ordr.net

ordr

HOW ORDR MAPS TO THE DATA SECURITY & PROTECTION TOOLKIT (DSPT)

2023

Data Security and Protection Toolkit (DSPT) Overview

In the United Kingdom, all organisations that work with or have access to data and systems of the National Health System (NHS) are required to undergo a data privacy and security self-assessment, known as the Data Security Protection Toolkit (DSPT) every two years. The DSPT is based on 10 Data Security Standards established by the Department of Health and Social Care. The self-assessment process is intended to maintain a baseline of security and privacy for sensitive information in the NHS digital supply chain.

These standards are intended to:

1. Ensure that all staff handle, store, and transmit personal and confidential data properly.

2. Ensure that all staff understand their responsibilities under the National Data Guardian's Data security standards.

3. Conduct annual data security training, including mandatory passage of a test as provided through the Information Governance Toolkit.

4. Restrict access to personal confidential data to staff who need it for their current role, and remove access immediately when it is no longer required.

5. Review and update data management processes annually.

6. Respond to cyberattacks immediately in accordance with CareCERT guidelines, and report data breaches within 12 hours of detection.

7. Maintain a cyberattack continuity and response plan.

8. Use no unsupported software, operating systems, and browsers.

9. Maintain a program for protecting IT systems from threats and update at least annually.

10. Maintain contractual accountability for data protection among all IT suppliers.

According to a February 2023 DSPT v4 update webinar, more than 45,000 self-assessments have been published since the program's inception in 2017. Since then, the DSPT has been updated four times; DSPT v4 went into effect in June 2022 and compliance guidance was published in September 2022. The deadline for completing and publishing self-assessment results under DSPT v4 is June 30, 2023.

There are four possible outcomes for a self-assessment, including:

- Standards exceeded
- Standards met
- Approaching compliance with an improvement plan in place
- Standards not met

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.

Overview of Ordr and the DSPT

To help organisations exceed the standards established by the Department of Health and Social Care as articulated under DSPT v4, Ordr has created a guide to DSPT program compliance. Ordr's guide details each point of DSPT v4 compliance and outlines how Ordr's "whole hospital approach" to connected device security–built on the SEE, KNOW, and SECURE philosophy–can help organisations close security gaps endemic to connected device deployments which are increasingly common in healthcare IT environments today.

Internet of Things (IoT), Internet of Medical Things (IoMT), and operational technology (OT) device deployments are rapidly expanding the total IT inventory of hospitals, home care and hospice services, dental practises, pharmacies, community healthcare facilities, and more. According to a recent study by IBM, the average hospital maintains an inventory of 10-to-15 connected medical devices per patient bed. That doesn't include the many non-medical devices that connect to the IT estate and are common to running a hospital. Other types of devices, like environmental and building controls, communications systems, security and surveillance devices, and more are integral to delivering the best possible patient care today.

Ordr has even found things like vending machines, Peloton exercise bicycles, smart assistants, and Tesla electric vehicles connected to networks, outside the view of IT and security management. Given the proliferation of IoT, IoMT, and OT in healthcare today, here are some statistics that should concern you:

75% of medical devices contain security flaws that make them vulnerable to exploitation by threat actors, and nearly half contain at least two flaws.

As much as **15%** of an organisation's total connected device inventory may be operating as "shadow IoT."

88% of cyberattacks involve an IoMT device, and

Connected devices are the vector for **21%** of ransomware attacks on healthcare organisations.

Key Ordr Capabilities

Asset Visibility

Ordr automatically discovers and accurately classifies every device connected to the network including newly connected devices. The solution collects high fidelity details of every device and integrates with CMMS and CMDB products to ensure device inventories are always up to date with accurate details.

Vulnerability and Risk Management

Ordr identifies devices with vulnerabilities and risk such as outdated operating systems, unpatched or unauthorized software, PHI, recalls, risky communications, and anomalous behaviour. The solution combines these factors with customizable parameters and calculates a real-time risk rating per device to help organisations prioritize remediation and mitigation efforts. Ordr also provides robust vulnerability management and mitigation capabilities and integrates with existing IT tools and workflows in addition to network and security infrastructure to help teams efficiently manage risk for all connected devices.

Behavioural Profiling

Ordr automatically creates a baseline of normal communications for every device known as the Ordr Flow Genome. The baseline is used to identify malicious anomalous behaviour that can be an indication of an active threat such as a zero-day attack. The baseline is also essential to automating reactive policy to stop threats and proactive policy to improve security.

