WHITE PAPER

A Solution Guide to Operational Technology Cybersecurity

Table of Contents

Executive Summary

As new digital tools like cloud applications, artificial intelligence (AI), and smart devices improve production efficiencies and capabilities in industrial and critical infrastructure sectors, it is essential 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 any security impacts on IT functions are typically restricted to the organization itself, many components of OT are critical to public safety and global economic health.

Sensitive OT systems were traditionally isolated from common IT networks. This "air gap" protection dissolves in most organizations because the business advantages of interconnectivity are significant. The many benefits of connectivity between IT and OT systems include reducing costs, boosting productivity, and achieving a competitive advantage. The challenge is that interconnecting the environments increases exposure to cyber intrusions. Cybercriminals often target IT networks to gain access to OT systems, and attacks on power grids, shipping lines, manufacturing plants, and other types of critical infrastructure are steadily increasing.

Cyberattacks on OT systems endanger critical infrastructure, impacting global energy, water, and manufacturing.[2] Organizations around the globe are experiencing high numbers of intrusions. In a global survey of OT security professionals, nearly 50% experienced one or more incidents last year with impacts that included brand degradation, loss of business-critical data, and decreased productivity.[3]

Companies are scrambling to invest in security for their vulnerable OT infrastructure in response to greater threat activity. The OT cybersecurity market is projected to grow from $12.75 billion in 2023 to around $21.6 billion by 2028, with an approximate compound annual growth rate (CAGR) of 9.2%.[4] Network security and segmentation technologies will grow the most, followed by identity and access management and endpoint protection.

Along with market growth, some OT security postures are showing some progress in terms of maturity. According to a 2025 Fortinet survey, 26% of organizations report establishing visibility and implementing segmentation, up from 20% in 2024 and only 13% in 2023. There has also been a steady increase in organizations that have already rolled OT security under a CISO, from only 16% in 2022 to 52% in 2025.[5]

Cyberattacks on OT systems surged by 73% last year.[1]

The Fortinet OT Security Platform supports five critical use cases for protecting interconnected digital ecosystems:

1. Wide area network (WAN) security
2. Local area network (LAN) security
3. Advanced threat protection
4. Security automation, operations, and management
5. Third-party vendor integrations

Continuing investments in both IT and OT security will help prepare organizations for the latest sophisticated attacks. Today's cybersecurity infrastructure must be designed to protect the growing digital landscape from cyberthreats, share threat intelligence among security products, and automate threat responses.

This comprehensive guide explains how Fortinet effectively provides security throughout the interconnected IT and OT infrastructure, fully enables integration across Fortinet and partner security solutions, and supports security automation across the entire security ecosystem. This guide also explores how IT and OT are different yet increasingly interconnected and addresses the increased security risks arising from these integrations.

This guide also reviews how elements of the Fortinet OT Security Platform 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). It also suggests actionable next steps organizations can take on their cybersecurity journey and includes a helpful appendix that maps existing OT security needs to Fortinet OT Security Platform solutions.

The Latest Cybersecurity Trends

OT networks comprise industrial automation and control systems (IACS), also known as industrial control systems (ICS), which control and regulate equipment in industrial sectors such as manufacturing, energy and utilities, and transportation. Many ICS still in use today were originally based on proprietary technologies and deployed decades before modern IT networks. Their highly sensitive nature led to the practice of "air gap" protection. OT networks were kept safe through isolation, lacking any connectivity with IT systems or other external networks.

The air gap has eroded as organizations adopt new digital tools and technologies. Although the Internet of Things (IoT), Industrial Internet of Things (IIoT), cloud computing, AI, and other innovations help optimize operations, improve safety and reliability, and deliver a competitive edge, they have simultaneously created interconnections between OT and IT environments and beyond.

All the improved agility and efficiency that come from IT-OT interconnectivity also come with increased security 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, a cyber intrusion on OT systems can compromise industrial processes and equipment or critical infrastructure, potentially causing dire health and safety consequences if the systems are breached.

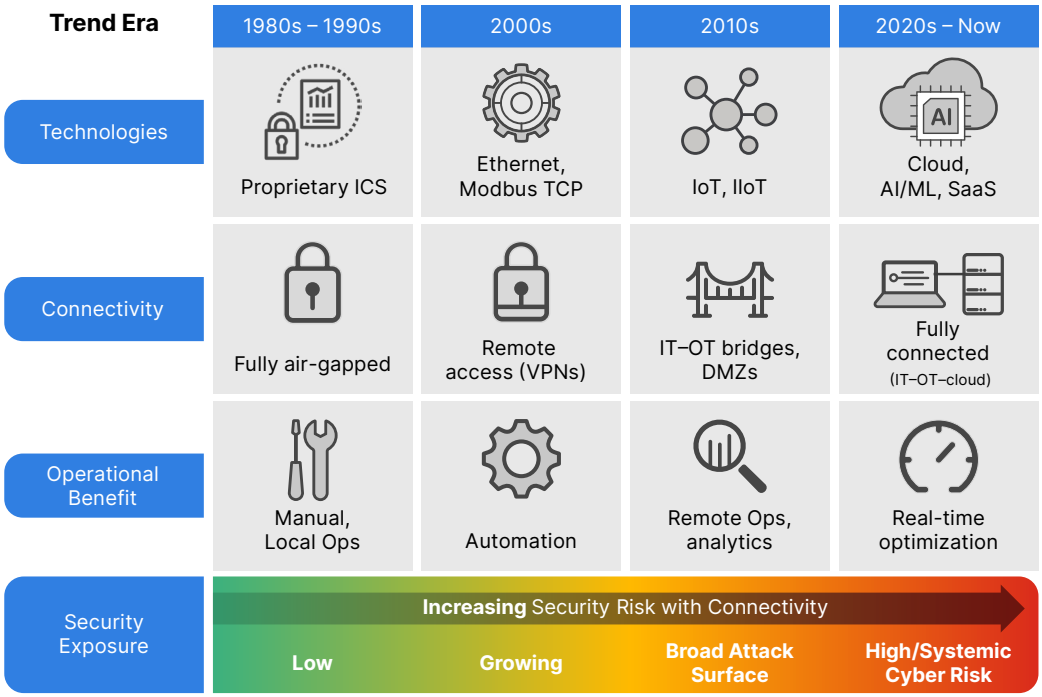

Figure 1: Air gap erosion has enabled digital transformation, but significantly increased cybersecurity risk in OT environments.

Even though many organizations have made gains in security program maturity in recent years, many OT systems remain vulnerable for a number of reasons. For example, the majority (52.6%) of the OT cybersecurity workforce has spent five years or less in the field, and less than half have earned specific certifications relevant to OT security.[6] Five key trends help frame the specific challenges of securing today's OT environments:

Increasing OT security risks: Geo-political events continue to drive targeted cyberattacks on cyber-physical systems (CPS) and critical infrastructure, such as recent attacks on satellite networks and manufacturing companies in the U.S. and Europe. Some attacks were linked to events in the Middle East, where attackers went after programmable logic controllers (PLCs) that happened to be produced in Israel and took down some small water districts.

Changes in patching: In addition to PLCs, patching needs to include the networking solutions located in the OT environment, physical security systems, such as cameras and vision systems, and the various other sensors and controllers used in production. Most OT organizations have outdated legacy devices without updates or patches, yet the business must maintain production 24×7. In many cases, it simply isn't feasible to take a system offline for weeks or months to update or maintain it. Some industries now face regulations that require patching certain issues or implementing a specific patching strategy. At the same time, patching older OT systems can lead to compatibility and interoperability issues that can be difficult to troubleshoot and impossible to fix.

Greater cloud adoption: Cloud-enabled devices within the OT perimeter will increase, and there will be a rise in IT cloud and OT dependencies as more companies move from isolated OT systems to integrated environments. Over the last several years, business process optimizations have continued to drive OT integration with industrial IT, cloud, and wireless systems. According to a recent SANS survey, 26% of organizations currently leverage cloud technologies for ICS and OT applications (a 15% increase in just one year).[7]

The majority (52.6%) of the ICS/OT cybersecurity workforce has worked in the field for five years or less. And less than half have earned specific certifications relevant to OT security.[8]

Increased 5G connectivity: Many OT environments depend on low-latency connectivity as a failover for business continuity. Today's 5G networks offer better performance and reliability than traditional broadband access or satellite connectivity. In addition, 5G adoption will increasingly be used as an industrial LAN technology for factory robotics, such as automated guided vehicles, autonomous mobile robots, and other IIoT devices. 5G is also used for mobility and OT field sites, which often exist in places where wired options don't exist, so 5G becomes the primary link.

Growth of AI in OT security: AI is already being applied in OT environments for things like predictive maintenance, process optimization, and autonomous operations. It is increasingly being used for OT security for anomaly detection, profiling network behavior, vulnerability management, and security automation and orchestration. Physical security systems will also leverage AI for access control systems, video surveillance and intelligent video analytics, environmental monitoring and threat detection, and perimeter security, such as cameras, sensors, and drones.

