NODE4

Managed XDR

Cross-domain detection and response, operationalised on Microsoft Defender XDR

Modern attacks cross silos. Your defence should too.

The XDR gap

The mid-market runs 15-30 security tools. Identity over here, email over there, endpoint somewhere else, cloud workloads in a different console entirely. Each one reports its own alerts. None of them know what the others are seeing. Modern attackers rely on this — they pivot through the gaps in minutes, not days.

What Managed XDR delivers

- Correlated detection across identity, endpoint, email, cloud, SaaS and network
- 24x7 UK SOC analysts who pivot across signals — not just acknowledge alerts
- Active response anywhere: revoke a token, isolate a host, reverse a malicious inbox rule
- Native operation on Microsoft Defender XDR, plus support for major non-Microsoft estates
- Proactive threat hunting across cross-domain telemetry, not just rule-based alerts
- IR retainer hours, named SOC lead, and quarterly service reviews

How we deliver

1. Onboard Defender XDR (or equivalent) in under 5 working days
2. Calibrate cross-domain correlations and active-response playbooks
3. Provide 24x7 detection, investigation and active response
4. Hunt proactively across identity, endpoint, email and cloud
5. Report monthly to the board, review quarterly with a named SOC lead

Operationalise the XDR capability you already licence through Microsoft 365 E5 — no new tool to buy, no rip-and-replace, no new console for your team.

Service at a glance

Service levels

Targets below are contractual. Coverage is 24x7x365 from the UK SOC, with named tier 1-3 analysts and Microsoft security specialist engineering escalation.

Service level	Target
P1 detection → analyst contact	< 15 mins
P1 cross-domain containment	< 30 mins
Identity compromise response	< 15 mins
P2 triage initiated	< 1 hour
Monthly posture report	5th working day
Service review cadence	Quarterly

Why Node4

Microsoft Solutions Partner with the Security designation. Defender XDR specialism with cross-domain detection engineering. UK sovereign SOC, SC-cleared analysts, board-ready reporting. We operationalise what you already own — we don't sell you another console.

Try it for 14 days

Our 14-day Threat Assessment runs your live estate through our SOC. You receive a findings pack — what we detected, what we'd have contained, and a prioritised remediation roadmap. No obligation. The findings pack is yours to keep.

Talk to us

Book a Microsoft-aligned Cyber Security Envisioning Workshop. Microsoft-funded, delivered by Node4's UK SOC leads. Visit node4.co.uk/cyber to get started.