Automated Policy and Actions

Ordr provides built in actions, automated policy creation, and integration with security and network infrastructure to help teams accelerate security efforts. From Ordr, teams can respond to threats by sending commands to block traffic at perimeter firewalls, move devices to a quarantine VLAN, or restrict communications with segmentation. Ordr also automates the creation of Zero Trust policy such as NAC or segmentation to help reduce the attack surface and improve security.

Ecosystem Integrations

Ordr has over 80 integrations with security, network, and IT products to enrich device insights, integrate with existing workflows, enable security actions, and accelerate Zero Trust initiatives.

Compliance

Ordr provides custom reports that map directly to the DSPT submission. In addition, the Ordr platform is SOC 2 Type 2 certified and meets GDPR data privacy requirements by ensuring that all data collected remains in the United Kingdom. Ordr does not collect any PHI or PII data and any data that is collected is encrypted when in motion and at rest.

Data Security Standard 1: Personal Confidential Data

Assertion 1.1: The organisation has a framework in place to support Lawfulness, Fairness and Transparency

Evidence text – NHS Ref Trusts	Ordr Solution
1.1.2 Your organisation has documented what personal data you hold, where it came from, who you share it with and what you do with it.	Ordr provides a list of medical devices that hold personal data such as Protected Health Information (PHI). In addition, Ordr identifies devices with storage that is not encrypted. This information can be submitted as part of the information asset register (IAR).
1.1.4 Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.	Ordr provides a "whole hospital" view of all network connected devices including traditional devices such as servers, workstations, and PCs as well as unmanaged devices such as IoT, IoMT, and OT devices. Each device is automatically identified and accurately classified with detailed information such as make, model, serial number, operating system, installed software, network details, and business/IT owners. This data can be viewed within the Ordr dashboard, exported as a report, or sent via API to an inventory tool such as a CMMS or CMDB as well as other IT tools.

Assertion 1.3: Individuals' rights are respected and supported (GDPR Article 12-22)

Evidence text – NHS Ref Trusts	Ordr Solution
1.3.5 Your organisation operates and maintains a data security and protection risk register (including risks from supply chain) which links to the corporate risk framework providing senior visibility.	Ordr identifies devices with risk and provides insights into devices with outdated operating systems, outdated or unauthorized software, vulnerabilities, PHI, manufacturer recalls, risky communications, anomalous behaviour, and other risk factors. Ordr helps teams prioritize remediation and mitigation efforts by combining these factors with customizable parameters to align with corporate risk frameworks and calculate a real-time risk rating for every device. Ordr also alerts teams when a risk rating for any device changes. Ordr's device risk ratings can be viewed in the Ordr dashboard, exported in reports, and integrated with other security and IT tools.
1.3.6 List your organisation's top three data security and protection risks.	The Ordr dashboard enables organisations to identify top data security and protection risks with a summary of the number of critical, high, medium, and low devices, device categories, vulnerabilities, and incidents. Ordr also provides detailed dashboards to help teams gain a granular understanding of top incidents and vulnerabilities. These insights can also be exported in reports. In addition to helping teams plan remediation efforts, Ordr can help teams deploy mitigations (e.g., compensating controls) to protect at risk devices with dynamically created policies for segmentation and Zero Trust.

Evidence text – NHS Ref Trusts	Ordr Solution
1.3.7 Your organisation has implemented appropriate technical and organisational measures to integrate data protection into your processing activities.	Ordr provides a detailed list of medical devices that hold PHI based on their MDS2 certificate. Ordr alerts when a device holding PHI goes offline and provides "last seen" details to help teams with location efforts. These capabilities are especially critical for devices with PHI where encryption of data at rest is not possible.
1.3.8 Your organisation understands when you must conduct a Data Protection Impact Assessment and has processes in place, which links to your existing risk management and project management, to action this.	Ordr supports the Data Protection Impact Assessment process by providing real-time, up-to-date connected device insights such as granular device details, vulnerabilities, and risk. Insights can be found in the Ordr dashboard, are available as reports, and can be sent to external risk management and project management tools.

Data Security Standard 4: Managing Data Access

Assertion 4.1: The organisation maintains a current record of staff and their roles

Evidence text – NHS Ref Trusts	Ordr Solution
4.1.1 Your organisation understands who has access to personal and confidential data through your systems, including any systems which do not support individual logins.	Ordr integrates with products such as Microsoft Active Directory (AD) to provide insights into user access to devices including devices that store personal and confidential data such as PHI. Ordr also analyses network data to identify user details for devices that do not require a login.

