

REBUILDING A CRITICAL IT ESTATE UNDER TIGHT DEADLINES

Client: Aspect Maintenance
Project: Infrastructure Recovery & Modernisation



Client

Aspect Maintenance is a leading property maintenance provider operating across London, the South and East of England.



Founded in 2004, it supports over 10,000 businesses with 24/7 services spanning plumbing, electrics, roofing, drainage and fire safety, delivered through a fleet of 300+ vans.

Key takeaways

Central's partnership with Aspect Maintenance transformed a high-risk, low-visibility IT environment into a stable, secure, and strategically aligned platform.

Key outcomes include:

- Full restoration of control and visibility for internal IT
- Replacement of core server infrastructure in a month
- Replacement of entire network without disruption
- Implementation of security and disaster recovery services; 24/7 MDR, user awareness training and full back up across M365, Entra ID and Salesforce
- Starters and leavers process overhauled, eliminating a major recurring burden on HR and IT
- M365 Licence Optimisation
- A clear, cloud-aligned strategy to support future growth

<1mo

Full server
infrastructure
replaced

450+

Users
migrated, zero
disruption

~200

Devices
deployed in
under a week

24/7

MDR security
monitoring in
place

Overview

Aspect Maintenance engaged with Central at a key point in their IT journey, where there was a clear opportunity to improve visibility, control and scalability across the environment. With a growing user base and a 24/7 operation, the demands on IT were increasing. Pavlo, the IT manager, had a strong vision for how technology could better support the business, but realising that vision required a more structured, transparent and collaborative operating model.

Following a competitive tender, Central was selected to take over. What followed was a time-critical transition, requiring rapid action to avoid service disruption and rebuild the IT estate while establishing a long-term, scalable operating model.

This engagement was not a standard onboarding, it required Central to take control of a restricted environment, operate under significant time pressure, and rebuild critical infrastructure while maintaining business continuity. Central also needed to rebuild trust at every level, from Pavlo and internal IT to end users, many of whom had lost confidence in external support and defaulted to internal teams. The outcome was not just a change of provider, but a complete reset of how IT supports the business in its growth ambitions.

Challenge

Pavlo understood the changes the business needed, but the limitations in how the environment was structured and accessed meant internal IT could not execute those plans with the speed, control or confidence required. The incumbent provider had restricted administrative access, meaning their internal IT team were unable to make changes, troubleshoot effectively or fully manage the systems they were responsible for.

Once Central gained access, the true scale of the challenge became clear. The environment was significantly larger than initially scoped, and critically, all on-site infrastructure was owned by the outgoing provider. This included servers, SAN, and network equipment across the entire company, as well as a large estate of end-user devices.

With less than one month before service withdrawal, Central had to replace, configure and set up:

- New servers and SAN
- Full network infrastructure, including switches and access points
- Approximately 200 laptops and desktops

All while ensuring continuity for more than 450 users. This created a very real risk of business disruption across the entire organisation. Compounding this, the outgoing provider was uncooperative throughout. Central took full ownership of this process, engaging the incumbent directly through a combination of formal requests, persistent negotiation, and escalation where necessary. Rather than placing that burden on the internal team, Central absorbed the operational friction entirely, ensuring the project could continue to move forward without stalling.

Alongside these immediate risks, Aspect needed a practical long-term direction that could finally be delivered. The environment was heavily reliant on on-premise systems, with the existing cloud ambitions, optimisation priorities and growth roadmap unable to progress under the previous arrangement. Moreover, following the previous support model, many users had lost confidence in external support and would default to internal IT, making it critical to demonstrate that Central were accessible, responsive and there to support them directly.

Solution

Central delivered a structured, multi-phase response that addressed immediate risk while establishing a long-term, scalable IT strategy.

Phase 1: Stabilisation

The first priority was gaining control. Engineers were deployed on-site to rapidly assess the environment, recover access, and build a clear understanding of infrastructure, dependencies, and risks.

With the scale of the challenge clear, Central moved quickly to replace critical infrastructure. As existing hardware was not owned by Aspect, new servers, SAN, and network equipment were designed, deployed, and configured within a matter of weeks. This included a full network refresh across the site, covering switches and access points, ensuring the business had a stable and fully owned foundation moving forward.

