Wipro's Unified Monitoring and Assessment

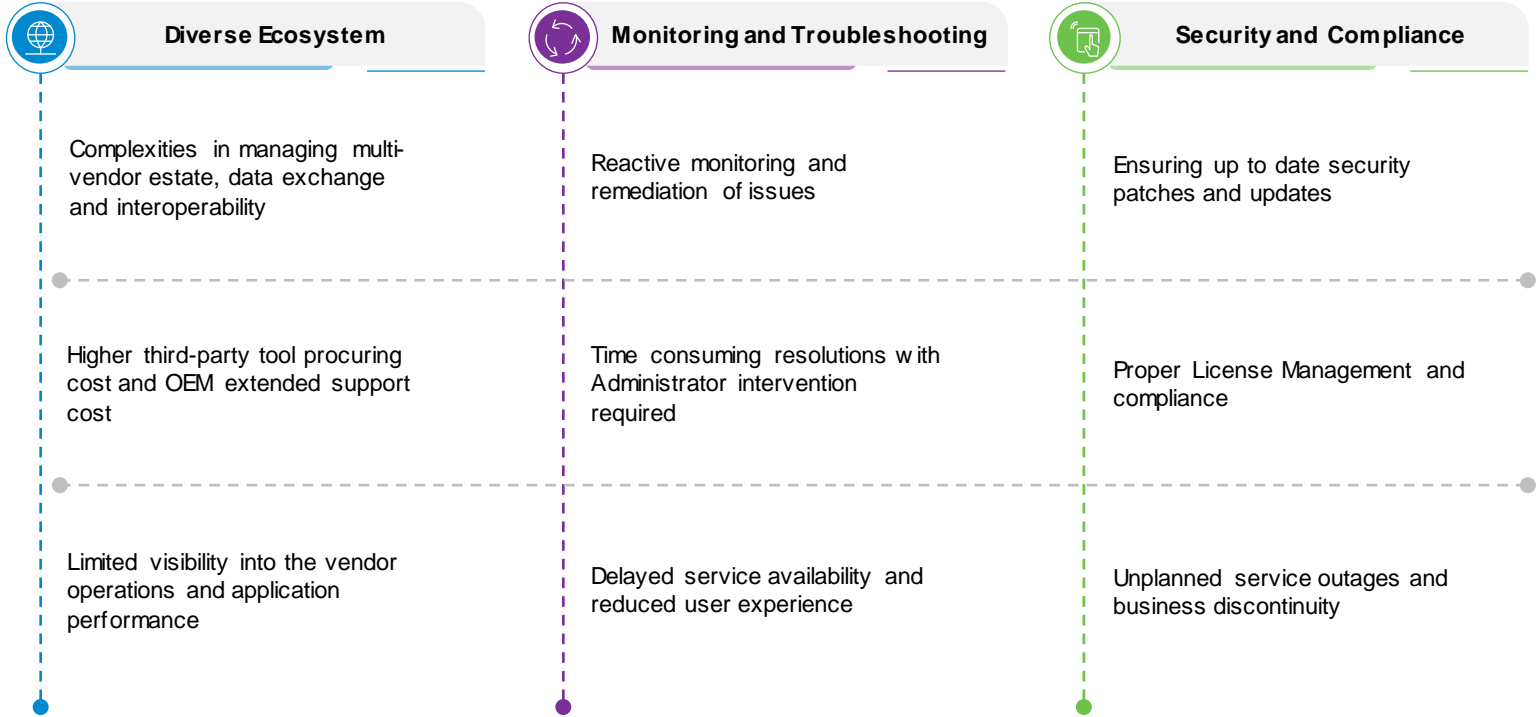**of Microsoft On-Prem and Cloud Services**

Navigating the Complexities :
Need to overcome the challenges in managing the Microsoft environment

Key Challenges

Ensuring effective management of the Microsoft environment is critical to deliver positive employee experiences and improve productivity

