WHITE PAPER

Securing OT, Remote Access, and Converged SOC Operations

New Strategies for Industrial CIOs and CISOs

Executive Summary

Digital transformation (DX) is propelling organizations forward and accelerating the convergence of operational technology (OT) with information technology (IT). Note for the purposes of this paper that OT is synonymous with industrial control systems (ICS). OT-ICS environments perform supervisory management of cyber-physical processes in a production environment. They are composed of a variety of different kinds of software and hardware, including programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, and human-machine interfaces (HMI).

Previously air-gapped OT environments are now increasingly connected due to DX initiatives and the growing need for highly skilled technicians to support dispersed industrial assets remotely. The fundamental assumption—a discrete OT disconnected from the rest of the enterprise network—is now undermined by this increased connectivity. New solutions are required to connect the networks that operate industrial assets securely. The Fortinet Security Fabric provides a broad, integrated, and automated defense-in-depth suite of solutions. It is engineered to address the unique requirements of both IT and OT environments.

With digital transformation and the convergence of IT and OT, organizations can now leverage the Internet of Things (IoT), cloud computing, artificial intelligence (AI), and other digital technologies to optimize operations, improve safety and reliability, and gain a competitive edge.

The Convergence of OT and IT

Many believe digital transformation is the most important business trend in IT today. DX empowers businesses to operate with more agility and scale more quickly by moving more services to the cloud. Slightly different for each organization, DX is almost always marked by increasing reliance on hybrid-cloud architectures. This means bringing existing on-premises resources together with multiple external cloud networks and ensuring their availability and performance—no matter where a user is located.

With digital transformation and the convergence of IT and OT, organizations can now leverage the Internet of Things (IoT), cloud computing, artificial intelligence (AI), and other digital technologies to optimize operations, improve safety and reliability, and gain a competitive edge. Despite the many benefits that the IT-OT convergence brings to the table, there is a significant downside—expansion of the OT attack surface and an increased vulnerability to cyberthreats affecting physical systems.

The Challenges of Securing OT

ICS and PLCs are inherently insecure because they were designed with an assumption that their networks would be isolated in an era of assumed trust. OT creators did not foresee that there would be a need for remote access to OT environments. The first challenge of securing OT starts with the PLCs. Most PLCs deployed are not following any kind of zero-trust approach; rather, they are following an assumed-trust philosophy. For example, when a PLC receives a message from elsewhere on the same network where the PLC is connected and that message is formatted in the protocol that the PLC expects to see, most PLCs will assume that the message is legitimate and simply follow the command. The PLC will turn things on. The PCL will turn things off. The PLC will reset itself to a factory baseline. PLCs are not verifying the message sender's authenticity or authorizing it with questions such as: Who are you? Are you authorized to command me? Is this a secure encrypted channel?

This lack of authorization, authentication, and encryption underlines the fundamental insecure-by-design nature of PLCs deployed in industry today. The reality is that newer PLCs have much better native security, utilizing technologies such as firmware code-signing, Trusted Platform Modules, and so on, requiring encryption, authorization, and authentication checks. But industrial systems are deployed for very long life cycles (20–30 years is typical), so the fact remains that most PLCs deployed today are fundamentally insecure.

Knowing When It's Going to Break Before It Breaks

PLCs reside in sensitive environments and, historically, they were secured by being air gapped. But organizations are trading away that innate protection for the digital transformation benefits of connecting these industrial environments to the data center or the cloud to get data out of them. This enables organizations that own the industrial equipment to anticipate when the machine controlled by the PLC will break before it actually breaks.

Organizations will often build a digital twin to anticipate industrial equipment failure, which typically runs in the cloud or data center. The digital twin requires a lot of operational data. It models the physics, and it looks at what's happening in the environment to generate insights, such as "this industrial equipment is vibrating or shaking too much," or "this part is getting too hot." Asset owners want the data to inform them when something is not right, or when something is different from the other units that they own.

This kind of smart analysis, digital transformation, digital-twin analytics requires a considerable quantity of operational data. To facilitate that kind of insightful observation, it must be done in the cloud or a data center, and that essentially means industrial assets must be connected outside of the previously air-gapped OT zone.

Condition-based Maintenance

Another benefit of DX with OT comes with moving from calendar-based maintenance to condition-based maintenance. Before DX, calendar-based maintenance meant, for example, that a technician had to climb up a wind turbine every six months to tighten the nuts and bolts that connect the tower sections. This is done because the wind turbine equipment manufacturer requires it to be done to maintain the warranty and for the asset to remain healthy.

