The Secure Enclave

Written for KAMIND, IT, Inc.

By Ravi Das

Introduction

In many of our blogs and whitepapers, we have examined in detail what the Cybersecurity Maturity Model Certification, or the CMMC is all about. Essentially, this is where all of the contractors and the subcontractors in the Defense Industrial Base (also known as the "DIB") need to come into compliance with the various statutes and provisions that have been set forth by the Department of Defense (DoD).

This means that the contractors and the subcontractors need to reach certification at some sort of Maturity Level. Under the CMMC 1.0 there were a total of five Maturity Levels in which this could be accomplished, but under the current CMMC 2.0, there are only three of them in which certification needs to be achieved. These range specifically from Maturity Levels 1-3.

However, it should be noted that the CMMC 2.0 is still under works, and has not been formally approved yet. It is anticipated that this still at least a year to a year and a half out, possibly going as late as 2025. But there is a new feature that is coming out, and this is called the "CMMC Enclave", and will be further reviewed in this whitepaper.

What It Is An Enclave?

The first question that you are probably asking at this point is what exactly an enclave is. Well, as it relates to Cybersecurity and the needs of the DoD, it can be technically defined as the following:

"Secure enclaves allow applications to execute securely and enforced at the hardware level by the CPU itself. All data is encrypted in memory and decrypted only while being used inside the CPU. The data is still completely protected, even if the operating system, hypervisor or root user are compromised. With secure enclaves, data can be fully protected across its full life cycle—at rest, in motion and in use—for the first time."

(SOURCE: 1).

In other words, for example, if you are using a Cloud based platform to conduct your work for the DoD, the Secure Enclave will let you carve out a very secure area of it, and isolated from the rest of the shared environment. One of the biggest advantages of taking this kind of approach, is that your business is afforded the amongst the highest levels of protection that are possible, as it was eluded to in the above definition.

But you can still use your common Identity and Authorization Management (IAM) tools to grant access to the Secure Enclave. You can also continue to use other defensive based tools such as Firewalls, Routers, Hubs, Network Intrusion Devices, Virtual Private Networks (VPNs) and even virtual based LANS, which are commonly referred to as "vLANS".

As it relates to the CMMC, the Secure Enclave is primarily meant for the further protection of both the CUI and FCI datasets that your organization will be using, as supplied by the DoD. Although each Maturity Level specifies what controls are needed to safeguard these datasets, having a Secure Enclave in the Cloud, especially using the Microsoft Azure platform, will give you more ammunition to show to the DoD of your intentions of being compliant.

This point is further fortified by these following quotes, both from the DoD and NIST. First, is the quote from the former:

"When implementing CMMC, a DIB contractor can achieve a specific CMMC level for its entire enterprise network or for a particular segment(s) or enclave(s) depending upon where the information to be protected is handled and stored."

(SOURCE: 2).

Second, is the quote from the latter:

"Isolating CUI into its own security domain by applying architectural design concepts may be the most cost-effective and efficient approach for non-federal organizations to satisfy the security requirements and protect the confidentiality of CUI."

(SOURCE: 2).

So, even the DoD fully supports the use of some sort of Secure Enclave, and by doing so, you could quite possibly achieve compliance from Maturity Levels 1 – 3 in a very quick time period.

But before we go any further, it would be useful to provide a brief review of what CUI and FCI datasets actually are.

What the FCI and CUI Are

The FCI

FCI stands for "Federal Contract Information". A technical definition of it as follows:

"It is information not intended for public release. It is provided by or generated by for the Government under a contract to develop or deliver a product or service to the Government. FCI does not include information provided by the Government to the public."

(SOURCE: 3).

By the very nature of its name, the FCI has a much narrower scope than the CUI datasets (as just reviewed). In other words, these are the proprietary datasets that have been created and developed when the defense contractor and their third parties actually provide a tangible good to the Federal Government, under the terms of the contract that were awarded.