Assertion 4.2: Organisation assures good management and maintenance of identity and access control for its networks and information systems

Evidence text – NHS Ref Trusts	Ordr Solution
4.2.3 Logs are retained for a sufficient period, managed securely, reviewed regularly and can be searched to identify malicious activity.	Ordr collects and aggregates detailed information for each connected device to help teams identify current and past malicious activity. The retention of this data within the Ordr dashboard is configurable to align to organizational policies. Details collated includes information such as that pertaining to vulnerabilities, security incidents, and network communications. Ordr also provides insights into user access via integrations with products such as Microsoft AD, and maintains historical IP address assignments through integration with DHCP tools. All of these details can be viewed in the Ordr dashboard or sent to a log management tool for further analysis. Ordr also provides retrospective capabilities to enable teams to search provious activity against newly defined IoC, thus identifying impacted devices quickly.

Assertion 4.3: All staff understand that their activities on IT systems will be monitored and recorded for security purposes

Evidence text – NHS Ref Trusts	Ordr Solution
4.3.2 Users, systems and (where appropriate) devices are identified and authenticated prior to being permitted access to information or systems.	Organisations may want to employ Zero Trust capabilities such as network access control (NAC) to identify and authenticate devices prior to being permitted access to information or systems. However, such capabilities can be difficult to enforce for IoT, IoMT, OT, and other unmanaged devices. Ordr analyses network data and establishes a normal baseline of communications for each device and each class of device. These insights help teams identify and review essential device communications requirements and are used by Ordr to automate the creation of network access control (NAC) or other Zero Trust policies. Ordr created policies are enforced through integrations with security and/or networking products that exist in the environment.

Assertion 4.4: You closely manage privileged user access to networks and information systems supporting the essential service

Evidence text – NHS Ref Trusts	Ordr Solution
4.4.3 The organisation only allows privileged access to be initiated from devices owned and managed or assured by your organisation	Ordr can automate the creation of Zero Trust policies such as network access control (NAC) to identify and authenticate devices prior to being permitted access to information or systems. Ordr can also automate the creation of Zero Trust policies such as segmentation to control what devices can connect and communicate with across the network. Ordr created policies are enforced through integrations with security and/or networking products that exist in the environment and help to ensure privileged access can only be initiated from devices owned and managed or assured by your organisation.

Assertion 4.5: You ensure your passwords are suitable for the information you are protecting

Evidence text – NHS Ref Trusts	Ordr Solution
4.5.4 Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.	Ordr identifies all devices, including highly privileged systems, that are configured with a weak or default password.

Data Security Standard 6: Responding to incidents

Assertion 6.1: A confidential system for reporting data security and protection from breaches and near misses is in place and actively used

Evidence text – NHS Ref Trusts	Ordr Solution
6.1.1 A policy/procedure is in place to ensure data security and protection incidents are managed/reported appropriately.	Ordr provides multiple capabilities to help teams detect, manage, and report potential data security and protection incidents. The solution utilizes an integrated intrusion detection system (IDS) to identify known attack traffic. The solution also creates a baseline of normal behaviour for each device and uses machine learning (ML) to detect potentially malicious deviations that may indicate compromise or an attack, including zero-day activity. Ordr alerts teams when a security incident is detected and provides detailed insights to aid incident response and forensics efforts. Insights can be viewed in the Ordr dashboard or sent to security information and event management (SIEM) products for security operations centre (SOC) team review. The solution also integrates with existing security and network products and provides automated actions and policies to help accelerate the response to incidents. Ordr also provides retrospective capabilities that are used to analyse how a newly defined/released indicator of compromise (IoC) may relate to previously seen device activity in an environment. This allows teams to identify compromised devices through previous activity such as command and control, ransomware, or other malware related communications. With this insight teams can pinpoint impacted devices and focus remediation and mitigation efforts. A variety of related reports are also available for viewing or exporting from the Ordr dashboard.

Assertion 6.2: All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway

Evidence text – NHS Ref Trusts	Ordr Solution
6.2.1 Antivirus/anti-malware software has been installed on all computers that are connected to, or are capable of connecting to the Internet.	Ordr provides details of antivirus/anti-malware software on devices including installation status, version number, and active/inactive state. With these insights Ordr helps teams identify devices with out of date, disabled or missing antivirus/anti-malware software. Ordr can also confirms devices are communicating with antivirus/anti-malware update servers, to ensure devices are in compliance and have the latest software patches. These details can be viewed in the Ordr dashboard, integrated with ITSM tools, or exported in reports. For IoT, IoMT, OT and other devices that cannot support antivirus/anti-malware software, Ordr monitors all device communications for anomalous and known malicious activity such as communications with command-and-control servers or other malicious destinations. Ordr sends alerts when anomalous activity is detected and enables rapid response with automated actions and dynamically created policies to quarantine or segment impacted devices.

