THREATLOCKER

CMMC Compliance as a Service

Expanding the MSP Customer Base

Table of Contents

Introduction

In 2020, the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD)A&S)) from the Department of Defense (DoD) released the Cybersecurity Maturity Model Certification (CMMC). Understanding the cybersecurity supply chain risks across the Defense Industrial Base (DIB), the DoD will require that contractors meet the compliance requirements at the time it awards a contract.

Designed by a combination of federal and private experts, CMMC is a maturity model, not a regulation. Compliance requirements are based on the data that a company manages.

CMMC discusses two types of information

Federal Contract Information (FCI): information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.[1]

Controlled Unclassified Information (CUI): government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulation, and government-wide policies.[2]

Understanding CMMC Levels

CMMC sets out five different compliance levels, all based on the type of data a company manages. Every contract will include the type of information a company will collect, transmit, process, or store so that companies will know what CMMC level they need.

Most small and mid-size contractors will need to meet either Level 1 or Level 3 certification requirements.[3]

Level 1

- Companies that handle FCI need to perform 17 specified Basic Cyber Hygiene practices outlined in Federal Acquisition Regulation (FAR) 52.204-21.
- They do not need to prove they have processes in place.

Level 3

- Companies that handle FCI and CUI must establish, maintain, and resource a plan for managing and documenting their ability to manage 130 Good Cyber Hygiene practices as defined by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 and Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012.
- They need to prove that they have processes in place with policies for each domain, documentation for implementing CMMC practices, and appropriately resource the plan.

The DoD incorporates Level 2 as a “transition” state, giving credit to organizations trying to meet Level 3 compliance. However, the DoD will not allow them to manage CUI.

[1] Casey, D. (2020, June 19). FCI and CUI, what is the difference? CUI Program Blog. https://isoo.blogs.archives.gov/2020/06/19/%E2%80%8Bfci-and-cui-what-is-the-difference/
[2] Defense Counterintelligence and Security Agency. (n.d.). *Controlled Unclassified Information.* https://www.dcsa.mil/mc/ctp/cui/
[3] Office of the under Secretary of Defense for Acquisition & Sustainment. (2020). *Cybersecurity Model Certification (CMMC).* Office of the under Secretary of Defense for Acquisition & Sustainment. https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

Introduction

And Then There's the Interim Rule

To throw an additional curveball at DIB members, the Defense Acquisition Regulations System within the DoD published a new updated rule on September 29, 2020. The "Defense Federal Acquisition Regulation Supplement Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)" ("Interim Rule") implements a DoD Assessment Methodology and CMMC framework that assesses contractor cybersecurity program implementation.[4]

The Interim Rule implements a Scoring Methodology aligned with NIST SP 800-171. The Interim Rule amends DFARS 252.204.7012 to incorporate NIST SP 800-171 assessment requirements effective November 30, 2020. Meanwhile, it also adds a CMMC compliance requirement to another portion of DFARS.

The NIST SP 800-171 Scoring Methodology requires organizations to achieve a score of 110, aligned with the NIST controls. It deducts either 5, 3, or 1 point for missing controls. The different point assignments align with whether a control is a Basic Security Requirement or a Derived Security Requirement.

In short, while the DoD may not fully incorporate CMMC requirements into contracts until 2026, but the Interim Rule sets the stage for meeting many of the same security requirements.

Then There's the Supply Stream Flow Down

Managing the DIB supply chain requires all contractors to manage the cybersecurity posture of their business partners. In other words, prime contractors are responsible for ensuring security for all their subcontractors. Each subcontractor should be monitoring their contractors.

This "flow down" requirement means that everyone is responsible for everyone else.

[4] Defense Acquisition Regulations System (2020). *Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)*. Department of Defense. https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation -supplement-assessing-contractor-implementation-of

Unique Challenges Facing Managed Services Providers (MSPs)

Generally speaking, small and mid-sized organizations use MSPs because staffing their own IT departments is cost-prohibitive. As MSP customers seek CMMC certification, they need business partners who can support their strategic goals.

Meanwhile, MSPs find themselves trying to understand what certification level they require so that their customers can trust them.