At the same time, Central delivered a large-scale device rollout. Around 200 laptops and desktops were deployed all made possible by the implementation of Microsoft Intune and autopilot, enabling rapid configuration and consistent security policies. This allowed the deployment to be completed in under a week, significantly reducing disruption to users.

Phase 2: Security

Security was addressed as a core priority and a layered approach was introduced, including Managed Detection and Response across all 450 users, alongside user awareness training and comprehensive backup solutions covering Microsoft 365, Entra ID, and Salesforce. This shifted Aspect from a reactive security posture to a proactive, continuously monitored model.

A defining element of the engagement was the move to a co-managed operating model. Rather than replacing the internal IT function, Central worked alongside the internal team to restore full administrative access, establish shared ownership of systems, and provide integrated 1st, 2nd, and 3rd line support. This removed the dependency on a single provider and enabled internal IT to operate with confidence and control.

Alongside the technical work, Central placed a strong emphasis on rebuilding user trust, providing visible, responsive support and encouraging users to engage directly with the service desk, rather than defaulting to internal IT.

Phase 3: Strategy

Governance and transparency were also rebuilt. Clear documentation, improved reporting, and structured processes replaced the previous setup. Commercially, pricing was simplified and aligned to actual usage and business value, giving leadership confidence in IT spend.

Beyond stabilisation, Central introduced a clear strategic direction. A roadmap was developed to define which systems should move to Azure, which could be decommissioned, and how the organisation could reduce its on-premise footprint over time. This ensured that the transformation was not just reactive, but aligned to a modern, cloud-first future.

A full Microsoft licence review was also conducted, this review looked at feature usage as well as licence utilisation highlighting over subscriptions and areas where additional features were available at no charge. This review gave Aspect significant cost savings across their licences without losing any additional features.

Outcomes

Business risk removed

The most immediate outcome was the removal of business risk. Aspect successfully avoided service disruption during the transition and moved onto reliable and secure infrastructure it controlled. What had been a high-risk situation was stabilised within weeks.

Commercial clarity & savings

From a commercial perspective, the organisation now benefits from both cost savings and clarity.

Full IT control restored

Control was fully restored to the internal IT team, they now have complete visibility of the environment, the ability to make changes, and the confidence that comes from working in a collaborative, co-managed model. Rather than being restricted by a provider, they are now supported by one. User trust in IT support has also been re-established, reducing reliance on internal teams.

Security strengthened

Security across the organisation has been significantly strengthened. With a 24/7 MDR in place, improved user awareness, and robust backup solutions, Aspect is far better protected against evolving threats, with reduced operational burden internally.

Starters & leavers automated

Prior to Central's involvement, there was no formal starters and leavers process. Account creation was handled manually, draining IT resource and causing a bottleneck for HR — a compliance risk and recurring drain at Aspect's scale.

New starters are now provisioned automatically to a defined standard. When someone leaves, access is revoked promptly and completely, reducing cyber risk. Neither team needs to actively manage the process. Both HR and IT have reclaimed time previously lost to ad hoc requests and manual administration.

Clear path forward

Perhaps most importantly, Aspect now has a clear path forward. With a defined cloud strategy and Azure roadmap in place, the business is no longer reacting to immediate challenges but proactively planning for growth, scalability, and long-term success.

All of this is underpinned by an ongoing, SLA-backed support relationship, with Central continuing to provide 1st, 2nd, and 3rd line support as Aspect's long-term IT partner.

“From the outset, Central approached our engagement as a true partnership. What stood out to me was their willingness to understand the business, the challenges we were facing, and where we wanted to get to in the future. They quickly became an extension of our team, working alongside us to provide the expertise, capacity and support we needed during a particularly critical period.

Throughout our engagement, the team has been responsive, transparent and easy to work with. They have always been willing to take ownership, provide clear guidance and work collaboratively to find the right solutions, regardless of the challenge. The level of communication and visibility they provide has given us confidence that we always know where we stand and what comes next.”

Pavlo Manko, IT Manager, Aspect