ITHealth

The NHS Data Security and Protection Toolkit 2023/24

How the ITHealth Dashboard helps

Supporting 38 evidence codes (33 mandatory) - DSPT v.6.

October 2023

The Data Security and Protection Toolkit (DSPT) enables organisations to measure and publish their performance against the National Guardian's ten data security standards. All organisations that have access to NHS patient data and systems must use the toolkit to provide assurance that they are practising good data security. This document outlines how ITHealth's Dashboard solution maps to key requirements of the toolkit and provides supporting evidence to maintain ongoing compliance.

ITHealth Dashboard Solution Overview

The **ITHealth Dashboard** gives NHS IT teams greater control of their connected estates through increased security visibility of all assets. It helps to better manage exposure to risk and easily report and act upon it, ensuring NHS organisations stay cyber assured and compliant.

Key features:

- **Complete asset discovery and management**
  All assets are viewable and manageable in one place, including network kit, IOT, and medical devices.
- **Software asset management**
  Tracks all software, compares licence entitlements, and allows software authorisation.
- **Patch management**
  Verifies that patches are being fully installed, with trending reports and drillable views.
- **NHSD Cyber Alert automation**
  Reduces manual processes linked to NHS Digital Cyber Alert response, and targets and tracks remediation.
- **DSPT reporting**
  Streamlines submissions with one-click exportable reports against evidence requirements.
- **AV, ATP and Encryption reporting**
  Ensures compliance to NHS Digital national guidelines and local Trust policies.
- **End of Support software**
  Views showing EOL/EOS software across the estate, as required by the DSPT and CE+.
- **Vulnerability CVE ranking**
  Reports on all vulnerabilities found across the IT estate to supplement Cyber Alert reports.
- **Active Directory (AD) auditing**
  Highlights risks within your AD management, allowing you to address these easily.
- **An ITHealth supported solution**
  Provision of monthly status quo reports to monitor trends, plus access to technical experts.

Over 150 NHS organisations rely on the ITHealth Dashboard to more efficiently reduce exposure to threat and maintain a secure, vigilant and resilient IT environment.

How is the DSPT structured?

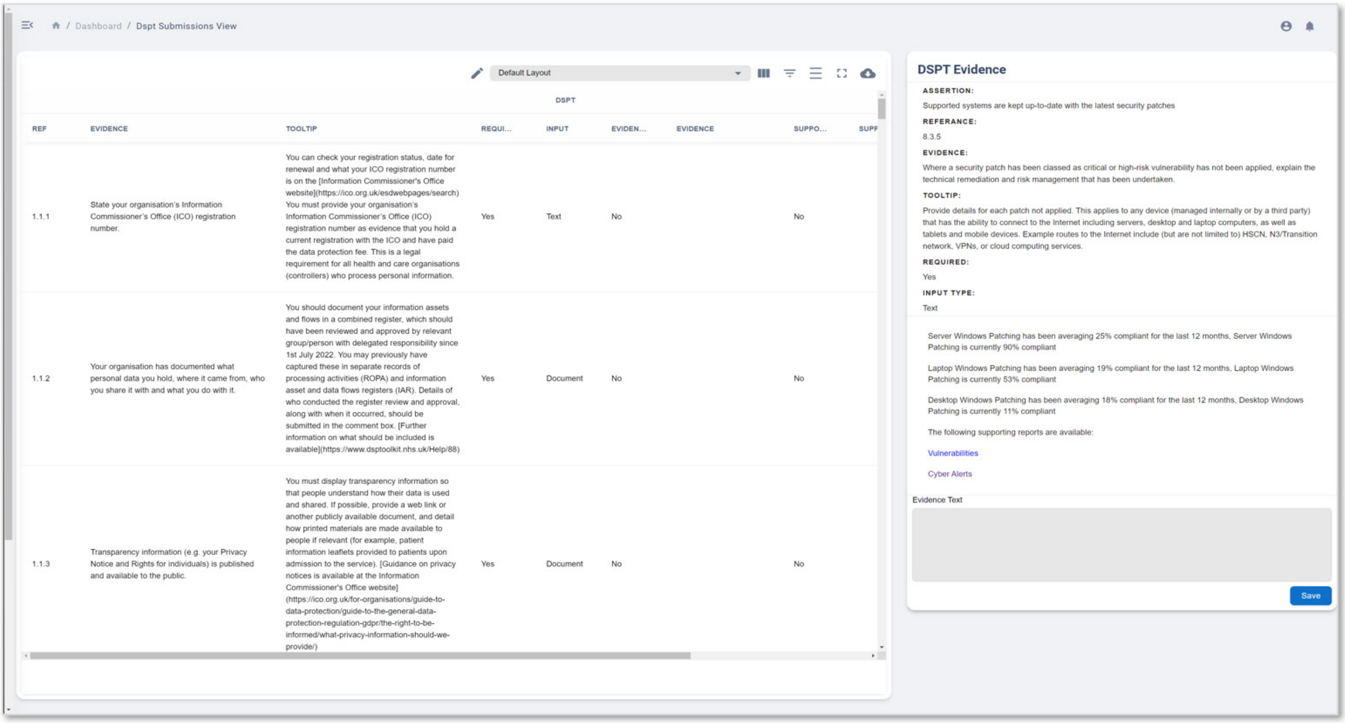
The DSPT is composed of ten data security standards addressing issues arising from people, processes, and technology. Against each standard are assertions - specific themes or controls that substantiate the standard. Evidence items then follow against assertions. There are various Category applications of the Toolkit and the organisation type determines what Category of Toolkit is to be completed. NHS Trusts, CSUs (Commissioning Support Units), ALBs (Arm's Length Bodies) and ICBs (Integrated Care Boards) all fall under Category 1 of the Toolkit - which includes 128 evidence items - 108 of which are mandatory (v.6. 2023-24). For an NHS Trust to be deemed 'Satisfactory' it must be able to provide evidence, upon request, for all mandatory evidence items.

How the ITHealth Dashboard helps

The ITHealth Dashboard solution supports 33 of the DSPT's mandatory evidence items and 5 non-mandatory evidence items, as applicable to Category 1. The tables that follow detail all 38 evidence codes and how these are supported by the ITHealth Dashboard solution.

Before we delve into the detail, it's important to note that **there is also a dedicated 'DSPT View' within the ITHealth Dashboard**. This view includes best matched reports against evidence items for which the ITHealth Dashboard can provide supporting information. The best matched reports will always present near real-time information, and can be viewed either within the ITHealth Dashboard or easily exported to Excel. All reports remain obtainable at the click of a button *all year round* and not only at the time of audit.

Dedicated DSPT View



DSPT

REF	EVIDENCE	TOOLTIP	REQUI...	INPUT	EVIDEN...	EVIDENCE	SUPPO...	SUPF
1.1.1	State your organisation's Information Commissioner's Office (ICO) registration number.	You can check your registration status, date for renewal and what your ICO registration number is on the [Information Commissioner's Office website](https://ico.org.uk/esdwebpages/search) You must provide your organisation's Information Commissioner's Office (ICO) registration number as evidence that you hold a current registration with the ICO and have paid the data protection fee. This is a legal requirement for all health and care organisations (controllers) who process personal information.	Yes	Text	No		No	
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.	You should document your information assets and flows in a combined register, which should have been reviewed and approved by relevant group/person with delegated responsibility since 1st July 2022. You may previously have captured these in separate records of processing activities (ROPA) and information asset and data flows registers (IAR). Details of who conducted the register review and approval, along with when it occurred, should be submitted in the comment box. [Further information on what should be included is available](https://www.dsptoolkit.nhs.uk/Help/88)	Yes	Document	No		No	
1.1.3	Transparency information (e.g. your Privacy Notice and Rights for individuals) is published and available to the public.	You must display transparency information so that people understand how their data is used and shared. If possible, provide a web link or another publicly available document, and detail how printed materials are made available to people if relevant (for example, patient information leaflets provided to patients upon admission to the service). [Guidance on privacy notices is available at the Information Commissioner's Office website] (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-privacy-information-should-we-provide/)	Yes	Document	No		No	

DSPT Evidence

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

REFERANCE:
8.3.5

EVIDENCE:
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.

TOOLTIP:
Provide details for each patch not applied. This applies to any device (managed internally or by a third party) that has the ability to connect to the Internet including servers, desktop and laptop computers, as well as tablets and mobile devices. Example routes to the Internet include (but are not limited to) HSCN, N3/Transition network, VPNs, or cloud computing services.

REQUIRED:
Yes

INPUT TYPE:
Text

Server Windows Patching has been averaging 25% compliant for the last 12 months, Server Windows Patching is currently 90% compliant

Laptop Windows Patching has been averaging 19% compliant for the last 12 months, Laptop Windows Patching is currently 53% compliant

Desktop Windows Patching has been averaging 18% compliant for the last 12 months, Desktop Windows Patching is currently 11% compliant

The following supporting reports are available:

Vulnerabilities

Cyber Alerts

Evidence Text

Fig.1. Example of the dedicated DSPT view within the ITHealth Dashboard. This view details all DSPT evidence items, indicating whether supporting evidence can be found within the ITHealth Dashboard. Upon clicking on an evidence item, further information appears including links to easily navigate to the supporting reports.

How the ITHealth Dashboard maps to the DSPT

Data Security Standard 1: Personal Confidential Data

Evidence code	**Evidence Text** (NHS Trusts, CSUs, ALBs, and ICBs - Category 1)	**Mandatory?**	**How the ITHealth Dashboard helps**
1.1.4	Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.	Yes	The ITHealth Dashboard discovers and records all hardware and software assets within a Trust's network, including the security and compliance status of the assets. This data can be trended over time for continuous monitoring or exported to form part of an Asset Register, as required.
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.	Yes	The ITHealth Dashboard collects and reports data on the Trust's exposure to CVE vulnerabilities, NHS Cyber Alerts and other IT security risks. This data can feed into the Trust's risk register as a mechanism for identifying various risks.
1.3.6	List your organisation's top three data security and protection risks.	Yes	The ITHealth Dashboard provides detailed information on the most common risks to NHS Trusts. Unprotected user endpoints, rogue devices, unpatched workstations and more. This information can be reviewed and assessed by the Trust's leadership to assist in defining the top three risks to the organisation.