Examples of FCI datasets include the following:

- Any emails that are transmitted from the DoD to the defense contractor (and vice versa);
- Any other subcontracts and policies that are needed by the defense contractor;
- Any information that has been garnered as a result of instant messaging, video conferencing, etc.

The Levels At Which The FCI Is Implemented

It should be noted that with regards to the FCI, it impacts only the first two Maturity Levels which are as follows:

1) Level One:

This is deemed to be the initial phase, where there is no formal structure yet in place in order to accomplish the work processes that are needed in order to deliver the good or service to the Federal Government. Rather, the approach is Ad Hoc until it is all formalized. These typically can include the first round of meetings, information/data gathering, preliminary analysis requirements, etc.

2) Level Two:

At this level, the respective workflows and processes needed to fulfill the terms of the DoD contract become more defined. In other words, the ability to track in more detail what is happening can now take place. This also involves the following activities:

- The tracking of various costing schedules;
- Workflow scheduling;
- Defining the functionalities of the established workflows (in other words, defining in further detail the output that is expected, with an emphasis on the FCI related datasets that are to be created when developing the good or service to the Federal Government).

The CUI

CUI stands for Controlled Unclassified Information. Simply put, these are the datasets that are owned by the Federal Government in which the defense contractor (and their affiliates) must have the minimum level of controls put into place in order to safeguard them.

This can be initially misleading, because of the term "Unclassified". This means that these datasets can be shared with other entities that are CMMC certified, but they cannot be released to the public.

Very often, the CUI is needed by the defense contractor in order to submit a comprehensive Request For Proposal (RFP) to the DoD, and to initiate the work that needs to be done.

Typical examples of CUI datasets include the following:

- Intellectual Property;
- Technical drawings;
- Blueprints;
- Other forms of related documentation, such as those for export control, Cyber vulnerability information, and other sorts of financial data.

Assets & Security Protection Assets

The next important component of the Secure Enclave are the Security Protection Assets. In the world of Cybersecurity, assets are often referred to as the "Digital Assets". These include other pieces of information and data, which are used in the normal, everyday usage of business transactions. These are also commonly known as the "Personal Identifiable Information" datasets, or simply known as "PII" for short. These typically consist of the confidential data as it relates to customers, employees, and other relevant stakeholders in your organization.

The DoD would also like to see that your organization is taking proactive steps to safeguard the PII as well, by making use of the appropriate set controls and making sure that they are updated and patched on a regular cycle. In other words, it is not just enough to protect the FCI and CUI datasets. There is an inherent understanding that everything will be protected to the best of your ability, and that any remediations which are needed will be implemented quickly.

