



Security & Identity for Microsoft 365 (Zero Trust, Entra ID, Defender & Sentinel)

Microsoft 365: Modern Workplace

we commit. we deliver.

Delaware public sector cloud services

Delaware delivers outcome-led cloud services across the **Microsoft and SAP ecosystems**, with the assurance, governance and delivery discipline public sector organisations expect. Whether you need stable BAU support, a safe migration, or a change programme to unlock value, we provide a consistent, repeatable approach designed to reduce delivery risk and improve service performance over time.

With **5,000 professionals across 38 offices in 20 countries**, our **UK & Ireland teams** combine local delivery confidence with global capability for scale and specialist reach.



At a glance



Assurance-led cloud services across Microsoft and SAP, shaped for public sector governance and audit needs.



Menu-style Managed Services and cloud support: choose what you need (from break/fix to proactive improvement), with coverage scalable as requirements change (including extended hours/ out-of-hours by agreement).



Delivery and change services across the lifecycle: discovery, design, implementation, migration, integration, testing, training, adoption and optimisation.



Responsible AI by design: where AI-enabled capabilities are introduced, governance and controls are treated as essential foundations (not optional extras).



UK delivery, with data residency options where supported by the underlying cloud service and buyer policy (for example, UK-hosted environments and UK-based operational processes where in scope).

How buyers engage with us

We support both **direct award** and **competitive selection**, depending on your requirement and the route you choose on G-Cloud. Services can be bought as discrete “outcome packages” or combined into an end-to-end plan → deliver → run → improve engagement.

Why delaware



UK & Ireland delivery capability, backed by global delivery centres for resilience, continuity and specialist reach.



Deep SAP heritage, including being one of only **11 Global Platinum SAP Partners** and **RISE with SAP recognition** for cloud migration and modernisation pathways.



Microsoft credentials that support public sector assurance, including all six **Microsoft solution designations**, participation in the **Microsoft Portfolio FastTrack programme**, and recognition as an **Azure Expert MSP**.



Advanced Microsoft specialisations spanning areas such as Adoption & Change Management, Teams Calling, Azure Virtual Desktop, Analytics on Azure, AI, and SAP on Azure.



A consistent delivery method (PROMAR) that makes governance, risk management and quality controls repeatable across projects and Managed Services — giving buyers early visibility, clear decision points and a controlled path into BAU.



Always ahead of the crowd: we are one of the first UK organisations to achieve the new **ISO 42001 (AI Management Systems)**

Why delaware

Managed Services: choose what you need

Delaware provides tailor-made Managed Services. Buyers can select only the components they require and **scale coverage as needs change** -helping avoid paying for unused capability while retaining a clear path to expand support as services become more critical.

Sustainability and social value

We align delivery to the Social Value Model and embed sustainability into how we work — including remote-first delivery by default and practical “green IT” improvements (for example, right-sizing non-production environments and retention/data lifecycle controls). Contract-specific commitments are agreed at mobilisation and reported through governance.



Assurance, security and responsible AI

We operate with an assurance-first mindset, with governance and evidence built into how we deliver and run services. Typical measures include security monitoring and logging aligned to platform tooling (where in scope), BCDR planning with tested runbooks, and responsible AI governance for any AI-assisted delivery.

Pricing and value for money

We aim for transparent, auditable pricing that maps clearly to roles and outcomes, with explicit assumptions and change control to prevent unplanned cost growth. Menu-style service design helps avoid paying for unnecessary coverage, and we use automation and repeatable accelerators to improve consistency and reduce BAU effort where possible.

