InfraPro
Microsoft 365 managed services and cybersecurity

MANAGED SERVICES MONTHLY REPORT

ARVELLE

October 2026

CLIENT	ARVELLE
PERIOD	October 2026
CONFIGURATION READ ON	31/10/2026
ISSUED ON	03/11/2026
ISSUED BY	InfraPro · your contact
REFERENCE	RM-2026-10

THE MONTH AT A GLANCE

In October 2026 we carried out 31 interventions for you, blocked 412 sign-in attempts, quarantined 64 dangerous or unwanted e-mails and handled 9 alerts. Your team sent us 11 requests; 9 are resolved.

No confirmed security incident this month. Your Secure Score is 78 %, out of a ceiling of about 88 % with your licences. Of the 8 checkpoints verified, 7 are compliant; the last one, a PC that no longer reports to the antivirus, is reinstalled on 3 November. 1 decision awaits you.

SECURE SCORE	MFA-PROTECTED ACCOUNTS	COMPLIANT DEVICES	CONFIRMED INCIDENTS
78 %	**24/24**	**23/24**	**0**
+26 pts since 30/06	Every account enrolled	24 Windows · 1 restarting tonight	Accounts and devices

ANTIVIRUS ACTIVE	ACCESS RULES ON	LICENCES IN USE
23/24	**5**	**24/25**
1 PC no longer reporting	All 5 reference rules	1 Microsoft 365 Business Premium spare

RECORDED CHANGES

52% → 78%	1 → 7 of 8	118
Microsoft Secure Score	control points compliant	interventions logged

Changes since 30/06/2026, the first reading available: Microsoft keeps only 90 days of Secure Score history, so earlier progress does not show here.

DECISIONS WE NEED FROM YOU

1 Limit how long external sharing links last

Today a link shared outside never expires. We suggest 90 days, renewable by the person who shares it. Do you agree?

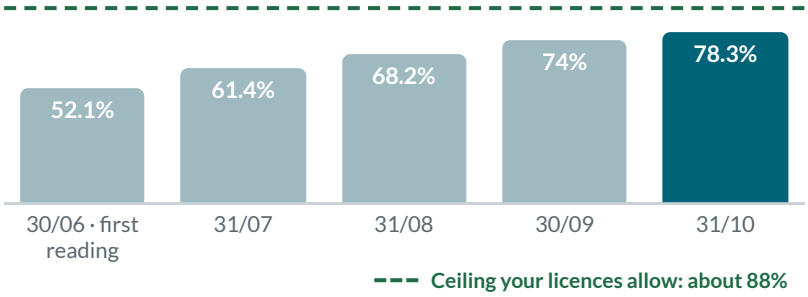
Asked on 28/10 · situation on 31/10/2026

MICROSOFT SECURE SCORE

905 / 1,156 points, or 78%.

Microsoft's score of your security configuration, capped by your licences (Microsoft 365 Business Premium).

Room left with your current licences: 10 points.



CONTROL POINTS

CONTROL	FINDING	STATUS
MFA for everyone A stolen password is no longer enough to get in.	Access rule on. 24 accounts out of 24 enrolled.	● Compliant
Legacy protocols blocked They get around two-factor sign-in.	Access rule on since 08/07.	● Compliant
Compliant devices required Only managed devices reach your data.	Access rule on. 23 managed devices compliant out of 24; 1 restarts tonight for its update.	● Compliant
Systems up to date Out of support means no more security fixes.	24 PCs out of 24 on a supported Windows version.	● Compliant
Antivirus active on PCs A device that stops reporting is no longer watched.	23 PCs out of 24 protected. PC-COMPTA-02 no longer reports to the antivirus: reinstall booked for 03/11.	▲ To address
Privileged accounts Fewer administrators, less risk.	3 Global Administrator assignments. Aim: 2 to 4 named, dedicated accounts.	● Compliant
MFA on admin portals Your settings safe from a stolen password.	Two-factor sign-in required for the admin portals.	● Compliant
Workstation backup A lost device loses no documents.	No data kept on the PCs: documents, desktop and pictures are redirected to OneDrive.	● Compliant

HIGHLIGHT

A phishing attempt stopped on 14/10

An unusual sign-in from abroad on an assistant's account, after a fake delivery e-mail: checked with her, sessions closed and password changed. Two-factor sign-in had blocked the access.

24/7 monitoring: not subscribed. What Microsoft 365 blocked, what it let through and who looks at it: page 5.

SIGN-IN ATTEMPTS

412
failed or blocked

96
on administrator accounts

58
from France

United States: 141
Netherlands: 62
Brazil: 38
Vietnam: 27
Germany: 19

Refused attempts, often robots trying passwords one after another: two-factor sign-in and the access rules stop them. Successful sign-ins from a country not allowed: none this month.

Sources: Entra ID, Defender, Intune, Microsoft Secure Score.

The month's work

What the InfraPro service did for you in October 2026: the threats stopped before they reached you, the fixes made, the requests handled. Every figure comes straight from Microsoft's tools, our monitoring tools and our support desk.

476
Threats stopped
412 sign-ins blocked · 64 emails quarantined · 3 risk detections

46
Interventions, fixes and alerts
31 interventions · 6 fixes · 9 alerts handled

9
Requests resolved
your staff's requests closed (alerts apart)

ACCOUNT PROTECTION

Sign-ins blocked by the access rules	0
Sign-ins stopped by two-factor sign-in	12
Accounts locked against a brute-force attack	301
Wrong passwords refused	64
Total sign-ins refused	**412**
Risky sign-ins detected	3
of which dealt with or dismissed after analysis	3

EMAIL PROTECTION

Phishing	9
Malware	1
Spam	47
Bulk mail	7
Emails quarantined	**64**

2 legitimate emails released after analysis.

