SOLUTION BRIEF

Secure OT Environments with HCLTech and Fortinet

Executive Summary

As the line between information technology (IT) and operational technology (OT) networks fades and cyberattacks continue to increase, securing converged IT/OT networks requires a specialized infrastructure with advanced security controls. Today, solutions should provide unified visibility of all assets, detect anomalies and threats, and include measures to add security extensions for protection against cybercriminals.

HCLTech 360° SecureOT powered by Fortinet is a dynamic and evolving cybersecurity framework that focuses on three areas: securing the Purdue model, zero trust for OT, and protection of critical infrastructure.

93% of OT organizations experienced an intrusion incident in the past year, with 61% of intrusions impacting the OT environment.[1]

The Challenges of OT Security

In OT environments, the proliferation of OT devices and new technologies brings added risks and has altered the dynamics of managing cybersecurity. Industrial organizations face multiple security challenges, including:

- **Lack of security by design:** Most industrial control systems (ICS) do not have security built in and are sensitive to change.
- **Expanding attack surface:** The attack surface for cyber-physical assets is expanding as air gapping declines.
- **IT/OT network convergence:** The digitization of processes is driving IT/OT network convergence, which opens the door to new threats.
- **Insecure remote access:** The reliance of asset owners on original equipment manufacturers and system integrators exposes critical systems to additional risks.

HCLTech 360° SecureOT powered by Fortinet

HCLTech 360° SecureOT is a dynamic and evolving cybersecurity framework that helps organizations assess, strategize, define, design, and manage their OT landscape. It adheres to industry-accepted cybersecurity guidelines and standards, such as SANS CSC, NIST SP 800-82, ISA 95, and IEC 62443. The framework offers a range of holistic solutions and services that address assets, people, technology, processes, and compliance. The framework offers the following benefits:

- Reduces operational downtime from cyberattacks
- Establishes a solid defense to secure OT environments
- Lowers the total cost of ownership for securing the OT-Internet-of-Things (IoT) landscape
- Enhances the resilience of industrial systems and networks
- Embeds continuous threat and vulnerability monitoring
- Provides visibility into security risks across the enterprise
- Eliminates the risk of revenue leakage due to cyberattacks

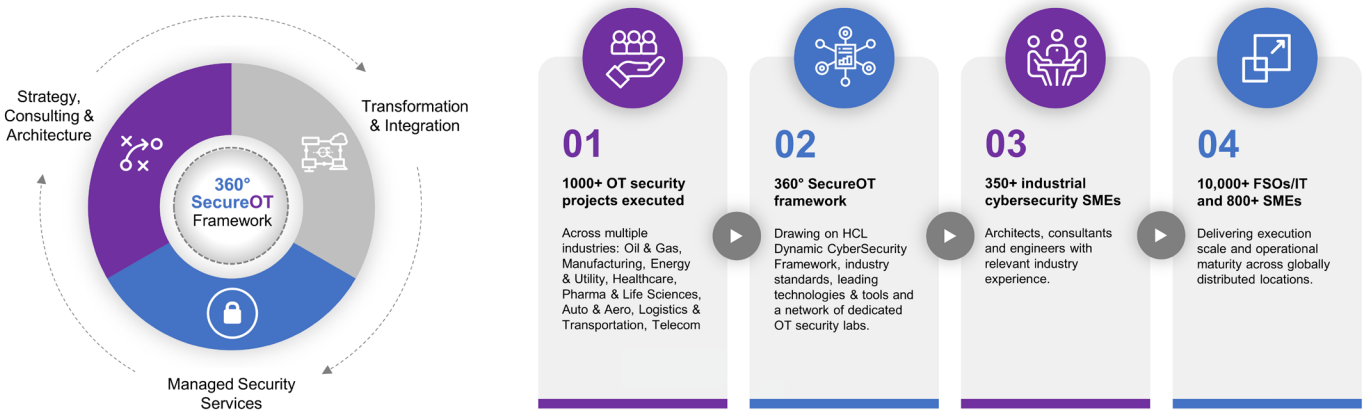

Figure 1: HCLTech helps enterprises secure their OT devices across key focus areas.

To secure OT environments, HCLTech 360° SecureOT focuses on three pillars.

Securing the Purdue model

The different layers in the Purdue model are the logical separation between devices, fields, or cloud gateways and the service back end. Enterprises can secure OT networks using network segmentation and establish security controls at each layer, which eventually creates a cyber-resilient backbone of the OT environment. OT professionals commonly use the Purdue model, separating OT from IT at the base and having a demilitarized zone (DMZ) in between for access control. Fortinet has enhanced the Purdue model with HCLTech best practices to secure every layer from external and internal threats. Within the zones, there are layers describing industrial control components:

- Level 0: Physical components such as motors, pumps, and sensors
- Level 1: Systems monitoring Level 0 devices, such as programmable logic controllers, remote terminal units, and intelligent end devices
- Level 2: Devices controlling system processes, such as human machine interfaces and supervisory control and data acquisition software
- Level 3: Production workflow management, such as batch management, manufacturing execution systems, and data historians
- iDMZ Zone: Separates IT and OT networks to prevent infections
- Level 4: Systems such as enterprise resource planning software, databases, email servers
- Level 5: The enterprise network, which collects data from ICS

Zero trust for OT

Zero trust provides secure monitoring and control for anything inside or outside of the network perimeter. Using zero-trust security principles, perimeter defenses are divided into microsegmented borders, which create a security overlay to enhance OT devices and the associated system. With an effective zero-trust architecture in place, any user can only access the applications and systems they need, with no complex firewall stacks or VPNs required. At the same time, the applications and networks are not visible to the internet.