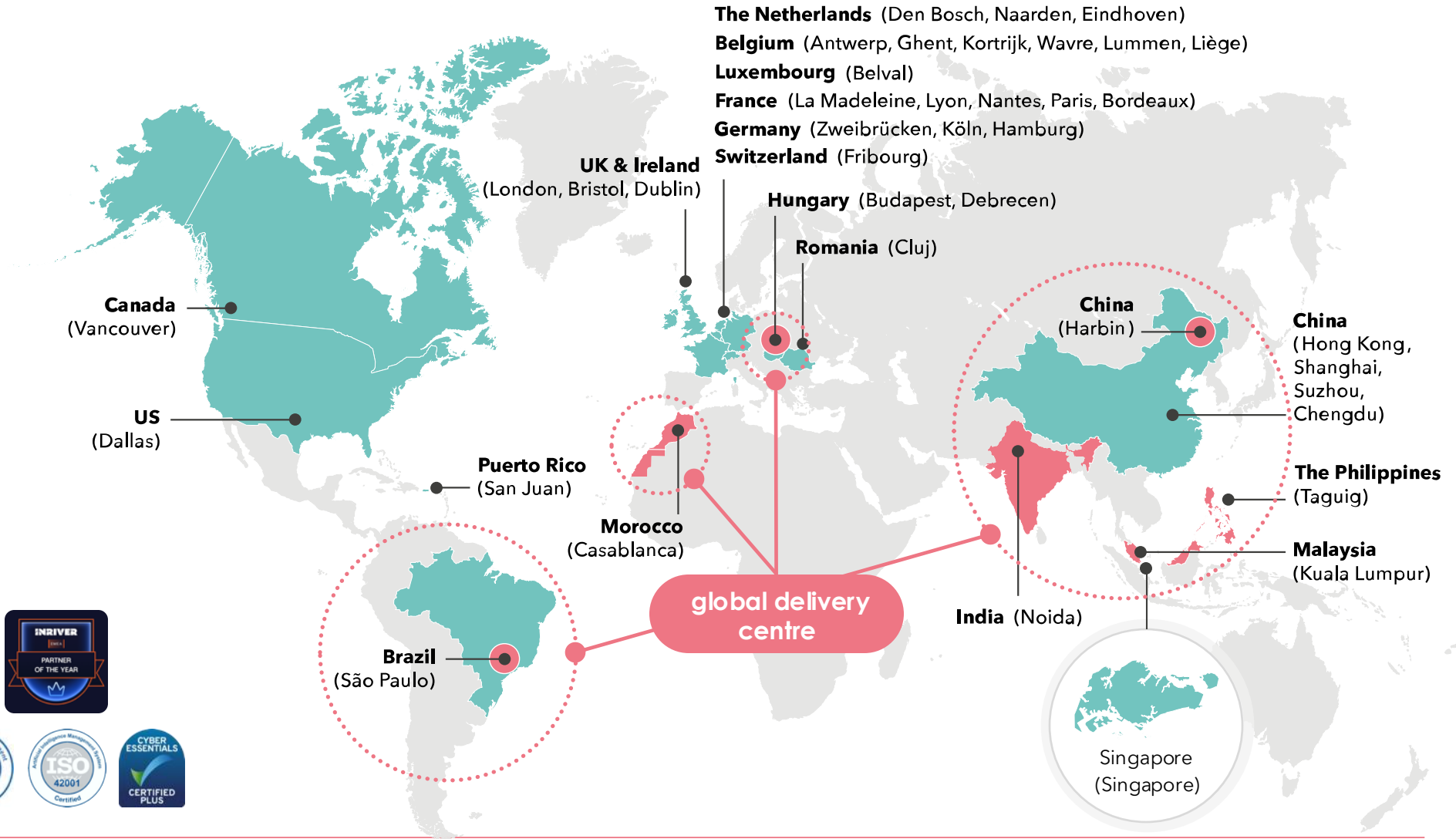
About Delaware

5,000 professionals

38 offices in
20 countries

£500M+
revenue

Our partner ecosystem



Microsoft 365: modern workplace - secure collaboration and employee experience on microsoft 365

A practical, governance-led approach to hybrid working for UK public sector teams.

What we help you achieve

Our Modern Workplace practice helps public sector organisations create a Microsoft 365 based digital workplace that is usable day-to-day, governed properly, and sustainable to run.

Typical outcomes include:

- Secure hybrid collaboration that works across departments, partners and locations
- Reduced operational risk through clear configuration baselines, documentation and ownership
- Better information control (sharing, retention and audit readiness) aligned to your policies
- Improved productivity by simplifying how people communicate, meet and work with content
- A platform foundation for change, including readiness for AI-assisted ways of working in Microsoft 365
- A smoother path into business-as-usual (BAU) with clear handover, runbooks and support enablement



Practice capability overview

Modern Workplace brings together the capabilities required to **plan, implement, govern and improve Microsoft 365 services as a coherent whole** — not as isolated technical changes.

In practice, this commonly spans:



Tenant and identity foundation:

establishing secure access patterns and baseline controls so collaboration operates within the right guardrails



Information governance and auditability:

helping content remain findable, protected and managed through its lifecycle (aligned to your policies)



Collaboration and content services:

implementing and improving services designed around how teams actually work



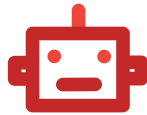
Hybrid access and endpoint patterns:

supporting secure access and consistent policy enforcement across devices and locations (where in scope)



Employee experience layers:

intranet/workhub experiences to support communications, engagement and self-service (where in scope)



AI readiness for Microsoft 365:

readiness-led preparation for AI assistants, focusing on data, permissions, governance and adoption to reduce avoidable risk



Operational readiness:

documented processes, admin enablement and structured hypercare so the service can be operated and improved after go-live

This practice-level approach aligns to delaware's corporate delivery principles - outcome-led delivery, repeatable governance and an assurance-first mindset - while keeping engagement modular so buyers can select the specific service line that matches the outcome they want to procure.

