WHITE PAPER

A Solution Guide to Operational Technology Cybersecurity

Table of Contents

Executive Summary

Operational technology (OT) and information technology (IT) have traditionally been kept separate in most cases, but now they are being integrated. OT controls processes that have physical impact, guiding equipment in manufacturing plants, pipelines, railways, and other infrastructure. Many components of OT are critical to public safety and global economic health.

IT generally refers to computing, networking, and managing information in organizations. Integrating IT with OT reduces costs, boosts productivity, and delivers competitive advantage. That is why, in a recent survey, three-quarters of OT organizations reveal they have made, at least, basic connections between the two environments.[2] The downside is that integrating the environments increases exposure to cyberattacks, with cyber criminals targeting IT networks to gain access to OT systems. Nearly 90% of OT organizations have reported a breach of their OT networks, and 56% have been breached in the past year.[3] Attacks on power grids, shipping lines, steel plants, and other facilities are increasing.

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

Organizations must ensure their OT and IT security postures are ready for the most sophisticated attacks. To do this, a cybersecurity solution must cover the entire attack surface, share threat intelligence between security products, and automate responses to threats. This guide explains how Fortinet enables integration of IT with OT while increasing protection throughout the network. It spotlights how OT and IT are different, why they are converging, and how to address increased risk. It presents Fortinet cybersecurity solutions for OT and IT and outlines five best practices to protect a converged environment:

1. Identify assets, classify, and prioritize value
2. Segment the network
3. Analyze traffic for threats and vulnerabilities
4. Control access by users and devices
5. Secure both wired and wireless access

This guide also reviews how elements of the Fortinet Security Fabric map to security controls in leading regulations. And it outlines an architectural framework for securing OT, correlated to the Purdue Network Model. It suggests next steps in a journey to a desired state for cybersecurity. Finally, an appendix maps OT security needs to Fortinet Security Fabric offerings.

Fourth Industrial Revolution: Opportunities and Challenges

OT networks control equipment in sectors such as manufacturing, energy and utilities, and transportation. They were developed decades before IT networks and were at first analog and proprietary, with little or no connectivity to IT networks. This led to the "air-gap" myth, meaning that OT networks were protected by their relative isolation. Now, however, OT and IT networks are converging in a digital transformation big enough to be called the Fourth Industrial Revolution. Current changes are best understood after a quick summary of the first three revolutions:

1. A change from muscle-powered to steam-powered processes in the late 18th and 19th centuries.
2. A move from steam to electrically powered assembly lines in manufacturing, or electrically powered controls in other sectors such as energy and transportation in the 20th century.
3. Advances in computer-driven automation beginning in the 1980s.
4. Changes in all industries as a result of converging digital capabilities. These are opening new opportunities for many companies, such as:
   - **Big data** from sensors helped a gold mine change its process, boosting yield and saving $20 million.[4]
   - **Machine learning (ML)/artificial intelligence (AI)/analytics** enabled an HVAC manufacturer to predict commercial systems failure in the field with 90% accuracy. [5]
   - **Augmented reality** glasses helped warehouse pickers drop error rates by 40%.[6]
   - **3D printing** enabled an automaker to build new models sixfold faster than its competitors.[7]
   - **Internet of Things (IoT)** will save New York state taxpayers $100 million per year by cutting energy use in 20,000 public buildings.[8]
   - **Cloud** computing capabilities have enabled Amazon Web Services (AWS) to help grow businesses ranging from Airbnb to Zillow and earn Amazon $17.5 billion in revenue in 2017.[9]

What Is OT?

OT and IT have evolved to serve different purposes:

- OT is hardware or software that causes a change through direct monitoring or control of physical devices, processes, and events.
- IT has the ability to store, retrieve, transmit, and manipulate data or information.

Item	OT	IT
Definition	■ Detect or cause a change through direct monitoring or control of physical devices, processes, and events	■ Store, retrieve, transmit, and manipulate data or information
Focus	■ Physical	■ Data
Industry Examples	■ Manufacturing ■ Energy and utilities ■ Transportation (e.g., trains)	■ All industries
Business Goals (Listed in order of priority)	■ Safety (worker and customer) ■ Availability ■ Integrity ■ Confidentiality (process, IP formulations)	■ Confidentiality (financial, customer, partner, IP data) ■ Integrity ■ Availability

Item	OT	IT
Relationship to Business	■ Is the business (creates revenue)	■ Supports the business (cost center)
Environment	■ Includes environmentally controlled as well as distributed environments: May be exposed to heat, cold, moisture, vibration, and electrical interference	■ Within data centers or other controlled environments
Cyberattack Consequences	■ Potential loss of life, injury, environmental damage ■ Immediate, high-revenue losses per hour or even minute (e.g., stopped assembly line) ■ Adverse economic effects ■ Risk to national security ■ Supply chain disruptions ■ Loss of service such as power or water ■ Production and operational disruption or complete outage ■ Brand damage ■ Regulatory penalties ■ Potential loss and theft of intellectual property	■ Operations disrupted ■ Typically, lower revenue losses per hour in IT compared to OT cyberattack ■ Data loss and theft (personally identifiable information [PII], financial data, IP) ■ Loss of customer trust ■ Brand damage ■ Regulatory penalties ■ Loss of business (some industries have high churn rates—e.g., retail)
Standards	■ Standard and proprietary: Serial and other legacy protocols. Evolving to standards-based architectures, resulting in mixed environments.	■ Open: Ethernet, IP
Software Changes, Patching, Maintenance	■ Infrequent/annual, increasing risk ■ Changes made by vendors (by remote access, by bypassing security and auditability)	■ Recommended often/weekly ■ Changes made by IT team
Processor Total Capacity	■ Often limited, outdated processors ■ Requirements designed when implemented and upgraded as needed	■ Highly scalable processing
System Life Cycle	■ Previously 20 to 30 years, now expectations are shorter because of OT-IT convergence	■ Three to five years
System Availability	■ Very high	■ Frequently low-medium

Table 1: Understanding OT and IT Differences.

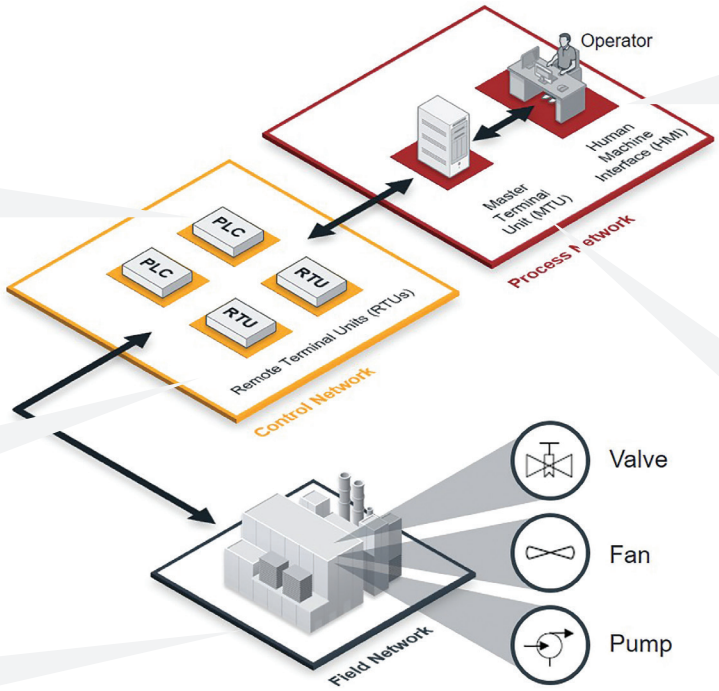
Clarifying OT terms

OT, industrial control systems (ICS), and supervisory control and data acquisition (SCADA) systems often are used interchangeably. ICS is a subset of OT and SCADA is a subset of ICS. SCADA is defined as a graphical user interface for high-level process management.[10] SCADA's history is rooted in distributed applications, such as power, natural gas, and water pipelines. Figure 1 provides a basic topology for OT system elements.

Programmable logic controllers (PLCs) are sometimes used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose remote terminal units (RTUs). However, many PLC devices are notoriously delicate, and even actively scanning these devices can cause them to fail.

RTUs connect to sensors, convert their signals to digital data, and then send them on to the supervisory system.

Field sensors/actuators include sensors, monitors, actuators, and other technologies that are deployed on or near physical devices and processes (generators, pipelines, fans, robotics) to monitor and initiate changes. On occasion, these components, along with RTUs and PLCs, are informally referred to as the "Industrial Internet of Things (IIoT)," a term associated with the manufacturing industry.



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

Master terminal unit (MTU) or **SCADA Master** is the component in charge of collecting all data from different devices, and it controls the entire process.

Safety instrumented systems (SIS) (not shown) 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. SIS are designed to provide corrective action if other elements of the control system fail or give faulty instructions.

Serial communication protocol (not shown) is the process of sending data one bit at a time, sequentially, over a communication channel or computer bus. It is found often in OT, and it is different than the IP protocol used in IT, in which packets travel in a seven-layer Open Systems Interconnection (OSI) model.

Figure 1: Basic OT Elements.

How Did OT and IT Evolve?

Though OT and IT 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" is the simplest form of machine control. Zero or one is the simplest bit of information. However, there is power in simplicity: zero and one in the binary number system provide the basis in computing to encode virtually all knowledge.[11] In addition to being built on the same binary notion, OT and IT have evolved alongside each other in similar fashion.

