FORTINET

Buyer's Guide to OT Security

Five Considerations for Securing Your OT Network

Table of Contents

Challenges

According to recent research from Fortinet, the number of CISOs who oversee OT infrastructure has tripled over the past two years. Yet, many of those tasked with transforming and securing OT find such ownership challenging because traditional OT networks lack visibility, segmentation, and essential cybersecurity best practices such as patch management. In addition, OT networks are an increasingly attractive target for well-funded threat actors due to the heightened impact and implications of a breach.

Connectivity is also rapidly expanding across OT. Once-siloed areas such as remote sites, factories, plants, and vehicles are now connected into enterprise IT systems, which expose OT networks and devices to untrusted networks like the internet and the cloud. These new connections drastically increase the OT attack surface and expose legacy and unpatched systems to threat actors.

Securing OT also can be difficult because the protocols, hardware, architectures, and priorities differ from enterprise IT.

What Is OT?

Operational technology (OT) refers to the hardware and software used to monitor and control physical devices, processes, and infrastructure. Unlike information technology (IT), which focuses on data and networks, OT directly interacts with the real world. OT keeps factories running, power grids stable, and transportation systems moving. OT systems are essential in industries like manufacturing, energy, transportation, and utilities, ensuring the safe and efficient operations of critical infrastructure. Examples include programmable logic controllers, distributed control systems, and supervisory control and data acquisition systems.

OT is essential to businesses and governments worldwide, including critical infrastructure, healthcare systems, and manufacturing operations. The indispensable nature of ICS and OT is precisely what puts them at elevated risk.

Source: Fortinet, 2024 State of Operational Technology and Cybersecurity Report.

How OT Security Addresses OT Challenges

OT security enables the understanding of assets, vulnerabilities, and threats in an OT setting, including OT-specific technologies, such as automation and control systems, industrial machinery, and robotics. OT security often requires the ability to secure OT-specific protocols, such as Modbus, Profinet, and DNP3, as well as OT-specific applications to prevent threats.

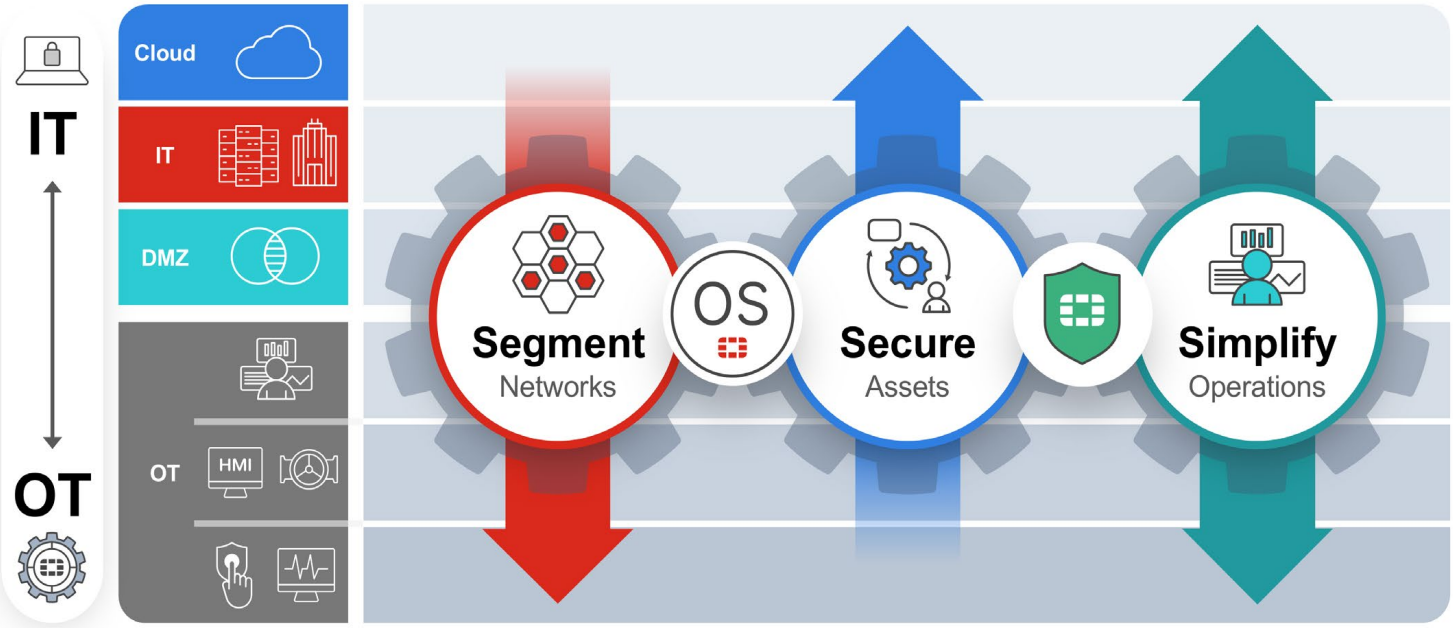
OT security solutions include various technologies, from industrial next-generation firewalls (NGFWs) to security information and event management systems. These solutions can help segment flat OT networks and shield legacy or unpatched OT systems from cyberthreats. Adding OT security can help reduce the time needed to detect and remediate intrusions, bring OT networks into the corporate security operations center (SOC), and help create incident response plans.

