Solution Brief

Healthcare and Life Sciences

AI in the Operating Room Starts with Intel:

Next-Generation Medical Computers Enable AI in Digital Operating Rooms

The Advantech USM-500 medical-grade computer, based on Intel® Core™ and Intel Core Ultra processors, provides AI inference in care settings such as digital operating rooms. It is designed specifically for customization to the individual needs of equipment providers and highly extensible with capture cards, hardware accelerators and other devices.

Key takeaways:

- Digital operating rooms integrate AI to drive better patient outcomes before, during and after surgery.
- Advantech USM-500 medical computers are powered by Intel AI hardware and software technologies.
- Systems are IEC certified for safety and highly customizable for specific implementations.
- AI capabilities can also be applied for security usages, including to prevent growing threats from ransomware.
- This medical grade computer is suitable for deployment in operating rooms and readily integrates with existing medical equipment.

Advancements in healthcare AI applications are especially beneficial in high-intensity clinical settings such as digital operating rooms (ORs). Edge devices powered by AI that enable real-time access to patient vital signs — respiration rate, blood pressure, oxygen saturation — can be lifesaving. Often, hospitals integrate software solutions to streamline surgical workflows, from preoperative planning to postoperative follow-up. By deploying these hardware and software technologies, surgical teams can easily access critical data when they need it and improve patient outcomes. However, the rapid digitization of operating rooms comes with a new category of risk — cyberattacks.

Advantech's USM-500 medical-grade computer was purposefully built to bring secure, low-latency AI inferencing to ORs and other critical-care environments. Manufactured in Advantech's facilities with IEC 60601-1 certification for enhanced patient safety, this white-box device can be easily customized by hospital technology providers.

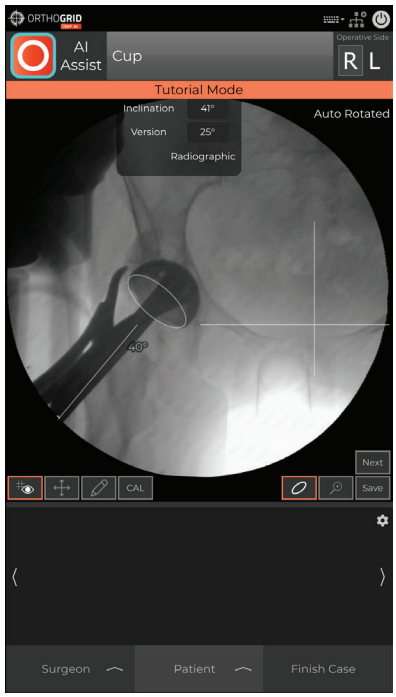
Advantech USM-500 medical computers power AI for digital operating rooms.

In the preoperative stage, Advantech's USM-500 can enhance surgical planning by using discrete GPUs to train AI models to detect key anatomical features and suggest interventional approaches. During intraoperative procedures, the USM-500 can be integrated with cameras, medical imaging equipment, patient monitoring devices and the hospital's electronic medical record (EMR) system. AI applications deployed on Advantech's USM-500 can perform real-time AI inferencing, augmenting surgery through data analytics. Surgeons and surgical staff may leverage data insights to mitigate intraoperative adverse events. Postoperatively, Advantech's USM-500 can be used to drive AI analytics that assess surgical outcomes, evaluate the performance of surgical teams and augment patient recovery.

Intel® Core™ and Intel Core Ultra processors enable Advantech's USM-500 to be extensible with the comprehensive range of devices and technologies found on Intel's edge-to-cloud AI roadmap, including CPUs, GPUs and accelerators, as well as software tools, optimizations and other building blocks. This ecosystem approach streamlines solution development and deployment, accelerating time to market and optimizing product quality.

Advancing solutions for real-time medical AI

USM-500 systems provide the real-time, deterministic performance needed for AI inference at the medical edge. Since many developers are familiar with Intel CPUs and Intel's software enablement for AI on heterogeneous architectures, the USM-500 is an ideal hardware platform for innovation. Advantech can add system components, customize the enclosure and even the board design, thereby building customer-specific devices at scale while maintaining medical certification transparently to the solution provider. This enablement can dramatically lower the barriers to entry for companies in this market segment.



Visual AI assistance during a total hip replacement.

