

<YOUR LOGO>

Managed Services Report

Auto-generated by <Your Name>

Microsoft 365 Tenant Health — PRO Report with AI Analysis

Comprehensive Security & License Report | Managed by <Your Name>

Customer: Demo Corporation Ltd.

Report Data as of: 25/06/2026

Reporting Period: Last 30 Days

This PRO report provides a comprehensive deep-dive into the security posture, license inventory, storage usage, security alerts, and AI-powered recommendations for the Microsoft 365 tenant of Demo Corporation Ltd.. It is generated by your Microsoft partner <Your Name> for detailed technical analysis and managed services review.

Security Posture

Microsoft security recommendations

51%

SECURE SCORE

489

TOTAL LICENSES

0

UNASSIGNED LICENSES

10

SECURITY ALERTS (30D)

SECURE SCORE

51%

MEDIUM RISK

Overall security health percentage.

POINTS ACHIEVED

138 / 272

Raw secure-score points out of total available.

ASSIGNED LICENSES

489

Currently active license assignments across Demo Corporation Ltd..

<YOUR LOGO>

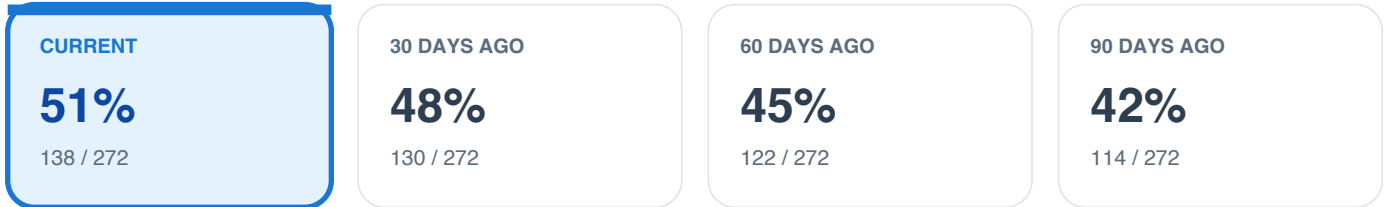
Managed Services Report

Auto-generated by <Your Name>

Secure Score Trend

Past 90 days

Tracking your organization's security posture over the past 90 days.

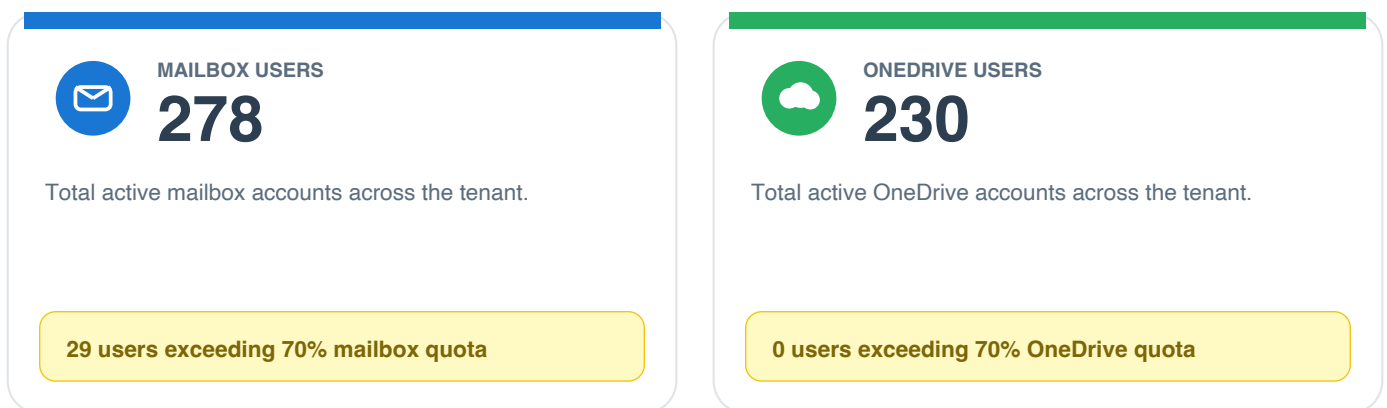


- Enable Multi-Factor Authentication**
Activate MFA for all user accounts to reduce credential compromise risk.
- Review Email Security Policies**
Audit anti-phishing and anti-spam policies in Microsoft Defender for Office 365.
- Resolve Open Security Alerts**
Investigate and close all medium/high severity alerts promptly.
- Optimize License Assignments**
Identify and reassign unused licenses; right-size SKUs to reduce cost.
- Schedule Quarterly Security Reviews**
Conduct quarterly posture reviews with your Microsoft Partner.

