Cyber Assessment Framework (CAF) Aligned Data Security and Protection Toolkit (DSPT) for UK NHS Organisations

How Forescout helps NHS organisations meet new CAF aligned DSP Toolkit requirements

The Forescout Platform 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 for detailed reporting and customisable dashboards
- Enforces compliance, access control and segmentation with automated policy actions
- Continuously assess security risk and threat posture leveraging rich threat intelligence and log ingestion
- Automate Software Updates, patch management and incident response

Recently, the DSP Toolkit adopted the National Cyber Security Centre's Cyber Assessment Framework (CAF) as its basis for cybersecurity assurance. The CAF was created to address the growing need for a consistent and effective approach toward cybersecurity risk management in the public sector.

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 organsisations, 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 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 Organisations Meet the Following DSP Toolkit Requirements

Principle	Outcome	How Forescout Helps
Objective A: Managing Risk		
A1: Governance The organisation has appropriate management policies, processes and procedures in place to govern its approach to the security and governance of information, systems and networks.	**Key: A1.a Board Direction**	
	Your organisation's approach and policy relating to the security of network and information systems supporting the operation of your essential function(s) are owned and managed at board-level. These are communicated, in a meaningful way, to risk management decision-makers across the organisation.	The Forescout platform offers a streamlined, user-friendly interface for creating, customising, and scheduling various reports related to Threat Detection and Response (TDR) and Network Security. Executive and operator level reports use generative AI to serve specific needs of different departments or stakeholders, and reports can provide real-time data and track progress over time. Reports can be scheduled to run automatically and sent to selected recipients, ensuring that key stakeholders receive necessary information promptly.
	Regular board-level discussions on the security of network and information systems supporting the operation of your essential function(s) take place, based on timely and accurate information and informed by expert guidance.	
A2: Risk Management The organisation takes appropriate steps to identify, assess and understand risks to the security and governance of information, systems and networks supporting the operation of essential functions. This includes an overall organisational approach to risk management.	**Key: A2.a Risk Management Process**	
	Your organisational process ensures that security risks to network and information systems relevant to essential function(s) are identified, analysed, prioritised, and managed.	The Forescout platform 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
	Your approach to risk is focused on the possibility of adverse impact to your essential function(s), leading to a detailed understanding of how such impact might arise as a consequence of possible attacker actions and the security properties of your network and information systems.	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. The Forescout platform also 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.
	Your risk assessments are based on a clearly understood set of threat assumptions, informed by an up-to-date understanding of security threats to your essential function(s) and your sector.	
	Your risk assessments are informed by an understanding of the vulnerabilities in the network and information systems supporting your essential function(s).	
	The output from your risk management process is a clear set of security requirements that will address the risks in line with your organisational approach to security.	The Forescout platform provides suggested actions and remediations to mitigate and lower risk levels.
	Your risk assessments are dynamic and updated in the light of relevant changes which may include technical changes to network and information systems, change of use and new threat information.	The Forescout platform continuously identifies exposures across all cyber assets, managed and unmanaged, for real-time visibility of the attack surface. Organisations can strategically assess and prioritise asset risks to make better security and business decisions.
	The effectiveness of your risk management process is reviewed regularly, and improvements made as required.	The Forescout platform provides a timeline for every asset which shows progress towards organisations goals with reducing risk.

