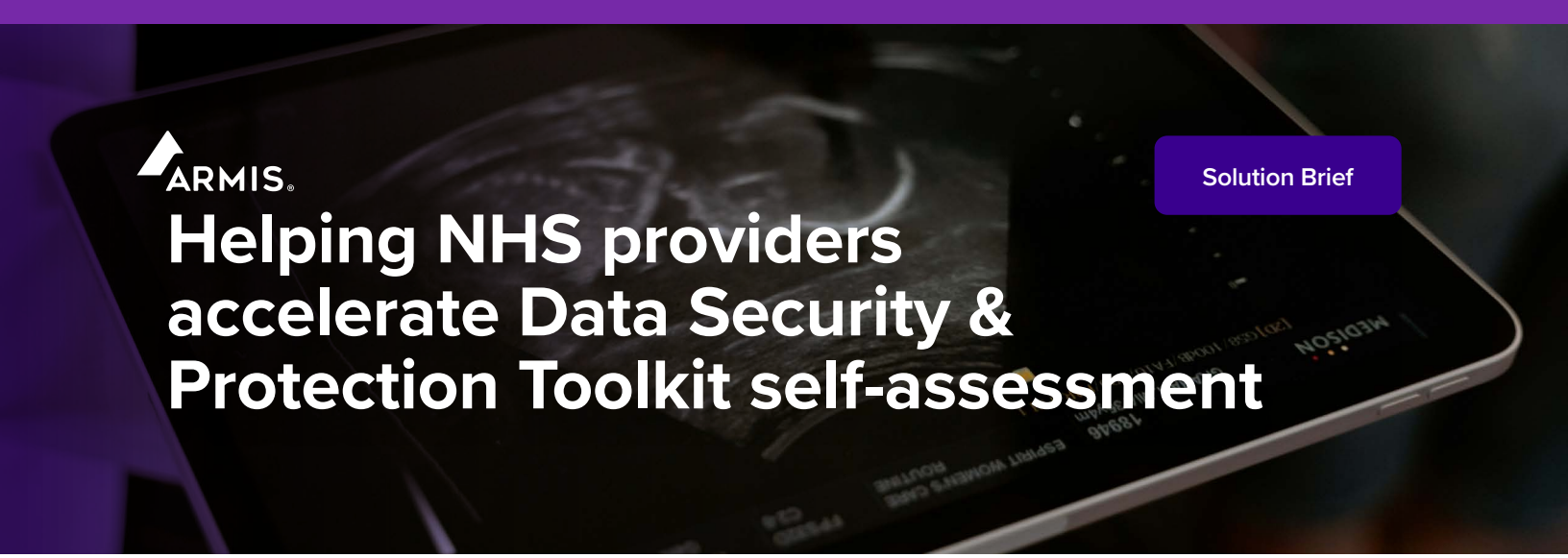

ARMIS

Solution Brief

Helping NHS providers accelerate Data Security & Protection Toolkit self-assessment

The Data Security and Protection Toolkit (DSPT) is a tool organisations can use to evaluate their adherence to the National Data Guardian's 10 data security standards. All organisations handling NHS patient data and systems, including electronic personal health information (ePHI) are required to use this toolkit to ensure proper handling of personal information and sound data security practices.

But for many organisations, creating and maintaining an accurate and up-to-date inventory of devices can be a heavy draw on already strained resources. By automating the identification of devices communicating over the network and identifying risks and vulnerabilities including those in NHS cyber alerts.

Key Takeaways:

- Detect all IoMT, IoT and OT managed and unmanaged assets
- Identify organisational risk and prioritise response
- Reduce resource requirements to achieve DSPT compliance reporting
- Out of the box compliance templates for simplified reporting

Healthcare environments are increasingly hard to secure

Connected devices are growing at an unprecedented rate in healthcare. Advances in virtual and connected care are driving compelling use cases for the additional data, cost savings and improvement to patient experience and patient safety that IoT, IoMT, IT and OT assets can provide.

Some organisations will have platforms that provide a status on managed devices such as Windows machines. While this can provide some sense of security today's attacks are increasingly coming from the unmanaged devices such as IoT, medical devices and building management systems such as the HVAC and lift control systems, most of which cannot have security agents installed. Without a single consolidated view of these assets, attack surfaces remain exposed and unmonitored leaving the organisation vulnerable.

