wanstor

Microsoft 365 Optimisation

Service Description

EXECUTIVE SUMMARY

Microsoft 365 is a cloud-based service that brings together Office 365 but with advanced device management features, intelligent security, and innovative online services. Microsoft 365 helps drive productivity, collaboration, and communication securely across many devices.

While customers often right size the migration to Microsoft 365 initially, and ensure the correct licensing, features, and security measures are implemented, over time customer requirements change, gaps emerge between what companies would like to have in place vs what they currently have, and changes to licensing and features are not realised.

If left unoptimized, customer environments often face the following risks:

Licensing risks: Licensing becomes difficult to manage when factoring in employee turnover, ongoing licensing management, new license bundle releases and not reviewed, customer innovation changing licensing requirements, duplication of features doubling licensing costs.

Administrative risks: administration of users, groups, and privileged accounts not optimally managed leading to increased license usage for inactive users, unused groups (some with privileged access) and privileged account sprawl increasing risk to the business.

Security risks: Gaps emerge in security and not governed correctly including a mixed user creation process, degraded enforcement of security features such as MFA, or conditional access policies, weak and non-expiring passwords, and lack of monitored and reviewed privileged security groups.

Mailbox risks: Mailbox estate is not always clear, and lead to risks such as mailbox size growth trends not tracked hitting hard limits, lack of backups for mailbox data, connection using unsecure protocols (automated or manual), lack of insight into deprecated or soon to be deprecated authentication.

OneDrive, SharePoint, and Teams governance: The introduction of these collaboration tools have allowed teams flexibility to create sites, channels, teams on the fly, which quickly spirals out of control, naming conventions are not adhered to (if any), initial policies, roles and responsibilities have stagnated, implemented controls have not been reviewed since initial implementation, guest access and external sharing policies might no longer be understood and overall governance might no longer be in line with company goals.

Intune and Autopilot: As companies move to modern provisioning and management, left un-checked, un-managed or orphaned devices are never cleared, new devices are not associated to autopilot, baselines fall out of date, conditional access policies might not be configured correctly, key configuration such as disk encryption, attack surface reduction or endpoint detection and response policies are not implemented, policies covering BYOD or corporate devices might not be implemented.

Service Outline

Wanstor's M365 optimisation service provides a detailed snapshot of your current environment, including a review of your tenant's current configuration, and a complete fully documented report detailing core information to help your organisation make informed decisions, understand current risks, and provide recommendations to remediate these.

Optimisation consultancy

As part of the consultancy, Wanstor will assign a cloud engineer to undertake the assessment, and during the engagement Wanstor will:

Configure the environment – Deploy the required custom tools and any other access configuration needed to fully assess your entire Microsoft 365 subscription, this step ensures our engineer has all the required access to generate and obtain the required data for analysis.

Generate and collect data – Engineer runs Wanstor's custom tooling across the Microsoft 365 subscription, collecting all the data required for analysis, data is then checked to ensure we have enough information to create our end reports. In some cases, data takes time to compile, and the engineer might need to revisit the tooling to retrieve any remaining data.

Collect further data – Certain parts of Microsoft 365 cannot be collected using custom tooling, and our engineer will collect the information manually to ensure we have a full picture of your environment for reporting purposes.

Review and create the optimisation report – Wanstor's engineer will review the data collected and build the optimisation report, this includes useful data that will allow further insights into your environment, detail risks found, and recommendations based on these risks which improve your cost, security, governance, and overall Microsoft 365 environment.

A typical optimisation report consists of the following:

- **Licencing and cost recommendations** – A full review of your:
  - Current licensing assignments, products, and feature usage with current user adoption including licenses that are left unassigned.
  - Reporting for active users without any licensing assignments
  - Reporting for your current process for applying licenses to users identifying any recommendations for improving the process.
  - Identify and reporting unused, active, inactive, abandoned, and underutilised user licenses in your subscription.
  - A review and comparison of your current licensing SKUs against all Microsoft licensing bundles to identify cost reductions, recommendations, and optimisation opportunities.