Principle	Outcome	How Forescout Helps
A2: Risk Management The organisation takes appropriate steps to identify, assess and understand risks to the security and governance of information, systems and networks supporting the operation of essential functions. This includes an overall organisational approach to risk management.	**Key: A2.a Risk Management Process**	
	You perform detailed threat analysis and understand how this applies to your organisation in the context of the threat to your sector and the wider CNI.	The Forescout platform enriches and analyses IT, IoT and OT telemetry from across your organisation, leveraging AI and other data science techniques to correlate signals and more accurately reveal true threats, empowering you to respond quickly and appropriately.
	You validate that the security measures in place to protect the network and information systems are effective and remain effective for the lifetime over which they are needed.	Forescout 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 can also assess the underlying computer and network infrastructure.
	The methods used for assurance are reviewed to ensure they are working as intended and remain the most appropriate method to use.	The Forescout platform can assure that assets are compliant to stay connected to the network, and you have the capability to audit zero trust policies for any violations.
A3: Asset Management Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).	**Key: A3.a Asset Management**	
	All assets relevant to the secure operation of essential function(s) are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date.	The Forescout platform maintains a real-time, up-to-date asset inventory with customisable device functions. The platform also allows bi-directional synchronisation with CMDB systems.
	You have prioritised your assets according to their importance to the operation of the essential function(s).	The Forescout platform provides a customisable device criticality field to help prioritise the most essential assets.
	You have assigned responsibility for managing all assets, including physical assets, relevant to the operation of the essential function(s).	All assets in the Forescout platform can be assigned to a specific device owner based on functional roles.
Objective B		
B1: Policies, Processes, and Procedures The organisation defines, implements, communicates and enforces appropriate policies, processes and procedures that direct its overall approach to securing information, systems and data that support operation of essential functions.	**Key: B1.b Policy, Process and Procedure Implementation**	
	All your policies, processes and procedures are followed, their correct application and security effectiveness is evaluated.	Forescout continually assesses each device 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.
	Appropriate action is taken to address all breaches of policies, processes and procedures with potential to adversely impact the essential function(s) including aggregated breaches.	Any asset that is out of compliance can be isolated or uninstalled via the Forescout platform control policies. Endpoints that remain non-compliant can automatically be isolated or have their access restricted on the network until the issue is resolved or accepted.

Principle	Outcome	How Forescout Helps
B2: Identity and Access Control The organisation understands, documents and manages access to information, systems and networks supporting the operation of essential functions. Individuals (or automated functions) that can access data or systems are appropriately verified, authenticated and authorised.	**Key: B2.a Identity Verification, Authentication and Authorisation**	
	Your process of initial identity verification is robust enough to provide a high level of confidence of a user's identity profile before allowing an authorised user access to network and information systems that support your essential function(s).	Forescout enforces and automates zero trust policies for least-privilege access for all managed and unmanaged devices across your network, including IT, OT, IoT and IoMT devices. You can apply policy-based controls to enforce device compliance, proactively reduce your attack surface and rapidly respond to incidents. The Forescout platform enforces network access based on user (employee, guest, contractor), device classification and security posture – in any heterogeneous network with or without 802.1X.
	Only authorised and individually authenticated users can physically access and logically connect to your network or information systems on which your essential function(s) depends.	
	Your approach to authenticating users, devices and systems follows up to date best practice.	Forescout can classify, assess, and authenticate devices utilising industry stands such as 802.1X, RADIUS, LDAP, SAML, and more.
	Key: B2.b Device Management	
	All privileged operations performed on your network and information systems supporting your essential function(s) are conducted from highly trusted devices, such as Privileged Access Workstations, dedicated solely to those operations.	Forescout 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.
	You either obtain independent and professional assurance of the security of third-party devices or networks before they connect to your network and information systems, or you only allow third-party devices or networks that are dedicated to supporting your network and information systems to connect.	The Forescout platform assesses every device 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.
	You perform certificate-based device identity management and only allow known devices to access systems necessary for the operation of your essential function(s).	Forescout can perform certificate-based authentication such as EAP-TLS for user and machine certificates.
	You perform regular scans to detect unknown devices and investigate any findings.	The Forescout platform discovers all managed and unmanaged devices upon connecting to the network, leveraging techniques tailored specifically IT, IoT, OT and IoMT assets as well as cyber-physical systems. Devices are then automatically classified based on 150+ attributes that are then referenced for asset compliance, network access control, segmentation and incident response.
	Key: B2.d Identity and Access Management	
	Attempts by unauthorised users, devices or systems to connect to the systems supporting the essential function(s) are alerted, promptly assessed and investigated.	The Forescout platform can monitor and provide alerts for any inbound or outbound device communication that is considered unauthorised.

