



Fortinet OT Security Platform Customer Success Stories

Comprehensive Security for
Converged IT/OT Environments



Table of Contents

Executive Overview	3
Introduction	6
Fortinet OT Security Platform Use Cases	8
Customer Success Stories	10
Why Fortinet?	20
Why Fortinet for OT Security?	21
Conclusion	22



Executive Overview

As OT organizations introduce new digital tools and technologies, security challenges have grown more complex. As the National Institute of Standards and Technology notes, “While security solutions have been designed to deal with these issues in typical IT systems, special precautions must be taken when introducing these same solutions to OT environments. In some cases, new security solutions that are tailored to the OT environment are needed.”¹

The [Fortinet OT Security Platform](#) seamlessly enables security for converged IT/OT networks. The OT Security Platform has features and products extending Fortinet Security Fabric capabilities to OT networks in factories, plants, remote locations, and ships. To alleviate security risks across OT organizations, the OT Security Platform continues to be updated with enhancements ranging from edge products to network operations center (NOC) and security operations center (SOC) tools and services designed to improve performance and operations.



Executive Overview

As an extension of the Fortinet Security Fabric, the OT Security Platform offers secure networking, zero-trust capabilities, network operations, and security operations solutions. AI-powered OT threat intelligence protects against the latest threats. As a broad, integrated platform, the OT Security Platform helps organizations consolidate OT vendors and converge critical IT/OT security resources.

This ebook includes short case studies featuring organizations across multiple industries that have deployed the Fortinet OT Security Platform and can act as a helpful guide for your organization's OT security journey.



The FortiGuard OT Security Service provides:

- Support for over 80 OT protocols
- Almost 3,500 OT protocol rules
- Over 700 OT IPS rules
- Over 1,300 virtual patches
- Almost 1,200 OT app detection rules

Introduction

What is the Fortinet OT Security Platform?

The Fortinet OT Security Platform has several main components:

- Secure networking products, including ruggedized and indoor next-generation firewalls (NGFWs), switches, access points, 5G/LTE gateways, and FortiSRA secure remote access.
- The FortiGuard OT Security Service, a FortiGuard subscription service that makes your FortiGate NGFW “OT aware” with the ability to recognize many popular OT protocols such as Modbus, PROFINET, and OPC. The service also provides visibility into common OT device hardware and device vulnerabilities and protects the network from OT-specific malware.
- Security operations (SecOps) for OT, including deception; network detection and response (NDR); endpoint detection and response (EDR); security information and event management (SIEM); security orchestration, automation, and



response (SOAR); and other robust cybersecurity capabilities to help OT organizations incorporate their OT assets into SecOps ecosystems and incident response (IR) plans, as well as to better understand their compliance posture and adhere to regulations, such as NERC-CIP and NIS2.





Why is the Fortinet OT Security Platform needed?

Many OT organizations have embraced IT/OT convergence to improve various aspects of their organization or business, such as safety, efficiency, production output, and real-time decision-making. IT/OT convergence removes the air gap, connecting traditionally siloed OT assets to IT networks. Unfortunately, many OT devices are years or decades old and remain unpatched due to fear of system failure or lack of patch availability because a vendor has gone out of business. OT organizations often leave their critical assets open to untrusted networks, inviting ransomware, cyberattacks, and potential tragedy. To safely facilitate IT/OT convergence and modernization, OT networks must be properly connected and secured, which is why deploying the Fortinet OT Security Platform is critical to reducing risk.



The Fortinet OT Security Platform Use Cases

Segment OT, establish visibility, and enable compensating controls

Many OT organizations have embraced IT/OT convergence to improve various aspects of their organization or business, such as safety, efficiency, production output, and real-time decision-making. IT/OT convergence removes the air gap, connecting traditionally siloed OT assets to IT networks.

Unfortunately, many OT devices are years or decades old and remain unpatched due to fear of system failure or lack of patch availability because a vendor has gone out of business. OT organizations often leave their critical assets open to untrusted networks, inviting ransomware, cyberattacks, and potential tragedy. To safely facilitate IT/OT convergence and modernization, OT networks must be properly connected and secured, which is why deploying the Fortinet OT Security Platform is critical to reducing risk.



