

Falcon for XIoT for Healthcare

Delivering extended asset protection across
healthcare environments

Rapidly expanding attack surfaces driven by connected, traditionally unmanaged devices are proliferating across mission-critical clinical environments. Hospitals rely on thousands of legacy and modern internet of medical things (IoMT), internet of things (IoT), and operational technology (OT) assets that are difficult to patch and built with limited security by design, while facing increasing regulatory pressures and a surge in ransomware and supply-chain threats.

Healthcare organizations must balance patient safety and clinical uptime when implementing cybersecurity processes and controls and defining their organizational risk tolerance. This has driven demand for solutions that deliver passive visibility, risk prioritization, and seamless integration with broader hospital IT and clinical workflows. As regulations tighten, new clinical devices are developed, and device connectivity grows beyond traditionally managed IT devices in patient care settings, extended internet of things (XIoT) security — the protection of IoMT, IoT, and OT devices — becomes a core component of effective healthcare cybersecurity.

Unified healthcare XIoT security with the Falcon platform

CrowdStrike Falcon® for XIoT delivers advanced security support for IoMT, IoT, and OT devices. The lightweight, cloud-native CrowdStrike Falcon® sensor provides continuous visibility, monitors device behavior and traffic, and detects anomalies and threats before they can impact patient care.

Falcon for XIoT's asset intelligence, exposure management, and threat intelligence help healthcare organizations safeguard sensitive data, maintain device integrity, and reduce attack surfaces without disrupting clinical workflows. By combining scalable endpoint protection, threat detection, and compliance reporting, the Falcon platform enables security of medical and operational technologies, alongside traditional IT processes and controls, while addressing regulatory requirements and evolving cybersecurity risks.

Key benefits

- **Complete Asset Visibility:** Gain a unified view of all XIoT assets without disrupting patient safety or hospital operations.
- **Comprehensive Risk and Threat Detection:** Prevent shutdown-inducing ransomware, malware, and targeted attacks — the Falcon sensor protects IoT and clinical assets supporting DICOM, HL7, and more.
- **Integration into Existing Healthcare IT Security Workflows:** Integrate with endpoint detection and response (EDR), security information and event management (SIEM), security orchestration, automation, and response (SOAR), and other incident response tools to deliver clinical context within proper prioritization, investigation, and triage to mitigate any clinical disruptions.

Key capabilities

Protects Clinical and Operational Data

Medical devices are mission-critical to patient care and transmit sensitive clinical and patient data. Healthcare environments consist of a wide array of XIoT devices that are internet-connected and susceptible to attacks, and the first step to protecting XIoT in your healthcare environment is knowing exactly what's connected.

- The CrowdStrike Falcon platform delivers detailed visibility into IoMT, IoT, and OT device on your network — from infusion pumps, patient monitors, and imaging systems to IoT devices and IT endpoints.
- The lightweight Falcon sensor provides protocol scanning across unique healthcare IT formats such as DICOM, HL7, and other connected clinical assets.
- Falcon for XIoT provides a detailed profile of XIoT devices, with critical insights such as operating system, firmware version, and potential vulnerabilities that might otherwise go unnoticed.
- Integrated, XIoT-specific vulnerability insights from ExPRT.AI, CrowdStrike's predictive risk prioritization AI engine, enable organizations to take control of their most pressing risks and exposures.

Eliminates Data Silos and Expands SOC Transformation

For optimal patient care, medical device safety and uptime are crucial. Clinical context surrounding incoming threats and efficient detection, triage, and incident response maintain operational continuity and mitigate any patient disruption. Falcon for XIoT expands SOC transformation:

- The lightweight Falcon sensor leverages threat intelligence and AI-driven analytics to detect, prevent, and respond to ransomware, malware, and zero-day attacks specifically targeting clinical assets and other XIoT devices.
- One unified console for IT and XIoT threats detects lateral movement and supports IT/OT boundary protection across converged attack surfaces for under-resourced healthcare security teams.
- Add-on managed detection and response (MDR) services correlate XIoT telemetry to provide continuous, expert-led investigation and response for hands-on security management, operations, and support.

Streamlines Audit and Supports Compliance Requirements

Healthcare is a highly regulated industry with rules and best practices shifting at the federal, state, and local levels. Compliance requirements are constantly evolving with regulatory best practices and increased scrutiny for representation of XIoT assets in audits.

- Falcon for XIoT provides asset visibility across IT endpoints, IoMT, IoT, and OT devices, reducing complexity when identifying assets for required audits.
- Deep device profiling helps to ensure the right processes and controls for auditing and compliance requirements such as HIPAA and other industry regulations.
- Falcon for XIoT integrates with Falcon® Next-Gen SIEM for robust dashboard and reporting across all connected assets across your healthcare network.

Disclaimer

This data sheet includes descriptions of products, features, or functionality that may not be currently generally available. Any such references are provided for information purposes only. The development, release, and timing of all features or functionality remain at our sole discretion and may change without notice. These statements are subject to risks, uncertainties, and assumptions that may cause actual results to differ materially from those expressed or implied. Customers should make purchasing decisions based only on services and features that are currently generally available. For more information on our existing offerings, please talk to your CrowdStrike representative.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Free Trial

