DARKTRACE

Securing Healthcare Environments with Darktrace / OT & Self-Learning AI

Darktrace / OT delivers real-time visibility, proactive risk management, threat detection, and autonomous investigation across clinical networks, spanning enterprise IT, connected IoMT devices, building automation systems, and on-site facility infrastructure that support patient care.

The Challenge

Hospitals operate highly interconnected environments where clinical care depends on a mix of enterprise IT, IoMT, OT, and building systems. These technologies support patient diagnostics, pharmacy automation, imaging, and the facilities and life-safety systems that keep hospitals operational.

This convergence increases cyber risk. Many medical and building systems run legacy software, cannot be easily patched, and lack traditional endpoint protection. At the same time, ransomware and supply-chain attacks continue to disrupt clinical operations, causing system outages, delayed procedures, and emergency department diversions.

To protect patient safety and maintain operational continuity, healthcare organizations need security that understands how clinical technologies actually behave, continuously learning device and workflow patterns in real time, rather than relying on static rules or signatures that fail to reflect modern healthcare environments.

Why Darktrace / OT?

Unified visibility across clinical and operational environments
Automatically discovers and classifies all connected assets across IT, IoMT, OT, and facility systems, from workstations and servers to infusion pumps, imaging equipment, BMS controllers, and access control. Enriches assets with vulnerability and lifecycle context to improve situational awareness for security teams.

AI-driven threat detection
Self-Learning AI establishes normal behavior across IT, IoMT, and OT devices and protocols. Detects anomalous activity such as unsafe commands, ransomware precursors, and lateral movement early, enabling response before patient care is impacted.

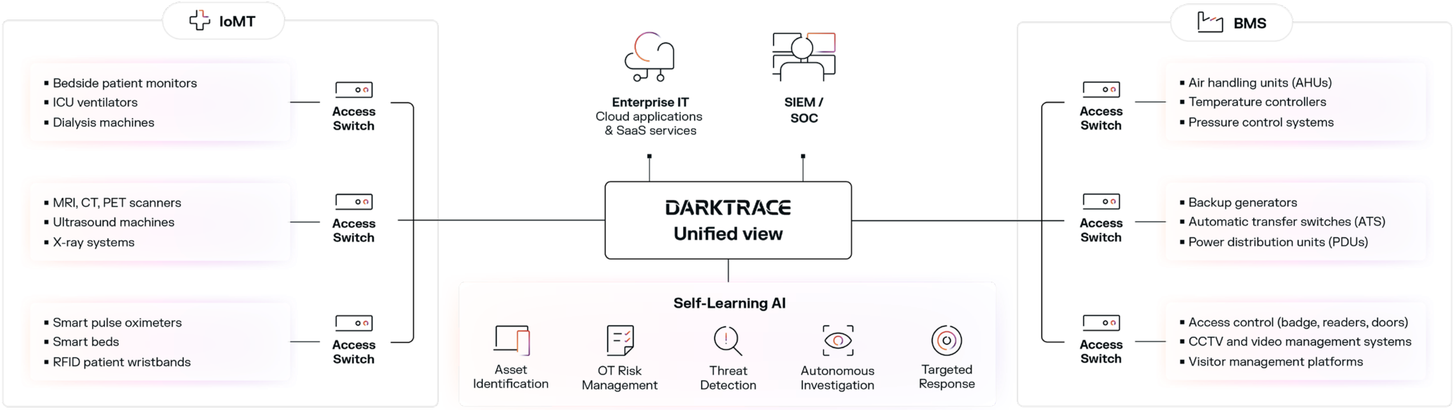
Contextual risk modeling
Continuously maps potential attack paths across clinical systems, BMS networks, and IT-to-IoMT/OT convergence points, prioritizing mitigations by their potential impact on patient safety, operability, and compliance requirements.

Autonomous Investigation & operator-validated response
Darktrace's Cyber AI Analyst automatically investigates and correlates activity across clinical and IT systems, reducing triage time and isolating affected devices within seconds. Optional human approval ensures safe response for medical and life-safety systems.

Compliance without complexity
Automates asset inventory, monitoring, logging, and reporting to support HIPAA, NIST CSF, IEC 62443, ISO/IEC 27001 and HICP. Reduces manual workload for IT, biomed, and compliance teams while improving audit readiness.

Core Capabilities

- Self-Learning AI that adapts to normal behavior across clinical IoMT, OT, and enterprise IT environments.
- Comprehensive discovery and visibility across medical devices, IoT, OT, and facility systems.
- Attack path modeling that reveals realistic lateral movement between IT, IoMT, OT, and BMS infrastructure.
- Deep packet inspection for healthcare and OT protocol traffic, including HL7, DICOM, BACnet, Modbus, MQTT, and RTSP.
- Autonomous investigation with Cyber AI Analyst, reducing mean time to triage by up to 92%.
- Native integration with SOC, security engineering, and clinical engineering workflows.



Compliance Support

HIPAA Security Rule (U.S.)
Supports administrative, technical, and audit controls through continuous monitoring, incident detection, and activity logging to aid breach investigation and reporting.

NIST Cybersecurity Framework
Aligns to Identify, Protect, Detect, Respond, and Recover functions through continuous mapping and AI-driven detection.

HICP & FDA Medical Device Cybersecurity Guidance
Supports secure operation of connected medical devices through behavioral monitoring, anomaly detection, and visibility aligned with FDA pre- and post-market cybersecurity expectations.

IEC 62443 (Global)
Provides continuous monitoring, segmentation validation, and protocol-level visibility across IoMT and OT systems to support industrial cybersecurity requirements.

ISO/IEC 27001
Supports information security management requirements through continuous monitoring, incident detection, and evidence generation across clinical, OT, and enterprise systems.

Key use cases for hospitals & healthcare systems

Clinical asset and device visibility
Maintains a live inventory of imaging systems, patient monitoring stations, infusion pumps, ventilators, ultrasound consoles, lab analyzers, medication cabinets, and building equipment. Flags rogue, duplicate, or misconfigured devices that may introduce safety or security risks.

Detection of unsafe communications or device misuse
Identifies unauthorized access attempts, abnormal remote maintenance activity, unexpected firmware behavior, and anomalous DICOM or HL7 traffic. Detects unusual command execution on pumps, sterilization units, and surgical equipment that could impact patient care.

Containment of IT-to-clinical spillover threats
Recognizes ransomware propagation, credential abuse, and malicious lateral movement from corporate IT systems toward clinical networks, lab systems, or BMS infrastructure, stopping activity before it disrupts care delivery.

Monitoring and securing vendor access
Tracks OEM access to imaging, treatment, and building systems. Identifies off-hours maintenance, unsafe command sequences, or deviations from expected service behavior, supporting supply chain risk management.

Risk management for unpatchable or legacy devices
Provides operationally contextual risk scoring for legacy imaging equipment, end-of-life pumps, older sterilizers, or proprietary OT controllers that cannot be upgraded without impacting clinical operations.

Operational technology protection (BMS + facilities)
Detects unusual BACnet commands, unsafe HVAC adjustments in OR environments, unauthorized changes to power or UPS configurations, and abnormal behavior that could affect surgical, pharmacy, or imaging operations.