Advantech has established itself as a market leader for low-latency visual AI systems in surgical settings by leveraging their expertise in hardware encoding and real-time video broadcasting solutions. This distinct skill set is especially beneficial in endoscopy. Advantech's best-in-class support for endoscope solutions enables pre-processing of 4K video inputs, after which AI inferencing can occur on the integrated GPU or a discrete GPU before the video output is displayed to the surgical team. Performing AI inference directly on the 4K signal would provide far higher precision than what is required and consume extensive compute resources without delivering added benefit.

The Advantech team's experience building video broadcasting solutions provides the ability to handle such tasks effectively and tune them for high throughput and ultra-low latency required in surgical settings. That expertise extends to concepts such as using hardware encoders, which are outside the familiarity and skillsets of many development organizations.

This type of AI-driven innovation helps advance the state of personalized and precision medicine in the digital operating room. For example, precise orientation is critical during the surgical placement of a prosthetic joint. AI models can be used to minimize or eliminate distortions in preoperative imaging to improve fidelity with actual musculoskeletal structures on the patient. Mapping relative positions in real time between biological markers in the patient's body, the prosthesis and instruments can help ensure accurate placement. By interfacing medical devices with the USM-500, healthcare providers can improve patient outcomes.

Purpose-built systems for AI at the medical edge

The USM-500 medical grade computer incorporates Advantech's decades of hardware engineering expertise to provide a robust, durable solution for low-latency AI inference at the edge that is powerful enough for the real-time compute demands of deep learning applications. Per the device's IEC 60601-1 certification, it is safe to use near vulnerable patients and sensitive monitoring equipment, and long-term system availability helps ensure future-readiness for healthcare facilities.

To accommodate the broad spectrum of system requirements for AI at the edge, the USM-500 can be configured for medium-to-high processing power, as well as with peripheral devices such as discrete GPUs for AI inferencing and video capture cards that connect to sources such as cameras and endoscopes.

- **High performance** for real-time AI algorithms and analysis.
- **IEC 60601-1 certified** for medical use, providing electrical isolation to prevent injury to patients and caregivers as well as service disruptions from outside forces such as electrostatic discharges.
- **Highly extensible** for GPUs, video capture cards, etc.

AI inference can be scaled up with processing on CPUs, integrated GPUs with high execution unit counts on the 12th/13th Gen Intel Core CPUs[1] and discrete Intel® Arc™ GPUs. Intel FPGA-based capture cards may be added for video capture, acquisition and stream processing.

The USM-500 connects wirelessly to the broader digital operating room environment using Wi-Fi and Bluetooth. This full stack of hardware components is supported by Intel's open, non-proprietary programming model, to simplify the development of solutions while avoiding vendor lock-in.

Advantech furnishes safety certifications for the USM-500 computer — including all peripheral components — that are passed through to solutions based on the platform, such as electromagnetic compatibility (EMC) requirements to ensure non-interference with other systems. For example, the systems are rigorously tested for protection against electrostatic discharge (ESD) to comply with international regulations and standards for medical use. Eliminating such considerations from the solution development pipeline for Advantech customers helps accelerate development and reduce the cost of bringing medical edge AI solutions to market.

