Technical Configurations
&
Requirements

Our Commercial Statement

Copyright: All Intellectual Property Rights belonging to MCCORMICKCO Limited shall remain vested in that Party and no Party shall have ownership or use rights over MCCORMICKCO Limited Intellectual Property except as expressly granted in writing. The Company owns all rights, including Intellectual Property rights, in the Company's Technology and in the Services, any materials relating thereto, and any modifications, enhancements, customizations, updates, revisions or derivative works thereof. All rights not expressly granted to the CUSTOMER are reserved by the Company.

Non-disclosure agreement: Each Receiving Party agrees that it will not use or disclose any Confidential Information received from the Disclosing Party other than as expressly permitted under the terms of the Agreement or as expressly authorized in writing by the Disclosing Party. The Receiving Party will use the same degree of care to protect the Disclosing Party's Confidential Information as it uses to protect its own confidential information of like nature, but in no circumstances less than reasonable care. The Receiving Party will not disclose the Disclosing Party's Confidential Information to any person or entity other than its officers, principals, employees and permitted subcontractors, advisors, auditors and regulators who need access to such Confidential Information in order to effect the intent of the Agreement or to perform their regulatory function and who are bound by confidentiality terms no less restrictive that those in this Agreement.

Contract Terms: MCCORMICKCO have developed this document in line with our standard terms and conditions, a copy of which can be provided to the customer upon request. We believe these terms and conditions to be fair and reasonable in protecting the interests of both parties. Any quotation provided is subject to the use of these terms. Should the customer require amendments, MCCORMICKCO Limited will endeavour to meet the clients needs, however should this increase our risk or costs, we reserve the right to amend our quotation to reflect this.

MCCORMICKCO have taken reasonable steps to ensure that the information held within this document is accurate. We do not accept any liability for any loss or damages for the information or advice provided in this document or incorporated into this document by reference, or which is incurred as a result of the use or, or reliance upon, the information and advice contained within this document.

Our Contact Details

If you have any queries regarding this document, please contact:

Info@mccormickco.co.uk
MCCORMICKCO Limited
319 Hersham Road
Hersham
Surrey
KT125QA
Mobile: (+44) 7579003088

Document History

Date	Version	Owner	Status	Update
01/11/2021	.01	Matt McCormick	Draft	Initial Document
20/11/2021	1.0	Emily Pratt	Final	Final Document

Contents

About DSPT View®

We know from personal experience that Healthcare and Local Government use a great proportion of resource compiling the information necessary to submit the reassessment each year. Moreover, as a point in time snapshot of compliance, random audits tend to identify lapses or errors.

Remediation running up to each assessment also expends resource, but to put it simply, most organisations bound by the requirements of DSPT don't have the endless resource required to check, compile and maintain every aspect of the DSPT standard.

There are many management tools that bring insight into cyber security frameworks and standards that require the use on premise infrastructure, agents, a commitment to infrastructure resources and a high degree of access to your systems to gather the data and report.

DSPT View is a compliance tool to bring insight into your cyber posture and allowing remediation.

We have designed this to ensure there is a minimal impact on your on-premise or cloud-based presence with the key aim to release key resources to focus on remediation

We have APIs directly in to three (current) cyber threat intelligence feeds providing near real time data on your vulnerabilities include NHS Digital CareCerts without any manual intervention.

From the 149 assertions within the DSPT, we are able to provide evidence for 54 mandatory and support an additional 22 non-mandatory (Total 76) with 14 currently in our roadmaps for 2022 – 2023. Importantly all support is included in the price you can see in our proposal as well as any relevant development (released at our discretion).

Imagine a tool, built from experience that visualizes the assertions of Data Security Protection Toolkit. Imagine a tool, built to enable a safer cyber security threat horizon for NHS service providers.

