Offshore Delivery POD for Microsoft 365 & Security

Prospient Solutions Pvt Ltd

Executive Summary

Prospient Solutions delivers dedicated Offshore Delivery PODs for Microsoft 365 and Security services, enabling UK and DACH partners to modernise workplace collaboration, strengthen security posture, and ensure regulatory compliance at enterprise scale. Our POD model provides specialist capacity across identity management, endpoint security, collaboration platforms, compliance governance, and managed security operations—helping partners accelerate digital workplace transformation, reduce security risk, and build scalable managed security services offerings while maintaining alignment with European security standards and data protection requirements.

About Prospient Solutions

- **Founded:** 2018

- **Team Size:** 52+ certified consultants with security specialisation

- **Location:** India (with European client focus)

- **Certifications:** ISO 27001 (Data Security & Compliance); Microsoft Security Engineer, Identity Administrator, Compliance Administrator certifications

- **Experience:** Enterprise security and Microsoft 365 consulting since 2012; security operations and compliance focus since 2015

Our team combines deep technical expertise in identity, endpoint security, data governance, and managed security operations with proven ability to deliver to European security standards, including NIS2 compliance, GDPR security requirements, and ISO 27001 frameworks.

Microsoft 365 & Security Specializations

Identity & Access Management (IAM)
- Entra ID (Azure AD) architecture, migration, and governance
- Conditional Access policies and Zero Trust implementation
- Multi-factor authentication (MFA) and passwordless authentication

- Hybrid identity (on-premises to cloud synchronisation)
- Role-based access control (RBAC) and privileged identity management
- Single Sign-On (SSO) and federation strategies

Collaboration & Productivity

- Microsoft Teams deployment, governance, and adoption
- SharePoint Online and OneDrive configuration and management
- Microsoft 365 Groups and modern teamwork enablement
- Collaboration security and data loss prevention (DLP)
- Communication compliance and eDiscovery
- Employee experience and adoption programs

Endpoint Security & Device Management

- Intune device management (Windows, macOS, iOS, Android)
- Mobile Device Management (MDM) and Mobile Application Management (MAM)
- Endpoint Detection and Response (EDR) integration
- Windows 10/11 deployment and management
- Device compliance policies and conditional access
- Remote work security and VPN alternatives

Compliance & Governance

- Microsoft 365 Compliance Centre setup and operations
- Data governance, retention, and lifecycle management
- Information barriers and sensitivity labels
- Audit logging and compliance reporting
- Records management and eDiscovery workflows
- GDPR, NIS2, and industry-specific compliance alignment

Managed Security Services (MSSP)

- Security Operations Centre (SOC) staffing and operations
- Threat monitoring, detection, and incident response
- Threat intelligence and security trend analysis
- Vulnerability management and patch orchestration
- Security awareness training and phishing simulations
- 24/7 security monitoring and alerting

The Prospient Offshore Microsoft 365 & Security POD Model

What is a Microsoft 365 & Security POD?

A Prospient Offshore Microsoft 365 & Security POD is a dedicated, semi-autonomous team of 5–9 specialists assigned exclusively to your organisation. The team works as an

PROSPIENT ®

extension of your security and IT operations teams, aligned to your security strategy, compliance requirements, and business objectives.

Typical POD Composition

Role	Count	Responsibility
Security Architect / Lead	1	Overall security strategy, architecture, governance, technical leadership
Identity & Access Specialist	1–2	Entra ID, Conditional Access, IAM governance, Zero Trust strategy
Microsoft 365 Administrator	1–2	Teams, SharePoint, Exchange, compliance, adoption, governance
Endpoint Security Specialist	1	Intune, device management, EDR integration, mobile security
Compliance & Governance Analyst	1	Compliance policies, DLP, retention, audit, regulatory alignment
Security Operations / SOC Analyst	1–2	Threat monitoring, incident response, security alerting, threat analysis
QA & Documentation Specialist	0.5–1	Testing, validation, security runbooks, documentation

Core Benefits

Benefit	Details
Scalable Security Capacity	Rapidly scale security operations and Microsoft 365 management without permanent headcount.
Cost Efficiency	Reduce onsite security and M365 admin costs by 50–70%; predictable monthly investment.
24/7 Security Coverage	Time zone advantage enables round-the-clock monitoring, incident response, and threat detection.
Expert Access	Access to specialised security architects, compliance officers, and SOC analysts without hiring constraints.
Compliance Assurance	ISO 27001 certified; GDPR, NIS2, and European security standards built into

Benefit	Details
	every engagement.
Reduced Risk	Professional security governance reduces breach risk, improves incident response time, and strengthens posture.
Rapid Deployment	2–3 week onboarding; minimal disruption to existing security operations and business continuity.
Managed Services IP	Package security services as Managed Security Services (MSS) and resell to your customers.

