

How Robust Are Your Cybersecurity Solutions?

From Compliance to Real-World Threats

- Trends & Regulations
- IEC 62443 Standards
- Security Management
- Product Selection Guide



Why Advantech

At Advantech, we see cybersecurity as a cornerstone of digital transformation. With decades of experience in industrial computing and a commitment to continuous innovation, we lead with a secure-by-design mindset. Our cybersecurity practices align with global standards like IEC 62443 and ISO/IEC 27001, helping customers reduce risk, accelerate compliance, and stay ahead of evolving threats. When security matters, trust Advantech to deliver more than just technology—we deliver peace of mind.

ADVANTECH

Enabling an Intelligent Planet

Est.

1983

Headquarters: Taipei, Taiwan

Edge Computing and AI-Powered WISE Solutions

iFactory, Energy & Utilities, Intelligent System & AMR, iHealthcare, iCity Services & iRetail



\$9.2B

MARKET CAP (USD)

(Feb., 2026)

HONORS & AWARDS

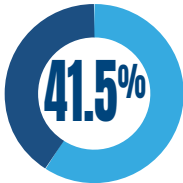
- No.4 in Best Taiwan Global Brands
- Top 5% S&P Global CSA Score
- No.9 in Top 100 Industrial IoT Companies
- Red Dot Product Design Award
- iF Product Design Award

WORLD'S LARGEST IPC COMPANY

Advantech IPC WW Revenue Share

- Advantech
- Other IPC Companies

Source: OMDIA – Market Share estimates for Industrial PCs: World, 2025 Edition



\$2.27B 2025 REVENUE (USD)

KEY ECO-SYSTEM PARTNERS

intel

Microsoft

nvidia

micron

AMD

Canonical Ubuntu

TEXAS INSTRUMENTS

arm

NXP

Qualcomm

MEDIATEK

and more...

QUALITY SYSTEMS IN PLACE

- ISO 9001
- ISO 27001
- ISO 14001
- TL9000
- ISO 17025
- ISO 45001
- ISO 13485
- IECEX QAR
- ISO 14064
- AS 9100
- SONY GP
- ISO 50001

1.8 MILLION+ sq. ft.

MANUFACTURING PLANTS

Linkou, Taiwan



- 10 SMT, 13 system lines
- Engineering sample services
- Complex product lines
- Flexible & quick production

Kunshan, China



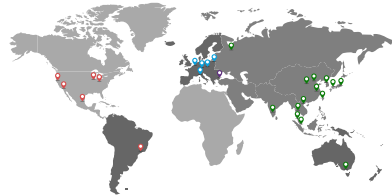
- 12 SMT lines, 15 system lines, 6 chassis lines
- Chassis design & production
- Mature product lines
- Cost-effective production



Nogata, Japan

- 4 SMT lines, 1 system line
- Japan design center, CTOS service, logistics center, repair center

WORLDWIDE OFFICES



- Manufacturing 3
- On-site service 6
- Design centers 11
- Repair centers 15
- CTOS centers 17
- Logistics centers 20

More than 90 offices globally!

9400+ EMPLOYEES



The New Age of Cybersecurity: Are You Ready?

As digital transformation accelerates, cybersecurity threats continue to evolve, driving the need for stringent regulations and proactive security measures. The European Union has introduced critical cybersecurity directives, including NIS2, the Cyber Resilience Act (CRA), and Radio Equipment Directive Delegated Act (RED DA). These regulations highlight the global shift toward stricter cybersecurity governance, urging organizations to adopt robust security frameworks and comply with industry standards.

Regulation	Who is affected?	Which products/sectors matter?	Penalties
NIS2	Companies who operate essential or important IT/OT systems	Sectors that are • Essential for infrastructure (e.g. energy, transport) • Important industries (e.g. manufacturing chemicals, digital services, food)	• Up to 10 million Euros or 2% of annual turnover • Personal liability of management
CRA	Manufacturers, distributors and importers of products with digital elements	Software and hardware products with a direct or indirect data connection to another device or network	• Up to 15 million Euros or 2.5% of annual turnover • Product recalls

Cybersecurity Standards



NIS2 Directive

The NIS2 directive aims to extend the scope of obligations on entities required to take measures to increase their cybersecurity capabilities. The Directive also aims to harmonize the EU's approach to incident notifications, security requirements, supervisory measures, and information sharing.

