Harbour IT

QUARTERLY REVIEW

Fabrikam Dental Group

August to October 2026

PREPARED BY
Harbour IT

DATE
17 October 2026

COMPARED WITH
1 August

MICROSOFT 365 TENANT
fabrikam.onmicrosoft.com

Action needed

Fabrikam Dental Group's Microsoft 365 has a critical security gap that should be fixed now.

Most urgent: 1 admin without MFA, and 2 whose registration isn't known.

IN THIS REPORT

Summary . . . 2
Key figures . . . 2
The last three months . . . 2
What was fixed . . . 3
Projects . . . 3
Licence spend . . . 4
Coming up . . . 4
What we recommend next . . . 5
Questions? . . . 5

Harbour IT · help@harbourit.example · 0161 496 0000

Confidential. This report describes security settings for Fabrikam Dental Group; share it only with people who need it.

Summary

We ran 64 security checks and 49 need attention (1 critical, 15 high, 20 medium and 13 low priority).

On the positive side, 15 checks passed, including “Between 2 and 4 Global Administrators”, “Automatic forwarding to outside addresses is off” and “The Microsoft 365 audit log is on”.

Since 1 August, Microsoft Secure Score rose from 30% to 33%, users with MFA rose from 42% to 50%, 2 issues were fixed and 17 new items came up.

About £164.40 a month (£1,972.80 a year) goes on licences that are unused or assigned to disabled or inactive accounts.

7 checks couldn't run because the data or a licence they need is missing.

Key figures

Secure Score	Users with MFA	Inactive accounts	Licence waste / month
33%	**50%**	**8**	**£164.40**
↑ 3 pts since 1 August	↑ 8 pts since 1 August		

The last three months

Secure Score rose from 30% to 33% over the quarter. Found counts new findings and ones that came back; fixed counts findings resolved in the month.



Month	Secure Score	Found	Fixed
August 2026	31%	–	–
September 2026	33%	0	0
October 2026	33%	17	2

What was fixed

2 findings fixed from August to October 2026.

FIXED **Every active user has MFA registered** · 2 items: george.walker@fabrikam.example, ella.hughes@fabrikam.example

Projects

1 **Email security** SUGGESTED

Email is how most attacks arrive and how fraud gets paid. Locking down the domain stops others pretending to be the business, and closing forwarding and old protocols stops mail leaking out.

12 findings · 58 mailboxes

2 **Identity and Conditional Access** PROPOSED

Most break-ins start with a stolen password, and admin accounts are the biggest prize. Requiring a second factor everywhere, blocking the old sign-in methods that can't ask for one and locking down admin accounts stops nearly all of them.

8 findings · 57 users

3 **Device management with Intune** SUGGESTED

Company data lives on laptops and phones. Managing them means they're encrypted, kept up to date and can be wiped if lost, and unmanaged devices can be kept away from company data.

8 findings · 57 devices

4 **File sharing and guest access** SUGGESTED

Files shared with anyone who has the link, guests nobody remembers inviting and sites and teams nobody owns are an easy way for data to end up in the wrong hands.

7 findings · 7 sites

5 **Windows upgrade and hardware refresh** SUGGESTED

Computers on a Windows version that no longer gets security updates stay open to every flaw found from now on. Upgrading, or replacing machines that can't upgrade, closes that gap.

1 finding · 36 computers

6 **Storage and archiving** SUGGESTED

When storage runs out, people can't save files or receive email. Clearing old versions and archiving is usually cheaper than buying more space.

2 findings

12 quick fixes that don't need a project:

- 1 admin without MFA, and 2 whose registration isn't known
  Goal: Every admin has MFA registered
- 2 high or medium severity alerts open in Defender, 1 not picked up
  Goal: No high or medium severity Defender alerts are left open
- 1 app with access to mail, files or the directory
  Goal: Third-party apps hold only the access they need
- 1 domain had sign-in settings changed in the last 30 days
  Goal: No unexpected changes to how domains sign in
- 8 accounts inactive for 90+ days or never used
  Goal: No inactive accounts
- …and 7 more

Licence spend

Licences a month
£896.30

Licences a year
£10,755.60

Wasted a month
£164.40
unassigned or on disabled or inactive accounts

Licence	Purchased	Assigned	Each / month	Cost / month	Waste / month
Microsoft 365 Business Premium	46	43	£18.10	£832.60	**£144.80**
Microsoft 365 Business Basic	13	11	£4.90	£63.70	**£19.60**
Total	**59**	**54**		**£896.30**	**£164.40**

Coming up

When	What	Detail
Now 6 Nov 2026	**Visio Plan 2 (suspended)** Subscription	5 licences. Suspended: people can't use it, though admins can still back up its data. Reactivate it before this date or it's deleted.
Now 10 Nov 2026	**aisha.brown@fabrikam.example is nearly full** Mailbox quota	47.2 GB of 49.5 GB (95%). At its current growth it's full around 10 Nov 2026. It stops sending mail when it's full: turn on its archive or clean it up.
Now	**accounts@fabrikam.example is nearly full** Mailbox quota	44.8 GB of 49.5 GB (91%). It stops sending mail when it's full: turn on its archive or clean it up.
Now	**thomas.robinson@fabrikam.example is nearly full** Mailbox quota	45.6 GB of 49.5 GB (92%). It stops sending mail when it's full: turn on its archive or clean it up.

When	What	Detail
10 Nov 2026 in 24 days	**Board expires** Team or group expiry	Team with 2 members. Anna Kowalski can renew it; otherwise it's deleted, and can be restored for 30 days.
3 Dec 2026 in 47 days	**Project Phoenix expires** Team or group expiry	Team with 3 members. No owner can sign in to renew it; otherwise it's deleted, and can be restored for 30 days.

What we recommend next

1. **Have every admin without MFA register a strong method**
   1 admin without MFA, and 2 whose registration isn't known.
2. **Make sure each admin is included in an enabled Conditional Access policy that requires MFA for all apps, and isn't excluded from it directly or through a group**
   1 admin not covered by MFA.
3. **Remove admin roles from guest accounts**
   1 guest with admin roles.
4. **Review each app with the people who use it**
   1 app with access to mail, files or the directory.
5. **Turn on BitLocker**
   6 of 54 computers not encrypted.

Questions?

Harbour IT

help@harbourit.example · 0161 496 0000
Reply to this report or call us, and we'll take it from there.

About this report

Prepared by Harbour IT (help@harbourit.example · 0161 496 0000). Everything here was read from Microsoft 365 with read-only access; nothing was changed. Changes are compared with the data from the start of the quarter (1 August). Data collected 17 Oct 2026, 10:49 UTC.