Mechanical Era

OT and IT were mechanically driven for centuries. OT mechanical controls include an Egyptian clock regulated by water in 250 BCE, and James Watt's steam engine governor from 1788.[12]

IT mechanical era devices include an ancient Greek computer/clock that predicted eclipses in the first century and a mechanical calculator from 1645 that could perform all four mathematical operations.[13]

Electrical Era

IT was electrically driven when the Zuse Z3 was completed in 1941 as the world's first programmable computer. The digital era of IT included the first transistorized computer, which went into operation at the University of Manchester in 1953.[14]

In OT, the electrical era is represented by relays, or manually assembled logic switches that first provided automation for industrial equipment from roughly 1900 through the 1920s. Relays are based on electromagnets and were developed in the 1830s. One of their first uses was as a telegraph signal amplifier.

Relays pass a low-powered signal through a coil to move a contact that controls a high-powered signal. Later relays were solid-state, with no moving parts. Because they were manually assembled, and many were required to drive a typical process, changes were costly to implement.

Digital Era

PLCs were developed in 1968, when General Motors wanted to find a more efficient alternative to relays for driving the assembly line. PLCs are digital, enabling changes to be made in minutes instead of days. They are also ruggedized for harsh environments. One of the first PLCs lasted 20 years on an automotive line.[15]

PLCs can range from small modular devices with tens of inputs and outputs (I/O) to large rack-mounted devices with thousands of I/O, which are often networked to other PLC and SCADA systems.

Why Is OT Converging with IT?

As digital technologies advance, IT solutions can add impressive value when integrated with OT operations. As a result, cyber and physical control systems are converging. Gains run across all industries: Organizations scoring in the top quartile of digital transformation obtained almost twice the margins and profits of the bottom quartile.[16]

Figure 2 shows some of the ways that new digital technologies in an OT environment can optimize decision-making, improve safety and reliability, optimize operations, improve customer experience, and create new value.

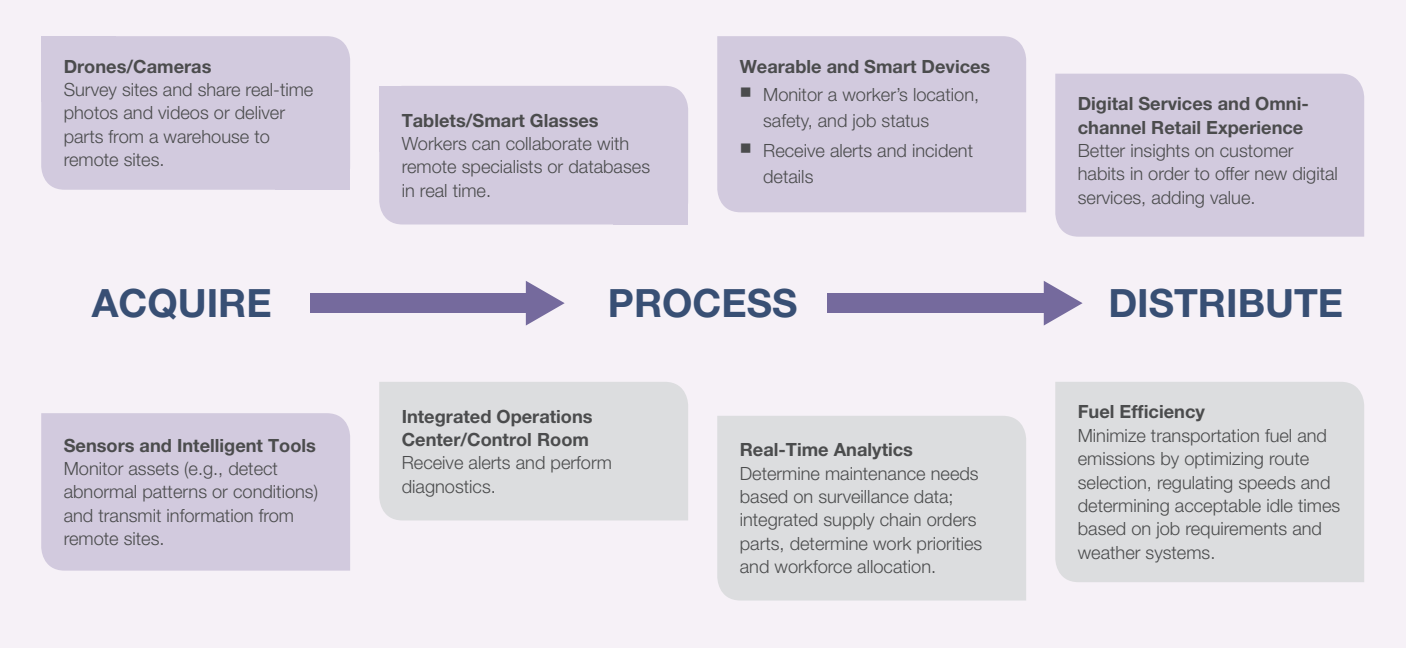


Figure 2: Options and Benefits in Digitizing the Value Chain. From IP sensors to drones, new digital technologies can add value to OT environments.

Trends in Cybersecurity: Threats to OT

When controls for physical equipment connect to broader computer networks, the digital attack surface expands, allowing cyberattackers to penetrate industrial organizations in new ways. As a result, breaches are more frequent. Nearly 9 in 10 organizations using ICS indicate they have experienced a breach in those systems, with nearly 6 in 10 breached in the past year. Many of those organizations are adding to their risk by allowing partners as well as IT networks a high level of access into their OT systems.[17]

The following are representative examples of how OT environments are attacked and the ensuing damage:

German Steel Mill Suffers Massive Damage to Equipment

According to a German government report, a 2014 cyberattack in a German steel mill began when an employee opened a spear-phishing email and clicked on a link. Malware downloaded and allowed an attacker to enter the plant's business network and eventually move to the OT systems controlling the plant. Details about tactics used were not specified. Once in the OT environment, the attacker compromised a "multitude" of systems, showing expertise in industrial controls. "Failures accumulated in individual control components or entire systems," the report notes. As a result, the plant was "unable to shut down a blast furnace in a regulated manner," resulting in "massive damage to the system." Neither attacker nor motive has been discovered to date.[18]

Malware Shuts Down Operations in Major Businesses Globally

In June of 2017, allegedly state-sponsored malware known as NotPetya appeared in Ukraine and raced within hours to countless machines around the world, destroying master boot records in IT systems. It used a Windows vulnerability that many firms had not patched and combined that exploit with one that retrieved credentials out of system memory to break into other, adjacent systems. Together, the two techniques created "the fastest propagating piece of malware we've ever seen," a security researcher told *WIRED* magazine.[19] Before NotPetya was done, it had caused OT shutdowns in a prominent global shipping firm and pharma firm, among others, and triggered an estimated $10 billion in total damage.[20]

Two Dozen Utilities in America's Energy Grid Breached in State-Sponsored Attack

Between 2016 and 2018, security experts believe that as many as two dozen utilities serving America's energy grid were infiltrated by a state-sponsored team preparing for possible sabotage, according to a *Wall Street Journal* investigation.[21] Instead of striking the utilities head-on, attackers approached hundreds of contractors and subcontractors who did business with the utilities, knowing they would have no reason to suspect they might be targets for foreign agents. Strategies included planting malware on sites read by utility engineers and sending out fake resumes with infected attachments. Hackers then used impersonation and trickery to steal user credentials.

The Federal Bureau of Investigation (FBI) sought to retrace the steps of the attackers and notify possible victims. The FBI found that targets included utilities that provide power to military and strategic defense facilities as well as companies that help utilities with their industrial control systems. Once attackers had obtained credentials, they entered the utilities' corporate networks and sought to move to the OT networks that monitor and control electricity flows. The critical step was crossing the gap between IT to OT networks, which in some cases has no connection, and in others has a protected connection.

Hackers found a bridge in some utilities in the form of "jump boxes" or systems that enable technicians to move between the two networks. If the jump boxes lacked adequate safeguards, the attackers could use them to get inside the OT network. They were successful in a few cases, an ICS security executive from the U.S. Department of Homeland Security told utility executives. The breaches put attackers in position to take actions that could have temporarily knocked out power. The U.S. government warned the public about the hacking campaign in an October 2017 advisory. As of today, industry experts say hackers likely have backdoor code remaining on some systems, awaiting further orders.

Trail of Vulnerabilities Leads Attackers to Water Company's Controls

Administrators at an unnamed water utility noticed there had been unexplained valve and duct movements in its OT environment over the previous 60 days. A Verizon Breach Digest Report called the organization the "Kemuri Water Company" (KWC), and a Verizon team began an investigation.[22]

KWC supplies water to several counties, and some of its PLCs regulate chemicals that make the water safe to drink. They had been manipulated, disrupting flow rate and water service.

What exactly had happened? Verizon researchers found a trail of vulnerabilities providing clues: There were IP addresses in KWC's web application server log that had previously been involved in attacks on other organizations investigated by the Verizon team. KWC had a web-based payment application that did not require two-factor authentication. And from the web application server, a cable ran to an AS400 system that managed the OT environment. On the web server, investigators found an initialization (INI) file in KWC's payment application that contained the internal IP address and administrative credentials for the AS400 system in clear text. That meant unauthorized access to the payment application could lead directly to sensitive information on the AS400.

Apparently, that is what happened. Attackers compromised an unpatched vulnerability in the payment application and extracted 2.5 million customer records containing personally identifiable information (PII). In addition, the attackers breached the AS400 and manipulated KWC's valve and flow control application on four occasions. Fortunately, alert functionality in the valve and pipe infrastructure enabled the organization to identify and reverse the changes and minimize customer impact.

