ingest and analyze log data from IT and OT, enabling correlations for threat actor behavior that spans both environments. FortiSIEM can also show threat activity in the ATT&CK framework for both Enterprise IT and ICS environments.
- **FortiSOAR** is a holistic security orchestration, automation, and response workbench, designed for SOC teams to efficiently respond to the ever-increasing influx of alerts, repetitive manual processes, and shortage of resources. FortiSOAR's customizable security operations platform provides automated playbooks and incident triaging, plus real-time remediation for IT/OT enterprises to identify, defend, and counter cyberattacks.
- **Fabric-ready partner solutions** offer deep integration into partner technologies and platforms enabling security automation through a broad range of integrated solutions to enable advanced end-to-end security across the digital infrastructure.

Must-Do #1 Compliance Reference

- NIST CSF Identify – Asset Management (ID.AM)-1, -2
- ISA/IEC 62443-2-1:2009 4.2.3.4
- ISA/IEC 62443-3-3:2013 SR 7.8

Must-Do #2: Segment the Network into Zones and Implement Security Boundaries

Traditional OT networks lacked restrictions—especially those that were running in an isolated or air gap environment, disconnected from the external networks. Some OT networks have implicit trust, making it possible for any digital asset in the network to be controlled or administered from anywhere regardless of the criticality of the asset for ICS/OT operations.

A key step to improve OT security posture is network segmentation. According to the United States Cybersecurity and Infrastructure Security Agency (CISA), it is one of the most effective architectural concepts and a recommended best practice for securing and protecting OT environments from internal and external threats.[16] A recent publication released by CISA for Cross-Sector Cybersecurity Performance Goals (CPGs) for reducing cyber risk to the critical infrastructure also highlights network segmentation as one of the key security practices to reduce the likelihood of adversaries accessing the OT network after compromising the IT network.[17]

How Should OT Networks Be Segmented?

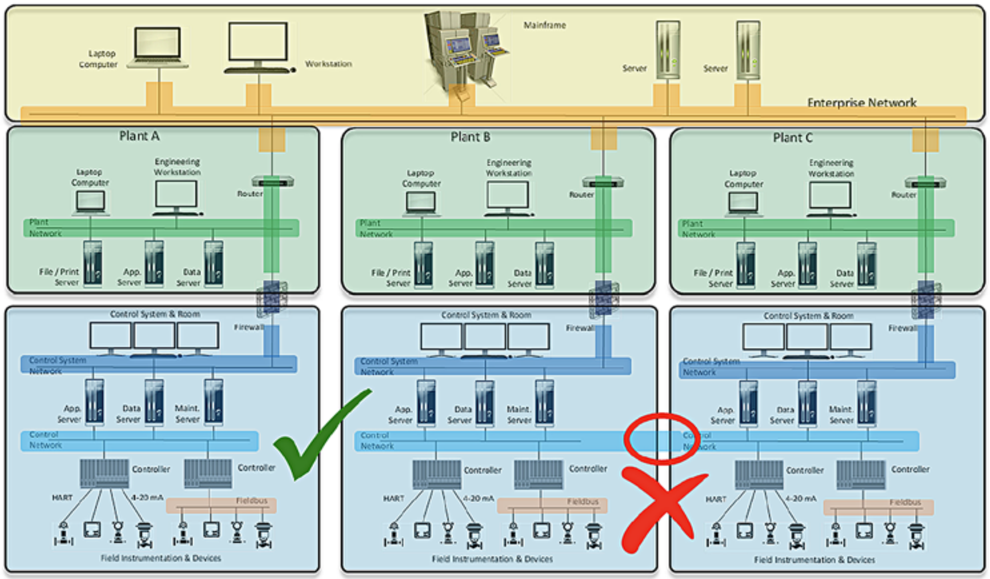
The idea is to divide the network into a series of functional segments or "zones" (which may include sub-zones or microsegments) and make each zone accessible only by authorized devices, applications, and users. A "conduit"—typically a firewall—defines and enforces the zone boundaries, which are channels that enable essential data and applications to cross securely from one zone to another. Conduits are introduced between different zones to control communication between zones and to implement security controls. Conduits act as control mechanisms (gatekeepers) between the different zone boundaries.

- **FortiGate NGFW** is for security control and policy enforcement.
- **FortiAP** is for security and access control policy enforcement for the end users as devices try to access the network.
- **FortiSwitch** is for complete visibility and control of users and devices in the network.
- **FortiNAC** is for visibility, control, and automated response for everything that connects to the network.
- **FortiExtender** is a bridge between local Ethernet LANs and wireless LTE/5G WAN connections.

How to Define Security Zones and Conduits?

- A zone **can** have sub-zones.
- A conduit **cannot** have sub-conduits.
- A zone **can** have more than one conduit. Cyber assets within a zone use one or more conduits to communicate.
- A conduit **cannot** traverse more than one zone.
- A conduit **can** be used for two or more zones to communicate with each other.

This architectural model of zones and conduits reduces the attack surface by dividing networks into segments and microsegments. While network segmentation controls the north-south traffic, network microsegmentation controls east-west traffic. If a network intrusion or breach occurs, network segmentation restricts an attacker's movement, thereby reducing the impact by limiting the lateral movement of threats. Users or devices authorized for a specific activity in a specific zone are limited to operating within that zone.



Source:ISA GCA

Security Boundaries: How to Implement Them

Zone and conduit strategy and segmentation capabilities can be enforced by Fortinet NGFWs – FortiGate. Whereas FortiGate perimeter firewalls are focused on defending an external border, internal segmentation FortiGate firewalls are used in conjunction with FortiSwitch (or without FortiSwitch) to implement security policies and inspect and filter network communications within the ICS/OT networks for inter-VLAN or intra-VLAN communication. The FortiGate firewalls sit between two or more points on the internal network and analyze packets and network streams. They provide:

- Authentication, user, and device controls
- Intrusion detection and prevention—OSI Layer 2 and above
- Inspection and control for allowed and disallowed applications
- Antivirus/anti-malware protection
- Customizable security policy features for next-generation firewall/intrusion prevention systems (NGFW/NGIPS)
- The ability to log traffic and record packet captures when required

The network segmentation and microsegmentation architecture protects against malicious files, applications, and exploits. It also provides asset and network visibility as well as protection at multi-gigabit speeds—all without slowing down the network. The architecture can be deployed for both wired and wireless industrial networks.

