Lansafe

MANAGED SECURITY · IT & TELECOMS



LanGuard

by Lansafe

Always-on security monitoring for your Microsoft 365, network, website and email domain, explained in plain English every morning.

AI-driven monitoring that watches every hour, scans what attackers can see, and tells your team only what matters. A flat monthly fee, no per-seat licences.

Microsoft 365
Sign-ins, MFA, sharing and admin changes

Network
Firewall, internet lines, devices and VPN

Website and email
Uptime, SSL, DMARC and lookalike domains

Exposure
Port scans, breach and dark-web alerts

THE CHALLENGE

Security monitoring built for big IT teams doesn't fit small businesses

Small and mid-sized firms face the same attacks as large enterprises: password spraying, compromised mailboxes and constant scanning of anything exposed to the internet. But they rarely have a security team to watch for them.

£

Per-seat costs add up

Traditional monitoring tools charge for every user, every month. As you grow, the bill grows, whether or not the risk does.

!

Alert fatigue

Dashboards produce hundreds of alerts. Most are harmless, so real warnings get missed or ignored.

1

Small IT teams

Often one person looks after everything. They need clear answers, not another console to check.

THE LANGUARD SERVICE

Watches every hour. Reports every morning.

LanGuard connects to the systems you already run, checks them every hour, looks at your business from the outside the way an attacker would, and uses AI to triage what it finds. Harmless events are dismissed with a written reason; anything real is escalated straight away.

Microsoft 365 security

Hourly sign-in watch, mail forwarding, inbox rules and app consents, plus MFA coverage, admin role changes, external sharing, Secure Score trend and unused licences.

Network, devices and backups

Firewall, internet lines, intrusion prevention, VPN, firmware and new devices; patch and antivirus status and nightly backup checks where you have the tools.

Website, email and exposure

Uptime, SSL and website errors; SPF, DKIM and DMARC; lookalike domains; external port scans and alerts when staff addresses appear in a data breach.

Reports people actually read

A plain-English email every morning around 08:00 UK time, urgent alerts as they happen, and a monthly board-level PDF with a security score and trend.

Tested checks first. AI where it earns its place.

Scripted checks gather and count the data the same way every hour; AI interprets what is unusual. Every finding is classified as dismissed or escalated, and the report says why: "all from the office IP, looks like a mistyped password" or "not the office IP, please confirm". Your team can check the reasoning instead of reading raw logs. Urgent problems trigger an alert straight away rather than waiting for the morning report.

WHY CUSTOMERS CHOOSE LANGUARD

Three checks that change the conversation

Most small businesses have never seen their own network the way an attacker sees it, don't know which staff addresses are already in data breaches, and get no regular, readable view of their security. LanGuard Professional and Complete fix all three.

1 External port scan

We regularly scan your public internet addresses from outside, list every open port and exposed service, and flag anything new or risky with a plain-English fix.

- Finds forgotten port forwards, remote-desktop and admin pages
- New exposures alert straight away; known ones are tracked until closed
- Matched with what your firewall is actually blocking

REAL EXAMPLE

In a live LanGuard deployment, a time-and-attendance server was reachable from the internet through a port forward. It was probed every day: **71 attempts across five daily reports** in November 2026, 26 of them from 26 addresses in 11 countries on one day alone. Every attempt was blocked, and LanGuard kept recommending the fix: limit access to the addresses that need it, or move it behind the VPN.

2 Breach monitoring

We monitor your company email domains against Have I Been Pwned, the widely used breach-notification service. When staff addresses turn up in a newly loaded data breach, you hear about it with the action to take.

- Which addresses, which breach, when, and what data was exposed
- Clear next steps: password reset, MFA check, sign-in review
- Add dark-web and leaked-credential alerts for wider coverage

EXAMPLE ALERT, ILLUSTRATIVE ONLY

2 company addresses found in a newly added breach. An online service used by staff was breached; email addresses and passwords were exposed. Both accounts have MFA. Action: ask both users to change any reused passwords, and we'll watch their Microsoft 365 sign-ins closely for 14 days.