The four attacks above share similarities with other OT attacks:

Date	Cyberattack Name	Industry	Place	Effect	Defenses Needed
2018	TRITON[23]	Energy	Middle East	Petrochemical facility underwent safety system shutdown as result of a malware attack targeting Schneider	Segmentation, traffic visibility, and threat analysis between IT and OT networks
2017	WannaCry[24]	Manufacturing Banks Government Healthcare	Globe	Exploited Microsoft server message block (SMB) protocol, encrypting with $300 bitcoin ransom, affecting 200,000 systems worldwide, including production systems of major aerospace manufacturer	Patching, segmentation, advanced threat protection
2015	Industroyer[25]	Energy	Ukraine	Phishing email planted malware, spoofed data caused power outage for 250,000 people	Email protection, segmentation, traffic visibility and threat analysis, control access by users and devices
2013	New York Dam Attack[26]	Water	U.S.	Allegation that Iranian hackers compromised dam's command and control system using cellular modem	Segmentation, control access by users and devices
2010	Stuxnet[27]	Energy	Iran, then spread	Infected USB flash drive introduced worm that used zero-day flaws to find and sabotage its target: centrifuges creating nuclear material	Segmentation, traffic visibility, threat analysis, and policies controlling removable media

Table 2: Examples of Disclosed OT Cyberattacks.

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.
- The cultural gap between IT and OT generates safety and security risks within organizations. In particular, organizations where OT and IT are divided are more 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 (e.g., ransomware and worms) are making their way into OT systems and are traversing laterally, as no real segmentation is in place to slow their spread.
- Attackers are gaining expertise in OT sabotage. They are developing, selling, and buying specialized toolsets designed to penetrate OT protocols and equipment.
- Nation-states are the biggest threat actors and have demonstrated an ability to inflict global damage.
- Lack of segmentation is the most exploited vulnerability, especially lack of or inadequate segmentation between IT and OT networks.
- Spear phishing, compromised endpoints, and stolen credentials are a common attack vector. This underlines the value of two-factor authentication, employee security education, and continuous system monitoring for indicators of compromise (IOCs).

The Fortinet Cybersecurity Solution for OT/IT

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, the desired end state is an environment optimized to respond to all manner of threats across both OT and IT.

It is common to deploy best-of-breed point security solutions to solve different security challenges. However, point security solutions are not integrated and work in silos. As a result, security becomes complex and difficult to manage, as shown in Figure 3.

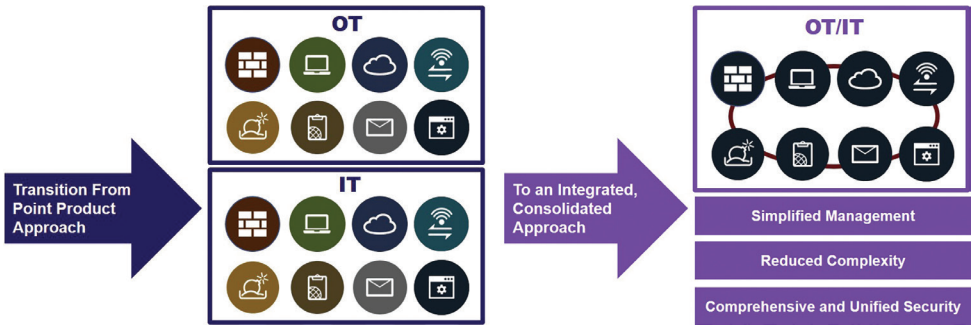


Figure 3: The Need to Bring OT and IT Security Together. A point-product security approach, with different security products in IT and OT environments, adds complexity, is difficult to manage, and introduces security gaps. A unified solution simplifies management and reduces complexity.

What is needed is a communication backbone between different security solutions. The Fortinet Security Fabric, as shown in Figure 4, provides:

- **Broad visibility** of the entire digital attack surface
- **Integrated protection** across all devices, networks, and applications, sharing global intelligence on advanced threats
- **Automated operations and response,** driven by machine learning
- **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 5).

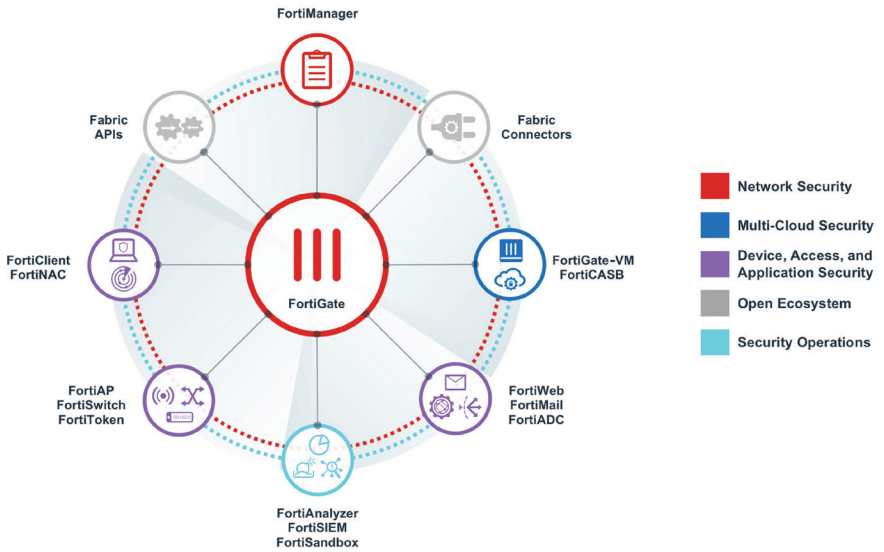


Figure 4: The Fortinet Security Fabric for OT and IT. The Fortinet Security Fabric provides broad visibility of the entire attack surface, integrated protection that shares global and local threat intelligence, and automated operations and response.

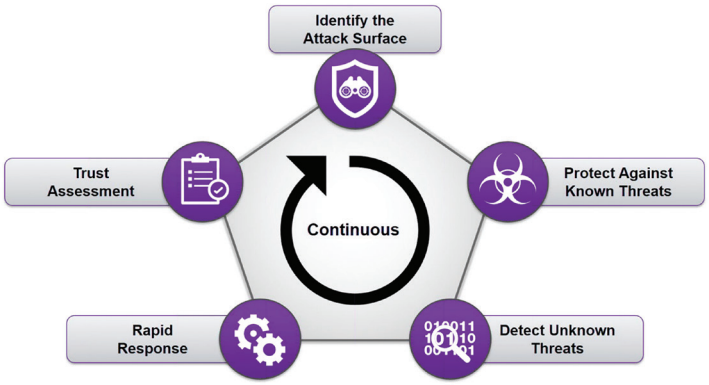


Figure 5: Framework for Digital Transformation Security. Continuous trust assessment from multiple points in the network enables faster detection and automated responses, minimizing mitigation time.

Security Fabric Safeguards for OT

In an OT environment, the Fortinet Security Fabric provides network visibility by authenticating and classifying devices. Unlike other security solutions, it does this without scanning—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 fabric 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.

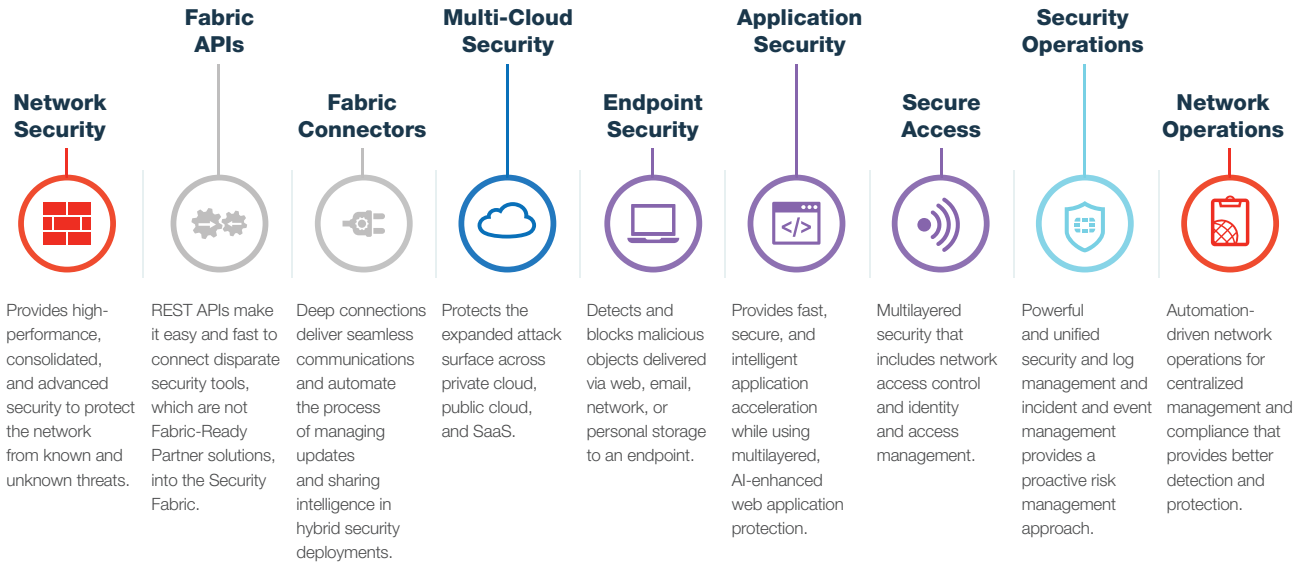


Figure 6: The Fortinet Security Fabric Realized for the Converged OT and IT Organization. Broad visibility from integrated security solutions, which also share local and global threat intelligence, provides a security foundation for organizations with IT and OT environments. For a list of OT security needs matched to Fortinet offerings, see the Appendix.