Principle	Outcome	How Forescout Helps
B4: System Security Network and information systems and technology critical for the operation of essential functions are protected from cyber-attack. An organisational understanding of risk to essential functions informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.	**Key: B4.a Secure by Design**	
	Your network and information systems are segregated into appropriate security zones (e.g. systems supporting the essential function(s) are segregated in a highly trusted, more secure zone).	The Forescout platform accelerates the design, planning and deployment of dynamic network segmentation. You can perform dynamic VLAN assignment, SGT tagging, and firewall tagging, and can audit traffic between segments.
	The network and information systems supporting your essential function(s) are designed to have simple data flows between components to support effective security monitoring.	Forescout can visualise traffic flows to see what should / should not be communicating and simulate policy changes to avoid gaps and misconfigurations, without causing business disruption.
	Key: B4.b Secure Configuration	
	You have identified, documented and actively manage (e.g. maintain security configurations, patching, updating according to good practice) the assets that need to be carefully configured to maintain the security of the essential function(s).	The Forescout platform 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 can also assess the underlying computer and network infrastructure, including operating system, which software / OS versions are installed, and patch levels
	All platforms conform to your secure, defined baseline build, or the latest known good configuration version for that environment.	
	You regularly review and validate that your network and information systems have the expected, secure settings and configuration.	
	Only permitted software can be installed.	
	Generic, shared, default name and built-in accounts have been removed or disabled. Where this is not possible, credentials to these accounts have been changed.	The Forescout platform has unique assessment capabilities to discover if known default, weak or commonly used credentials are still in use on devices and network infrastructure
	Key: B4.c Secure Management	
	Your systems and devices supporting the operation of the essential function(s) are only administered or maintained by authorised privileged users from highly trusted devices, such as Privileged Access Workstations, dedicated solely to those operations.	The Forescout platform provides a detailed 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.
	You prevent, detect and remove malware, and unauthorised software. You use technical, procedural and physical measures as necessary.	The Forescout platform can detect and remove unauthorised software on managed IT devices.
	Key: B4.d Vulnerability Management	
	You maintain a current understanding of the exposure of your essential function(s) to publicly-known vulnerabilities.	The Forescout platform assesses all assets – IT, OT, IoT, and IoMT - and quantifies their risk and potential exposure to the network and can highlight information such as known exploited vulnerabilities.
	Announced vulnerabilities for all software packages, network and information systems used to support your essential function(s) are tracked, prioritised and mitigated (e.g. by patching) promptly.	The Forescout platform provides real-time assessment of vulnerabilities for each asset type and augments the data with feeds from third-party VA tools and threat intelligence, to provide asset-specific risk scores, for cybersecurity risk, operational risk, and biomedical risk (to human life)
	You regularly test to fully understand the vulnerabilities of the network and information systems that support the operation of your essential function(s) and verify this understanding with third-party testing.	Forescout ensures vulnerability scans are occurring regularly and triggering scans when needed.

Principle	Outcome	How Forescout Helps
B5: Resilient Networks and Systems The organisation builds resilience against cyber-attack and system failure into the design, implementation, operation and management of systems that support the operation of essential functions.	**Key: B5.a Resilience Preparation**	
	You use your security awareness and threat intelligence sources to identify new or heightened levels of risk, which result in immediate and potentially temporary security measures to enhance the security of your network and information systems (e.g. in response to a widespread outbreak of very damaging malware).	Forescout Vedere Labs conducts threat intelligence research that is consumable via reports, dashboards and machine-readable threat feeds that are delivered to key community stakeholders – and ingested by the Forescout platform, to help ensure organisations have timely, state-of-the-art network security.
	Key: B5.b Design for Resilience	
	Network and information systems supporting the operation of your essential function(s) are segregated from other business and external systems by appropriate technical and physical means (e.g. separate network and system infrastructure with independent user administration). Internet services are not accessible from network and information systems supporting the essential function(s).	The Forescout platform accelerates the design, planning and deployment of dynamic network segmentation. You can perform dynamic VLAN assignment, SGT tagging, and firewall tagging, and have the ability to audit traffic between segments.
Objective C		
C1: Security Monitoring The organisation monitors the security status of the network and information systems supporting the operation of essential functions in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.	**Key: C1.a Monitoring Coverage**	
	Monitoring is based on an understanding of your networks, common cyber attack methods and what you need awareness of in order to detect potential security incidents that could affect the operation of your essential function(s) (e.g. presence of malware, malicious emails, user policy violations).	Forescout converts telemetry and logs into high fidelity, SOC-actionable probable threats. It automates and accelerates the process of detecting, investigating, hunting for and responding to advanced threats across an entire organisation. From cloud, campus, remote and datacenter environments to IT, OT/ICS, IoT and IoMT devices, Forescout combines essential SOC technologies and functions into a unified, cloud-native platform —and makes it viewable and actionable within a single console.
	Your monitoring data provides enough detail to reliably detect security incidents that could affect the operation of your essential function(s).	
	Extensive monitoring of user activity in relation to the operation of your essential function(s) enables you to detect policy violations and an agreed list of suspicious or undesirable behaviour.	Forescout can monitor network traffic to verify zero trust policies are being enforced and take actions when necessary.
	You have extensive monitoring coverage that includes host-based monitoring and network gateways.	Forescout can integrate with the entire security ecosystem including endpoint protection and network firewalls/ gateways. The Forescout platform can be customised to ingest logs from any security platform so they can be parsed and correlated with other events.
	All new systems are considered as potential monitoring data sources to maintain a comprehensive monitoring capability.	
	Key: C1.c Generating Alerts	
	Log data is enriched with other network knowledge and data when investigating certain suspicious activity or alerts.	The Forescout platform supports a wide range of third-party vendor solutions and can ingest data from any managed and unmanaged device (IT, OT/ICS, IoT, IoMT). This ensures more comprehensive, powerful, flexible, and effective threat detection
	A wide range of signatures and indicators of compromise is used for investigations of suspicious activity and alerts.	
	Alerts can be easily resolved to network assets using knowledge of networks and systems. The resolution of these alerts is performed in almost real time.	The Forescout platform triggers vulnerability scans upon connect, verifies agents are installed, up-to-date, and functioning properly, and detects illegitimate privileged accounts. Response actions can be initiated automatically and coordinated using policy-based remediation / mitigation actions based on prioritised risk, allowing immediate response to true threats using existing security tools.
	Security alerts relating to all essential function(s) are prioritised and this information is used to support incident management.	
	Logs are reviewed almost continuously, in real time.	
	Alerts are tested to ensure that they are generated reliably and that it is possible to distinguish genuine security incidents from false alarms.	