MSPs Leverage CMMC Compliance for Competitive Advantage

The first step to determining whether an MSP must be CMMC compliant lies in the customer data it collects, transmits, processes, or stores. If an MSP will be managing FCI or CUI, then it needs to be at the appropriate CMMC Level.

In reality, most MSPs do not manage FCI or CUI. In fact, even those that manage FCI would only need to be certified to Level 1, which requires proving that the company follows Basic Cyber Hygiene practices across the 17 processes. Most organizations with a cybersecurity program already meet this standard.

In a recent interview, MAD Security, an MSP, noted:

> "On daily operations such as managing firewalls and looking for incidents – that's not exactly CUI, it is just log data and events occurring in the environment. This is why having a (sic) MSP or MSSP that works with DIB clients and is intimately familiar with CMMC and CUI is so important."[5]

[5] *Do MSSPs and MSPs need to become CMMC Compliant?* (2020, August 28). PreVeil. https://www.preveil.com/blog/mssps-and-msps-need-to-become-cmmc-compliant/

Unique Challenges Facing Managed Services Providers (MSPs)

In the same interview, the MSP also noted that some of its DoD contractor customers plan to require them to meet CMMC Level 3 certification.

For MSPs that want to maintain or expand their DIB customer base, CMMC may be used as a market differentiator rather than a contract requirement. Not only would they be able to prove their own cybersecurity maturity, but they will understand the certification process, making them better suited to support DIB members.

MSPs Will Help Customers Get Compliant

MSPs already see their customers struggling. MAD Security noted that their customers already struggle to distinguish CUI. In fact, most organizations find themselves struggling with this.

Small and mid-size business customers will likely look to MSPs to explain how their services enable compliance. Since internal IT teams would normally manage the controls that enable a cybersecurity program, MSPs will find themselves in a similar position.

To protect themselves from customer churn, MSPs will need to do several things:

- Understand CMMC documentation, attestation, and audit requirements
- Know how their services meet these requirements
- Articulate these benefits to customers
- Help customers set the right controls to meet CMMC documentation, attestation, and audit requirements

> As our dependence on software and other technologies grow, regulators will continue to enact data privacy laws. This presents an opportunity for MSPs to develop and leverage a niche expertise in this space to help clients maintain compliance with an increasingly complex set of regulations.[6]

- HelpNet Security *May 2020*

[6] Security, H. N. (2020, May 12). Cybersecurity and compliance: Vital priorities for MSPs and their clients. Help Net Security. https://www.helpnetsecurity.com/2020/05/13/msps-priorities/

Helping Customers Set Best CMMC Practices

"Compliance-as-a-service" (CaaS) is nothing new to MSPs. With this in mind, MSPs should start understanding how the technologies they use with their customers helps them maintain and grow their customer base.

CMMC opens up a new market for MSPs. Many small businesses looking to be CMMC Level 1 or Level 3 compliant may start outsourcing services that they previously handled in-house. To use CMMC as a market differentiator, MSPs need to understand where their services enable customers to set Basic Security Requirements or mature programs to meet Good Cyber Hygiene standards. As MSPs look to develop offerings that enable their DIB customers, they should understand CMMC and look to the "CMMC Assessment Guide - Level 3" to gain insight into how the CMMC Accreditation Body (AB) will review practices.[7]

Although not an exhaustive list of CMMC control families and practices, the following discussion provides insight into some pain points facing DIB customers that use MSPs. Many of the "Example Best Practices" are drawn from the "CMMC Assessment Guide - Level 3" to give MSPs better visibility into how auditors and the CMMC-AB will be assessing their customers.

[7] Office of the under Secretary of Defense for Acquisition & Sustainment. (2020). *CMMC Assessment Guide - Level 3 Office of the under Secretary of Defense for Acquisition & Sustainment*. https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl3_20201208_editable.pdf

Helping Customers Set Best CMMC Practices

Access Controls (AC)

Every organization, from five-person teams to 500,000 employee enterprises, struggles with Identity and Access Management (IAM). While Identity has been titled “the new perimeter” for years, it has become even more important in a COVID-19 and post-COVID era.