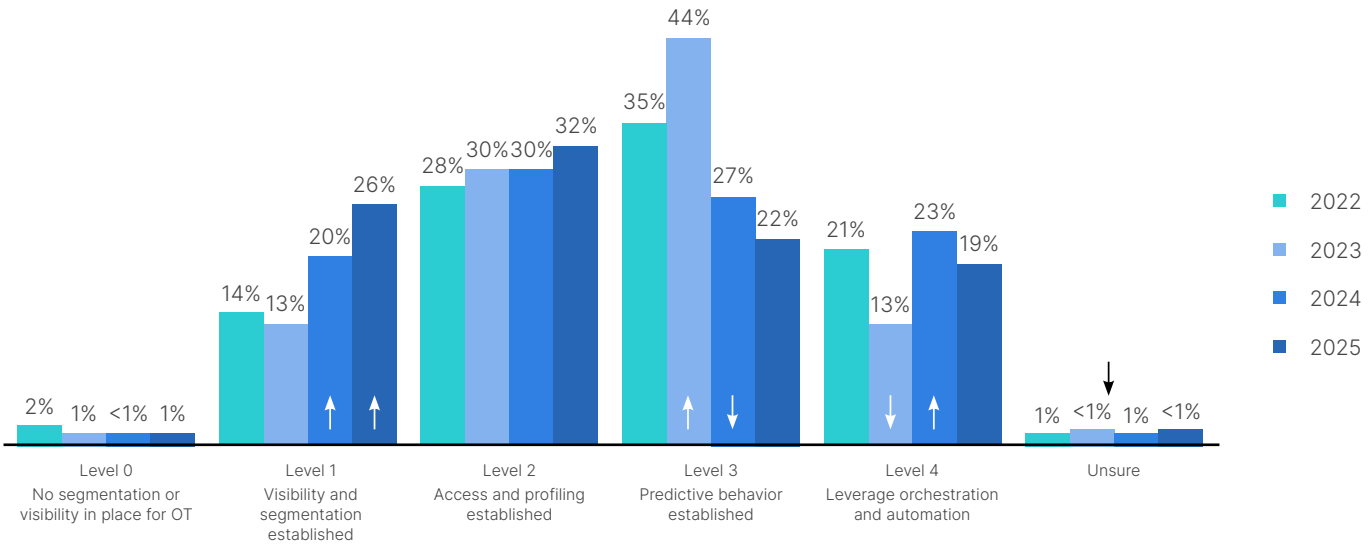

Figure 2: OT cybersecurity maturity

Cybersecurity Threats to OT

According to the *Fortinet 2025 Threat Landscape Report*, nation-state actors continue to actively use ransomware against manufacturing companies, which is the most targeted sector.[9]

Figure 3: Common attack vectors

Today's targets and threats are global in scope. Recent ICS-specific malware variants include "FrostyGoop" (which targets technology used by more than 46,000 internet-enabled ICS devices worldwide) and "PIPEDREAM" (the first ICS malware with the ability to scale attacks across systems and sectors).[10]

Cyberattacks against PLCs used by water facilities, chemical plants, and manufacturers have become very common, while espionage threats continue to threaten energy, water, transportation, and communications infrastructure.[11]

As outlined by the MITRE ATT&CK for ICS framework, specific tactics[12] (the reasoning behind an attacker's actions) and techniques[13] (how the attacker achieves their tactical goal) will vary. Still, the result of a successful OT breach is nearly always crippling for the affected organization.

Takeaways from Latest Attack Trends

Analysis of the latest attack trends offers some interesting takeaways:

- Because OT was traditionally isolated, security was not a key consideration. As a result, basic security hygiene is not implemented within many OT environments. Safety and security must be systemic within an organization to facilitate the adoption of security best practices. Organizations must consider how to systematically apply best practices to manage risk from connected OT environments.
- Unlike IT cybersecurity, which prioritizes data protection, OT cybersecurity is fundamentally concerned with physical systems' operational continuity and safety.[14]
- Spear phishing, compromised endpoints, and stolen credentials are common attack vectors, underscoring the need for two-factor authentication, employee security education, and continuous system monitoring for indicators of compromise (IOC).
- Attackers are gaining expertise in OT sabotage. They develop, sell, and buy specialized toolsets to penetrate OT networks and systems.
- Inadequate segmentation between IT and OT networks remains a critical vulnerability. As a result, malware like ransomware and worms can find pathways from IT networks to OT networks, where they are free to move laterally across the environment.
- Although detection of cyber incidents in OT environments has improved from an average of days in 2019 to hours in 2024, nearly half (44%) of organizations still lack ICS/OT-specific incident response after an attack is detected.[15]
- Less than a third of organizations have a security operations center (SOC) with ICS/OT-specific incident reporting capabilities. While much has been done to improve OT network visibility, only 12% of respondents had extensive network monitoring capabilities, the number one indicator for how quickly a cyber incident was detected.[16]

The Fortinet OT Security Platform

Securing an OT environment can seem daunting at first, but risk mitigation 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 a variety of threats that span IT and OT.

It is common practice to deploy best-in-class point security solutions to solve different security challenges. However, point security solutions don't integrate well and often work in silos. As a result, security can become complex, difficult to manage, and introduce security gaps. Point solutions also can leave asset owners saddled with technical debt. Owners have to make sure their integrations continue to perform as expected as vendors release upgrades. A platform-based approach to cybersecurity can simplify security management and reduce complexity.

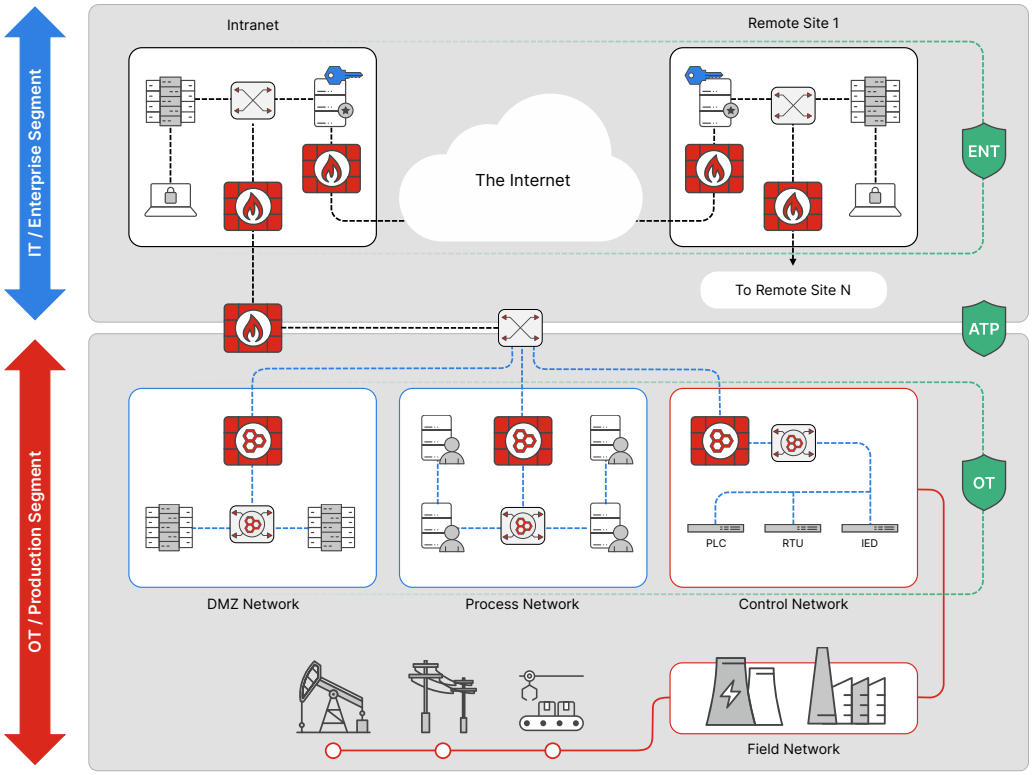

Figure 4: Interconnected IT enterprise and OT networks secured using FortiGate NGFWs

Fortinet protects IT and OT

The Fortinet OT Security Platform includes the FortiGate Next-Generation Firewall (NGFW), FortiSwitch switches, and other secure networking and security operations solutions (as shown in Figure 4). It provides convergence, consolidation, ease of management, integration, and automation for comprehensive cybersecurity protection for users, devices, and applications across all network edges. This platform enables:

- 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 network security 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 while dynamically adapting as network configurations change (see Figure 4).

