

CASE STUDY

Technology Firm Builds Innovative AI Tools for National Security Agencies Without Sacrificing CMMC Compliance



SENTINELBLUE

CASE STUDY QUICK FACTS



CLIENT TYPE/INDUSTRY

Technology Firm

LOCATION

Charleston, South Carolina, U.S.

SERVICES

CMMC Level 2 assessment prep

GCC High implementation

Automated asset management

Tailored cybersecurity strategy

vCISO advisory

On-site support

The Challenges of Securing AI Tools in the DIB

[Ignite Digital](#), a Charleston, SC-based technology firm offering mission, commercial technology, and forward deployed solutions to national security agencies, needed a cybersecurity and compliance partner that could keep pace with the speed of its AI and analytics development. Ignite Digital is in the business of helping government agencies achieve mission outcomes, which meant security and compliance couldn't become the bottleneck that slowed down the tools they were building.

Ignite Digital had worked with other MSPs before, but they repeatedly ran into partners who didn't know how to translate policy into technology decisions that supported their business objectives. Rather than a compliance vendor who would box Ignite Digital into a rigid framework, the company needed a partner who could implement strong cybersecurity practices while respecting their existing workflows and speed of execution.



Sentinel Blue isn't just an MSP or a compliance team; it's a business partner. The way I see it, Andy and his team really do try to help us solve our problems and support our outcomes, not just fit us into a box of cybersecurity frameworks that may or may not be relevant to our business."

– Oscar Mancía, Executive Vice President, Ignite Digital



The Solution: Security Architecture That Supports the Speed of Innovation

Building Security into the Foundation

Rather than developing its AI and analytics tools first and retrofitting compliance later, Ignite Digital worked with Sentinel Blue to build its security architecture around its data objectives from the start. Ignite Digital stood up its own models in Azure Government, with Sentinel Blue evaluating architectural paths early so the environment wouldn't be constrained by compliance or security requirements down the road.

The guiding principle to ensure CMMC compliance was straightforward: Nothing lives outside the protected cloud boundary, and nothing goes unprotected. That foundation meant Ignite Digital could keep using the everyday tools and devices its team already relied on to remain compliant, rather than adopting new workflows or bolting on third-party software for simple operating functions.

Leveraging Early GCC High Adoption

GCC High has a reputation for being difficult to work within, but Ignite Digital's early adoption, combined with Sentinel Blue's experience in the environment, gave the company an advantage most organizations don't have. That relationship opened doors directly to Microsoft's engineering teams, giving Ignite Digital a level of platform insight and troubleshooting support that isn't typically available to organizations working through GCC High's constraints on their own.

Automating Asset Management with Intune

Beyond the core security architecture, Sentinel Blue combined its deep security expertise with Ignite Digital's analytic capabilities to build an automated Intune asset management system. The result was full automation of Ignite Digital's asset management processes, saving the company hundreds of thousands of dollars a year and removing a significant operational burden from its internal team.

Key Outcomes: Successful Audits & A Partnership Geared Toward Future Growth

Passing High-Profile Assessments

Ignite Digital achieved CMMC Level 2 certification with Sentinel Blue's support. The assessment process was straightforward, with a first-try pass and no surprises along the way.



Separately, Ignite Digital underwent a high-level assessment conducted by the DoW as part of an award it won. Passing that audit alongside its CMMC certification reinforced Ignite Digital's standing as a trusted, secure partner to the agencies it serves.

Notably, Ignite Digital passed both audits without ever having to build out an internal IT team. By relying on Sentinel Blue as a fully managed partner rather than hiring and staffing an in-house function, Ignite Digital saved significant costs while still meeting the same rigorous compliance bar as organizations with dedicated internal teams.

Not a Compliance Shop, But a Partnership Built to Last

Ignite Digital also gained a partner that's invested in where they're headed next. The company can continue to grow its AI and analytics offerings alongside a security provider already familiar with its architecture and ambitions and eager to problem-solve with them. As Ignite Digital builds future tools and capabilities, its security will keep pace as a built-in part of the innovation process, not a separate hurdle to clear afterward.



Sentinel Blue has taken the time to actually understand what we're building, so they're already thinking a step ahead with us. As we onboard new technologies and develop new models, we can work together and figure out how to protect those models before they're deployed so the probability of success is higher from day one."

– **Oscar Mancía**, Executive Vice President, Ignite Digital



Ready to Get to Work?

Reach out to us at sentinelblue.com/contact