Diverse Ecosystem	Monitoring and Troubleshooting	Security and Compliance
Complexities in managing multi-vendor estate, data exchange and interoperability	Reactive monitoring and remediation of issues	Ensuring up to date security patches and updates
Higher third-party tool procuring cost and OEM extended support cost	Time consuming resolutions with Administrator intervention required	Proper License Management and compliance
Limited visibility into the vendor operations and application performance	Delayed service availability and reduced user experience	Unplanned service outages and business discontinuity

Proactive Monitoring and Assessment
Microsoft On-Prem and Cloud Services

Data-driven Analytics Platform to monitor critical services

from a single location, simplifying the assessment process, enabling transparency and improving productivity

Active Directory Assessment
- Automated Data Collection of Active Directory Infrastructure & Generating automated compliance reports

Exchange Online Assessment
- Actionable guidance grouped in Focus Areas to mitigate the risks of Exchange Online Tenant

Exchange On-Prem Assessment
- On-demand assessment for proactive diagnoses of future risks and concerns related to Technology (Design, Architecture, Best Practice, Capacity, and Performance)

M365 Health Monitoring
- Ensure service availability, manage service outages & performance, maintain compliance, and improve the user experience

■ Office 365 Cloud   ■ On Premises

Assessment Focus Areas

Security and Compliance	Business/IT Alignment	Availability and Business Continuity
Performance and Scalability	Operations and Monitoring	Change and Configuration Management

Exchange

Microsoft Teams

Microsoft Exchange Server

Active Directory

Wipro ensures comprehensive capturing of Telemetry data to unlock insights for optimized performance

| Requirement Study and Situation Analysis | → | Establish Approach and Requirements | → | Data Collection and Analysis | → | Risks and Gap Identification | → | Reporting and Briefing | → | Suggest Improvement, Track and Closure |

Automated Monitoring and Analysis

- Automation of Manual Tasks - Data Capturing, Analysis and Remediation
- Real-time monitoring to quickly identify and resolve issues as they arise which improves overall service quality
- Historical Analysis to identify trends and patterns that can help with capacity planning and ticket resolution

ROI Enhancement

Risk Identification and Mitigation

- Conducting audits, risk identification related to security & compliance, operations, performance and scalability
- Identification of single point of failures and recommendations
- Auto generate and execute a remedy plan for noncompliant parameter
- Best practices recommendation

Cost Optimisation

Unified Performance and Compliance View

- Single pane of glass view of infrastructure to the administrator
- Allow enhancement of performance, optimization of operations and security upgradation along with better monitoring
- Avoid potential major incidents by proactively modifying critical situations

Reduction in Service Downtime

Customized Reporting Dashboards

- Automated Analysis/Compliance Report generation based on pre-defined solutions
- Help admin filter reports based on various search options
- Service Dashboards, to ensure correct functioning and manage service performance & maintain compliances