Summary

Network Segmentation and Microsegmentation

Network Segmentation

- Fortinet’s core offering with FortiGate NGFW
- Implementation of security zones and conduits
- Security for inter-VLAN communication
- North and south network traffic monitoring and threat protection
- IPS signatures help with implementing virtual patching and prevent exploitation of system vulnerabilities from internal or external threats

Network Microsegmentation

- Fortinet's core offering with FortiGate NGFW and integrated FortiSwitch
- Futher segmentation of security zones based on different security requirements
- East and west network traffic monitoring and deep packet inspection
- Security for intra-VLAN communication
- Application control signatures help with implementing granular protocol and application policies and stop lateral movement of threats

Network Segmentation and Microsegmentation Are Dynamic

The zone and conduit model needs to be adaptable based on the target network architecture to implement security policies dynamically.

Traditional segmentation assumes unchanging, static trust values for users, devices, and applications. In reality, however, the trustworthiness of all these elements changes frequently, either due to normal changes in business operations or as the result of developing threats. Some ICS/OT deployments may follow static network architecture that may not change for several years; in such cases, static security policies can be implemented for network segmentation and microsegmentation.

To cover every situation, Fortinet solutions offer dynamic network segmentation and microsegmentation; however, static configuration is also supported. Dynamic implementation continuously monitors trust levels and adapts security policies accordingly. Organizations can intelligently segment network and infrastructure assets regardless of their location—whether distributed across multiple sites or located in a single area. High-performance, advanced security isolates critical ICS/OT assets from potential exposure to threats. It also ensures mitigation measures are in place from the perspectives of both detection and prevention.

Securing Both Wired and Wireless Networks

Traditionally, OT environments have not contained wireless connections. In many cases, however, organizations are deploying sensors and other devices in their OT environments and connecting them wirelessly. This further expands the digital attack surface. Wireless access points (APs), as well as wireless gateways, are attractive targets for cyberattacks.

In the past, the ICSs were based on flat communication networks, whether it be wired or wireless. Gradually, these flat networks have been improved by segmenting them using network switches and virtual LANs. While implementing VLANs is a good first step, switches and VLANs do not provide any intelligence in terms of identifying advanced threats embedded within the protocol payload. Switches and VLANs merely forward frames from one side of the network to the other side.

VLAN-based segmentation is better than having a flat physical LAN. However, it still leaves a big gap in terms of securing interconnected ecosystems such as IIoT that may utilize complex and/or internet-enabled protocols for communication.

Both wired and wireless networks need security by design, administered from one central interface, instead of being protected by add-on point security solutions managed through multiple interfaces. Centralized security management—as discussed in Must-Do #5, further in this document—not only reduces risk but also improves visibility and minimizes administration time for network and security operations teams.

Must-Do #2 Compliance Reference

- NIST CSF Protect – Protective Technology (PR.PT)-4
- NIST CSF Protect – Identity Management, Authentication, and Access Control (PR.AC)-5
- NIST CSF Respond – Mitigation (RS.MI)-1
- ISA/IEC 62443-2-1:2009 4.3.3.4, 4.3.4.5.6
- ISA/IEC 62443-3-3:2013 SR 3.1, 3.5, 3.8, SR 4.1, 4.3, SR 5.1-5.4, SR 7.1, 7.6

Must-Do #3: Monitor and Control Access to Digital Assets and Networks

Network segmentation is an important part of OT security. However, devices, users, and applications should always be authenticated before they can use the resources assigned to them. Authentication and authorization are critical, especially as remote work continues to trend. Many of OT's most damaging security breaches have been due to compromised user accounts and passwords, exacerbated by users being provided with inappropriate levels of access.

Zero-Trust Access for OT With Fortinet

Fortinet has developed solutions for implementing zero-trust architecture in IT and OT environments. A zero-trust strategy provides comprehensive visibility and protection across devices, users, endpoints, cloud, and IT/OT infrastructures with a "never trust, always verify" approach to security. Fortinet Zero-Trust Access (ZTA) focuses on role-based access control to the network, while zero-trust network access controls user access to applications. Together, the zero-trust architecture continually verifies who and what is using the resources—with access granted only after verification. IT, OT, and IIoT devices are identified and secured, while the asset owners and operators gain full visibility into and control over anything that's connected to the network.

Several solutions in the Fortinet Security Fabric work together to validate who and what is connecting to the OT network, and then limit their access to only the appropriate resources based on their roles.

- **FortiGate NGFW** is for security control and policy enforcement.
- **FortiAP** is for security and access control policy enforcement for the end users as devices try to access the network.
- **FortiSwitch** provides complete visibility and control of users and devices in the network.
- **FortiAuthenticator** enables single sign-on and user authorization identifying users, querying access permissions from third-party systems, and communicating the access requests to FortiGate to implement identity-based security policies.
- **FortiPAM** offers identity and privileged access management capability and enables zero-trust security implementation for critical assets. It controls users' access to critical applications and systems, monitors and tracks users' activity, and enables secure remote access to critical assets.
- **FortiClient** is for endpoint management and ZTNA.
- **FortiToken** provides two-factor authentication with one-time password (OTP) application with push notifications or a hardware time-based OTP token.

Who Is Connecting: ZTA Solutions for Authenticating Users

When users connect, FortiAuthenticator validates their identities. It simplifies and centralizes the management and storage of user identity information while applying granular control of access to each zone and conduit. It also integrates with Active Directory, RADIUS, LDAP, 802.1x wireless authentication, certificate management, and single sign-on (SSO).

FortiAuthenticator is compatible with and complements the FortiToken—a software and hardware-based token technology for two-factor authentication and secure access, enabling authentication with multiple FortiGate network security appliances and third-party devices. FortiToken requires users to have the appropriate software or hardware token, not just a correct username and password. It makes two-factor authentication simple for users and administrators.

FortiAuthenticator builds on the foundations of Fortinet single sign-on (SSO), adding a greater range of user identification methods and greater scalability. FortiAuthenticator is the gatekeeper of authorization into the Fortinet-secured enterprise network. It identifies users, queries, accesses permissions from third-party systems, and communicates this information to FortiGate devices so they can enforce identity-based policies.

Fortinet SSO saves time and boosts productivity by providing secure identity and role-based access to the Fortinet connected network. Through integration with existing Active Directory or LDAP authentication systems, Fortinet SSO enables enterprise-wide, user-identity-based security without impeding the user or generating additional work for network administrators.

FortiPAM is specifically focused on managing and securing administrator and user accounts with elevated privileges. This is valuable because accounts that have privileged access permissions are particularly attractive targets for attackers.

FortiNAC can also be used to identify network users. It then implements appropriate network access control policies to restrict access to critical data and sensitive assets while ensuring compliance with internal, industry, and government regulations and mandates.