3 Monthly security score report

A board-level PDF every month: one security score out of 100 with its trend, progress by area, what was fixed, and the top actions for next month. Written for directors, not engineers.

- Like-for-like checks every month, so the trend means something
- Evidence for insurers, auditors and Cyber Essentials work
- Includes savings found, such as unused Microsoft 365 licences

EXAMPLE, ILLUSTRATIVE ONLY

See the next page for a sample monthly report. All figures on it are invented to show the layout; they are not from a real customer.

THE MONTHLY BOARD REPORT

One page your board will actually read

Each month LanGuard Professional and Complete customers receive a short PDF that turns hundreds of hourly checks into a single score, a trend and a short list of actions.

EXAMPLE · ILLUSTRATIVE DATA

LanGuard monthly security report

Example Company Ltd · November 2026 · prepared by Lansafe

Lansafe

SECURITY SCORE

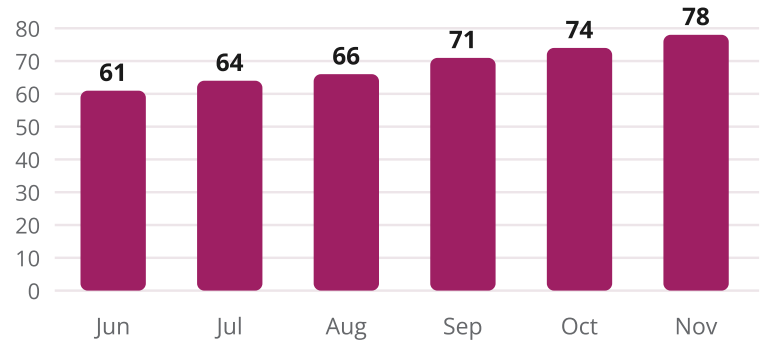
78/100

▲ 4 points on October

Up 17 points since onboarding in June

Score trend

Same checks every month, so the trend is like-for-like



Score by area

Microsoft 365	82
Network and firewall	88
Website	91
Email and domain	64
Exposure	70
Backup and continuity	75

Top actions for December

- **Move DMARC from monitor to quarantine.** Reports show one unknown service sending as your domain.
- **Turn on MFA for the last 2 accounts.** Coverage is 23 of 25 users.
- **Close the old port forward** found by the external scan, or put it behind the VPN.
- **Remove 4 unused licences.** Saving about £67.60 a month at Business Premium list price.

Fixed this month

Admin role removed from a leaver's account; SSL certificate renewed 21 days before expiry; firewall firmware updated.

Watched, no action

1,850 sign-ins reviewed; 312 intrusion attempts blocked; 1 Microsoft 365 outage reported to you before staff noticed.

Still open

Anonymous sharing links on 3 SharePoint folders; agreed with your IT lead to review by 15 December.

Everything inside the dashed frame is invented example data to show the report layout, including the company, scores and counts. The £67.60 saving uses Microsoft's UK list price for Business Premium (£16.90 per user per month, paid yearly, ex VAT). Each LanGuard check scores pass, partial or fail, weighted by risk.

Seven areas, one plain-English report

Every check feeds the same daily report and monthly score. The baseline (firewall, Microsoft 365 sign-ins, website uptime and SSL) is in every tier.

Tier key: **All tiers** **Professional +** **Complete** Professional + means Professional and Complete.

Microsoft 365

Identity and tenant security, reviewed every hour.

Sign-in watch — All tiers
Hourly review of sign-ins, failed logins and mail sent from unfamiliar connections.

External mail forwarding — All tiers
Flags any mailbox quietly forwarding mail outside the business.

New inbox rules and OAuth app consents — All tiers
Each one checked and scored, a common sign of a compromised mailbox.

Secure Score trend — Professional +
Microsoft's own security score, tracked month by month.

MFA coverage per user — Professional +
Who has multi-factor authentication, and who doesn't yet.

Admin role changes — Professional +
Alerts when anyone is given, or removed from, an admin role.

External sharing and anonymous links — Professional +
Files and sites in Teams and SharePoint shared outside the business.

Unused licences — Professional +
Licences assigned to nobody, or to leavers: an easy monthly saving.