Implement secure connectivity and unified management for OT sites

The Fortinet OT Security Platform includes ruggedized options of our popular secure networking infrastructure products' ruggedized FortiGate NGFWs, FortiSwitch secure Ethernet switches, FortiAP access points, and FortiExtender 5G gateways. Using these ruggedized products, OT organizations can extend the OT Security Platform into their harshest, most-remote locations, including outdoor and fleet vehicle deployments for protection against temperature extremes, shock, vibration, humidity, dust, splashing liquid, and even explosive environments. Fortinet ruggedized products are all managed using the same dashboard and have the same operating system as our indoor products, giving OT organizations a single view across their entire global networking footprint.

Incorporate OT systems into SOC systems and IR plans

As OT organizations converge their OT and IT networks, OT assets must be incorporated into SOC systems and IR plans. The Fortinet OT Security Platform includes deception, NDR and EDR, SOAR, and other cybersecurity solutions to bring OT into the SOC.



Customer Success Stories

The Fortinet OT Security Platform is a comprehensive portfolio of solutions designed to secure OT environments. The following case studies show how Fortinet OT solutions can be successfully deployed in organizations from various industries. We hope you find these real-world success stories inspiring.

1

Toyota Material Handling Converges Its IT and OT Environments with the Fortinet Security Fabric

- 750,000 forklifts sold
- \$5 billion annual revenue
- 1.5 million square feet of manufacturing space



Customer Challenges

- Network reliability
- Securing east-west traffic
- Lack of access controls
- Lack of visibility
- Aging, legacy infrastructure lacking support
- Disjointed solutions and complex management

Fortinet Solutions

- [FortiGate NGFW](#)
- [FortiSwitch](#)
- [FortiAP](#)
- [FortiNAC](#)
- [FortiManager](#)
- [FortiEDR](#)
- [FortiDeceptor](#)

Results

- Significant time savings from consolidated networking and security
- Increased visibility and security of OT environment
- Increased visibility of on-premises devices and remote workers

Business Outcomes

- Improved network and security teams' efficiency
- Improved user experience and satisfaction
- Reduced to training, triage, and new user setup
- Support for secure remote and hybrid work
- Improved networking and security team alignment

[Read the case study](#)



2

Hospital System Consolidates IT/OT Security

- 25-bed critical access hospital with five clinics serving Rush County, Indiana
- The present Rush Memorial Hospital was opened in 1950 and has expanded several times to add new facilities
- HIMSS Analytics Stage 6 accreditation



Customer Challenges

- Lackluster security for on-premises networking and remote teleworkers and vendors
- No security or visibility for IoT/OT devices
- Flat networks with open access
- Lack of visibility into unknown network devices

Fortinet Solutions

- [FortiGate NGFW](#)
- [FortiNAC](#)
- [FortiToken](#)
- [FortiAnalyzer](#)
- [FortiAP](#)

Results

- Consolidated and consistent security policy enforcement across WAN and WLAN networks
- Purpose-built security processors enforce granular security
- Microsegmentation keeps the network healthy
- Increased visibility and control with centralized monitoring over hospital networks including OT

Business Outcomes

- Greater visibility and improved security capabilities for much better protection of IT and operational technology (OT) network resources
- Enhanced protection for physical security systems, such as video surveillance
- Streamlined process for providing guests, such as medical-equipment vendors, access to only the equipment they need

[Read the case study](#)

3

European Renewable Energy Sets Benchmark for Secure IT/OT Convergence in the Cloud

- 1,000+ municipal districts
- 35-Gigawatt portfolio in wind and solar
- 400 employees across 16 offices



Customer Challenges

- Managing the complexity of expanding, diverse, and distributed IT/OT environments
- Disjointed products and providers, including wired and wireless networking providers, maintenance workers, and contractors
- Security concerns related to data to cloud network migration plans

Fortinet Solutions

- [FortiGate NGFW](#)
- [Fortinet Secure SD-WAN](#)
- [FortiSwitch](#)
- [FortiAP](#)
- [FortiClient](#)
- [FortiAuthenticator](#)
- [FortiToken](#)
- [FortiManager](#)
- [FortiAnalyzer](#)
- [FortiSIEM](#)

