HOW IOT SECURE MAPS TO THE CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) CONTROLS

CASE STUDY

IoT Secure®

How IoT Secure Can Prepare Your Organization for CMMC 2.0

The Defense Industrial Base is and will continue to be a target of frequent and complex cyberattacks. The Defense Industrial Base is a critical supplier of products, solutions and services to the Department of Defense (DoD) and ultimately to national security.

Recognizing the dependence on industry, the DoD established the Cybersecurity Maturity Model Certification (CMMC) program to reinforce the importance of cybersecurity for all vendors that do business with the Department.

The intent of CMMC is to ensure that information that supports and enables the Department of Defense and the military services is safeguarded.

Recently, the Department published CMMC 2.0, which is an update to CMMC 1.0, DoD's initial vision for the CMMC program. According to the DoD, the newly updated CMMC 2.0 would achieve the following goals

- Safeguard sensitive information to enable and protect the warfighter
- Enforce defense industrial cybersecurity standards to meet evolving threats
- Maintain public trust through high professional and ethical standards

CMMC 2.0 will be required for all DoD contracts and this will significantly impact all companies that do business with the Department of Defense, including small and medium size businesses that typically sub-contract under prime contractors. The DoD is currently undergoing a rulemaking process for CMMC 2.0, and once that is complete, CMMC 2.0 as a contractual requirement will take effect.

The costs to implement CMMC 2.0 can be significant. Costs alone to CMMC Assessors and CMMC 3rd Party Auditors (C3PAO) only cover the services of assessment and auditing for compliance and not the compliance work itself.

With the proliferation of Internet of Things (IoT) devices and other unmanaged devices in the world, the challenges of a DoD vendor to protect its networks and its information, including Federal Contract Information (FCI) and Controlled Unclassified Information (CUI), will only grow. Any devices that contain this information need to be protected from these IoT threats.

IoT Secure®

sales@iotsecure.io | 1.404.260.7405 | www.iotsecure.io
Copyright © 2022 IoT Secure, Inc. | All Rights Reserved

How IoT Secure Can Prepare Your Organization for CMMC 2.0

Unmanaged IoT devices lack visibility and are hard to secure. In addition, they are easily deployed by Operational Technology and end users without involving IT for securing the device.

They can automatically connect to the internet or other devices, and commonly do not support software agents for centralized management and security. They also can't be patched or don't support a patching process, because patching and security in general was never built into these devices. Instead, manufacturers use open-source operating systems like BusyBox or embedded Linux to speed up the product distribution to market, and as a result, security becomes an afterthought after these devices have already hit the market.

In fact, many of these unmanaged devices have default risky behavior like insecure services, hard-coded passwords or automated data transmissions.

Current scanning like NMAP, Network Access Control (NAC) tools or Vulnerability Scanners fail to identify IoT devices and detect IoT–specific vulnerabilities. These network scanners have gaps in device visibility, context and security with unmanaged devices, because they do not tell exactly what the device is, or exactly what other devices are on the same network. This results in the network manager having to conduct a manual IT asset inventory, which is neither efficient nor practical and will be extra overhead that organizations possess neither the time or the headcount to perform on a regular basis. That being said, the requirement to comply with CMMC 2.0 does not change, and if organizations want to continue to do business with the Department, they must comply.

Many organizations lack the visibility and capability to secure their devices and as a result, their ability to do business with the Department of Defense could be jeopardized. Let IoT Secure be your solution. Unlike other competitors, we offer a high value/low cost solution that allows you to stay compliant. We also provide a regular report capability to you so that you can have it ready whenever you need to present it to auditors an accountability of your asset inventory.

Below are just a subset of CMMC controls that our IoT Secure security appliances address, and how those controls are mapped to our product features and capabilities.

IoT Secure®

sales@iotsecure.io | 1.404.260.7405 | www.iotsecure.io
Copyright © 2022 IoT Secure, Inc. | All Rights Reserved

CMMC Controls Addressed By IoT Secure

Control ID	Maturity Description Level	How IoT Secure Maps
AC.1.003	Verify and control/limit connections to and use of external information systems.	IoT Secure enables 1.003 through its SmartBlock feature, allowing you to block devices on your network with a single button press, instantly isolating and securing your device.
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	IoT Secure supports separation of duties by empowering its customers to monitor and report on vulnerabilities of devices that may be owned and maintained by a separate business unit.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	IoT Secure's SmartBlock feature prevents privileged actions from taking place by blocking ports that devices on your network should not even have open, whether it's FTP, Telnet, or SSH. With a single button press, our customers can instantly isolate and secure their devices.
AC.3.020	Control connection of mobile devices.	IoT Secure can identify mobile devices, and using either the Block or Smart Block feature, restrict mobile device connections when connected to the network.
AC.5.024	Identify and mitigate risk associated with unidentified wireless access points connected to the network.	IoT Secure provides clear visibility into all network connected devices, including wireless access points, with data and device behavior analytics.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation and reporting of unlawful or unauthorized system activity.	IoT Secure maintains a record of network transmissions for every device to every internal and external destination, on every port, on every protocol. This record can be critical to investigations of unlawful or unauthorized system activity.