Licence Requirements

To use DSPT View® you will need one of the following licences which will gives you access to Microsoft 365 Defender (Defender for Endpoints):

- Microsoft 365 E5 or A5
- Microsoft 365 E3 with the Microsoft 365 E5 Security add-on
- Microsoft 365 A3 with the Microsoft 365 A5 Security add-on
- Windows 10 Enterprise E5 or A5
- Windows 11 Enterprise E5 or A5
- Enterprise Mobility + Security (EMS) E5 or A5
- Office 365 E5 or A5
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Defender for Office 365 (Plan 2)

Additionally, you will need following:

- One email account (service account) correctly permissioned (see required permissions)
- One PowerBi Pro Licence

Note

Your organisation must have setup, configured and deployed Microsoft 365 Defender to use DSPT View®. If your organisation is just getting started with Microsoft 365 defender please visit Microsoft Documentation [Get started with Microsoft 365 Defender | Microsoft Docs](#)

Check your Existing Licenses

Go to Microsoft 365 admin center (admin.microsoft.com) to view your existing licenses. In the admin center, go to **Billing** > **Licenses**.

Note

You need to be assigned either the **Billing admin** or **Global reader role in Azure AD** to be able to see license information. If you encounter access problems, contact your global admin or IT Helpdesk.

Browser Requirements

Access Microsoft 365 Defender in the Microsoft 365 Defender portal using Microsoft Edge, Internet Explorer 11, or any HTML 5 compliant web browser.

Required Permissions

There are two ways to manage access to Microsoft 365 Defender

- **Global Azure Active Directory (AD) roles**
- **Custom role access**

Accounts assigned the following Global Azure Active Directory (AD) roles can access Microsoft 365 Defender functionality and data:

- Global administrator
- Security administrator
- Security Operator
- Global Reader
- Security Reader

To review accounts with these roles, view Permissions in the Microsoft 365 Defender portal.

Custom role access is a new capability in Microsoft 365 Defender and allows you to manage access to specific data, tasks, and capabilities in Microsoft 365 Defender. Custom roles offer more control than global Azure AD roles, providing users only the access they need with the least-permissive roles necessary. Custom roles can be created in addition to global Azure AD roles. Please visit Microsoft for support on custom roles Custom roles for role-based access control | Microsoft Docs
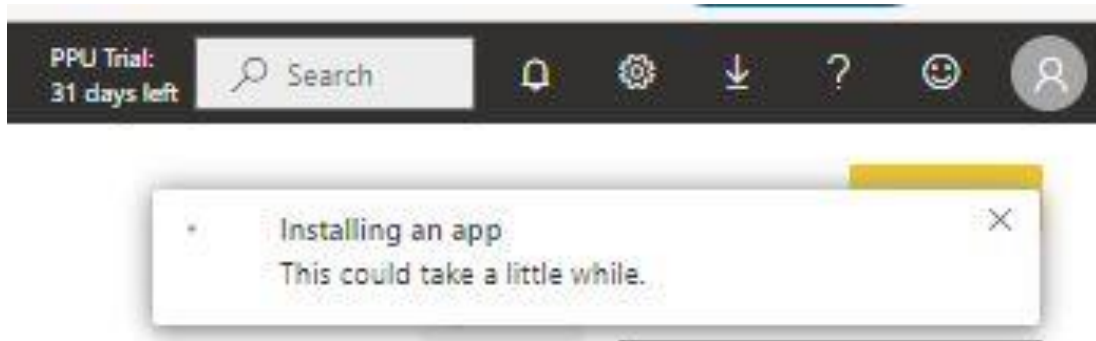
PowerBi App