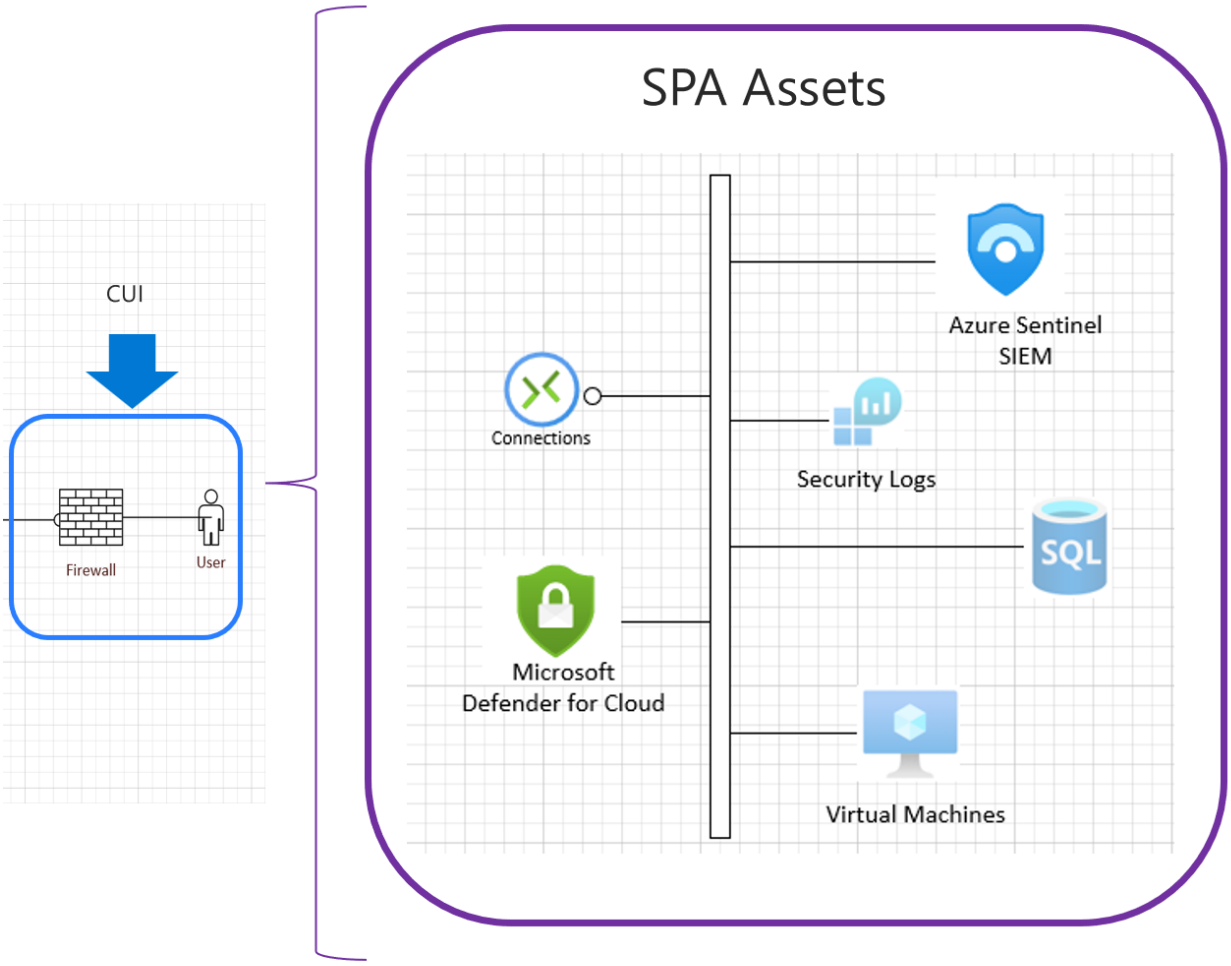
We can now extend this definition of Digital Assets, and apply to what are known as "Security Protection Assets.", also known as "SPAs". According to the DoD, SPAs can be specifically defined as follows:

"These are the assets that perform a CMMC-required security function and are described in the system security plan in this regard."

In other words, any asset that is used from within your organization to protect any other asset that is deemed to be "in scope" (provide some level of functionality) with any of the other Maturity Levels of the CMMC is an SPA.

(SOURCE: 4).

An example of an SPA is as follows:

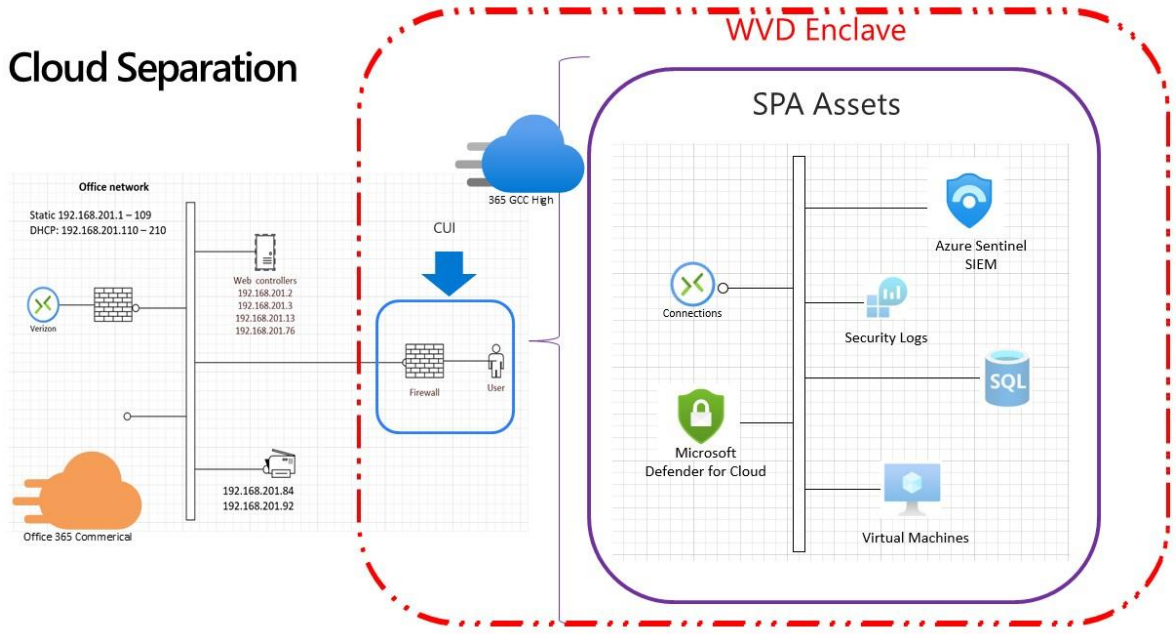


From this diagram, it is assumed that you are using Microsoft Azure for your CMMC deployments. It is evident that the Microsoft Defender for Cloud at least on a theoretical basis, is providing a primary lines of defense for the SPAs, which include the following:

- Azure Sentinel SIEM;
- The Security Logs;
- The SQL database;
- The Virtual Machines.

What The Secure Enclave Consists Of

When it comes to using Microsoft Azure, the Secure Enclave is typically housed in what is known as a "Windows Virtual Desktop", or also known as a "WVD" for short. It consists of everything from the last figure, and also what is known as the "GCC High." This is illustrated in the diagram below also:



KAMIND IT Company Confidential

At this point, it is important to provide a review of what the WVD and GCC High are all about.

<u>What Exactly Is the Windows Virtual Desktop (WVD)?</u>

The WVD is considered to be a set of tools, or technologies, which are available in Microsoft Azure, which allows the IT department of any kind or size of business to almost instantaneously create a brand-new desktop computer which makes use of the Windows 10 OS.

But instead of being physically deployed at your office, you can now access it with a few clicks of the mouse in just a matter of a few seconds.

But the nice thing about this is since it is all based in the Cloud, you do not have to worry about any licensing issues yourself directly, or even deploying any software upgrades and patches. It is all handled for you at Azure.

This breakthrough was actually launched last year in 2019, but has not gained serious traction until now. It stems from the Remote Desktop Protocol (RDP), in which an end user could access a remote computer virtually, and have a direct interface with the desktop.

Here are some of the key benefit of using the Windows Virtual Desktop:

- It is much easier for all of your employees (if not most of them) to access a single instance of it. In other words, each individual does not need to have their own desktop. From one single Virtual Machine (aka VM), you can create one desktop, and from there, the employees can access it, depending upon the rights, privileges, and permissions that have been assigned to them.
- For security purposes, all of the user profiles that have been created are actually stored separately from the Windows Virtual Desktop environment, in separate Cloud Storage Containers.
- It offers a more secure way for employees to access. This was traditionally done by making use of the RDP, but with Azure, a separate Platform as a Service (aka PaaS) is offered so that it can automatically manage the login sessions onto the WVD.
- It supports the usage of all employees, not just a select few. For example, these are the kinds of workers that would make the most usage of the WVD:

  *The Kiosk Workers: If you want your customers to access certain parts of your website that are designed specifically for them, such as a client login portal, you can now migrate this to the WVD environment, in a safe and secure manner. This transition actually decreases the security risks that are posed to your Web based application.