Fortinet OT Expertise

For more than a decade, Fortinet has been protecting OT for 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.[28]

One key OT differentiator is FortiGuard Industrial Security Services, which continuously updates signatures to identify and police most of the common OT protocols for granular visibility and control.[29] Additional vulnerability protection is provided for applications and devices from major OT manufacturers. This combination provides more sophisticated application control of the traffic between zones on an OT network, and it enables the FortiGate next-generation firewall (NGFW) to detect attempted exploits of known vulnerabilities. OT environments are known to operate with minimal or periodic patching, so being able to detect and block attacks on known vulnerabilities is important.

The intelligence delivered through FortiGuard Industrial Security Services comes from the global FortiGuard Labs development team, with 200-plus researchers working to provide real-time protection against advanced threats (see Figure 7).[30] This award-winning team combs through a constant stream of data from nearly 3 million sensors and hardware 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.

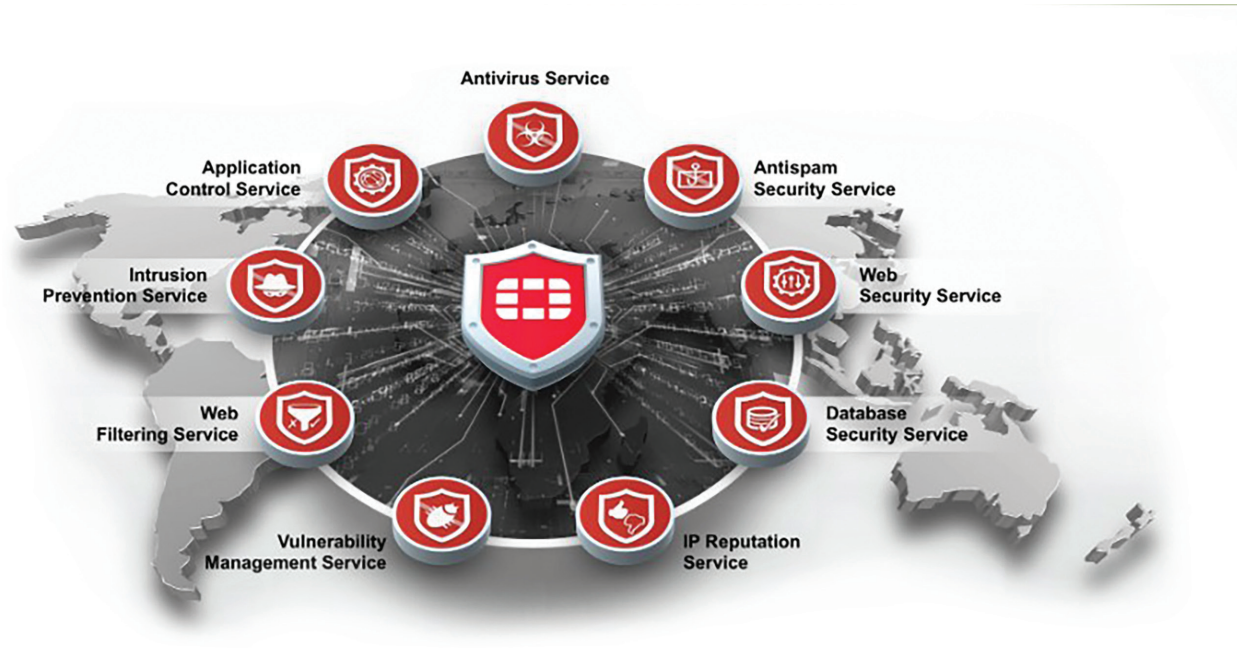


Figure 7: FortiGuard Labs Security Services. FortiGuard Labs includes 200-plus experts using in-house and patented technologies to provide real-time security services.

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

These assumptions enable OT security teams to implement a more proactive approach to identifying and neutralizing access to critical and highly valued OT assets. They also encourage processes for fast recognition of actions that are beyond normal. Proactive security needs to be engineered directly into the environment. Next is a closer look at what that entails.

Best Practice #1: Identify Assets, Classify, and Prioritize Value

A security team cannot protect assets it cannot see. This results in a critical security gap for many organizations: 82% are unable to identify all the devices connected to their networks.[31]

The first step in improving OT security posture is to have an up-to-date inventory of devices and applications running on a network. This can be accomplished via a complementary Fortinet Cyber Threat Assessment, which is available to qualified customers.[32] It begins by using a FortiGate NGFW or FortiNAC on-premises appliance to passively observe network traffic, identifying and profiling devices on your network based on their characteristics and behavior. The resulting report:

- Notes high-risk applications
- Detects and identifies top exploits of application vulnerabilities
- Identifies indications of malware, botnets, and devices that may be compromised
- Categorizes applications and analyzes their network usage

An up-to-date inventory of devices and applications on the network serves as a foundation for planning security architecture. It enables best practices to be deployed based on an organization's particular needs.

Best Practice #2: Segment the Network

Frequently, a key step to improve OT security posture is network segmentation. It is one of the most effective architectural concepts for protecting OT environments.[33]

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 firewall defines and enforces the zones, and it also defines conduits, which are channels that enable essential data and applications to cross from one zone to another.

This architectural model of zones and conduits greatly reduces the risk of intrusion. It also limits the potential impact of a breach by restricting an attacker's ability to move in an "east-west" or lateral direction. Users or devices authorized for a specific activity in a specific zone are limited to operating within that zone.

Intent-based Segmentation Is Dynamic

The model of zones and conduits needs to be dynamic rather than static, because trust assessments evolve. Traditional segmentation assumes unchanging, static trust values for users, devices, and applications. In reality, the trustworthiness of all these elements changes frequently, either due to normal changes in business operations or the result of developing threats.

Therefore, Fortinet Intent-based Segmentation is dynamic. It provides granular access control that continuously monitors trust levels and adapts security policies accordingly. Organizations can intelligently segment network and infrastructure assets regardless of their location, whether on-premises or on multiple clouds. High-performance, advanced security isolates critical IT assets to ensure quick detection and prevention of threats using analytics and automation capabilities found in the Fortinet Security Fabric. Access controls change automatically as trust levels do because they query an external trust database that collects continuous trust assessment.[34]

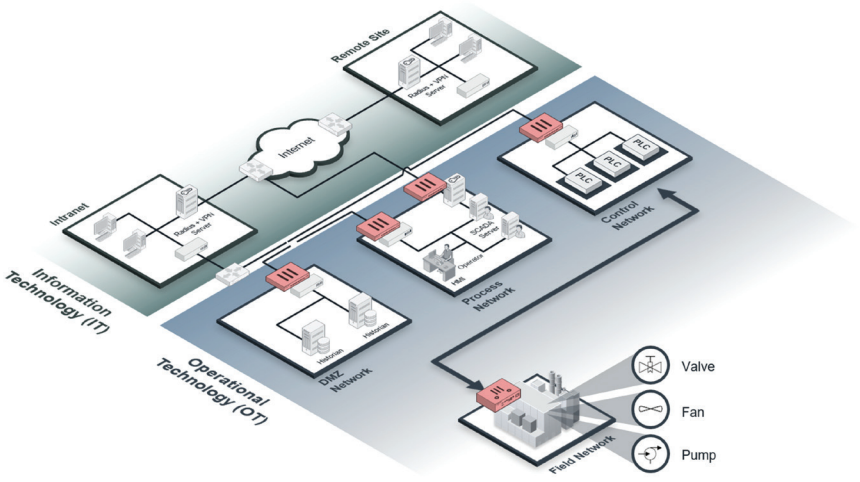


Figure 8: Segmented IT and OT Networks. FortiGate NGFWs segment the network into zones and enable analysis and control of traffic whether it uses OT or IT protocols.

Intent-based Segmentation Is Critical for OT Networks

If a network breach occurs, Intent-based Segmentation restricts an attacker's movement and impact. Traditional OT networks lacked restrictions—especially those that were air-gapped from IT networks. Some OT networks have implicit trust, making it possible for any PLC in the network to be controlled from a single administrator's laptop.

Segmentation in an OT network minimizes exposure to attacks, and therefore, it is a recommended best practice for securing OT as described in ISA/IEC-62443 (formerly ISA-99) security standards.[35] The standards were created by the International Society of Automation (ISA) as ISA-99 and later renumbered to 62443 to align with the corresponding International Electrotechnical Commission (IEC) standards.

How should OT networks be segmented? ISA/IEC-62443 standards provide practical guidance. Each zone can be assigned a security level from 0 to 4, with 0 representing the lowest level of security and 4 the highest. Strict access controls limit access to each zone and conduit based on the authenticated identity of the user or device.

The zone and conduit strategy and Intent-based Segmentation capabilities can be enforced by Fortinet NGFWs, and in particular, the Internal Segmentation Firewall (ISFW).[36] Whereas perimeter firewalls are focused on defending a border, FortiGate ISFWs sit between two or more points on the internal network and analyze traffic packets. They provide:

- Authentication, user, and device controls
- Intrusion detection and prevention
- Inspection and control for allowed and disallowed applications
- Antivirus/anti-malware protection
- Other customizable security policy features
- The ability to log traffic and record packet captures when required

The FortiGate ISFWs protect against malicious files, applications, and exploits. And they provide this visibility and protection at multi-gigabit speeds, without slowing down the network.