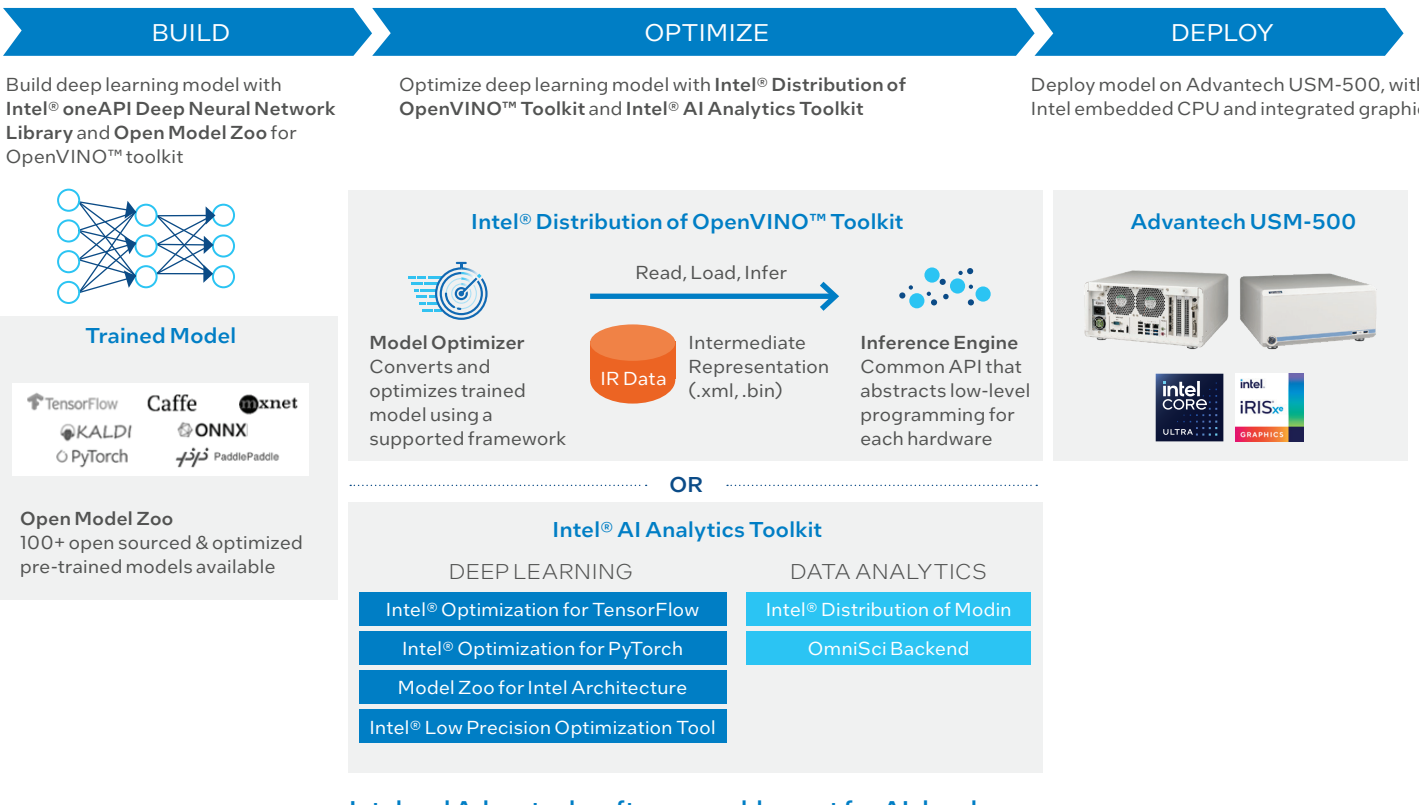
This comprehensive approach to system development for medical applications relieves solution providers from the burden of creating custom products across a spectrum of suppliers. Advantech handles the integration and certification, enabling medical solution providers to focus on their value-added intellectual property, rather than low-level system and deployment considerations. The solution pipeline is improved further by being tightly aligned with Intel's AI technology roadmap as well as the forthcoming introduction of USM-500 designs based on 12th and 13th Gen Intel Core processors.

These platforms will provide up to 96 graphics execution units on Intel® Iris® Xᵉ Graphics integrated GPU to support a high degree of parallelization for AI workloads. Combined with built-in AI acceleration from Intel Deep Learning Boost and the Intel Distribution of OpenVINO™ toolkit, the USM-500 enables fast AI inferencing. Intel Core processors also support Intel Advanced Vector Extensions 2.0, which provides 256-bit instructions that help accelerate many integer and floating point operations to deliver high compute throughput for the digital operating room.

Tapping into an unmatched AI software ecosystem

The value proposition of developing medical AI solutions on the USM-500 is anchored in Intel's broad-based software enablement, which includes upstreaming of performance optimizations wherever possible. Intel is a top contributor to popular open source tools and frameworks, from Python libraries to popular frameworks such as PyTorch and TensorFlow, providing out-of-the-box performance optimizations on Intel architecture.

A common open standards programming model enables performance across CPUs, GPUs and accelerators using Intel development tools such as compilers, libraries, profilers and code-migration utilities. Intel AI developer tools help Advantech customers accelerate time to market with solutions that take full advantage of heterogeneous hardware within USM-500 systems for maximum interoperability.



Intel and Advantech software enablement for AI developers.