Risky sign-ins and impossible travel — Complete
Sign-ins Microsoft rates as risky, and logins from places too far apart to be one person.
Needs Microsoft Entra ID P1

Website watch

Your website, checked from the outside the way customers see it.

Uptime and response time — All tiers
Regular checks from outside your network; down or slow pages alert straight away.

SSL certificate expiry — All tiers
Warning well before the padlock certificate runs out.

http to https redirect — All tiers
Checks that visitors are always sent to the secure version of the site.

Dead links and pages crashing in the browser — Professional +
Broken links and JavaScript errors that stop pages or forms working.

DNS, SPF and DMARC record changes — Professional +
Alerts when a record that controls your website or email is changed.

Content change detection — Professional +
Spots unexpected edits or defacement of key pages.

Domain blacklist checks — Professional +
Tells you if your web domain appears on a reputation blocklist.

Email and domain

Protects your domain from spoofing and expiry.

Domain and certificate expiry — All tiers
Reminders before a domain or certificate lapses.

SPF, DKIM and DMARC monitoring — Professional +
Checks your email authentication records are present and correct.

DMARC report summaries — Professional +
Who is sending email as you, including spoofers, in plain English.

Lookalike domain alerts — Professional +
New registrations of domains that imitate yours, often used for phishing.

Mail IP blacklist checks — Professional +
Tells you if your outgoing mail servers are blocklisted.

WHAT LANGUARD WATCHES · 2 OF 2

From the firewall to the boardroom

Checks that need extra Microsoft licences or access to your backup systems sit in Complete, or can be added to other tiers.

Tier key: **All tiers** **Professional +** **Complete** Professional + means Professional and Complete.

Endpoints and network

Your firewall, internet lines and devices.

Firewall, WAN and IPS watch — All tiers
Gateway status, intrusion prevention mode, blocked attacks and admin logins.

Secure remote access (VPN) watch — All tiers
Who connected, from where and for how long.

Firmware updates waiting — All tiers
Updates pending on the firewall, switches and access points.

WAN uptime and latency, with ISP outage log — All tiers
A record of every internet line drop, to hold your provider to account.

New or unknown devices on the network — Professional +
Alerts when an unrecognised device joins.

Missing patches and Defender or antivirus off — Complete
Devices that are behind on updates or unprotected.
Needs Intune and Defender

Exposure and threat intel

What an attacker can see of your business from the internet.

External port scan of your public IPs — Professional +
Finds open ports and exposed services before attackers do.

Breach monitoring of company addresses — Professional +
Alerts when staff email addresses appear in a newly loaded data breach (Have I Been Pwned domain search).

Dark-web and leaked-credential alerts — Complete
Watches for company credentials being traded or leaked.
Add-on for Professional: £49/month

Backup and continuity

Proof your backups would work on the day you need them.

Nightly backup success checks — Complete
Microsoft 365, NAS and cloud backups checked every morning.
Add-on for Essentials and Professional: £99/month (Backup assurance)

Quarterly restore tests — Complete
A real test restore each quarter, with the result written up.
Included in Backup assurance add-on

Reporting

Clear answers, not another console.

Plain-English daily report and urgent alerts — All tiers
One email each morning; urgent problems alert straight away.

Third-party outage alerts — All tiers
Hear about Microsoft 365 and other supplier outages from Lansafe first.

Monthly board-level PDF report — Professional +
A security score with trend, progress by area and the top actions.

Lansafe engineers act on escalations — Complete
We carry out agreed fixes for you, within fair-use hours.

Quarterly review with Lansafe — Complete
Trends, exposures and priorities for the next quarter.

What you need for the Complete-tier checks

Risky sign-in and impossible-travel checks need **Microsoft Entra ID P1** on your user accounts. Patch and antivirus checks need devices managed in **Microsoft Intune** with **Microsoft Defender**. Both are included in Microsoft 365 Business Premium. Backup checks need read access to your backup platform. We confirm what you have at the free review.

REAL-WORLD EXAMPLE

A week with LanGuard

These figures come straight from the last five daily reports sent to the IT team at **NW Metal Sections (NWMS)**, a UK manufacturer where the LanGuard approach is already running. Reports dated 2, 4, 5, 9 and 11 November 2026.