Best Practice #3: Analyze Traffic for Threats and Vulnerabilities

Once firewalls divide an OT network into zones, segments, and conduits, it is valuable to analyze network traffic to detect known and unknown threats.

The first requirement is to make traffic visible. The Fortinet Management and Analytics solution delivers this capability. It integrates information from the core elements of the Fortinet Security Fabric:

- FortiManager for device and policy management
- FortiAnalyzer for reporting and analytics

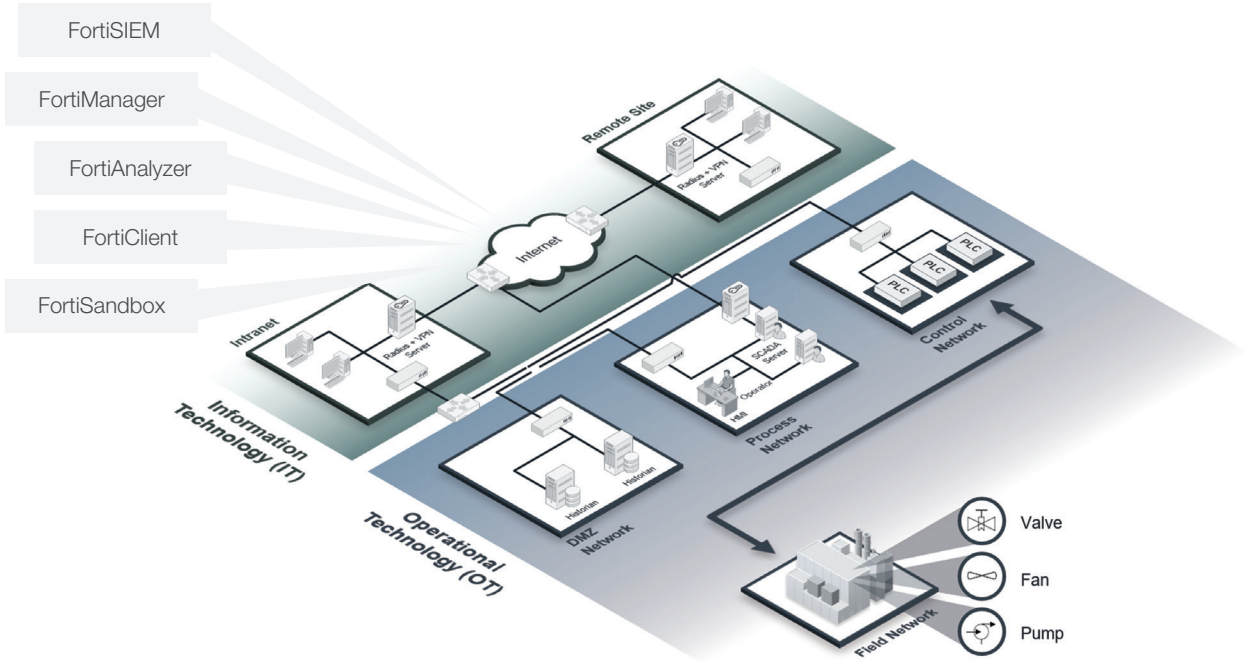


Figure 9: Inspecting Traffic for Known and Unknown Threats. The Fortinet Management and Analytics solution analyzes traffic and ensures real-time dissemination of alerts and responses among all devices in the network.

- FortiGate NGFWs for control and security policy enforcement
- FortiClient for advanced endpoint protection
- FortiSandbox for advanced persistent threat protection
- FortiSIEM (security information and event management) to build a model and record of traffic across IT and OT environments, including third-party elements.

FortiSIEM enables visibility by automatically discovering everything attached to a network—even as devices join or leave or move from one location to another. FortiSIEM establishes baselines and continually monitors changes.

It also builds a configuration management database (CMDB) of IT and OT networks, providing adaptive awareness across them.

Traffic in OT networks is made visible by integrating **FortiGuard Industrial Security Services** with FortiGate NGFWs. FortiGuard Industrial Security Services continuously update signatures on the NGFWs that enable them to identify and police most of the common ICS/SCADA protocols. (See Figure 10 for a partial list of popular protocols and applications supported. A more extensive list is also available.)[37]

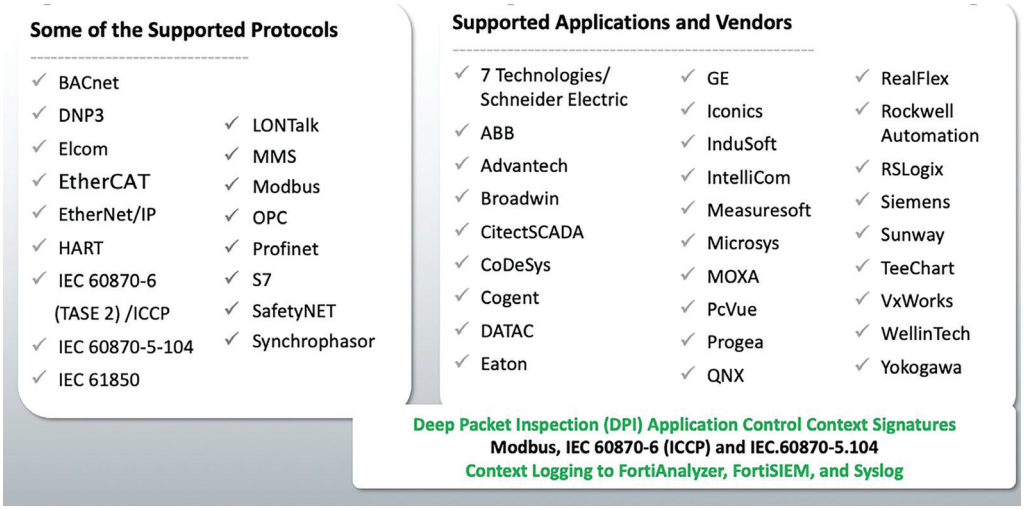


Figure 10: OT Support with Fortinet Industrial Security Services. Fortinet Industrial Security Services feed updated signatures to the FortiGate NGFW, enabling it to provide granular cybersecurity and control and detect attempted exploits of known ICS vulnerabilities.

Beyond enabling visibility, Fortinet Industrial Security Services provide additional vulnerability protection for applications and devices 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 run without patches, having the ability to catch these exploits and protect against them—providing "virtual patching"—is valuable.

FortiClient integrates with FortiGate NGFWs to provide visibility into all endpoint devices. When a vulnerability is detected, FortiClient triggers an alert in an OT environment. In an IT environment, FortiClient can do more—it can also patch the vulnerability or shield it and quarantine the rogue device. And thanks to policy-based automation, containing threats and controlling outbreaks happens immediately and automatically. Intelligence is shared with the entire Fortinet Security Fabric network.

In independent tests by NSS Labs of advanced endpoint protection from 20 vendors, FortiClient demonstrated a 100% block rate on exploits, document- and script-based malware, as well as web and offline threats, all with zero false positives. FortiClient has received NSS Labs' coveted "Recommended" rating since this test's inception in 2017, and in 2018, it received an overall security effectiveness rating of 97.3%.[38]

Getting the Big Picture

Network traffic should not only be visible, it needs to be presented in context with network events. Many log analysis and SIEM vendors require administrators to provide this context manually, cross-referencing security alerts with operational data. This type of analysis quickly becomes stale and highly prone to human error, in addition to being prohibitively time-consuming for OT and IT teams that are overstretched.

Instead, traffic should be automatically correlated with data from other relevant devices on the network. It should be presented with an understanding of device relationships and norms. To accomplish this, Fortinet has developed an intelligent infrastructure and application discovery engine. It is able to 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 CMDB in FortiSIEM enables sophisticated, context-aware event analytics using CMDB objects in search conditions.

The Fabric View dashboard in FortiManager 6.0 draws on this and other data to present the big picture: a unified perspective for both security and network operations teams. Through this dashboard, administrators can obtain an accurate, up-to-the-minute status on every device in the organization's Security Fabric. In particular, security teams can use the feed of operational data from the FortiSIEM CMDB to accurately assess the scope of security alerts and issues. Operations 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 security team requests to reconfigure or quarantine network assets.

The fabric topology of the Fortinet Management and Analytics solution ensures real-time dissemination of alerts and responses among all devices in the network. This, combined with a real-time global intelligence feed from FortiGuard Labs, enables security teams to identify even new and sophisticated threats, thus stopping them in their tracks.

Automating and Streamlining Responses

Managing a security incident typically involves multiple steps and touchpoints: a security analyst, an internal or external IT service management (ITSM) team, and the operations team. To minimize response times, the Fortinet Management and Analytics solution automates nearly every part of the workflow.

One part of the workflow is ITSM. Fortinet is working with various ITSM vendors to create seamless integration between their software and Fortinet management consoles. For instance, security incidents in FortiAnalyzer or FortiSIEM can be automatically passed to an organization's existing ServiceNow Security Incident Response system. Analysts working from the ServiceNow platform can determine how to resolve an incident and choose from a catalog of responses. Any responses that change device configuration are automatically implemented through FortiManager. This reduces response times to minutes rather than days.

Automation makes processes happen faster, and AI can optimize those processes based on new patterns of cyber-criminal behavior. Fortinet's FortiGuard Labs has been developing and training its FortiGuard AI self-evolving threat-detection system using supervised ML techniques. FortiGuard AI autonomously collects, analyzes, and classifies threats, and subsequently develops highly accurate defensive signatures to block them in rapid succession. It then disseminates the 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 discovered after they have already caused harm somewhere in the world. The FortiGuard Indicators of Compromise (IOCs) 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, which is delivered daily to FortiAnalyzer and FortiSIEM devices. Armed with this global threat intelligence, security analysts can scan weblogs to identify past communications with servers that are now known to be malicious. They can work with the operations team to mitigate the impact of such communications.