What Is Connecting: ZTNA Solutions for Authenticating Devices and Accessing Applications

The solutions from Fortinet Security Fabric can analyze network traffic and profile each network element based on observed characteristics and behavior, as well as noting the need for software updates to patch vulnerabilities. As with user access, however, everything must be rooted in zero-trust network access.

FortiClient, FortiPAM, and FortiGate are the foundation of ZTNA. In conjunction with FortiPAM, FortiClient establishes application identities and confirms to FortiGate whether those applications should be given access or not, and to which users. FortiClient's zero-trust feature provides telemetry to FortiClient Enterprise Management Server (FortiClient EMS), a security management solution that enables scalable and centralized management of multiple endpoints. FortiClient EMS provides efficient and effective administration of endpoints running FortiClient. It provides visibility across the network to securely share information and assign security profiles to endpoints. It is designed to maximize operational efficiency and includes automated capabilities for device management and troubleshooting.

In addition to identifying users as previously noted, FortiNAC can also identify network devices. To further protect networks, FortiNAC can lock down ports as desired: no devices are allowed on the network unless they are permitted. A port will not provide network connectivity until the connecting device is authorized. This helps enforce a policy that any device added to an OT network must first be approved by the network administrator. If a device is compromised, the intruder's ability to travel in the network and attack other assets will be limited. An alert can be triggered to notify the network administrators, or the solutions can be configured to respond automatically and contain the device in real-time. Automating this entire process reduces the containment time from days to mere seconds.

Securing the Connected Industrial Worker

IT/OT convergence isn't the only trend increasing the vulnerabilities of OT networks. The COVID-19 pandemic sent company employees home, leaving both IT and OT teams scrambling to support and secure a fully remote workforce. Even though some companies are shifting to hybrid or even going back to fully onsite work models, the paradigm shift of remote-first work revealed some significant advantages to industrial workers having offsite access to onsite systems and resources. With instant access from anywhere, facility downtime can be reduced through the efforts of employees who are not at the facility. Travel costs and safety risks can also be reduced by remote equipment operation, while unneeded office space can be repurposed for revenue-generating operations. Finally, productivity is increased when workers have instant access to subject matter experts (SMEs), cloud analytics, smart devices, and even augmented reality—all of which require connectivity from outside the OT network.

To preserve these benefits, network users need the same access in a residence, airport, or hotel room that they would sitting in an office on a plant floor. Yet, providing that level of access introduces additional cybersecurity risks—especially for companies operating with a perimeter-based approach to security. To provide secure remote access, companies must adopt a holistic approach to cybersecurity that also relies on the zero-trust approach to access, making no distinction between "trusted" internal traffic and traffic from the outside. Robust network segmentation must be bolstered by behavior-based ways to detect when user accounts and devices are compromised.

The Fortinet work-from-anywhere (WFA) solution enables companies and IT/OT enterprises to provide extensive access to remote industrial workers while protecting network segments that specific employees do not need.The Fortinet Zero-Trust Network Access (ZTNA) framework securely connects users to applications no matter where the user is located and no matter where the application is hosted. FortiPAM, FortiAuthenticator, and FortiToken identity and access management solutions help companies limit access to authorized users. FortiGate segmentation enables the IT/OT networks to be divided according to business needs, enabling zero-trust access. Advanced endpoint protection tools, such as FortiEDR (endpoint detection and response) and FortiClient, help prevent infiltration through the endpoint devices used by remote workers. These Fortinet solutions enable companies and IT/OT enterprises to provide full and secure access to remote workers while protecting digital assets against cyberattacks from remote locations.

Streamline Network Access with FortiSwitch and FortiAP

Through a single interface in a FortiGate NGFW, network or security operations teams can push firewall capabilities and policies to ports on FortiSwitches and FortiAPs throughout the organization. The proprietary FortiLink protocol creates a secure tunnel between Switches or APs and the firewall to protect and encrypt traffic. This solution makes it easy for an organization to maintain separate VLANs for employees, equipment, and guests or contractors, if permitted. Each VLAN can have its own centrally administered and granular security policies. It’s important to note that no known competitive solution offers these capabilities without requiring additional hardware and complex configuration.

Must-Do #3 Compliance Reference

- NIST CSF Protect – Identity Management, Authentication, and Access Control (PR.AC)-1, -3, -4, -6, -7
- NIST CSF Protect – Protective Technology (PR.PT)-3
- ISA/IEC 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.1-4.3.3.5.18, 4.3.3.6.1-4.3.3.6.9, 4.3.3.7.1-4.3.3.7.4
- ISA/IEC 62443-3-3:2013 SR 1.1-1.13, SR 2.1-2.7

Centralized monitoring of switch and AP security also simplifies compliance reporting. The integration of switches and APs also enables all users—including any guests or contractors that are permitted—to be authenticated against the same user database. They are controlled by the security policy appropriate for their identity, regardless of whether they connect to the wired or wireless network.

Must-Do #4: Implement Proactive Measures for Threat Detection and Prevention

It's imperative to implement proactive security measures to equip the security teams with sufficient capability and intelligence to pre-emptively identify any known and unknown threats and prevent them from becoming security incidents. Mindset is half the battle—with threats constantly evolving, the ideal security posture is to act as if you've already been breached. The other half is having the right technology in place. Fortinet Security Fabric has several solutions that, when integrated together with FortiGate, can offer such capabilities, including:

- **FortiGate NGFW** is for security control and policy enforcement
- **FortiClient** is for endpoint management and ZTNA
- **FortiEDR** provides real-time, automated endpoint threat detection, protection, orchestrated incident response, and forensics
- **FortiSandbox** provides advanced persistent threat detection and protection
- **FortiDeceptor** provides honeypot deployments to deceive, expose, and eliminate both external and internal threats before any significant damage is done
- **FortiGuard Labs** provides real-time, up-to-date, actionable information and mitigation measures on threats, vulnerabilities, and zero-day exploits

Fortinet's FortiGuard Labs offers an OT-specific security service that integrates with FortiGate NGFWs, FortiSandbox, and FortiDeceptor to offer in-depth visibility for the OT assets and network communication. The service receives periodic signature updates that enable FortiGate NGFWs to identify and police most of the common ICS/OT applications and protocols, supporting advanced threat protection. (See Figure 7 for a list of popular applications and protocols supported. An up-to-date, exhaustive list is available on the FortiGuard Labs website.)

The OT-specific security service provides broader coverage for ICS and OT applications and protocols through application control (AppCtrl) and IPS signatures. For an up-to-date list of supported signatures, please visit fortiguard.com.