How buyers typically engage this practice

Public sector buyers typically engage Modern Workplace services through a small number of common journeys:



Stabilise and govern an existing Microsoft 365 environment

Improve baseline configuration, governance and day-to-day operability - reducing risk and enabling internal teams to manage change safely.



Enable hybrid working at scale

Secure endpoint and access patterns, repeatable onboarding, and (where required) virtual workspace approaches to support remote access.



Roll out or re-launch collaboration and content services

A structured rollout including policy configuration, content design, migration from legacy file stores (where in scope), and a clear operating model for ownership.



Prepare for AI-enabled working

A readiness-led approach to AI assistants in Microsoft 365 - focusing on permissions, information governance and adoption so benefits can be realised without introducing avoidable risk.



Improve security, information governance and audit readiness

Strengthen identity, access, sharing and information protection controls - especially where external collaboration, retention or reporting requirements drive risk.



Transition cleanly into BAU

Clear handover artefacts, training and a support model so operations remain stable after go-live.

Delivery approach

Modern Workplace engagements follow a structured approach designed to apply **consistent governance, quality gates and risk controls**:



Readiness-led discovery

to confirm goals, constraints and current-state realities (including dependencies across identity, devices and information governance)



Design and decision capture

so the buyer can see and agree the “why” behind policy choices and governance models



Controlled implementation

with clear scope boundaries, configuration baselines and documented assumptions



Pilot and rollout support

(where appropriate) so change is introduced safely and iterated based on feedback



Handover and enablement

including runbooks, admin guidance, support readiness and operational ownership



Optimisation

based on usage insight, operational feedback and governance reviews — not one-off go-lives

“Run and improve” thread (managed service / BAU)

A modern workplace is not “done” at go-live. Buyers typically need a practical path into stable operations, including:

- Clear ownership for configuration, content and lifecycle management
- Incident and request handling patterns aligned to the buyer’s service desk model
- Release/change awareness so Microsoft 365 can evolve without disrupting users
- Regular governance touchpoints to review adoption, risk and simplification opportunities.



Delaware application managed services

Delaware Application Managed Services provide reliable, ongoing operational support for cloud applications and platforms, helping public sector organisations keep services stable, secure, and up to date.

Our managed service model is designed to be:



Predictable and reliable:

clear service processes for incidents, requests, releases and reporting.



Proactive:

continuous improvement, health checks, and insight-led recommendations to reduce repeat issues over time.



Scalable:

service hours can be aligned to operational needs, from standard business hours through to extended and out-of-hours coverage (by agreement).



Cost-effective:

a menu-style approach so buyers can select the support activities they need, rather than paying for unused capacity.

Credibility in practice



Assurance-first delivery:

controls, documentation and governance are built in — not bolted on afterwards



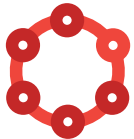
End-to-end coherence:

identity, information, devices, collaboration and adoption are considered together, reducing downstream risk from partial implementations



Public sector fit:

auditability, policy alignment and sustainable BAU operation — not just technical configuration



Reusable patterns:

repeatable baselines, templates and runbooks that support consistency across teams and programmes



Responsible AI orientation:

where AI-enabled working is in scope, governance and guardrails are treated as essential foundations



Evidence-led assurance:

any certifications or partner designations referenced in buyer-facing materials can be evidenced for the contracting entity

Security & Identity for Microsoft 365 (Zero Trust, Entra ID, Defender & Sentinel)

Lot: G-Cloud 15 — Lot 3: Cloud Support

Service type: Security services (assessment, implementation, optimisation)

Platforms: Entra ID, Defender, Sentinel

Service overview

Delaware designs, implements and optimises **Microsoft 365 identity and security controls**. We assess your current posture, configure **Entra ID access controls** (including **MFA**, **Conditional Access** and **privileged access**), and support **Defender** and **Sentinel onboarding and tuning**. We provide **documentation**, **runbooks** and **handover**.

