OT Security for Cyber Risk Management at the Edge in Factory Automation

An In-Depth Look at OT Cybersecurity with IEI's
Network Appliance and Edge Gateway

intel partner

Titanium

▶ **In the ever-changing industry landscape, integrating traditional and modern systems poses cybersecurity challenges. In 2022, the global count of malware attacks surged to 5.5 billion, marking a two percent rise from the previous year∗.**

This highlights the vulnerability of interconnected systems, especially in Operational Technology (OT) security. Cybersecurity experts stress the need for comprehensive solutions, emphasizing adaptability and cost-efficiency. Notably, there's been a 2000% increase in cyber-attacks on industrial control systems (ICS), according to IBM∗.

Project Requirements and Challenges

At the core of every industrial facility lies a network of industrial control systems (ICS), consisting of purpose-built controllers commonly referred to as Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs). These controllers are specialized devices that form the foundation of all industrial processes. In today's advanced Operations Technology (OT) environments, the attack surface is extensive, with numerous potential points of vulnerability. Without comprehensive visibility, security, and control across the integrated IT and OT infrastructure, the question is not if an attack will occur, but rather when it will happen.

Our client, a leading cybersecurity service provider, has observed a rising demand for OT cybersecurity solutions as IT and OT converge. This growing interest comes from companies seeking efficient ways to tackle the expanding scope of OT cyber threats. Specifically, handling cyber risks in operational technology (OT) presents major challenges, especially for industrial organizations that don't have strong asset visibility and vulnerability management strategies.

In response to these complex requirements and challenges, our client embarked on a search for a highly experienced and reliable hardware solution. The objective was to maximize the reliability and longevity of its OT security solution."

Integrated OT Security Suite

Grounded in a longstanding collaboration, our client turned to IEI and its extensive range of networking and edge hardware. IEI had the scale and supply chain in place to keep pace with future demand as well as the technical capability to customize its standard models as needed.

The OT security solution offers unparalleled visibility across both IT and OT security operations, ensuring comprehensive situational awareness across all global sites and their corresponding assets. This powerful solution is designed to provide a single interface for monitoring and managing security, allowing for seamless control and coordination. With its advanced capabilities, organizations can confidently safeguard their operations and assets, mitigating potential risks and ensuring the highest level of protection.

The solution has already demonstrated its effectiveness in practice by monitoring, alerting potential attack routes and protecting vital industrial infrastructure from cyber threats for various industries. IEI's network security appliance and edge gateway are essential in improving visibility, security, and control across all operations.
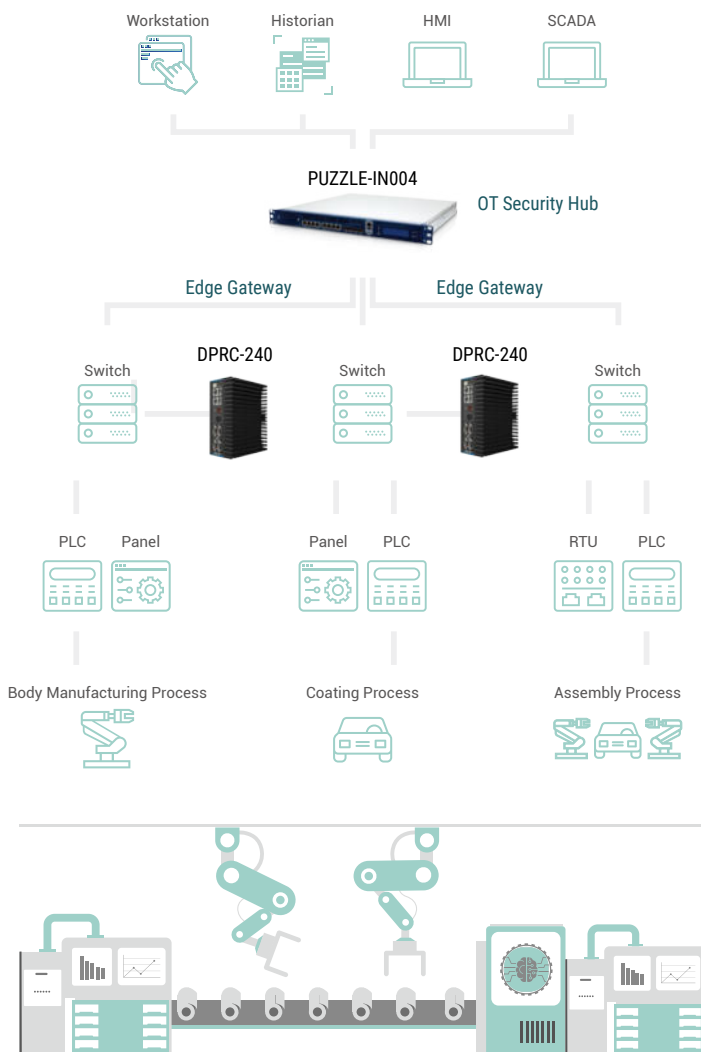
Next-gen OT Security Hub

IEI's PUZZLE-IN004 is a versatile white-box verified to meet the criteria for the Intel Select Solutions for uCPE configuration, powered by Intel® Xeon® D processor. Its 1U sleek enclosure prioritizes space efficiency and reliability with a redundant power supply. Furthermore, the platform has been validated as a VNF-ready system.

