SOLUTION BRIEF

IT/OT Convergence Provides an Opportunity for Streamlining Operations

Executive Summary

The benefits of converging information technology (IT) and operational technology (OT) outweigh the risks when the proper security is put in place. One of the frequently overlooked benefits of IT/OT convergence is the ability to streamline the security operations in IT and OT environments in a converged security operations center (SOC). The opportunities to manage devices on both sides of the divide, to hunt threats by correlating data input from both sides, and to manage endpoints and deploy deception technologies are tantalizing.

Caution Required

It is extremely important to bring OT awareness and skilled resources into a converged SOC environment. IT best practices may be extremely inappropriate when applied to OT environments and risk doing more harm than good. These risks include accidentally:

- Bricking programmable logic controllers (PLCs)
- Harming the production process by applying patches without consideration of safe and continuous operations of the supervisory control and data acquisition (SCADA) and industrial control system (ICS) processes
- Overdoing the integration of users and account management using the same user authentication system across IT and OT

Also, to minimize process and safety disruptions, operators and managed service providers should hire and train OT experts and leverage their knowledge when staffing SOCs.

With Convergence Comes Risks

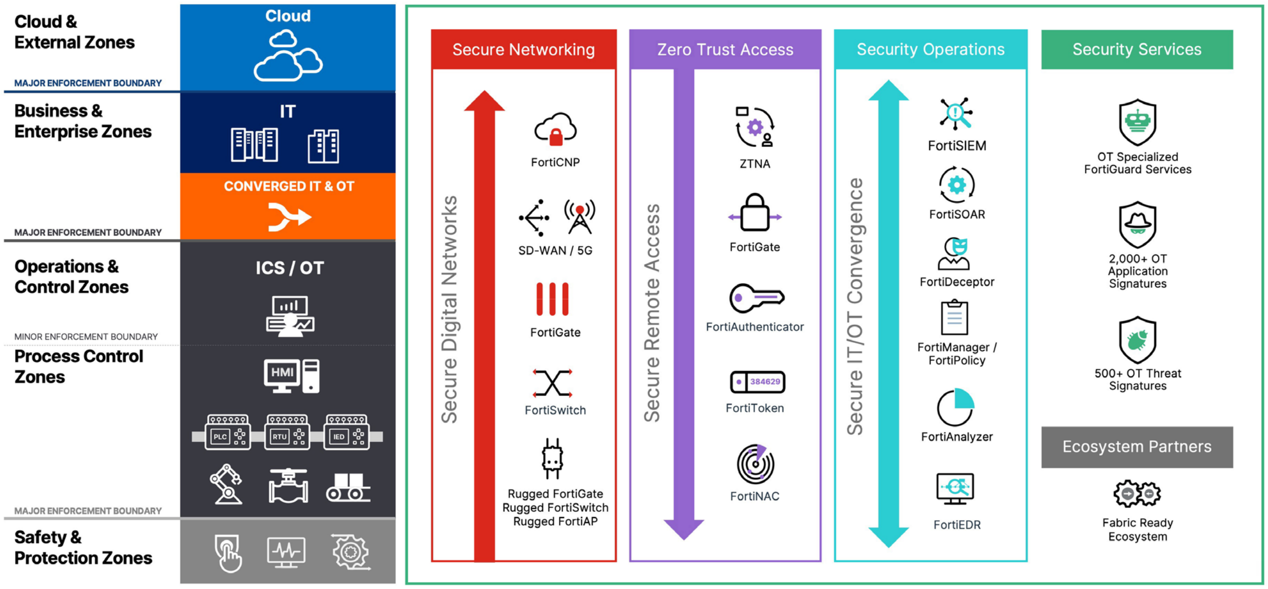
Cyber-physical convergence risks increasing the number of devices exposed to threats and gives attackers a hybrid ecosystem to leverage in their attack chain. Advanced threats can effectively make their way across all parts of an organization's network, including OT systems in industrial, manufacturing, and critical infrastructure environments.

Without proper segmentation protection post-convergence, any threat capable of a successful IT breach has a pathway to vulnerable and potentially valuable targets on the OT side. Introducing new technologies such as the Industrial Internet of Things (IIoT) and 5G further expands the attack surface, exposing industrial systems to increased risk.

"OT environments that were traditionally separated are no longer completely isolated. They now have direct connections for business, OEMs, and other third parties."[1]

Security Fabric – Operational Technology

Typically Deployed Solutions



© Fortinet Inc. All Rights Reserved.

Converged Security Operations

Fortinet has solution sets that help asset owners keep a strong security posture during IT and OT convergence.

Our research has found that asset owners who streamline security network operations from one converged NOC/SOC have the fewest breaches and the best outcomes. The surveyed OT operators who were breached the fewest times were 32% more likely to have their SOC monitor and track OT security.[2]

The key components in a converged SOC that can address IT and OT are:

- Security information and event management (SIEM)
- Security orchestration, automation, and response (SOAR)
- Deception-based breach protection
- Centralized policy management
- Centralized logging and reporting
- Endpoint detection and response (EDR)

Centralized Visibility

FortiSIEM provides centralized visibility to help security operations teams better manage a variety of rapidly changing security, performance, and compliance needs. It also provides real-time, industry-leading, and patented threat detection by cross-correlating network operations center and security operations center analytics. This helps security teams better understand the greater context of their extended environment. And FortiSIEM natively supports multitenant architectures by reporting on separate network segments and virtual and logical environments.

