Week commencing 9 November 2026

ClearPath Partnership

COVERAGE
26 October – 8 November 2026

AUDIENCE
Technology and security leadership · platform and delivery leads

HANDLING
Internal use — not for onward distribution

IF YOU JUST REMEMBER ONE THING FROM THIS BRIEFING…

Microsoft switched on AI agent creation for every user this fortnight, with no admin action needed to allow it.

From 4 November, Entra ID lets any licensed user build agent blueprints by default, on a setting separate from app registration. It lands the same week NCSC judged most environments will stay exploitable by AI-driven attack tools through 2028. Ask this week: who can create an agent in our tenant today, and have we actually turned the setting off.

THIS FORTNIGHT

Platform change and AI regulation

PRIORITY

4 NOV

Entra ID defaults every user to building AI agents, not just apps

Microsoft's Entra ID update, effective 4 November, lets every licensed user create AI agent blueprints by default — a setting separate from app registration. Admins who already blocked app registration are not automatically covered; the toggle sits under Entra ID > Users > User settings.

So what: check whether "users can create agent blueprints" is set to no today — app-registration lockdown alone leaves this gap open.

PRIORITY

9 NOV

Entra ID self-service password reset now demands registered methods

From 9 November, SSPR only accepts verification through methods a user has explicitly registered; inferred or unregistered methods no longer qualify. Microsoft revised this rollout date twice over the summer, so confirm your tenant's actual enforcement date in the message centre.

So what: run a registration-compliance report now — unregistered users will be locked out of self-service reset and land on the helpdesk instead.

PRIORITY

15 NOV

Sentinel retention triples as migration to Defender's unified SOC opens

From 15 November, eligible customers can migrate Sentinel workspaces into Defender's integrated security operations centre, and retention for Defender, Azure Activity and Office 365 Activity logs extends from 30 to 90 days free. Analysts expect a gradual standalone-Sentinel retirement; Microsoft has not confirmed that timeline.

So what: treat this as the start of a multi-year SOC migration and plan the move, rather than waiting for a forced cutover.

WATCH

3 NOV

NCSC: most systems will stay exploitable by AI attack tools to 2028

NCSC's new assessment judges it almost certain that many UK systems remain open to AI tools that find and exploit weaknesses through 2028, and warns AI-assisted malware is likely to feature in a ransomware attack on UK critical infrastructure. The assessment is a judgement, not a forecast of a specific incident.

So what: benchmark your time-to-patch against how far AI narrows the gap between disclosure and exploitation, not against last year's figure.

ACTION QUEUE

Changes to act on this fortnight

CHANGE	PLATFORM	WHAT IT BREAKS OR REQUIRES	ACT BY
Agent blueprint creation default	Microsoft Entra ID	Any user can build agents unless an admin disables the setting.	Immediate
SSPR needs registered methods	Microsoft Entra ID	Unregistered users fail self-service password reset.	Immediate
.NET 8/9 and Functions in-process model EOS	Microsoft Azure	Apps keep running but lose security updates.	10 Nov 2026
Sentinel retention and ISOC migration window	Microsoft Sentinel/Defender	Retention extends to 90 days; migration eligibility opens.	15 Nov 2026
Copilot Business usage-based billing by default	Microsoft 365 Copilot	New CSP licence purchases get metered AI billing.	~1 Dec 2026

Dates as published by Microsoft; the Copilot billing date has shifted twice and should be confirmed in Partner Center before budgeting against it.

REGULATORY AND SECTOR WATCH

What changed, and what is coming

In force now

- Entra ID agent-blueprint creation is open to every user by default since 4 November; admins must act to restrict it.
- Entra ID SSPR requires registered authentication methods from 9 November.

Approaching

- EU AI Act Article 50(2) watermarking grace period for pre-August systems ends 2 December 2026.
- Sentinel-to-Defender ISOC migration eligibility and 90-day retention open 15 November 2026.

Standing watch — sovereign cloud and data residency. No new sovereign-cloud move this fortnight. Keep tracking supplier data-boundary commitments at contract renewal.

AWS and Google Cloud: a quiet fortnight for both — nothing met the inclusion bar on either platform.

RECOMMENDED

Three things to do before the next edition

- Check now whether agent-blueprint creation is disabled in your tenant, and inventory any agents already built.
- Run a registration-compliance report before SSPR enforcement locks out unregistered users at the helpdesk.
- Decide whether to migrate Sentinel workspaces to Defender's unified SOC, or set a deliberate review date.

OUTLOOK — NEXT FORTNIGHT

We assess it is likely further Entra ID default changes follow as Microsoft extends agentic AI across the tenant, and a realistic possibility Microsoft confirms a phased Sentinel retirement before the next edition. Expect AWS and Google to stay quiet for a second fortnight.

NEXT EDITION

Monday 23 November 2026. Send additions, corrections or platform intelligence to your ClearPath engagement lead.

ClearPath Partnership