Another important category of threat is found inside the company: 30% of data breaches involve organization insiders acting negligently or maliciously. FortiInsight protects organizations from insider threats by continuously monitoring users and endpoints with automatic detection and response capabilities. Leveraging ML and advanced analytics, FortiInsight automatically identifies noncompliant, suspicious, or anomalous behavior and generates an alert about any compromised user accounts.

Responding to Advanced Persistent Threats

With the stakes for OT intrusion so high, it is essential to prepare for attacks which 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 and the local intelligence is shared in real time with Fortinet and third-party, vendor-registered devices and clients to remediate and immunize against new advanced threats.

Quantifiable Security for Better Decision-making

With Fortinet security solutions in action, network operations analysts or security architects are often called on to demonstrate results. They may need to respond to demands for proof of compliance or to executive requests for clear information on security posture. And nearly every executive wants to know, "How secure are we?"

The Security Rating feature in FortiAnalyzer helps security architects answer this question competently and efficiently. Fortinet has leveraged its deep experience in the security industry to develop a series of tests, based on the most important security best practices, which run repeatedly on the deployed FortiGate NGFWs. The results are presented as a cumulative companywide score, called a Security Rating, as well as a prioritized list of issues to be resolved (see Figure 11).

Security Ratings can be tracked over time to indicate trends and show the return on investment of various security initiatives. Also, because every organization must balance the need for security controls with the network performance demands of the business, the Security Rating provides two forms of context to support risk tolerance analysis.

First, the Security Ratings trendline (the red line in Figure 11) can be plotted on a timeline of known threats, which demonstrates due diligence in protecting against those threats. Second, the trendline can be compared with an appropriate industry average trendline (the blue line in Figure 11, delivered through a FortiGuard service). This offers a real-world assessment of the organization's security posture. This is a useful metric for top management and the board of directors.

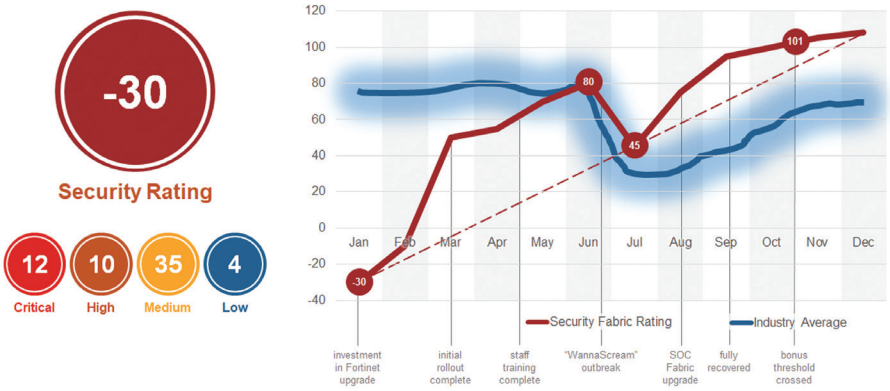


Figure 11: Fortinet Security Rating Feature. The Security Rating feature provides point-in-time and trend analysis as well as comparison with industry averages.

Best Practice #4: Control Access by Users and Devices

Devices, users, and applications need to be authenticated before they can access OT network segments. Secure authentication is critical: 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. Several solutions in the Fortinet Security Fabric work together to validate who and what is connecting to your network and limit their access to only appropriate resources.

Who Is Connecting?

When users connect, FortiAuthenticator validates their identities. It simplifies and centralizes the management and storage of user identity information and applies 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 range of two-factor authentication tokens for 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.

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 user identity-based security without impeding the user or generating work for network administrators.

FortiAuthenticator builds on the foundations of Fortinet 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 access permissions from third-party systems, and communicates this information to FortiGate devices so they can enforce identity-based policies.

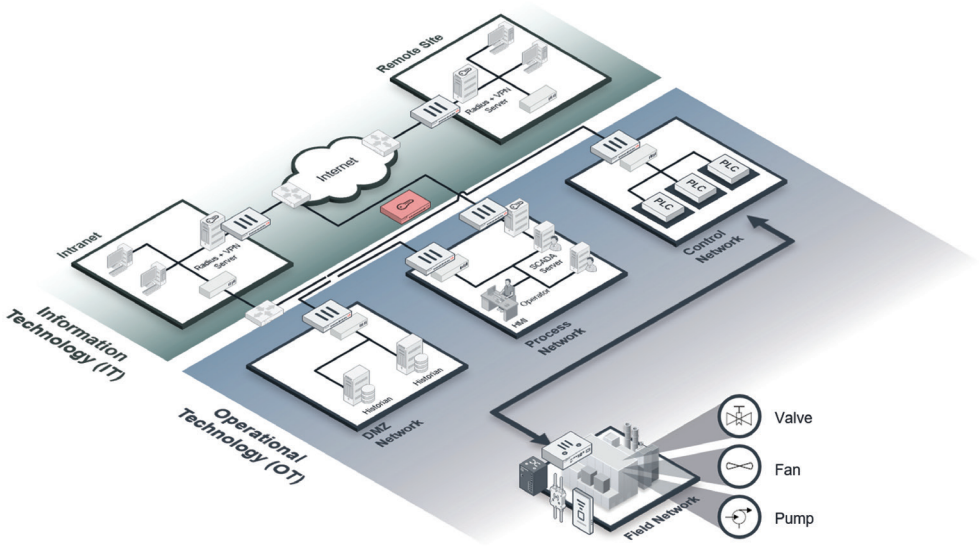


Figure 12: Enable role-based access control for users, devices, applications, and protocols using FortiGate, FortiAuthenticator, and FortiNAC.

What Is Connecting?

The Fortinet Security Fabric can passively 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.

One of FortiNAC's roles in the Security Fabric is to identify network users and devices. FortiNAC then implements appropriate role-based network access policies to protect critical data and sensitive assets while ensuring compliance with internal, industry, and government regulations and mandates.

To further protect networks, FortiNAC can lock down ports as desired: No devices or applications are allowed unless they are permitted. A port will not provide network connectivity until the connecting device is authorized. This can enforce a policy that any device added to an OT network must first be approved by authorized staff.

FortiNAC uses dynamic role-based network access control to logically create network segments by grouping applications and like data together to limit access to a specific group of users. It can implement segmentation policies and change configurations on switches and wireless products from more than 70 vendors, extending the reach of the Security Fabric. In this manner, if a device is compromised, its ability to travel in the network and attack other assets will be limited. The Security Fabric can trigger an alert to authorized staff. The Security Fabric could also be configured to respond automatically and contain the device in real time. Automating this entire process reduces the containment time from days to seconds.

Best Practice #5: Secure Both Wired and Wireless Access

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 increases the digital attack surface. Wireless access points (APs), as well as network switches, are attractive targets for cyberattacks. Both 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 not only reduces risk but also improves visibility and minimizes administration time for security and operations teams. Fortinet gives organizations with OT environments two options for centralizing wired and wireless access management.

Option 1: Streamline Access Management with FortiSwitches and FortiAPs

Through a single interface in a FortiGate NGFW, a security or OT team can push firewall capabilities and policies to ports on FortiSwitches and FortiAPs throughout the organization. The proprietary FortiLink protocol creates a secure tunnel between APs and the firewall to protect and encrypt traffic. The 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. No known competitive solution offers these capabilities without requiring additional hardware and complex configuration.

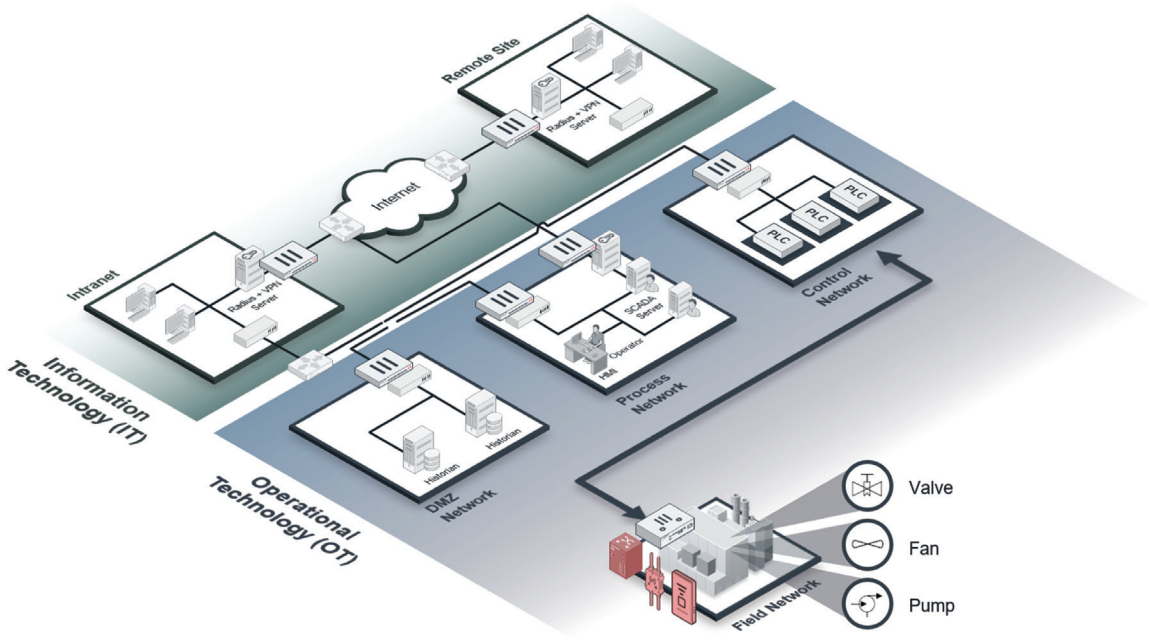


Figure 13: Centralizing Switch and Wireless AP Management. Enable secure wired and wireless access with FortiSwitch and FortiAP, controlled from a single console.