Engagement Models

Model 1: Microsoft 365 Implementation & Migration POD
- **Scope:** Plan, design, and execute Microsoft 365 adoption, migration from on-premises, identity sync, Teams rollout, security configuration.
- **Duration:** 6–18 months.
- **Cost:** Time-and-materials with fixed milestones, or fixed price against detailed scope.
- **Ideal For:** Partners modernising customer IT environments or building managed services capabilities.

Model 2: Managed Security Operations Centre (SOC) POD
- **Scope:** 24/7 security monitoring, threat detection, incident response, vulnerability management, security reporting.
- **Duration:** 12+ months (ongoing).
- **Cost:** Monthly retainer with agreed SLAs for response times and uptime.
- **Ideal For:** Partners offering Managed Security Services (MSS) or building security operations capabilities.

Model 3: Compliance & Governance POD
- **Scope:** Design and operate Microsoft 365 compliance framework, DLP policies, retention, audit, regulatory alignment (GDPR, NIS2, ISO 27001).
- **Duration:** 6–18 months.
- **Cost:** Monthly retainer plus project fees for major compliance initiatives.
- **Ideal For:** Organisations establishing enterprise-grade compliance governance across Microsoft 365 and security infrastructure.

Model 4: Hybrid M365 & Security POD
- **Scope:** Blend of Microsoft 365 adoption/migration, endpoint security management, compliance governance, and ongoing security operations.

- **Duration:** 12+ months with flexible team sizing.
- **Cost:** Combination of project fees, monthly retainer for ongoing operations, and surge capacity.
- **Ideal For:** Growing partners with mixed M365 deployment and security operations demand.

Typical Deliverables

Strategy & Design

- Microsoft 365 and security architecture aligned to Zero Trust and EU security frameworks.
- Identity governance and access management strategy.
- Compliance roadmap aligned to GDPR, NIS2, ISO 27001, and industry-specific requirements.
- Incident response and business continuity plans.
- Security awareness and training strategy.

Implementation & Configuration

- Entra ID setup, synchronisation, Conditional Access policies, and MFA deployment.
- Teams, SharePoint, Exchange configuration with security and compliance controls.
- Intune device management policies and endpoint security configurations.
- Data Loss Prevention (DLP) policies and sensitivity labels.
- Compliance Centre configuration and retention policies.

Operations & Monitoring

- 24/7 security monitoring dashboards and alert configurations.
- Threat detection rules and incident playbooks.
- Vulnerability scanning and patch orchestration.
- Security audit logs and compliance reporting.
- Monthly security briefings and trend analysis.

Governance & Compliance

- Compliance documentation and audit trails.
- Regulatory alignment reports (GDPR, NIS2, ISO 27001).
- Access review and entitlement management processes.
- Data governance and records management workflows.

Training & Enablement

- Security awareness training and phishing simulations.
- Administrator training on Microsoft 365 and security tools.
- End-user adoption training for Teams, OneDrive, security features.
- Incident response drills and tabletop exercises.

Why European Partners Choose Prospient Microsoft 365 & Security PODs

1. **Time Zone Overlap** – Real-time collaboration with European working hours; follow-the-sun security monitoring and support.
2. **European Security Expertise** – Deep understanding of GDPR, NIS2, EU Data Governance Act, and European security standards.
3. **Zero Trust & Modern Security** – Not legacy security; modern architecture aligned to Zero Trust principles and cloud-first security.
4. **Compliance Assurance** – ISO 27001 certified; compliance documentation and audit readiness built into every engagement.
5. **24/7 SOC Operations** – Time zone advantage enables round-the-clock security monitoring and rapid incident response.
6. **Proven Scaling** – Multi-year engagements with European enterprises securing 10,000+ users and managing complex hybrid identities.
7. **Cost-Effective MSS** – Build and scale managed security services without large fixed security team overhead.

Client References & Case Studies

Microsoft 365 Migration & Security – Financial Services Group - Scope: Migrate 3,000 users from on-premises Exchange/AD to Microsoft 365; implement Entra ID, Teams, Intune, Conditional Access. - Result: 95% user adoption in 3 months; 40% reduction in IT admin costs; zero security incidents during migration. - Team: 5-person M365 & Security POD over 12 months; transitioned to ongoing management retainer.

