SYNCDOG

Use Case Study:
Defense Contractor Achieves CMMC Compliance

Defense Contractor Achieves CMMC Compliance with SyncDog's Zero-Trust Mobile Security Solution

A leading U.S. Defense Industrial Base (DIB) contractor successfully implemented SyncDog's "Trusted Mobile Workspace" endpoint security solution to achieve CMMC compliance while enabling secure access to sensitive data on employee-owned devices. The solution's unique process-level isolation and FIPS 140-2 certified encryption capabilities provided superior protection for Controlled Unclassified Information (CUI) without compromising employee privacy on BYOD devices.

Challenges

The DIB contractor faced several critical challenges in securing their mobile workforce:

- Need to maintain CMMC compliance while supporting BYOD initiatives
- Requirement to house all data in GCC High secure cloud environment
- Organization-wide privacy mandates prohibiting invasive MDM solutions on personal devices
- Diverse security requirements across different departments and roles
- Previous struggles with complex MDM/EMM solutions

As a previous customer of Airwatch and after evaluating numerous other MDM/EMM/UEM solutions, we found that SyncDog offered the most complete, secure and flexible solution available. It's use of Validated FIPS 140-2 encryption puts it well ahead of almost all other vendors who do not have FIPS 140-2 certification, plus it's ability to secure BYOD devices without the need to install invasive MDM agents on our employees BYOD devices, put the SyncDog solution in a league by itself. When we realized we could install the solution in a matter of just minutes, we knew we found the right Vendor."

- Chief Information Security Officer, DIB Contractor

Solution Evaluation

The organization evaluated multiple enterprise mobility solutions including Microsoft Intune, Hypori, Mobile-Iron, and had previous experience with AirWatch. These solutions presented several limitations:

- Required installation of invasive MDM agents that conflicted with privacy mandates
- Complex deployment processes unsuitable for varied security needs
- Limited or no support for GCC High environment
- Extensive setup time and resource requirements

SYNCDOG

Use Case Study: Defense Contractor Achieves CMMC Compliance

About SyncDog

SyncDog is a leading provider of endpoint security solutions, specializing in securing corporate data on mobile devices without compromising user privacy. Its innovative approach ensures data encryption and isolation, making it ideal for organizations with stringent security and compliance requirements. Learn more at www.syncdog.com.

SyncDog Implementation

The contractor selected SyncDog's endpoint security solution for its unique advantages:

- Process-level isolation separating work and personal data
- FIPS 140-2 certified encryption for data at rest and in transit
- Native GCC High cloud environment support
- Agent-free BYOD security approach
- Rapid deployment without requiring physical device access

Results and Benefits

The implementation of SyncDog's solution delivered multiple advantages:

- Immediate CMMC compliance through data-centric security approach
- Complete isolation and encryption of work-related email, data, and apps
- Seamless BYOD support without compromising personal privacy
- Significant cost savings through simplified deployment
- Enhanced security posture at competitive pricing

Conclusion

By choosing SyncDog, the DIB contractor achieved their security and compliance objectives while respecting employee privacy and maintaining operational efficiency. The solution's focus on securing data rather than devices, combined with its GCC High compatibility and rapid deployment capabilities, provided an optimal balance of security, usability, and cost-effectiveness. The organization realized substantial savings in implementation costs while obtaining superior security features compared to traditional MDM solutions.