

McCormickCo Security

DSPT View[®]



What's Your Next Move?



TABLE OF CONTENTS

01 CONTENTS

02 MISSION & VISION

03 THE CHALLENGE

04 COMPLIANCE WITH DSPT VIEW® & MICROSOFT DEFENDER ENDPOINT

05 BENEFITS OF DSPT VIEW®

06 OUR DESIGN



Microsoft
Partner



SOPHOS

MISSION & VISION

WE BELIEVE HONESTY AND TRANSPARANCY ARE OF THE UPMOST IMPORTANCE WHEN DEALING WITH THE THREAT LANDSCAPE AND CYBER MATURITY

MCCORMICKCO Limited was founded in April 2021.

We have a diverse technology background spanning 20 years, with experience in both the Public and Private sectors.

Sustainable growth has enabled us to develop relationships with a number of partners and associates to afford our clients the best service offering.

We provide critical leadership and capability to enable organisations to achieve effective threat management and to strengthen cyber security postures.

Trust in technology is changing, as is the ever changing threat landscape. Organisations of all sizes, and sectors must continue to mature their cybersecurity posture. Creating the right strategy, utilising the right toolset and doing so efficiently is at our core.

THE CHALLENGE

Many businesses lack vital knowledge, leadership or strategy and are unable to invest in a full-time executive.

The threat landscape of cyber security is evolving, four in ten organisations were impacted by a breach in 2020. Most Don't know how...or when.

The Data Security and Protection Toolkit (DSPT) is the cornerstone of standards for Healthcare organisations, and their associates. It is designed to show care providers what is required of them in order to keep information safe. It is updated annually, and organisations are required to submit their online self-assessment every year.

DSPT is designed to help instill public confidence in NHS organisations by supporting their compliance with the legal and Regulatory Regulations such as the General Data Protection Regulation (GDPR), Health and Social Care Act 2012 and the Network & Information System Regulations 2018 (NIS Regulations).

DSPT is composed of 10 Data Security Standards in the following categories:

- People
- Process
- Technology

The DSPT framework is subject to on going development and comprises of 42 assertions with a total of 149 evidence objectives currently 110 are mandatory, auditors or assessors are expected to use their professional judgement and expertise when conducting an audit.

The output is assurance, at a set point in time.

We know from personal experience that Trusts 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 framework.

40% of IT Managers say that improving efficiency is on their to do list for next year (Sophos,2021)

The Data Security Protection Toolkit submission is not intended to be an exhaustive or overly prescriptive process.

Each organization must recognize that this is now an organization risk not the responsibility or accountability of the Information Technology (IT) or Digital Departments within Healthcare organisations.

Over 100 organisations did not meet the DSPT standards in 2020 to 2021, with many more 'approaching' standards.

Imagine a tool, that could, close to real time, visualize compliance, suggest remediation action, and be affordable to the sector. Imagine ready to present, fit for purpose reporting to C-Level, from people who understand the requirements best.

COMPLIANCE WITH DSPT VIEW[®] & MICROSOFT DEFENDER ENDPOINT

A tool providing deep analysis of your server and endpoint estate scored against DSPT, for high impact and severity reports, available to both central and local deployments of Defender for Endpoint.

DSPT View is designed to reduce the burden on an organisation's resources. We know that DSPT submissions are mandatory and will continue to be so whilst the threat horizon continues to evolve. By improving real time transparency between auditors, c-level and digital technology teams, we can foster a culture of increased cyber security awareness, increase funding opportunities for digital technology teams, and enable a culture of shared cyber threat responsibility and increased compliance.

DSPT View displays easy to interpret data, with the ability to drill down through visualisations to understand issues and see recommended remediation steps. It aligns to the evidence objectives of DSPT, providing the evidence required for submissions for many of those objectives.

As a near-to-real-time tool, it can be used by auditors, trusts, and associated organisations to ensure continued compliance with DSPT,

eradicating the annual race to comply and reducing the burden on staff to hunt for issues and threats.

DSPT View includes a holistic view which can be customised to organizational requirements, Risk exposure scores, displays asset vulnerabilities, collates your software inventory and pinpoints devices running end of life (EOL) or windows operating systems within hours.

DSPT View improves economic efficiency, whilst helping those responsible know their next steps in Cyber Maturity.

For those without the resource or capability to carry out their own remediation, DSPTViewaaS is available. Using our inhouse experts we can provide further guidance or carry out remediations as per your requirements to ensure continued compliance, even as the yearly standards evolve.

