CASE STUDY

Aerospace Defense Manufacturer Achieves CMMC Level 2 Compliance with Custom MSP Support

SENTINELBLUE

CASE STUDY QUICK FACTS

WIN-TECH INC

CLIENT TYPE/INDUSTRY

Precision Aerospace Manufacturing

LOCATION

Kennesaw, Georgia, U.S.

SERVICES

GCC High migration

Security governance

Software & hardware upgrades

Employee training

CMMC Level 2 assessment prep

vCISO advisory

Scalable, Compliant Cybersecurity Support for Precision Manufacturing Company Win-Tech

Win-Tech Inc., a defense manufacturer and AS9100-certified aerospace machine shop, needed to improve its cybersecurity posture. As a small government contractor with fewer than 50 employees, Win-Tech lacked the resources for a full-time IT or security department but still needed a way to respond to increasing regulatory requirements and a rise in cyberattacks. The company sought an MSP with deep knowledge in defense industry compliance, IT, and cybersecurity to support their strategic growth.

In order to continue doing business with the federal government and making competitive contract bids, Win-Tech also needed CMMC certification. The company initially hired a commercial managed service provider (MSP) to help with their immediate IT and security needs, such as patching and system monitoring.

It soon became apparent, however, that commercial MSPs cannot always provide tooling to meet federal cybersecurity standards or deep insights into defense industry compliance. Win-Tech turned to Sentinel Blue to update their IT and cybersecurity infrastructure, migrate to a secure Microsoft environment, and earn their CMMC certification.

The Solution: A Compliance- and Growth-Based Cybersecurity Partnership

Seamless GCC High Migration

Sentinel Blue began by migrating Win-Tech's system to Microsoft Government Community Cloud (GCC) High, the ultra-secure, physically isolated cloud environment built for federal agencies and defense contractors. GCC High was the right choice for Win-Tech for several reasons, including the ability to introduce multi-factor authentication (MFA) to essential workflows and a critical baseline aligned with strict compliance requirements like CMMC 2.0.

Next, Sentinel Blue coordinated with Win-Tech's previous MSP to transition IT operations and security governance, enabling full-service delivery and vCISO advisory support. Throughout the transition, deliberate steps were taken to help Win-Tech adapt to architectural changes while minimizing disruption to day-to-day workflows.

Defining Compliance Goals and a Security Mindset

To help set CMMC compliance goals that made sense for Win-Tech, Sentinel Blue performed a detailed gap analysis and proposed a variety of scalable solutions ranging in cost and effort. Clear milestones were established to keep Win-Tech on track without overwhelming its leaders, and big-ticket needs were identified in advance to help with budgeting. Mitigation strategies were implemented with a mindset of progress, not immediate perfection.

Sentinel Blue also imparted its core philosophy on effective compliance: When agile, appropriate security processes and plans are 1) informed by thorough risk assessment and 2) implemented and documented carefully, compliance is an almost-inevitable outcome. With a strong risk-based approach, Win-Tech was able to prioritize what made sense for its business while preparing for CMMC certification.

> During the migration to GCC High, Sentinel Blue anticipated my employees' reactions to changes in their environment and helped to communicate and offer resources in advance. This type of planning ahead ensured that the migration ran as smoothly as possible.
> **– Allison Giddens**, Co-Owner, Win-Tech

Risk Management Tailor-Made for Manufacturing

Securing workflows that have been engrained in Win-Tech's production processes for years required Sentinel Blue to develop specific, creative, and compliant solutions. Older industrial machines, for example, only communicated with antiquated workstation systems that no longer supported necessary versions of Windows operating systems. With the compounded complexity of unique on-prem applications and many employees sharing a single workstation, simple practices like USB flash drive data transfers between workstations and CNC machines created more layers of risk.

Sentinel Blue has extensive experience tackling the challenges specific to manufacturing environments, so the team was able to support Win-Tech in evolving their security practices and ensuring compliance without significantly disrupting work or slowing down production.

Up-Leveling IT Maturity

Sentinel Blue took a number of steps to advance Win-Tech's IT and cybersecurity maturity and provide critical day-to-day technical support.

- **Hardening flat networks:** Sentinel Blue redesigned networks developed over 30+ years, often pieced together along the way, and hardened for swift and direct implementation of wireless printers within the main network. To meet the client's preferences, efforts were made to mitigate risk in some areas and completely remove identified risk in others.

- **Implementing enterprise-grade resources on an SMB budget:** Sentinel Blue not only provided cloud-based services that are generally reserved for enterprise clients; we also provided continuous monitoring of those services and ensured minimal to no disruption to everyday business during the migration process.

- **Upgrades for old hardware:** Major pieces of equipment like network switches were replaced with Sentinel Blue's recommendations.

- **In-depth, ongoing phishing training and reporting:** Along with developing training tools to help employees gain awareness of common threat vectors, Sentinel Blue implemented company-wide practices to help employees report phishing emails and to immediately block malicious senders based on those reports.

> Sentinel Blue is our sounding board. I can go to Andy Sauer and say, 'In the next 12-16 months, I may want to consider migrating to a cloud-based ERP. What should I consider when I'm shopping for that?' Andy will tell me things I didn't think to ask. He is a translator between business risk and security risk that is invaluable to a small business in the DIB.
> **– Allison Giddens**, Co-Owner, Win-Tech

Key Outcomes: Improved Security, CMMC Success, and Consistent Cyber Support

CMMC Certification

Win-Tech not only successfully achieved their CMMC Level 2 certification in Spring 2025; they were also one of the first 300 contractors in the country to be certified. As early adopters of CMMC, they have a competitive edge in the defense marketplace and were proud to achieve certification on their first try.

Up-to-Date Expertise on All Things Compliance

By staying ahead of geopolitical developments, regulatory changes, and DIB requirements, Sentinel Blue provided Win-Tech with timely insights and greater confidence in their cybersecurity posture. With a deep understanding of federal compliance requirements, Sentinel Blue tackles SMB challenges head-on to ensure business growth and cybersecurity integrity for its clients.

> I've gone through AS9100 audits for nearly two decades, and I figured CMMC would just be like that. But it was completely different, and I'm glad SB was leading us on this. CMMC assessments are much more black and white, and the level of technical expertise needed is high. I was confident that since SB had experience in the CMMC realm, we'd be fine – and I was right."
> **– Allison Giddens**, Co-Owner, Win-Tech

Ready to Get to Work?

Reach out to us at sentinelblue.com/contact

SENTINELBLUE