Allen-Bradley DF-1 →
Allen-Bradley PCCC
BACnet →
CC-Link →
CN/IP CEA-852 →
CoAP →
DDSI-RTPS
Digi ADDP →
Digi RealPort(Net C/X)
Digi RealPort(Net C/X) DNP3 ≣
Direct Message Profile →
DLMS/COSEM(IEC62056) →
DNP3 →

ECHONET Lite →
ECOM100
ELCOM 90 →
Emerson DeltaV
Emerson ROC
EtherCAT →

Ethernet POWERLINK
EtherNet/IP-CIP →
Ether-S-Bus →
Ether-S-I/O →
FactorySuite NMXSVC
FL-NET →
GE EGD
GE SRTP →
Hart IP →
IEC60870-5-104 ≣
IEC 60870-6 (ICCP/TASE.2) →
IEC 61850 MMS →
IEC 61850-90-5 R-GOOSE

IEC 61850-90-5 R-SV
IEEE 1278.2 DIS →
IEEE C37.118 Synchrophasor →
KNXnet/IP (EIBnet/IP →
LonTalk IEC14908-1 CNP →
Mitsubishi MELSEC →

ISO 9506 MMS →
Modbus TCP/IP ≣
Moxa modbus RTU →
Moxa UDP Device Discovery
MQTT
MTConnect
Niagara Fox
oBIX
OCPP →
Omron FINS →
OPC AE →
OPC Common →
OPC DA →

OPC DA Automation →
OPC HDA →
OPC HDA Automation →
OPC UA →
OpenADR →
OSIsoft PI

Profinet CBA →
Profinet IO →
Rockwell FactoryTalk view SE
SafetyNET p →
Schneider UMAS →
SECS-II/GEM →
Siemens LOGO →
Siemens S7 →
Siemens S7 1200 →
Siemens S7 Plus →
Siemens SIMATIC CAMP →
STANAG 4406 Military Messaging
STANAG 5066

Triconex TSAA →
TriStation →
Vedeer-Root ATG
Vnet/IP

→ message layer policy ≣ message and parameter policy (FortiOS v6.4 and above)

Figure 7: Application Control and IPS signatures for OT with FortiGuard Industrial Security Service. FortiGuard Industrial Security Service provides up-to-date signatures to the FortiGate NGFW, enabling it to support granular security policy configuration to detect and control attempted exploits to ICS.

Beyond enabling asset and network visibility, the security service provides vulnerability protection for OT applications and protocols from major ICS manufacturers. Updated signatures and vulnerability protection data enable a FortiGate NGFW to detect attempted exploits of known vulnerabilities. Because many OT devices and systems run without patches, having the ability to catch these exploits and protect against them—providing virtual patching or vulnerability shielding—is invaluable.

The following diagram illustrates the concept of "virtual patching" or "vulnerability shielding" in the ICS/OT networks.

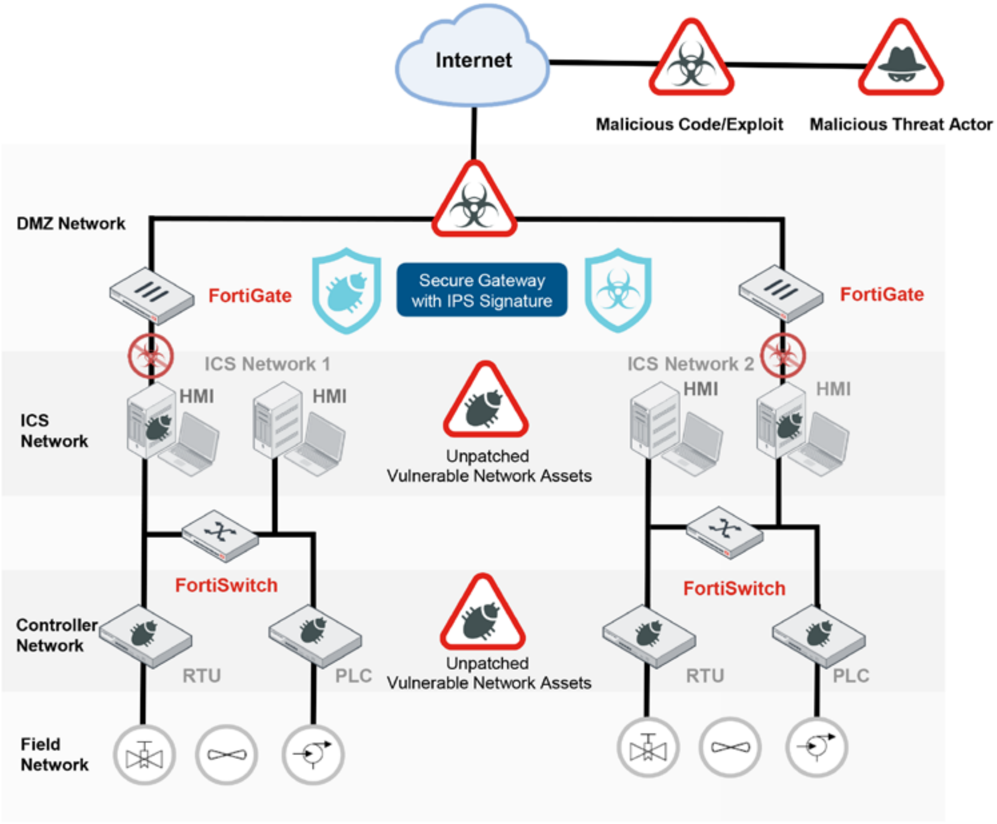


Figure 8: Virtual Patching or Vulnerability Shielding—acts as a compensating security control against threats that have the potential to exploit known or unknown vulnerabilities. Virtual patching works by implementing layers of security controls that intercept and prevent an exploit from compromising the vulnerable assets connected on the network(s).

Endpoint Threat Detection, Protection, and ZTNA

FortiClient integrates with FortiGate NGFWs to provide visibility into all endpoints. When a vulnerability is detected in an endpoint, FortiClient triggers an alert—a preferred choice in an OT environment, instead of automatically patching the endpoint. In an IT environment, FortiClient can do more—it can also patch the vulnerability or shield it and quarantine the rogue system. With FortiClient's policy-based automation, containing threats and controlling outbreaks happen immediately and automatically. Intelligence is shared with the entire Fortinet Security Fabric. FortiClient also acts as a ZTNA agent, enabling VPN and ZTNA for users and applications.