In July 2020, industry analyst Gartner surveyed 421 Human resources leaders, 4,535 employees, and 317 finance leaders. The research projects that 48% of the workforce will remain remote always or sometimes, compared to 30% before the pandemic.[8]

Four Level 1 CMMC compliance requirements focus on Access Control (AC). To meet CMMC Level 3 compliance, organizations need to adopt an additional eighteen AC controls. In other words, AC makes up 27% of Level 1 and 20% of Level 3 CMMC practices.

Example Best Practices

- Limit user access according to the principle of least privilege
- Limit privileged access according to the principle of least privilege
- Identify system administration or security functions that can be executed remotely
- Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities

ThreatLocker Ringfencing reinforces Identity and Access Management (IAM) least privilege controls by establishing application controls that limit what applications can access the internet and how applications can access each other. With ThreatLocker’s Storage Control and Ringfencing capabilities, organizations can control access to information for better data protection.

[8] Human Resources Team. (2020, July 16). *Remote Work After COVID-19.* Gartner. https://www.gartner.com/en/human-resources/trends/remote-work-after-covid

Helping Customers Set Best CMMC Practices

Asset Management (AM)

Organizations seeking Level 3 certification already struggle trying to sort what data constitutes CUI. The move to cloud makes this more difficult because organizations need to understand data flow across their increasingly complex IT stack. Defining the procedures for handling CUI requires companies to define how data travels from devices to applications and between applications in on-premise, cloud, and multi-cloud infrastructures.

ThreatLocker enhances CUI data handling procedures by establishing device and application access controls that can more precisely define how data travels from devices to applications and from application to application. Additionally, ThreatLocker's Storage Control logs all data access, enabling organizations to document the identification processes involved in handling CUI.

Example Best Practices

Identify people technology, information, and facilities involved in CUI handling

Document processes for establishing common CUI handling such as information creation, modification, dissemination, and disposal

Document procedures for protecting CUI inside the organization, outside controlled environments, and electronically located off premise

Helping Customers Set Best CMMC Practices

Audit and Accountability (AU)

Only organizations seeking CMMC Level 2 or 3 need to create AU practices. For companies that do not already have these practices in place, establishing policies and documenting the practices can be difficult.

ThreatLocker enhances CUI data handling procedures by establishing device and application access controls that can more precisely define how data travels from devices to applications and from application to application. Additionally, ThreatLocker's Storage Control logs all data access, enabling organizations to document the identification processes involved in handling CUI.

Example Best Practices

- Collect event log data for all devices, users, and software
- Track, log, and document all data access in real-time
- Track, log, and document all changes to data in real-time
- Limit user access to event log data
- Securely archive event data access and data changes for after-the-fact security investigation

Helping Customers Set Best CMMC Practices

Configuration Management (CM)

CM practices are necessary for Level 2 and 3 organizations, requiring them to harden systems and software. While on-premises devices, software, and access may be manageable, small and mid-sized businesses struggle when trying to enforce these controls across cloud-based and hybrid ecosystems.

ThreatLocker ensures the principle of least functionality by allowing organizations to set detailed controls over what applications can run in their environment, what applications can connect to the internet, how applications can share data, and what devices can be used to access resources.

ThreatLocker enables organizations to create a Zero Trust application architecture. With ThreatLocker, organizations can specify applications allowed to connect to the network, limit data sharing between applications, and set controls for applications that can run on devices but not connect to the internet. Additionally, after setting these access controls, organizations can set *deny all* controls for all other applications at both the device and network level.

In combination with our Universal Audit function, organizations can securely archive event data access and data changes for after-the-fact security investigation.

Example Best Practices

- Set logical access controls that prevent unauthorized users from changing configurations
- Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system
- Enable only applications and services that are needed for the function of the system
- Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets
- The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process

Helping Customers Set Best CMMC Practices

Identity and Authentication (IA)

As with the AC practices, IA reaches into the compliance mandate for Level 1 certification. While organizations at this layer only need to prove that they adopted Basic Cyber Hygiene, many may be engaging in the right practices without realizing it.

However, IA controls also apply to devices and applications, which is something that Level 1 customers may not realize. MSPs will need to ensure that their customers understand where and how they enable these security measures.

ThreatLocker Ringfencing reinforces user access controls by placing device and application access controls on identity and access management controls to act as an additional layer of security.