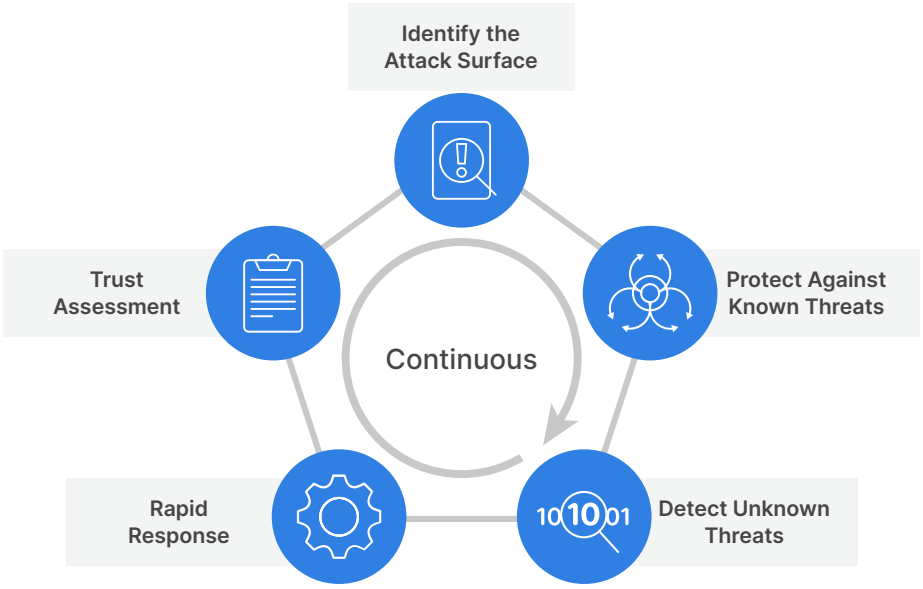

Figure 5: Framework for digital transformation security. Continuous trust assessment from multiple points in the network enables faster detection and automated responses, minimizing mitigation time.

A Platform-Based Approach to Cybersecurity

In an OT environment, the Fortinet OT Security Platform provides application and network visibility by classifying IT, OT, and IIoT devices. Unlike other security solutions, this capability is directly integrated using the FortiOS network operating system built into the FortiGate NGFW. Application and network visibility can be further enhanced by integrating other Fortinet solutions like FortiSwitch, FortiAP, and FortiExtender.

FortiOS discovers and classifies assets, including users, applications, and protocols. It then dynamically assigns them risk scores depending on their security posture. By making the environment visible, OT organizations can enable intent-based segmentation to group assets into secured network zones. The assets can be protected in zones by enforcing customized policies that are dynamically updated by continuous trust assessment. This zone-based approach allows the network to automatically grant and enforce baseline privileges for each OT asset, enabling the critical distribution and collection of data without compromising the integrity of critical systems.

FortiOS enables Fortinet Security Fabric integration to support centralized correlation of intelligence between security tools. Because of this platform integration, organizations can quickly identify anomalous behavior and send an alert, as specified, to the network operations center (NOC) or security operations center (SOC). This level of responsiveness is possible only if devices can see and share information. The Fortinet OT Security Platform can automatically wall off potentially compromised assets to contain incidents and respond in a coordinated way. In an OT environment. The OT Security platform can be configured to monitor, detect, and alert without affecting production.

Fortinet OT Customer Success Stories

For two decades, Fortinet has been offering cybersecurity solutions for OT and critical infrastructure customers in sectors such as energy, defense, manufacturing, food, and transportation.

Toyota Material Handling North America (TMH) is an industry leader in the manufacture of material handling solutions, including tuggers and forklifts. Facing an aging security infrastructure with key products falling out of license, TMH needed to increase network visibility, reduce vulnerabilities, and eliminate east-west lateral movement risks. TMH turned to Fortinet to upgrade its core and LAN networks. The company deployed FortiGate NGFWs at the network edge, FortiSwitch Ethernet switches, and FortiAP wireless access points. The FortiGate appliances are managed by FortiManager for centralized control. TMH also deployed a FortiDeceptor deception solution for OT breach protection and additional visibility. These and other Fortinet solutions immediately enabled more proactive security controls and significant time savings for the company's IT team.[17]

Nordlaks is a Norwegian breeder and marketer of premium salmon and rainbow trout. It needed to extend the Fortinet solutions protecting its existing land and sea-based operations to its newly launched sustainable sea farm. This cutting-edge stationary sea farm is a colossal 385-meter vessel that operates in the harsh conditions of the Norwegian Sea, housing a complex array of industrial monitoring and communication devices, including its network operations center. Fortinet provides ruggedized, secure network switching and wireless access as well as robust next-generation threat protection that enables Nordlaks staff to monitor the health and growth of their fish securely in real time.[18]

Siemens Switzerland supplies customers with a comprehensive array of building technologies, including fire detectors, video surveillance solutions, and access control products. Its security team needed to standardize the IT components used in customer projects, including IIoT deployments that required network segmentation using VLANs. The idea was for it to be as simple as possible to set up, centrally manage, and implement. Siemens Switzerland weighed several options before choosing Fortinet. As a result, the technical IP networks for customer projects and their operations are now protected by FortiSwitch secure Ethernet switches and FortiGate NGFWs.[19]

California Water and Wastewater District is a utility operator in California that had concerns about the security and usability of its existing OT network. The district's operations staff needed an easy-to-use system to monitor, access, make adjustments, and mitigate the additional risk of external network access. They chose a turnkey solution centered on FortiGate NGFWs and FortiSwitch switches to manage notifications, troubleshoot issues, and add and delete user credentials. Fortinet's solution improved the security of the district's OT systems and increased the safety of area residents.[20]

Herzog Technologies, Inc. (HTI) provides communications and technology services to support its parent company, Herzog, which is the only organization in the world to build, operate, and maintain every aspect of railroad transportation. Safeguarding the IT and OT systems that support many freight trains and tens of millions of passengers had become a significant burden for its lean networking team. It needed a more cost-effective way to secure, monitor, and manage those systems as a whole. HTI rolled out the Fortinet OT Security Platform and centered on FortiGate NGFWs. This solution met HTI's need for centralized threat detection, mitigation, and control while improving the reliability and cost of connectivity across the company's distributed network.[21]

RH Marine is a leading systems integrator and innovator of electrical and automation systems for the maritime industry. Serving both the defense and private sectors, the company provides a full range of solutions and services, including project management, consultancy, system design, and support. RH Marine's ongoing efforts to improve its operations' performance, efficiency, and security while maintaining the strict compliance required of a marine defense contractor led it to upgrade the network security architecture for its facilities with the tight integration of the Fortinet OT Security Platform.[22]

Your OT Security Plan

As organizations plan their OT security transformation, they should assume their organization will be compromised at some point or that it could be compromised already. The wisest organizations plan for the possibility that malware can reach an OT environment that has traditionally given attackers little constraint, the opportunity for lateral movement, and the ability to elevate privilege.

By making these assumptions, OT security teams can implement a more thorough approach to identifying and managing access to critical and highly valued OT assets. It also encourages controls that enable quick recognition of abnormal actions in the critical environment. Modern, proactive OT security must be engineered directly into these environments. The following security use cases illustrate ways an OT organization can improve the security of its IT/OT environments.

Use Cases

These security use cases are based on industry-standard recommendations and best practices to enhance security of OT and critical infrastructure environments.

Use case #1: WAN security

WAN security applies to both wired and wireless WAN connections. The external perimeter of an OT network needs to be secured as both a boundary against cyberattacks and an entry point for authorized users and network connections. For example, remote employees and third parties need access to systems to perform requisite tasks. These users may require access to retrieve records or may need to perform routine maintenance on ICS. Employees who are responsible for the upkeep of the OT infrastructure must be able to remotely monitor the uptime performance of OT assets as well as perform basic troubleshooting in the event of an issue.

As part of a secure remote access implementation, features such as multi-factor authentication (MFA) for the access and encryption of network links can be implemented. Features such as secure SD-WAN can play an important role if the control center and ICS sites are connected using multiple communication links, and it's important to maintain the availability of these links cost-effectively.

