censornet.

UNCOVERING MICROSOFT 365'S BLIND SPOTS

To create a truly agile and secure Microsoft 365 (M365) 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.

M365 features are built for use on a range of devices, with dedicated mobile apps.

BLIND SPOTS:

M365 requires multiple, persistent connections that can stress traditional infrastructure, including firewalls and proxies.

Microsoft advises using direct-to-internet connections, bypassing proxies and security controls entirely.

Bandwidth-intensive apps may suffer, leading to frustrations like broken video and audio in Teams or longer download times.

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).

Security updates are mostly automated.

BLIND SPOTS:

Limited protection against zero-day attacks and sophisticated, highly-targeted threats such as CEO fraud/impersonation.

Phishing catch rates are significantly lower than with specialist third-party security solutions.

M365 does not include web security, reducing protection against multi and cross-channel attacks.

COMPLIANCE

STRENGTHS:

Multiple 'Security Centres' provide insight into user interaction with apps and data.

BLIND SPOTS:

Multiple dashboards result in no single view of the entire M365 suite.

SIM/SEM integration is needed for full visibility and a comprehensive audit trail across all admin and user activity.

AVAILABILITY

STRENGTHS:

Component services in M365 are highly distributed to limit the impact of downtime.

M365 internal monitoring services drive automated recovery in the event of a failure.

BLIND SPOTS:

8HRS 45MIN 57SEC

Microsoft's uptime SLA of 99.9% allows for 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:

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

Azure Information Protection (AIP) makes data classification and Digital Rights Management (DRM) more accessible than ever before.

BLIND SPOTS:

DLP policies offer only partial coverage of M365 workloads.

Limited content scanning leads to potential data loss through malicious or unintentional sharing - using multiple apps.

DATA MANAGEMENT

STRENGTHS:

SharePoint and OneDrive organise and store documents centrally (with careful planning).

Tools like OneNote can help organise informal, unstructured data.

BLIND SPOTS:

DLP policies aren't automatically enabled and can't be easily assigned to individual regions or groups.

Data sprawl across M365 gives users unauthorised access to data through multiple applications, with opportunities to inadvertently share data externally.

80–90% of data in M365 is unstructured, moving the problem to the cloud.

Whilst M365 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.

SECURING 365

Uncompromising M365 protection 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 Microsoft 365 environment you need. To find out more, visit:

censornet.

www.censornet.com