By limiting device and application access to resources, organizations enhance their ability to limit information that can be posted or processed on publicly accessible information systems.

Example Best Practices

- Assign unique identifiers to all users
- Ensure authorized users initiate identified processes and service accounts
- Assign devices that access the system unique identifiers

Helping Customers Set Best CMMC Practices

Maintenance (MA)

MA practices generally focus around keeping software and operations systems updated. However, CMMC does not clearly articulate the way in which companies should manage these practices. In this case, the CERT Resilience Management Model (CERT RMM), referenced within CMMC, provides additional insight. Meeting hardware availability requires regular maintenance.

While some of this maintenance is physical, some are virtual or electronic, like software patches.[9] Organizations can find this difficult if they have a distributed workforce and lack control over end-user devices sitting outside the corporate network.

ThreatLocker's ability to prevent applications from executing and/or interacting with other applications can help mitigate the risks of diagnostic and test programs in organizational systems.

Example Best Practices

Identify technology systems that require regular maintenance

Maintenance tools can be directly brought into a facility by maintenance personnel or downloaded from a vendor's website. If, upon inspection of the maintenance tools, organizations determine that the tools have been modified in an improper manner or the tools contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.

[9] https://resources.sei.cmu.edu/asset_files/Handbook/2016_002_001_514462.pdf

Helping Customers Set Best CMMC Practices

Media Protection (MP)

MP focuses on data collection procedures and tools as well as data storage procedures. According to the CERT RMM, collection media can include electronic logs, data files, databases, as well as physical media. Additionally, the MP section references CIS Controls v7.1 14.6 which requires organizations to protect all information stored on systems with file systems, network share, claims, application, or database-specific access control lists.[10] This means that companies need to create controls that limit access to devices and applications. However, physical media can include USB drives. Controlling activities like USB drive use is especially difficult when managing a remote or hybrid workforce.

Example Best Practices

> Limit access to media storage including within file shares

> Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports or disabling or removing the ability to insert, read, or write to such devices.

ThreatLocker Ringfencing reinforces user access controls by placing application access controls on identity and access management controls to act as an additional layer of security. Since Ringfencing can apply data access restrictions for applications, ThreatLocker's solution enables the enhanced media protection controls necessary for CMMC compliance.

By limiting application access to resources, organizations enhance their ability to limit information that can be posted or processed on publicly accessible information systems.

ThreatLocker's Storage Control solution enables organizations to enforce encryption across portable storage devices and prevent users from copying data to unencryptedexternal storage locations. By configuring application-level security policies, organizations can prevent ransomware, viruses, and other malicious code. Finally, organizations can create detailed, fine-grained application access controls across devices, file shares, and file types to mitigate risks.

[10] https://www.cisecurity.org/wp-content/uploads/2018/03/CIS-Controls-Measures-and-Metrics-V7.pd

Helping Customers Set Best CMMC Practices

Personnel Security (PS)

PS practices provide guidance that intends to mitigate risk arising from employment practices. Many of the controls stress the need to engage in background checks prior to hiring new workforce members. Additionally, PS also discusses the need to protect CUI during and after personnel actions like terminating employment or moving within an organization. Many companies struggle to appropriately terminate users' access because they have a difficult time managing IAM.

ThreatLocker reinforces IAM controls by linking a user to a device. With ThreatLocker, organizations can remove a device's ability to access resources, acting as an additional control over personnel actions.

Example Best Practices

- Ensure that users return all company IT equipment like laptops, cell phones, and storage devices
- Disable or close employee accounts
- Disable devices from connecting to networks upon employment termination

Helping Customers Set Best CMMC Practices

Risk Mitigation (RM)

Organizations that need to meet Level 3 certification need to engage in a risk assessment process. The formal process includes identifying all users, devices, software, and data. From there, they need to assess the risk level for each and engage in an analysis that ties these risks to data breach likelihood. Finally, they need to decide what risks they want to accept, transfer, refuse, or mitigate.

Although CMMC does not take a risk approach, it does require organizations to engage in risk mitigation activities. As organizations mature their cybersecurity practices to meet this mandate, creating risk mitigation practices can feel overwhelming, especially in complex IT stacks with interconnected applications across various devices.