BENEFITS OF DSPT VIEW®

Our tool consists of:

Software as a Service (SaaS): Zero impact on current on-premise infrastructure. Cloud native design.

DSPT View: Near real time view of Data Security Protection Toolkit

The View: Organisation key performance risk scores

Alerts View: A timeline of all of your Defender Alerts

Holistic View: Recommended security controls to strengthen your foundations.

Cyber View: Aligned to the NCSC for Cyber Essentials.

CC View: Aligned to the NHS Digital CareCerts

Windows and Server Vulnerabilities View: Insight into your assets

Secure Configuration Assessment (Critical Security Controls - CIS)

Secure Configuration View (Microsoft)

Secure Configuration Assessment (Security Technical Implementation Guides - STIG)

Information Asset View: Know your key Information Asset's weaknesses and vulnerabilities.

Software Inventory: Your installed software, end of support and end of lifecycles.

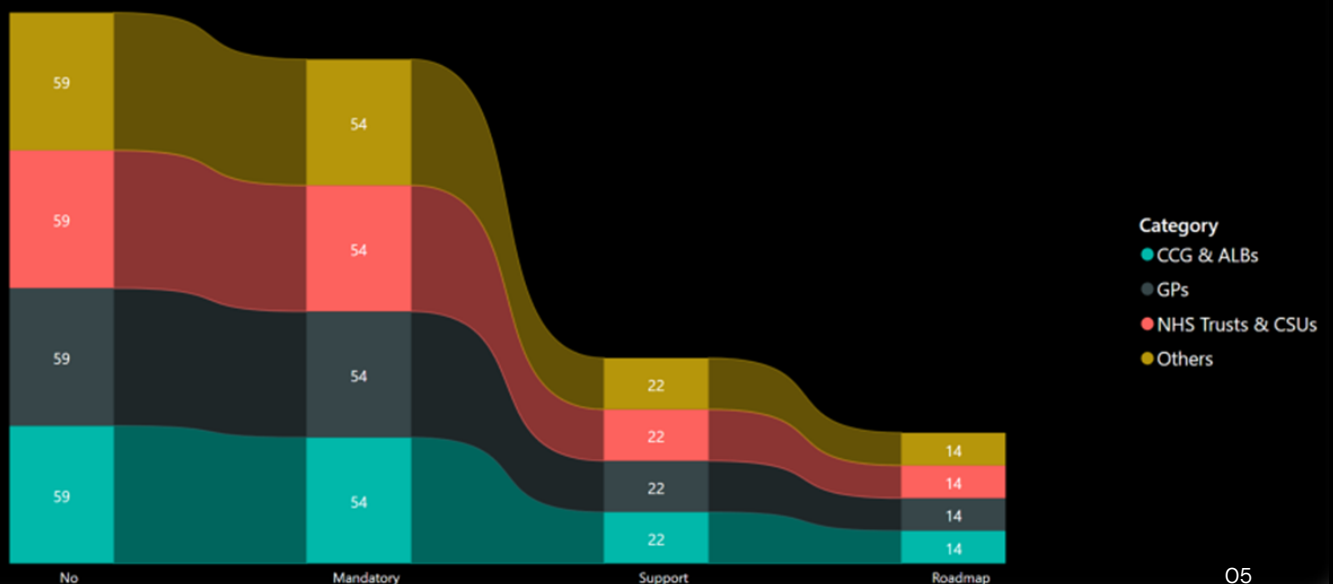
Common Vulnerabilities & Exposure View: All your asset's common vulnerabilities.

Advanced Threat Protection Health: Your agent health on your assets

From the 149 assertions within the toolkit, our on-premise tool we are able to provide evidence for **54 mandatory** and support an additional **22 non-mandatory** (76 total) with a further 14 currently in our roadmaps for 2022 - 2023.