Cyberthreats to OT networks have enormous implications for those involved. A successful attack can harm worker and public safety, cause costly physical damage, and have political and societal ramifications. As a result, it is critical to implement effective OT security solutions that are easy to use and can help OT infrastructure keep up with changes in the threat landscape.

Worker Safety

Operational Efficiencies

Real-Time Decision Insight



When properly implemented, OT security benefits organizations by securing users, applications, and protocols and defending against advanced threats. Additional capabilities include automating security operations, implementing secure remote access, and extending secure connectivity to remote sites, including vehicles and fleets.

5

Five Considerations for Securing Your OT Network

Securing OT networks with a broad set of protections reduces the attack surface and overall risk. It helps maximize operational efficiency and output, enable real-time decision making, and improve worker safety. To select the most effective and comprehensive OT security solution, keep the following in mind:

1. **Network segmentation:** Many OT networks are flat by design, so if a malicious hacker were to get in, they could easily move laterally (east-west) and access all critical systems. Network segmentation blocks unauthorized east-west communication across the network and prevents the spread of malicious traffic; segmentation is a crucial component of basic OT security.

   An OT security solution should offer robust network segmentation capabilities, including network access control (NAC) functionality and the ability to enforce security policies at the individual switch-port level across and within the virtual local area network (VLAN) segments.

   These capabilities protect OT networks and significantly reduce OT security risk.

   Questions to ask:

   - How does your solution provide network segmentation capabilities?
   - Do those capabilities extend to each switch port and VLAN?
   - Do those capabilities include NAC functionality?
   - How does your solution automate enforcement?

2. **Visibility and compensating controls:** You can't segment and secure what you can't see. Visibility of assets, vulnerabilities, and threats is a key requirement in basic OT security.

   OT networks are packed with technologies that are not typically found in IT networks, such as industrial automation and control systems, pumps, actuators, furnaces, and conveyor belts. In addition, most of these technologies communicate in clear text protocols that aren't used in IT networks, such as Modbus, Profinet, and DNP3, which can make OT security more complicated.

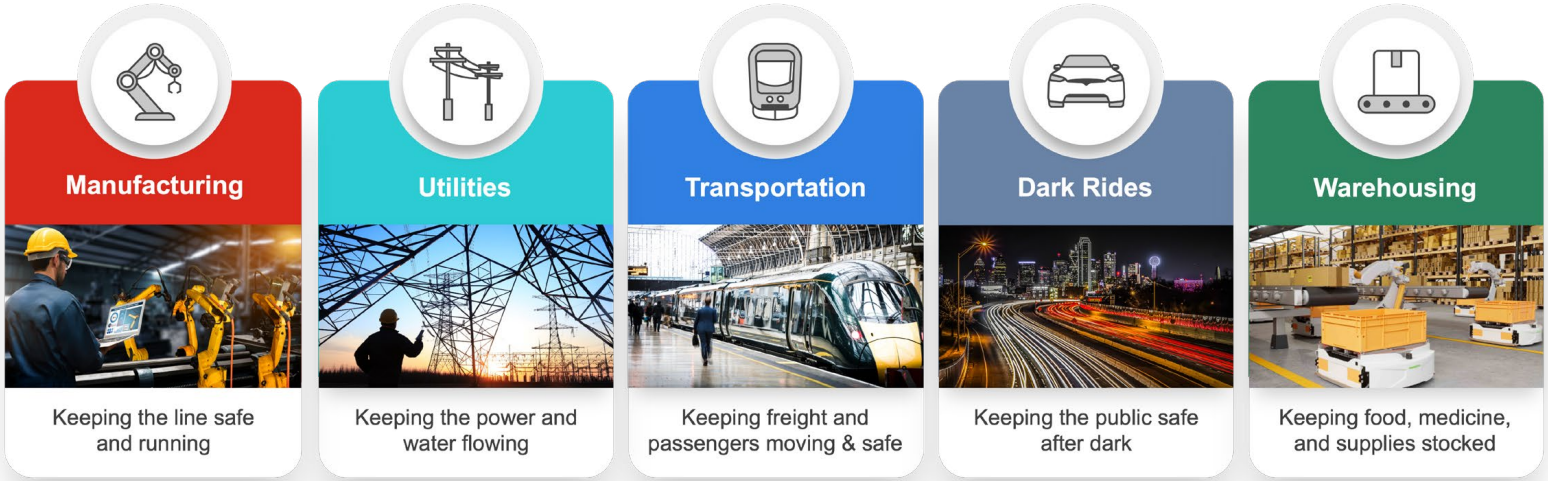
   Many technologies in OT networks are decades old and remain unpatched. Often tied to critical processes such as water pumps or electrical grids, these technologies cannot be shut down for software updates.