Results

- Reduced the digital attack surface, enabling self-healing security and automated protection for all users, devices, data, and applications
- Facilitated secure migration of SCADA supervisory control systems to Google Cloud
- Provided real-time, automated response to threats via cutting-edge threat intelligence

Business Outcomes

- Defined new industry benchmark for secure OT/IT convergence in the cloud
- Increased access security through a cloud-based access hub for third-party contractors
- Enhanced OT data acquisition security through secure SDWAN architecture
- Increased visibility and simplified administration with the Fortinet Security Fabric architecture

[Read the case study](#)



4

Swiss Industrial Systems Provider Integrates OT and IT to Enable New Services

- 700 customers
- Founded in 1985



Customer Challenges

- Lack of visibility and data-driven insights in OT systems
- Inability to provide new products and services due to legacy infrastructure
- Insufficient cybersecurity controls to safely facilitate IT/OT convergence

Fortinet Solutions

- [FortiGate NGFW](#)
- [FortiAP](#)

Results

- Enhanced performance and reliability of the OT network
- Implemented robust and comprehensive range of advanced threat-protection capabilities
- Facilitated secure IT/OT convergence, which enabled new routes to revenue
- Offered secure Wi-Fi across all customer sites

Business Outcomes

- Enabled profitable new services through IT/OT integration
- Massively increased cybersecurity for Sisag's customers

[Read the case study](#)

5

Chemicals Manufacturer Secures IT and OT Networks across Five Continents

- \$6.56 billion in revenue
- 7,400+ employees
- Customers in 100+ countries



Customer Challenges

- Global footprint presents increasing cybersecurity challenges
- Disjointed security management and monitoring
- High cost of infrastructure

Fortinet Solutions

- [FortiGate NGFW](#)
- [FortiManager](#)

Results

- Unified security across global locations
- ASIC architecture enabled high-performance threat protection
- Centralized management over multiple firewall devices
- Streamlined policy creation, management, and provisioning

Business Outcomes

- Robust protection of corporate and operational technology networks
- Savings in circuits and equipment
- Cost-effective path to secure networks across five continents
- Increased network visibility with centralized management
- Confidence in long-term value of network security investment

[Watch the video](#)

6

Rural Electricity Co-op Fortifies Its IT and OT Networks with an MSP-Delivered OT Security Platform

- 5,000 miles of power lines
- Serving 25,000 members
- Leading energy nonprofit in 1964



A Touchstone Energy® Cooperative 

Customer Challenges

- Rise in global cyberattacks against OT energy infrastructure
- Securely storing members' personally identifiable information
- Growing attack surface due to unstaffed substations, SCADA, automated metering, and distributed energy systems
- Flat network built without security in mind
- Many end-of-life and end-of-service products in IT stack
- Need for the network to comply with regulations such as NERC-CIP

Fortinet Solutions

- [FortiGate NGFW](#)
- [FortiSwitch](#)
- [FortiManager](#)
- [FortiAnalyzer](#)
- [FortiSIEM](#)

Results

- Consolidated legacy networking and security solutions
- Improved security operations and response time with consolidated management
- Enhanced reliability of IT and OT networks
- Better compliance with industry standards

Business Outcomes

- For HCEC, significant improvement in security posture without increasing IT headcount
- For SkyHelm, a reliable roadmap to service growth by leveraging the Fortinet Security Fabric and through collaboration with Fortinet

[Read the case study](#)

7

Fortinet Solutions Bring Extended Protection to Industrial Networks

- Supplies energy to more than 48 countries worldwide
- Over 96,000 employees
- Over \$100 billion in yearly revenue



Customer Challenges

- Expanding attack surface and network complexity post-acquisition
- Insufficient MPLS circuits to connect remote branches to data centers
- Lack of full visibility over edge traffic to identify threats
- Ballooning costs to manage growing network

Fortinet Solutions

- [FortiGate NGFW](#)
- [FortiSwitch](#)
- [FortiAP](#)
- [FortiManager](#)
- [FortiAnalyzer](#)

Results

- Simplified hardware ecosystem
- Centralized remote management
- Implemented automation
- Streamlined network operations and troubleshooting
- Introduced network segmentation to reduce attack surface