NIS2 is about laws and policies that mandate critical infrastructure must have cybersecurity measures appropriate to the threats and must report cyber incidents to the regulatory authority.

Cyber Resilience Act (CRA)

The CRA is an EU regulation for improving cybersecurity and cyber resilience in the EU through common cybersecurity standards for products with digital elements in the EU, such as required incident reports and automatic security updates. Products with digital elements are mainly hardware and software whose "intended and foreseeable use includes direct or indirect data connection to a device or network".

For the CRA, product manufacturers are required to develop digital products and software that meet certain cybersecurity requirements. The CRA entered into force on December 10, 2024, with reporting obligations applying from September 11, 2026, and full application from December 11, 2027.



Fortifying Cybersecurity from Within



Cybersecurity Committee (CSC)

For the purpose of enhancing security development and operation process of Advantech's product or service, the Cybersecurity Committee (CSC) is authorized as the taskforce, with efficient communication and effective management, leading relevant business unit and respondents to achieve the goal for product security development and information security.



ISO/IEC 27001

Certified to ISO/IEC 27001, we implement a rigorous, risk-based information security management system that strengthens corporate governance, regulatory compliance, and operational resilience. With a structured security framework and continuous optimization, we ensure a robust foundation for secure and efficient business operations.

Securing the Product Development Lifecycle



Security is integrated into every phase of our product development to identify and address potential vulnerabilities. With IEC 62443-4-1 certification, our Secure Software Development Lifecycle (SSDLC) meets top industrial cybersecurity standards. From development to deployment, our products offer strong protection against cyber threats.

IEC 62443-4-1

The IEC 62443-4-1 specifies the process requirements for the secure development of products used in industrial automation and control systems (IACS). It defines secure development life-cycle requirements related to cybersecurity for products intended for use in the IACS environment.

Secure Software Development Lifecycle (SSDLC)

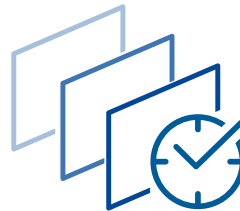
Advantech's SSDLC, based on the IEC 62443-4-1 V-model, integrates security and automation into every phase. With requirement-based testing and thorough validation, it ensures early risk mitigation, faster compliance, and secure, reliable solutions for industrial applications.

IEC 62443-4-2

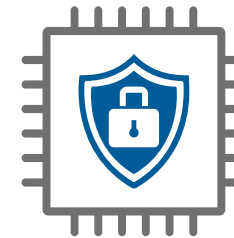
Advantech offers a comprehensive solution to enhance software protection and significantly improve the efficiency of testing and certification. Advantech joins forces with Bureau Veritas, a global leader in testing, inspection, and certification, to help customers overcome security challenges in AIoT and edge computing.



Simplify security assessments and regulatory compliance



Reduce deployment time by integrating pre-certified, security-hardened solutions



Enhance overall system resilience against cyber threats

Proactive Security Measures to Mitigate Emerging Risks

Security Advisory

Advantech maintains a comprehensive vulnerability management process. The ACIRT (Advantech Cybersecurity Incident Response Team) rigorously assesses potential threats to products and provides timely and transparent advisories to the customers. These advisories offer clear guidance and resources to help mitigate risks and maintain the security of the deployments. [Visit our website](#) to stay tuned and secure.

Software Bill of Materials (SBOM)

In line with IEC 62443-4-1, Advantech has implemented an SBOM management mechanism to track and update third-party components with security patches. SBOM provides full visibility into the software supply chain, helping businesses identify vulnerabilities, ensure compliance, and strengthen cybersecurity. By proactively managing dependencies, organizations can mitigate risks and maintain a resilient, secure development lifecycle.

