WHITEPAPER

Meeting the NHS Data Security and Protection Toolkit Standards

BeyondTrust

Contents

Introduction: What is the NHS Data and Protection Toolkit?

The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards.

All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

The Importance of meeting the NHS Toolkit Standard

Participation is mandatory for all organisations that process NHS patient data in order to ensure robust data security and data privacy standards are in place across the healthcare sector.

The DSP Toolkit builds on the general principle that organisations should maintain the security of personal information and support the key requirements of the General Data Protection Regulation (GDPR).

How BeyondTrust Can Help You

For this brief, we will explore some of the fundamental assertions and requirements from the NHS DSP Toolkit, and show how they align with BeyondTrust capabilities. In the pages that follow you will find specific control guidance directly from the official NHS Specification document, and information regarding how BeyondTrust supports each.

NHS Data and Security Protection Requirements Chart

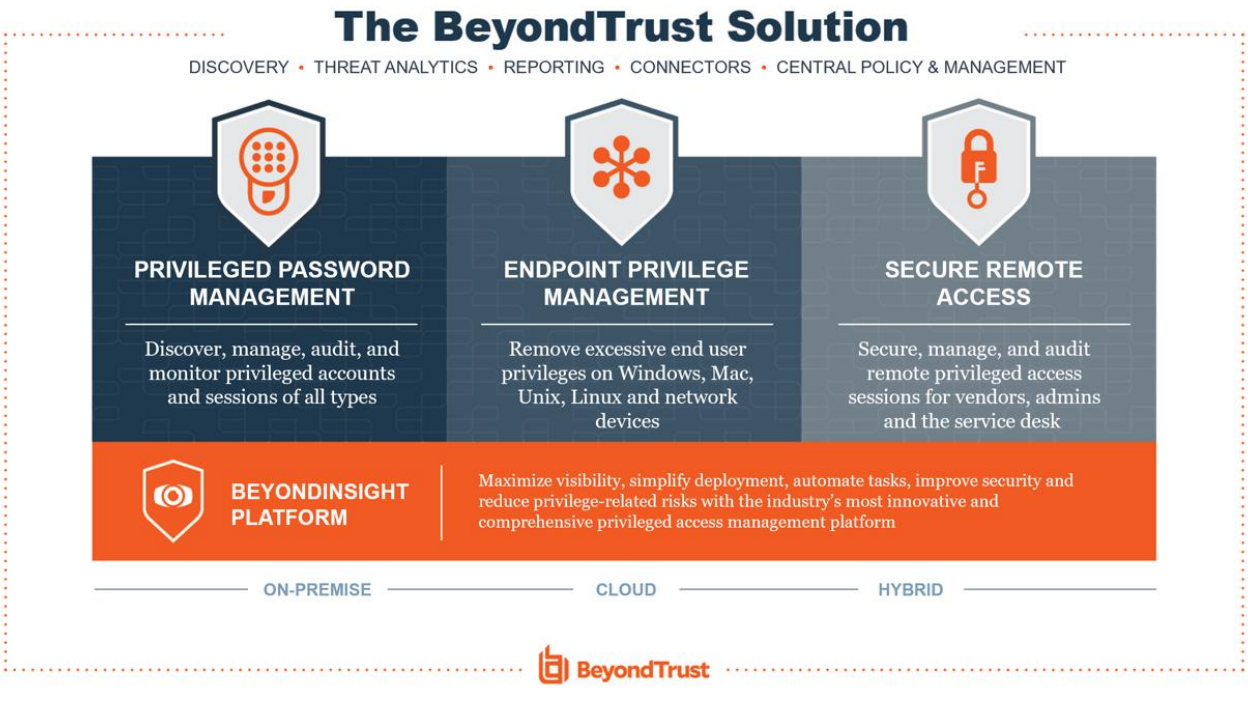
Assertion	Ref	How BeyondTrust Align
Is there is an approved procedure that sets out the organisation's approach to data protection by design and by default, which includes pseudonymisation requirements?	1.6.1	BeyondTrust enables System Administers to easily comply with pseudonymisation requirements by offering a built-in tool to allow a user or endpoint to be anonymised as required.
There are technical controls that prevent information from being inappropriately copied or downloaded.	1.6.2	BeyondTrust allows administrators to define full role-based access for Remote Support and Privileged Remote Access. Our solutions provide granular access controls for tools like the clipboard and file transfers.
Does the organisation understand who has access to personal and confidential data through your systems, including any systems which do not support individual logins?	4.1.2	BeyondTrust helps control and manage privileges across the entire network. Using the solutions, Administrators can download user account reports which can help to demonstrate privileged user access levels and entitlement within the network.
Are users in your organisation only given the minimum access to sensitive information or systems necessary for their role?	4.1.3	BeyondTrust helps organisations implement the principles of least privilege in an effective, pragmatic manner. Customers can easily define granular policies for groups or individual users to help control access and permissions within the network. The combination of endpoint-least privilege and credential management ensures that users are only given the necessary permissions to do their job, at the time privileges are required.
Logs are retained for a sufficient period, reviewed regularly and can be searched to identify malicious activity.	4.2.3	BeyondTrust can help supplement these logs with additional context of Privilege Use - by using session recordings, metadata and access session forensics. Data is stored on the appliance for up to 90 days and can be off loaded to a file share or database for longer term storage.
Are unnecessary user accounts removed or disabled?	4.2.5	Administrators can view and report on credentials which have not been used for a long period of time. It is also possible to view the age of privileged credentials, to decide on whether an account should be removed or disabled.