Evidence text – NHS Ref Trusts	Ordr Solution
6.2.3 Antivirus/anti-malware is kept continually up to date.	Ordr identifies devices with missing, disabled, and/or out of date antivirus/anti-malware software. Ordr does this by confirming the installation of antivirus/anti-malware software including version and running status. The solution also identifies communications between devices and antivirus/anti-malware update servers to ensure devices are in compliance and can receive the latest antivirus/anti-malware updates.
6.2.5 Connections to malicious websites on the Internet are prevented.	Ordr continuously analyses network traffic to gain an understanding of device communications and establish a baseline of normal communications for each device. Through this analysis, Ordr identifies device communications to known malicious websites such as command and control (C2) servers or domains in risky geographies such as Russia or N. Korea. Ordr also uncovers zero-day activity by identifying device communications that deviate from a normal device baseline. Ordr integrates with existing security and network products to help teams respond and stop malicious communications. Response options with Ordr include actions such as blocking ports at perimeter firewalls, moving devices to a quarantine VLAN, or dynamically creating and enforcing segmentation policy. Ordr segmentation policy can also be used to proactively prevent potentially malicious connections by restricting device communications to only those that are essential and authorized.
6.2.6 Number of phishing emails reported by staff per month.	Ordr is not an email security/anti-phishing tool, however, the solution does detect malware activity by identifying communications with known C2 servers or other malicious destinations. Ordr also creates a baseline of normal activity for each device and detects deviations from that baseline to identify malicious activity for zero-day threats that do not have a defined indicator of compromise (IoC). Ordr enables teams to block malicious communications and/or isolate impacted devices to stop the spread of threats. This is done with automated actions and dynamically created policy enforced with existing security and network products.

Assertion 6.3: Known vulnerabilities are acted on based on advice from NHS Digital, and lessons are learned from previous incidents and near misses

Evidence text – NHS Ref Trusts	Ordr Solution
6.3.1 If you have had a data security incident, was it caused by a known vulnerability?	Ordr identifies devices with one or more security incident and provides details on all known vulnerabilities for each identified device. Vulnerability details are provided through Ordr integrations with NHS Digital Data Security Centre (DSC) cyber alerts (formerly CareCERT) and other industry standard threat feeds. With these integrations Ordr also helps teams proactively identify devices with known vulnerabilities and provides a device risk rating for each device to help teams prioritize remediation and mitigation efforts.

Evidence text – NHS Ref Trusts	Ordr Solution
	Device vulnerability and incident details are also available as reports viewed or exported from the Ordr dashboard.
6.3.2 The organisation acknowledges all 'high severity' cyber alerts within 48 hours using the respond to an NHS cyber alert service.	Ordr integrates with NHS Digital Data Security Centre (DSC) cyber alerts (formerly CareCERT) and other industry standard threat feeds to enable the immediate identification and risk classification of all devices impacted by each Cyber Alert vulnerability. The solution automatically categorizes devices by vulnerability and severity and alerts when a newly impacted device is identified to help teams meet requirements to acknowledge all 'high severity' cyber alerts within 48 hours. Ordr also helps with remediation and mitigation by providing a device risk rating to help prioritize efforts, vulnerability management capabilities, integration with IT service management (ITSM), and automated actions or policies enforced with existing security and network products. Device vulnerability details are also available as reports viewed or exported from the Ordr dashboard.
6.3.3 The organisation has a proportionate monitoring solution to detect cyber events on systems and services.	Ordr continuously analyses network data to detect and help teams respond to cyber events. The solution utilizes an integrated intrusion detection system (IDS) to identify known attack traffic. The solution also creates a baseline of normal behaviour for each device and uses machine learning (ML) to detect potentially malicious deviations that may indicate compromise or an attack, including zero-day activity. Ordr alerts teams when a cyber event is detected and provides detailed insights to aid incident response and forensics efforts. Cyber events can be viewed in the Ordr dashboard or sent to security information and event management (SIEM) tools for security operations centre (SOC) team review. The solution also integrates with existing security and network products and provides automated actions and policies to help accelerate the response to cyber events. Ordr also provides retrospective capabilities that are used to analyse how a newly defined/released indicator of compromise (IoC) may relate to previously seen device activity in an environment. This allows teams to identify compromised devices through previous activity such as command and control, ransomware, or other malware related communications. With this insight teams can pinpoint impacted devices and focus remediation and mitigation efforts.
6.3.4 All new digital services that are attractive to cyber criminals (such as for fraud) are implementing transactional monitoring techniques from the outset.	Ordr continuously analyses network data to automatically discover and accurately classify every device connected to the network including newly connected devices. Ordr can alert teams when a new device is connected to the network and integrate with device onboarding workflows to ensure devices meet organisational policy. Ordr continuously monitors device transactions and employs an integrated IDS to identify known attack traffic. Ordr also creates a baseline of normal behaviour for each device and can identify anomalous communications that deviate from the baseline.

