How Forescout aids NHS Trusts with DSP Toolkit Alignment

Forescout Continuum delivers unparalleled insight into your entire network without disrupting critical business processes.

Gain actionable insights from out-of-the-box, customisable dashboards to quickly pinpoint, prioritise and proactively mitigate risks across your connected IT, OT, IoT and IoMT devices.

Key Features

- Discovers and classifies all IT, OT, IoT and IoMT devices upon connection, evaluates their security posture and segments them appropriately
- Enforces compliance and provides reporting through detailed, customizable dashboards
- Continuously assesses security risk posture by device classification
- Automates software updates, patch management and incident response

We live in an era of increased cybersecurity activity. Beyond uptime and availability, privacy and security are essential for mission critical operations in the healthcare sector. The number and complexity of inadequately protected IT, OT, IoT and IoMT devices has only ballooned in the past few years, requiring organisations to be able to wrap their hands around their assets and risks.

This has brought compliance to the forefront of many organisations, whether we're talking Cyber Essentials, Cyber Essentials+, NIS, ISO27001, or other security and compliance frameworks.

In addition to providing valuable cybersecurity protection of your critical assets, the Forescout Continuum Platform can also help to satisfy critical compliance assertions within the DSP Toolkit.

What is the DSP Toolkit?

The Data Security and Protection (DSP) Toolkit is an online tool that enables relevant organisations to measure their performance against the data security and information governance requirements mandated by the Department of Health and Social Care (DHSC). All organisations that have access to NHS patient data and systems must use the DSP Toolkit to provide assurance that they are taking proper steps to secure patient data and that personal information is handled accordingly. Self-assessments of compliance are required to be conducted by these organisations against the assertions and evidence contained within the DSP Toolkit.

As this is a critical set of requirements that healthcare organisations must comply with, Forescout can help you to meet your obligations with respect to the DSP Toolkit self-assessment.

How Forescout helps NHS Trusts meet the following DSP Toolkit assertions

Assertion	Evidence Ref	Evidence Text – NHS Trusts (Category 1)	Tool Tips – NHS Trusts	What Forescout Continuum Provides
The organisation has a framework in place to support Lawfulness, Fairness and Transparency	1.1.3	Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities	Please provide documentary evidence	Forescout Continuum automatically classifies connected cyber assets and provides actionable contextual information to create governance policies. This includes providing full visibility and continuous asset discovery and inventory for the IT, OT, IoT and IoMT cyber assets on your network.
All staff understand that their activities on IT systems will be monitored and recorded for security purposes	4.3.2	Are users, systems and (where appropriate) devices always identified and authenticated prior to being permitted access to information or systems?	Please provide details. For critical systems you should consider if device authentication is required.	Forescout Continuum provides automatic, real-time detection and identification of all IP-connected network devices and allows organisations to tag each device and assign compliance policies and risk thresholds, which in turn can be leveraged for control and segmentation actions.
You closely manage privileged user access to networks and information systems supporting the essential service	4.4.3	The organisation only allows privileged access to be initiated from devices owned and managed or assured by your organisation	Explain any exceptions or risk management applied.	Forescout Continuum provides a real-time assessment of the connected device type, function, manageability and ownership, with the currently logged in user including group membership. This context is utilised to define logical business taxonomy groups, map out network communication flows between assets, and enforce network segmentation rules to help ensure privileged access is only granted to the correct user, on known safe, compliant and risk-free devices.
	4.5.1	Do you have a password policy giving staff advice on managing their passwords?	The password policy must cover: a. How to avoid choosing obvious passwords (such as those based on easily discoverable information). b. Not to choose common passwords (use of technical means, such as using a password blocklist, is recommended). c. No password reuse. d. Where and how they may record passwords to store and retrieve them securely. e. If password management software is allowed, and if so, which. f. Which passwords they really must memorise and not record anywhere. g. Assessing risks to ensure systems use appropriate authentication measures e.g. high-strength passwords enforced technically for all users of internet-facing authentication services.	The Forescout Continuum Platform can assist in this regard by helping to ensure all default or compromised passwords in devices are not present. When these passwords are discovered, the device can automatically have its networks access restricted and support tickets raised for remediation.
	4.5.2	Technical controls enforce password policy and mitigate against password-guessing attacks.	Examples of technical controls are provided by the National Cyber Security Centre.	As 4.5.1