All system administrators have signed an agreement which holds them accountable to the highest standards of use.	4.3.1	During login, it is possible to display an agreement that an Administrator must accept before accessing the solution. This prompt can be customized.
Are users, systems and (where appropriate) devices always identified and authenticated prior to being permitted access to information or systems?	4.3.2	Within BeyondTrust, users must be authenticated with a username and password before use. Multifactor authentication is also supported, alongside integration to LDAP, RADIUS, SAML and SCIM protocols. All information can also be exported into SIEM logging tools to increase visibility of user activity.
Have all staff been notified that their system use could be monitored?	4.3.5	During login, it is possible to display an agreement that can be customized to inform the user that their session could be monitored. The user must accept this banner before accessing the solution.
Has the Head of IT, or equivalent, confirmed that IT administrator activities are logged and those logs are only accessible to appropriate personnel?	4.4.1	The BeyondTrust solution will log all privileged activity, and reports can be generated on demand or on a scheduled basis. These logs are controlled by Role Based Access Controls, ensuring the confidentiality of data is not compromised.
The organisation does not allow users with wide ranging or extensive system privilege to use their highly privileged accounts for high-risk functions, in particular reading email and web browsing.	4.4.3	BeyondTrust removes excessive end user privileges across desktops and server estates, regardless of operating system. Quick start policies are available out of the box to reduce the time taken to deploy the solution and reduce the need for excessive user privilege.
The organisation only allows privileged access to be initiated from devices owned and managed by your organisation.	4.4.4	BeyondTrust solutions offer conditional access policies. For example, an administrator can restrict access to the solution based on date, time, or segments of the network. Allowed or Denied networks ranges can be defined.
You record and store all privileged user sessions for offline analysis and investigation.	4.4.5	When using BeyondTrust, all privileged users sessions are recorded in real time and provide searchable session meta data. All events, clicks, applications launched and screen data is captured for potential analysis and investigation.
Technical controls enforce password policy and mitigate against password-guessing attacks.	4.5.2	BeyondTrust can enforce a password policy for privileged accounts, and offer rotation on demand, on a schedule or after each time a privileged account is used. This combination of credential changes mitigates the risk of a privileged credential being guessed.

