digicert®

DIGITAL TRUST IN CONNECTED HEALTHCARE

Delivering IoMT Security with Device Trust Manager

Overview

Innovations in connected medical devices are revolutionizing patient care, but they are accompanied by a crucial challenge: guaranteeing the security and reliability of these interconnected devices and ecosystems. DigiCert Device Trust addresses security challenges for connected medical devices with a comprehensive solution to meet the needs of the unique security and regulatory requirements within the IoMT ecosystem.

DigiCert Device Trust

Device Security: Device Trust Manager protects IoMT devices and the data they handle with encryption, authentication and device identity management..

Future-Proofed Innovation: Device Trust Manager embeds adaptable security measures directly into the architecture and lifecycle of connected healthcare devices, enabling continuous innovation.

Simplified Compliance: Device Trust Manager adheres to industry and regional regulations, meeting rigorous compliance demands and ensuring devices align with necessary standards.

Flexible Integration: Device Trust Manager seamlessly integrates systems, enabling you to incorporate security measures and delivery secuirty with existing systems.

Risk Mitigation: Device Trust Manager mitigates the risk of breaches, data leaks, and cyberattacks, allowing you to focus on product development without exposing yourself to risk.

Simplifying Complexity

Ensuring security for connected medical devices can be a complex undertaking and one that can be exacerbated by the increasing sophistication of cyber threats. Device Trust Manager simplifies this objective using digital certificates and Public Key Infrastructure (PKI), providing a comprehensive solution that fortifies your IoMT ecosystem. Here's a closer look at how Device Trust Manager utilizes these advanced technologies to safeguard your devices:

Digital Certificates: Creates and manages unique device identities for secure communication.

PKI Framework: Establishes a secure network with cryptographic keys.

Device Authentication: Ensures trusted access and prevents unauthorized entry.

Data Encryption: Safeguards exchanged communication from interception.

Device Lifecycle Management: Delivers end-to-end security from enrollment to decommissioning.

To learn more about DigiCert Device Trust, contact us at sales@digicert.com