With Armis, NHS Trusts and Integrated Care Board (ICB) Management can automate and accelerate the process of DSPT reporting. Armis provides an NHS Compliance assessment module complete with the necessary dashboards, reports and policies to assess compliance and monitor for any deviations. This compliance module enables organisations to:

- Quickly aggregate managed asset information from existing tools to produce a single source of truth
- Detect unmanaged assets such as IoT, IoMT and OT assets that are communicating across the network
- Quickly identify, classify and provide risk information and reduction steps for every asset based on the more than 3 billion assets tracked by the Armis Collective Asset Intelligence Engine
- Access out of the box views of DSP compliance including:
  - Highlighting medical devices exhibiting potentially compromised / malicious behaviour
  - Assets without endpoint security protection installed or installed but out of date
  - Access to known malicious websites

Without Armis, organisations often engage in manual processes that are built around spreadsheets, are extremely time consuming, and liable to human error and mis-identification.

This manual process ultimately only provides a point in time assessment, with no on-going, continuous monitoring for malicious, suspicious, and anomalous behaviours. Hundreds of additional resource hours will be spent manually assessing every control as the deadline approaches, and manually figuring out remediation steps.

Armis is able to standardise and automate the DSPT process saving thousands of hours across multiple reporting cycles and enabling valuable IT resources to focus on supporting patient care.

Specifically, the DSPT controls Armis will automatically check on, fulfil or help with are:

V5 22-23 Evidence Reference	Evidence Text - NHS Trusts and CSUs (Category 1)	How Armis Addresses
1.1.4	Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.	Armis can identify, classify and provide a complete inventory of hardware and software assets for the organization whether they are on-prem, cloud, or remote. Armis has the ability to assign business criticality / impact and owners of each asset.
1.3.2	Your organisation monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.	Armis' passive monitoring enables 24/7 monitoring of an organizations data being transmitted through its traffic and assessment of security controls.
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.	Armis does real time security assessment of the environment as well as manufacturer risk rating and devices that can help feed and maintain and up to date security risk register.
1.3.6	List your organisation's top three data security and protection risks.	Armis can provide organizations with a smart adaptive risk scoring of cyber security risks.
1.3.7	Your organisation has implemented appropriate technical and organisation-al measures to integrate data protection into your processing activities.	Armis provides custom policy/report/dashboard to enable monitoring of compliance, anamalous behaviors, unencrypted data, PII / PHI transmission.
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.	Armis supports this by automatically inventorying new devices that appear on an organizations network and displaying their risk scores
3.3.2	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.	Armis provides a Managed Threat Service along with Technical Account Managers that can act as an extension to the NHS Trust cyber security teams. These are in house experts that help monitor and assit orgnizations to adapt, prevent, detect, and remediate risk and cyber attacks. Armis proactively assists its clients as the landscape evolves by creating dashboards, reports, policies, and alerts to new and emerging threats and vulnerabilities.

4.1.2	Users in your organisation are only given the minimum access to sensitive information or systems necessary for their role.	Armis can display user access rights and leverage integrations to help facilitate review of access to applications / sensitive systems
4.2.1	When was the last audit of user accounts held?	Armis can get user information through appropriate integrations.
4.2.3	Logs are retained for a sufficient period, managed securely, reviewed regularly and can be searched to identify malicious activity.	Armis can retain logs and even push logs out to a SIEM through integrations for regular review since Armis can see all traffic that is spanned to it.
4.2.4	Unnecessary user accounts are removed or disabled.	Armis can integrate with active directory and show disabled accounts that are still being utilized on the network.
4.3.2	Users, systems and (where appropriate) devices are identified and authenticated prior to being permitted access to information or systems.	Armis can identify users and devices that are not authenticated on the network helping support and enforce Zero Trust security policies.
4.4.1	The organisation ensures that logs, including privileged account use, are kept securely and only accessible to appropriate personnel. They are stored in a read only format, tamper proof and managed according to the organisation information life cycle policy with disposal as appropriate.	Armis has role based access functionality to ensure information within Armis platform is only accessible to those who require it.
4.4.3	The organisation only allows privileged access to be initiated from devices owned and managed or assured by your organisation.	Armis can help monitor for access violations.
4.5.2	Technical controls enforce password policy and mitigate against password-guessing attacks.	Armis has the ability to detect brute force attempts and usage of default credentials.
4.5.3	Multifactor authentication is used wherever technically feasible.	Armis can help identify (through integration) where user accounts are lacking MFA.