Endpoint Insight View

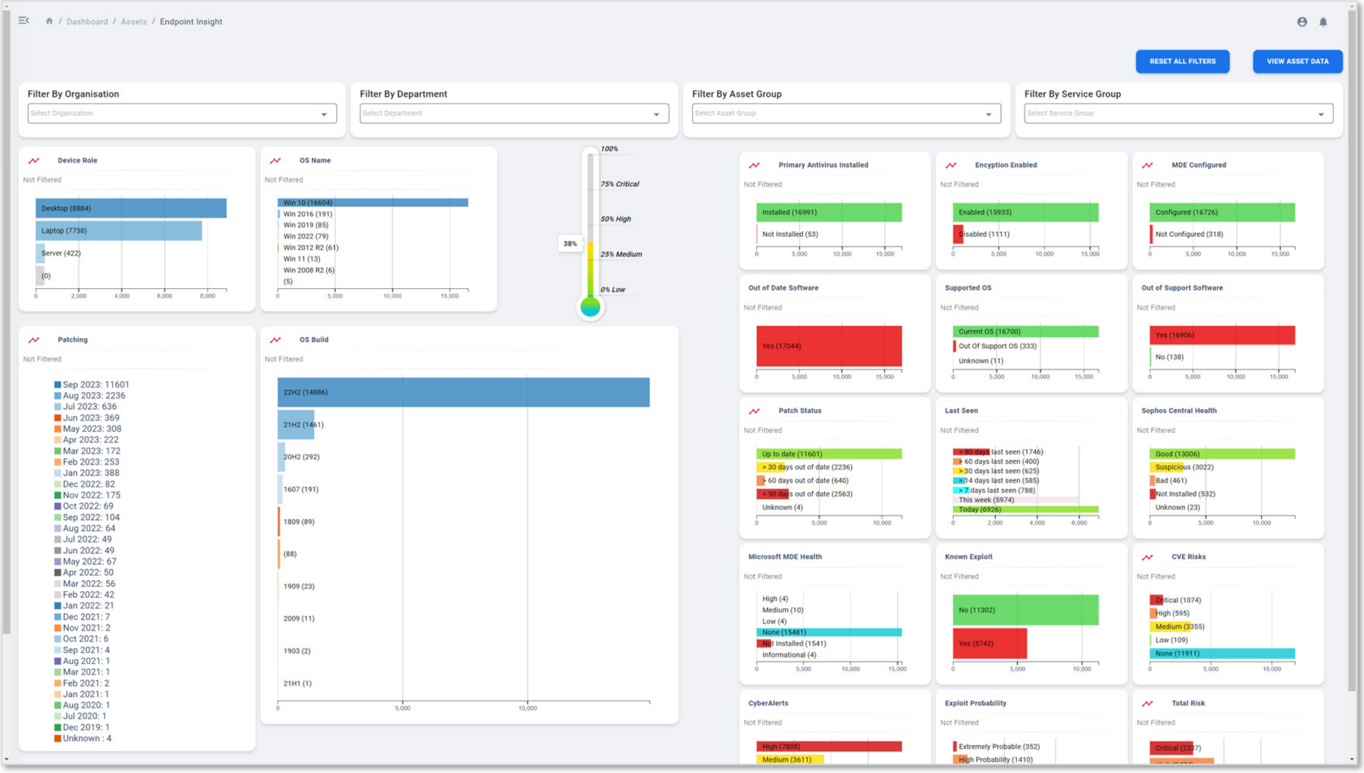
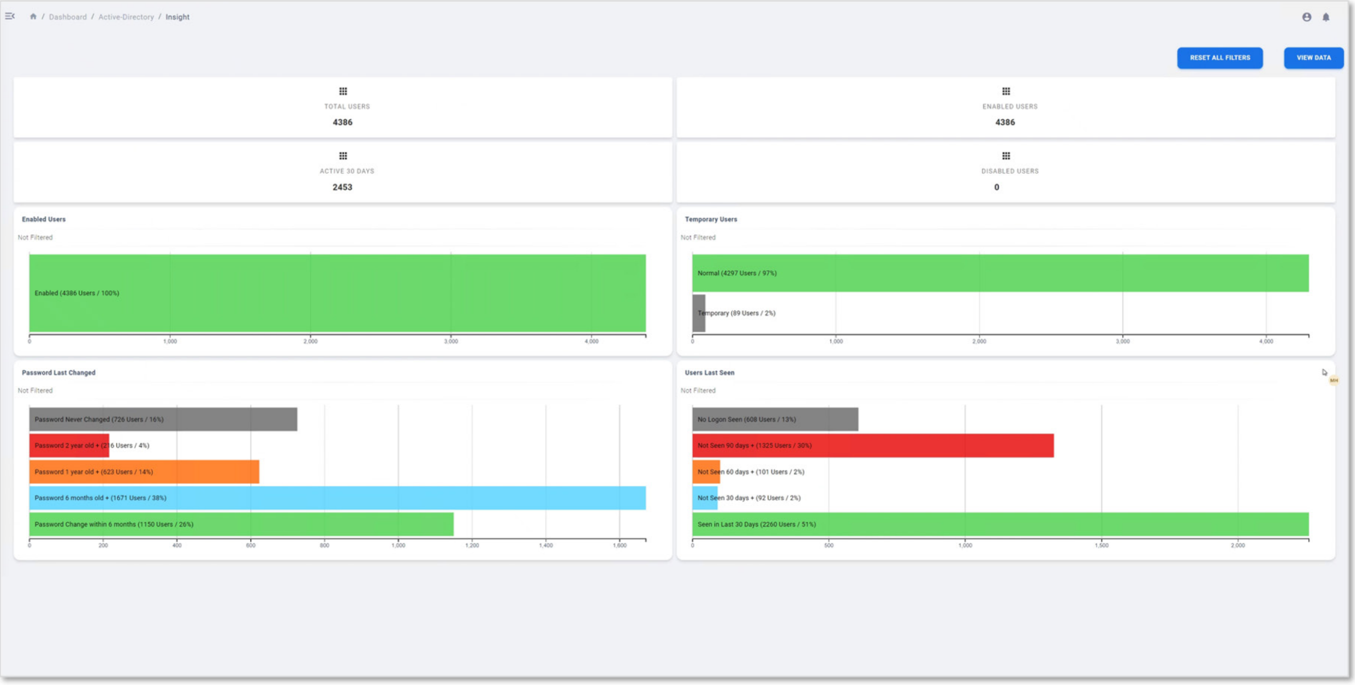


Fig.2. Example of how the ITHealth Dashboard provides information on patch status, anti-virus, encryption, CVE risk, devices not seen and much more. All information is drillable to a more granular view to assist in risk management and remediation prioritisation.

Data Security Standard 4: Managing Data Access

Evidence code	**Evidence Text** (NHS Trusts, CSUs, ALBs, and ICBs - Category 1)	**Mandatory?**	**How the ITHealth Dashboard helps**
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.	Yes	The ITHealth Dashboard can integrate with Active Directory to identify user accounts that have no job role assigned. Ensuring these remain accurate once completed will be a manual process.
4.2.1	When was the last audit of user accounts with access to the organisation's systems held?	Yes	Through integration with Active Directory the ITHealth Dashboard can identify users with access to the Trust's domain in order to assist audit purposes.
4.2.4	Unnecessary user accounts are removed or disabled.	Yes	The ITHealth Dashboard highlights users that haven't logged on to the network for a defined period of time (by default 60 and 90 days, but this is configurable). These user reports can be reviewed by the Trust to determine which user accounts could be removed or disabled.
4.3.3	All staff have been notified that their system use could be monitored.	No	The ITHealh Dashboard can provide supporting information to check that Windows legal notices are configured appropriately on the Trust's network.
4.4.3	The organisation only allows privileged access to be initiated from devices owned and managed or assured by your organisation	No	The ITHealth Dashboard can identify domain and non-domain devices.