Business Outcomes

- Increased the security and visibility of branch offices and remote industrial networks
- Reduced geographical connectivity costs through a single MPLS networkReduced mean time to remediation by up to 90%
- Simplified the hardware ecosystem with SD-Branch, centralized management and automation
- Improved collaboration between IT and OT teams

[Read the case study](#)



8

Chilean Fishing Company Integrates Network and Security Infrastructure for Remote Locations with the Fortinet OT Security Platform

- Exports to 60 countries
- 3,600 employees
- \$640 million in annual sales



Customer Challenges

- Poor network performance
- Flat, insecure network
- Lack of visibility into network traffic
- Limited visibility into offices by IT
- Distributed locations, including some in harsh environments

Fortinet Solutions

- [FortiGate NGFW](#)
- [FortiSwitch](#)
- [FortiEDR](#)
- [FortiClient](#)
- [FortiAnalyzer](#)
- [Fortinet Secure SD-WAN](#)
- [FortiCare Services](#)

Results

- Protected the entire network from threats
- Enabled each site to address information protection and connectivity needs as they arise
- Converged networking and security

Business Outcomes

- 93% reduction in cyber incidents
- High network availability for remote offices and plants
- New business process availability with a secure network
- Improved satellite internet connectivity at remote locations with secure SD-WAN features
- Complete network infrastructure integration on a single platform
- High visibility of network traffic for improved connectivity and security
- Infrastructure capable of supporting OT projects

[Read the case study](#)



9

Digital Transformation Focused on Enhancing Scale, Security, and Standards for Operational Excellence

- Over 69,000 oil and gas wells
- Over \$860 million in annual revenue
- 17,700-mile midstream system
- 1,600 employees



Customer Challenges

- Unique operating model made integrating new sites into IT stack difficult
- Planned a 100% cloud strategy
- Fragmented point products resulted in vendor finger-pointing and integration challenges

Fortinet Solutions

- [FortiGate NGFW](#)
- [FortiGate VM](#)
- [FortiGate Cloud](#)
- [FortiSwitch](#)
- [FortiAP](#)
- [FortiNAC](#)

Results

- Cloud-first technology strategy driving enterprise digitization
- Common systems driving the DEC digitization strategy

- Enhanced cybersecurity oversight
- IT/OT convergence and data warehousing

Business Outcomes

- Greatly improved security because of increased visibility and the ability to isolate prospective incidents
- Dramatic cost savings as FortiGate virtual machines (VMs) and LTE modems displace MPLS connections, physical firewalls, virtual private network hardware, and other technology
- Cloud and network team can easily manage IT and OT environment across thousands of sites using a single view

[Read the case study](#)

Why Fortinet?