Original equipment manufacturers (OEMs) have safety margins built into all these recommendations in their manuals. However, when an organization can move to condition-based maintenance, it's able to squeeze out some extra margin and improve its profitability. The asset-owning energy company would rather climb the tower when the bolts are loose, not just because six months have gone by.

New Tech = New Risks

Another DX benefit that motivates organizations to get on the digital transformation expressway is the ability to employ new technologies such as 5G, IoT, the Industrial Internet of Things (IIoT), and the cloud. However, in addition to providing improvements and cutting-edge applications, these new technologies also bring new risks. They have complicated supply chains leveraging open source and other third-party libraries, and they are immature technologies, which can lead to introducing even more vulnerability to the OT when connected.

Securing Operational Technology Challenges

- Most industrial control systems lack security by design and are brittle to change.
- The attack surface for cyber-physical assets is expanding as a dependence on air-gap protection diminishes with digital transformation initiatives driving IT-OT network convergence.
- Increasing adoption of new technologies, such as 5G, IoT, and cloud.
- Remote access requirements for third parties and employees causing additional risks.
- Asset owners' reliance on OEMs and SIs exposes critical systems to additional risks.

Secure Remote Access

The risks do not end with digital transformation and these different environments. Organizations also have a need for secure remote access. For example, many oil production companies that own pump jacks, which are used to take oil out of the ground, own hundreds if not thousands of them. It is not cost-effective to have a person at each pump jack, just like a renewable energy company cannot have a person in each wind turbine. Therefore, the organization needs a secure way to enable access for both employees and trusted third parties—such as OEMs and system integrators.

Asset owners need a mechanism for people to get into these environments to do remote monitoring and diagnostics, perform upgrades, reset tripped equipment, and command restarts. Many industrial asset owners simply require remote access to operate profitably. However, that remote connection creates additional risk.

A real-world example of this type of risk was the 2021 attack on a water treatment facility in Oldsmar, Florida (near Tampa). The facility's SCADA system was put on TeamViewer, which is not a particularly secure way of creating remote access to an industrial environment. Therefore, an attacker was able to hack into the water treatment facility and change a setpoint that put "100 times higher than normal" sodium hydroxide, or lye, in the drinking water. Though water treatment officials say the public was never in danger because of the safeguards in place to test the water before it was released, it is an indication of how vulnerable OT systems can be abused.

There is an additional risk that many don't often think of that comes with dealing with OEMs or systems integrators. Consider the risks they bring to an organization when they need to do maintenance. Many technicians outside of the asset-owning company may need to physically come on-site and bring their phones, laptops, and USB sticks—and the company that owns the equipment may not have control over what those third-party technicians are plugging in.

What Are Organizations Trying to Do?

1. **Digital transformation:** Acquiring data to anticipate failures and moving from calendar-based maintenance to condition-based maintenance requires connecting assets so that data can flow from the OT environment into the data center or cloud. In other words, DX requires the connecting of assets. The challenge is that this increases the attack surface vulnerabilities.
2. **Secure remote access:** Asset owners need to enable their trusted employees and trusted third parties to remotely access their industrial environments so they can perform maintenance activities such as:
   a. Remotely monitor and run diagnostics
   b. Reset a trip
   c. Update the control code
   d. Update the runtime firmware in the PLC
3. **Address IT and OT environment from a converged security operations center (SOC):** Tremendous benefits, as seen in our research reports, indicate that organizations want to:
   a. Manage assets and policies in both the IT and OT environments
   b. Ingest data from both IT and OT environments into a common security information and event management (SIEM) for enhanced correlation
   c. Deploy deception technologies to both environments
   d. Analyze data from both IT and OT environments
   e. Protect endpoints on IT and OT systems such as jump boxes, historians, and engineering workstations
4. **Keep everything up to date:** Maintain IT and OT network security as the threat evolves. Keep up with sophisticated threat actors as they get more sophisticated.

In short, organizations want to implement attractive DX initiatives to reduce costs and increase profits. Unfortunately, they also increase risk on the attack surface and require new security solutions.

How Fortinet Helps Address the Challenges

The attack surface for cyber-physical assets is expanding as the dependence on air gaps as a protection mechanism diminishes. Most ICS lack security by design, and many OT operations teams prioritize the industrial equipment's uptime and availability over a security mindset and training. Also, many OT environments include a mix of legacy and new technologies from multiple automation vendors. Most endpoint protection solutions won't work in such environments. Fortinet products will.