Principle	Outcome	How Forescout Helps
C1: Security Monitoring The organisation monitors the security status of the network and information systems supporting the operation of essential functions in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.	**Key: C1.d Identifying Security Incidents**	
	You have selected threat intelligence sources or services using risk-based and threat- informed decisions based on your business needs and sector (e.g. vendor reporting and patching, strong anti-virus providers, sector and community-based infoshare, special interest groups).	Forescout Vedere Labs focuses on increasing visibility of cybersecurity threats and vulnerabilities for all connected asset types and providing mitigation steps organisations can use to protect themselves. Our research is fed into the Forescout platform and shared with the cybersecurity community, including CISA and other cybersecurity agencies, CERTs, ISACs, open-source projects, device manufacturers, universities, and other researchers.
	You apply all new signatures and IoCs within a reasonable (risk-based) time of receiving them.	The Forescout platform can leverage threat detection and threat prevention mechanisms from third-party systems with the network visibility and enforcement capabilities we provide. This allows organisations to accelerate response time, automate workflows, improve operational efficiency, and provide superior security.
	Key: C1.e Monitoring Tools and Skills	
	Your monitoring tools make use of all log data collected to pinpoint activity within an incident.	The Forescout platform collects telemetry and logs from a wide range of sources, including security tools, applications, infrastructure, cloud and other enrichment sources; correlates attack signals to generate high-fidelity threats for analyst investigation and enables automated response actions across the network.
	Monitoring staff and tools drive and shape new log data collection and can make wide use of it.	
	Monitoring staff are aware of the operation of essential function(s) and related assets and can identify and prioritise alerts or investigations that relate to them.	
C2: Proactive Security Event Discovery The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades standard signature-based security prevent/ detect solutions (or when standard solutions are not deployable).	**Key: C2.a System Abnormalities for Attack Detection**	
	Normal system behaviour is fully understood to such an extent that searching for system abnormalities is a potentially effective way of detecting malicious activity (e.g. You fully understand which systems should and should not communicate and when).	Forescout can monitor network traffic to verify zero trust policies are enforced and send alerts when necessary.
	System abnormality descriptions from past attacks and threat intelligence, on yours and other networks, are used to signify malicious activity.	Forescout feeds real-time security event data into SIEM tools and has SOC in the cloud services to provide L1 and L2 analyst capabilities. The Forescout platform lets organisations query, investigate and analyse contextual asset data over a 90-day timeline to establish historical compliance and identify potential risks and gaps.
	Key: C2.b Proactive Attack Discovery	
	You routinely search for system abnormalities indicative of malicious activity on the network and information systems supporting the operation of your essential function(s), generating alerts based on the results of such searches.	Forescout can monitor network traffic to verify zero trust policies are enforced and send alerts when necessary.

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