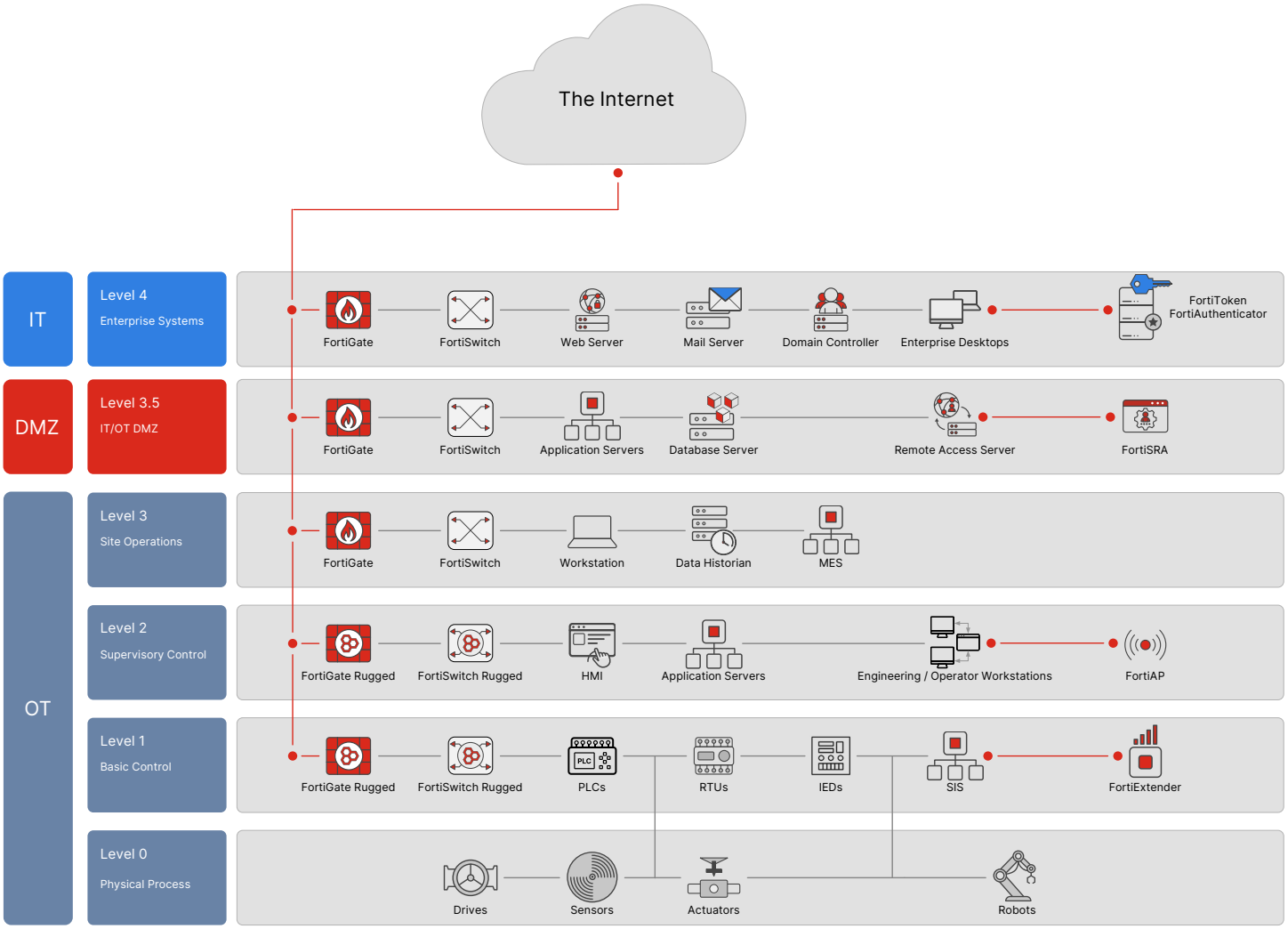

Figure 6: Fortinet WAN security is represented by the red lines in the diagram.

The specific solution capabilities required include:

- Security for wireless WAN (Wi-Fi, 3G, 4G LTE, 5G)
- IPsec, VPN
- SSL and TLS encryption
- Secure remote access
- Secure SD-WAN
- Secure access service edge (SASE)

A number of core Fortinet solutions support this use case:

- **FortiGate** NGFWs and intrusion prevention systems (IPS) enable security control and policy enforcement, IPsec, VPN, SSL and TLS encryption, and secure SD-WAN.
- **FortiAP** access points provide security for Wi-Fi networks covering both wireless LAN and WAN segments.
- **FortiExtender** establishes a bridge between LANs and wireless LTE, 5G WAN connections.
- **FortiSRA** provides secure remote access, credential management, live session monitoring and recording, secure file transfers, and role-based access control.
- **FortiToken** enables two-factor authentication with one-time password (OTP) application with push notifications or a hardware time-based OTP token. FortiToken Mobile (FTM) and hardware OTP tokens are fully integrated with FortiClient, secured by FortiGuard, and leverage direct management and use within the FortiGate and FortiAuthenticator security solutions.

Use case #2: LAN security

As OT network-connected assets and applications continue to proliferate, LANs present increasingly large and attractive attack surfaces. To enhance protection, organizations need additional security with reduced complexity. At the same time, reliable network performance for critical devices and systems must be ensured.

The Fortinet secure networking solution consolidates network management into our industry-leading FortiGate NGFW, which provides comprehensive security for LAN infrastructure plus simplified day-to-day management. Fortinet enables the deployment of large-scale networks with minimal technical expertise using built-in best-practice configurations. Zero-touch provisioning delivers quick and easy application of device templates to sites at scale.

The specific solution capabilities required include:

- Asset and network visibility
- Network segmentation and microsegmentation
- Network access control (NAC)
- User access control (MFA, SSO)
- LAN redundancy protocols (MRP, PRP, HSR)
- Wireless LAN (Wi-Fi) security

In addition to the Fortinet solutions from the WAN security use case, the Fortinet solutions below can help with the LAN security use case:

- **FortiGuard OT Security Service** enables a FortiGate NGFW to monitor, detect, and protect against network-level threats targeting OT environments, supports virtual patching, and provides extensive visibility into OT applications and protocols over LAN and WAN.
- **FortiSwitch** provides complete visibility and control of users and assets in the network.
- **FortiLink** supports improved visibility, segmentation, and microsegmentation. It enables auto-discovery of assets to implement least-privilege access and also helps with centralized management of one or more FortiSwitch appliances from within the FortiGate.

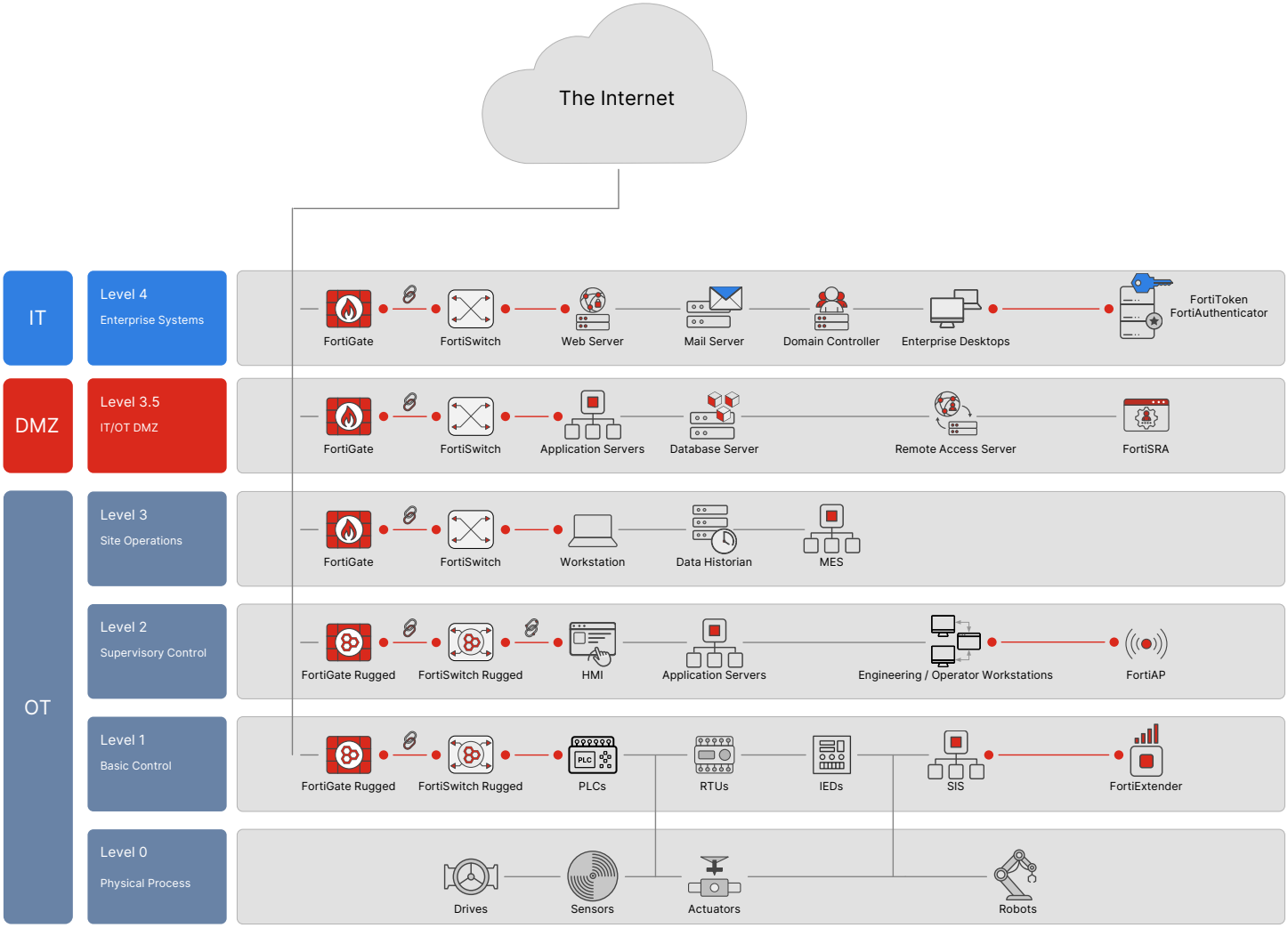

Figure 7: Fortinet LAN security is represented by the red lines in the diagram.