PowerBi Installation
Once you have received the link to install the PowerBi App you will be prompted to install.
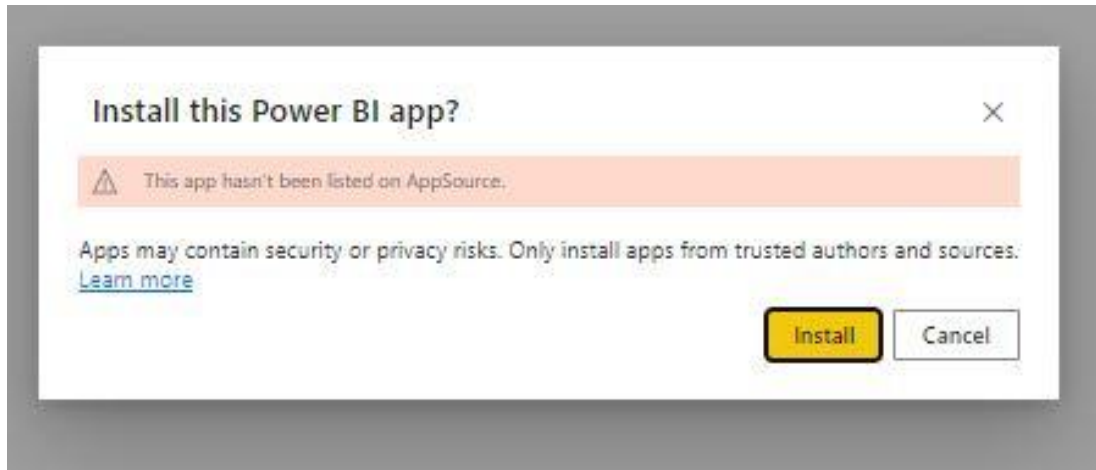
Press Install

Once pressed you will see the following on the top right of PowerBi

DSPT View Template App
One the app has completed installing your screen will refresh with the below presented

Click on DSPT® View Template

DSPT View® Report

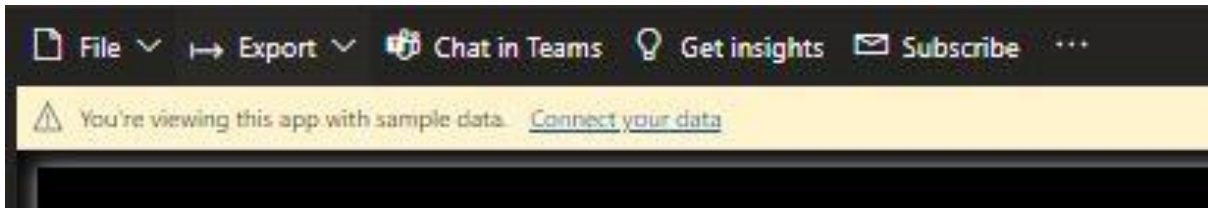Once you have clicked on the template PowerBi will display the following
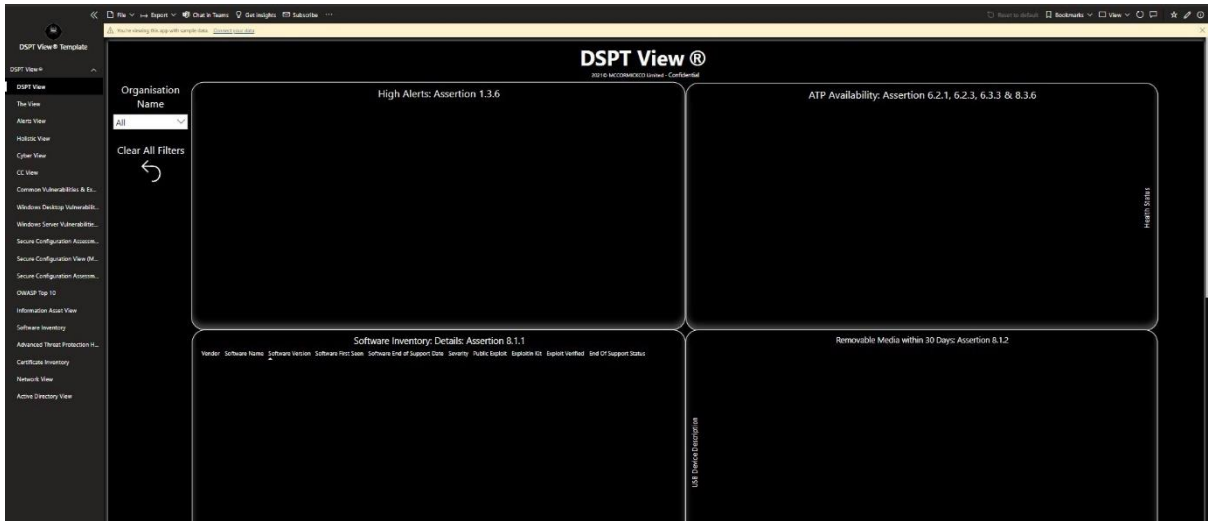
Note: The report is blank as no API feeds have been connected.