ThreatLocker's device and application controls capabilities enable organizations to place controls around what devices can access resources, what applications can connect to the internet, and how applications can share data with one another.

Additionally, ThreatLocker enables organizations to prevent risky privileged access between applications reducing the risk associated with privileged users.

Example Best Practices

- Develop a risk response plan for all accepted or mitigated risks
- Define actions that prevent or limit an actor from exploiting a threat or vulnerability
- Set controls that reduce exposure, including administrative, physical, and technical controls
- Assign staff who are responsible for implementing and monitoring the response plan

Helping Customers Set Best CMMC Practices

System and Communications Protections (SC)

Even at Level 1, organizations need to prove activities that monitor, control, and protect communications. A Basic Security Hygiene practice is boundary protection, like setting firewall policies and monitoring web traffic. As organizations continue to mature their cybersecurity posture, the practices become more complex. For example, companies need to apply systems security engineering principles. As organizations mature these practices, they find that continuous monitoring for all devices, users, and software is difficult. Challenges that these organizations face include:

- Complex architectures
- Multiple network segments
- Employee-owned devices, like smartphones and tablets

ThreatLocker enables organizations to create a layer of control between their IAM and network layer that helps reinforce both of these and enables organizations to create a Zero Trust application architecture. With ThreatLocker, organizations can specify applications allowed to connect to the network, limit data sharing between applications, and set controls for applications that can run on devices but not connect to the internet.

ThreatLocker access controls can limit more precisely than firewall access, meaning that a user trying to access an application that the firewall allows may be restricted based on a ThreatLocker control.

Additionally, a user that may access an application under an IAM control may find that the application is not allowed to access the internet or share data with other applications based on a ThreatLocker control.

Example Best Practices

Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system

Implement the security design principle of minimized sharing that no computer resource is shared between system components (e.g., subjects, processes, functions) unless it is absolutely necessary to do so

Prevent unauthorized information transfer via shared resources in accordance with when system processing explicitly switches between different information classification levels or security categories

Denying by default and allowing by exception applies to inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections that are essential and approved are allowed. Deny by default, allow by exception also applies to a system that is connected to an external system.

Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary

Prevent unauthorized and unintended information transfer via shared system resources

Helping Customers Set Best CMMC Practices

System Integrity (SI)

SI practices intend to combat malicious code like malware and ransomware. As malicious actors increasingly leverage these, all organizations find themselves struggling with mitigating this risk. Even organizations at the CMMC Level 1 compliance level need to prove that they are acting to mitigate these risks.

Many organizations use an anti-virus tool to meet this requirement. However, anti-virus alone is unable to protect endpoints fully. At the lower maturity levels, many organizations may not realize that relying solely on anti-virus leaves them at risk. Additionally, they may not be implementing their anti-virus in a secure manner. For example, if they have not configured their software to update malware signatures daily, then they may not have Level 1 practices in place.

ThreatLocker enhances traditional anti-virus protections by preventing the riskiest access that can lead to malicious code installations. ThreatLocker blocks device and application access that prevents malicious code from being downloaded.

As such, it does not need to update malicious code signals because it prevents the access that leads to malicious code downloads, preventing malware attacks.

Example Best Practices

- Implement malicious code protection mechanisms at system entry and exit points like firewalls, remote access servers, workstations, electronic mail servers, notebook computers, and mobile devices
- In situations where malicious code cannot be detected by detection methods or technologies, organizations rely on other types of controls, including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to ensure that software does not perform functions other than the functions intended.
- Perform real-time scans of files from external sources as they are downloaded, opened, or executed
- Prevent malicious code from executing on devices, systems, and networks