In some cases, vendors of these older devices no longer provide updates. As a result, when OT networks are connected to IT, the internet, and the cloud, the unpatched OT systems are exposed to a wide range of threats, which significantly increases organizational risk.

An effective OT security solution provides visibility into OT-specific assets, vulnerabilities, and protocols. It also should offer compensating security controls for unpatched systems. Most often, compensating controls come in the form of vulnerability shielding or virtual patching. In this case, an NGFW leverages OT-specific threat intelligence for information regarding OT-specific vulnerabilities and establishes an intrusion prevention system (IPS) rule, which exists in front of those vulnerable systems to prevent attacks. As a result, the legacy OT system can continue operating uninterrupted while also remaining secure.

Questions to ask:

- How many OT-specific protocols, applications, IPS signatures, and virtual patching rules does your OT security solution support?
- What compensating controls and enforcement mechanisms can your OT security solution provide for legacy technologies in my OT environment?



3. **SOC and incident response:** Although OT network segmentation and visibility are important, these two strategies alone do not provide complete OT security. As CISOs increasingly take ownership of OT infrastructure, they need to show meaningful reductions in the mean time to detect (MTTD) and mean time to respond (MTTR) to cyberthreats as part of a larger effort to reduce organizational risk.

   OT networks should be included in corporate SOC and incident response plans. By incorporating OT infrastructure into these business areas, organizations can begin to converge IT and OT and simplify cybersecurity management. With the ability to detect and respond to threats wherever they occur, CISOs and their teams can drastically reduce the impact of a breach and stop attacks from spreading into more sensitive areas of the OT environment.

   Tools such as network detection and response, endpoint detection and response, deception technologies, and OT-focused central management and reporting can all make the CISO's job easier and make the effort to secure OT more effective. These solutions can also help CISOs on their journey to assess their adherence to often complex regulatory compliance standards.

   Questions to ask:

   - What advanced cybersecurity capabilities does your OT security solution offer?
   - How does your OT security solution enable me to visualize threats and make assessments?

4. **Platform approach:** Many organizations acquire various security solutions from different vendors to address rapidly evolving OT threats and the expanding attack surface. Having a collection of disparate solutions often results in an overly complex security architecture that can inhibit visibility while increasing the burden on already limited security teams.

   A platform-based approach to security can help organizations consolidate vendors and simplify their architecture. A robust security platform with specific capabilities for IT networks and OT environments can simplify solution integration, improve security, and enable centralized management for enhanced efficiency. Integration can also provide a foundation for automated threat response.

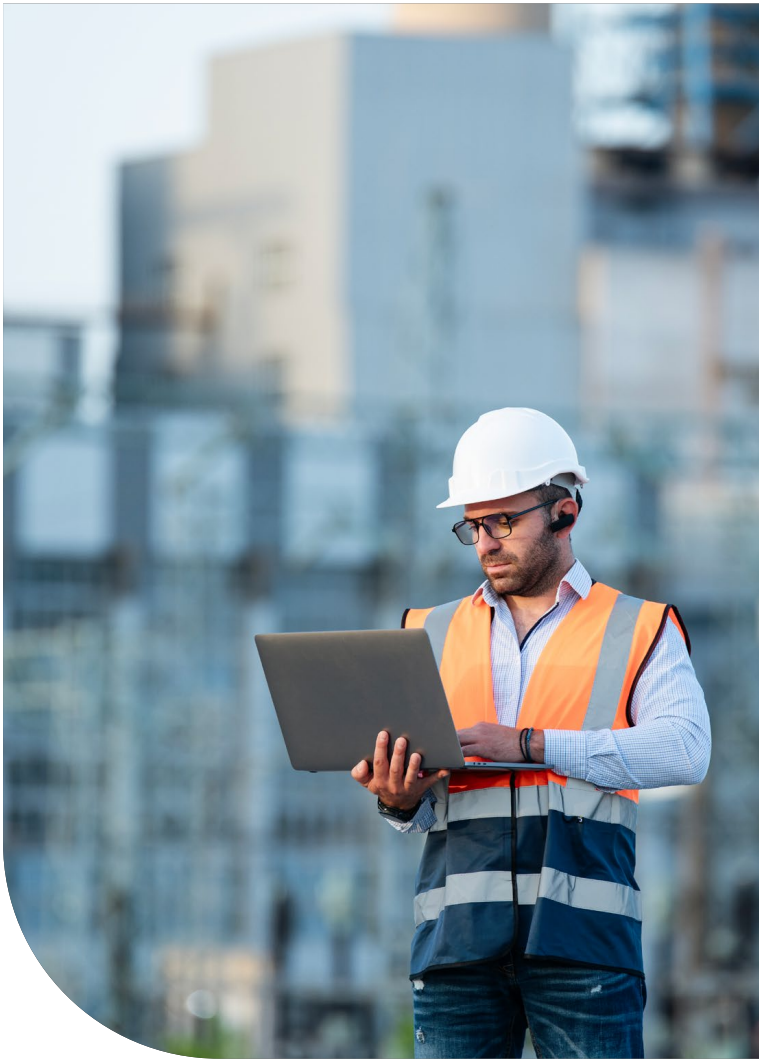
   Questions to ask:

   - What capabilities does your cybersecurity platform include?
   - Can I manage and automate those capabilities with a single management console?
   - Which third-party integration partners does your cybersecurity platform support?

5. **OT threat intelligence:** OT security depends on timely awareness and precise analytical insights about imminent risks. A platform-based security architecture integrates threat intelligence for near-real-time protection against the latest threats, attack variants, and exposures. Although many OT security breaches originate through IT-targeted cyberattacks that spread laterally, some of the most significant incidents over the past 15 years were generated through malware explicitly crafted to exploit OT technologies. Organizations should ensure their threat intelligence and content sources include robust, OT-specific information in their threat feeds and threat-intel services.

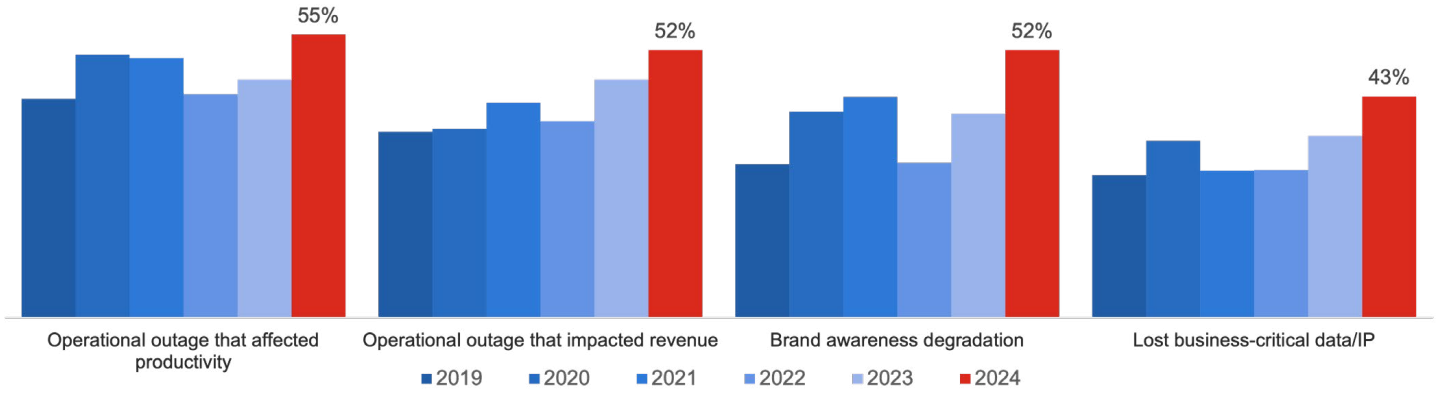
   Questions to ask:

   - What is the scope of threat intelligence backing your security product or solution?
   - How many OT protocols, applications, IPS signatures, and virtual patching or shielding rules are included?



6 out of 10

OT organizations experienced **at least three intrusions** in the past year



Source: Fortinet, 2024 State of Operational Technology and Cybersecurity Report.

Take a Straightforward Approach to OT Security

A comprehensive OT security solution must provide basic OT security, such as asset visibility and network segmentation because they are critical to securing OT environments. The solution also must incorporate and integrate more advanced capabilities, such as advanced threat protection and OT-specific threat intelligence. Incorporating OT assets and networks into SOC and incident response plans is critical to reducing MTTD and MTTR.

Unifying these security capabilities into a platform with a single management console helps reduce security gaps and overall organizational risk. It can relieve overburdened security teams of repetitive, task-based work, so they can be more strategic and implement OT network automation.

The journey to a comprehensive OT security platform does not have to be complicated. It's essential to partner with a highly rated vendor that can provide all the key components in a unified solution. Securing OT is much more straightforward with an OT security platform and increases the likelihood that you'll be successful in improving OT security.

May 20, 2025 10:31 PM / MKTG-939-0-0-EN