Enhance Stability and Efficiency

Solution Snapshots

Exchange Online Compliance Discovery

Severity	Parameter	Status	Remarks
High	Block Basic Authentication (Basic Auth) using Exchange Online Authentication Policies	Non-Compliant	
High	Block sign-in for shared mailboxes are not enforced in Exchange Online	Non-Compliant	
High	Disable Remote PowerShell for Regular Users	Non-Compliant	
High	DKIM Signing is not enabled for the Accepted Domains	Non-Compliant	
High	Enable Admin Audit Logs	Compliant	
High	Configure Impersonation Setting in the Anti-phishing policy	Non-Compliant	
High	Verify Safe listing Sender Domains in the Anti-spam Policy	Non-Compliant	
High	Configure Spam Policies to Send Bulk Email to Junk Mail Folder	Non-Compliant	
High	Configure Spam Policies to Send High Confidence Phishing Emails to Quarantine	Non-Compliant	
High	Configure Spam Policies to Send High Confidence Spam to Quarantine	Non-Compliant	
High	Configure Spam Policies to Send Phishing Emails to Quarantine	Compliant	
High	Control email auto forwarding in the outbound spam filter policy	Compliant	
High	Disable click through for potentially malicious URLs in email messages	Non-Compliant	
High	Enable Anti Spoof Protection in the Anti Phishing Policy	Non-Compliant	
High	Enable custom domain protection in the Anti-Phishing policy	Non-Compliant	
High	Enable impersonation protection for owned domains	Non-Compliant	
High	Enable intelligence for impersonation protection in the Anti-phishing policy	Non-Compliant	
High	Enable Safety Tips for Domain Impersonation in the Anti-phishing policy	Non-Compliant	
High	Enable Safety Tips for unauthenticated senders for spoof in the Anti-phishing policy	Non-Compliant	
High	Enable safety tips for unusual characters in the Anti-phishing policy	Non-Compliant	
High	Increase the Advanced phishing threshold level in Anti-phishing policy	Non-Compliant	
High	Enable common attachment type filtering in the malware filter policy	Non-Compliant	
High	Enable Zero Hour Auto Purge in the Malware filter policy	Non-Compliant	
High	Enable Safe Links for internal email messages	Non-Compliant	
High	Set the Bulk Complaint Level to 6 in Anti-spam policy	Compliant	
High	Enable Zero Hour Auto Purge to Provide Additional Protection for Mailboxes	Non-Compliant	
High	Enable quarantine notification and set the frequency to less than or equal to 3 days	Non-Compliant	
High	Reduce the Number of high privileged accounts	Non-Compliant	
High	Enable Multi-Factor Authentication for all Exchange Online Users	Non-Compliant	
High	Inactive Office 365 users are observed in the organization	Non-Compliant	
High	Multi Factor Authentication is not enabled for Admin Accounts	Non-Compliant	

Exchange On-Prem Remediation Guide

One or more Exchange databases has not been backed up within the last 24 hours

Description: Backup and recovery procedures are an important part of overall system availability and integrity. Complete backups reduce the chance of accidental deletion of important information, and make it possible to have complete recoveries

Impact: Backup of most of the Mailbox databases are too old, also Circular logging has been enabled on these databases. Circular logging is not recommended in production environments. In this configuration Backup is out-most important to have to recover the point-in time data.

Severity: Critical

Remediation: Team need to work with Backup team for Exchange database backups.

More Info/References:

https://docs.microsoft.com/en-us/exchange/backup-restore-and-disaster-recovery-exchange-2013-help

Affected Entities: -

Backup_NonCompliance File.xlsx   ExchangeAnalyzer.html

Active Directory On-Prem Assessment

Severity	Script	Status	Object
Critical	Active Directory Backup performed regularly	Compliant	Backup
Critical	Enable Accidental deletion protection on DNS Zones	Non-Compliant	DNS
Critical	Enable Accidental deletion protection on OUs	Non-Compliant	OU
Critical	Monitoring Active Directory Replication	Compliant	Monitoring
Critical	Monitoring Domain Controller health	Non-Compliant	Monitoring
Critical	Restrict membership of Privileged groups	Non-Compliant	Security
Major	Blocking Internet Access for Domain Controllers	Compliant	Security
Major	Configure appropriate NTP settings on Domain PDC Emulator	Non-Compliant	Time
Major	Configuring Account Lockout Policy with appropriate parameters	Compliant	GPO/Security
Major	Configuring Password Policy with appropriate parameters	Non-Compliant	GPO/Security
Major	Disable anonymous Lightweight Directory Access Protocol (LDAP) binds	Non-Compliant	Security
Major	Enable AD Strict Replication Consistency on all domain controllers in the Forest	Compliant	DC
Major	Fine grained password policy	Compliant	GPO/Security
Major	Limit GPO Level Full Control or potential Full Control or Edit permission delegation	Non-Compliant	Security
Major	Limit Organizational Unit Level Full Control or potential Full Control delegation	Non-Compliant	Security
Major	Rename the Built-in Administrator account	Non-Compliant	Security
Major	Reset password of KRBTGT account	Non-Compliant	Security
Major	Secure LDAP (Ldap Over SSL) is enabled on Domain Controllers	Compliant	Security
Major	Unsecure User Account Control Flags set on user accounts	Non-Compliant	Security
Major	Migrate SYSVOL replication from FRS to DFSR	Compliant	Performance and Security
Medium	Account and Group Management housekeeping to be performed	Non-Compliant	Cleanup