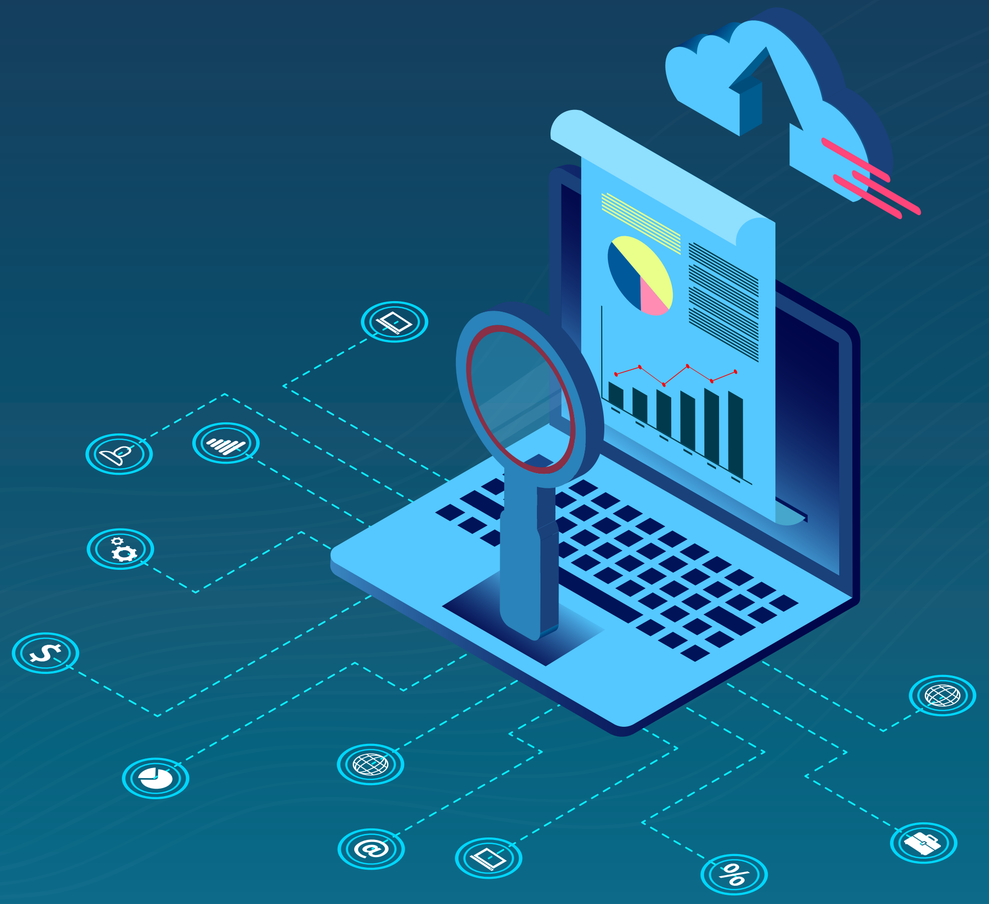
7 Defense In-Depth Best Practices to Enable Customer CMMC

MSP customers that need to meet CMMC compliance should take a defense-in-depth approach to mitigate cybersecurity risk. At Level 1, customers do not need to document their activities. However, they need to prove that they have Basic Cyber Hygiene practices built into their culture. From an audit perspective, this means that they should have these practices in place before they engage with an auditor. For example, if they only start securing data the month before the audit begins, they may not meet the threshold for having cybersecurity embedded into their culture.

Meanwhile, organizations that need Level 3 certification will need to create written policies and processes that show they have repeatable processes for managing cybersecurity risk. Additionally, as part of Level 3 certification, companies need to prove that they have allocated enough resources to the program to maintain effectiveness.

For small and mid-sized organizations, resourcing a program in-house may be cost-prohibitive. To meet the requirement that they appropriately fund and staff an effective IT department, many will look to outsource these activities.

MSPs need to find innovative ways to help their customers navigate these new compliance waters. As more customers look to mature their IT and security programs to meet CMMC compliance requirements, MSPs can help them by offering them a full suite of services aligned to best practices and help walk them through the process.



7 Defense In-Depth Best Practices to Enable Customer CMMC

1. Ensure Responsibility: Level 1, 2, 3

Level 1 organizations only need to prove that they perform practices. They do not need to prove funding or documentation since this level does not require process maturity. However, even at Level 1, organizations need to show that they have adopted specified practices for managing cyber risks.

While they do not need to formally assign responsibility, they do need to ensure that they have people managing the practices. They also need to prove that they have been managing these practices as part of their daily operations.