Use case #3: Advanced threat protection

Organizations need visibility and control over how OT applications and protocols communicate with one another over the network. FortiGate NGFWs include a built-in IPS that enables application control signatures to enforce application-specific firewall policies for OT network traffic. They also support virtual patching for insecure legacy devices running in the network without the need for security fixes or software patches.

The specific solution capabilities required include:

- OT application control
- OT and IT vulnerability protection (IPS)
- Virtual patching
- Anti-malware
- Web filtering
- Sandboxing
- Endpoint security

Several Fortinet solutions help enable this use case:

- **FortiGate** NGFW includes built-in next-generation IPS that integrates with FortiGuard security services and offers DPI and intrusion prevention.
- **FortiGuard OT Security Service** combines application control and vulnerability signatures that are developed specifically for OT. It provides the capability to detect and protect against network-level threats while enabling extensive visibility and control over OT applications and protocols. The service can perform virtual patching of unprotected devices while awaiting a patch. Fortinet works closely with automation and control system vendors to develop IPS signatures to address known platform vulnerabilities.
- **FortiSandbox** delivers advanced persistent threat detection and protection. It is available as a service integrated into the FortiGate or as a standalone solution.
- **FortiEDR** endpoint detection and response provides real-time, automated endpoint threat detection, protection, orchestrated incident response, and forensics. FortiEDR can also integrate with FortiGate NGFWs to mitigate threats.
- **FortiClient** supports endpoint management and zero trust network access (ZTNA). FortiClient also integrates with FortiGate NGFWs to offer client posture security assessment as part of ZTNA.

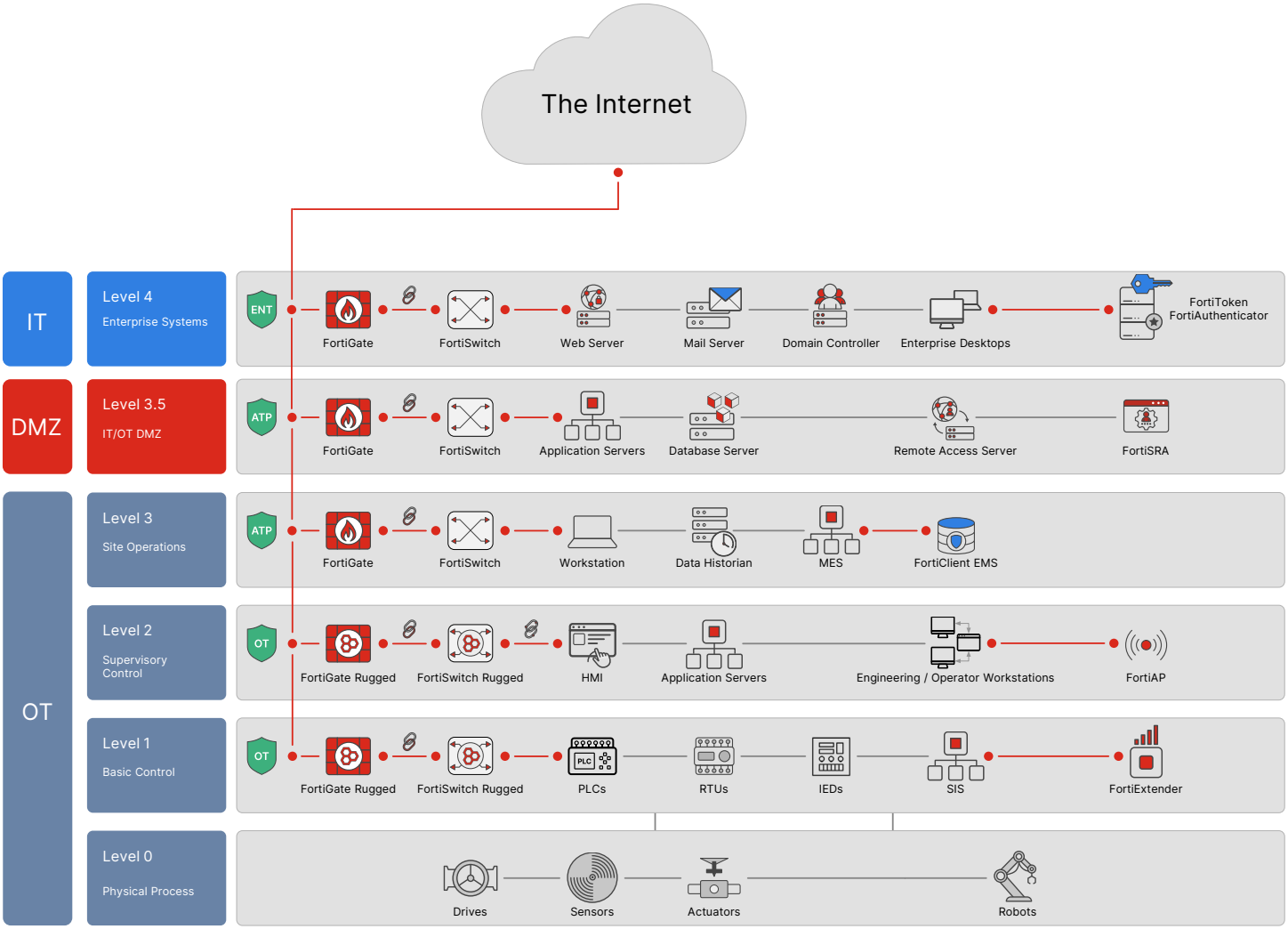

Figure 8: Advanced threat protection across IT/OT, using FortiGate NGFWs and FortiGuard Security Services is represented by the red lines in the diagram (1/2).

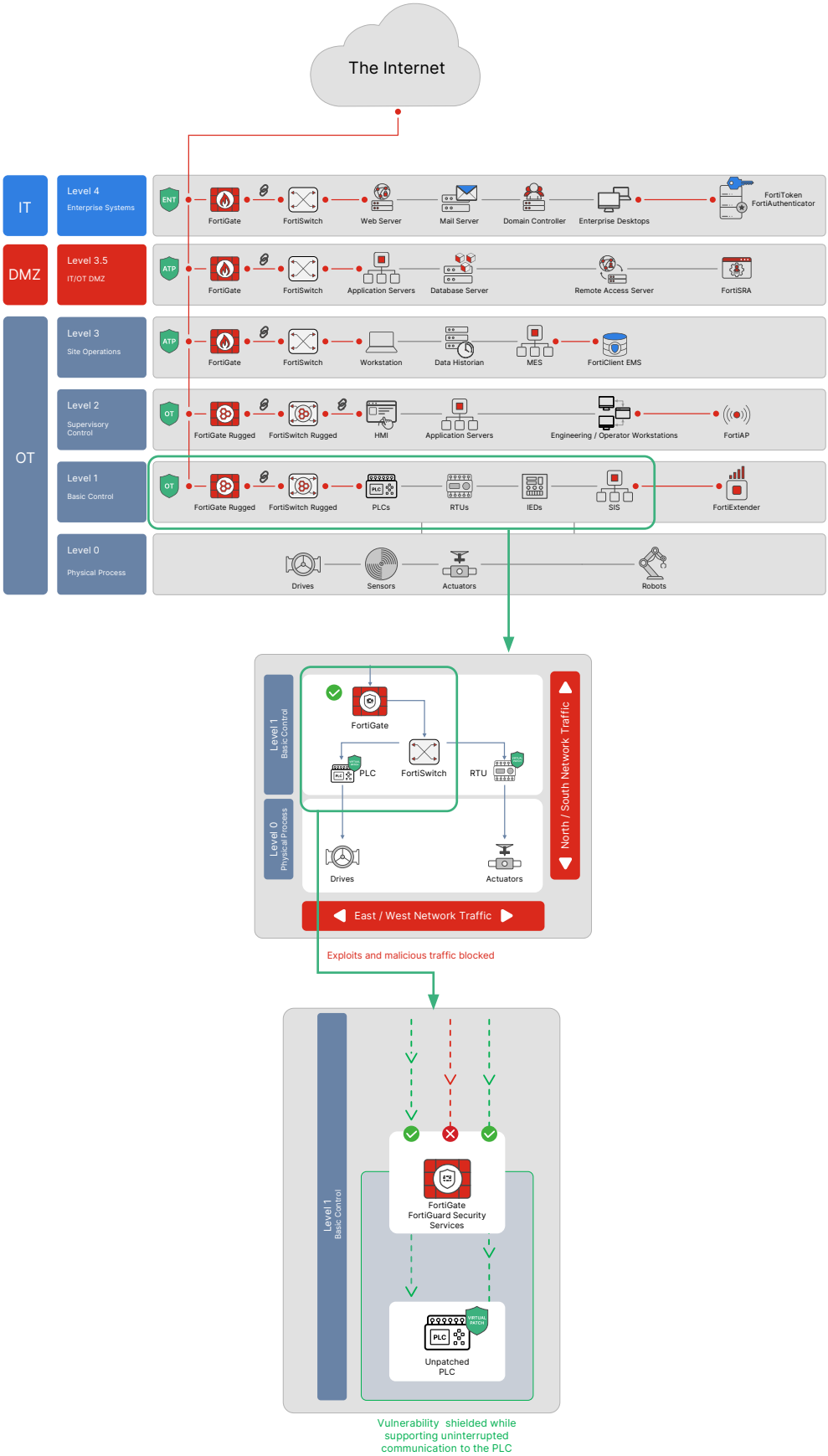

Figure 9: Advanced threat protection across IT/OT, using FortiGate NGFWs and FortiGuard Security Services is represented by the red lines in the diagram (2/2).