71
intrusion attempts stopped at the firewall: all blocked, none merely detected

457
successful Microsoft 365 sign-ins reviewed, all from the office or a known home connection

41
failed sign-ins triaged: all from the office network, dismissed as mistyped passwords

2
items escalated for a human to check, each with a recommended action

0
sign-ins from the attacker IP range linked to an earlier mailbox incident

0
failed VPN logins or failed firewall admin logins

100%
main internet line (WAN1) uptime, about 9 ms latency, wherever measured

36/36
network devices online on four of five days (see note on 11 Nov)

Day by day

Report	Status	IPS blocks	M365 sign-ins	Failed	VPN	Admin logins	Devices online	IPS mode
Mon 2 Nov	All clear	26	4	0	6 sessions	0	36 / 36	Block
Wed 4 Nov	All clear	9	218	25	26 connects	6	36 / 36	Block
Thu 5 Nov	Attention needed	11	126	13	34 connects	7	36 / 36	Block*
Mon 9 Nov	All clear	15	16	0	4 connects	1	36 / 36	Block
Wed 11 Nov	All clear	10	93	3	Normal (1 user)	10	33 online, 0 offline	Block
Total	4 clear, 1 attention	**71**	**457**	**41**	**0 failed logins**	**24**	**0 offline**	**Correct on all 5**

Each report covers the 24 hours to about 08:10 UK time on the date shown. IPS blocks on 2 Nov: 25 high severity, 1 low; all others high severity. *5 Nov: firewall logs were readable up to 00:50; after 01:52 the vendor API refused log access (see page 9), so the 11 blocks are a minimum and IPS mode was last confirmed at 00:50. 11 Nov: 33 devices counted online and none offline, against a baseline of 36, flagged in the report for a sanity check. VPN on 2 Nov counted as sessions; 11 Nov activity was all from one known user and not counted. Nobody was paid per seat to produce these numbers.

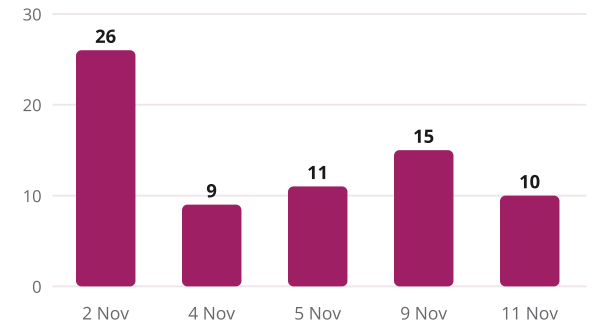
WHAT THE WEEK LOOKED LIKE

Constant probing, all of it stopped

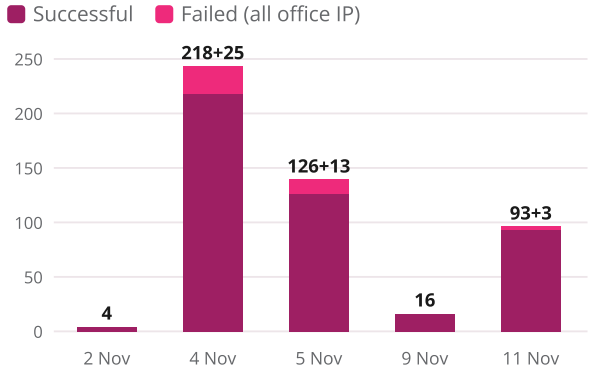
Every one of the 71 intrusion attempts targeted the same internet-facing service (a [redacted] time-and-attendance server behind a port forward). LanGuard spotted the pattern, kept counting it, and repeated its advice to restrict that exposure.

Intrusion attempts blocked per report

Firewall IPS in detect-and-block mode on all five days



Microsoft 365 sign-ins per report



On 2 Nov alone the 26 attempts came from 26 different addresses in 11 countries: US 9, Hong Kong 4, Nigeria 3, Netherlands 3, and one each from China, Thailand, Brazil, the UK, Japan, Canada and Germany. Sources were typically internet scanners (such as Censys) and cloud hosting ranges. Lower sign-in counts on 2 and 9 Nov are reports covering a Sunday.