By Level 3, organizations need to ensure that they assign responsibility to designated parties. As part of maturing their cybersecurity practices, they need to have written policies that not only ensure responsibility for cybersecurity activities, but they need to formally designate roles managing them.

Create Policies: Level 2, 3

- Beginning with Level 2, organizations need to document their cybersecurity program with policies and practices so that they can perform the activities in a repeatable manner. Recognizing the effort this requires, CMMC created the Level 2 transition certification. Although Level 2 certified organizations will not be able to handle CUI, the DoD determined that they should be given credit for starting to formalize their practices.

Develop a Plan: Level 3

- At Level 3, organizations need to turn their written policies and practices into a plan that includes a mission, goals, project plans, resourcing, training, and includes relevant stakeholders.

2. Allocate Resources

At Level 1, allocating resources simply means having the people and technologies necessary for performing Basic Cyber Hygiene. At Level 3, allocating resources is more formalized. It requires ensuring that the organization has the people, technologies, and processes underlying a more robust program. While resourcing a plan is a Level 3 requirement, functionally all levels will require organizations to allocate some resources.

Allocating resources can include:

- Staff with the knowledge to manage the day-to-day activities
- Event log monitoring capabilities to detect potential security events
- Technologies that help manage the day-to-day activities

7 Defense In-Depth Best Practices to Enable Customer CMMC

MSPs offer a cost-effective solution to allocating resources. At Level 1, organizations need to prove that they can adequately perform cybersecurity practices, even if they do not have anything written down. However, many Level 1 organizations will find that they need to outsource certain IT functions to meet this basic requirement.

For Level 3 organizations, MSPs provide additional value. Beyond filling the staffing gap, MSPs provide a single location for IT control setting and documentation.

3. Set Identity and Access Controls

Regardless of an organization's CMMC Level, it needs a way to limit access to systems, networks, and software. When setting access controls, all organizations need to make sure that they can identify all users, devices, and software. From there, they need to build out policies that limit access according to the principle of least privilege.

MSPs who can manage endpoint devices can enable their customers by providing an additional layer of defense that sits between the user and application layer. If an MSP has an endpoint agent that controls whether a device can connect to a network or system, they can revoke this access. This enhances any IAM controls the organization has in place.

ThreatLocker Ringfencing reinforces Identity and Access Management (IAM) least privilege controls by establishing application controls that limit what applications can access the internet and how applications can access each other.

IAM practices should include:

- Creating a unique identifier for each user
- Using an authentication tool for users accessing systems, software, and networks, like a password, key card, cryptographic device, or one-time password
- Removing access to systems, networks, and software when users terminate their employment or contract with the company
- Ensuring that users have the least amount of access necessary to complete their job functions
- Limiting privileged access, such as Administrator access, as much as possible

7 Defense In-Depth Best Practices to Enable Customer CMMC

4. Manage Device Access

For all levels, organizations will need to identify all their IT assets. While they may not need to have these written down at Level 1, they will need to prove that they can identify them all. At Level 3, organizations will need to provide documentation proving that they know the devices connecting to their networks, systems, and software.

MSPs can help their customers move toward a Zero Trust approach by using endpoint management solutions. For example, MSPs can mitigate the risks associated with employee-owned devices by setting deny-all for devices not running their endpoint monitoring software. Additionally, MSPs provide value by linking user and device activity as part of their monitoring processes.

Example Best Practices

- Assigning each device a unique ID
- Linking the unique device ID to a unique user ID
- Preventing end-user owned devices from connecting to networks, systems, and software
- Tracking and documenting user and device activity

7 Defense In-Depth Best Practices to Enable Customer CMMC

5. Manage Access and Data Sharing

One of the biggest CMMC compliance challenges organizations face is managing data flow and application-to-application data sharing. Often, setting IAM controls is not enough. For example, privileged users can often circumvent access controls by moving from an administrative tool into another tool. For example, a privileged user can circumvent application access protections by opening PuTTY then use that elevated access to open PowerShell.

Additionally, when applications can share data with one another, they increase access risk. For example, Ringfencing can prevent Word from communicating with PowerShell, or any other risky applications.