Evidence text – NHS Ref Trusts	Ordr Solution
	Ordr creates a risk rating for each device that combines device vulnerabilities, communications, and customizable clinical factors. Device risk ratings help teams identify high risk devices and prioritize monitoring and security efforts.
6.3.5 Have you had any repeat data security incidents within the organisation during the past twelve months?	Ordr identifies all devices impacted by a vulnerability and/or incident and helps teams track remediation and enforce mitigation efforts. Device vulnerability and security incident details are also available as reports viewed or exported from the Ordr dashboard to help teams identify any repeat data security incidents during a given period (e.g., past twelve months).

Data Security Standard 7: Continuity Planning

Assertion 7.1: Organisations have a defined, planned and communicated response to data security incidents that impact sensitive information or key operational services

Evidence text – NHS Ref Trusts	Ordr Solution
7.1.1 Your organisation understands the health and care services it provides.	Ordr automatically discovers every device connected to the network including IoT, medical (IoMT), and OT devices for a “whole hospital” view of all devices that comprise health and care services. The solution accurately classifies each device and provides granular details to help teams efficiently group and align devices with services. Ordr also creates a risk rating for each device that combines device vulnerabilities, communications, and customizable clinical factors. Ordr device risk ratings help teams understand device risk in their unique environment to aid in the identification of high-risk devices and prioritization of remediation and mitigation efforts.
7.1.4 You use your security awareness, e.g. threat intelligence sources, to make temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.	Ordr integrates with threat feeds such as NHS Digital Data Security Centre (DSC) cyber alerts (formerly CareCERT) and identifies all connected devices impacted by a given vulnerability. Ordr enables teams to take quick action and make temporary security changes in response to new threats. Ordr actions are enforced with existing security and network products and include actions such as blocking known malicious IPs at perimeter firewalls, quarantining impacted devices, or applying segmentation to reduce the attack surface while keeping devices operational. Ordr also continuously analyses network data and creates a baseline of normal behaviour for each device. The solution identifies and alerts to deviation from the baseline to help teams identify active attacks including zero-day activity.

Data Security Standard 7: Unsupported Systems

Assertion 8.1: All software and hardware has been surveyed to understand if it is supported and up to date

Evidence text – NHS Ref Trusts	Ordr Solution
8.1.1 Provide evidence of how the organisation tracks and records all software assets and their configuration.	Ordr provides an agentless solution to collect comprehensive details from all managed and unmanaged devices running any operating system (Windows, macOS, and Linux) without impact to device operations. Device details collected by Ordr include hardware and software information such as device manufacturer/model, serial number, MAC/IP address, firmware version, operating system type/version/patches, installed software including versions, antivirus version/status, and network/physical location. With these details teams can identify devices with outdated or unpatched operating systems, outdated or unauthorized software, and antivirus that is missing, disabled, or outdated. Device details can be viewed in the Ordr dashboard, viewed/export as reports, or sent to CMDB, CMMS or other inventory tools.
8.1.2 The organisation tracks and records all end user devices and removable media assets.	Ordr automatically discovers and classifies all connected devices including newly connected devices and those used by end users. Device details can be viewed in the Ordr dashboard, viewed/export as reports, or sent to CMDB, CMMS or other inventory tools. Ordr does not provide details on removable media used on end user devices.
8.1.3 Devices that are running out-of-date unsupported software and no longer receive security updates (patches) are removed from the network, or the software in question is uninstalled. Where this is not possible, the device should be isolated and have limited connectivity to the network, and the risk assessed, documented, accepted, regularly reviewed and signed off by the SIRO.	Ordr helps teams identify devices with unpatched, out-of-date, or unsupported operating systems and software, many of which no longer receive security updates or otherwise cannot be patched. Ordr insights help teams identify software that should be uninstalled or devices that should be removed from the network. If uninstalling software or removing a device from the network is not practical or not possible, Ordr enables teams to apply compensating controls such as NAC or segmentation, to reduce the attack surface and limit network connectivity to only those communications essential to operations. Ordr simplifies the process of applying compensating controls by automating the creation of NAC or segmentation policy and enforcing policy with security and network products such as firewalls, switches, and wireless controllers that exist in your environment.