Asset owners' reliance on OEMs and systems integrators exposes their critical systems to additional risks, including:

- Unsupervised access to the critical systems
- Lack of endpoint security controls
- Ineffective logging and monitoring
- Missing bring-your-own-device (BYOD) security
- Unregulated wireless access
- Lack of removable media security
- ICSs have 20–30-year life cycles

The Fortinet Security Fabric integrates industry-leading security solutions to provide broad visibility across the IT-OT attack surface while automating operations and providing continuous trust assessments.

Fortinet Security Fabric

Organizations can mitigate the cyber risks imposed by converging IT and OT with the Fortinet Security Fabric, a transformative and unique security architecture. The Security Fabric enables a secure digital transformation journey providing solutions that can:

- Securely bring data out of the operational environment up to the cloud
- Enable secure remote access
- Provide opportunities to address IT and OT environments from a common SOC securely

The Fortinet Security Fabric integrates industry-leading security solutions to provide broad visibility across the IT-OT attack surface while automating operations and providing continuous trust assessments. This way, the Fortinet Security Fabric can serve as a secure foundation for converging IT and OT environments. The following solution sets show which products from the Fortinet Security Fabric can help organizations maintain a coherent security posture as they meet the challenges posed by inherently insecure industrial controls and adopt the benefits offered by new trends.

Cybersecurity Designed by Fortinet for Converging IT-OT Networks

As organizations adapt their IT-OT infrastructure to account for convergence and DX, they must also undergo a security transformation to protect against evolving cyberthreats. The Fortinet Security Fabric provides a proactive and transformative approach to cybersecurity, as shown in Figure 1.

The Security Fabric delivers:

- Broad visibility of the entire IT-OT attack surface for coordinated threat detection and policy enforcement
- Integrated and unified security, operations, and performance across different technologies, locations, and deployments for complete visibility
- Automated operations and response by AI and ML to deliver near-real-time, user-to-application coordinated protection across the Security Fabric

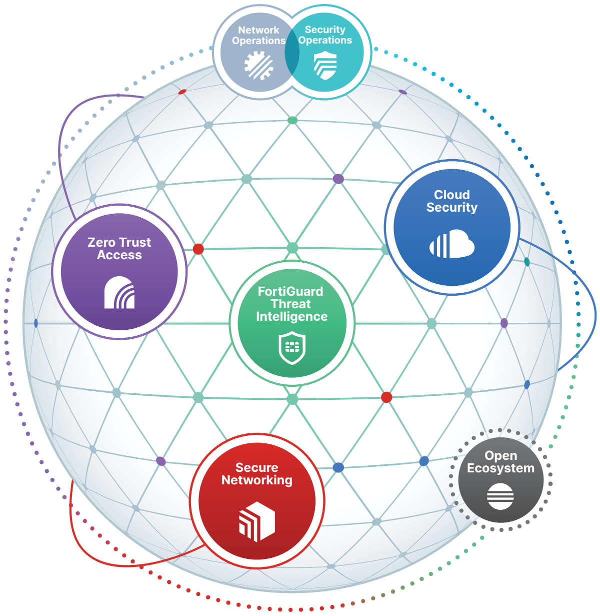
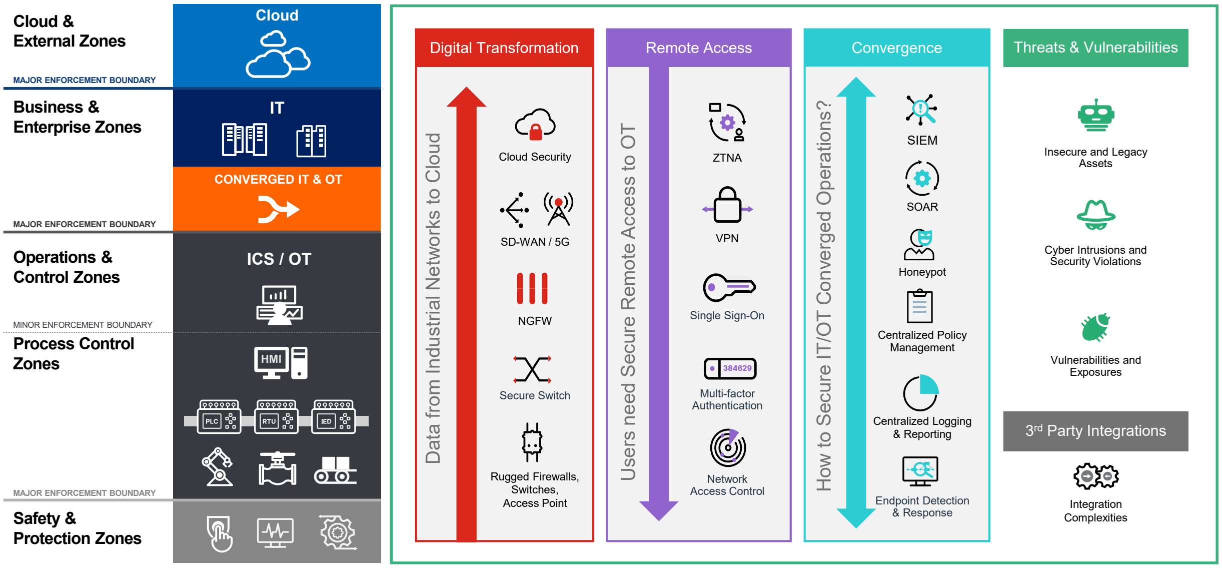