Managed Security Operations Centre – Mid-Market Technology Partner - Scope: Establish 24/7 SOC with threat monitoring, incident response, vulnerability management for 500+ customers. - Result: Average incident response time 12 minutes; 30% reduction in customer security incidents; new MSS revenue stream. - Team: 6-person SOC POD (3 shifts); ongoing 24/7 operations.

GDPR & NIS2 Compliance Programme – European Insurance Company - Scope: Design and implement GDPR- and NIS2-aligned compliance framework across Microsoft 365, Azure, and on-premises infrastructure. - Result: Achieved NIS2 certification; reduced compliance audit findings by 85%; improved data governance maturity. - Team: 3-person Compliance & Governance POD over 8 months; ongoing quarterly reviews.

Endpoint Security & Intune Rollout – Healthcare Organisation - Scope: Design and deploy Intune-managed device strategy for 2,000 users; implement conditional access, DLP, and endpoint detection. - Result: 100% device compliance achieved; security incidents reduced by 60%; HIPAA alignment strengthened. - Team: 2-person Endpoint Security POD over 6 months; ongoing support included.

How to Get Started

1. **Security Posture Assessment** – Evaluate current Microsoft 365 adoption, security maturity, compliance status, and business priorities.
2. **Security & Compliance Roadmap** – Co-design identity strategy, security architecture, compliance programme, and MSS opportunities.
3. **POD Design & Ramp-Up** – Define team composition, responsibilities, SLAs, and engagement model; 2–3 week onboarding.
4. **Pilot Phase** – Execute focused security initiative (e.g., Entra ID deployment, SOC setup, compliance baseline) in 6–8 weeks.
5. **Scale & Optimise** – Expand to full Microsoft 365 adoption, security operations, or managed services based on pilot success; continuous monitoring and improvement.

Technical Stack & Certifications

Microsoft Security & Compliance Technologies

- **Entra ID (Azure AD)** – Identity, access management, Conditional Access, privileged identity management
- **Microsoft 365 Apps** – Teams, SharePoint, Exchange, OneDrive, Outlook
- **Intune** – Device management, MDM/MAM, compliance policies, endpoint protection
- **Microsoft Defender** – Endpoint, Cloud Apps, Identity, Office 365
- **Microsoft Purview** – Compliance Centre, DLP, retention, eDiscovery, information barriers
- **Azure Security Centre** – Cloud security posture management, threat protection

Security Operations & Monitoring

- **Microsoft Sentinel** – Security information and event management (SIEM), threat detection, incident response
- **Azure Monitor** – Logging, alerting, threat analytics
- **Third-party SIEM integration** (Splunk, ArcSight where needed)

Certifications

- Microsoft Certified: Security Engineer Associate
- Microsoft Certified: Identity and Access Administrator
- Microsoft Certified: Compliance Administrator
- Microsoft Certified: Teams Administrator
- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH) or equivalent

PROSPIENT®

Contact & Next Steps

Prospient Solutions Pvt Ltd
Managing Partner: Satish Babu Desikan
Email: satish.desikan@prospient.in
Phone: +91 90957 22200

Let's explore how a Prospient Offshore Microsoft 365 & Security POD can modernise your workplace, strengthen security posture, and build managed security services.

Appendix: Security, Compliance & Data Governance

Prospient is ISO 27001 certified and implements comprehensive security practices:

- **Data Security:** Encryption at rest and in transit; secure key management; multi-factor authentication; Zero Trust principles.
- **GDPR & Data Privacy:** Consent management, data minimisation, privacy-by-design in all M365 and security workflows. Will be working on Partner's GDPR Policy and framework and Governance.
- **NIS2 & EU Security Standards:** Compliance with Network and Information Security Directive; regular security audits and vulnerability assessments.
- **Incident Response:** 24/7 SOC with defined incident response procedures, escalation protocols, and forensic capabilities.
- **Business Continuity:** Disaster recovery and high-availability architectures for security infrastructure; backup and restore procedures.
- **Audit Readiness:** Complete audit trails, compliance documentation, and evidence collection for regulatory inspections.
- **Continuous Improvement:** Monthly security reviews, threat landscape updates, and proactive security enhancement roadmaps.

Document Version: 1.0 | Last Updated: November 2025