Active Directory Insight



/ Dashboard / Active-Directory / Insight

TOTAL USERS 4386

ENABLED USERS 4386

ACTIVE 30 DAYS 2453

DISABLED USERS 0

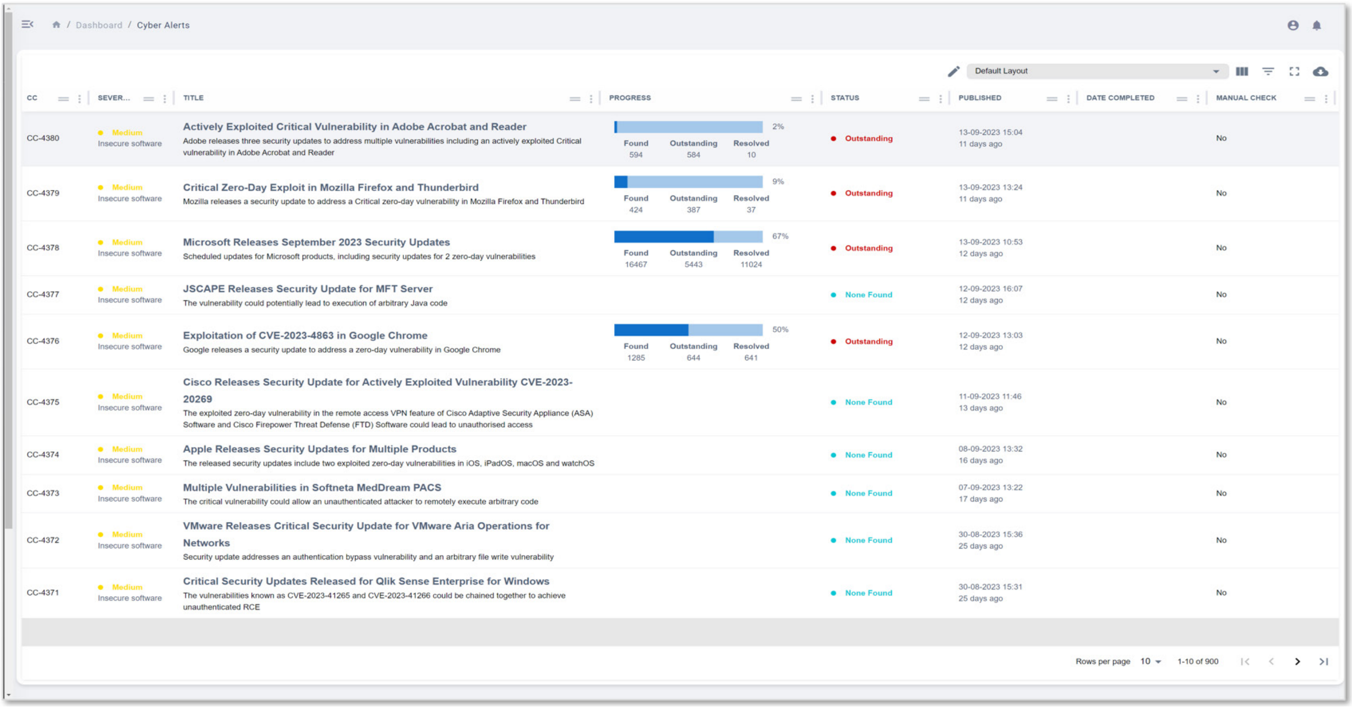
RESET ALL FILTERS
VIEW DATA
Enabled Users
Not Filtered
Enabled (4386 Users / 100%)
0
1,000
2,000
3,000
4,000
Temporary Users
Not Filtered
Normal (4297 Users / 97%)
Temporary (89 Users / 2%)
0
1,000
2,000
3,000
4,000
Password Last Changed
Not Filtered
Password Never Changed (726 Users / 16%)
Password 2 year old + (216 Users / 4%)
Password 1 year old + (623 Users / 14%)
Password 6 months old + (1671 Users / 38%)
Password Change within 6 months (1150 Users / 26%)
0
200
400
600
800
1,000
1,200
1,400
1,600
Users Last Seen
Not Filtered
No Logon Seen (608 Users / 13%)
Not Seen 90 days + (1325 Users / 30%)
Not Seen 60 days + (101 Users / 2%)
Not Seen 30 days + (92 Users / 2%)
Seen in Last 30 Days (2260 Users / 51%)
0
500
1,000
1,500
2,000
MH

Fig.3. The ITHealth Dashboard highlights users that haven't logged on to the network for a defined period of time.

Data Security Standard 6: Responding to Incidents and Cyber Alerts

Evidence code	**Evidence Text** (NHS Trusts, CSUs, ALBs, and ICBs - Category 1)	**Mandatory?**	**How the ITHealth Dashboard helps**
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.	Yes	The ITHealth Dashboard includes a full anti-virus status report for all devices and servers. The anti-virus report highlights devices where anti-virus is disabled and missing. (Integration with Sophos Central is available for Trusts who use this suite of products for more granular visibility of device protection status.)
6.2.3	Antivirus/anti-malware is kept continually up to date.	Yes	The ITHealth Dashboard includes a full anti-virus status report for all devices and servers. The anti-virus report highlights devices where anti-virus is not up to date or expired. (Integration with Sophos Central is available for Trusts who use this suite of products for more granular visibility of device protection status.)
6.2.4	Antivirus/anti-malware software scans files automatically upon access.	Yes	This information can be shown in the ITHealth Dashboard if the AV provider is supported. (Integration with Sophos Central is available for Trusts who use this suite of products for more granular visibility of device protection status.)
6.3.1	If you have had a data security incident, was it caused by a known vulnerability?	Yes	Devices that contain known vulnerabilities are highlighted within the various reports in the ITHealth Dashboard, specifically the NHS Cyber Alert reporting and Software CVE modules. These areas will assist the Trust in their post-event investigations and provide attention areas for remediation to avoid repeat instances. The ITHealth Dashboard provides a fully automated Cyber Alert compliance view. This shows in real-time your compliance against each Cyber Alert vulnerability, allowing you to prove that the bulletins and advice are being acted upon. The ITHealth Dashboard highlights non-compliant assets for each Cyber Alert and provides an actionable worklist for swifter remediation.
6.3.2	The organisation acknowledges all ‘high severity’ cyber alerts within 48 hours using the respond to an NHS cyber alert service.	Yes	By quickly identifying all devices that are subject to NHS Cyber Alerts the ITHealth Dashboard ensures the 48-hour response timescale is achievable by taking out the manual process of identifying and prioritising assets for remediation.
6.3.3	The organisation has a proportionate monitoring solution to detect cyber events on systems and services.	Yes	The ITHealth Dashboard will provide monitoring of devices and their health status, including the presence of anti-virus, encryption and Microsoft Defender.