On the upper top left click on "Connect your Data" as shown below.

Connect DSPT View®

When you have clicked on "connect your data" you will be present with the following:

To allow data to connect to the template you must change the following parameters:

Under partial select "TRUE" and click on next.

Note: Under advanced the data is set to automatically refresh at midnight

Authentication Method

DSPT View® currently uses 12 different API feeds, each feed needs to be connected too to establish the overall data flow. Each API must be connected for the tool to perform correctly.

List of API Sources:

Web

https://digital.nhs.uk/restapi/CyberAlert

Authentication Method:
Anonymous

Privacy Level:
Public

https://services.nvd.nist.gov/rest

Authentication Method:
Anonymous

Privacy Level:
Public

OData

https://api.securitycenter.microsoft.com/api

Authentication Method:
OAuth2

Privacy Level:
Organisational

You will need to sign in and continue to each API, please ensure that the URL matches
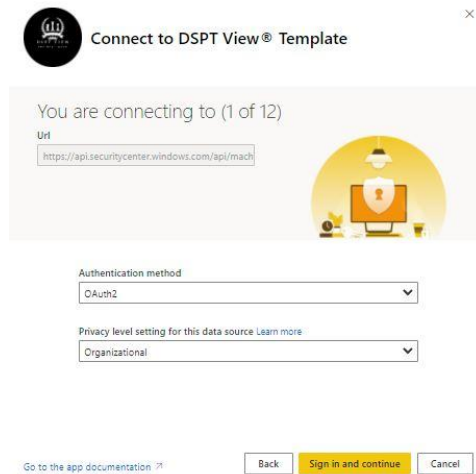
The below is an example of your login account that needs to be selected, if MFA has been enabled you will receive an additional window asking you to authenticate against a onetime pass code.

Note: We recommend that your account has multi-factor authentication as this has access to sensitive data.

Once all of the credentials have been entered you will be returned to DSPT View® in which the data will start to refresh

Note: depending on the size of your organisation the refresh can take between 1 to 10 hours.

Once the refresh has been completed the reports will populate with the pre-defined reports.