Managing access and data sharing should include:

- Setting approve and deny policies based on user access entitlements
- Elevating privileges on a just-in-time basis
- Limiting what applications can connect to the network
- Limiting how applications share data with one another

Small and mid-size businesses struggle to manage these activities internally. MSPs can leverage endpoint management solutions to set precise access and data sharing controls. By providing this service, MSPs enable their customers to mature their cybersecurity risk mitigation strategies.

6. Manage Removable Media

With remote and hybrid workforces, managing removable media is even more difficult for small and mid-sized businesses. They need to prevent workforce members, including contractors, from contaminating their environment. However, they may not be able to control what end-users connect to devices when they are at home.

MSPs can enable their customers by setting policies for USB use. With endpoint management solutions, MSPs can provide their customers with the ability to deny all or allow only encrypted USBs.

7. Prevent Malicious Code Execution

Most small and mid-sized businesses only use anti-virus software to mitigate malware and ransomware threats. However, these protections often leave gaps. The database the anti-virus software uses needs to be updated regularly, and the organization needs to ensure that all devices stay up-to-date.

As customers move towards CMMC certification, MSPs can enable them by providing more robust malicious code protection. With an endpoint solution that prevents malicious code from executing, MSPs can offer a malicious code execution protection that their customers would be unable to manage on their own.

THREATLOCKER

Zero Trust Policy-Driven Security Enabling Customer CMMC Compliance

ThreatLocker's suite of solutions enables MSPs to provide a robust approach to endpoint security that protects customers from malicious code and misused software. ThreatLocker fills the access gaps that exist between IAM and firewall controls, allowing MSPs to provide more precise application access than either of these alone can offer. Our solution adds another layer of defense between the Identity perimeter and the network layer. This reinforces both control sets while ensuring that neither can act as a single point of failure. This enables MSPs to enhance their customers' defense-in-depth strategies as they seek CMMC certification.

ThreatLocker Application Control with Ringfencing

ThreatLocker is neither a firewall nor an access management tool. It is a solution that reinforces access controls. For example, a firewall may allow an application to access the network, but ThreatLocker will restrict an application's ability to connect to a specific network address, regardless of whether the firewall allows the communication, putting a second layer of control around the resource and creating defense in depth. Additionally, a user that may access an application under an IAM control may find that the application is not allowed to access the internet or share data with other applications based on a ThreatLocker control.

MSPs can leverage ThreatLocker to offer their customers a Zero Trust application architecture. With ThreatLocker, organizations can specify applications allowed to connect to the network, limit data sharing between applications, and set controls for applications that can run on devices but not connect to the internet. After setting these access controls, they can set "deny all" controls for all other applications at both the device and network level.

ThreatLocker Storage Control

ThreatLocker Storage protection enables organizations to limit the use of USBs to only those using encryption to reinforce storage on digital media. Although ThreatLocker does not push out updates to devices, organizations can set controls that limit an outdated, unpatched application from running in their environment. Organizations can define what version of an application is safe to access their network and deny access if the application version is not considered secure.

MSPs can leverage ThreatLocker to enhance customer data access governance. ThreatLocker tracks and documents file activity for executables, DLLs, and files on shared drives, tying these to activities to users and devices. This functionality adds additional risk mitigation and documentation capabilities beyond traditional IAM monitoring.

ThreatLocker Elevation Control

ThreatLocker Elevation Control, in conjunction with Ringfencing, enables application access controls that reinforce remote user access controls for remote execution of privileged commands so that privileged users can only use the defined applications for their intended purpose and not connect to additional applications while engaging in privileged activities related to security-relevant information. Leveraging ThreatLocker, MSPs can set just-in-time privileged access to and across applications for enhanced monitoring of risky privileged access.

ThreatLocker Unified Audit

ThreatLocker's Unified Audit capability tracks, logs, and documents all activities (move, delete, write, read) for every piece of data on a server share while also logging data access on USB devices, and local folders such as Documents and desktop. Users can create customized reports or use one of ThreatLocker's out-of-the-box reports, then export the reports for auditing.ThreatLocker's Unified Audit capability

THREATLOCKER

555 Winderly Place
Suite 300
Maitland, Fl 32751

+1 (833) 292-7732

@ThreatLocker
sales@threatlocker.com
www.threatlocker.com