Protection of critical infrastructure

Any disruption to infrastructure can have serious consequences, including loss of life, environmental damage, and economic losses. In addition, the impact of a cyberattack on these systems can be significant because attackers can gain unauthorized access, manipulate processes, or cause physical damage. HCLTech 360° SecureOT powered by Fortinet provides a comprehensive portfolio of security tools to protect OT resources and critical infrastructure.

HCLTech and Fortinet Integration

The HCLTech 360° SecureOT framework seamlessly integrates with the Fortinet ecosystem, harnessing the combined strengths of people, processes, and tools to deliver a robust OT security framework for enterprises. The HCLTech Security of Things service is dynamic and ever evolving, enhancing security for plants, manufacturing firms, and ICS within OT and IoT. The HCL services encompass the entire spectrum of security, spanning from consultancy and architecture to transformation and managed services.

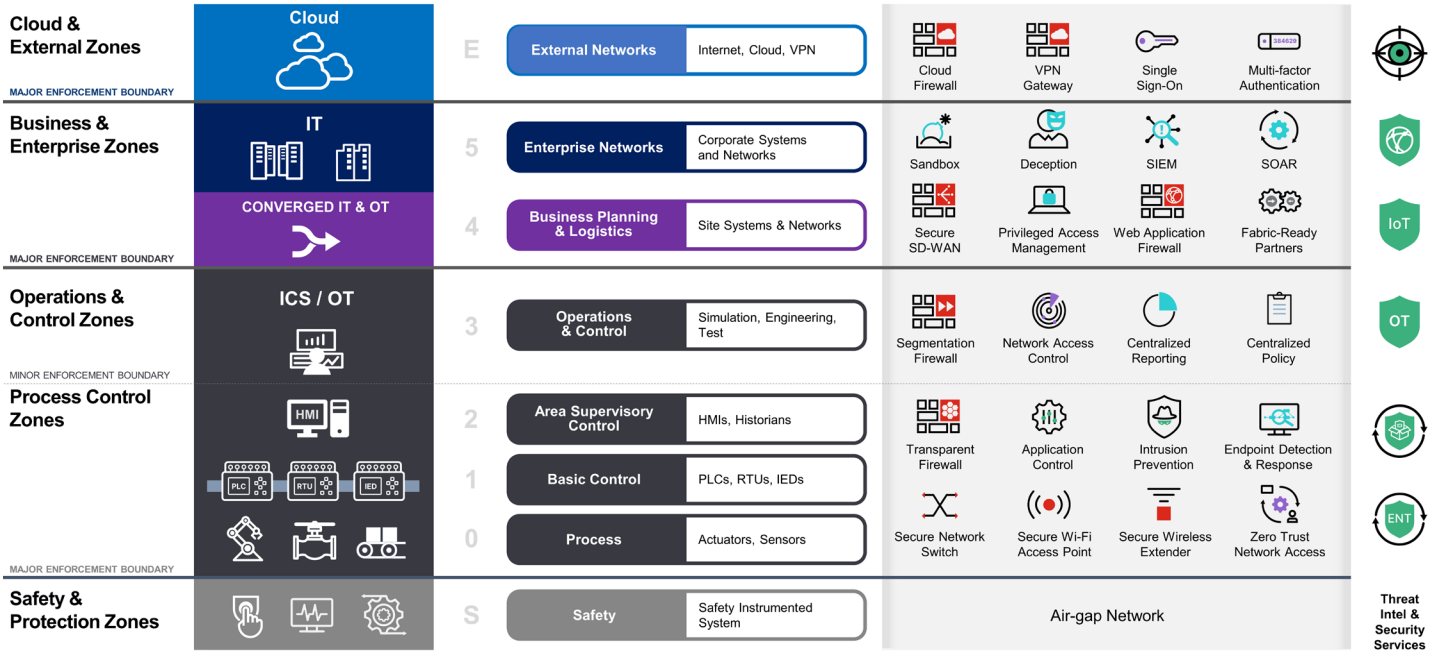

Figure 2: The Purdue model and associated security concepts, serving to safeguard an organization's OT assets

Why HCLTech and Fortinet?

Both HCLTech and Fortinet possess deep security knowledge to help protect public, hybrid, and multi-cloud infrastructure. With over 25 years of experience, HCLTech offers expertise in the form of consulting and managed services from its mature cybersecurity practice to help customers build the right solution for their needs. Fortinet and HCLTech safeguard workloads, privacy, and data for any cloud architecture. Learn more by visiting Fortinet and HCLTech.

[1] Fortinet, 2022 The State of Operational Technology and Cybersecurity, June 2022.

Copyright © 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

November 18, 2023 1:00 AM
2425591-0-0-EN