

How an Aerospace Manufacturer Modernized its IT Stack with SPK Managed Services

For a midsize aerospace manufacturer, technology is the backbone of production. It runs the ERP system that schedules the shop floor, the SOLIDWORKS PDM vault that holds engineering data, and the remote desktops that connect global teams. When that infrastructure is reactive, fragmented, or loosely secured, the risk reaches far beyond the IT department.

THE CHALLENGE

While this manufacturer's internal team had begun migrating infrastructure into Microsoft Azure, they lacked deep cloud infrastructure experience. Modernization was the goal, but their day-to-day workload left little room to grow their knowledge. In addition to this, the company was unhappy with its current managed services provider (MSP). Cost was one concern. The larger complaint was that the MSP was reactive rather than strategic and forward-thinking. The manufacturer wanted a partner who would anticipate needs, not just close tickets.

~72% Savings on Server Infrastructure

2 Cloud Providers Consolidated to 1

Up to 152 Staff Hours Saved per Year

Several underlying issues made the situation more urgent:

- **A single point of failure.** The company ran a largely traditional network with servers on-premises. Critical systems depended on the local network staying up.
- **A split cloud environment.** Engineering applications ran in one cloud, while IT systems were moving to another. This added cost, complexity, and management overhead.
- **A basic security posture.** Microsoft 365 security lacked conditional access policies and enforced multi-factor authentication (MFA). Access controls were largely open.
- **Global, remote collaboration.** Teams in the US and the Middle East relied on an existing Azure Virtual Desktop (AVD) environment to work together. That environment needed secure, reliable support.
- **A stretched internal IT team.** IT staff spent most of the day deskside, supporting users across the facility. They had little time to learn Azure, Entra ID, or infrastructure maintenance as issues came up.

Without a capable partner, the manufacturer's own staff would carry the burden of researching and implementing new IT solutions, at a higher cost. The business would also be left managing a more complex, two-cloud environment. Fortunately, SPK had already supported this organization's SOLIDWORKS PDM environment for years, and that track record had built deep trust. The manufacturer's request was simple: expand the scope of the engagement.

© 2026 SPK and Associates. All rights reserved.

THE SOLUTION: GETTING FULL VALUE FROM BEST-IN-CLASS TOOLS

Our work had a good foundation, as the manufacturer already owned best-in-class tools. They simply weren't being used to their full potential. Rather than layering on new platforms, SPK focused on helping the company get more from the investments it had already made.

A dedicated five-person SPK team completed the official handoff from the incumbent MSP within one month. From there, we built a prioritized backlog of work. Priorities combined the business needs SPK identified with the pain points the manufacturer's team raised directly. SPK worked closely with stakeholders across the business, including the COO, VP of Operations, and members of the IT department.

The engagement now spans eight core service areas:

1. **SOLIDWORKS PDM Application Management.** The foundation of the relationship. SPK provides ongoing application support, configuration, customization, help desk, patching and upgrades, and vendor liaison.

2. **Microsoft Azure Cloud Infrastructure.** SPK manages the company's Azure environment and moved critical infrastructure, including the IQMS ERP system, into Azure. We also support the Azure Virtual Desktop environment and manage platform changes such as Azure VPN Gateway SKU retirements and upgrades.

3. **24/7 Infrastructure Monitoring.** Using Zabbix, SPK monitors key servers around the clock, including the domain controller, the SOLIDWORKS PDM server, an IQMS test server, and a Linux proxy server. This monitoring has detected and resolved multiple P1 heartbeat alerts and disk space warnings.

4. **Cybersecurity with Huntress EDR and Microsoft Defender.** SPK manages Huntress endpoint detection and response, reviews monthly and quarterly threat reports, and resolves escalations when Microsoft Defender flags endpoints. SPK also rolled out Huntress phishing simulation training. Employees who click a simulated phishing email are routed to a short training video.

5. **Microsoft 365 and Entra ID Administration.** SPK implemented Microsoft Conditional Access Policies (CAPs). These dynamic policies allow sign-ins only under defined conditions. For example, because the workforce is based in the U.S. and the UAE, logins from other locations are blocked unless an exception is requested. SPK also enforces MFA and acts on Microsoft security advisories that affect the company's Entra Connect Sync configuration.

6. **Email Security and Backup.** SPK hardened the company's DMARC policy from "quarantine" to "reject," so spoofed messages are refused outright. We also use afi.ai to back up the Microsoft 365 environment.

7. **SSL Certificate Management.** When a wildcard certificate expired, SPK handled the SSL certificate renewal for the company's IoT domain.

8. **Data and Reporting Enablement.** SPK helped the IT team set up a Power BI on-premises data gateway. This enables more advanced reporting on IQMS data.

© 2026 SPK and Associates. All rights reserved.

THE OUTCOME: A LEANER, MORE SECURE, STRATEGICALLY MANAGED IT STACK

By expanding its partnership with SPK, the manufacturer replaced a reactive support model with a strategic one. Critical systems now run in a single, actively managed cloud environment. Security controls protect the business without slowing down legitimate users, and the internal IT team can stay focused on supporting people on the floor.

"It's been an awesome partnership. SPK is constantly bringing new things to us to consider because they understand our business. I feel very comfortable that our team is in good hands with SPK."

Chief Operating Officer

~72%
Savings on Server Infrastructure

2 to 1
Cloud Providers Consolidated

Up to 152
Staff Hours Saved per Year

SPK helped them achieve:

- **~72% Savings on Server Infrastructure:** SPK implemented Azure reservations for high-uptime servers, cutting those infrastructure costs by roughly 72%.
- **2 Cloud Providers Consolidated to 1:** Engineering applications and IT systems now run in a single cloud, reducing complexity and management overhead.
- **Up to 152 Staff Hours Saved per Year:** By taking on Azure management, Entra ID administration, and infrastructure maintenance, SPK saves the internal IT team an estimated 1-3 hours per week.
- **Lower Licensing Costs with Monthly Flexibility:** Through SPK's Microsoft partnership, the company pays for Microsoft licenses monthly at annual pricing. Month-to-month billing typically runs about 20% higher, so the company gains flexibility without the premium.
- **A Hardened Security Posture:** The company moved from basic Microsoft security with no conditional access or enforced MFA to a tailored, secure configuration. It keeps intruders out while minimizing disruption to legitimate users. DMARC enforcement, EDR, Microsoft 365 backup, and ongoing phishing training add further layers of protection.

© 2026 SPK and Associates. All rights reserved.