Figure 1: Powered by FortiOS, the Fortinet Security Fabric enables multiple technologies to work together across IT and OT environments. With a rich open ecosystem, the Security Fabric spans the extended digital attack surface and cycle, enabling self-healing security and networking to protect devices, data, and applications.

Fabric Solutions – Operational Technology

Most commonly deployed Security Fabric Solutions


Cloud & External Zones
Cloud
MAJOR ENFORCEMENT BOUNDARY
Business & Enterprise Zones
IT
CONVERGED IT & OT
MAJOR ENFORCEMENT BOUNDARY
Operations & Control Zones
ICS / OT
MINOR ENFORCEMENT BOUNDARY
Process Control Zones
HMI
PLC
RTU
IED
MAJOR ENFORCEMENT BOUNDARY
Safety & Protection Zones
Digital Transformation
Data from Industrial Networks to Cloud
Cloud Security
SD-WAN / 5G
NGFW
Secure Switch
Rugged Firewalls, Switches, Access Point
Remote Access
Users need Secure Remote Access to OT
ZTNA
VPN
Single Sign-On
384629
Multi-factor Authentication
Network Access Control
Convergence
How to Secure IT/OT Converged Operations?
SIEM
SOAR
Honeypot
Centralized Policy Management
Centralized Logging & Reporting
Endpoint Detection & Response
Threats & Vulnerabilities
Insecure and Legacy Assets
Cyber Intrusions and Security Violations
Vulnerabilities and Exposures
3rd Party Integrations
Integration Complexities

Fortinet Solutions for Addressing IT and OT Convergence Challenges

Digital transformation

When asset owners connect their ICS to the cloud, it is imperative that they protect those environments with next-generation firewalls. SD-WAN helps asset owners lower their connectivity costs and provides enhanced network reliability. Ruggedized switches and access points enable secure connectivity down to the level of those PLCs. Recalling how these networks are brittle to change, Fortinet can enhance the security via our convergence of network and security, and the rugged switches and access points enable security directly in the network infrastructure.

Although the digital transformation arrow is pointing up, it is also notable that another important DX use case is delivering edge analytics from the cloud to the edge of the industrial network. Although in this case binary code is flowing from the cloud to the edge, the same network security considerations and capabilities are required to provision edge applications securely as to enable data exfiltration.

Secure remote access

Another use case driving connectivity is secure remote access to distributed industrial assets. In this case, asset owners want to enable their employees and trusted third parties, such as OEMs, to remotely access their systems to perform SCADA maintenance and enable remote monitoring and diagnostics of their industrial investment. To reiterate, this is much more about remote access for employees and the supply chain accessing the industrial environment network from far away. In this case, it's critical to provide protected communications leveraging zero-trust capabilities such as VPN, single sign-on (SSO), and multi-factor authentication (MFA).

Fortinet has a major differentiator with our zero-trust proxy, which can be deployed in FortiOS (and thus in SaaS, in FortiGate hardware—both ruggedized or standard, in the VM, and in the container). As such, our proxy can be served anywhere, unlike other vendors that are forcing a cloud-based proxy that is rarely easy to provision in OT environments.

Fortinet has a major differentiator with our zero-trust proxy, which can be deployed in FortiOS (and thus in SaaS, in FortiGate hardware—both ruggedized or standard, in the VM, and in the container).

