

CASE STUDY

Navy Contractor Achieves CMMC
Level 2 Without Slowing Down the
Shop Floor



SENTINELBLUE

CASE STUDY QUICK FACTS



CLIENT TYPE/INDUSTRY

Specialty Manufacturing

LOCATION

Huntington, West Virginia, U.S.

SERVICES

SOC-as-a-Service

CMMC Level 2 assessment prep

Tailored cybersecurity strategy

GCC High migration

vCISO advisory

Change management support

Real-World Compliance Challenges in Manufacturing

Level 1 Fasteners, a West Virginia-based specialty fastener manufacturer and defense contractor, needed to strengthen its cybersecurity posture and achieve CMMC certification. With more than 60 years of experience producing certified fasteners, Level 1 serves customers in military, aerospace, medical, and other highly regulated industries.

When the challenge of implementing NIST 800-171 landed on one team member's plate, the company turned to outside help. Previous attempts with local MSPs and consultants went nowhere, since most didn't understand CMMC or weren't able to take on the complexity of a manufacturing environment. Level 1 had been managing compliance, IT, and security across multiple providers, but what they needed was one partner with true DIB expertise and support they could rely on. Sentinel Blue delivered both.



Most MSSPs that deal with CMMC environments have never experienced the challenges of a machine shop. Their idea is to just update your machines so they can run the right software, but that's not always possible. At the same time, CMMC is giving you 300 pages of technical requirements to figure out on your own. Having Sentinel Blue explain all the technical details and how they apply to our environment was the support we needed when we were drowning."

– **Amanda Webb**, Information Systems Security Officer, Level 1 Fasteners



The Solution: Purpose-Built Cybersecurity for a Busy Machine Shop

Modernizing an On-Prem Environment

Sentinel Blue began by migrating Level 1 Fasteners from an almost entirely on-premises infrastructure to an ultra-secure hybrid environment anchored by Microsoft Government Community Cloud (GCC High). The transition introduced a new firewall configuration, remote monitoring and management (RMM) tools, and controls to lock down external device access, replacing what had previously been an informal trust system with consistently rigorous protocols. Beyond the core engagement, Sentinel Blue also delivered vCISO advisory services, including tabletop exercises that put Level 1's team in realistic incident scenarios to surface gaps and clarify responsibilities.

Real-Time Threat Detection with SOC-as-a-Service

Sentinel Blue's dedicated SOC team added significant visibility and responsiveness to Level 1's existing security measures. The Overwatch SOC-as-a-Service delivered a comprehensive, fully managed stack covering everything from endpoint protection and vulnerability management to email security, identity and access management, and backup and disaster recovery.

To date, Sentinel Blue's continuous monitoring capabilities have flagged several serious incidents, including accidental malware downloads and phishing emails designed to harvest Microsoft credentials. Thanks to the SOC team's deep industry expertise, these threats were flagged and action was taken before damage was caused.

Tackling Compliance Challenges in a Machine Shop Environment

Achieving CMMC Level 2 in a specialty manufacturing environment comes with challenges that most MSPs have never encountered. Level 1's shop floor presented a number of them: dozens of operators sharing workstations, IOT devices with visibility blind spots, a harsh environment that accelerated wear on hardware, and legacy machines (including one dating back to the 1930s).

Another reality for this manufacturing environment was the volume of printed CUI (Controlled Unclassified Information). Sentinel Blue worked to eliminate printed CUI where possible, which meaningfully reduced the compliance scope. For what remained on paper, including files for specific customers that still required pen-and-ink signatures, Sentinel Blue suggested starting points for a physical security strategy.

Finally, for legacy systems that couldn't be replaced, including a half-million-dollar machine running on Windows 7, Sentinel Blue helped determine what could be moved to a separate VLAN, what could be removed from the network altogether, and what could be configured to operate within the GCC High environment.



Supporting Change Management Across the Organization

In a small business where processes have been in place for years, achieving CMMC compliance isn't just about implementing technical controls. When internal advocacy wasn't enough to get buy-in on some specific updates, Sentinel Blue stepped in directly. Having a trusted expert there to clearly and credibly explain the stakes proved to be the ticket to getting the final necessary changes adopted before assessment.



When we needed to make security changes, it could take months to get everyone aligned internally. Finally Andy came in and said, 'Here's what you need to do, otherwise you're not going to pass your assessment.' He had the expertise to persuade the team and get things moving quickly."

– Amanda Webb, Information Systems Security Officer, Level 1 Fasteners

Key Outcomes: CMMC Certification, Improved Processes, and Ongoing Peace of Mind

CMMC Certification

Level 1 Fasteners passed their CMMC Level 2 assessment on the first attempt. They estimated that certification would take several years to prepare for independently; with Sentinel Blue, they were able to cut that time to three months. Because Sentinel Blue handled both the technical control implementation and the policy documentation, Level 1 was well prepared when it came time for certification.



I was super stressed out about the assessment, but Andy was on the call with me, and he made it so simple. I assumed we'd have at least a week of dealing with the assessors. It was a day and a half. Andy handled almost everything, and whenever it came time for my part, I was already prepared with what was required."

– Amanda Webb, Information Systems Security Officer, Level 1 Fasteners



Operational Improvements Beyond Compliance

Although it initially met some internal resistance, the move away from printed CUI turned out to be a genuine operational improvement for the company. Paper documentation that was once difficult to read became digital, searchable, and tied directly to manufacturing jobs in the system. Similarly, the GCC High implementation improved security across the board for the sales team.

Reliable, Ongoing Support

Achieving CMMC certification was a milestone but not a finish line. Level 1 now has a long-term partner to help them maintain compliance through future assessment cycles and stay ahead of evolving regulatory requirements. Sentinel Blue is also helping the company plan strategically for what comes next, including a potential move away from their remaining on-premises infrastructure to a fully cloud-based environment.

That support extends to the day-to-day. For a small team where everyone wears multiple hats, having a friendly and responsive help desk to handle technical complexity in the background has made an ongoing difference.



I'm able to go on vacation without getting calls. Having Sentinel Blue there to help with the upgrades I've planned for the future — without adding it all to my plate — is tremendous. We're a small company, and that support makes a huge difference."
— **Amanda Webb**, Information Systems Security Officer, Level 1 Fasteners



Ready to Get to Work?

Reach out to us at sentinelblue.com/contact