Assertion	Evidence Ref	Evidence Text – NHS Trusts (Category 1)	Tool Tips – NHS Trusts	What Forescout Continuum Provides
All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway	6.2.1	Has antivirus/anti-malware software been installed on all computers that are connected to or capable of connecting to the Internet?	This applies to: application servers; desktop computers; laptop computers, tablets and mobile devices running windows desktop operating systems. Please include the name of your anti-virus product in the comments.	Real-time discovery and assessment of every connected asset - IT, OT, IoMT, IoT, as well as assessment of AV/EDR, and other security agents currently installed on every relevant asset type. Monitor network communication patterns for device type, including Internet connectivity. The multifactor risk score combines exposed services and communication to malicious internet IP addresses.
	6.2.3	Antivirus/anti-malware is kept continually up to date	Provide an explanation of how this is achieved. This could be through automatic update, central deployment, ATP etc.	Real-time discovery and assessment of connected assets, as well as assessment of AV/EDR and other security agents currently installed, running and up to date.
	6.2.7	Does the organisation maintain a list of approved applications, and are users prevented from installing any application that is unsigned or has an invalid signature?	This applies to: email, Servers, desktop computers, laptop computers; tablets and mobile phones. Provide details of how this is enforced.	Forescout Continuum provides a real-time assessment of the software and services running on desktops, laptops, workstations and servers. Policies can be defined to assess unauthorised applications and initiate remediation actions where required.
	6.3.3	The organisation has a proportionate monitoring solution to detect cyber events on systems and services.	Since 1st July 2022, all systems monitoring requirements have been assessed and technology solutions and processes have been implemented to detect cyber security events. A risk based approach to monitoring for all systems should be in place ensuring that the organisation's most critical services and assets are in scope of its monitoring solutions. Where any gaps have been identified, mitigations have been put in place.	Forescout Continuum hits this requirement in two distinct areas, firstly it feeds real-time security event data into SIEM tools. Secondly the Forescout platform has SOC in the cloud services to provide L1 and L2 analyst capabilities.
	7.1.2	Do you have well defined processes in place to ensure the continuity of services in the event of a data security incident, failure or compromise?	This may include the preservation of manual processes for essential services.	The Forescout Continuum Plaform assists in the area by providing the capability of isolating or restricting any compromised devices from the network, thereby reducing the blast radius and restricting the device from being a pivot point for lateral movement.
	8.1.1	Provide evidence of how the organisation tracks and records all software assets and their configuration.	This is a list of all the software that is used in the organisation including version numbers and whether the software is supported i.e. it still receives security updates.	Forescout Continuum can assist in this requirement by reporting on all installed software with versions details across the managed device estate. This data can also be sent to a CMDB for a centralised view.
	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.	Provide summary details in the comments box. Documentation should be held locally for protections for these devices. This applies to any device (managed internally or by a third party) that can connect to the Internet including application servers; desktop computers; laptop computers, tablets and mobile devices running windows desktop operating systems. Example routes to the Internet include (but are not limited to) HSCN, N3/Transition network, VPNs, or cloud computing services. Devices that are standalone or air-gapped should be captured under 9.5.9.	The Forescout Continuum Platform provides 100% visibility of all devices (IT, IOT, IoMT and OT) connecting to the network as soon as they connect. Each device is continually assessed for compliance, and any device that is deemed a security risk can be isolated on the network. A support ticket can be raised through integration with ITSM tooling, so the device is investigated. When the issue is resolved or accepted the device will be allowed to rejoin the relevant network.