Multifactor authentication is used [wherever technically feasible].	4.5.3	BeyondTrust solutions offer MFA support using SAML2, LDAP, RADIUS, Kerberos or SCIM protocols.
Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.	4.5.4	The BeyondTrust Solution will automatically scan and discover privileged and built in accounts across the organisation. It is then possible to take these credentials under management, by automatically changing the password and storing it in an encrypted database. Role based access controls are then configured to ensure only the correct user(s) have access to Privileged Credentials. Password policies can also be defined to ensure high strength value.
Does your organisation grant limited privileged access and third-party access only for a limited time period, or is it planning to do so?	4.5.5	BeyondTrust allow organisations to define limited privileged access endpoints for 3rd Parties. This includes a connection period that may be limited to a particular application, requiring approval, or restricted to a date and time. This achieves just in time access.
How can staff report data security and protection breaches and near misses?	6.1.2	BeyondTrust offers Security Analysts the option to review privileged access sessions and make comments on them. Any suspicious behaviour can be flagged and raised as a concern within the solution for additional review. This action could also be captured in a SIEM tool.
How do your systems receive updates and how often?	8.3.1	BeyondTrust offers a single web-based interface for updating the solutions. Cloud customers are automatically kept on the latest release. Updates are typically released in 1-3 month cycles.
The Head of IT, or equivalent role, confirms all networking components have had their default passwords changed to a high strength password.	9.1.1	BeyondTrust solutions can scan your environment to detect privileged accounts. Using smart rules, privileged accounts can be automatically onboarded, and default credentials changed to long complex passwords, adhering to the password policy. Rotation can then be performed periodically, or after each use.
The Head of IT, or equivalent role, confirms all organisational devices have had their default passwords changed.	9.1.2	BeyondTrust solutions can scan your environment to detect privileged accounts. Using smart rules, privileged accounts can be automatically onboarded, and default credentials changed to long complex passwords, adhering to the password policy. Rotation can then be performed periodically, or after each use.
The organisation is protecting its data in transit (including email) using well-configured TLS v1.2 or better.	9.3.6	BeyondTrust uses TLS 1.3 to encrypt data in transit.
Only approved software can be installed and run and unnecessary software is removed.	9.6.4	BeyondTrust solutions can ensure that only approved software within the organization can be installed on an endpoint.
All remote access is authenticated.	9.6.9	BeyondTrust solutions can be configured to ensure Technicians are authenticated and authorized before they connect to remote endpoints.

The BeyondTrust Privileged Access Management Platform

The BeyondTrust Privileged Access Management platform is an integrated solution to provide control and visibility over all privileged accounts and users across all enterprise platforms. By uniting best of breed capabilities that many alternative providers offer as disjointed tools, the BeyondTrust Privileged Access Management platform simplifies deployments, reduces costs, improves system security, and closes gaps to reduce privileged risks.



Privilege Management for Windows and Mac

BeyondTrust Privilege Management for Desktops elevates privileges to known good applications that require them, controls application usage, and logs and reports on privileged activities using security tools already in place.
Learn more

Privilege Management for Windows Servers

BeyondTrust Privilege Management for Windows Servers reduces the risk of privilege misuse by assigning admin privileges to only authorized tasks that require them, controlling application and script usage, and logging and monitoring on privileged activities.
Learn more

Privilege Management for Unix/Linux Servers

BeyondTrust Privilege Management for Unix & Linux is an enterprise-class, gold-standard privilege management solution that gives you unmatched visibility and control over complex server environments.
Learn more

Password Safe

BeyondTrust Password Safe unifies privileged password and privileged session management, providing secure discovery, management, auditing, and monitoring for any privileged credential. Password Safe enables organizations to achieve complete control and accountability over privileged accounts.
Learn more

Privileged Remote Access

Secure, manage, and audit vendor and internal remote privileged access without a VPN. Privileged Remote Access enables security professionals to control, monitor, and manage privileged access to critical systems.
Learn more

Remote Support

Support everything with one secure Remote Support solution. With Remote Support, you can support Windows, Mac, Linux, iOS, network devices and peripherals with one secure tool. Elevate sessions with the built-in vault. Customize and brand the user experience.
Learn more

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network.

Learn more at beyondtrust.com.