AI TRIAGE IN PRACTICE

Escalated vs dismissed, and why

Escalated to a person

5 Nov · Monitoring gap

From 01:52 the firewall vendor's API started refusing access to IPS settings and security, VPN and admin logs. An alert went out at once, every hourly check confirmed it, and the morning report gave the exact fix: check or recreate the API key with log and IPS access.

11 Nov · Mail sent from an unfamiliar IP

One mailbox sent a message from [redacted], which is not the office IP. Low priority (a single send, no failed logins) but flagged: confirm the user was working remotely, otherwise reset the password and review sign-in history.

Ongoing · Exposed service

Repeated probes of the [redacted] port forward. Advice: limit it to the addresses that need it, or put it behind the VPN.

Dismissed, with the reason given

41 failed sign-ins

All from the office IP, including 18 for one account on 4 Nov. Pattern consistent with mistyped passwords, not an attack.

Mail sent from home and mobile connections

Matched to UK broadband and mobile providers, Microsoft's own servers, or the user's known VPN address. Normal remote working.

Early-morning VPN session (2 Nov)

6 minutes at about 04:37 from the user's usual home IP, matching her earlier pattern.

Wi-Fi channel changes

An access point detected radar on a DFS channel and moved. Normal Wi-Fi behaviour.

WHAT LANDS IN YOUR INBOX

A real daily report

This is the report sent to the NWMS IT manager and engineering director on 11 November 2026, trimmed and condensed for length. No dashboards to learn, just a short email that says what happened and what to do.

NWMS firewall & M365 daily report – 11 Nov 2026: All clear

Sent 09:01 GMT · To: IT Manager, Engineering Director

Window: 08:16 GMT 10 Nov to 08:16 GMT 11 Nov. No suspicious activity found. One small item to check.

To check (low priority)

- The M365 feed shows [redacted] sending mail from [redacted], which is not the office IP. It was a single send with no failed logins from it. Please confirm [redacted] out of the office or on a personal connection. If not, reset [redacted] and check [redacted] history.

Firewall ([redacted])

- Gateway connected; both WANs up.
- 33 devices online, none offline (baseline is 36, so please sanity-check the count).
- Only pending firmware update: [redacted] itself, [redacted].
- IPS mode is "ips" (detect and block), correct.
- Intrusion attempts: 10, all High severity, all blocked, none merely detected. All targeted the [redacted] server [redacted]. From the address ranges, sources look like Google Cloud, AWS and Censys scanners. The [redacted] port forward is still exposed and still being probed, but everything was blocked.
- VPN: all activity was from one known user and looks normal (several short connect/disconnect cycles and one 4h 34m session).
- Admin: 10 logins, all [redacted] from the office IP, no failures, nothing from unknown IPs.
- Wi-Fi: AP "[redacted]" detected radar on channel 124 and moved to 157, then back to 124 at 02:10. Routine.

Microsoft 365 sign-ins (3,609 events reviewed)

- 93 successful sign-ins, all from the office IP.
- 3 failed sign-ins, all from the office IP ([redacted] twice, [redacted] once), which looks like a mistyped password.
- Nothing from [redacted]; no inbox rule or forwarding changes; no app consents.
- Mail sent from outside the office: via Microsoft addresses (normal), a known VPN address, a likely Azure address and a UK ISP; plus [redacted] from [redacted] (see above).
- The 21 Oct [redacted] incident: nothing from [redacted] in this window, so it is not recurring.

Every number in this brochure's example section comes from reports like this one.

Plain English

Written for the people who run the business, not just the IT team. No jargon, no raw log dumps.

Actions, not alerts

Every item to review comes with a clear recommended next step and how urgent it is.

Follow-through

Open issues are carried forward and re-checked each morning until they are resolved.

HOW IT WORKS

Up and running without new hardware

LanGuard connects to the cloud management interfaces of the platforms you already use and checks your public-facing systems from the outside. There are no agents to install on staff PCs and no appliances to rack.