  *The Administrative Workers: These employees are typically the executive administrative assistants, secretaries, and other essential support personnel that required to keep your business running seamlessly on a daily basis.

  *The Knowledge Workers: These are those kinds of employees that are always on the go, and need constant, remote access to company resources. Typically, this group includes the outdoor account managers, members of the C-Suite, etc.

  *The Power Users: This is the classification that is most often given to those employees that use computing processing powers to its maximum availability. These are the software developers that are creating new applications for your company to offer to customers and prospects, and even graphic designers that make usage of video production in order to advertise/showcase your products and services. In the past, these employees would very often require having their own dedicated servers and workstations in order to serve these high intense CPU and memory needs. But, this can now all be offered through the WVD.

The GCC High

The DoD requires a special type of Cloud environment in order to secure its most sensitive dataset. which is often used by third parties, such as defense contractors. In order to satisfy this need, Microsoft

devised a new kind of Cloud Platform called the "Government Community Cloud", or the "GCC" for short, in order to meet its compliance standards.

Apart from the CMMC, this is also available to those entities that are involved with the following:

- FedRAMP High;
- DFARS 7012;
- The International Traffic in Arms Regulations (ITAR);
- The Criminal Justice Information Services Policies.

What Are The Differences Of GCC High With The Commercial M365?

It differs in four key areas, which are as follows:

1) Storage:

   Microsoft Azure has datacenters located throughout the entire world, and the end user typically has a choice as to which one of them they would like to deploy their Cloud environment in. But with the GCC High, this is not the case. All data that is stored, processed, and archived are stored in US based datacenters only. Further, access to this is severely restricted, as individuals must be employees of Microsoft, and have to also be thoroughly screened and background checked. Also, access to the DoD datasets is only allowed on a request only basis.

2) Access to M365 applications:

   When a business establishes their Azzure account along with M365, all applications from within them are available instantaneously. This is not the case with GCC High. Applications are much slower to roll out, given all of the security checks that must be conducted first.

3) Licensing:

   While the licensing for the commercial versions of M365 and Azure can be purchased from just about any Cloud Services Provider (CSP), licensing for the GCC High Cloud can only be purchased from Microsoft directly.

4) The sharing of information:

   The data that is stored and processed in the GCC High Cloud cannot be shared at all with other commercial Cloud Platforms that use Azure. It can only be shared from within other GCC environments. Also, there are some Public Switched Telephone Network (PSTN) features that are available in the GCC, versus the commercial deployments of Microsoft Teams and Skype (which is soon to be retired – click here to see more details on this.).

