# Meet Data Security and Protection Toolkit (DSPT) Requirements with Ordr

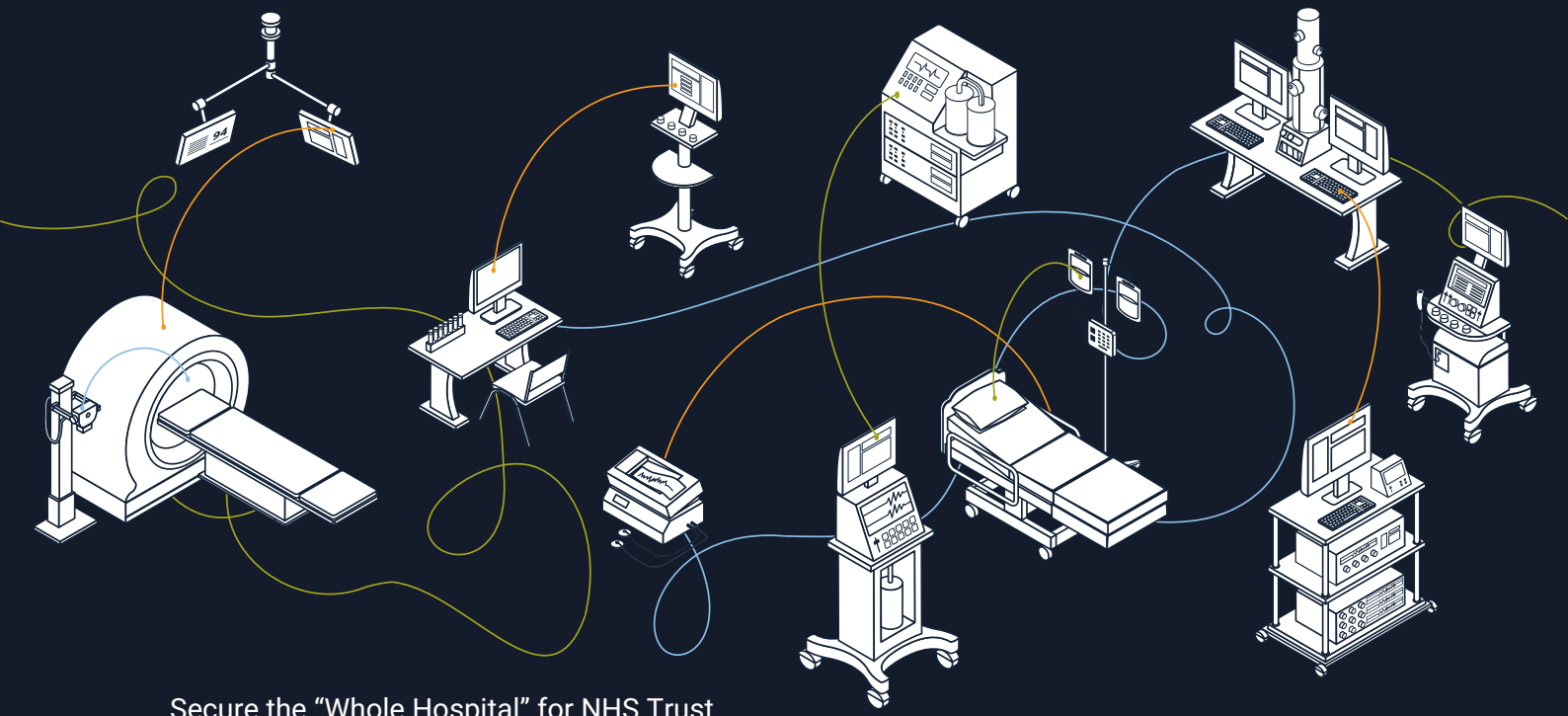
## Overview

Organisations that work with or have access to data and systems of the National Health System (NHS) are required to meet the Data Security Protection Toolkit (DSPT) requirements to maintain a baseline of security and privacy for sensitive information in the NHS digital supply chain.

Because cybersecurity is a dynamic environment, with evolving threats demanding evolving strategies for countering those threats, the DSPT regularly updates its guidelines and recommendations. That makes it imperative to maintain a cybersecurity program that is state-of-the-art to achieve and maintain compliance. It is also important to invest in cybersecurity tools that are engineered to automate the hard work.

## Ordr Connected Device Security

Ordr enables a "Whole Hospital" approach to connected device security built on the philosophy of SEE, KNOW, and SECURE to help organisations close security gaps endemic to connected device deployments which are increasingly common in today's healthcare IT environments.



Secure the "Whole Hospital" for NHS Trust

**The Ordr solution helps the NHS Trust exceed the standards established by the Department of Health and Social Care as articulated under DSPT v4.**

Learn how Ordr maps to the Data Security and Protection Toolkit (DSPT) v4

DOWNLOAD THE GUIDE

ordr.net

ordr

| SEE<br>every asset and connection | KNOW<br>all risks and behaviors | SECURE<br>every thing |
|---|---|---|
| • Discover and profile every device<br>• Map every network connection and flow<br>• Understand device utilization | • Identify devices with vulnerabilities<br>• Identify potential exploits<br>• Identify anomalous behavior | • Proactive Zero Trust policies on NAC, FW, switches<br>• Reactive policies for incident response<br>• Retrospective analysis for new IoCs |

# Key Ordr Capabilities

## Asset Visibility

Automatically discover, accurately classify, and collect high fidelity details of every device on the network including newly connected devices.

## Asset Inventory

Integrate with CMMS and CMDB products to ensure device inventories are always up to date with accurate details.

## Vulnerabilities and Risk

Identify devices with vulnerabilities and risk such as outdated operating systems, unpatched or unauthorized software, PHI, recalls, risky communications, and anomalous behaviour.

## Device Risk Rating

Automatically calculate real-time risk ratings per device by combining vulnerabilities, risk, and customizable parameters to help prioritize remediation and mitigation efforts.

## Vulnerabilitiy Management

Robust vulnerability management and mitigation capabilities including integration with existing IT tools, workflows, and network and security infrastructure to help teams efficiently manage risk.

## Behavioural Profiling

Establish a baseline of normal communications for every device to identify active threats including zero-day attacks.

## Threat Response

Improve threat response and with dynamically created policy enforced with existing security and network infrastructure.

## Accelerate Zero Trust

Automate the creation of Zero Trust policy such as NAC or segmentation to reduce the attack surface and improve security.

## Ecosystem Integrations

80+ integrations with security, network, and IT products to enrich device insights, enable existing workflows, improve security efforts, and accelerate Zero Trust initiatives.

## Compliance

Generate custom reports that map to the DSPT submission and a solution that is SOC 2 Type 2 certified, encrypts data at rest and in motion, does not collect PHI or PII data, and meets GDPR data privacy requirements by ensuring that all data collected remains in the United Kingdom.

The deadline for completing and publishing DSPT v4 self-assessment results is June 30, 2023.

Visit https://ordr.net/dspt to download the guide and learn how Ordr can help or schedule a demo by visiting https://ordr.net/request-a-demo/.