Evidence text – NHS Ref Trusts	Ordr Solution
8.1.4 The organisation ensures that software that is no longer within support or receiving security updates is uninstalled. Where this is impractical, the endpoint should be isolated and have limited connectivity to the network.	Ordr helps teams identify devices with unpatched, out-of-date, or unsupported operating systems and software, many of which no longer receive security updates or otherwise cannot be patched. Ordr insights help teams identify software that should be uninstalled or devices that should be removed from the network. If uninstalling software or removing a device from the network is not practical or not possible, Ordr enables teams to apply compensating controls such as NAC or segmentation, to reduce the attack surface and limit network connectivity to only those communications essential to operations. Ordr simplifies the process of applying compensating controls by automating the creation of NAC or segmentation policy and enforcing policy with security and network products such as firewalls, switches, and wireless controllers that exist in your environment.

Assertion 8.2: Unsupported software and hardware is categorised and documented, and data security risks are identified and managed

Evidence text – NHS Ref Trusts	Ordr Solution
8.2.1 List any unsupported software prioritised according to business risk, with remediation plan against each item.	Ordr collects details of all software installed on connect devices and helps teams identify software that is outdated, unpatched or unauthorized. The solution also calculates a risk score for every device that is a combination of device risk factors such as vulnerabilities, communications, and customizable factors to align with organisational risk frameworks. Ordr then dynamically creates a prioritised list to help teams focus remediation and mitigation efforts.
8.2.2 The SIRO confirms that the overall risks of using unsupported systems are being managed and the scale of unsupported software is reported to your board along with the plans to address.	Ordr identifies all devices with outdated/unsupported operating systems and software and calculates a risk rating for every device. The solution also enables teams to apply compensating controls such as NAC and segmentation by automating policy that is enforced with security and network products that exist in your environment. Reports can be viewed and exported from the Ordr dashboard with details that include the overall risks of using unsupported systems and how those risks are being managed with compensating controls. Exported reports can be shared across teams and with executive staff or board members.

Assertion 8.3: Supported systems are kept up-to-date with the latest security patches

Evidence text – NHS Ref Trusts	Ordr Solution
8.3.1 How do your systems receive updates and how often?	Ordr provides detailed insight into the operating system, installed software, and patch levels of all network connected devices. The solution also integrates with various sources such as the NHS Cyber Alerts (formerly CareCERT) or other threat feeds, MHRA, and manufacturer databases to dynamically identify and alert based on new vulnerabilities, recalls, or available updates. Combining these insights with Ordr created device risk ratings enables teams to prioritise remediation and mitigation efforts or make decisions to remove devices from operations as needed.
8.3.2 How often, in days, is automatic patching typically being pushed out to remote endpoints?	Ordr maintains a view of the patch status for each connected device. This allows teams to not only report on the number of days patching is typically being pushed but also, confirm that automatic patching has successfully been applied.
8.3.4 Where a security patch has been classed as critical or high-risk vulnerability it is applied within 14 days, or the risk has been assessed, documented, accepted, reviewed regularly and signed off by the SIRO with an auditor agreeing a robust risk management process has been applied.	Ordr identifies devices impacted by vulnerabilities and classifies each based on risk level. The solution provides details on when a vulnerability is discovers and when that vulnerability has been cleared providing insight into vulnerability status as well as duration to mitigate risk. These details can be viewed in the Ordr dashboard and are also available as exportable reports.
8.3.5 Where a security patch has been classed as critical or high-risk vulnerability has not been applied, explain the technical remediation and risk management that has been undertaken.	Ordr can dynamically create segmentation policy as a compensating control to protect devices with open vulnerabilities that have not or cannot be patched. Ordr created policies are enforced with security and network products that exist in your environment and enable vulnerable devices to remain in operations while preventing exploitation by reducing the attack surface of the device. The application and status of Ordr policy can be viewed in the Ordr dashboard and details are available as exportable reports.
8.3.6 Your organisation is actively using and managing Advanced Threat Protection (ATP) and regularly reviewing alerts from Microsoft defender for endpoint.	Ordr integrates with IT and security products such as Advanced Threat Protection and enriches these tools with information such as connected device details, vulnerability status, connectivity insights, and device risk scoring. Ordr also integrates with Microsoft Defender for Endpoint to gain additional device related context and alerts.
8.3.7 95% of your organisation's server estate and 98% of your desktop estate are on supported versions of operating systems.	Ordr identifies the operating system and patch level for every connected device. This enables teams to identify devices that require updates as well as those that have reached end-of-life/end-of-support status. For devices that cannot be updated, Ordr can automate the creation of Zero Trust policy such as segmentation to reduce the attack surface and protect outdated or unpatched devices that must remain operational.