The Disadvantages Of The GCC

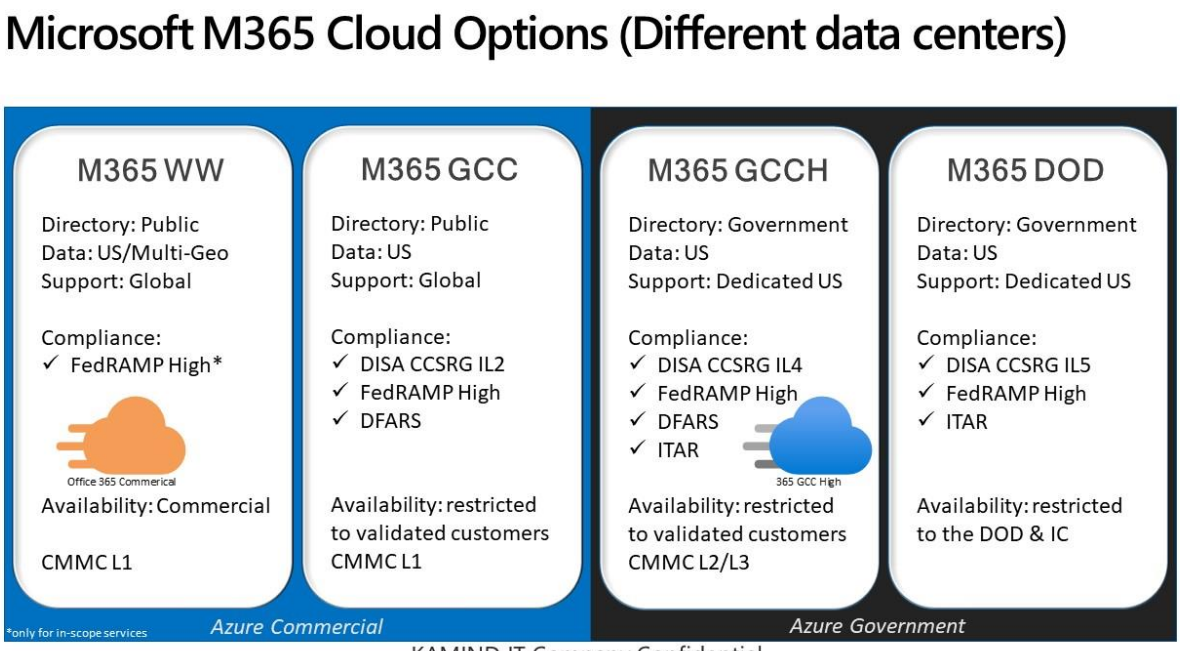
While the primary advantage of the GCC is that it offers a very secure and robust environment for the DoD datasets, because of that it also has a number of limitations as well:

- It can be murky to decide if you need this kind of platform for the CMMC. While using the GCC offers the other advantage of full compliance with the statutes and mandates of the CMMC, the question very often arises if you really need it, given that it can be a time consuming and tedious

process to deploy. There is no clear-cut answer to this, as a lot will depend upon the Maturity Level certification that you are seeking. The best way to get a clear-cut answer to this is to have a fully trained CMMC consultant first assess the controls you have in place, and from there, see what else is needed. It is important to keep in mind that the GCC is primarily designed for the applications listed in the first section of this article.

- Given the tightness of the environment, many other features of it are still quite limited, and there is virtually no interaction allowed with 3rd party applications.

It is important to note at this point there are different versions of the GCC High that you could possibly use for your company, and these can be seen in the diagram below:



Typically, you will need an M365 E5 or a (MS365 E3 + E5 security) for your Security Enclave, and is typically required at Maturity Level 2 or higher, if GCC High is going to be deployed into it.

Conclusions

Overall, some of the strategic benefits of using a Secure Enclave are as follows:

- The costs of CMMC Compliance are lower, as well as maintaining your certification for the long term;
- It can help with the reduction of any training requirements that are needed for others that will have access to your Secure Enclave;
- It will support the concept of Least Privilege (this is where you are giving only the authorized personnel access to the Secure Enclave to do only what they need to do, and nothing more);

- It will help to reduce the total amount of SPAs that are needed to conduct and transact CMMC functionalities.

Keep in mind that the Secure Enclave is still very new, but at KAMIND IT, we are keeping up to date with all of the latest developments. Contact us if you would like more information, or have questions about it.

Sources

1) https://securityboulevard.com/2020/01/secure-enclaves-a-new-approach-to-cybersecurity/
2) https://www.linkedin.com/pulse/enclave-approach-cmmc-ben-gerenstein/
3) https://www.cmmcaudit.org/what-is-fci-in-cmmc/
4) https://www.cmmcaudit.org/cmmc-scope-are-you-ready-for-an-assessment/#:~:text=Security%20Protection%20Assets%20(SPA),security%20plan%20in%20this%20regard.