PREVEIL

DoD Supplier's Journey to Cybersecurity Compliance

Context

A Midwest parts supplier with 250 employees and $100M+ per year in annual revenue was faced with the challenge of meeting the DoD's cybersecurity compliance requirements. 20%-30% of the company's revenue is generated via Defense Industrial Base (DIB) contracts, which are subject to DFARS 7012, NIST 800-171 and soon CMMC Level 3. If the company could not quickly come up with a cost-effective way to improve its cybersecurity hygiene and properly protect Controlled Unclassified Information ("CUI"), its revenue base would be at significant risk.

Faced with this challenge, the company's CIO launched a compliance program to evaluate technology solutions to deploy across their multiple divisions and suppliers. In reviewing their existing G-Suite and O365 commercial solutions for email and file sharing, they discovered these platforms did not meet the DoD's requirements for DFARS and CMMC. The company had to find an alternative solution for storing, synching, and sharing their files that contained CUI.

Challenge

The CIO knew the solution he chose could not disrupt the technology or the productivity of the 70-80% of their business that did not work with the DoD. As a result, the CIO was inclined to pursue an "enclave" approach in which they would only deploy new technologies and processes to the subset of divisions and employees subject to the DoD's cybersecurity compliance requirements.

The CIO reviewed the cost, business impact and cybersecurity of three options: an on-premise implementation, Microsoft GCC High, and BoxGov. However, each choice fell short. The following chart highlights the challenges of each:

SOLUTIONS EVALUATED

	On-Prem	Microsoft GCC High	Box Gov
Financial burden	Hardware and software costs IT manhours Maintenance	Significant upfront migration fees License fees 2-3x vs O365 Expensive licenses required for all employees	Add on modules required Set-up costs Expensive annual licensing
Business impact	Further stressed capabilities of company's 2 person IT team Reduced IT availability for business-critical projects	6-9 month company-wide migration project Retraining required for all employees	Substantial upfront implementation effort Complex configuration and administration
Cybersecurity compliance architecture	Burden of architecting a secure and compliant on-prem platform Requires in-house IT staff to manage patching and related security maintenance Vulnerable to server breaches, password theft, and admin compromise	Requires extensive and specialized compliance configuration Vulnerable to server breaches, password theft, and admin compromise	Requires extensive and specialized compliance configuration Requires customer key server Vulnerable to server breaches, password theft, and admin compromise

None of these options were feasible options for the company to pursue. As a result, the CIO broadened his search which led to his discovering PreVeil.

Winning Approach

The CIO chose to go with the **PreVeil for Gov Community** offering to support the company's DoD cybersecurity compliance efforts. PreVeil's strengths were:

VERY AFFORDABLE PreVeil was a fraction of the cost of GCC High, required no up-front implementation fees, and only required paid licenses for those employees who used it. This reduced the TCO by $150-200K over a 3-year horizon.

MINIMAL BUSINESS DISRUPTION PreVeil was deployed in weeks to only those employees and divisions subject to DoD regulations. No company-wide migration was necessary. They also did not need to overhaul their existing infrastructure.

FUNDAMENTALLY BETTER CYBERSECURITY Built with end-to-end encryption and device-based cryptographic authentication, PreVeil's platform provides exceptional protection and control for email and files containing CUI, both within their company and with their suppliers.

Ultimately, by implementing PreVeil along with relevant policies and procedures, the company **significantly accelerated its cybersecurity compliance journey** and **addressed virtually all of the the DoD's required controls** relating to protecting CUI in Emails and File Sharing.

"We were looking for a DoD compliant file hosting platform. [It]... **became a frustrating hunt**...We were referred to PreVeil, a **very simple to implement and simple to use** application. We have been using PreVeil since October and have been **thrilled with the performance of the application itself and the level of attention and customer service** that we've received. It is also **VERY reasonable from a cost perspective**. PreVeil is definitely something you should **feel confident in the security, performance, and support across the board.**"

–CIO AND CHIEF STRATEGY OFFICER

By using PreVeil, the company was able to ensure exceptional protection for its sensitive files and communications containing CUI and maintain their revenue stream from DoD contracts.

CONTACT
SALES@PREVEIL.COM
TO LEARN MORE

PREVEIL.COM