- **User, Group and Privileged Account review and recommendations** – a full review and report of:
  - Current users including active users that have not logged in for a long duration, disabled users, users with errors and any recommendations around user accounts.
  - All external users, internal guest users and groups with external users.
  - A list of cloud-only and guest accounts within your tenant.
  - A list of groups that can potentially be removed including empty, mail-enabled, nested, security, cloud only, distribution groups and groups with RBAC roles associated to them.
  - Administrative account review that will show you a list of all accounts that have administrative access over parts of your M365 tenant

- **General security review with recommendations** – review of security recommendations across the subscription including:
  - Users without MFA (Multi-Factor Authentication) enforced or enabled.
  - Users with MFA that have not yet been activated.
  - Users with:
    - Expired passwords
    - Passwords that never expire
    - Passwords that have never been changed
    - Passwords that have not changed within 90 days
  - Users with weak passwords allowed, with a review of password policies.
  - Administrator accounts without MFA (Multi-Factor Authentication)
  - Review of your current conditional access policies vs Wanstor's baseline policies.
  - Report of all external users including groups with external users
  - Report on confirmed risky sign-ins with a list of currently open risky sign-ins.
  - Report of users with MFA not configured to best practice.
  - Report of non-interactive sign-ins and un-managed device sign-ins.

- **Mailbox and office configuration reporting and recommendations** – Mailbox reporting covers:
  - Active mailboxes vs inactive mailboxes over the last 60 days.
  - List of mailboxes that have never been used
  - A report of mailbox users approaching their mailbox usage limit.
  - List of shared mailboxes, mailboxes with litigation hold, in-place host or retention hold enabled.
  - Mailbox App usage including SMTP, POP, IMAP, and other app usage.
  - Reporting on delegated permissions, full access permissions and send-as permissions.
  - Mailbox forwarding summary.
  - Quota and Size comparison including mailboxes over quota warning.
  - Office 365 service configuration checks, including mail flow protection settings.
  - A review of standards such as DMARC, SPF, connection filters and DKIM configuration for up to 5 primary email domains.

- **Teams, SharePoint and OneDrive reporting and recommendations** – covering:
  - Reports detailing active, and inactive sites, teams, sites with teams, OneDrive, with usage analysis.
  - External user sharing, guests, and disabled users with access across OneDrive, Teams, and SharePoint.
  - List of document libraries including details on empty or hidden libraries and versioning status.
  - Team statistics, including public and private teams, teams with guests, storage usage per team, empty teams.
  - Anonymous links, External guest link usage reporting.
  - Overall Storage for OneDrive, SharePoint, and Teams usage.
  - Details of current naming conventions.

- **Intune and Autopilot reporting and recommendations** – including:
  - Detailed report on current devices, including inactive, orphaned, un-managed and corporate devices not linked to Autopilot.
  - Review of Intune and Autopilot configuration against Wanstor recommended baseline configuration including a review of current device security baselines.
  - Conditional access configuration and review against Wanstor's recommended baseline configuration.

- Review of expected protection configuration including disk encryption standards, endpoint detection and response configuration, antivirus policies and other policies configured.
- Review of Corporate configuration, BYOD configuration and Mobile configuration against Wanstor's baseline configuration.

Run an on-site or remote workshop – Once all the required data has been reviewed, Wanstor will produce a final report in the form of a presentation accompanied by a detailed appendix, Wanstor will book in either an on-site or remote workshop to go through the findings and discuss recommendations.

The workshop is an opportunity for the customer to ask questions around best practice or understand any areas around Microsoft 365 that the customer might be interested in better understanding.

Clean up the environment – Once Wanstor has completed the collection of data required for the reporting, the engineer will remove any application registrations, and revert any changes that might have been made during the optimisation consultancy.

Assumptions, Dependencies and Constraints

1. To ensure we have the required access to complete our optimisation service, Wanstor will provide you with a form that needs to be filled out by your Microsoft 365 or IT team. This form includes information about the required access to your subscriptions and information about application registrations for our custom tooling.
2. Where required, Wanstor's tooling will require write or full access to the systems where the permissions are limited to these access rights. To complete a full analysis, these permissions will need to be granted.
3. Deliverables and tasks not covered in this document are excluded from this project.
4. Wanstor business hours are Monday to Friday, 8am to 6pm. Project work done outside of these periods will need advanced notice to remain on track on the project schedule.
5. Organising downtime is a customer responsibility.
6. The customer team will ensure availability of relevant and appropriate IT staff and resources for project work.
7. Solution specific details provided are correct. If the provided information is determined to be incorrect or inaccurate, the projects may be delayed.