Centralized monitoring of switch and AP security also simplifies compliance reporting. And the integration of switches and APs 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.

Option 2: Simplify Management of Third-Party Switches and APs

Organizations can protect their investments in legacy switches and wireless APs by centrally managing and provisioning them from FortiGate NGFWs. FortiNAC can configure third-party switches and wireless APs, including devices from more than 70 vendors. The solution writes to command-line interfaces (CLIs), APIs, or uses other protocols to set up VLANs and quarantine devices when appropriate.

Protection for Extreme Conditions

When switches and APs are used in an OT environment, they must be able to perform and not degrade even in harsh conditions. They should:

- Be resilient, sturdy, and capable of withstanding intense temperature fluctuations
- Have a mean time between failure (MTBF) greater than 15 years for APs and 25 years for switches
- Offer fanless passive cooling (switches)
- Use Power-over-Ethernet (PoE) capability to simplify installation of cameras, sensors, and wireless APs in the network, with power and data delivered over the same network cable, lowering total cost of ownership (TCO)
- Come in form factors designed in accordance with international substation automation standards, IEC 61850-3 and IEEE 1613

Ruggedized versions of FortiSwitches, FortiAPs, and FortiGate NGFWs are designed to meet these requirements.[39, 40, 41] They enable organizations to centrally create defenses at the far edges of the network, where cyber criminals are most likely to attack because they expect less security. The solutions are also ready for extreme conditions typical of remote locations. A failure of equipment at the network edge is not just an annoyance; it can mean costly critical downtime and time-sensitive deployment to resolve the equipment failure.

Simplifying and Automating Compliance Reporting

Compliance is a critical part of an OT cybersecurity strategy. While a compliant OT environment is not necessarily a secure one, it *is* an important starting point for getting the right security architecture in place.

Compliance initiatives differ by sector. See Table 3 for examples of prominent initiatives.

Sector	Region	Regulatory Initiative
Manufacturing	U.S.	NIST Cybersecurity Framework
	EU	NIS Directive
Energy and Utilities	U.S.	NERC Cybersecurity Standards
	EU	NIS Directive Tool for Energy
Transportation	U.S.	TSA Cybersecurity Roadmap
	EU	NIS Directive Tool for Transport

Table 3: Sample Cybersecurity Initiatives by Sector.

OT compliance has become more prescriptive over the course of time to include costly penalties for noncompliance. Deploying the Fortinet Security Fabric enhances compliance because its capabilities address a number of the SANS Institute's top 20 critical security controls, such as visibility, access control, and secure configuration.[42] Here are some examples:

Visibility

FortiSIEM can provide a single pane of glass for monitoring all aspects of OT and IT environments, including security, performance, availability, and change. It can provide details as to whether they are in compliance with relevant security regulations (see the Auditability section).

Access Control

FortiAuthenticator tracks user activities to comply with security policies and enables multiple authentication technologies for restricting user access, including two-factor authentication, identity verification, and network access control.

FortiNAC authenticates devices and users and locks down the network, restricting port access to only devices and applications that are approved.

Secure Configuration

FortiManager enables enforced fields, which can be configured to ensure consistency and enhance compliance with policies. Log management policies can be set so logs cannot be deleted.

Auditability

Use the **FortiGuard Security Rating Service** to indicate where noncompliance may have occurred, identifying shortfalls and simplifying reporting.[43] The service also enables the tracking and comparison of a security score against peer/industry groups, with explanations of what is behind the score.

FortiSIEM offers out-of-the-box, predefined reports supporting a wide range of compliance auditing and management needs including PCI DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13, and SANS Critical Controls.

High-Level Architecture: Planning OT Security by Purdue Model Layer

When developing a cybersecurity plan for an OT environment, it is useful to map security capabilities against the Purdue Enterprise Reference Architecture, which was developed by the Purdue University Consortium for Computer Integrated Manufacturing in the 1990s. Figure 14 shows the Purdue model from level 0, the physical OT process itself, up through level 5, the enterprise IT infrastructure.

In the Purdue model, the **Cell/Area Zone** consists of:

Level 0: High-value physical assets involved with the process, controlled by sensors and actuators.

Level 1: Basic, intelligent devices that sense and manipulate physical processes, such as PLCs and RTUs.

Level 2: Area control systems that supervise and monitor the processes, including HMIs and SCADA masters.

Manufacturing Zone consists of:

Level 3: Site manufacturing operations systems that manage flow to produce the desired output. Level 3 may also contain the operational historian, a database capturing supervisory control, performance monitoring, and quality assurance metrics.

Enterprise Zone consists of:

Level 4: Site business planning and logistics applications, including ERP, scheduling, material use, shipping, and inventory levels.

Level 5: Enterprise IT infrastructure and applications used by the controlling organization.

Different levels have different cybersecurity requirements.

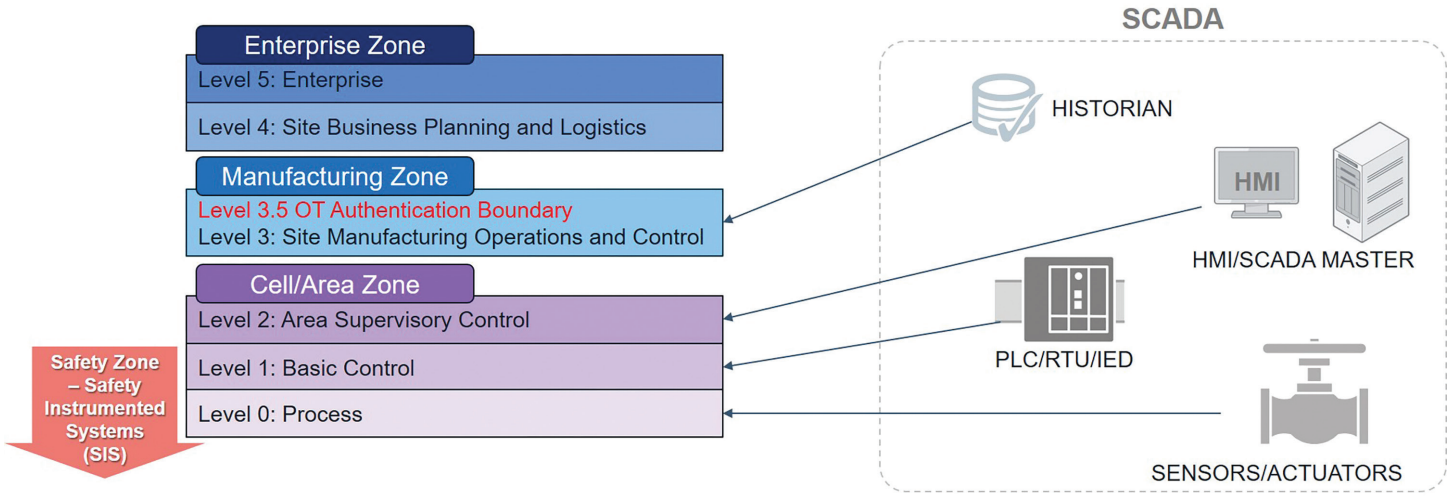


Figure 14: Purdue Model Applied to OT Environments.

