UNCOVERING BLIND SPOTS

To create a truly agile and secure Office 365 (O365) environment, it's crucial to understand where this suite can enhance organisational performance and where, without a complementary third-party solution, it can leave organisations vulnerable to attacks, outages, data sprawl and data loss,

with a less than enjoyable user experience.

USER EXPERIENCE

STRENGTHS:

Tools like SharePoint, Teams and OneDrive enable collaboration, driving efficiency.



Employees can easily access files in the Microsoft cloud, from any location.



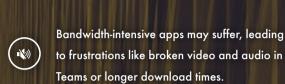
O365 features are built for use on a range of devices, with dedicated mobile apps.



BLIND SPOTS:

O365 requires multiple, persistent connections that can stress traditional infrastructure, including firewalls and proxies.





BLIND SPOTS:

CYBER SECURITY

STRENGTHS:

Exchange Online Protection (EOP) protects against traditional email attacks such as large-scale spam runs.

Advanced Threat Protection (ATP) adds Safe



Attachments and Safe Links to block malicious files and links (with some limitations).



mostly automated.

Security updates are



zero-day attacks and sophisticated, highly-targeted threats such as CEO fraud/impersonation. Phishing catch rates are significantly lower

Limited protection against



reducing protection against multi and cross-channel attacks.

COMPLIANCE

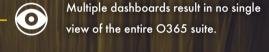
STRENGTHS:

into user interaction with apps and data.

Multiple 'Security Centres' provide insight



BLIND SPOTS:



SIM/SEM integration is



needed for full visibility and a comprehensive audit trail across all admin and user activity.

STRENGTHS:

AVAILABILIT

Component services in O365

are highly distributed to

event of a failure.

limit the impact of downtime. O365 internal monitoring services

drive automated recovery in the



Microsoft's uptime SLA of 99.9% allows for

BLIND SPOTS:

8 hours, 45 minutes and 57 seconds of downtime each year.

Limited protection from outages without

third-party non-Microsoft services on a



separate infrastructure. Azure AD outages can have a significant impact on user and admin access to



applications and resources. **DATA SECURITY**

STRENGTHS: BLIND SPOTS:

Organisational data is secured at rest in Microsoft's data centres.

Azure Information Protection (AIP)



DLP policies offer only partial coverage of O365 workloads.

makes data classification and Digital

Rights Management (DRM) more accessible than ever before.

STRENGTHS:



potential data loss through malicious or unintentional sharing - using multiple apps.



Limited content scanning leads to

(with careful planning).

informal, unstructured data.

Tools like OneNote can help organise

and store documents centrally

SharePoint and OneDrive organise



regions or groups. Data sprawl across O365 gives users

BLIND SPOTS:



80-90% of data in O365 is unstructured, moving the problem to the cloud.

unauthorised access to data through

multiple applications, with opportunities to inadvertently share data externally.

DLP policies aren't automatically enabled

and can't be easily assigned to individual



Whilst O365 does offer default basic security configurations, it cannot protect you from

sophisticated cyber threats and outages. To combat these threats, remain compliant and maintain optimum user performance, additional third-party security is crucial.

DEFENCE[§]

Office 365 protection

Uncompromising

and performance.

For organisations that won't accept less than complete protection, always-on availability and superior user experiences, Censornet's integrated cloud platform offers the streamlined, secure O365 environment you need. To find out more, visit:

www.censornet.com

censornet.