SENTINELBLUE

CASE STUDY

Cybersecurity Partnership Prepares Win-Tech, Inc., a Small Business Defense Manufacturer for Scalable, Compliant Growth

BACKGROUND

Win-Tech, Inc., a small business aerospace and defense manufacturer and government contractor in full growth mode, recognized the need to improve its cybersecurity posture due to the increase of regulatory compliance requirements, rise in cyber attacks, and noticeable constraints and across the board IT support. An organization with fewer than 50 employees, Win-Tech lacked the resources for a full-time IT and Cybersecurity department, along with a solid understanding of defense industry compliance requirements. It was clear that an external consultant was needed, and the consideration of engaging a compliance-driven MSP became essential in strategically scaling for competitive contract bids.

Win-Tech sought to improve its cyber readiness and achieve compliance and implement modern cybersecurity tools to secure its data. In order to be able to continue to do business with the federal government, the company initially hired a commercial-focused MSP to help with the more substantial IT and Cybersecurity needs such as patching and system monitoring. It became apparent, however, that in strategic compliant conversations, commercial MSPs do not always focus on government contracting defense regulations, or understand how they work, when discussing compliance with frameworks such as CMMC.

The idea of changing MSPs and potentially making significant and expensive enhancements to the company's infrastructure was daunting. Critical considerations such as cash outlay and the impact to day-to-day business workflow were of particular concern.

THE BEGINNING

HOW DID THE MSP / SMB RELATIONSHIP START?

After researching the government contracting community and identifying several MSPs with deep experience and knowledge in the defense space, Sentinel Blue, a defense contractor focused MSP was selected to create a hybrid architecture utilizing Win Tech's existing on-premises infrastructure with Microsoft 365 GCC High. GCC-High was the right choice for Win-Tech for several reasons, including the enablement of making multi-factor authentication part of essential workflow and email security as a baseline.

THE SOLUTION

CYBERSECURITY PARTNERSHIP ENABLING GROWTH AND COMPLIANCE PREPARATION

Following the initial GCC-High integration, Sentinel Blue worked with Win-Tech's existing MSP to transfer IT and security governance, and assumed responsibility of the Covered Contractor Information System, serving as vCISO and full-service MSP.

Sentinel Blue performed a gap analysis and proposed a variety of solutions designed to scale with Win-Tech's business operations while supporting the CMMC Level 2 requirements. Identified risks were documented and analyzed. Mitigation strategies were implemented with the focus on progress and not immediate perfection. Steps were taken to allow Win-Tech to integrate the architectural changes into the culture of the organization, mitigating potential disruption in workflow and product realization.

Sentinel Blue's position is that security is propelled by risk awareness, with compliance serving as the tangible outcome of effectively executed security protocols and strategies. This entails showcasing a grasp of the agile adjustments required in the alignment of Win-Tech's cybersecurity planning and philosophy. Finding a partner that took the same risk-based approach enabled Win-Tech to prioritize what made the most sense for its business.

Supporting Win-Tech's IT, Cybersecurity program, and day to day technical support included:

- **Replacement of old hardware:** Major pieces of equipment, like network switches, were budgeted and replaced. Sentinel Blue's industry and regulatory expertise made Win-Tech confident in the recommended choices.
- **Hardening flat networks:** Redesigning networking developed over 30+ years, often pieced together along the way, and hardened for swift and direct implementation of wireless printers within the main network. Efforts were made to layer the network and mitigate unacceptable risk in some areas and completely remove identified risk in others.
- **Creative solutions to mitigate risk:** Implementing specific, compliant solutions to secure workflows ingrained in production operations for decades and enabling for flexible operational changes that do not impact business continuity and growth.

> "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, WIN-TECH'S CO-OWNER**

For example, older industrial machines only communicate with workstations that host antiquated systems that no longer supported versions of Windows operating systems. With the compounded complexity of many employees sharing a single workstation, simple practices such as data transfer, which may happen via USB flash drives between workstations and CNC machines created more layers of risk.

Sentinel Blue was able to support Win-Tech with creating and evolving security practices and ensuring compliance without significantly disrupting work and negatively affecting production.

- **In-depth, on-going phishing training and reporting:** Along with developing training tools to help employees gain awareness on hacking techniques in the industry, Sentinel Blue implemented company-wide essential practices where employees at Win-Tech actively report phishing emails, thus allowing for the immediately blocking of malicious senders and threats, and proactive analysis of those threats.
- **Developing enterprise-grade resources to SMBs often reserved for businesses with larger budgets:** Sentinel Blue provided cloud-based services that are generally reserved for enterprise clients, and monitored as part of the managed service practice offered to SMBs designed for minimal to no disruption to everyday business flow during the migration.

THE SENTINEL BLUE DIFFERENCE

WHAT SETS THE SENTINEL BLUE PARTNERSHIP APART FROM OTHER MSPS?

Sentinel Blue has been actively engaged in industry as a leading small business practitioner and is particularly empathetic to the challenges SMBs face in the Defense Industry Base. With a deep understanding of evolving compliance requirements, leading cybersecurity practices, and creating solutions for small business-specific challenges, Sentinel Blue is passionate about staying engaged in the small business community, maintaining a compliance program focused on scalability and growth that impacts the IT and cybersecurity integrity for its clients.

READY TO GET TO WORK? SO ARE WE.

Contact info@sentinelblue.com to get started. We want to learn more about your IT and cybersecurity needs so let’s get the conversation started.