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.	Armis has the ability to detect usage of default credentials.
6.1.1	A policy/procedure is in place to ensure data security and protection incidents are managed/ reported appropriately.	Armis can provide reports and dashboards to reduce the person hours required creating and maintaining incident reports.
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.	Armis can identify if devices connected to the internet have antivirus or antimalware software installed or not. Armis can compare its inventory with that of a security platform and identify any misconfigured or failed installs.
6.2.3	Antivirus/anti-malware is kept continually up to date.	Armis can identify the version of the antivirus or antimalware
6.2.5	Connections to malicious websites on the Internet are prevented.	Armis can detect threats and malicious IP / Web connections and automate the blocking of access to them.
6.3.1	If you have had a data security incident, was it caused by a known vulnerability?	Armis can identify exploits / exploit attempts and correlate them to known vulnerabilities.
6.3.2	The organisation acknowledges all 'high severity' cyber alerts within 48 hours using the respond to an NHS cyber alert service.	Armis can assist with rapid assessments against NHS Cyber Alerts.
6.3.3	The organisation has a proportionate monitoring solution to detect cyber events on systems and services.	Armis will be that solution to detect cyber events on devices and solutions through monitoring.
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.	Armis provides risk scoring, vulnerability management and threat intelligence feed information

7.3.1	On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary.	Armis can be the tool to discover incidents and provide mitigating measures such as reports / dashboards of incidents on the network, automate enforcement. Armis also offers an Managed Threat Service to detect, and mitigate threats as well.
8.1.1	Provide evidence of how the organisation tracks and records all software assets and their configuration.	Armis can provide a list of all assets and software/ software version running those assets.
8.1.2	The organisation tracks and records all end user devices and removable media assets.	Armis can provide a list of all end user devices, it can report on removable media through integrations.
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 and signed off by the SIRO.	Armis can provide a list of all out of date supported software on the network, can detect orphaned devices and servers that are EOL, and for those that cannot be removed from the network, Armis can identify communication patterns, and assist in the creation and enforcement of network segmentation policies.
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.	Not only can Armis provide a list of unsupported/ unupdated software on the network, but it can set policies to isolate the device utilizing integrations such as NAC or firewall solutions. (same as above)
8.2.1	List any unsupported software priori-tised according to business risk, with remediation plan against each item.	With Armis' Unified Asset Intelligence Platform, Armis can provide a list of unsupported software on the network and prioritize them based on business risk.
8.2.2	The SIRO confirms that the 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.	Armis can provide the list of unsupported systems and software.

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 and signed off by the SIRO with an auditor agreeing a robust risk management process has been applied.	Armis can identify critical or high risk vulnerabilities and even assist with documenting within Armis that the risk has been accepted with reason with the AVM module.
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.	Armis can identify critical or high risk vulnerabilities and provide the remediation of those vulnerabilities when available, or also assist in mitigating controls such as segmentation.
8.3.6	Your organisation is actively using and managing Advanced Threat Protection (ATP) and regularly reviewing alerts from Microsoft defender for endpoint.	Armis though not considered a traditional ATP, it has the capability of alerting on threats on the network/ devices. Whether they are known threats or anomolous, Armis can identify and help prevent any further damage through identification and enforcement. Armis can help identify assets that are not using ATP software.
8.3.7	95% of your organisation's server estate and 98% of your desktop estate are on supported versions of operating systems.	Armis can identify operating system versions of all devices on the network and highlight EOL operating systems, vulnerabilities and risks.
8.4.1	Your organisation's infrastructure is protected from common cyber-attacks through secure configuration and patching.	Armis can help assess the security configuration and controls of the environment and infrastrcuture to help assess risk and offer mitigating controls. Armis can unite tools that specialize in specific operating systems to provide a single rationalized view of every device regardless of O/S.
8.4.2	All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support.	Armis can provide the all software and software version running on the network. Armis can also provide a list of all operating system versions on the network.
8.4.3	You maintain a current understanding of the exposure of your hardware and software to publicly-known vulnerabilities.	Armis provides a complete list of CVE's and CVSS scores for every asset discovered on the network.
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.	Armis can help identify the use of default credentials and the use of unencrypted credentials across systems.