M365 Health Service Monitoring

Message Center

Id	Title	Service	LastUpdatedTime	LastUpdatedDays	ActionRequiredByDateTime	ActionRequiredDays	Tags	RoadmapId	Category
MC557956	Microsoft Teams: Intelligent Meeting Recap (Premium)	Microsoft Teams	2023-04-06T00:52:01.567Z	0			New feature; Admin impact	122529	stayInformed
MC557955	Plan sharing with the container	Planner	2023-04-06T00:31:13.640Z	0			Feature update; Admin impact		stayInformed
MC557952	Microsoft Teams for Mobile: Chat Details Update	Microsoft Teams	2023-04-06T00:29:07.477Z	0			Feature update; User impact; Admin impact	114808	stayInformed
MC557415	Profanity filtering on/off control for Live Captions in Teams meetings	Microsoft Teams	2023-04-05T03:34:36.447Z	1			User impact; Admin impact	113412	stayInformed
MC557413	Teams Rooms: Windows 11 support for Teams Rooms on Windows devices	Microsoft Teams	2023-04-05T03:30:10.282Z	1			New feature; Admin impact	122148	stayInformed
MC557341	Updates available for Microsoft 365 Apps for Current Channel	Microsoft 365 apps	2023-04-05T00:26:16.793Z	1			Feature update		stayInformed
MC515528	(Updated) Microsoft Purview compliance portal: eDiscovery PowerShell cmdlet support for certificate-based	Microsoft 365 suite	2023-04-04T20:39:58.523Z	1			Updated message: New feature; Admin impact	106112	stayInformed

Current Status

ID	Service	ServiceStatus	StatusTime	Incidents
microsoftteams	Microsoft Teams	extendedRecovery	2/27/2023 5:12:15 PM	TM517049; TM511174; TM495255
OSDPPlatform	Microsoft 365 suite	serviceDegradation	2/27/2023 5:12:15 PM	MO519810
OneDriveForBusiness	OneDrive for Business	serviceDegradation	2/27/2023 5:12:15 PM	OD518715
Exchange	Exchange Online	serviceOperational	2/27/2023 5:12:15 PM	
OrgLiveID	Identity Service	serviceOperational	2/27/2023 5:12:15 PM	
Lync	Skype for Business	serviceOperational	2/27/2023 5:12:15 PM	
SharePoint	SharePoint Online	serviceOperational	2/27/2023 5:12:15 PM	
DynamicsCRM	Dynamics 365 Apps	serviceOperational	2/27/2023 5:12:15 PM	

Optimization of Exchange Online Platform to measure business efforts and enhance the customer experience

Systematizing the assessment data and account analysis through automated compliance reports

Business Requirements

- Online tenant audit to assess the configuration, topology, data, integrity, etc.
- Identify probable risks and prepare a mitigation plan
- Establish best practices to increase productivity and cost savings

Solution Overview

- An on-demand assessment was performed by the Wipro Team to gain an elaborate insight. It proactively diagnosed the future risks and concerns related to:
  - Security and compliance
  - Operations and monitoring and
  - Performance and Scalability
- The assessment was performed to understand the specific actionable guidance grouped under above mentioned focus areas to diminish the risks of the exchange online tenant

Client's Benefits

- Saved ~3 weeks efforts per Subject Matter Expert (SME) per Technology Assessment
- Saved OEM Extended support cost and cost of procuring third party tool
- Holistic recommendations that enabled the client to improve their technical capabilities
- Expert analysis and detailed solution to fix a glitch as per the priority
- Evaded potential major incidents and reduced service downtimes by proactively modifying critical situations
- Enhancement of online infrastructure services stability and operation efficiency