Protecting OT environments from advanced threats requires an integrated security operations platform that can provide visibility of the state of converged assets; detect incidents using known and unknown tactics and techniques; and facilitate a fast and comprehensive incident response plan. From simple log-based correlations to advanced anomalous behavior analytics featuring artificial intelligence (AI) and machine learning (ML), FortiSIEM includes solutions that are specifically designed to protect both OT and IT systems from advanced threats. FortiSIEM can show the tactics, techniques, and procedures (TTPs) of malicious actors leveraging the MITRE ATT&CK Framework for ICS. Also, the MITRE ATT&CK for IT environments and can show how data is moving through the Purdue model.

Unify People, Processes, and Technologies

Integrated into the Fortinet Security Fabric and as an agnostic offering, FortiSOAR is an advanced SOAR product, designed to unify people, processes, and technologies. FortiSOAR supports security teams in rapidly investigating, responding, and improving operational effectiveness across an organization's entire security stack.

Due to lengthy incident response processes, it has become increasingly difficult for analysts to keep up with the pace of incoming alerts. FortiSOAR aggregates these alerts in one place while enriching them with added context to help speed resolution. FortiSOAR streamlines tasks such as alert ingestion, prioritization based on severity levels, and assigning tasks. It also automates more complex exchange-to-exchange (E2E) tasks, such as triage, enrichment, investigation, and remediation, cohesively centralizing security processes by automatically correlating alerts from across a security stack into a single incident.

Only 13% of security operations teams feel they have 100% visibility of OT activities, a number that has declined from 2020 when it was 23%.[3]

FortiSOAR's comprehensive and adaptable features fill gaps opened by complex multivendor systems and processes. It provides a centralized command post for teams throughout the organization to communicate, coordinate, consolidate, and collaborate.

Distributed Deception Platform

OT environments are diverse, with numerous, multivendor devices and systems designed without built-in security. Hardening mostly legacy systems via monitoring agents or security patching to mitigate risks is not always an option due to continuity, costs, patch availability, and more. Organizations need to adopt an assume-breach strategy with in-network detection.

FortiDeceptor is a distributed deception platform (DDP) that provides a non-intrusive, agentless IT/OT deception network to accurately detect active in-network threats. Decoys generate high-fidelity, actionable alerts, resulting in an automated incident response to help stop zero-day attacks.

FortiDeceptor can simulate various types of OT, ICS, and IoT decoys, such as SCADA PLC and HMI, medical IoT, such as PACS and infusion pumps, printers, IP cameras, routers, modems, UPS units, as well as critical applications, such as SAP and other enterprise resource planning (ERP) systems, and more. With advanced built-in quarantine capabilities, FortiDeceptor enables automated response to prevent attacks from progressing. FortiDeceptor is available as either a physical appliance, virtual appliance, or cloud instance, and integrates with enterprise IT infrastructure—and is an integral part of the Fortinet Security Fabric.

Centralized Policy Management and Log Analytics

FortiManager is the single pane of glass for managing FortiGate appliances to consolidate network and security solutions across the IT and OT divide and at multiple levels of the Purdue model. This reduces the organization's attack surface while enabling digital innovation initiatives and it simplifies operations for networking teams.

As an integrated part of the Fortinet Security Fabric, FortiManager provides zero-touch provisioning, centralized management, consistent policies, and automation-driven networking at scale with an extensive open ecosystem. FortiManager can be deployed on-premises in a federated architecture for organizations without internet connectivity and in the cloud for customers that embrace a cloud-native approach.

FortiManager with FortiAnalyzer enhances analytics and improves compliance reporting to drastically reduce the opportunities for configuration errors that lead to cyber-risk exposures and network outages. FortiAnalyzer is the central logging and reporting and advanced analytics platform for FortiGate. It provides easy-to-configure threat monitoring and detection for network anomalies and security policy violations, along with built-in event handlers, threat triage, and out-of-the-box reporting mapped to various IT and OT security compliance frameworks.

Behavior-based Endpoint Protection

EDR solutions are designed to deliver behavior-based endpoint security with real-time visibility, threat analysis, and remediation. They should proactively shrink the attack surface, prevent malware infection with or without an internet connection, detect and defuse potential threats in real time, and automate response and remediation procedures with customizable playbooks.

FortiEDR integrates with the Fortinet Security Fabric natively with hundreds of third-party solutions, and retains the ability to build a custom connector through the REST API framework.

FortiEDR has two critical features that make it well designed for OT environments: First, FortiEDR continues to support legacy end-of-life operating systems such as Windows XP and Windows Server 2003. Second, FortiEDR can be deployed in a hybrid architecture that enables updates from the cloud to be proxied through the customers' data center or other proxy infrastructure.

FortiEDR can block malicious IP addresses on FortiGate or automatically route infected devices to a remediation VLAN with FortiNAC. It can also interface with FortiAnalyzer or FortiSIEM to correlate alerts, logs, and more.

Conclusion

Like cleaning out a cluttered garage so a second car can get inside, the convergence of IT and OT networks provides IT teams an excellent opportunity to streamline the NOC/SOC in a similar way. A successful IT/OT SOC can be built with the knowledgeable input and organizational skills of OT specialists who have significant training and experience in OT.

A well-designed IT/OT SOC should enable it to:

- Ingest data from both IT and OT and provide actionable intelligence relevant to both environments
- Manage firewall and switch policies across IT and OT environments
- Deploy deception capabilities to both environments
- Manage EDR systems appropriate to both environments

Converging IT and OT networks will help your organization streamline operations, cohesively manage devices, hunt threats, and protect important endpoints with a single SOC.

[1] Gartner, Reduce Risk to Human Life by Implementing This OT Security Control Framework, June 17, 2021

[2] Fortinet, 2022 State of Operational Technology and Cybersecurity Report, July 21, 2022

[3] Ibid

November 4, 2022 9:34 AM
1791726-0-0-EN