Use case #4: Security automation, operations, and management

One goal of a mature IT/OT security program should be a unified and integrated NOC/SOC serving both IT and OT environments with semi or fully automated, 24×7 remedial action and incident response capabilities. This combined operations center is responsible for threat intelligence, analytics, threat detection, incident response, and threat hunting, as well as governance and compliance. With a unified NOC/SOC for IT and OT, organizations can gain full visibility of users, systems, access provisions, incidents, threat alerts, and intelligence feeds from external agencies.

FortiAnalyzer establishes a unified perspective for NOC/SOC teams. Its dashboard gives administrators an accurate, up-to-the-minute status on every asset in the broader Fortinet Security Fabric. Additionally, SOC teams can use the feed of operational data from the FortiSIEM configuration management database to assess the scope of security alerts and issues.

Real-time global intelligence from FortiGuard Labs helps identify and stop even the newest and most sophisticated threats. NOC teams can use the FortiAnalyzer dashboard to spot performance degradations or irregularities due to 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 specific solution capabilities required include:

- Cybersecurity risk management
- Cybersecurity compliance
- Network security management
- Network detection and response
- Incident response
- SIEM/SOAR

Several solutions within the Fortinet Security Fabric help enable this use case:

- **FortiAnalyzer** provides centralized monitoring, logging, and reporting for FortiGate appliances deployed across IT and OT.
- **FortiManager** provides centralized device management and implementation of security policy for all FortiGate appliances. It enables consistent security policy enforcement and software updates from a single and streamlined user interface.
- **FortiNDR** provides network detection and response, combining AI-based, human, and behavioral network traffic analysis to look for signs of malicious activity while reducing false positives.
- **FortiSIEM** ingests and analyzes log data from IT and OT, enabling correlations for threat actor behavior that spans both environments. FortiSIEM can also show threat activity in the MITRE ATT&CK framework for both Enterprise IT and ICS/OT 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. The FortiSOAR customizable security operations platform provides automated playbooks, incident triaging, and real-time remediation for IT/OT enterprises to identify, defend, and counter cyberattacks.

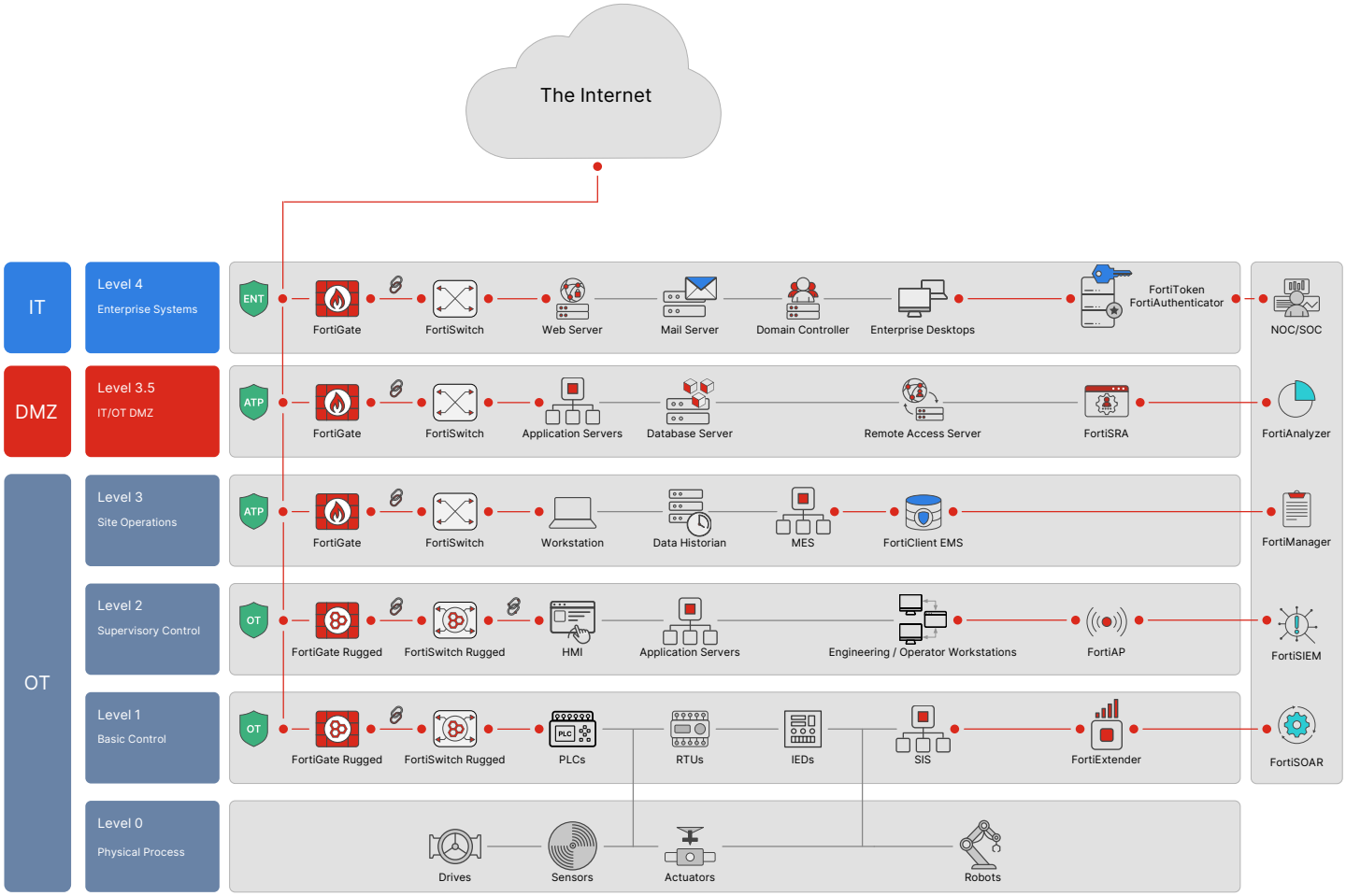

Figure 10: Fortinet security automation, operations, and management is represented by the red lines in the diagram.

Use case #5: Third-party vendor integrations

Deploying reliable connectivity and security in OT environments (which are often remote) is not solved with a single solution. Fortinet collaborates with ICS partners (such as Siemens, Schneider Electric, and Rockwell Automation) and OT security vendors (including Armis, Nozomi Networks, Claroty, and Dragos) to deliver platform-integrated end-to-end solutions.

The underlying Fortinet open architecture and integration interface make it easy and fast to integrate new solutions with the Fortinet OT Security Platform and the broader Fortinet Security Fabric architecture. This open ecosystem approach extends the benefits of the Security Fabric to the Fabric-Ready Partner solutions through Fortinet-developed Fabric Connectors and to other partner solutions through the Fabric APIs and DevOps tools.

- **The Fortinet Open Ecosystem** is one of the largest cybersecurity ecosystems in the industry, composed of Fabric-Ready technology alliance partners, threat-sharing organizations, and other Fabric integrations. This ecosystem provides integrated security solutions for advanced end-to-end security.
- **The Fortinet Fabric-Ready Technology Alliance Partner Program** brings together a global community of partners with specialized technology expertise. It makes resources and tools available to facilitate integration. Alliance solutions are pre-integrated to help customers save time and resources in deployment, operations, and support.