Advantech's expertise and its partnership with Intel enable it to engage with solution providers on a consultative level to enable software design. This integration of expertise from the silicon level up through the application tier adds to the comprehensiveness of the stack and helps providers mitigate business risk as they pursue innovative healthcare solutions based on edge AI.

- **The oneAPI programming model** is an open, unified set of technologies and tools for standards-based programming across hardware architectures. It includes common Python, C and C++ APIs that abstract low-level programming for Intel CPUs, GPUs, NPUs (neural processing units) and FPGAs. oneAPI toolkits, libraries and frameworks accelerate both development projects and the AI inference pipelines created by those projects, for benefits that manifest in reduced development time and project cost as well as enhanced solution quality.
- **Intel Distribution of OpenVINO toolkit** is an open source project, powered by oneAPI, that makes it easier to write applications once and deploy them across heterogeneous hardware. It is especially beneficial to software developers who want to leverage Intel performance libraries for compile-time as well as run-time optimizations. It enables Advantech customers to rapidly convert and optimize deep learning models based on almost any framework and deploy them with best-in-class performance on multiple hardware platforms, requiring minimal or no code changes. A faster and more flexible path from concept to production enhances competitive posture and increases agility for future changes.
- **Intel AI Analytics Toolkit** gives AI developers familiar Python tools and frameworks to accelerate end-to-end analytics pipelines on Intel architecture. Developers who want to maintain use of native APIs such as PyTorch or TensorFlow may benefit from this toolkit.

oneAPI and OpenVINO provide the basis for developing software built to operate in today's distributed networks, making them cloud-ready to extend solutions beyond the Advantech device, such as for bulk analytics or federated learning. Moreover, Intel performance engineers continue to refine the performance and energy efficiency of solutions based on these tools, including for future hardware iterations. This orientation adds to solution longevity, with little or no added development burden by digital operating room solution providers.

Securing against ransomware attacks

Ransomware attacks on hospitals are increasingly common. Some hackers gain access to the hospital network by sending phishing emails to hospital employees. Others target vulnerabilities in the environment such as legacy PCs, servers and discrete medical devices. Once hackers gain access, they encrypt the files that run on the computer system, then demand payment for a decryption key to unlock access.

Recent ransomware attacks have cost hospitals millions of dollars for ransom payments, wrongful death lawsuits and loss of revenue because of hospital downtime.[2] Rescheduled surgeries, delays in chemotherapy treatments and patient deaths due to clinicians' inability to access electronic health records highlight the sheer importance of cybersecurity in hospital settings. Many hospitals implement software-based security solutions that help protect against attacks at the software application and operating system (OS) levels. However, hackers have begun exploiting hardware and firmware vulnerabilities.

To mitigate cyberattacks below the OS level, Advantech's USM-500 is equipped with Intel vPro® technology, which delivers built-in, hardware-enhanced security and remote management capabilities. Two key features of the Intel vPro platform that enable detection, protection and recovery from ransomware attacks are Intel Threat Detection Technology (Intel TDT) and Intel Hardware Shield. In addition, Advantech's POC_Link software uses Intel Active Management Technology (Intel AMT), a key ingredient to Intel vPro technology, to enable out-of-band connectivity and remote troubleshooting and repair of USM-500 computers, even when the OS is nonfunctional or missing.