FortiEDR offers endpoint detection and response (EDR) that prevents, detects, and defuses threats while keeping systems online across IT/OT environments. It comprehensively secures endpoints in real-time—both pre- and post-infection. It includes several key capabilities for protecting vulnerable OT endpoints: ML-based next-generation antivirus, application communication control, automated EDR, real-time blocking, threat hunting, incident response, and virtual patching capabilities. It ensures high availability for OT systems, supporting multiple and legacy operating systems even amid a security incident or breach. FortiEDR leverages the Fortinet Security Fabric architecture and integrates with many Security Fabric components including FortiGate NGFWs, FortiSandbox, and FortiSIEM.

Responding to Advanced Persistent Threats

With the stakes for OT intrusion so high, it is also essential to prepare for attacks that have yet to be encountered. In such a scenario, it becomes crucial that the intrusion is detected rapidly, its propagation limited, and its impact minimized. Here, a critical component of the Fortinet Advanced Persistent Threat Protection Framework is FortiSandbox, which is designed to detect and analyze advanced attacks that might bypass more traditional, signature-based defenses. Once malicious code is identified, FortiSandbox will return risk ratings. The local intelligence is shared in real-time with Fortinet and third-party, vendor-registered devices and clients to remediate and immunize against newly discovered advanced threats.

With FortiDeceptor, decoys or honeypots can easily be deployed in both IT and OT networks. The goal is to implement innocuous decoys, mimicking the other real digital assets on the network and luring attackers while they are in the reconnaissance phase of an attack. FortiDeceptor creates a network of decoys to lure attackers and monitor their activities on the network. When an intruder attacks a decoy, an alert is generated and their malicious activities are captured and analyzed in real-time. This analysis generates a mitigation and remediation response that protects the network.

FortiDeceptor can mimic servers such as jump servers, human-machine interfaces (HMIs), engineering/operator workstations, and even programmable logic controllers (PLCs) in the ICS/OT networks. Likewise, in the IT networks, it can emulate typical IT services such as RDP, SSL VPN, etc. It supports several OT protocols and integrates with the Fortinet Security Fabric for a simplified setup, with flexible deployment options plus easy operation and monitoring. For example, the alerts and events generated by FortiDeceptor can be seamlessly forwarded to FortiSIEM for analysis and threat response. The asset discovery feature in FortiDeceptor generates the network asset inventory using passive network sniffing for network threat visibility and automating decoy deployment. The network asset discovery supports both IT and OT networks. FortiDeceptor also supports MITRE ATT&CK for ICS framework—both as an independent dashboard and inside the incident alert itself—to provide better visibility to incident alerts in the ICS network.

Must-Do #4 Compliance Reference

- NIST CSF Detect – Security Continuous Monitoring (DE.CM)-4, -5
- NIST CSF Respond – Mitigation (RS.MI)-1, -2, -3
- ISA/IEC 62443-2-1:2009 4.3.4.3.8, 4.3.4.5.6, 4.3.4.5.10
- ISA/IEC 62443-3-3:2013 SR 2.4, SR 3.2, SR 5.1-5.4

Must-Do #5: Streamline Security Operations Across NOC and SOC

While many organizations are farther along in the maturity model for securing their IT environments, the protection of their ICS/OT environment has lagged. At Level 1 on the maturity scale, it's not unusual to find IT/OT enterprises still implementing asset and network visibility for monitoring purposes only, but any remedial actions on the observed incidents is taken manually. Further, at Level 2, threat remediation is done selectively via automation, but not too much for the fear of disrupting the more brittle ICS/OT environment. At the mature level, Levels 3 to 5, there is automatic or dynamic remediation on security incidents. The network and/or security operations center (NOC/SOC) are running playbooks, with a threat intel team doing the forensics and then providing feedback to the operations team for mitigations.

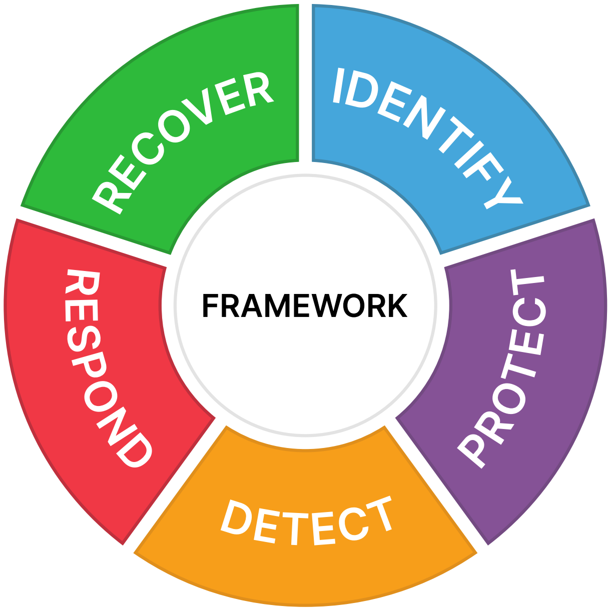
The goal of any IT/OT security paradigm—the path to which is paved by adhering to the first four "Must-Dos" outlined in this guide—is to develop a fully operational, 24×7, mature "cyber fusion center"[18] that converges the NOC and SOC environments and offers automated remedial action that will not disrupt the ICS/OT environments. A cyber fusion center would be responsible for threat intelligence, analytics, threat detection, incident response, threat hunting, and governance and compliance. Fortinet research has shown that organizations that streamline NOC/SOC operations across IT and OT environments achieve the best outcomes, such as the fewest breaches and reduced impact of breaches.[19]

With a cyber fusion center, an organization has full visibility of devices, access provisions, incidents, threat alerts, intelligence feeds coming from third parties, and more. With Fortinet, this is made possible by combining the power of solutions that comprise the Fortinet Security Fabric.

- **FortiGate NGFW** is for security control and policy enforcement.
- **FortiSIEM** delivers the ability to ingest and analyze log data from IT and OT, enabling correlations for threat actor behavior that spans both environments. FortiSIEM can also show threat activity in the ATT&CK framework for both enterprise IT and ICS environments.