9.1.2	The Head of IT, or equivalent role, confirms all organisational devices have had their default passwords changed.	Armis can help identify the use of default credentials and the use of unencrypted credentials across systems.
9.3.5	The organisation understands and records all IP ranges in use across the organisation.	Armis can identify the IP every device communicationg on the network whether IoT, IoMT, OT and IT
9.3.6	The organisation is protecting it's data in transit (including email) using well-configured TLS v1.2 or better.	Armis can identify communications with any protocols, including TLS v1.2 or better and report on ciphers used.
9.3.8	The organisation maintains a register of medical devices connected to its network.	Armis can provide an inventory of all medical devices connected to the network.
9.3.9	What is the organisation's data security assurance process for medical devices connected to the network?	Armis can be a part of this process.
9.5.1	All devices in your organisation have technical controls that manage the installation of software on the device.	Armis can help identify which devices do have the control to limit installation of software and those that don't.
9.5.3	You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.	The Armis platform has the ability to monitor for changes, particularly to high priority and business critical assets such as infrastructure and medical devices. This can pertain to changes such as IP addresses, changes in risk or vulnerabilities, detection if the devices are taken offline, as well as configuration states of devices.
9.5.6	End user device security settings are managed and deployed centrally.	Armis can identify managed devices including those that should be managed, but don't have the necessary agents, and those that have misconfigurations, thereby are noncompliant to the asset management policies set by the organisation.
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 and signed off by the SIRO.	Armis can assess the security and risk of devices even if they are air-gapped or unable to connect to the Internet.

9.6.3	The organisation has checked and verified that firewall rules ensure that all unauthenticated inbound connections are blocked by default.	If these connections are not being blocked by the firewall, Armis will be able to identify and report on them.
9.6.6	All of your organisation's desktop and laptop computers have personal firewalls (or equivalent) enabled and configured to block unapproved connections by default.	Armis will be able to show your desktops and laptops communicating to any domains or IP addresses that they should not be communicating with, thus ensuring that unapproved connections are not occuring and if they are, to stop them immediately.

Armis is a proven leader in healthcare

Armis has been ranked as a clear leader for Medical Device Security Solutions by leading analysts including the Quadrant Spark MATRIX: Connected Medical Device Solutions. Armis brings together biomedical, security and IT teams to identify, assess and secure IoMT, IoT, OT and IT assets enabling improved security, visibility and utilisation.

Knowledge

The Armis Collective Asset Intelligence Engine contains detailed accumulated anonymized knowledge of more than 3 billion devices from Armis customers. When Armis finds a device on your network, it can instantly compare configuration and traffic pattern information, removing a learning period and yielding fast time to value.

Integrated

Capable of both sending and ingesting data from many leading security, SIEM, SOAR, CMDB, CMMS, cloud, infrastructure and networking solutions

Customisable

Armis' powerful query language and customizable dashboards can deliver the right view for the right team be that the IT, biomedical or operations teams.

Every Device - IoMT, IoT, OT AND IT

Medical devices are not the only attack surface that healthcare needs to protect. IoT such as security cameras, OT such as building management systems, IT are supporting networks where patients attach their own devices - we've even seen cars... Armis passively detects, identifies and assesses the risk of every device.

Agentless

Many IoT, IoMT and OT environments are unable to have agents installed, leaving them outside of the scope of traditional security tools. Armis utilizes passive scanning. This enables detection of every device communicating on the network, removes the risk of crashing devices through active scanning and simplifies ongoing updating and maintenance.

Contact Armis - Get a demo.

NHS@armis.com

About Armis

Armis is the leading unified asset intelligence and security platform designed to address the new threat landscape that connected devices create. Our customers trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in San Francisco, California.

1.888.452.4011 | armis.com