Assertion	Evidence Ref	Evidence Text – NHS Trusts (Category 1)	Tool Tips – NHS Trusts	What Forescout Continuum Provides
You closely manage privileged user access to networks and information systems supporting the essential service	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.	Covers software running on computers that are connected to the internet.	All installed software on managed IT endpoints is continually assessed, and software that is out of compliance can be uninstalled via Forescout Continuum control policies. Endpoints that remain as non-compliant can automatically be isolated or have their access restricted on the network until the issue is resolved or accepted.
	8.4.1	Is all your infrastructure protected from common cyber-attacks through secure configuration and patching?	Explain at a summary level. Where it is not possible to apply these measures, explain any mitigations (such as logical separation).	Forescout Continuum continually assesses the unique components for each specific device type by compliance policy, including patch level, running services, registry settings and vulnerabilities. The platform monitors network communication patterns for connected device type to assess exposed services or the use of unsecure communications protocols. Forescout Continuum can assess the underlying computer and network infrastructure.
You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service	8.4.2	All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support	Covers software running on computers that are connected to or capable of connecting to the Internet. Unsupported software should be covered under 8.3.4.	Forescout Continuum conducts real-time discovery and assessment of every connected asset - IT, OT, IoMT, IoT, operating system, and patch levels.
	8.4.3	You maintain a current understanding of the exposure of your hardware and software to publicly known vulnerabilities	This may include NHS Digital's VMS and / or Bitsight service.	Forescout Continuum provides real-time assessment of vulnerabilities for each asset type and augments the data with feeds from 3rd party VA tools and threat intelligence, to provide asset-specific risk scores, for cybersecurity risk, operational risk, and biomedical risk (to human life).
All networking components have had their default passwords changed	9.1.2	The Head of IT, or equivalent role, confirms all organisational devices have had their default passwords changed.	This covers the organisation's servers, desktop computers, laptop computers, tablets and mobile phones.	Forescout Continuum has unique assessment capabilities to discover if known default, weak or commonly used credentials are still in use on IoT devices and network infrastructure.
Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities	9.3.8	The organisation maintains a register of medical devices connected to its network.	The register should be uploaded and include Vendor, maintenance arrangements, any network segmentation is in place and whether network access is given to supplier/maintainer.	Forescout Continuum automatically classifies cyber assets and provides actionable contextual information to create governance policies. This includes providing full visibility and continuous asset discovery and inventory for the IT, OT, IoT and IoMT cyber assets on your network. This high granularity accounting includes the device's type, vendor, model, software version and hardware IDs (MAC, SN).
	9.3.9	What is the organisation's data security assurance process for medical devices connected to the network?	This should be a policy / process document or full explanation covering how the organisation assures data security during the full life cycle of the medical device.	Forescout Continuum identifies the device from the moment it connects to the network. Once an asset is identified, the solution analyses device communication, taking into account multiple variables. This includes the content of medical protocols, HTTP/S communication, DNS/DHCP, LDAP and more. This is matched against Forescout's extensive device database and then classified. Once the device is classified, the solution provides a risk assessment based on the complete ecosystem, the vulnerabilities of the device, the network flows and threats to it, who it communicated with and business risk factors throughout the device lifecycle.

Assertion	Evidence Ref	Evidence Text – NHS Trusts (Category 1)	Tool Tips – NHS Trusts	What Forescout Continuum Provides
You securely configure the network and information systems that support the delivery of essential services	9.5.1	All devices in your organisation have technical controls that manage the installation of software on the device.	Describe how this is managed across your devices with detail of any exceptions.	For IT networks, Forescout Continuum inspects and creates an inventory of software that is installed and running on devices in the system. It then compares that inventory to a whitelist of approved software versions or a blacklist of prohibited ones, and approves, denies or restricts access based on the result. This evaluation can also generate alerts, repair tickets and reports, and initiate remediation actions. Forescout Continuum can also integrate with third-party systems for software lifecycle management. For OT networks, Forescout Continuum provides elective scanning technology specifically for OT, and can track Windows patches and applications on the OT network.
	9.5.3	You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.	Provide details of your organisation's change management process that prevents changes to its IT environment from being implemented without being approved by the appropriate individuals and security implications being considered.	Forescout Continuum automates response workflows, including SIEM/SOC incident response and dynamic segmentation, to protect high risk networks and keep mission critical assets online. This is achieved natively and via other security tools using pre-built bi-directional integrations. By connecting the existing security ecosystem, Forescout Continuum multiplies the effect of each solution operating in isolation.
	9.5.4	Only approved software can be installed and run, and unnecessary software is removed.	This is for all devices in your organisation including servers, desktop computers, laptop computers, tablets, mobile phones. This could be an allow list solution.	Forescout Continuum provides a real-time assessment of the software and services running on desktops, laptops, workstations and servers. Policies can be defined to assess unauthorized applications and initiate remediation actions where required.
The organisation is protected by a well-managed firewall	9.6.6	Do all of your desktop and laptop computers have personal firewalls (or equivalent) enabled and configured to block unapproved connections by default?	Provide details of how you have implemented this and describe the confirmation process.	Forescout Continuum provides real-time discovery and assessment of every connected asset - IT, OT, IoT, IMoT asset, which includes an assessment of installed and running security agents such as a local firewall solution.

FORESCOUT®

Forescout Technologies, Inc.

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com