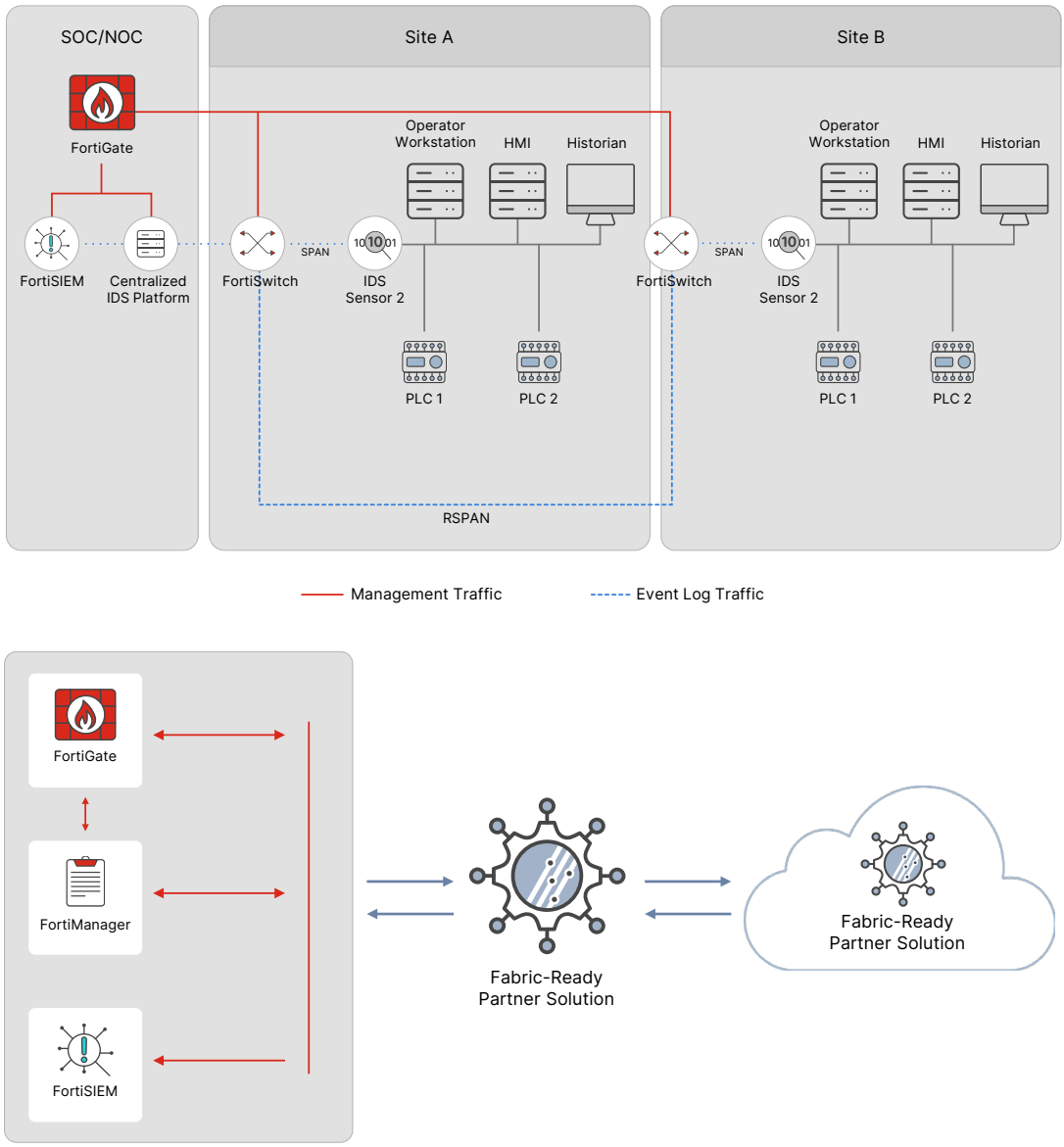

Figure 11: Fortinet third-party vendor integration.

Planning OT Security: IT/OT Cybersecurity Architecture

Reference architectures

When developing a cybersecurity plan for an OT environment, it is useful to map security capabilities against industry standards and frameworks to derive network and security architectures that may help understand the technology infrastructure and implement appropriate security controls. Some notable examples of technology reference architectures include:

Purdue Enterprise Reference Architecture (PERA): The Purdue University Consortium for Computer Integrated Manufacturing developed the Purdue model in the 1990s. Although it is not a security architecture, many organizations use PERA as a reference to model their IT/OT networks and manage their security controls. For example, it has been adapted to standards like ISA99. 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 hyper-convergence of IT and OT. With the addition of IIoT devices, enhancements to the model are needed.

Open Process Automation Standard (O-PAS): The mission of the Open Group's O-PAS is to create an open architecture specification supported by industry users, suppliers, and integrators. It provides a "standard of standards" that defines an open, interoperable, and secure architecture for industrial process automation systems. O-PAS requires a proactive secure-by-design approach in which security is integrated into systems during the design phase instead of retrofitting security controls as a post-deployment afterthought. O-PAS technology components must support a minimum of ISA/IEC 62443-4-2 security level 2 (SL2) capabilities before going into production.[23]

Industrial Internet Reference Architecture (IIRA): The IIRA is a standards-based open architecture that addresses the need for a common architectural framework to develop interoperable IIoT systems for diverse applications across a broad spectrum of industrial verticals in the public and private sectors. The IIRA distills and abstracts common characteristics, features, and patterns from use cases defined in the Industry IoT Consortium (IIC) and elsewhere. The IIRA is also intended to identify technology gaps and drive new development efforts within the IIoT community.[24]

Best Practices, Standards, and Regulations

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.[25]

IEC 62443: This is a set of industrial automation and control system security standards written by industry experts comprising asset owners, manufacturers, and integrators across a range of applications and sectors. It provides technical requirements that foster a cohesive approach to security that considers 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 OT environment. The IEC 62443 series adopts PERA to guide security architecture and its implementation.[26]

Maritime regulations: In 2023, the International Association of Classification Societies (IACS) issued unified requirements (URs) on cybersecurity for all new ships built after January 1, 2024. These baseline requirements for cyber resilience in the design, construction, commissioning, and operation of vessels and the shipboard systems provide a set of standards that credentialing companies utilize in certifying a ship for operation. UR E26 focuses specifically on the cyber resilience of the ship, and UR E27 focuses on the hardening of shipboard systems by suppliers. A common challenge when selecting and implementing the technology to meet these requirements is ending up with a mixed technology stack spread across multiple vendors, which increases complexity and costs.[27]

NERC-CIP: The NERC-CIP standards are goals-based requirements specifying what an asset owner operator must achieve. The standards do not provide prescriptive guidance on how the asset owner-operator needs to achieve strict compliance with a requirement. This omission is both a blessing and a curse, allowing organizations to develop the "best fit" solution for their specific environments; however, the organization-specific tailored solution will be evaluated through the lens of an auditor who will assess the solution to determine whether any potential violations result from that solution. This approach has often sent organizations searching for a compliant solution to purchase. Electric utilities and the vendor community need to know that no such solution exists. Many products can be configured, managed, and operated compliantly, but no solution can make organizations NERC-CIP compliant.[28]

NIS Directive (NIS-D): Originally adopted by the European Parliament in July 2016 and 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 operators by establishing a common framework to discuss cyber risk and cybersecurity incident response across the EU.[29]

Open Process Automation (OPA): An initiative to replace legacy components based on proprietary architectures by developing new process automation systems using an open architecture led by the Open Process Automation Forum (OPAF). OPA covers multiple systems, including manufacturing execution systems (MES), distributed control systems (DCS), programmable logic controllers (PLC), human-machine interfaces (HMI), safety instrumented systems (SIS), and I/O points. Advocates of OPA work to simplify the maintenance and updates of systems, allowing manufacturers to focus on improving their processes instead of managing the systems that automate them.[30]

Looking Forward: The Path to Modern OT Security

The Fortinet OT Security Platform protects the digital attack surface of IT and OT networks and can be deployed in stages that are aligned with organizational security priorities. Although the use cases summarize the current best-practice applications for OT security, organizations should also be anticipating several forward-looking trends:

Containerization: OT environments will soon take advantage of containerization technologies to simplify the deployment and management of many IoT and IIoT functions. This will once again change how security policies must be applied and enforced. The first issue will be establishing full visibility into all containers spread throughout the OT environment. Another key challenge is uncovering vulnerabilities and misconfigurations across host OS, container images, and containers before they are deployed.

GenAI: Generative AI capabilities for threat detection, predictive maintenance, and process optimization can modernize control systems and improve operations. But to realize these benefits, organizations must ensure that they have skilled personnel, high-quality data sets and managed AI models, and an understanding of AI's limitations and potential impact or inaccuracies that may occur.[31] AI-enabled security monitoring will also require new security controls to ensure that hackers aren't able to spoof physical security systems or inject malware into OT environments.[32]

Prioritizing workforce development: Compared to the broader IT security workforce, OT security teams are a relatively new capability within many organizations. OT team members may lack the amount of dedicated experience as IT team members and also need a specialized understanding of ICS/OT environments. Security practitioners tasked with protecting critical infrastructure will need to keep pace with the changing technologies and risks within modern industrial environments.[33]

Organizations seeking help in planning or continuing their cybersecurity journey can learn more at fortinet.com/ot or reach out to OT@fortinet.com. Visit the OT Security Solutions Hub for additional technical information on the Fortinet OT Security Platform.