Storage Usage Summary

Mailbox & OneDrive

Overview of mailbox and OneDrive storage utilization for your active users.



<YOUR LOGO>

Managed Services Report

Auto-generated by <Your Name>

License Inventory Breakdown

Detailed Microsoft 365 license types currently assigned to users in your organization.

LICENSE TYPE	ASSIGNED QUANTITY
Microsoft 365 Business Premium	245
Microsoft 365 Business Standard	120
Microsoft 365 Business Basic	75
Microsoft Defender for Office 365 (Plan 1)	32
Power BI Pro	18
Visio Plan 2	6
Project Plan 3	4
Microsoft Stream	5
Power Automate Free	184

LICENSE OPTIMIZATION

All Assigned

489

TOTAL PURCHASED

489

ASSIGNED

0

UNASSIGNED

✓ Status: All purchased licenses are currently assigned to active users.

Security Alerts (Past 30 Days)

Summary of detected threats, policy violations, and automated security mitigations.

ALERT TITLE	SEVERITY	DATE
Malware Alert Policy	MEDIUM	24/06/2026
Malware Alert Policy	MEDIUM	22/06/2026
Malware Alert Policy	MEDIUM	19/06/2026
Malware Alert Policy	MEDIUM	16/06/2026
Malware Alert Policy	MEDIUM	13/06/2026
Malware Alert Policy	MEDIUM	10/06/2026
Creation of forwarding/redirect rule	INFO	21/06/2026
Creation of forwarding/redirect rule	INFO	18/06/2026
Creation of forwarding/redirect rule	INFO	14/06/2026
Unusual sign-in activity detected	INFO	11/06/2026



AI-Powered Security Analysis

Personalised analysis & recommendations powered by Xpress Manage365 Intelligence

Executive Summary

Demo Corporation Ltd. currently maintains a Microsoft Secure Score of 51%, categorized as Medium risk. While this represents reasonable baseline hygiene, there is significant headroom to strengthen the tenant's security posture. The past 30 days saw 10 security alerts — predominantly malware policy detections (6) — indicating active threat targeting that warrants attention. License utilization is strong at 100%, with no unassigned licenses to optimize.

Security Commentary

The score of 51% (140/272 points) reflects partial implementation of Microsoft's recommended security controls. Priority gaps include MFA rollout completion, Conditional Access policy hardening, and email link/attachment policy enforcement. The 6 malware alerts in 30 days indicate Defender for O365 is detecting threats, but proactive policies should be reviewed to prevent recurring exposure. 29 users currently exceed mailbox quota — this creates operational risk.

AI Recommendations

- Complete MFA enforcement across all 489 licensed users via Conditional Access — this single change typically lifts Secure Score by 8-12 points.
- Enable Safe Links and Safe Attachments in Defender for Office 365 for all mailboxes; review Anti-Phishing impersonation protection for executives.
- Investigate the 6 malware policy alerts — confirm payload type, source, and whether end-user training is needed.
- Audit the 3 mail-forwarding rule creations — these are common indicators of compromised accounts; verify with each user.
- Schedule mailbox quota review for 29 affected users; either expand storage SKU or implement archive policies.

Action Plan

- Week 1: Roll out MFA + Conditional Access baseline policy to all users (target 100% coverage).
- Week 2: Enable Safe Links / Safe Attachments / Zero-hour Auto Purge tenant-wide.
- Week 3: Investigate all 10 security alerts — close, escalate, or document false positives.
- Week 4: Review mailbox quota for 29 users; deploy In-Place Archive or quota expansion as appropriate.
- Monthly: Track Secure Score trend; target 65% within 90 days, 75% within 180 days.

Leadership Summary

Demo Corporation's Microsoft 365 environment is operationally healthy but security-wise in the middle tier. With four focused actions over the next 30 days — completing MFA, hardening email defenses, closing open alerts, and addressing storage warnings — the tenant can realistically move from 51% to 65%+ Secure Score within one quarter. Recommended investment: 1-2 days of MSP consulting plus end-user MFA enablement support. Estimated risk reduction: significant.

Report generated by your Microsoft Partner

<Your Name>

<Your Name>

sales@yourcompany.com | +XX XXX-XXX-XXXX

DISCLAIMER

This report is generated using read-only Microsoft Graph API data via this reporting platform. No emails, files, chats, or confidential business data are accessed, stored, or processed. All metrics are derived from Microsoft 365 security and usage telemetry. Recommendations are AI-assisted and should be validated by your IT team before implementation.