Evidence text – NHS Ref Trusts	Ordr Solution
8.3.8 Your organisation is registered for and actively using the NCSC early warning service.	Ordr currently subscribes to a number of 3rd party threat information feeds that include indicator of compromise (IoC) and vulnerability details such as the NHS Digital alarms. The NCSC early warning service is currently only available via email. Once this feed is made available via API's or equivalent, it will be embedded into the Ordr solution and relevant data can be displayed with the Ordr dashboard.

Assertion 8.4: You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service

Evidence text – NHS Ref Trusts	Ordr Solution
8.4.1 Your organisation's infrastructure is protected from common cyber-attacks through secure configuration and patching?	Ordr analyses and documents network and communication details of all connected devices including information such as VLAN, subnet, destination, port, protocol, and device group. With this detail the platform identifies risk such as devices deployed in the wrong VLAN, use of high-risk ports/protocols, unauthorized internal connections, and risky communications with external destinations. Ordr integrates with security and network products that exist in your network to enable teams to perform actions such as moving devices to the correct VLAN, deploying blocking rules at perimeter firewalls, or automating the creation of segmentation policy to limit device communications.
8.4.2 All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support.	Ordr identifies all connected devices with out of date or unpatched operating systems and software. This enables teams to regularly review and prioritize remediation efforts to ensure devices and software are kept up to date. Many unmanaged connected devices such as CT scanners and other connected medical equipment cannot be patched or upgraded due to regulatory restrictions or end of support status. Ordr can help protect these devices by automating the creation of segmentation policy to reduce the attack surface. Ordr policy is enforced through integrations with security and network products that exist in your environment and limits devices to essential communications. With Ordr, organizations can keep out of date devices in production while reducing the risk of vulnerabilities.
8.4.3 You maintain a current understanding of the exposure of your hardware and software to publicly-known vulnerabilities.	Ordr combines insights from NHS Cyber Alert (formerly CareCERT), other industry standard threat feeds, NVD CVE/CVSS, various global sources, active threat defence activities, and primary threat research to help teams maintain an understanding of exposure to publicly known vulnerabilities. These insights also enable automatic, real-time identification and classification in the Ordr Dashboard so teams can prioritize and remediate threats.

Data Security Standard 9: IT Protection

Assertion 9.1: All networking components have had their default passwords changed

Evidence text – NHS Ref Trusts	Ordr Solution
9.1.1 The Head of IT, or equivalent role, confirms all networking components have had their default passwords changed to a high strength password.	Ordr analyses all connected devices including networking components and can identify devices with default or weak passwords.
9.1.2 The Head of IT, or equivalent role, confirms all organisational devices have had their default passwords changed.	Ordr analyses all connected devices including networking components and can identify devices with default or weak passwords. Devices with default or weak passwords are highlighted in the Ordr dashboard as well as reports that can be viewed or exported.

Assertion 9.3: Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities

Evidence text – NHS Ref Trusts	Ordr Solution
9.3.5 The organisation understands and records all IP ranges in use across the organisation.	Ordr uses passive methods to continuously analyse network data and uncover details such as VLAN, subnet information, inter-subnet communications, and subnet to internet communications. These insights enable teams to quickly identify and alert on erroneous traffic flows both internally and internet based.
9.3.6 The organisation protects its data in transit (including email) using appropriate technical controls, such as encryption.	Ordr identifies devices and communications that contain regulated data such as PHI, PII, and PCI in addition to the VLAN where each device is deployed. This enables organisations to ensure devices that transmit unencrypted and sensitive data, such as medical equipment, are appropriately secured and deployed in the correct VLAN (e.g., are not in a “Guest” or other insecure VLAN). Ordr also identifies devices using weak ciphers and expired certificates that can impact the security of data in transit.
9.3.8 The organisation maintains a register of medical devices connected to its network.	Ordr continuously analyses network data to automatically discover and accurately classify all network connected devices including medical devices. The solution gathers granular details for every discovered device such as make, model, serial number, operating system, and software version in addition to real-time vulnerability and behavioural status. Ordr also provides connectivity information such as VLAN, subnet, network switch, and port or access point each device is connected to. Details for each device is available in the Ordr dashboard, can be sent to a CMDB, CMMS, or other inventory tool and can be viewed or exported as a report.

