



Secure Enclave

12-Week Implementation

KTL will configure and implement Office 365, Enterprise Mobility & Security, and Windows 10 Enterprise features in a Virtual Desktop Infrastructure in Azure Government and configure Azure Sentinel in order to create a Secure Enclave.

Why use a secure enclave?

The enclave approach provides advantages over complex compliance upgrades. The deployment of a secure enclave can mitigate the need to secure an entire infrastructure, so long as that enclave meets CMMC Level 2 requirements.



Benefits

Secure Enclave:

- Provides data security for specific sections of infrastructure
- Simplifies the implementation process
- Ensures CMMC requirements are met

System Security Plan (SSP)

- Create a plan to document CMMC practices and objectives satisfied through technical configurations.

Federal Requirements

- Configuration and documentation of services mapped to CMMC/NIST 800-171

Infrastructure Segmentation

- Set up of Virtual Desktop Infrastructure (VDI) for users in Azure Government

Deployment and Configurations

- Azure Active Directory Domain
- Azure Virtual Desktops
- Azure Sentinel
- Microsoft Office 365
- Azure Information Protection
- Microsoft Defender for Endpoint

"KTL was instrumental in helping us navigate the requirements of GCC High. Their support and expertise played a part in our success of becoming the first Authorized C3PAO."

- Thomas Graham, Vice President & CISO, Redspin