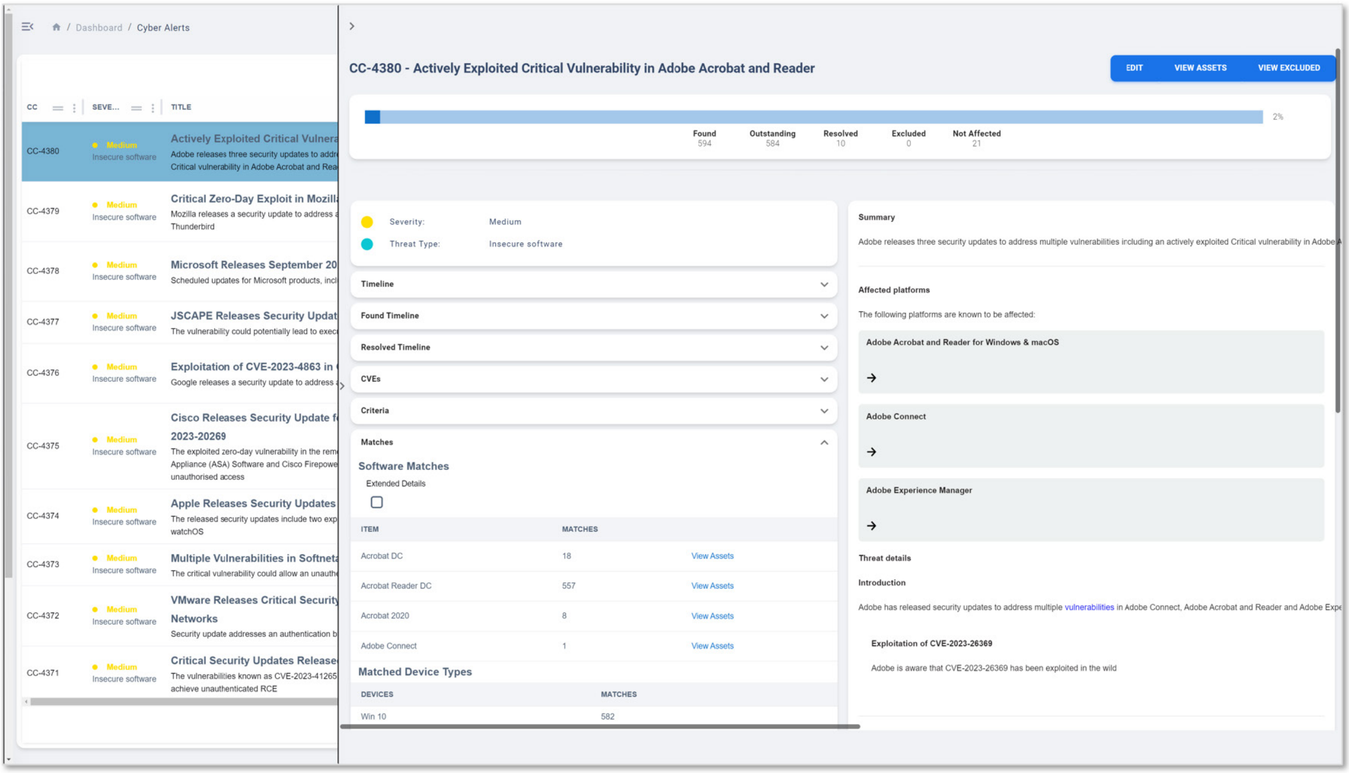
Cyber Alert Views



CC	SEVER...	TITLE	PROGRESS	STATUS	PUBLISHED	DATE COMPLETED	MANUAL CHECK
CC-4380	● Medium Insecure software	**Actively Exploited Critical Vulnerability in Adobe Acrobat and Reader** Adobe releases three security updates to address multiple vulnerabilities including an actively exploited Critical vulnerability in Adobe Acrobat and Reader	2% Found 594 Outstanding 584 Resolved 10	● Outstanding	13-09-2023 15:04 11 days ago		No
CC-4379	● Medium Insecure software	**Critical Zero-Day Exploit in Mozilla Firefox and Thunderbird** Mozilla releases a security update to address a Critical zero-day vulnerability in Mozilla Firefox and Thunderbird	9% Found 424 Outstanding 387 Resolved 37	● Outstanding	13-09-2023 13:24 11 days ago		No
CC-4378	● Medium Insecure software	**Microsoft Releases September 2023 Security Updates** Scheduled updates for Microsoft products, including security updates for 2 zero-day vulnerabilities	67% Found 16467 Outstanding 5443 Resolved 11024	● Outstanding	13-09-2023 10:53 12 days ago		No
CC-4377	● Medium Insecure software	**JSCAPE Releases Security Update for MFT Server** The vulnerability could potentially lead to execution of arbitrary Java code		● None Found	12-09-2023 16:07 12 days ago		No
CC-4376	● Medium Insecure software	**Exploitation of CVE-2023-4863 in Google Chrome** Google releases a security update to address a zero-day vulnerability in Google Chrome	50% Found 1285 Outstanding 644 Resolved 641	● Outstanding	12-09-2023 13:03 12 days ago		No
CC-4375	● Medium Insecure software	**Cisco Releases Security Update for Actively Exploited Vulnerability CVE-2023-20269** The exploited zero-day vulnerability in the remote access VPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could lead to unauthorised access		● None Found	11-09-2023 11:46 13 days ago		No
CC-4374	● Medium Insecure software	**Apple Releases Security Updates for Multiple Products** The released security updates include two exploited zero-day vulnerabilities in iOS, iPadOS, macOS and watchOS		● None Found	08-09-2023 13:32 16 days ago		No
CC-4373	● Medium Insecure software	**Multiple Vulnerabilities in Softneta MedDream PACS** The critical vulnerability could allow an unauthenticated attacker to remotely execute arbitrary code		● None Found	07-09-2023 13:22 17 days ago		No
CC-4372	● Medium Insecure software	**VMware Releases Critical Security Update for VMware Aria Operations for Networks** Security update addresses an authentication bypass vulnerability and an arbitrary file write vulnerability		● None Found	30-08-2023 15:36 25 days ago		No
CC-4371	● Medium Insecure software	**Critical Security Updates Released for Qlik Sense Enterprise for Windows** The vulnerabilities known as CVE-2023-41265 and CVE-2023-41266 could be chained together to achieve unauthenticated RCE		● None Found	30-08-2023 15:31 25 days ago		No

Rows per page 10 1-10 of 900

Fig.4. The Cyber Alert View within the ITHealth Dashboard details Cyber Alert information, including severity level and date released. It allows you to easily see how many affected assets have been found, as well monitor progess against 'outstanding' and 'resolved' instances.



CC	SEVE...	TITLE
CC-4380	● Medium Insecure software	**Actively Exploited Critical Vulnera** Adobe releases three security updates to addr Critical vulnerability in Adobe Acrobat and Rea
CC-4379	● Medium Insecure software	**Critical Zero-Day Exploit in Mozill** Mozilla releases a security update to address a Thunderbird
CC-4378	● Medium Insecure software	**Microsoft Releases September 20** Scheduled updates for Microsoft products, incl
CC-4377	● Medium Insecure software	**JSCAPE Releases Security Updat** The vulnerability could potentially lead to exec
CC-4376	● Medium Insecure software	**Exploitation of CVE-2023-4863 in** Google releases a security update to address a
CC-4375	● Medium Insecure software	**Cisco Releases Security Update f** **2023-20269** The exploited zero-day vulnerability in the rem Appliance (ASA) Software and Cisco Firepowe unauthorised access
CC-4374	● Medium Insecure software	**Apple Releases Security Updates** The released security updates include two exp watchOS
CC-4373	● Medium Insecure software	**Multiple Vulnerabilities in Softneta** The critical vulnerability could allow an unauthe
CC-4372	● Medium Insecure software	**VMware Releases Critical Security** **Networks** Security update addresses an authentication b
CC-4371	● Medium Insecure software	**Critical Security Updates Release** The vulnerabilities known as CVE-2023-41265 achieve unauthenticated RCE

CC-4380 - Actively Exploited Critical Vulnerability in Adobe Acrobat and Reader

EDIT VIEW ASSETS VIEW EXCLUDED

2%

Found	Outstanding	Resolved	Excluded	Not Affected
594	584	10	0	21

Severity: Medium
Threat Type: Insecure software

Timeline
Found Timeline
Resolved Timeline
CVEs
Criteria
Matches

Software Matches

Extended Details
□

ITEM	MATCHES	
Acrobat DC	18	View Assets
Acrobat Reader DC	557	View Assets
Acrobat 2020	8	View Assets
Adobe Connect	1	View Assets

Matched Device Types

DEVICES	MATCHES
Win 10	582

Summary

Adobe releases three security updates to address multiple vulnerabilities including an actively exploited Critical vulnerability in Adobe A

Affected platforms

The following platforms are known to be affected:

Adobe Acrobat and Reader for Windows & macOS →

Adobe Connect →

Adobe Experience Manager →

Threat details

Introduction

Adobe has released security updates to address multiple vulnerabilities in Adobe Connect, Adobe Acrobat and Reader and Adobe Expe

Exploitation of CVE-2023-26369

Adobe is aware that CVE-2023-26369 has been exploited in the wild

Fig.5. By clicking on a particular Cyber Alert, more detailed information is displayed allowing you to easily see a breakdown of associated affected assets; it is then possible to click-through to view these assets to assist with remediation.

Data Security Standard 7: Continuity Planning

Evidence code	**Evidence Text** (NHS Trusts, CSUs, ALBs, and ICBs - Category 1)	Mandatory?	How the ITHealth Dashboard helps
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 wide-spread outbreak of very damaging malware.	No	The ITHealth Dashboard provides detailed vulnerability information that allows changes to be made as required. Newly released CVE's are added to the vulnerability feed to assist the Trust's response to emerging threats.

Data Security Standard 8: Unsupported Operating Systems

Evidence code	**Evidence Text** (NHS Trusts, CSUs, ALBs, and ICBs - Category 1)	Mandatory?	How the ITHealth Dashboard helps
8.1.1	Provide evidence of how the organisation tracks and records all software assets and their configuration.	Yes	The ITHealth Dashboard provides a complete inventory of software assets and can identify assets which are end of life, unsupported and contain vulnerabilities.
8.1.2	The organisation tracks and records all end user devices and removable media assets.	Yes	All end user devices can be detected and recorded within the ITHealth Dashboard to create a holistic inventory of assets. Removable media devices can be manually created as assets within the ITHealth Dashboard with their details updated and recorded.
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.	No	The ITHealth Dashboard provides a complete software inventory, which is fully up to date at all times. This allows Trusts to easily identify devices that have instances of vulnerable, unsupported and/or end of life software installed. This includes Operating Systems, web browsers and other commonly used applications such as Microsoft Office and Adobe products.
8.2.1	List any unsupported software prioritised according to business risk, with remediation plan against each item.	Yes	By cross referencing all discovered software with data from global CVE and CIS feeds the ITHealth Dashboard makes it easy for Trusts to identify any critical systems that feature vulnerable software that cannot be removed.
8.3.1	How do your systems receive updates and how often?	Yes	Data on devices that contain out of date software or patches is compiled within the ITHealth Dashboard reports to ensure the Trust is able to ensure updates are being correctly deployed and installed.
8.3.2	How often, in days, is automatic patching typically being pushed out to remote endpoints?	Yes	The ITHealth Dashboard provides trending information to help support expectation versus reality on how often patches are deployed and devices remain compliant.
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.	Yes	The ITHealth Dashboard compiles patching and software version data in order to report on those devices that are missing critical updates. This allows the Trust to confidently report on the current patching status of devices across the estate to ensure that critical patches are applied within 14 days.
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.	Yes	The ITHealth Dashboard will allow you to see patch compliance, along with any notes you have kept against software assets for future reference. In the event that a recent patch or version cannot be applied, it is possible to annotate the vulnerable version with relevant comments and details.

Data Security Standard 8: Unsupported Operating Systems (cont'd)

Evidence code	**Evidence Text** (NHS Trusts, CSUs, ALBs, and ICBs - Category 1)	**Mandatory?**	**How the ITHealth Dashboard helps**
8.3.6	Your organisation is actively using and managing Advanced Threat Protection (ATP) and regularly reviewing alerts from Microsoft defender for endpoint.	Yes	The ITHealth Dashboard includes reports for identifying any devices that are not successfully enrolled in ATP/Microsoft Defender for Endpoint.
8.3.7	95% of your organisation's server estate and 98% of your desktop estate are on supported versions of operating systems. Where this is not possible, there is a SIRO approved plan to achieve 95% of your server estate and 98% of your desktop estate on supported versions of operating systems.	Yes	The ITHealth Dashboard includes reports and breakdowns of all discovered operating systems used throughout the desktop and server estate. This allows the trust to easily report on the % of which are supported versions. Windows builds and versions which have reached their end-of-life date are highlighted for attention.
8.4.1	Your organisation's infrastructure is protected from common cyber-attacks through secure configuration and patching?	Yes	The ITHealth Dashboard will provide assurance as to patching levels across all devices.
8.4.2	All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support. 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.	Yes	Operating system and software system patching information is available in the ITHealth Dashboard, along with supplier information and product details.
8.4.3	You maintain a current understanding of the exposure of your hardware and software to publicly-known vulnerabilities.	Yes	The ITHealth Dashboard regularly updates with more vulnerabilities/CVEs as they become known. This ensures Trusts are able to maintain visibility of their current exposure to each vulnerability.