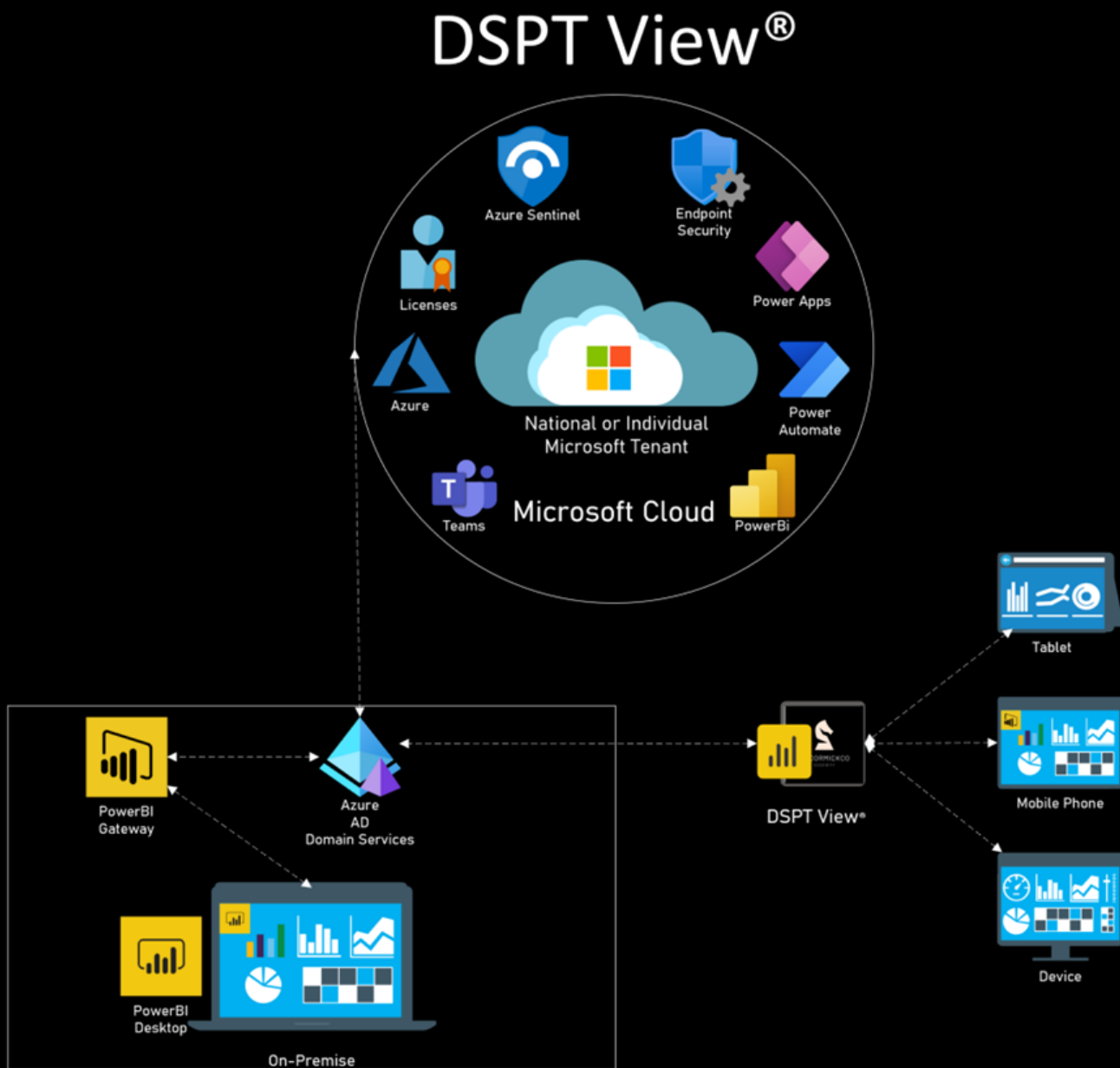
We have now introduced DSPTViewSaaS which can currently provide evidence for **42 mandatory** and support an additional **9 non-mandatory** (51 total) with a further 9 currently in our roadmaps for 2022 - 2023.

DSPT View: Assertions



OUR DESIGN

We use Microsoft Defender and Power Bi to provide insight into your vulnerabilities and risks.



Native to Microsoft PowerBi.

Software as a Service (SaaS)

DSPT View integrates to the National (NHS) or Individual Tenant.

API data is close to real time (Daily Refresh)

Minimum Infrastructure Requirement (On- Premise or Azure Based)

Minimum License Requirements (Server and PowerBi Pro and PowerBi Free)

Can Integrate with Microsoft Sentinel, Power Apps, Automate and Teams.

DSPT View can be accessed from any platform.

www.mccormickcosecurity.co.uk/dsptview
info@mccormickco.co.uk
+44 7579 003 088

MCCORMICKCO Limited
319 Hersham Road,
Hersham,
Walton on Thames,
Surrey
KT12 5QA