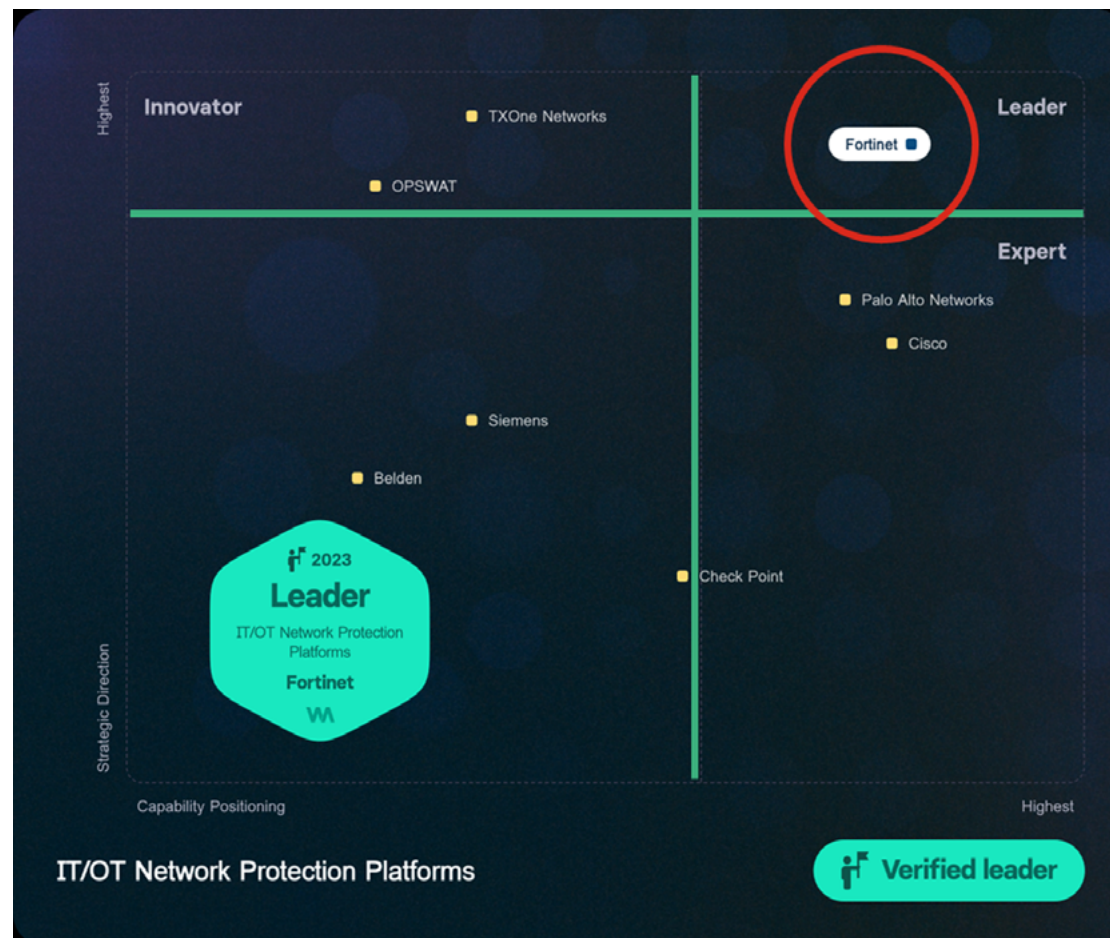
Fortinet is an industry leader in secure networking for OT, and the first vendor to organically develop and integrate SD-WAN, NGFW, advanced routing, and ZTNA application gateway functions into a single platform. These capabilities have been extended into OT environments as part of the Fortinet OT Security Platform. The OT Security Service enables a FortiGate NGFW to protect many popular OT protocols and defend organizations against OT device vulnerabilities and OT-specific malware.

Fortinet is the only vendor with purpose-built ASICs that accelerate and offload network and security functions. For more than 20 years, Fortinet has been driving the evolution of OT cybersecurity with networking and security convergence. Our network security solutions are the most deployed, most patented, and among the most validated in the industry. Our broad, complementary portfolio of cybersecurity solutions is built from the ground up with integration and automation in mind. It enables more efficient, self-healing operations, and a rapid response to known and unknown threats.



Why Choose the Fortinet OT Security Platform?

In addition to real-world customer case studies, industry analysts highly recommend the Fortinet OT Security Platform. Westlands Advisory rated Fortinet as the sole “Leader” in its 2023 IT/OT Security Platform Navigator.² Fortinet is the only vendor that achieved Leader status in the IT/OT Network Protection Platforms Navigator, highlighting the company’s OT network and security experience.



Protect Critical Systems with the OT Security Platform

The Fortinet OT Security Platform is a highly rated solution by customers across many verticals and industry analysts alike. It is foundational for safeguarding and transforming OT. By enabling multiple technologies to work together across IT and OT environments with shared threat intelligence and simplified management, the OT Security Platform helps organizations protect critical systems and data with robust, next-generation security.

Fortinet has a solid history of transforming and securing the networks of many global enterprises with the OT Security Platform. Fortinet continues to support our customers with continued investments in product development and enhancements to the OT Security Platform, and the success stories offer real-world examples of how the Fortinet OT Security Platform can help your organization.

¹ Keith Stouffer et al., [Guide to Operational Technology \(OT\) Security](#), NIST, September 2023.

² Fortinet, [Fortinet Named Sole Leader in 2023 IT/OT Network Protection Platforms Navigator™ Report](#), July 27, 2023.



www.fortinet.com