1

Discover

Lansafe reviews your Microsoft 365 tenant, firewall, website, email domains and public IPs, and agrees who gets the reports.

2

Connect

We set up read access through the vendors' own APIs, verify your domains for breach monitoring and agree the scan targets.

3

Baseline

LanGuard learns what normal looks like: office IPs, device counts, open ports, regular VPN users and known exposures.

4

Monitor

Hourly checks begin, with urgent alerts as they happen, a report every morning and a score report every month.

WHY LANGUARD

LanGuard compared with typical per-seat monitoring

	Typical per-seat security tools	LanGuard by Lansafe
How you pay	Licence per user, per month, often one per product	One flat monthly fee: no per-seat licence
What you receive	A dashboard and a stream of alerts	A daily plain-English report and a monthly board score
Noise	Your team triages every alert	AI dismisses benign events and states the reason
Coverage	Separate tools for identity, firewall, website and email	Microsoft 365, network, website, email domain, exposure and backups in one report
Outside view	Rarely included	External port scans and breach monitoring of your domains
Follow-through	Alerts close when acknowledged	Open issues are tracked and re-checked daily until resolved
Who's watching	Your staff, when they have time	Hourly automated checks, backed by your MSP

No per-user creep

The fee covers your tenant and main site up to 150 users. Growing headcount doesn't grow the bill.

Uses what you own

LanGuard reads from Microsoft 365, your firewall and your backup tools. Nothing to rip out or replace.

Monitoring, not lock-in

LanGuard reports and recommends. Changes are made by your IT team or by Lansafe, with your approval.

SERVICE OPTIONS

Choose your level of cover

Every tier includes the baseline: firewall and network watch, Microsoft 365 sign-in watch, website uptime and SSL, and the daily report. Prices per Microsoft 365 tenant, up to 150 users.

What's included	Essentials	Professional Most popular	Complete
Monthly price, ex VAT Flat fee, no per-user charge	**£199** per month	**£399** per month	**£749** per month
Included	1 site/gateway · 1 website · 1 email domain	1 site/gateway · 3 websites · 2 email domains · 8 public IPs	1 site/gateway · 5 websites · 3 email domains · 16 public IPs
Onboarding	Included	£295 one-off	£495 one-off
Website watch			
Uptime and response time	✓	✓	✓
SSL certificate expiry	✓	✓	✓
http to https redirect	✓	✓	✓
Dead links and pages crashing in the browser	–	✓	✓
DNS, SPF and DMARC record changes	–	✓	✓
Content change detection	–	✓	✓
Domain blacklist checks	–	✓	✓
Microsoft 365			
Sign-in watch	✓	✓	✓
External mail forwarding	✓	✓	✓
New inbox rules and OAuth app consents	✓	✓	✓
Secure Score trend	–	✓	✓
MFA coverage per user	–	✓	✓
Admin role changes	–	✓	✓
External sharing and anonymous links	–	✓	✓
Unused licences	–	✓	✓
Risky sign-ins and impossible travel **(Needs Microsoft Entra ID P1)**	–	–	✓
Email and domain			
Domain and certificate expiry	✓	✓	✓
SPF, DKIM and DMARC monitoring	–	✓	✓
DMARC report summaries	–	✓	✓
Lookalike domain alerts	–	✓	✓
Mail IP blacklist checks	–	✓	✓

Continued overleaf: exposure, endpoints and network, backup and reporting, plus add-ons.

Choose your level of cover

What's included	Essentials	Professional Most popular	Complete
Monthly price, ex VAT	**£199**	**£399**	**£749**
Exposure and threat intel			
External port scan of your public IPs	–	✓	✓
Breach monitoring of company addresses	–	✓	✓
Dark-web and leaked-credential alerts	–	**Add-on £49/month**	✓
Endpoints and network			
Firewall, WAN and IPS watch	✓	✓	✓
Secure remote access (VPN) watch	✓	✓	✓
Firmware updates waiting	✓	✓	✓
WAN uptime and latency, with ISP outage log	✓	✓	✓
New or unknown devices on the network	–	✓	✓
Missing patches and Defender or antivirus off **(Needs Intune and Defender)**	–	–	✓
Backup and continuity			
Nightly backup success checks	**Add-on £99/month**	**Add-on £99/month**	✓
Quarterly restore tests	**Add-on £99/month**	**Add-on £99/month**	✓
Reporting			
Plain-English daily report and urgent alerts	✓	✓	✓
Third-party outage alerts	✓	✓	✓
Monthly board-level PDF report	–	✓	✓
Lansafe engineers act on escalations	–	–	✓
Quarterly review with Lansafe	–	–	✓