Evidence text – NHS Ref Trusts	Ordr Solution
9.3.9 What is the organisation's data security assurance process for medical devices connected to the network.	Ordr audits all medical devices and gathers granular details such as make, model, serial number, operating system, and software version. The solution also identifies if devices transmit and/or hold encrypted or unencrypted PHI or other sensitive data. This information in addition to vulnerability, communication, and organisational factors are used to calculate a risk score for every device. Ordr insights including the device risk score can be used to aid data security assurance processes by identifying high risk devices and prioritizing remediation and mitigation efforts. Ordr also provides workflows to remediate vulnerabilities and apply compensating controls with automated policy enforced with security and networking products that exist in your environment.

Assertion 9.5: You securely configure the network and information systems that support the delivery of essential services

Evidence text – NHS Ref Trusts	Ordr Solution
9.5.9 You have a plan for protecting devices that are natively unable to connect to the Internet, and the risk has been assessed, documented, accepted, reviewed regularly and signed off by the SIRO.	Ordr provides real-time visibility and protection for all devices that are connected to the network, including those that are natively unable to connect to the Internet. Ordr provides insights into how each device is connected and how they communicate with internal and external (Internet-based) destinations. These insights enable teams to assess current device communications, identify abnormal activity, and take corrective action. Ordr also creates a baseline of normal communications for each device and can identify communications that deviate from that baseline. As an example, Ordr detects and alerts to Internet-based communications to/from a device that normally does not or should not communicate externally. Ordr can also ensure devices cannot communicate with the Internet by automating the creation of Zero Trust policy, such as segmentation. Ordr segmentation policy is enforced with security and network products that exist in your environment and restrict device communications to only those that are authorized and/or essential.

Assertion 9.6: You securely configure the network and information systems that support the delivery of essential services

Evidence text – NHS Ref Trusts	Ordr Solution
9.6.3 The organisation has checked and verified that firewall rules ensure that all unauthenticated inbound connections are blocked by default.	Ordr assesses firewall configurations and reports on enabled ports and services. If deviations from policy and known baseline configuration settings are detected, Ordr can alert, adjust policy, or create new policy as needed. Ordr also continuously analyses network data to identify newly attached,

Evidence text – NHS Ref Trusts	Ordr Solution
	moved, and changed devices and network infrastructure. The solution sends alerts when new devices or changes are detected and provides insights in the Ordr dashboard and through reports that can be viewed or exported from the dashboard.

Data Security Standard 10: Accountable Suppliers

Assertion 10.1: The organisation can name its suppliers, the products and services they deliver and the contract durations

Evidence text – NHS Ref Trusts	Ordr Solution
10.1.1 The organisation has an up to date list of its suppliers, which enables it to identify suppliers that could potentially pose a data security or data protection risk to the organisation. The list includes which suppliers process personal data or provide IT services on which critical services rely, details on the product and services they deliver, contact details and contract duration.	Ordr supports organisational efforts to achieve and maintain a list of suppliers and enable teams to identify suppliers that could potentially pose a data security or data protection risk. The solution does this by automatically discovering and classifying every network connected device, assessing device ownership, and assessing device risk such as outdated or unpatched operating systems and software, vulnerabilities, PHI, risky communications, or other factors. This data can be viewed in the Ordr dashboard or sent to a CMMS, CMDB, or other inventory and IT tools.

Conclusion

DSPT compliance means many organisations are taking a fresh look at their cybersecurity program and making changes to align with NHS Digital requirements. Core security functions such as inventory, risk management, and threat detection are essential to maintaining compliance, and organizations should look for efficient, automated systems that can help provide coverage for all connected devices—from traditional servers, workstations, and PCs to IoT, IoMT and OT devices. Ordr arms organisations with a powerful tool to gain visibility into their network-connected devices, automatically expose potential risk, and automatically enforce policies to either isolate high-risk devices, or to segment systems based on their unique needs, passively and without agents.

To learn more about Ordr and how the solution can help meet your DSPT goals, contact the Ordr team at **info@ordr.net**

ordr

See. Know. Secure.
Every connected device, everywhere

ordr.net