IEC 62443-4-2 Product Offerings

Compact Embedded Box IPC	Modular IPC	Power Automation Computer
		
UNO-2000 Series	MIC-770 Series	ECU-479
Embedded Box PC with iDoor expansion	Modular IPC with Intel® Core™ processors	IEC 61850-3 Certified Power Automation Computer
• Compact, robust, fanless and scalable Box PC with high stability • Stackable modular design with iDoor expandability for flexible configurations • Available in three form factors: regular size (UNO-2484 series), small size (UNO-2372 series), and pocket size (UNO-2271 series) • Scalable processor options from Intel Atom® and Celeron® to Intel® Core™ Ultra	• Certified products include MIC-770, MIC-770 V2, and MIC-770 V3. • Support Intel® Core™ processors across multiple generations. • Support i-Modules, Flex I/O, and iDoor expansion for flexible communication and control. • Compact, fanless design supporting wide DC input and operating temperature ranges	• 13th Gen Intel® Processor with 8+8 Cores • Quad display interfaces for SCADA and more multi-display use cases • Support for a RAID card, HSR/PRP expansion card, and redundant PSU • Supports Intel® AMT, iBMC, SNMP for remote management • Wide operating temperature range, fanless rugged design for harsh environments • Optional 10-year warranty and long product life cycle for substations

**The product offerings are constantly updated as our portfolio of IEC 62443-4-2 certified products expands.*

IEC 62443-4-2 Product Offerings

Touch Panel Computer		Modular HMI
		
TPC-100W	TPC-B300	TPC-B520
NXP® ARM® Cortex®-A53 quad-core processor		With 13th Intel® Core™ processors
• IEC 62443-4-2 Compliant: Secure boot and protection against unauthorized access for robust system integrity. • Versatile Web Terminals: Designed for factory control systems and HMI applications. • Powered by Arm® Cortex®-A53: High-performance processors supporting both Yocto Linux and Android OS. • Multiple Display Sizes: Available in 7" (TPC-107W), 10.1" (TPC-110W), 15.6" (TPC-115W), and 21.5" (TPC-121W). • Industrial-Grade Design: True-flat IP66-rated front panel with P-CAP multi-touch control, supporting -20~60°C operating temperatures.		• Compatible with modular displays (12"-24") featuring slim-bezel, P-CAP touch and high-brightness with 50+ configurations • Single DDR5 memory slot supporting up to 32GB with expansion via three M.2 slots (NVMe, WiFi, 5G) • LAN, POE, isolated serial port and isolated digital I/O via iDoor technology • USB Type-C supporting USB 3.2, DisplayPort 1.4a and 15W power delivery

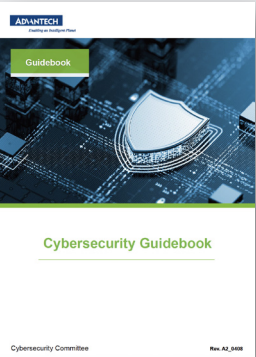
**The product offerings are constantly updated as our portfolio of IEC 62443-4-2 certified products expands.*

IEC 62443-4-2 Product Offerings

Industrial Ethernet Switches			Industrial I/O
			
EKI-5000, EKI-7000, EKI-9000 Series	EKI-8500, EKI-9200 Series	EKI-9500 Series	ADAM-6000/6200-E series
Managed Ethernet Switches	IEC 61850-3 Ethernet Switches	M12 Ethernet Switches	IoT Ethernet I/O Modules
• Offering a full portfolio from 6 to 28 ports, with optional PoE • Support VLAN-based network segmentation and enforce security with ACLs and DHCP snooping to prevent malicious access • Support authentication and identity verification through 802.1X, RADIUS, and MAB • Redundancy: X-Ring Pro (ultra high-speed recovery time < 20 ms), RSTP/STP (802.1w/1D)	• Certified to IEC 61850-3 • Offering a full portfolio with up to 28 ports • TSN and 1588v2 (PTP) supported • IEC 61850-3 protocol (GOOSE, SMV, and MMS) supported • IEC 62439-3 Clause 4 (PRP) and Clause 5 (HSR) compliant • Redundancy: X-Ring Pro (ultra high-speed recovery time < 20 ms), RSTP/STP (802.1w/1D), MSTP	• Certified to EN 50155 • Offering a full portfolio with 8, 10, 12, 16, 20, and 28 ports, with optional PoE • Capability to bind specific MAC addresses to designated switch ports • Support for RADIUS or TACACS+ servers enables centralized user management • Support strict password policy & account management	• IEC 62443-4-2-Compliant Security: Account and privilege management, secure boot, protected firmware and configuration updates, and audit logs safeguard device integrity. • Secure Web and API Access: HTTPS with TLS 1.3 and RESTful APIs enable encrypted I/O access, configuration, and remote device management. • Protected IoT Communications: MQTTs with TLS 1.3 mutual authentication strengthens data protection and device identity verification. • Secure Network Management: SNMPv3 with SHA-256 authentication and AES-128 encryption enables protected device monitoring and administration. • Centralized Device Management: EdgeHub enables cross-site device monitoring, configuration, firmware updates, and status tracking for distributed I/O locations.