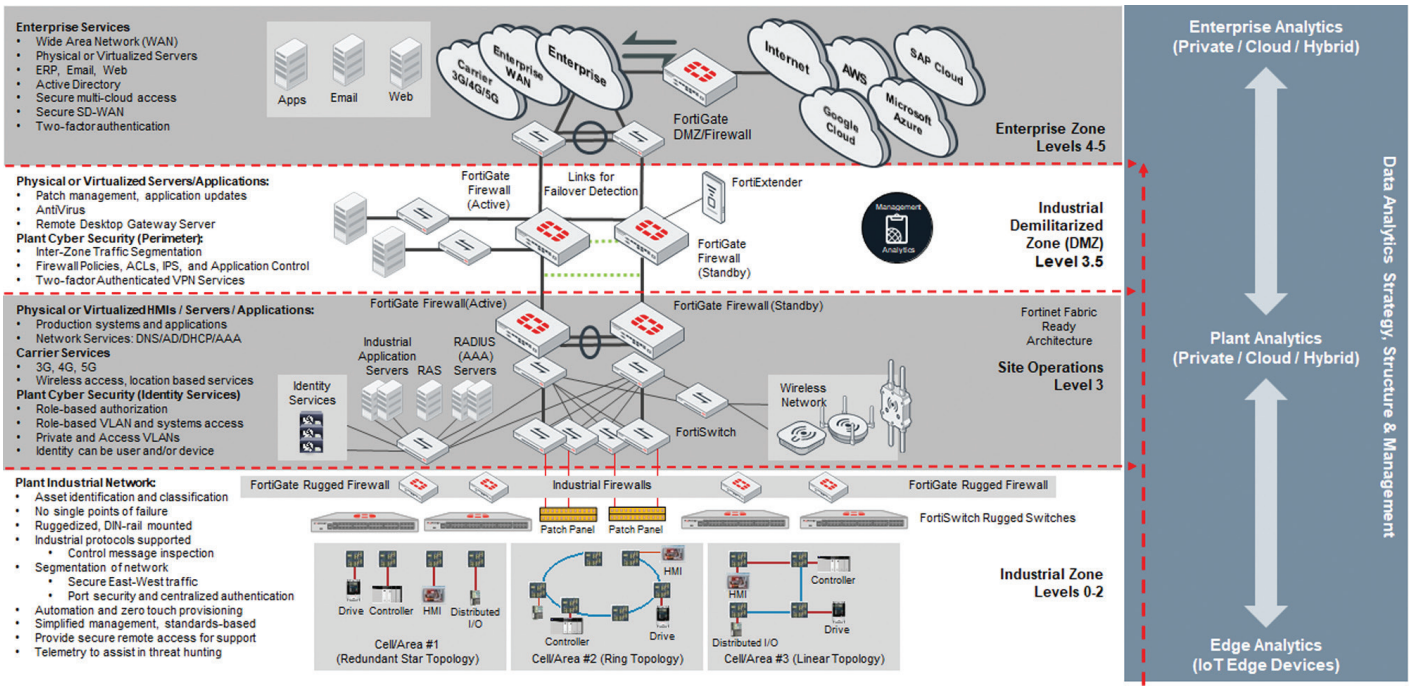


Figure 15: Fortinet Security Fabric Architecture for OT. This shows Fortinet Security Fabric architecture for OT cybersecurity mapped against the Purdue Network Model. The diagram illustrates recommended best practices, such as segmenting the network, analyzing traffic for threats and vulnerabilities, controlling access by users and devices, and securing wired and wireless access.

Next Steps: Pathway to a Security Fabric for OT

The Fortinet Security Fabric protects the digital attack surface of OT and IT networks. Deploying the Fabric is a journey to a desired state that provides visibility, integration, automation, and resilience in your security environment. The Security Fabric can be achieved in stages that are aligned with organizational security priorities. As an organization plans those stages, it is wise to incorporate these recommended best practices:

1. **Identify network assets, classify, and prioritize value** with a complimentary cyber threat assessment. The resulting up-to-date inventory of an organization's IT and OT environments facilitates security planning.
2. **Segment the network** to limit the impact of any intrusion. Lack of segmentation is the most exploited vulnerability in OT networks, especially lack of or inadequate segmentation between IT and OT networks.
3. **Analyze traffic for threats and vulnerabilities** with the ability to inspect OT protocols and centrally monitor the companywide security posture through a cumulative score—namely, the Fortinet Security Rating.
4. **Control access by users and devices** because stolen credentials are a leading tactic in penetrating OT environments. Two-factor authentication and the ability to lock down the network to authenticated users and devices are important capabilities.
5. **Secure wired (and wireless if present) access,** enforcing security policies throughout the environment from a single, central point of management.

Organizations seeking help in planning their cybersecurity journey should contact us online at www.fortinet.com/ot or email us at otci_global@fortinet.com.

Appendix: OT Security Needs Mapped to Fortinet Offerings

Need	Security Objective	Fortinet Offering
Asset discovery, visibility, profiling, and tracking	The ability to see profile, track, and manage assets	■ FortiSIEM ■ FortiNAC
Control access by users and devices	■ Manage identities ■ Control access to systems ■ Remote and privileged access ■ Identity of Things (IDoT)	■ FortiAuthenticator ■ FortiNAC ■ FortiToken ■ Fortinet Single Sign-On ■ FortiGate
Endpoint-based security	■ Protect endpoints besides computers/ mobile devices ■ Includes anti-malware, personal firewall, port and device control, encryption, memory protection, and related capabilities	■ FortiClient ■ FortiSandbox ■ FortiGate ■ FortiInsight
Network-based security	■ Managing data flow between defined networks (firewalls) ■ Unified threat management ■ Intrusion prevention	■ FortiGate ■ FortiGate ■ FortiGate IPS ■ FortiCamera/FortiRecorder
Anomaly detection and response, incident reporting	■ Detect and respond to anomalies, threats, incidents ■ Analyze behavior and report	■ FortiSIEM ■ FortiGate ■ FortiAnalyzer
Security management	■ Configuration and security-related patch management ■ Continuous assessment ■ Portable media management ■ Integration with other security management systems ■ Forensic investigation of OT security compromises and impacts	■ FortiGate ■ FortiManager ■ Fortinet Management and Analytics Solution ■ FortiClient ■ Fortinet Fabric-Ready Partner Program ■ Fortinet APIs ■ FortiSIEM
IT/OT security or OT security consulting, integration, and managed services (including cloud delivery)	Deliver assessments, strategic planning, policy development, architecture and design skills, as well as software and system integration across multiple technologies and processes Services delivered via platform, infrastructure, and/or software as a service from the cloud	■ Fortinet Partners ■ FortiGuard Industrial Security Services ■ FortiGuard Security Rating Service

Table 4: OT Security Recommendations Mapped to Fortinet Offerings.

[1] "State of Operational Technology and Cybersecurity Report," Fortinet, March 2019.
[2] "Independent Study Pinpoints Significant SCADA/ICS Cybersecurity Risks," Fortinet, May 7, 2018.
[3] Ibid.
[4] Bernard Marr, "What is Industry 4.0? Here's A Super Easy Explanation For Anyone," Forbes, September 2, 2018.
[5] Clint Boulton, "10 machine learning success stories: An inside look," CIO, December 4, 2018.
[6] Cornelius Baur and Dominik Wee, "Manufacturing's next act," McKinsey, June 2015.
[7] Ibid.
[8] Thor Olavsrud, "10 internet of things success stories," CIO, October 3, 2017.
[9] Gladys Rama, "AWS Clears the $5 Billion Mark in Q4 Earnings," AWS Insider, February 1, 2018.
[10] "Industrial control system," Wikipedia, accessed January 21, 2019.
[11] "History of binary code," Wikipedia, accessed January 21, 2019.
[12] Ernie Hayden, et al., "An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity," SANS Institute, August 2014.
[13] "Information technology," Wikipedia, accessed January 16, 2019.
[14] Ibid.
[15] "Relay," Wikipedia, accessed December 9, 2018.
[16] Robert Bock, et al., "What the Companies on the Right Side of the Digital Business Divide Have in Common," Harvard Business Review, January 31, 2017.
[17] "Independent Study Pinpoints Significant SCADA/ICS Cybersecurity Risks," Fortinet, May 7, 2018.
[18] Kim Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," WIRED, January 8, 2015.
[19] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," WIRED, August 22, 2018.
[20] Ibid.
[21] Rebecca Smith and Rob Barry, "America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It," The Wall Street Journal, January 10, 2019.
[22] Blackpiano, "Kemuri Water Company (KWC): Hackers change chemical settings at water treatment plant," I.C.F Cyber Warfare Intelligence, March 26, 2016.
[23] Lily Hay Newman, "Russia Linked to Disruptive Industrial Control Malware," WIRED, October 23, 2018.
[24] Josh Fruhlinger, "What is WannaCry ransomware, how does it infect, and who was responsible?," CSO, August 30, 2018.
[25] Charlie Osborne, "Industroyer: An in-depth look at the culprit behind Ukraine's power grid blackout," ZDNet, April 30, 2018.
[26] Mark Thompson, "Iranian Cyber Attack on New York Dam Shows Future of War," TIME, March 24, 2016.
[27] Josh Fruhlinger, "What is Stuxnet, who created it and how does it work?," CSO, August 22, 2017.
[28] "Fortinet Launches New Rugged, Industrial-Grade Devices to Connect and Secure Critical Infrastructure," Fortinet, December 9, 2014.
[29] "Industrial Control Systems," Fortinet, accessed March 15, 2019.
[30] "FortiGuard Labs," Fortinet, accessed March 15, 2019.
[31] Jeff Goldman, "IoT Security Fail: 82 Percent of Companies Can't Identify All Network-Connected Devices," eSecurity Planet, November 8, 2017.
[32] "Know Your Vulnerabilities—Get the Facts About Your Network Security," Fortinet, accessed March 15, 2019.
[33] Keith Stouffer, et al., "Guide to Industrial Control Systems (ICS) Security," NIST, May 2015.
[34] "A Network Operations Guide for Intent-based Segmentation," Fortinet, February 5, 2019.
[35] "ISA Standards: Numerical Order," International Society of Automation, accessed January 3, 2019.
[36] "Protecting Your Network from the Inside-Out," Fortinet, December 2016.
[37] "FortiOS IPS and Application Control Signatures of Industrial Environment," Fortinet, January 2019.
[38] "Fortinet Receives Recommended Rating in NSS Labs Latest Advanced Endpoint Protection Test Report," Fortinet, April 17, 2018.
[39] "FortiSwitch™ Rugged," Fortinet, accessed January 7, 2019.
[40] "Wireless Product Matrix," Fortinet 222C Wireless AP, March 2019.
[41] "FortiGate® Rugged Series," Fortinet, accessed January 14, 2019.
[42] Tim Greene, "SANS: 20 critical security controls you need to add," Network World, October 13, 2015.
[43] "FortiGuard Security Rating Service," Fortinet, accessed March 16, 2019.

FORTINET®

www.fortinet.com

March 1, 2021 11:17 AM
D:\Fortinet\Work\2021\0301\wp-operational-technology-design-guide-320863 Folder\wp-operational-technology-design-guide
320863-A-0-EN