- **FortiSOAR** is a holistic security orchestration, automation, and response workbench, is designed for SOC teams to efficiently respond to the ever-increasing influx of alerts, repetitive manual processes, and shortage of resources. FortiSOAR's customizable security operations platform provides automated playbooks and incident triaging, plus real-time remediation for IT/OT enterprises to identify, defend, and counter any attacks.
- **FortiNDR** offers network detection and response (NDR) capabilities through an artificial intelligence-driven breach protection technology. It's designed for short-staffed SOC teams to defend against various threats—including advanced persistent threats—through a trained Virtual Security Analyst™ that helps with identifying, classifying, and responding to threats, including those that are well camouflaged. FortiNDR employs deep neural networks based on advanced AI and artificial neural networks to provide sub-second investigation by harnessing deep-learning technologies that assist SOC analysts with an automated response to remediate different breeds of attacks. FortiNDR significantly reduces the time to identify network anomalies and malicious content on the network and then mitigates with Fortinet Security Fabric and third-party integration.
- **Security Operations Center-as-a-Service (SOCaaS)** is for cloud-based managed security monitoring service that analyzes security events generated from a customers' FortiGate and other Security Fabric products, performs alert triage, and escalates confirmed threat notifications.
- **FortiRecon Digital Risk Protection (DRP)** is a SaaS-based service, combines three powerful modules: External Attack Surface Management, Brand Protection, and Adversary Centric Intelligence. FortiRecon provides a view of what adversaries are seeing, doing, and planning to help you counter attacks at the reconnaissance phase and significantly reduce the risk, time, and cost of later-stage threat mitigation.

A mature cyber fusion center using Fortinet solutions also handles compliance monitoring and reporting. Internally, stakeholders such as CSOs or CIOs may want to report on risk flags. External compliance reporting may also be necessary for regulatory frameworks—for example, NIST CSF, IEC 62443, NERC CIP, NIS2 Directive, etc.—where third-party or regulatory bodies require compliance reporting. Regulatory compliance requirements for ICS/OT have become more prescriptive over the course of time, with increasingly costly penalties for noncompliance. Deploying Fortinet Security Fabric solutions enhances compliance as the solutions address a number of critical security controls as classified under the NIST Cybersecurity Framework (CSF)[20] – Identify, Detect, Protect, Respond, and Recover.



Regulatory, Compliance Body	Compliance Requirement	Sector, Region Applicability
NIST	CSF	Critical Infrastructure, USA/Global
ISA/IEC	IEC 62443	ICS/OT, Global
FERC	NERC CIP	Electric Power, USA
ENISA	NIS2 Directive	Critical Infrastructure, Europe

Table 1: Regulatory and compliance initiatives differ by region and sector. This table provides examples of prominent initiatives.

Seeing the Big Picture

The Fabric View dashboard in FortiManager draws on this and other data to present the big picture: a unified perspective for both network and security operations (NOC/SOC) teams. Through this dashboard, administrators can obtain an accurate, up-to-the-minute status on every device in the organization's Security Fabric. SOC teams can use the feed of operational data from the FortiSIEM CMDB to accurately assess the scope of security alerts and issues. NOC teams can use the Fabric View dashboard to immediately see if any of the performance degradations or irregularities they are experiencing are the result of a security incident. With this insight, the operations team is more likely to understand and readily consent to the SOC team's requests to reconfigure or quarantine a compromised asset on the network.

The Security Fabric topology in FortiManager ensures real-time dissemination of alerts and responses among all digital assets in the IT/OT networks. This, combined with a real-time global intelligence feed from FortiGuard Labs, enables SOC teams to identify and stop even the newest and most sophisticated threats.

FortiGuard Security Rating Service improves auditability to indicate where noncompliance may have occurred, both identifying shortfalls and simplifying reporting. The service also enables the tracking and comparison of a security score against peer/industry groups, with explanations of what is behind the score.[21]

Network traffic should not only be visible but also needs to be presented in context with network events. Many log analysis and SIEM solutions require administrators to provide this context manually, cross-referencing security alerts with operational data. This type of analysis quickly becomes stale and is highly prone to human error. It's also prohibitively time-consuming for NOC/SOC teams that are already stretched thin overseeing the IT/OT environments.

Instead, traffic should be automatically correlated with data from other relevant digital assets on the network. It should be presented with an understanding of the assets' relationships and norms. To accomplish this, Fortinet has developed an intelligent infrastructure and application discovery engine. It can discover and map the topology of both physical and virtual infrastructure, on-premises and in public/private clouds, simply using credentials and without any prior knowledge of what the devices or applications are. The configuration management database (CMDB) in FortiSIEM enables sophisticated, context-aware event analytics using CMDB objects in search conditions.

FortiSIEM and FortiSOAR offer out-of-the-box, predefined reports supporting a wide range of compliance and auditing frameworks for IT and OT infrastructures.

Automation is Critical

When it comes to cybersecurity, every second counts. Automation makes processes happen faster, and AI can optimize those processes based on new patterns of cybercriminal behavior. Fortinet's FortiGuard Labs has been developing and training its FortiGuard AI self-evolving threat-detection system using supervised machine learning techniques. FortiGuard AI autonomously collects, analyzes, and classifies threats, then develops highly accurate defensive signatures to block them in rapid succession. It also disseminates those signatures throughout the Fortinet Security Fabric. This includes the ability to define differences between clean and infected files and to develop signatures that catch zero-day threats.

Predictive analysis is not enough, however, as many malicious servers are only discovered after they have already caused harm somewhere in the world. The FortiGuard Indicators of Compromise (IOC) Service helps security analysts identify risky devices and users based on a collection of artifacts that are known to indicate a high probability of a computer intrusion. The IOC service consists of a package of approximately 500,000 IOCs gleaned from a variety of sources around the globe and delivered daily to FortiAnalyzer and FortiSIEM solutions. Armed with this timely global threat intelligence, SOC analysts can scan weblogs to identify past communications with servers that are now known to be malicious. They can work with the NOC team to mitigate the impact of such communications.

Must-Do #5 Compliance Reference

- NIST CSF Detect – Anomalies and Events (DE.AE)-1, -2, -3
- NIST CSF Respond – Analysis (RS.AN)-1, -2, -3
- ISA 62443-2-1:2009 4.4.3.3, 4.3.4.5.6 - 4.3.4.5.8
- ISA 62443-3-3:2013 SR 2.8 - 2.12, SR 3.9, SR 6.1, 6.2

Planning OT Security: IT/OT Cybersecurity Architecture

When developing a cybersecurity plan for an OT environment, it is useful to map security capabilities against the standards, models, frameworks, and architectures that have been developed for the purpose of securing OT and industrial environments. Some highly influential versions of these include:

NIST SP-800-82: The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82 was enacted by the U.S. Department of Commerce to help advance safe, effective practices in industrial settings. It provides guidance for establishing secure industrial control systems. These ICSs include SCADA systems, DCS, and other control system configurations such as programmable logic controllers that are often found in the industrial control sectors.