*The product offerings are constantly updated as our portfolio of IEC 62443-4-2 certified products expands.

Discover More



eCatalog

Cybersecurity
Guidebook

Download



eCatalog

Star Product
Guide

Download



eCatalog

Secure IT-OT
Connectivity

Download



NEWS

TPC-100W Series Earns
IEC 62443-4-2 Certification

Learn More



NEWS

Advantech and UL Solutions Mark First
IEC 62443 Certification Collaboration

Learn More



Video

Cybersecurity at
Advantech

Watch Now

Regional Service & Customization Centers

China	Kunshan 86-512-5777-5666	Taiwan	Taipei 886-2-7732-3399	Netherlands	Eindhoven 31-40-267-7000	USA	Milpitas, CA 1-408-519-3800	Ottawa, IL 1-800-346-3119
--------------	-----------------------------	---------------	---------------------------	--------------------	-----------------------------	------------	--------------------------------	------------------------------

Worldwide Offices

Asia Pacific		Asia Pacific		Europe		Americas	
Taiwan		Japan		Netherlands		United States	
Toll Free	0800-777-111	Toll Free	0800-500-1055	Eindhoven	31-40-267-7000	Call Center	1-888-576-9668
Taipei	886-2-7732-3399	Tokyo	81-3-6802-1021			Irvine	1-800-866-6008
Taichung	886-4-2372-5058	Osaka	81-6-6267-1887	Germany		Boston	1-949-420-2531
Kaohsiung	886-7-392-3600	Nagoya	81-052-291-4860	Munich	49-89-12599-0	Chicago	1-513-742-8895
		Nogata	81-949-22-2890	Düsseldorf	49-2103-97-885-0	Cincinnati	1-513-742-8895
				Amberg	49-9621-9732-100	Milpitas	1-408-519-3800
						Ottawa	1-800-346-3119
China		Korea		France		Canada	
Toll Free	800-810-0345	Toll Free	080-363-9494/5	Paris	33-1-4119-4666	Toronto	1-800-866-6008
Beijing	86-10-6298-4346	Korea HQ (Seoul)	080-363-9494/5				
Shanghai	86-21-3632-1616			Italy		Brazil	
Shenzhen	86-755-8212-4222	Singapore		Milan	39-02-9544-961	Toll Free	0800-770-5355
Xi An	86-29-8766-9933	Singapore	65-6442-1000			São Paulo	55-11-5592-5355
Kunshan	86-512-5777-5666			UK		Itajuba	55-35-3623-5949
Hong Kong	852-2720-5118	Malaysia		Newcastle	44-0-191-262-4844		
		Kuala Lumpur	60-3-7725-4188	London	44-0-208-317-1380		
		Penang	60-4-537-9188				
		Thailand		Spain		Mexico	
		Bangkok	66-02-2488306-9	Madrid	34-91-668-86-76	Toll Free	1-800-467-2415
						Mexico City	1-800-467-2415
		Vietnam		Sweden		Guadalajara	52-33-3169-7670
		Hanoi	84-24-3399-1155	Stockholm	46-0-864-60-500		
		Hochiminh	84-28-3836-5856				
		Indonesia		Poland			
		Jakarta	62-21-751-1939	Warsaw	48-22-31-51-100		
		Australia		Czech Republic			
		Toll Free	1300-308-531	Ústí nad Orlicí	420-465-524-421		
		Melbourne	61-3-9797-0100				
		India		Ireland			
		Bangalore	1-800-425-5071	Galway	353-91-792444		
		Pune	91-94-2260-2349				

www.advantech.com

Please verify specifications before ordering. This guide is intended for reference purposes only.
All product specifications are subject to change without notice.
No part of this publication may be reproduced in any form or by any means, electronic, photocopying, recording or otherwise, without the prior written permission of the publisher.
All brand and product names are trademarks or registered trademarks of their respective companies.
© Advantech Co., Ltd. 2026