Software Insights

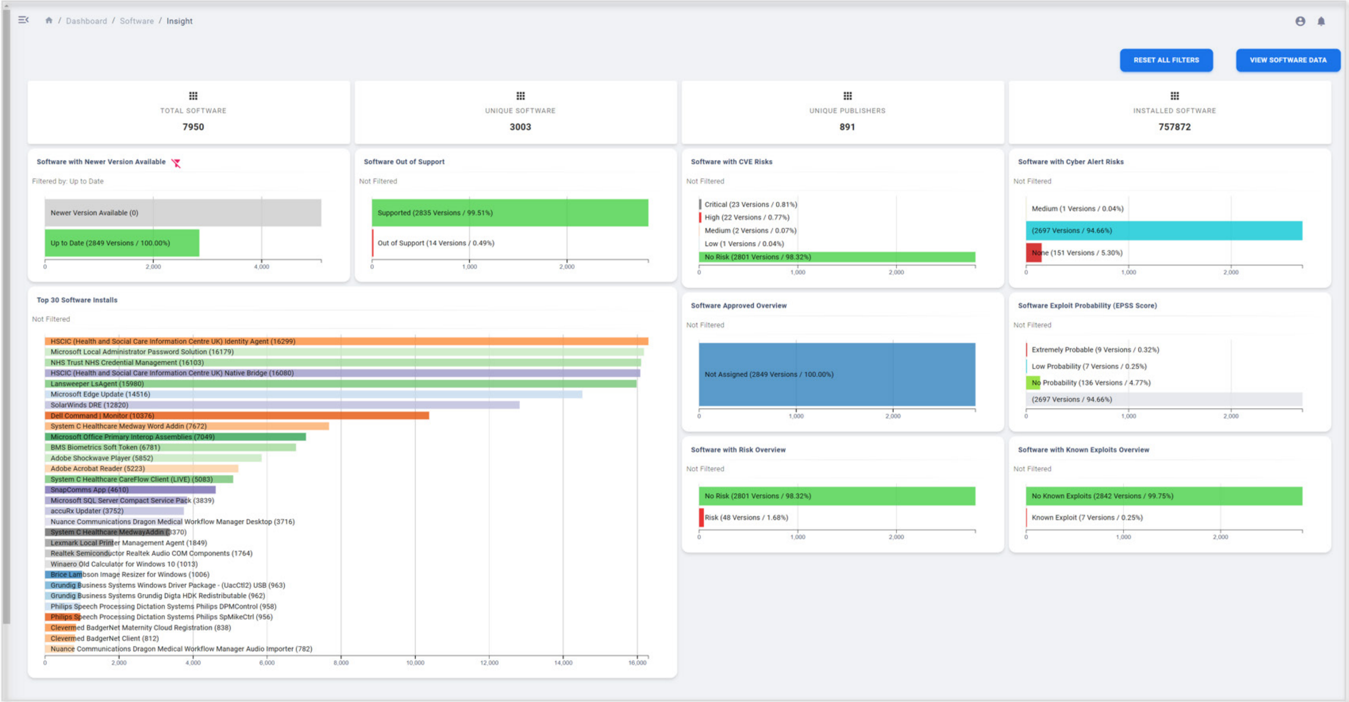
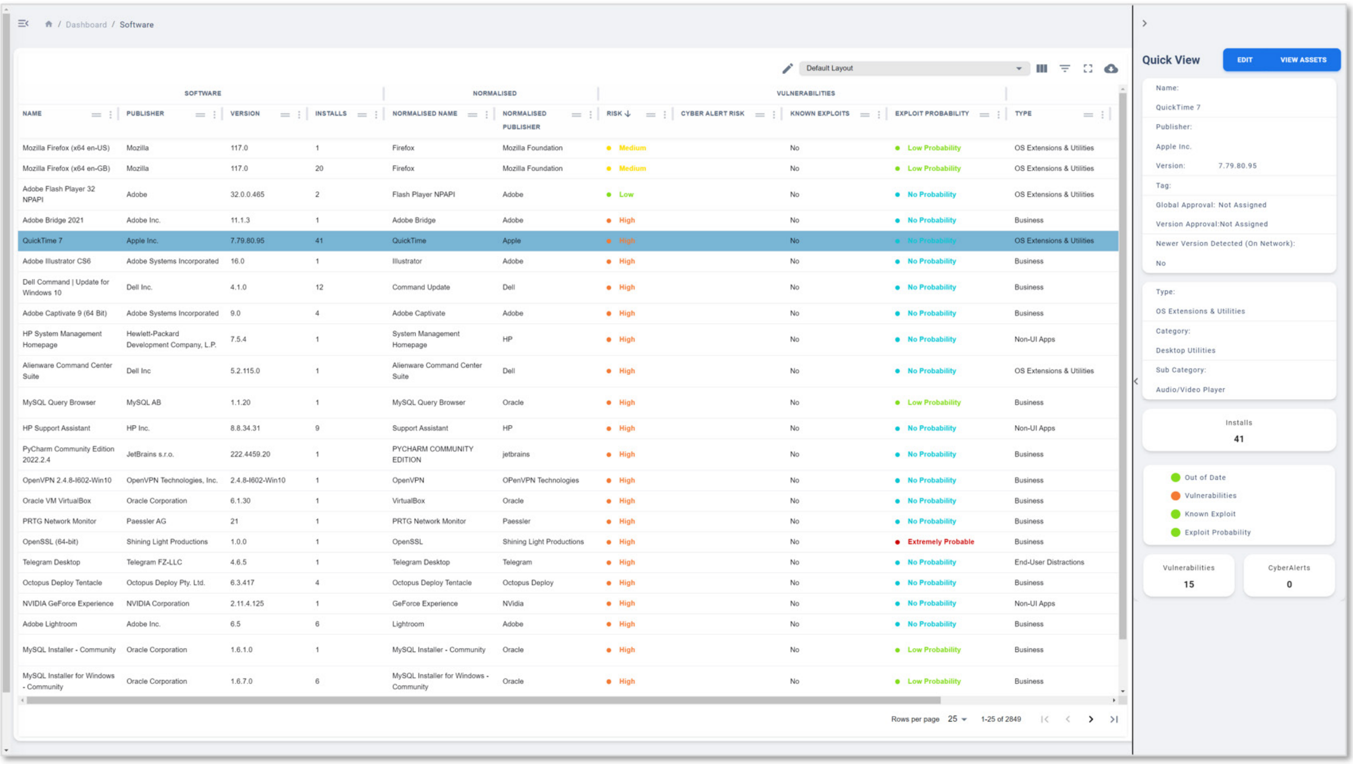

Dashboard / Software / Insight
RESET ALL FILTERS
VIEW SOFTWARE DATA
TOTAL SOFTWARE
7950
UNIQUE SOFTWARE
3003
UNIQUE PUBLISHERS
891
INSTALLED SOFTWARE
757872
Software with Newer Version Available
Filtered by: Up to Date
Newer Version Available (0)
Up to Date (2849 Versions / 100.00%)
0
2,000
4,000
Software Out of Support
Not Filtered
Supported (2835 Versions / 99.51%)
Out of Support (14 Versions / 0.49%)
0
1,000
2,000
Software with CVE Risks
Not Filtered
Critical (23 Versions / 0.81%)
High (22 Versions / 0.77%)
Medium (2 Versions / 0.07%)
Low (1 Versions / 0.04%)
No Risk (2801 Versions / 98.32%)
0
1,000
2,000
Software with Cyber Alert Risks
Not Filtered
Medium (1 Versions / 0.04%)
(2697 Versions / 94.66%)
None (151 Versions / 5.30%)
0
1,000
2,000
Top 30 Software Installs
Not Filtered
HSCIC (Health and Social Care Information Centre UK) Identity Agent (16299)
Microsoft Local Administrator Password Solution (16179)
NHS Trust NHS Credential Management (16103)
HSCIC (Health and Social Care Information Centre UK) Native Bridge (16080)
Lansweeper LsAgent (15980)
Microsoft Edge Update (14516)
SolarWinds DRE (12820)
Dell Command | Monitor (10376)
System C Healthcare Medway Word Addin (7672)
Microsoft Office Primary Interop Assemblies (7049)
BMS Biometrics Soft Token (6781)
Adobe Shockwave Player (5852)
Adobe Acrobat Reader (5223)
System C Healthcare CareFlow Client (LIVE) (5083)
SnapComms App (4610)
Microsoft SQL Server Compact Service Pack (3839)
accuRx Updater (3752)
Nuance Communications Dragon Medical Workflow Manager Desktop (3716)
System C Healthcare MedwayAddin (3370)
Lexmark Local Printer Management Agent (1849)
Realtek Semiconductor Realtek Audio COM Components (1764)
Winaero Old Calculator for Windows 10 (1013)
Brice Lambson Image Resizer for Windows (1006)
Grundig Business Systems Windows Driver Package - (UacCtl2) USB (963)
Grundig Business Systems Grundig Digta HDK Redistributable (962)
Philips Speech Processing Dictation Systems Philips DPMControl (958)
Philips Speech Processing Dictation Systems Philips SpMikeCtrl (956)
Clevermed BadgerNet Maternity Cloud Registration (838)
Clevermed BadgerNet Client (812)
Nuance Communications Dragon Medical Workflow Manager Audio Importer (782)
0
2,000
4,000
6,000
8,000
10,000
12,000
14,000
16,000
Software Approved Overview
Not Filtered
Not Assigned (2849 Versions / 100.00%)
0
1,000
2,000
Software Exploit Probability (EPSS Score)
Not Filtered
Extremely Probable (9 Versions / 0.32%)
Low Probability (7 Versions / 0.25%)
No Probability (136 Versions / 4.77%)
(2697 Versions / 94.66%)
0
1,000
2,000
Software with Risk Overview
Not Filtered
No Risk (2801 Versions / 98.32%)
Risk (48 Versions / 1.68%)
0
1,000
2,000
Software with Known Exploits Overview
Not Filtered
No Known Exploits (2842 Versions / 99.75%)
Known Exploit (7 Versions / 0.25%)
0
1,000
2,000

Fig.6. The Software Insights view within the ITHealth Dashboard highlights where software is out of support, where newer versions of software are available, where there is associated CVE and/or Cyber Alert risk, as well as the software exploit probability (EPSS score).