DSPT View® Menu

The navigation of tool can be seen on the left-hand side of the current published reports:
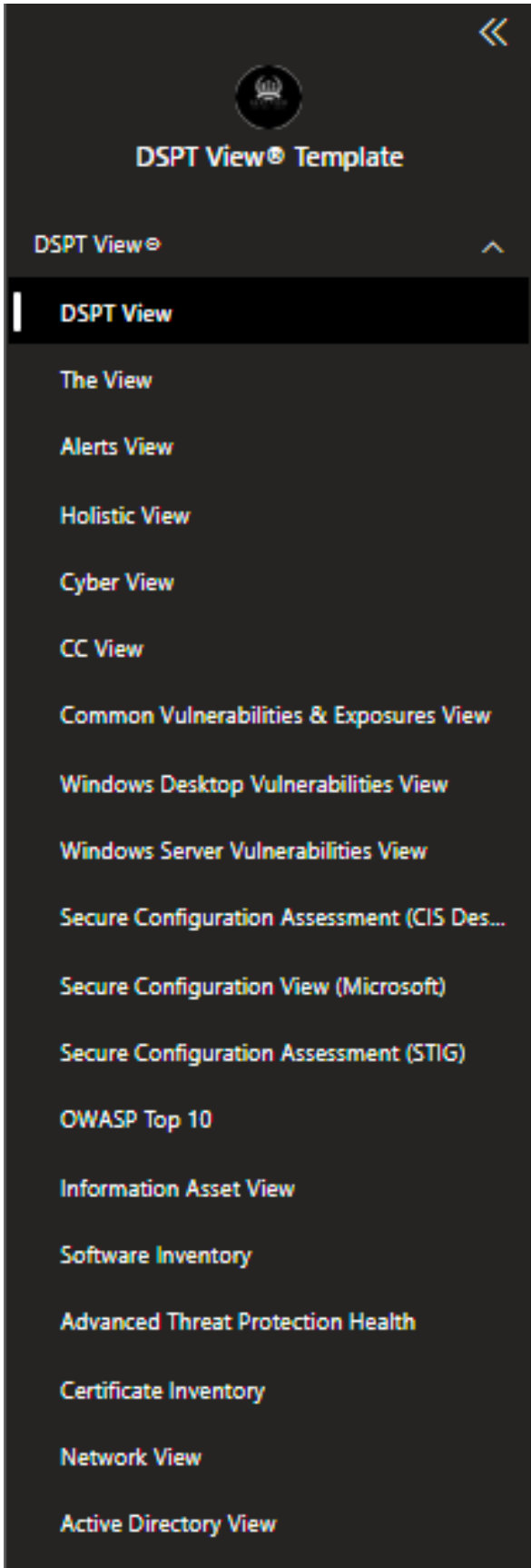
Menu Item	Description
DSPT View® Template	
DSPT View®	
DSPT View	DSPT View, near real time view of your organisations Data Security Protection Toolkit. Aligned to version 4.0.
The View	Organisations key performance risk scores
Alerts View	A timeline of all your Microsoft 365 alerts
Holistic View	Recommended security controls
Cyber View	Aligned to the NCSC for Cyber Essentials
CC View	Aligned to NHS Digitals CareCert feed
Common Vulnerabilities & Exposures View	Your exposure against publicly known information security vulnerabilities
Windows Desktop Vulnerabilities View	Exposer of your end user assets
Windows Server Vulnerabilities View	Exposer of your infrastructure assets
Secure Configuration Assessment (CIS Des...	87 mapped controls against center for internet security (CIS)
Secure Configuration View (Microsoft)	43 mapped controls against Microsoft best practice
Secure Configuration Assessment (STIG)	70 mapped controls against security technical implementation guide
OWASP Top 10	9 out of 10 mapped CWEs against OWASP
Information Asset View	Key named assets allowing your IAOs to understand risk
Software Inventory	Full software inventory of your assets
Advanced Threat Protection Health	Reporting fully on your 10 components of Defender health
Certificate Inventory	All of your asset's certificates
Network View	Details of your asserts network activities
Active Directory View	Details on your active directory activities

Knowledge Base

Failure to install the PowerBI App

When trying to install or access the PowerBi App you receive the following error message:
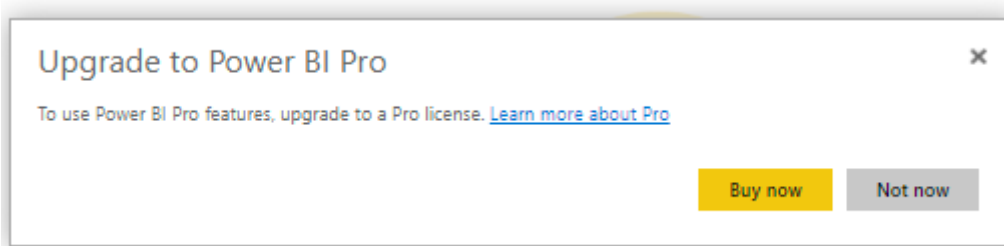
Recommendation: speak to your IT administrator to ensure that a PowerBI Pro licence has been allocated to this account. PowerBi Free will not support this app,

Blank Visualisation

The APIs we use are based on Microsoft best practice, there are only two reasons to see this

- There is no data for the API to download and build the report.
- Your tenant administrator has disallowed access or created additional permissions.