FIXES MADE

Risk dismissed after checking	3
Defender incident handled	2
Sessions closed and password changed	1

ALERTS HANDLED

Configuration alerts	4
Device security incidents	2
PCs no longer reporting to the antivirus	1
Risky accounts	1
Licences	1
Defender XDR incidents analysed	2
Detections analysed by the 24/7 monitoring centre	
Microsoft 365 configuration alerts watched	4

SUPPORT

11 requests received
9 requests resolved
1 d median time to resolve
2 open at the month's end

Security **11** · Access **9** · E-mail **6** · Devices **3** · Requests **2**

Interventions logged in the journal, by area.

24/7 monitoring

Microsoft 365 automatically blocks what it recognises as malicious. What it allows (a sign-in with the right password, a mailbox rule, a program started on a device) is not examined as it happens: your service does not include 24/7 monitoring. Here are both sides of your month in October 2026.

BLOCKED AT THE DOOR

By Microsoft 365, automatically: an instant decision on every email, sign-in or file.

Sign-ins refused	**412**
Emails quarantined	**64**
Microsoft Defender incidents	**2**
Risky sign-ins detected	**3**

LET THROUGH, NOT EXAMINED

Allowed by Microsoft 365. None of it is abnormal in itself, but nobody examined it as it happened.

Successful sign-ins from a country not allowed	**0**
Configuration changes made outside InfraPro 21 by your staff, 155 automatic	**176**
PCs no longer reporting to the antivirus PC-COMPTA-02	**1**
Rule requiring two-factor sign-in	**In place**

WHO LOOKS, AND WHEN

	TODAY	WITH 24/7 MONITORING
A successful sign-in with a stolen password	Seen at our next intervention or check	**Examined continuously, across your accounts and devices together**
At night, at weekends	Not watched	**An analyst, 24 hours a day, 7 days a week**
A compromised device or account	Isolated by us, once we are told	**Device isolated or account blocked straight away, day and night**

EXTERNAL EXPOSURE

What anyone can see from the internet: how well your domain names are protected against spoofing, and your addresses found in public data leaks.

DOMAIN	SPF	DKIM	DMARC	ENCRYPTION	GRADE
arvelle.example	OK	OK	OK	OK	**A**

SPF, DKIM and DMARC stop a third party sending emails in your name; encryption protects messages in transit between servers. Graded from A (best) to E. Last checked on 02/11/2026.

Guest accounts (people outside your organisation)	**7 of 31**

A guest keeps access to what was shared with it (files, teams) until it is removed.

COMPLIANCE LEVEL



Share of each framework's checkable requirements that your configuration meets, from the audit of 14/10/2026. NIS2: the European cybersecurity directive; CIS: international good practice; ANSSI: the recommendations of France's national cybersecurity agency.

CONFIGURATION CHANGES

Changes recorded by Microsoft	**214**
by InfraPro	**38**
by your staff	**21**
automatic (Microsoft, applications)	**155**

User accounts **71** · Devices **52** · Groups and teams **33** · Apps and permissions **18** · Access rules and policies **6**

Of which 12 changes made by a person to administrative rights, access rules or applications. Microsoft Entra audit log.

DEVICES AND ENCRYPTION

Encrypted computers	**24 of 24**
Windows 11 24H2	**9**
Windows 11 25H2	**15**

An encrypted computer (BitLocker, FileVault) protects your data if it is lost or stolen.

Your choices and the score

WHAT MOVED THE SECURE SCORE

30/09/2026 → 31/10/2026: +50 pts, control by control, from Microsoft's history.

− Fix Microsoft Defender Antivirus cloud service connectivity: 4 pts. Probably devices no longer reporting (PC-COMPTA-02): a PC in storage or switched off lowers it with no change in the configuration.

+ Do not allow users to grant consent to unreliable applications: 30 pts

+ Block Office applications from creating child processes: 21 pts

+ Ensure MailTips are enabled for end users: 3 pts

CHOICES MADE BY YOUR ORGANISATION

Protections left off or lighter at your request, for the needs of your business. They can be reversed; we review them with you.

Personal webmail allowed
At your request, for your sales staff on the road. Use is still monitored. Accepted on 12/09/2026, to review before 12/03/2027.

THIS MONTH'S INTERVENTIONS

DATE	AREA	INTERVENTION	STATUS
31/10	**Devices**	One PC no longer reports to the antivirus: reinstall booked for 03/11 with its user.	In progress
28/10	**Access**	A new starter on 03/11: account, licence and laptop ready.	**Done**
21/10	**E-mail**	Folder deleted by mistake in a shared space: restored at its user's request.	**Done**
14/10	**Security**	Sign-in alert from abroad: checked with the user, sessions closed and password changed.	**Done**
08/10	**Security**	Two unused apps removed from your directory, with your agreement.	**Done**

NEXT MONTH

1. **Reinstall the PC concerned**
   On 3 November, with its user; its documents are in OneDrive.
2. **Prepare two arrivals in December**
   Accounts, licences and laptops, ready before day one.

LICENCES

LICENCE	BOUGHT	ASSIGNED	SPARE
Microsoft 365 Business Premium	25	24	1

RENEWALS IN THE NEXT 60 DAYS

Microsoft 365 Business Premium — **due on 14/12/2026**

For information: we will contact you if a renewal needs a decision from you.