Data Security Standard 8: Unsupported Operating Systems (cont’d)

Software Inventory



Dashboard / Software

Default Layout

SOFTWARE				NORMALISED		VULNERABILITIES				
NAME	PUBLISHER	VERSION	INSTALLS	NORMALISED NAME	NORMALISED PUBLISHER	RISK ↓	CYBER ALERT RISK	KNOWN EXPLOITS	EXPLOIT PROBABILITY	TYPE
Mozilla Firefox (x64 en-US)	Mozilla	117.0	1	Firefox	Mozilla Foundation	● Medium		No	● Low Probability	OS Extensions & Utilities
Mozilla Firefox (x64 en-GB)	Mozilla	117.0	20	Firefox	Mozilla Foundation	● Medium		No	● Low Probability	OS Extensions & Utilities
Adobe Flash Player 32 NPAPI	Adobe	32.0.0.465	2	Flash Player NPAPI	Adobe	● Low		No	● No Probability	OS Extensions & Utilities
Adobe Bridge 2021	Adobe Inc.	11.1.3	1	Adobe Bridge	Adobe	● High		No	● No Probability	Business
QuickTime 7	Apple Inc.	7.79.80.95	41	QuickTime	Apple	● High		No	● No Probability	OS Extensions & Utilities
Adobe Illustrator CS6	Adobe Systems Incorporated	16.0	1	Illustrator	Adobe	● High		No	● No Probability	Business
Dell Command | Update for Windows 10	Dell Inc.	4.1.0	12	Command Update	Dell	● High		No	● No Probability	Business
Adobe Captivate 9 (64 Bit)	Adobe Systems Incorporated	9.0	4	Adobe Captivate	Adobe	● High		No	● No Probability	Business
HP System Management Homepage	Hewlett-Packard Development Company, L.P.	7.5.4	1	System Management Homepage	HP	● High		No	● No Probability	Non-UI Apps
Alienware Command Center Suite	Dell Inc	5.2.115.0	1	Alienware Command Center Suite	Dell	● High		No	● No Probability	OS Extensions & Utilities
MySQL Query Browser	MySQL AB	1.1.20	1	MySQL Query Browser	Oracle	● High		No	● Low Probability	Business
HP Support Assistant	HP Inc.	8.8.34.31	9	Support Assistant	HP	● High		No	● No Probability	Non-UI Apps
PyCharm Community Edition 2022.2.4	JetBrains s.r.o.	222.4459.20	1	PYCHARM COMMUNITY EDITION	jetbrains	● High		No	● No Probability	Business
OpenVPN 2.4.8-I602-Win10	OpenVPN Technologies, Inc.	2.4.8-I602-Win10	1	OpenVPN	OPenVPN Technologies	● High		No	● No Probability	Business
Oracle VM VirtualBox	Oracle Corporation	6.1.30	1	VirtualBox	Oracle	● High		No	● No Probability	Business
PRTG Network Monitor	Paessler AG	21	1	PRTG Network Monitor	Paessler	● High		No	● No Probability	Business
OpenSSL (64-bit)	Shining Light Productions	1.0.0	1	OpenSSL	Shining Light Productions	● High		No	● Extremely Probable	Business
Telegram Desktop	Telegram FZ-LLC	4.6.5	1	Telegram Desktop	Telegram	● High		No	● No Probability	End-User Distractions
Octopus Deploy Tentacle	Octopus Deploy Pty. Ltd.	6.3.417	4	Octopus Deploy Tentacle	Octopus Deploy	● High		No	● No Probability	Business
NVIDIA GeForce Experience	NVIDIA Corporation	2.11.4.125	1	GeForce Experience	NVidia	● High		No	● No Probability	Non-UI Apps
Adobe Lightroom	Adobe Inc.	6.5	6	Lightroom	Adobe	● High		No	● No Probability	Business
MySQL Installer - Community	Oracle Corporation	1.6.1.0	1	MySQL Installer - Community	Oracle	● High		No	● Low Probability	Business
MySQL Installer for Windows - Community	Oracle Corporation	1.6.7.0	6	MySQL Installer for Windows - Community	Oracle	● High		No	● Low Probability	Business

Rows per page 25 1-25 of 2849

Quick View

Name: QuickTime 7
Publisher: Apple Inc.
Version: 7.79.80.95
Tag:
Global Approval: Not Assigned
Version Approval:Not Assigned
Newer Version Detected (On Network): No

Type: OS Extensions & Utilities
Category: Desktop Utilities
Sub Category: Audio/Video Player

Installs 41

● Out of Date
● Vulnerabilities
● Known Exploit
● Exploit Probability

Vulnerabilities 15
CyberAlerts 0

Fig.7. The ITHealth Dashboard provides a complete software inventory, which is fully up to date at all times. This inventory is filterable and allows Trusts to easily pinpoint devices that have instances of vulnerable software or high exploit probability.

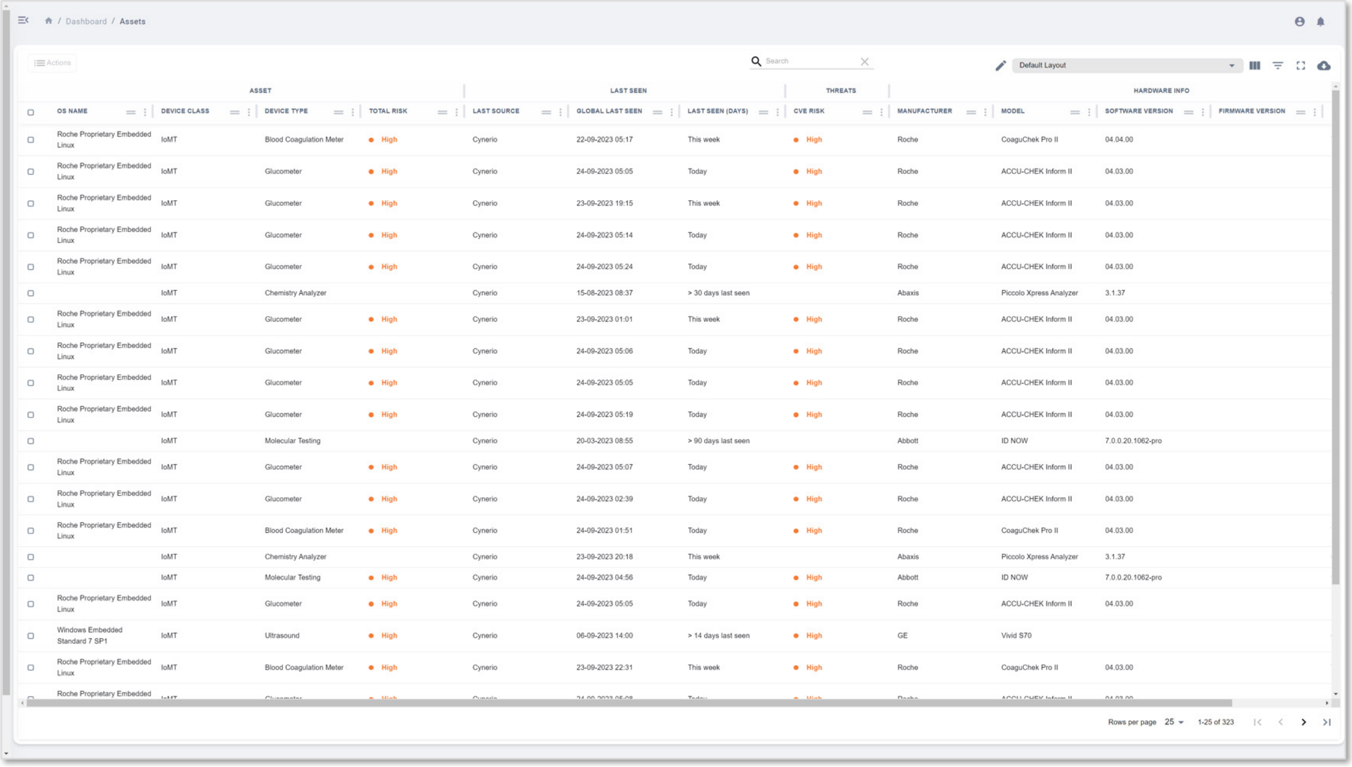
Data Security Standard 9: IT System Protection Strategy

Evidence code	**Evidence Text** (NHS Trusts, CSUs, ALBs, and ICBs - Category 1)	Mandatory?	How the ITHealth Dashboard helps
9.3.5	The organisation understands and records all IP ranges in use across the organisation.	Yes	The ITHealth Dashboard needs to be aware of all organisational IP ranges and will scan IP based devices. Passive Scanning technology can also be deployed to identify rogue devices that fall outside of the configured scanning targets.
9.3.8	The organisation maintains a register of medical devices connected to its network.	Yes	The ITHealth Dashboard can identify connected medical devices and be used to store information regarding maintenance arrangements and network location.
9.3.9	What is the organisation’s data security assurance process for medical devices connected to the network.	Yes	The ITHealth Dashboard can be used to identify vulnerabilities within medical devices, which can help with remediation and security management processes linked to these devices.
9.4.1	You validate that the security measures in place to protect the networks and information systems are effective, and remain effective for the lifetime over which they are needed.	No	The data contained within the ITHealth Dashboard’s many reports can be used to validate that security measures are in place and that devices comply with the local security policies and acceptance levels.
9.4.4	Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.	Yes	The ITHealth Dashboard makes it easier for Trusts to prioritise and remediate any security deficiencies.