Add-ons

Additional site or gateway
£59/month · All tiers

Additional website
£15/month · All tiers

Additional email domain
£35/month · Professional and Complete

Dark-web and leaked-credential alerts
£49/month · Professional (included in Complete)

Backup assurance: nightly checks + quarterly restore test
£99/month · Essentials and Professional (included in Complete)

LanGuard Exposure Check: one-off port scan and breach report
£195 one-off · Anyone; credited if you join Professional or Complete within 60 days

All prices exclude VAT and are billed monthly on a 12-month term. No per-user charges up to 150 Microsoft 365 users; larger organisations, extra tenants and multi-site estates are quoted individually. Microsoft licences (for example Entra ID P1 or Business Premium) are not included. Lansafe engineer work in Complete is subject to fair-use hours set out in your service agreement.

QUESTIONS AND ANSWERS

Frequently asked questions

Which platforms does LanGuard support?
Microsoft 365 (Entra ID, Exchange Online, Teams and SharePoint), UniFi gateways and networks, Tailscale secure access, and any public website, domain or IP address. Ask about other firewalls and backup platforms.

Do you install anything on our computers?
No. LanGuard reads from the platforms' cloud management APIs and checks your public systems from outside. Patch and antivirus checks use Intune and Defender, which you may already have.

Can LanGuard change our settings?
LanGuard is a monitoring service. It reports and recommends; changes are made by your IT team or your MSP, with your approval.

What happens if monitoring itself breaks?
LanGuard checks its own access every hour. When a vendor API stopped returning logs at NWMS, an alert went out within the hour, along with the exact fix.

Is the external port scan safe?
Yes. It only checks which ports answer on the public addresses you authorise, at a gentle rate. It doesn't try to break in or change anything.

What data do you look at?
Security and audit data: sign-in records, firewall events, device and sharing status, DNS records and breach notifications. LanGuard does not read the content of emails or files.

Which tier should we choose?
Most businesses start with Professional: it adds the port scan, breach monitoring and monthly score report. Choose Complete if you want Lansafe to act on findings and check backups.

Who sees our reports?
Only the people you nominate, usually your IT lead and a director, plus your MSP. Data handling and retention terms are set out in your Lansafe service agreement.

Do we need extra Microsoft licences?
Not for Essentials or Professional. Complete's risky sign-in and device checks need Entra ID P1 and Intune with Defender, all included in Microsoft 365 Business Premium.

Will we be flooded with alerts?
No. In the NWMS example, 498 sign-in attempts and 71 blocked attacks over five reports produced just two items for a person to check.

See what LanGuard would find on your network

Book a free review of your Microsoft 365, firewall, website and email domain, or start with a one-off Exposure Check. One company, one solution. The Lansafe Way.

lansafe.co.uk

CALL
01257 254 120

EMAIL
enquiries@lansafe.co.uk

HEAD OFFICE
Lansafe Ltd, Technology House, Skull House Lane, Appley Bridge, Wigan WN6 9DL

WIGAN OFFICE
Lansafe Ltd, Cotton Works, Swan Meadow Road, Wigan WN3 5EX

LanGuard is built by **Lansafe AI Studio** (lansafe.ai), part of Lansafe Technology Group: *Powerful software. Lasting benefit.*

Lansafe Ltd, company no. 05267904. Lansafe Technology Group, registered in England & Wales, company no. 16537113. Example figures: NW Metal Sections daily reports dated 2, 4, 5, 9 and 11 November 2026, reproduced with permission. The breach alert and monthly report on pages 3 and 4 use illustrative example data.