If you are unsure please contact our support team and we will happily investigate and provide guidance.

Example of blank report:
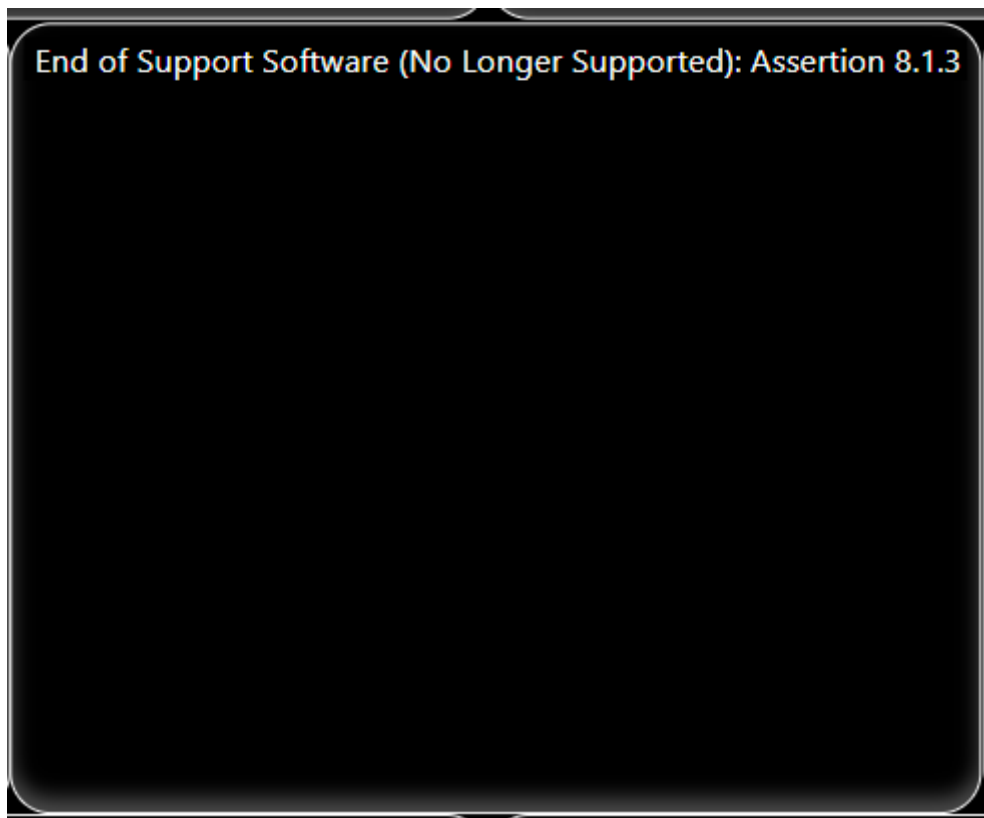
Automatic Refresh Failed

It is possible for the daily refresh to fail, if this does occur you will see a red triangle with an

exclamation mark. ⚠

Example of failed refresh:

🗄	DSPT View® Dataset		Dataset	DSPT Development	11/25/21, 5:23:19 PM ⚠	N/A

Click on the exclamation mark to see the below window and expand the "see details" to understand the error. If you are unsure, please contact our support team.

Something went wrong   ✕

There was an error when processing the data in the dataset.

Please try again later or contact support. If you contact support, please provide these details.

See details ⌄

Get help   Close

Note: We have no access to your PowerBi environment or infrastructure, please supply our team with as much detail as possible so we can support and guide.

Security

Our tool does **not** install or launch executable code within your environment beyond the data connectivity for APIs listed within this document "Authentication Method". We do not use R Scripting or Python Scripting within DSPT View®.

PowerBi Security White paper

Our tool conforms with the security paper from Microsoft which can be found here: Power BI security white paper - Power BI | Microsoft Docs

PowerBi Visuals

We only used Power Bi certified visuals within the tool, these are complaint with the Microsoft Azure Marketplace Terms which can be found here: Marketplace Terms | Microsoft Azure