Data Security Standard 9: IT System Protection Strategy (cont'd)

Evidence code	Evidence Text (NHS Trusts, CSUs, ALBs, and ICBs - Category 1)	Mandatory?	How the ITHealth Dashboard helps
9.5.1	All devices in your organisation have technical controls that manage the installation of software on the device.	Yes	The ITHealth Dashboard can be used as a management tool to deploy software installer packages to end user devices. If other software is used for this purpose the ITHealth Dashboard can identify that 'managed installation software' agents, like SCCM, is installed on all devices to provide assurance.
9.5.2	Confirm all data are encrypted at rest on all mobile devices and removable media and you have the ability to remotely wipe and/or revoke access from an end user device.	Yes	The ITHealth Dashboard identifies encryption status on devices that require it, such as laptops. Integration is possible with mobile device management solutions such as VMWare Workspace ONE, Microsoft Intune and Sophos Mobile to allow reporting on the status of mobile devices to ensure they comply with the enforced policies.
9.5.7	AutoRun is disabled.	Yes	The ITHealth Dashboard can report on the status of Auto-run across devices.
9.6.1	One or more firewalls (or similar network device) have been installed on all the boundaries of the organisation's internal network(s).	Yes	The ITHealth Dashboard will identify firewalls.
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.	Yes	The ITHealth Dashboard can identify devices without the host firewall enabled.

IoMT/Medical Device Asset Visibility

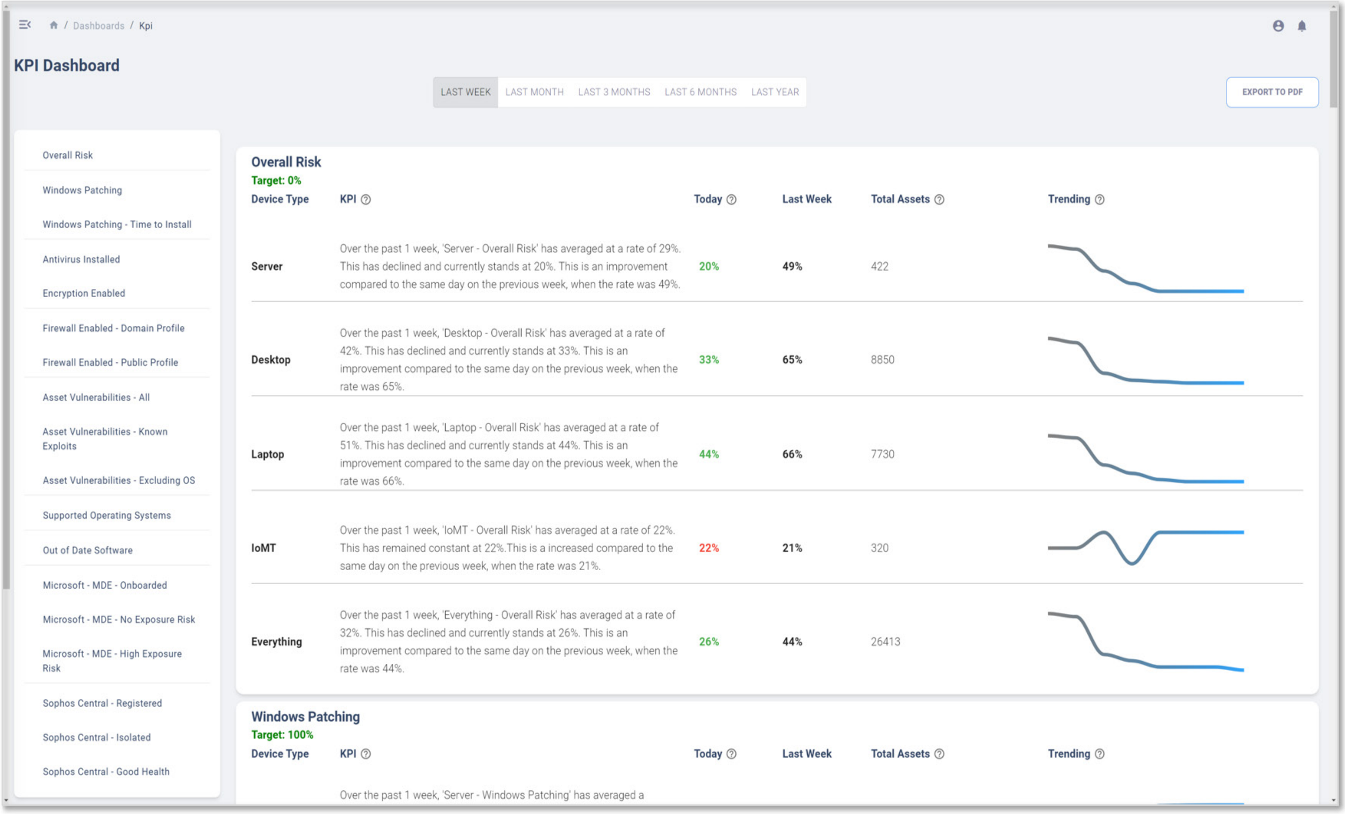


	ASSET				LAST SEEN			THREATS	HARDWARE INFO			
☐	OS NAME	DEVICE CLASS	DEVICE TYPE	TOTAL RISK	LAST SOURCE	GLOBAL LAST SEEN	LAST SEEN (DAYS)	CVE RISK	MANUFACTURER	MODEL	SOFTWARE VERSION	FIRMWARE VERSION
☐	Roche Proprietary Embedded Linux	IoMT	Blood Coagulation Meter	● High	Cynerio	22-09-2023 05:17	This week	● High	Roche	CoaguChek Pro II	04.04.00	
☐	Roche Proprietary Embedded Linux	IoMT	Glucometer	● High	Cynerio	24-09-2023 05:05	Today	● High	Roche	ACCU-CHEK Inform II	04.03.00	
☐	Roche Proprietary Embedded Linux	IoMT	Glucometer	● High	Cynerio	23-09-2023 19:15	This week	● High	Roche	ACCU-CHEK Inform II	04.03.00	
☐	Roche Proprietary Embedded Linux	IoMT	Glucometer	● High	Cynerio	24-09-2023 05:14	Today	● High	Roche	ACCU-CHEK Inform II	04.03.00	
☐	Roche Proprietary Embedded Linux	IoMT	Glucometer	● High	Cynerio	24-09-2023 05:24	Today	● High	Roche	ACCU-CHEK Inform II	04.03.00	
☐		IoMT	Chemistry Analyzer		Cynerio	15-08-2023 08:37	> 30 days last seen		Abaxis	Piccolo Xpress Analyzer	3.1.37	
☐	Roche Proprietary Embedded Linux	IoMT	Glucometer	● High	Cynerio	23-09-2023 01:01	This week	● High	Roche	ACCU-CHEK Inform II	04.03.00	
☐	Roche Proprietary Embedded Linux	IoMT	Glucometer	● High	Cynerio	24-09-2023 05:06	Today	● High	Roche	ACCU-CHEK Inform II	04.03.00	
☐	Roche Proprietary Embedded Linux	IoMT	Glucometer	● High	Cynerio	24-09-2023 05:05	Today	● High	Roche	ACCU-CHEK Inform II	04.03.00	
☐	Roche Proprietary Embedded Linux	IoMT	Glucometer	● High	Cynerio	24-09-2023 05:19	Today	● High	Roche	ACCU-CHEK Inform II	04.03.00	
☐		IoMT	Molecular Testing		Cynerio	20-03-2023 08:55	> 90 days last seen		Abbott	ID NOW	7.0.0.20.1062-pro	
☐	Roche Proprietary Embedded Linux	IoMT	Glucometer	● High	Cynerio	24-09-2023 05:07	Today	● High	Roche	ACCU-CHEK Inform II	04.03.00	
☐	Roche Proprietary Embedded Linux	IoMT	Glucometer	● High	Cynerio	24-09-2023 02:39	Today	● High	Roche	ACCU-CHEK Inform II	04.03.00	
☐	Roche Proprietary Embedded Linux	IoMT	Blood Coagulation Meter	● High	Cynerio	24-09-2023 01:51	Today	● High	Roche	CoaguChek Pro II	04.03.00	
☐		IoMT	Chemistry Analyzer		Cynerio	23-09-2023 20:18	This week		Abaxis	Piccolo Xpress Analyzer	3.1.37	
☐		IoMT	Molecular Testing	● High	Cynerio	24-09-2023 04:56	Today	● High	Abbott	ID NOW	7.0.0.20.1062-pro	
☐	Roche Proprietary Embedded Linux	IoMT	Glucometer	● High	Cynerio	24-09-2023 05:05	Today	● High	Roche	ACCU-CHEK Inform II	04.03.00	
☐	Windows Embedded Standard 7 SP1	IoMT	Ultrasound	● High	Cynerio	06-09-2023 14:00	> 14 days last seen	● High	GE	Vivid S70		
☐	Roche Proprietary Embedded Linux	IoMT	Blood Coagulation Meter	● High	Cynerio	23-09-2023 22:31	This week	● High	Roche	CoaguChek Pro II	04.03.00	
☐	Roche Proprietary Embedded	IoMT	Glucometer	● High	Cynerio	24-09-2023 05:08	Today	● High	Roche	ACCU-CHEK Inform II	04.03.00	

Rows per page 25 1-25 of 323

Fig.8. The ITHealth Dashboard displays all connected medical devices; it is possible to drill down into these devices to view associated vulnerabilities.