Purdue Enterprise Reference Architecture: Adopted by ISA99, the Purdue Model was developed by the Purdue University Consortium for Computer Integrated Manufacturing in the 1990s. The Purdue Model's advantage has always been that it provides a clear hierarchy for network segmentation, with different levels having different cybersecurity requirements. However, one challenge with this model has been the hyperconvergence of IT and OT. With the addition of devices that are part of the IIoT, enhancements are needed. As shown in Figure 9, the Fortinet Security Fabric aligns with Purdue Enterprise Reference Architecture.

Enhanced Purdue Enterprise Reference Architecture

Standards-Based Framework with Fortinet Security Fabric

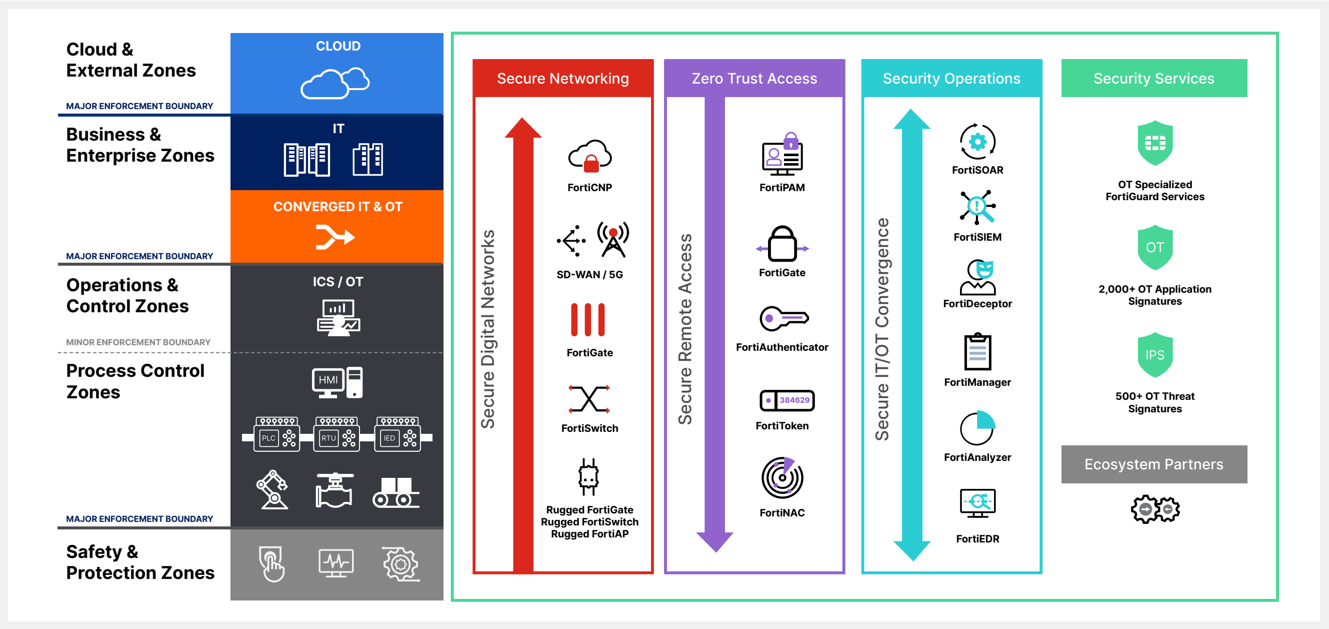


Figure 9: Typically deployed Security Fabric solutions across IT and OT

IEC 62443: This is a set of ICS security standards written by ICS experts for ICS owners, manufacturers, and integrators across a range of applications and sectors. It provides technical requirements that foster a cohesive approach to security that takes into account varying phases of maturity. Using a step-by-step process incorporating "maturity phases," these standards outline a lifecycle approach as part of a cybersecurity program. By segmenting ICS into security zones, organizations can better focus mitigation efforts related to risk, vulnerabilities, and compliance in both a localized and broad perspective within their ICS environment. IEC 62443 series adopt PERA for guidance on security architecture and its implementation.

NIS Directive (NIS-D): Originally adopted by the European Parliament in July 2016, now in its version 2 as NIS2, NIS-D addresses network and information systems security in relation to critical infrastructure. This framework does not prescribe what to achieve or hard requirements for each category. Instead, it examines the risk for each operator and outlines steps that can be taken to minimize the risk. It also establishes legal measures to increase cybersecurity capabilities within the EU across its multiple member states and various operators by establishing a common framework to discuss both cyber risk and cybersecurity incident response across the EU.

Next Steps: Pathway to Fortinet Security Fabric for OT

The Fortinet Security Fabric protects the digital attack surface of IT and OT networks. Deploying the Security Fabric is a journey to a desired state that provides visibility, integration, automation, resilience, and future proofing of the security environment. The Security Fabric can be deployed in stages that are aligned with organizational security priorities. While the section above has covered the minimum "must-dos" for all organizations, it is wise to also consider incorporating these recommended best practices for OT security:[22]

1. Full network mapping and connectivity analysis. Understanding the physical and digital locations of all devices mapped within a network should be a primary concern of OT managers. For example, if a PLC is communicating with a different PLC due to an error or an intrusion, it is crucial for the manager to be able to discover this issue, as well as implement a mitigation strategy as soon as possible. This can only be accomplished if the connections of all assets are accurately mapped.

