TRANSPUTEC

MANAGED SERVICE TRANSITION FOR TEXEL GROUP

The Customer

Texel Group is a specialist credit and political risk insurance broker operating across the UK, Europe, the United States, and Asia. Its people rely on a distributed Microsoft 365 and Azure environment, business applications, and regional infrastructure to serve clients and collaborate across locations.

Texel needed a managed IT services partner that could take responsibility for day-to-day support, infrastructure operations and security, while respecting the distinct requirements of each regional office and of the separate Tierra Underwriting environment.

The Challenges

Switching managed service providers is one of the highest-risk changes an IT function can make. Texel was moving from its incumbent provider to a new managed service model spanning Service Desk, infrastructure operations, monitoring, patching, security, Microsoft cloud services, and service governance. The scope covered a distributed estate of users, endpoints, Azure services, multiple Microsoft 365 tenants and third-party platforms.

A key challenge was coordinating the removal of SentinelOne and the deployment of Huntress, Microsoft Defender, Qualys, and NinjaOne across devices that weren't always online, without leaving any endpoint unprotected during the changeover.

The managed service transition also required clear governance, controlled knowledge transfer, validated support channels, agreed service designs, and evidence-based readiness decisions before Transputec assumed full operational responsibility.

Our Approach

Transputec began with structured technical and process discovery, validating the contracted assumptions against Texel's live environment. Workshops examined Service Desk processes, starters and leavers, governance, security, patching, backup, licensing, supplier management, networks, Azure services, and regional support requirements.

A detailed transition plan and a series of service take-on gates provided the control framework. Regular governance and readiness meetings reviewed risks, actions, dependencies, and decisions, while service designs documented the future operating model for the Service Desk, Service Delivery, SOC, infrastructure,



★★★★★

> Transputec worked with us as a genuine partner throughout the transition. Their team combined strong project governance with detailed technical and process discovery, clear service design, carefully managed tooling deployment, and thorough readiness assurance. Regular workshops and go/no-go reviews gave us confidence that dependencies were being addressed transparently and that the support models for Texel Finance and Tierra Underwriting were practical, well understood, and ready for operational handover.

Chris Murrell, Head of Data & IT Infrastructure, Texel Group

, and starters, movers and leavers.

Our teams transferred knowledge and access from both the incumbent provider and Texel's in-house IT team, configured the Servicely ITSM platform, introduced tailored starter and leaver workflows, validated remote support and prepared clear communications for end users.
Operational tooling was deployed and tested in sequence. NinjaOne established endpoint management, Huntress and Microsoft Defender replaced the previous endpoint security arrangement, and Qualys introduced continuous vulnerability management. Backup arrangements, third-party access, escalation routes and privileged access were reviewed and assigned to named operational owners.

The rollout was controlled through staged go/no-go decisions. A conditional go decision supported the security tooling milestone on 22 September 2026, followed by a period of dual running alongside the incumbent provider. End-to-end testing covered ticket routing, remote access, user consent, security coverage and regional support before Texel and Transputec agreed on the final go decision on 28 September.

The Outcome

Texel entered full managed service on 29 September 2026 with agreed support channels, trained resolver teams, approved service designs, and operational governance in place. Service Desk, remote support, monitoring, endpoint management, vulnerability management, and SOC capabilities were all validated for live operation before cutover.

The transition replaced fragmented knowledge and single-provider dependencies with documented processes, named ownership and measurable service controls. The result is a governed, scalable managed IT service with clearer visibility of incidents, assets, security events, and service performance. Remaining improvement activities are now managed through business-as-usual governance rather than left behind as unowned transition tasks.