KPI (Key Performance Indicator) Views


Dashboards / Kpi
LAST WEEK
LAST MONTH
LAST 3 MONTHS
LAST 6 MONTHS
LAST YEAR
EXPORT TO PDF
Overall Risk
Windows Patching
Windows Patching - Time to Install
Antivirus Installed
Encryption Enabled
Firewall Enabled - Domain Profile
Firewall Enabled - Public Profile
Asset Vulnerabilities - All
Asset Vulnerabilities - Known Exploits
Asset Vulnerabilities - Excluding OS
Supported Operating Systems
Out of Date Software
Microsoft - MDE - Onboarded
Microsoft - MDE - No Exposure Risk
Microsoft - MDE - High Exposure Risk
Sophos Central - Registered
Sophos Central - Isolated
Sophos Central - Good Health

KPI Dashboard

Overall Risk

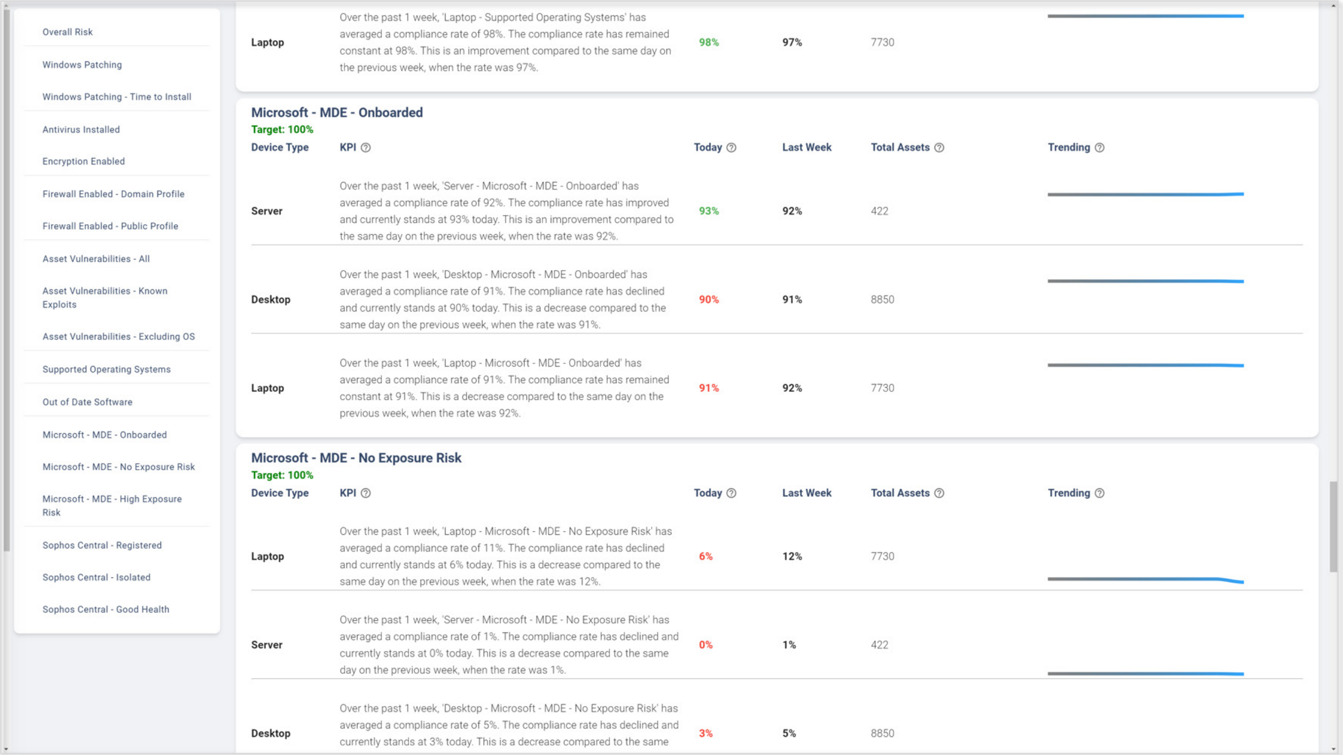
Target: 0%

Device Type	KPI ⓘ	Today ⓘ	Last Week	Total Assets ⓘ	Trending ⓘ
Server	Over the past 1 week, 'Server - Overall Risk' has averaged at a rate of 29%. This has declined and currently stands at 20%. This is an improvement compared to the same day on the previous week, when the rate was 49%.	20%	49%	422	
Desktop	Over the past 1 week, 'Desktop - Overall Risk' has averaged at a rate of 42%. This has declined and currently stands at 33%. This is an improvement compared to the same day on the previous week, when the rate was 65%.	33%	65%	8850	
Laptop	Over the past 1 week, 'Laptop - Overall Risk' has averaged at a rate of 51%. This has declined and currently stands at 44%. This is an improvement compared to the same day on the previous week, when the rate was 66%.	44%	66%	7730	
IoMT	Over the past 1 week, 'IoMT - Overall Risk' has averaged at a rate of 22%. This has remained constant at 22%.This is a increased compared to the same day on the previous week, when the rate was 21%.	22%	21%	320	
Everything	Over the past 1 week, 'Everything - Overall Risk' has averaged at a rate of 32%. This has declined and currently stands at 26%. This is an improvement compared to the same day on the previous week, when the rate was 44%.	26%	44%	26413	

Windows Patching

Target: 100%

Device Type	KPI ⓘ	Today ⓘ	Last Week	Total Assets ⓘ	Trending ⓘ
	Over the past 1 week, 'Server - Windows Patching' has averaged a				


Overall Risk
Windows Patching
Windows Patching - Time to Install
Antivirus Installed
Encryption Enabled
Firewall Enabled - Domain Profile
Firewall Enabled - Public Profile
Asset Vulnerabilities - All
Asset Vulnerabilities - Known Exploits
Asset Vulnerabilities - Excluding OS
Supported Operating Systems
Out of Date Software
Microsoft - MDE - Onboarded
Microsoft - MDE - No Exposure Risk
Microsoft - MDE - High Exposure Risk
Sophos Central - Registered
Sophos Central - Isolated
Sophos Central - Good Health

Laptop	Over the past 1 week, 'Laptop - Supported Operating Systems' has averaged a compliance rate of 98%. The compliance rate has remained constant at 98%. This is an improvement compared to the same day on the previous week, when the rate was 97%.	98%	97%	7730	

Microsoft - MDE - Onboarded

Target: 100%

Device Type	KPI ⓘ	Today ⓘ	Last Week	Total Assets ⓘ	Trending ⓘ
Server	Over the past 1 week, 'Server - Microsoft - MDE - Onboarded' has averaged a compliance rate of 92%. The compliance rate has improved and currently stands at 93% today. This is an improvement compared to the same day on the previous week, when the rate was 92%.	93%	92%	422	
Desktop	Over the past 1 week, 'Desktop - Microsoft - MDE - Onboarded' has averaged a compliance rate of 91%. The compliance rate has declined and currently stands at 90% today. This is a decrease compared to the same day on the previous week, when the rate was 91%.	90%	91%	8850	
Laptop	Over the past 1 week, 'Laptop - Microsoft - MDE - Onboarded' has averaged a compliance rate of 91%. The compliance rate has remained constant at 91%. This is a decrease compared to the same day on the previous week, when the rate was 92%.	91%	92%	7730	

Microsoft - MDE - No Exposure Risk

Target: 100%

Device Type	KPI ⓘ	Today ⓘ	Last Week	Total Assets ⓘ	Trending ⓘ
Laptop	Over the past 1 week, 'Laptop - Microsoft - MDE - No Exposure Risk' has averaged a compliance rate of 11%. The compliance rate has declined and currently stands at 6% today. This is a decrease compared to the same day on the previous week, when the rate was 12%.	6%	12%	7730	
Server	Over the past 1 week, 'Server - Microsoft - MDE - No Exposure Risk' has averaged a compliance rate of 1%. The compliance rate has declined and currently stands at 0% today. This is a decrease compared to the same day on the previous week, when the rate was 1%.	0%	1%	422	
Desktop	Over the past 1 week, 'Desktop - Microsoft - MDE - No Exposure Risk' has averaged a compliance rate of 5%. The compliance rate has declined and currently stands at 3% today. This is a decrease compared to the same	3%	5%	8850	

Fig. 9. Examples of the KPI views available within the ITHealth Dashboard. (The Data Security and Protection Toolkit isn't just about 'now', it's also about where you've been as an organisation and where you are heading.) ITHealth KPI views simplify risk monitoring and provide an effective way to measure the success of your organisation's cyber security efforts over time. KPI targets are customisable and benchmarking will also soon be available. KPI reports can include, for example, the average time taken to implement security patches, patch status in general, MDE (Microsoft Defender for Endpoint) onboarding, anti-virus/encryption installed, asset vulnerability and so on.

Conclusion

DSPT compliance naturally encourages NHS organisations to continually look at their cybersecurity measures and implement changes to adhere to requirements. Complete asset visibility, risk mitigation and threat detection will always remain core to ensuring compliance, and NHS organisations need access to systems that can effectively support in these three areas. The ITHealth Dashboard does just this as it provides a single source of truth for all network connected assets, increasing security visibility and allowing you to easily identify and manage exposure to cyber risk. Furthermore, not only does the ITHealth Dashboard support DSPT compliance, it is also extremely beneficial for other key regulatory requirements.

To learn more and request a demonstration of the ITHealth Dashboard Solution via WebEx, call 0115 987 6339 or visit www.ithealth.co.uk/dashboard-demonstration.

> "Yes - the ITHealth Dashboard significantly helps Trust compliance to the DSP Toolkit, but it is also instrumental in helping us meet ISO 27001, Cyber Essentials and Cyber Essentials Plus requirements."
>
> RICHARD PILKINGTON, IT Security Manager
> The Clatterbridge Cancer Centre NHS Foundation Trust

Stay assured and compliant

Get in touch for an ITHealth Dashboard demonstration

Call: 0115 987 6339

Email: info@ithealth.co.uk

Visit: www.ithealth.co.uk/dashboard-demonstration

About ITHealth

ITHealth provide NHS organisations with proven and trusted IT security and access management solutions. Our aim is threefold: to protect the availability, confidentiality and integrity of vital NHS systems and data, to protect staff, and to protect an NHS organisation's reputation. By doing so, we ultimately protect patient care.

Registered Office: ITHealth U.K. Ltd, 10 Churchill Park, Private Road, No 2, Colwick, Nottingham, NG4 2HF