In order to enhance network agility, Virtualized Network Functions (VNFs) optimize by transitioning individual network and traditional security functions into a virtualized environment. These functions operate within virtual machines (VMs) or containers, guaranteeing the delivery of agile and scalable services. IEI acts as the choreographer, seamlessly blending reliability and flexibility, while supporting open-source software and virtualization to deliver a tailored security solution.

Following extensive testing, our client opted for the customized PUZZLE-IN004 as the management server. The expertise of IEI's networking team proved invaluable throughout the testing and implementation phases. This collaboration has yielded solutions designed to meet the diverse needs of users.

▶ PUZZLE-IN004

1U Rackmount Network Appliance with Intel® Xeon® D Processor

- Intel® Xeon® D: Multi-core processor with Intel® QAT, Smart NIC SR-IOV and DPDK hardware acceleration
- VNF optimized: Specifically designed to host VNFs
- Multiple storage interfaces: Fast and stable data transmission through two PCIe NVMe and two SATA 6Gb/s connectors.
- High-speed networking: Eight GbE RJ-45 and four 10GbE SFP+ ports
- 300W redundant PSU: Ensures continued operation even if one PSU fails
- Open-source ready: Supports open-source software, such as pfSense® and OPNsense®

More Information about PUZZLE-IN004 please visit:
https://www.ieiworld.com/tw/product/model.php?II=691

DIN-Rail Edge Gateway

The DRPC-240, serving as the edge gateway, scans and collects data from connected devices, providing real-time responses. It transmits collected data to the PUZZLE-IN004 for cyber threat analysis before sending it to the data center for further examination.

These devices meet specific requirements, including, DIN-rail mounting methods, customizations for I/O ports, and the ability to handle thermal challenges. Our client chose IEI's edge systems for seamlessly fulfilling these needs and integrating into their product range with a unique logo and design.

▶ DRPC-240

Highly configurable modular embedded computer designed to cater to the full spectrum of usage requirements for performance-intensive and space-limited applications

- High processing capability: 11th Gen Intel® Core™ embedded processor
- DIN-rail mount: Easy installation on the factory floor
- Fanless design: Ensures more reliable operation, -20 to 60 degrees Celsius
- PoE power supplies: Quad 2.5GbE ports and 15W power output per port (Optional)
- DC input: Supports 12−28V DC power input
- Modular expansion: PCIe x4 slot for an AI accelerator or add-on card for faster edge computations.

  More Information about DRPC-240 please visit: https://www.ieiworld.com/tw/product/model.php?II=871

Results

IEI's networking powerhouse, the PUZZLE-IN004, transformed our OT security landscape. With unique support for top-tier security software, real-time analytics, and high-speed LAN ports, it fortified OT security while simplifying network management. The DRPC-240 was seamlessly integrated into factory field sites, contributing to enhanced data collection and real-time responses, and transmitting data for thorough network threat analysis. IEI's solutions proved to be the unsung heroes of industrial-edge computing, exceeding expectations.

Our clients affirmed: "We had a clear vision of what the unit should deliver. The PUZZLE-IN004 not only met but also exceeded our expectations, with IEI accommodating our specific customizations seamlessly. We were seeking a capable partner with extensive experience, especially in meeting industrial requirements. IEI delivered on all fronts, providing us with planning security for future evaluations."

Why choose IEI?

IEI, a globally recognized networking and edge computing solutions provider for over two decades, offers rapid customization services tailored to customer requirements. With international certifications, IEI products ensure cost optimization and quicker time-to-market in markets worldwide.

IEI Integration Corp. builds up the business as a leading industrial computer provider, and turns to artificial intelligence and networking edge computing.

IEI's products are applied in computer-based applications such as factory automation, computer telephony integration, networking appliances, security, systems, and in fields like AI, IoT (Internet of Things), national defense, police administration, transportation, communication base stations and medical instruments. IEI continues to promote its brand products as well as serving ODM vertical markets to offer complete and professional services.

For more information or sales inquiries, please click the button below to submit your inquiry.

Sales Inquiry

* Source:
https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/
https://www.sprintzeal.com/blog/cyber-attack-statistics-and-trends#:~:text=The%20number%20of%20reported%20attacks, significant%20economic%20and%20safety%20implications.