Appendix

Fortinet OT Security Platform solutions mapping to use cases

Solution	Use Cases
FortiAuthenticator	• Identity and Access Management • Single Sign-On
FortiToken	• Multi-Factor Authentication

Solution	Use Cases
FortiGate	• Advanced Threat Protection • Asset and Network Visibility • Next-Generation Firewall • Next-Generation Intrusion Prevention System • Network Segmentation • Secure SD-WAN • Virtual Private Network
FortiGate Rugged	
FortiLink	• Network Microsegmentation • Network Management
FortiLink NAC	• Network Access Control

Solution	Use Cases
FortiSwitch	• Asset and Network Visibility • Network Microsegmentation • Secure Networking
FortiSwitch Rugged	

Solution	Use Cases
FortiAP	• Security for Wireless WAN (Wi-Fi/3G/4G LTE/5G)
FortiExtender	

Solution	Use Cases
FortiSRA	• Secure Remote Access • Privileged Access Management • Role Based Access Control

Solution	Use Cases
FortiAnalyzer	• Centralized monitoring, logging, and reporting for FortiGate appliances and assets deployed across IT and OT
FortiManager	• Centralized device management and security policy implementation for FortiGate appliances deployed across IT and OT
FortiSIEM	• Centralized monitoring, logging, log correlation and reporting • Cybersecurity risk and compliance reporting
FortiSOAR	• Security orchestration, automation and response • Cybersecurity risk and compliance reporting
Fabric-Ready Partner Solution	• Third-party solution integrated with Fortinet technologies through Security Fabric APIs

Solution	Use Cases
FortiClient EMS	• Endpoint Detection & Response • Zero Trust Network Access
FortiClient	

Solution	Use Cases
FortiGuard Security Services	• IT/OT Threat Protection • IT/OT Vulnerability Management • IT/OT Virtual Patching

Mapping the OT Security Platform solutions to the industry standard cybersecurity requirements

Fortinet Products	US FERC NERC CIP	EU NIS2 Directive	ISA IEC 62443 Standard	NIST SP 800-82 Rev.3 NIST 800-53 Rev.5	SANS ICS 5 Critical Controls
FortiGate FortiSwitch FortiAP	**CIP-005-7** - Electronic Security Perimeter (ESP) **CIP-007-6** - System Security Management **CIP-008-6** - Incident Reporting and Response Planning **CIP-011-3** - Information Protection **CIP-012-1** - Communications Between Control Centers	Article 21-2(h) Article 21-2(i) Article 21-2(j)	**FR 4** - Data Confidentiality **FR 5** - Restricted Data Flow	System and Communications Protection (SC)	**2.** Defensible Architecture **3.** ICS Network Visibility and Monitoring
FortiSRA FortiToken	**CIP-005-7** - Electronic Security Perimeter (ESP) **CIP-007-6** - System Security Management **CIP-011-3** - Information Protection	Article 21-2(i) Article 21-2(j)	**FR 1** - Identification and Authentication Control **FR 2** - Use Control	Access Control (AC) Audit and Accountability (AU)	**4.** Secure Remote Access
FortiAnalyzer FortiSIEM	**CIP-007-6** - System Security Management **CIP-008-6** - Incident Reporting and Response Planning **CIP-010-4** - Configuration Change Management and Vulnerability Assessments **CIP-011-3** - Information Protection	Article 21-2(a) Article 21-2(b) Article 21-2(e)	**FR 6** - Timely Response to Events	Audit and Accountability (AU) Configuration Management (CM)	**3.** ICS Network Visibility and Monitoring
FortiNAC	**CIP-005-7** - Electronic Security Perimeter (ESP) **CIP-006-6** - Physical Security of BES Cyber Systems **CIP-007-6** - System Security Management	Article 21-2(b)	**FR 1** - Identification and Authentication Control **FR 2** - Use Control	Identification and Authentication (IA)	**2.** Defensible Architecture
FortiClient FortiEDR	**CIP-007** - System Security Management **CIP-008-6** - Incident Reporting and Response Planning **CIP-010-4** - Configuration Change Management and Vulnerability Assessments **CIP-011-3** - Information Protection	Article 21-2(b)	**FR 3** - System Integrity	Media Protection (MP) System and Information Integrity (SI)	**2.** Defensible Architecture
FortiSOAR	**CIP-008** - Incident Reporting and Response Planning **CIP-010-4** - Configuration Change Management and Vulnerability Assessments	Article 21-2(b)	**FR 6** - Timely Response to Events	Incident Response (IR)	**5.** Risk-Based Vulnerability Management

OT Security Terms

Air gap is a term 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, and it cannot 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 and 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 healthcare, emergency response, traffic flow management, smart manufacturing, defense and homeland security, and energy supply and use. In addition to CPS, many words and phrases such as IoT, machine-to-machine (M2M), and smart cities describe similar or related systems and concepts. There is a significant overlap between these concepts, in particular, CPS and IoT, and CPS and IoT are sometimes used interchangeably. CPS are complex systems of computational, physical, and human components integrated to achieve some function over one or more networks.

Distributed control systems (DCS) manage local controllers or devices of production systems in one 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 and 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 equipment on and off, such as motors, pumps, and breakers.

Historian server is a critical part of the industrial control system, such as DCS or SCADA environment. The historian server 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) 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 connect directly to the cloud or through an edge gateway that sends data to the cloud.

Internet of Things (IoT) refers to either user devices, industrial devices, or a network of devices that connect to the internet. IoT devices contain the hardware, software, firmware, and actuators that allow them 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. These workstations 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 based on that logic, send signals to actuators such as pumps, motors, and breakers to turn on or off physically. PLCs also receive commands from HMIs and send time-series data to historian servers.

Safety instrumented systems (SIS) are designed to override ICS, DCS, and SCADA systems as a fail-safe, last resort if these systems begin to operate outside of safe limits. SISs are designed to provide corrective action if other control system elements 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 other remote locations and then processes this data in a central system, which then manages and controls the field factory, plant, or site operations.

[1] "Four Key Trends in Operational Technology," Fortinet, July 30, 2024.

[2] "Why using IT cybersecurity to protect OT puts industrial organizations at risk," World Economic Forum, January 16, 2025.

[3] "2025 State of Operational Technology and Cybersecurity Report," Fortinet, June 9, 2025.

[4] "New ABI Research OT cybersecurity dataset highlights steady and stable growth," ABI Research, June 27, 2024.

[5] "2025 State of Operational Technology and Cybersecurity Report," Fortinet, July 9, 2025.

[6] "SANS 2024 ICS/OT Survey: The State of ICS/OT Cybersecurity," SANS, October 9, 2024.

[7] Ibid.

[8] Ibid.

[9] Fortinet, 2025 Global Threat Landscape Report, May 1, 2025.

[10] "Why using IT cybersecurity to protect OT puts industrial organizations at risk," World Economic Forum, January 16, 2025.

[11] Ibid.

[12] "ICS tactics," Mitre, accessed February 13, 2025.

[13] "ICS techniques," Mitre, accessed February 13, 2025.

[14] "The Distinctive Worlds of OT Cybersecurity and IT Cybersecurity," SAN, May 7, 2024.

[15] "SANS 2024 ICS/OT Survey: The State of ICS/OT Cybersecurity," SANS, October 9, 2024.

[16] Ibid.

[17] "Toyota Material Handling," Fortinet, accessed February 14, 2025.

[18] "Nordlaks," Fortinet, accessed February 14, 2025.

[19] "Siemens Switzerland," Fortinet, accessed February 14, 2025.

[20] "California Water and Wastewater District," Fortinet, accessed February 14, 2025.

[21] "Herzog Technologies, Inc.," Fortinet, accessed February 14, 2025.

[22] "RH Marine," Fortinet, accessed February 14, 2025.

[23] "Securing Open Process Automation Infrastructure with Fortinet," Fortinet, August 2024.

[24] "The Industrial Internet Reference Architecture," Industry IoT Consortium, November 7, 2022.

[25] "NIST SP 800-82 Rev. 3," NIST, September 2023.

[26] "Effective ICS Cybersecurity Using the IEC 62443 Standard," SANS, June 2023.

[27] "IACS Adopts New Requirements on Cyber Safety," IACS, accessed March 20, 2025.

[28] "How to Use NERC-CIP: An Overview of the Standards and Their Deployment with Fortinet," SANS, June 2024.

[29] "Enabling NIS2 Directive Compliance with Fortinet for Operational Technology," SANS, March 2023.

[30] "Securing Open Process Automation Infrastructure with Fortinet," Fortinet, August 2024.

[31] "ICS/OT Cybersecurity & AI: Considerations for Now and the Future (Part II)," SANS, October 1, 2024.

[32] "What's Next for Operational Technology Security?," Fortinet, February 07, 2025.

[33] "SANS 2024 ICS/OT Survey: The State of ICS/OT Cybersecurity," SANS, October 9, 2024.

August 15, 2025 10:55 AM / MKTG-1597-0-0-EN