Buyer outcomes

- Stronger identity and access controls to reduce security risk
- Safer remote and hybrid working using Zero Trust patterns
- Improved auditability through logging, alerts and documented controls
- Better security operations through Sentinel dashboards and playbooks
- Clearer processes for triage, escalation and incident communications

What's included

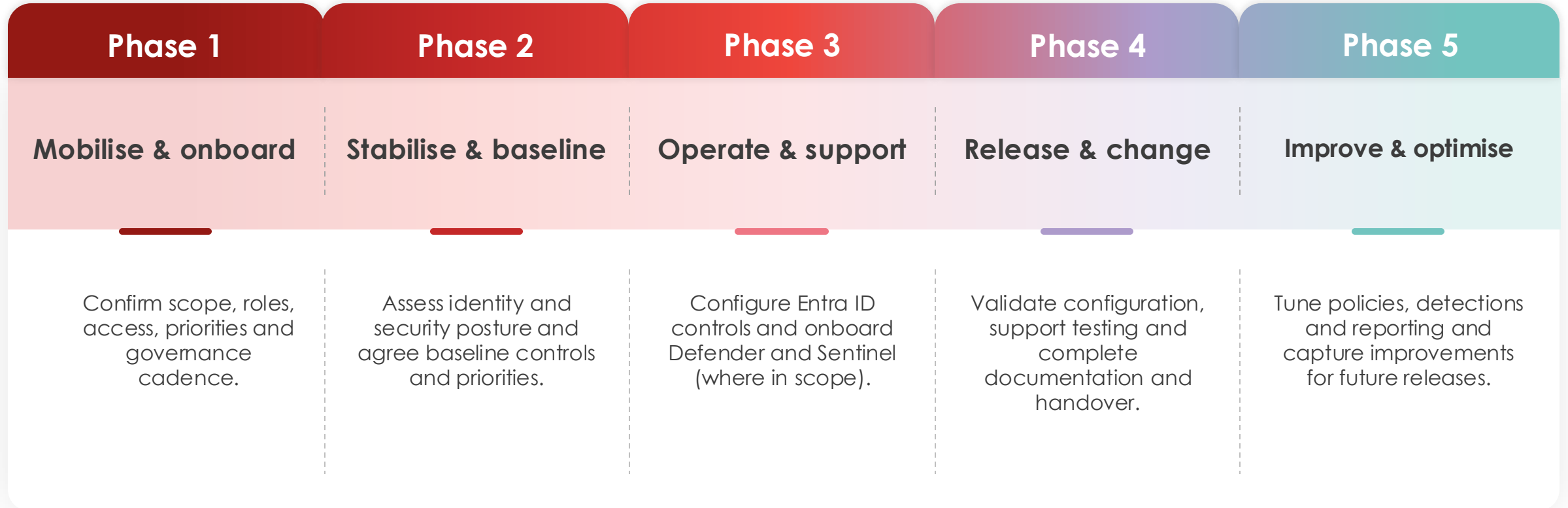
Run & support (BAU)

- Microsoft 365 identity and security posture assessment
- Entra ID configuration: users, groups, roles and access
- MFA and Conditional Access baseline policies and exceptions
- Privileged access management and admin role governance
- Defender onboarding for endpoint, identity and cloud apps
- Sentinel integration: log sources, alerts and playbooks
- Security incident processes: triage, escalation and communications
- Security audits, control reviews and remediation planning
- Documentation, runbooks and handover to buyer teams
- Ongoing optimisation: policy tuning, reporting and recommendations

Improve, assure & optimise (optional modules)

- Additional log source onboarding and detection tuning (where in scope)
- Expanded playbooks and alert triage workflows
- Regular control reviews and improvement backlog
- Targeted security awareness guidance for admins and power users
- Extended hypercare and post-change monitoring
- Managed support options post go-live (at extra cost)

Delivery approach (indicative)



Deliverables (typical)

- Security and identity posture assessment summary
- Entra ID configuration record (roles, groups, access patterns)
- MFA and Conditional Access policy baseline (with documented exceptions)
- Privileged access / admin governance configuration summary
- Defender onboarding and configuration notes (in scope)
- Sentinel onboarding pack (data sources, rules, dashboards, playbooks in scope)
- Incident triage and escalation runbook
- Control review findings and remediation plan
- Handover pack (runbooks, admin guidance)



Support model and service levels



Support channels and hours (baseline)

- **Online ticketing:**
09:00–17:00 UK time, Monday to Friday
- **Phone support:**
09:00–17:00 UK time, Monday to Friday



Support levels (options)

- **Standard Support:** baseline hours and targets above (via online ticketing for service administration and tenant provisioning queries).
- **Extended hours / Out-of-hours support:** by agreement for defined periods or priority incidents only.



Response targets (baseline)

- Ticket acknowledgement: **within 1 business hour** (during service hours)
- Initial response: **within 4 business hours** (during service hours)
- Tickets raised outside service hours are acknowledged by **09:00 UK time next business day**, unless enhanced/out-of-hours support is agreed.



Governance

We provide a named **Service Delivery Manager (SDM)** to oversee service governance, reporting, escalation and continuous improvement.

If you have any questions,
please contact:

James Lear

dlw-uk-enquiries@delaware.co.uk



delaware
we commit. we deliver.