Converged security operations

One valuable differentiator that Fortinet can provide is that the network security products deployed on both the IT and OT sides can be managed from a common SOC. With centralized management, logging, and SIEM and SOAR capabilities deployed in the SOC, organizations can effectively manage, monitor, and hunt threats and orchestrate responses from a common SOC. Endpoint detection and response (EDR) solutions help protect SCADA engineering workstations, historians, and jump boxes found in Purdue Level 3.

Fortinet OT-specific features are being developed into our SIEM and deception product lines. For example, FortiSIEM includes MITRE ATT&CK for ICS and Purdue dashboards. And FortiDeceptor can deploy not only Windows servers, printers, and active directory decoys typically found in IT, but it also can deploy decoys to fool an OT attacker by imitating PLCs, SCADA HMIs, and other OT kits. Similarly, FortiEDR offers strong protection and is relevant to OT endpoints by maintaining robust support for legacy operating systems often found in production environments, including Microsoft Windows XP.

Security services

All of these systems must be kept up to date as the threat landscape evolves. So FortiGuard Labs has engineered a rich industrial security service with 500+ OT intrusion-prevention signatures—which means asset owners can limit known vulnerabilities from being exploited in the OT environment and 2,000+ OT application signatures. They can also set network policies on Modbus and several dozen other industrial protocols that are unique to those ICS.

Ecosystem partners

Fortinet has developed a diverse set of ecosystem partners. These relationships enable us to show the value of the Security Fabric. Fortinet has excellent OT visibility partners, including the biggest names that specialize in OT. For example, companies such as Nozomi Networks, Dragos, and Claroty integrate with multiple points in the Security Fabric, which is both a testament to their understanding of how important it is to work with Fortinet and our understanding of how important it is to work with leading OT specialist vendors. And the Fortinet ecosystem is not limited to just those three companies. There are new partners coming online all the time, including in zero-trust access with XONA Systems, and in security operations with backup/restore vendors and OT SOAR specialists such as Otorio.

In addition to OT specialist vendors, Fortinet focuses on strong partner relationships with the automation and control and industrial engineering firms responsible for developing the underlying OT systems that operate cyber-physical processes. In this way, Fortinet can more quickly engineer OT IPS signatures in collaboration with those partners and provide them with solutions to secure their organizations' industrial environments from the moment they are commissioned.

Fortinet Specialized OT Teams and Solutions

Specialized products

Fortinet has industrial-grade firewalls, switches, and access points. Fortinet has the most deployed IT-OT next-generation firewall worldwide. These products feature OT-specific SIEM and EDR, along with sandbox and deception capabilities. Our specific OT offerings include:

- FortiGate Rugged NGFW
- FortiSwitch Rugged
- FortiAP IPS-rated

Specialized threat information

Regarding threat information for specific OT environments, Fortinet has deep packet inspection for 70+ OT protocols. Our solutions provide up to payload-level visibility and control. We also have unique vulnerability shielding for OT assets and more signatures than any other cybersecurity vendor.

Specialized talent

The Fortinet OT team boasts OT professionals with decades of experience and staff members who specialize in OT integrations. Our worldwide talent bench is 1,000+ Professional Services engineers ready and willing to help. Our solutions are industry validated and referenced.

Specialized ecosystem

The Fortinet Security Fabric is a comprehensive solution integration platform. There are currently 500+ Security Fabric ecosystem integrations and out-of-the-box integrations with leading OT security solutions.

Conclusion

Typically, DX anticipates machine failure and moves from a calendar-based maintenance strategy to a condition-based maintenance strategy by leveraging big data analytics in the cloud or data center. To do this effectively, asset owners must get operational data out of their industrial OT environments.

When connecting industrial control systems to the cloud, OT managers must protect these environments with next-generation firewalls and ruggedized switches and access points. Fortinet OT solutions fill the bill and enable secure connectivity down to the level of those PLCs.

Powered by FortiOS, the Fortinet Security Fabric enables multiple technologies to work together across IT and OT environments. With a rich open ecosystem, the Security Fabric spans the extended digital attack surface and cycle, enabling self-healing security and networking to protect industrial operations. In summary, the Fortinet Security Fabric provides a defense-in-depth suite of solutions that is broad, integrated, and automated—and it is engineered to address the unique requirements of IT and OT environments.

September 29, 2022 3:50 AM

1701707-0-0-EN