Microsoft Office 365 is an increasingly popular platform for UK public sector organisations looking to modernise with cloud services. This White Paper looks at what is driving organisations to enhance this environment with additional security layers, sandboxing for zero-day malware and advanced compliance controls.
Introduction

Global government CIOs questioned by Gartner in 2016 claimed that within the following five years 80% of government business processes will have undergone significant digital transformation. Microsoft Office 365 is an increasingly popular platform for UK public sector organisations looking to drive such projects via cloud-based services. But security and compliance remain major barriers to adoption for public sector IT buyers.

Here we set out to shed more light on Office 365 security: where Microsoft helps out, useful guidance from the National Cyber Security Centre (NCSC), and where third-party experts like Trend Micro can be brought in to enhance protection.

Driving transformation

Cost reduction is frequently cited as the main reason for moving to Office 365 – and with good reason - but there are many more. Trend Micro research highlights them below.

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduce the cost of delivering services</td>
<td>50%</td>
</tr>
<tr>
<td>Enable agility in a changing operating environment</td>
<td>47%</td>
</tr>
<tr>
<td>Drive user productivity</td>
<td>42%</td>
</tr>
<tr>
<td>Gain certainty over costs</td>
<td>39%</td>
</tr>
<tr>
<td>Streamline IT operations</td>
<td>38%</td>
</tr>
<tr>
<td>Improve organizational communication</td>
<td>36%</td>
</tr>
</tbody>
</table>

NCSC guidance

The NCSC is an advocate of Office 365 and has released several guidance documents designed to help government organisations implement the cloud-based service securely.

- Its 2018 Office 365 security review is available here.
- Its best practice guidance for IT administrators is available here.
- Its detailed guidance for Office 365 email protection is available here.

The NCSC has also been instrumental in helping to improve cybersecurity for government organisations and the wider public, via an Active Cyber Defence programme that has done a great deal to help prevent phishing, spam, malicious emails, DNS threats and much more. These initiatives are to be applauded in improving public sector security across the board. However, the cyber-threat landscape is an ever-evolving global phenomenon: that makes it important for IT bosses to ensure they have a trusted cybersecurity partner with trans-national reach to enhance whatever security is already in place.
Compliance and security gaps
Microsoft has built security into all aspects of Office 365. However, there are also areas where IT managers may feel they need extra assurance to mitigate the growing risk to data and system integrity. Here’s a quick run down of where you’re covered and where there are potential gaps:

— Email Security
Office 365 offers email security in the form of Exchange Online Protection, with anti-virus, anti-malware, and anti-spam capabilities. However, each organisation must consider whether that is enough. Many email security vendors offer a dual-layered cloud and on premises security approach, allowing organisations to leverage their email security investment while migrating to Office 365. These complementary solutions often provide a focus on mitigating advanced threats, such as targeted phishing and advanced malware, further strengthening overall protection.

— Compliance
Microsoft has implemented various compliance features into Office 365, including HIPAA Business Associate Agreements, EU Safe Harbour, Model Clauses, FISMA Authority to Operate, and PCI DSS Level One. Some compliance capabilities are not available in Office 365, however, and organisations may need to look elsewhere if they require guaranteed data retention or granular policies.

— Archiving
Many archiving vendors offer complementary capabilities to Office 365, so that organisations can continue to use proven archiving tools and approaches after migrating to Office 365.

— eDiscovery
Office 365 includes some eDiscovery capabilities, but they are limited.

— Disaster Recovery
Office 365 has been architected to deliver a highly available set of services. But it is still prone to failure, and the Exchange Online outages of 2014 and earlier ring the warning siren. Since email is mission-critical to almost every organisation, increasing the disaster recovery capabilities to ensure email service continuity is a worthwhile investment.

— Backup
Microsoft will back-up all content in Office 365, but decision makers may decide to keep a separate copy as part of good IT governance processes and peace of mind. This may require a hybrid deployment of on-premise and Office 365, or the use of a third-party cloud-based archiving service.

Why Trend Micro for Office 365
Countless UK organisations have contacted Trend Micro to see what options are available to enhance existing security in Microsoft® Office 365™. Office 365 protection is good but it only filters known threats, even though 90 percent of today’s malware is unknown to traditional antivirus techniques.

Trend Micro™ Cloud App Security™ provides state-of-the-art threat and data protection for Office 365 and cloud sharing environments, including email, SharePoint and OneDrive. It offers pre-execution machine learning, document exploit detection and behaviour analysis to spot ransomware, Business Email Compromise (BEC) and other advanced threats.

Over the past 2 years, Trend Micro Cloud App Security has stopped 6 Million high-risk threats that weren’t spotted by Microsoft

The platform has built in Data Loss Prevention (DLP) capability for Microsoft® OneDrive®, SharePoint® Online, Dropbox, Box, and Google Drive, and stops malware from spreading through cloud file-sharing services. Cloud App Security is powered by the Smart Protection Network: Trend Micro’s industry-leading cloud intelligence tool that helps to spot and block malicious URLs and email attachments, preventing damaging phishing attacks. Intelligence is shared with other Trend Micro products across the endpoint, network, gateway and datacentre to improve resilience and optimise protection.
Up-to-the-second threat intelligence

The Trend Micro Smart Protection Network delivers proactive global threat intelligence against zero-hour threats to ensure that you are always protected. We use our up-to-the-second threat intelligence to immediately stamp out attacks before they can harm you.

Every day in the Smart Protection Network:

| 2.8+       | 45+      |
| terabytes of data is processed | billion URLs, emails and files are checked |
|Billions of threats are blocked | 100+ million users are connected |

Cloud App Security delivers cloud-to-cloud integration, using APIs to ensure maximum protection with minimum hassle, installation or loss of functionality.

Expert protection for Microsoft systems: Trend Micro has been a Microsoft Gold Partner for 20 years and brings extensive experience in protecting on-premises email and collaboration systems to the cloud.

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

© 2018 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and Smart Protection Network are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [WPXX_templates_180130]