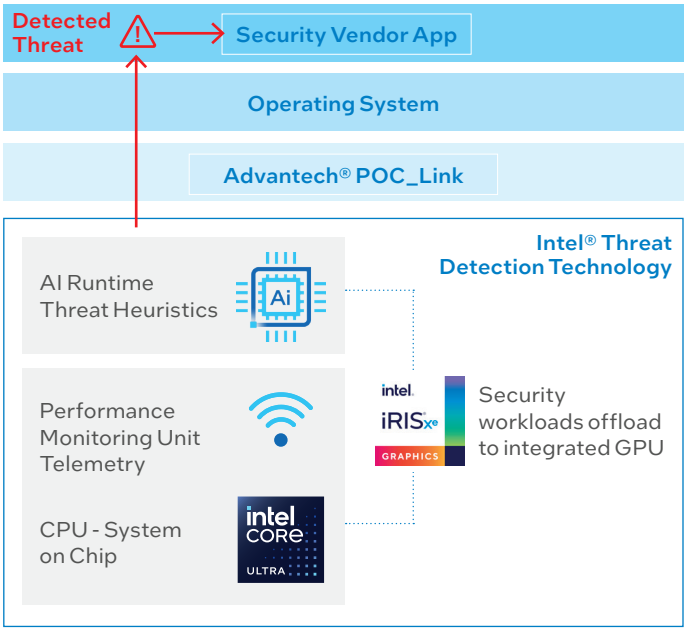
AI-enabled threat detection

Currently, there is a lack of commercially available OS-level telemetry solutions that can detect and monitor file encryption during ransomware attacks. Intel TDT solves this problem by using machine learning heuristics to detect cyberthreats in real time. Specifically, Intel TDT offloads security workloads to the Intel® Iris® Xᵉ Graphics integrated GPU, preserving CPU resources for edge computing. Next, Intel TDT monitors CPU-level telemetry and detects abnormalities in CPU run-time behavior, helping detect file encryption below the OS. Intel TDT is available out-of-the-box in Advantech's USM-500 medical-grade computer; no additional setup is needed to activate this feature when used with an endpoint detection and response (EDR) solution that is Intel TDT-enabled. These include Microsoft Defender, CrowdStrike Falcon and many other leading EDR solutions across both Windows and Linux.

When malware and ransomware attacks are detected by Intel TDT, a high-fidelity signal triggers remediation workflows in the security vendor's application. Leading endpoint security vendor applications such as Microsoft Defender, SentinelOne Singularity, BlackBerry Optics and CrowdStrike Falcon have AI-enabled Intel TDT. Remediation may include rapidly delivering critical security patches. Sometimes affected devices are segmented from the hospital network using perimeter network defenses, enabling the hospital to effectively quarantine the device without shutting down the entire network.

Another beneficial security solution that helps protect Advantech's USM-500 against cyberthreats is Intel Hardware Shield as defined by the set of features in the below table.

Intel® BIOS Guard	BIOS Flash update hardening
Intel Boot Guard	Mitigates unauthorized BIOS boot block modifications
Intel Firmware Restart / Recovery	Recovers from firmware failures
Intel Platform Trust Technology	Stores keys, passwords and digital certificates
Intel Runtime BIOS Resilience	Helps PC manufacturers enforce a below-the-OS policy
Intel System Resources Defense	Enforces resources access policies
Intel Trusted Execution Technology	Measures key components and enables the OS to check against a known good launch sequence
Intel System Security Report	Hardware-to-software channel to gain below-the-OS security visibility



Intel and Advantech security solutions for USM-500 systems.

Collectively, these security features create a tough, hardware-based root of trust that Advantech can tailor to health customer needs to ensure that platforms are protected from manufacturing all the way to deployment.

Rapid recovery

In addition to detecting threats early, Intel TDT also quickly identifies the best recovery points. What's more, Advantech's USM-500 has in-built remote manageability capabilities from Advantech's POC_Link, which leverages Intel AMT. POC_Link offers out-of-band recovery controls such as remote boot, remote patching or remote reload of the OS in a hardware-secured environment. For more information about Advantech's POC_Link, see here.

Conclusion

The Advantech USM-500 medical-grade computer gives healthcare AI solution developers a robust foundation of hardware and software expertise to build on, at any scale. These capabilities are central to building differentiated digital operating room solutions that improve efficiency for caregivers and procedures, helping to reduce costs and improve patient outcomes. With the ability to accelerate time to market and improve solution quality, this offering dramatically lowers barriers to entry and the cost of innovation. By abstracting away complexity, the USM-500 and supporting software ecosystem enable developers to focus squarely on their core expertise as they redefine what's possible.

Learn more:

Advantech USM-500 Medical Computer

AI in Healthcare and Life Sciences

Solution provided by:

intel + ADVANTECH

[1] Intel® Iris Xe Integrated GPU on 12th Gen Intel Core processors and later.

[2] Ryan Levi, "Ransomware attacks against hospitals put patients' lives at risk, researchers say", October 20th, 2023, NPR.

Performance varies by use, configuration and other factors. Learn more on the Performance Index site.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Your costs and results may vary.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Intel technologies may require enabled hardware, software or service activation.

0124/GR/MESH/356870-001US