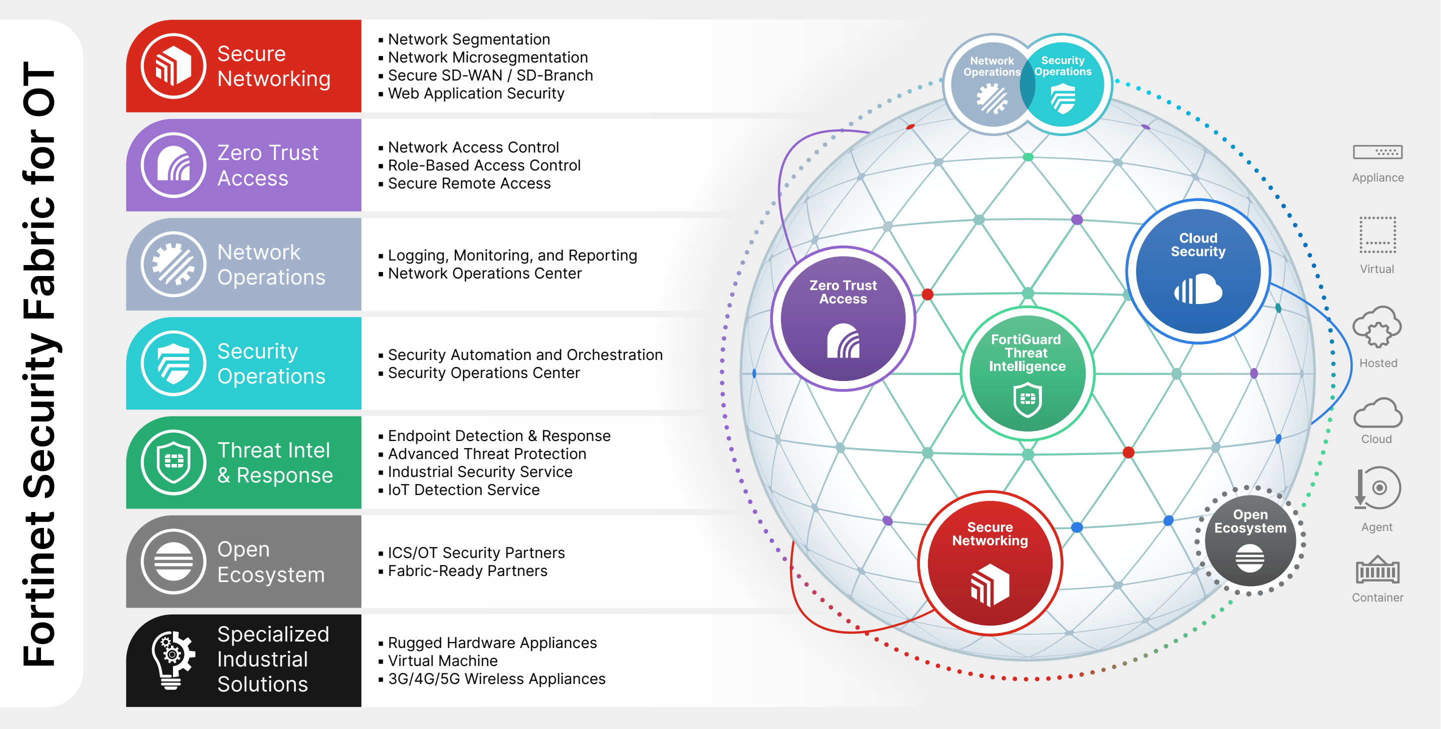
2. Implementing a zero-trust framework. A zero-trust framework is built on the principle of "never trust, always verify." Within this kind of system, every person, device, application, and network is presumed to be a threat. Therefore, each of these entities has the responsibility of proving its legitimacy before it is allowed to connect.

3. Aligning the right remote access tools. Ensuring that the right people and systems have access to the operational technology is essential, especially because they may be pivotal to the flow of business. An OT system is often different from an IT system because it usually does not have a full selection of tools that can be granularly configured to enable remote access.

Organizations seeking help in planning or continuing their cybersecurity journey can learn more at www.fortinet.com/ot or reach out at OT@fortinet.com.

Visit the OT Security Solutions Hub for additional technical information on the OT-aware Fortinet Security Fabric.

Appendix: OT Security Needs Mapped to Fortinet Offerings



Fortinet Security Fabric for OT

Secure Networking	▪ Network Segmentation ▪ Network Microsegmentation ▪ Secure SD-WAN / SD-Branch ▪ Web Application Security
Zero Trust Access	▪ Network Access Control ▪ Role-Based Access Control ▪ Secure Remote Access
Network Operations	▪ Logging, Monitoring, and Reporting ▪ Network Operations Center
Security Operations	▪ Security Automation and Orchestration ▪ Security Operations Center
Threat Intel & Response	▪ Endpoint Detection & Response ▪ Advanced Threat Protection ▪ Industrial Security Service ▪ IoT Detection Service
Open Ecosystem	▪ ICS/OT Security Partners ▪ Fabric-Ready Partners
Specialized Industrial Solutions	▪ Rugged Hardware Appliances ▪ Virtual Machine ▪ 3G/4G/5G Wireless Appliances

Figure 10: The Fortinet Security Fabric for IT and OT. The Fortinet Security Fabric provides broad visibility of the entire attack surface, integrated protection that shares global and local threat intelligence, and automated operations and response.

References

[1] "State of Operational Technology and Cybersecurity Report," Fortinet, 2022.

[2] "IT/OT & OT Total Available Market Analysis," Westlands Advisory Research for Fortinet, March 2022.

[3] "What Is OT Security?"

[4] "X-Force Threat Intelligence Index 2022," IBM, February, 2022.

[5] Abdulrahman H. Alamri, "Dragos ICS/OT Ransomware Analysis: Q1 2022," Dragos, May 3, 2022.

[6] Abdulrahman H. Alamri, "Dragos ICS/OT Ransomware Analysis: Q1 2022," Dragos, May 3, 2022.

[7] Nikkei Staff Writers, "Toyota stoppage highlights supply chain vulnerabilities," Nikkei, March 1, 2022.

[8] Nikkei Staff Writers, "Toyota stoppage highlights supply chain vulnerabilities," Nikkei, March 1, 2022.

[9] "5 Major Ransomware Attacks of 2022," Cyber Management Alliance, June 15, 2022.

[10] Andy Greenberg, "A Hacker Tried to Poison a Florida City's Water Supply, Officials Say," WIRED, February 8, 2021.

[11] Stephanie Kelly and Jessica Resnick-ault, "One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators," Reuters, June 8, 2021.

[12] Sean Michael Kerner, "Colonial Pipeline Hack Explained: Everything You Need to Know," TechTarget, April 26, 2022.

[13] "TSA revises and reissues cybersecurity requirements for pipeline owners and operators," TSA, July 21, 2022.

[14] Gontran Giraudeau, "Computer hacking: the Massey Ferguson tractor assembly site, AGCO Beauvais, victim of a cyberattack," FranceInfo, May 5, 2022.

[15] "FortiGuard Labs," Fortinet, 2022.

[16] "Layering Network Security Through Segementation," CISA, 2022.

[17] Bayard Johnson, "Consolidated Component Listing," CISA, 2022.

[18] "Cyber Fusion Center vs SOC," Guidepoint Security, 2023.

[19] "State of Operational Technology and Cybersecurity Report," Fortinet, 2022.

[20] "NIST Cybersecurity Framework," NIST, 2023.

[21] "Send Security Rating statistics to FortiGuard," Fortinet, 2022.

[22] "5 Best Practices for Operational Technology (OT) Security," Fortinet, 2022.

FORTINET

www.fortinet.com