IoT Secure®

sales@iotsecure.io | 1.404.260.7405 | www.iotsecure.io
Copyright © 2022 IoT Secure, Inc. | All Rights Reserved

CMMC Controls Addressed By IoT Secure

Control ID	Maturity Description Level	How IoT Secure Maps
AU.3.048	Collect audit information (e.g., logs) into one or more central repositories.	IoT Secure has integrations with all major SIEMs, including Splunk. IoT Secure also has a REST API that can feed data into a customized SIEM residing in the customer environment.
AU.3.051	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious or unusual activity.	IoT allows our customers to query data with regard to devices, threats, and vulnerabilities, allowing analysis and reporting on suspicious or unusual activity. This information can also be exported to SIEMs or other reporting tools through our REST API.
AU.3.052	Provide audit record reduction and report generation to support on-demand analysis and reporting.	Our cloud port allows for the exporting of information to spreadsheets or summarization. We also provide weekly reports that provide the most up to date information on new vulnerabilities detected on assets connected to your network.
AU.4.053	Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity.	IoT Secure automatically analyzes device, network, and security information and alerts when it detects critical indicators of compromise. Information can also be sent to a SIEM for external analysis and alerting or through a REST API to your data repository.
CA.2.158	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	IoT Secure delivers passive and continuous monitoring of your network assets, which can provide a clear picture of the effectiveness of controls (e.g., speed of patching systems, connections to malicious URLs, accuracy of VLAN assignments, etc.), across the organization.
CA.2.159	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	IoT Secure integrates with ITSM solutions like Service Now to trigger the appropriate workflow for a given deficiency or vulnerability. Our alerts also provide recommended actions with regard to handling of the device or asset.

IoT Secure®

sales@iotsecure.io | 1.404.260.7405 | www.iotsecure.io
Copyright © 2022 IoT Secure, Inc. | All Rights Reserved

CMMC Controls Addressed By IoT Secure

Control ID	Maturity Description Level	How IoT Secure Maps
CA.3.161	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	IoT Secure delivers passive and continuous monitoring of your network assets, which will provide a clear picture of the controls needed and effectiveness of implementation.
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware and documentation) throughout the respective system.	IoT Secure automatically discovers, tracks and provides detailed inventories of all devices. IoT Secure identifies devices by category, type, make, model, OS, ports and network so you always have a complete context and detailed inventory of devices, without any manual work.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	IoT Secure automatically detects insecure configurations on unmanaged devices such as default credentials and unwanted/unnecessary services without any disruption to devices or to the network, which is common with that traditional security tools and scanners. Additionally, IoT secure identifies risky device communications.
IA.2.078	Enforce a minimum password complexity and change of characters when new passwords are created.	IoT Secure can identify default passwords on network-connected devices.
IR.3.098	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	IoT Secure integrates with with SIEM or ITSM solutions, such as ServiceNow.
MP.2.119	Protect (ie., physically control and securely store) system media containing CUI, both paper and digital.	IoT Secure can support implementation as part of a complete system.
MP.2.120	Limit access to CUI on system media to authorized users.	IoT Secure can support implementation as part of a complete system.
PE.1.134	Control and manage physical access devices.	IoT Secure can support implementation as part of a complete system.

IoT Secure®

sales@iotsecure.io | 1.404.260.7405 | www.iotsecure.io
Copyright © 2022 IoT Secure, Inc. | All Rights Reserved

CMMC Controls Addressed By IoT Secure

Control ID	Maturity Description Level	How IoT Secure Maps
PE.2.135	Protect and monitor the physical facility and support infrastructure for organizational systems.	IoT Secure can support implementation as part of a complete system.
RM.2.141	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	IoT Secure performs vulnerability assessments by continuously monitoring (and reporting on) every action taken by organizational assets and systems.
RM.2.142	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	IoT Secure provides unique value because it automatically inspects devices for vulnerabilities both as they connect to the network and continuously and it does so safely without crashing devices. This allows vulnerability testing on unmanaged devices and fills a gap with traditional vulnerability scanners which commonly crash these devices and leave them untested on the network.
RM.4.151	Perform scans for unauthorized ports available across perimeter network boundaries over the organization's internet network boundaries and other organizationally defined boundaries.	IoT Secure is able to pull port data as well.
SC.1.176	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	IoT Secure's clear visibility of all your network-connected devices will enable you to set up VLANs or subnets to make sure that your network is properly segmented.
SC.3.180	Employ architectural designs, software development techniques and systems engineering principles that promote effective information security within organizational systems.	IoT Secure ensures passive and continuous monitoring of all network-connected devices to provide clear information security.
SI.1.210	Identify, report, and correct information and information system flaws in a timely manner.	IoT Secure ensures passive and continuous monitoring of all network-connected devices for timely reporting and remediation.

IoT Secure®

sales@iotsecure.io | 1.404.260.7405 | www.iotsecure.io
Copyright © 2022 IoT Secure, Inc. | All Rights Reserved

CMMC Controls Addressed By IoT Secure

Control ID	Maturity Description Level	How IoT Secure Maps
SI.2.216	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	IoT Secure can automatically and without any tuning monitor devices that don't run security monitoring agents and alert on any malicious or abnormal behavior. This would otherwise require resource and work to capture and research each type of unmanaged device's behavior, then building and maintain security rules and tracking any changes to the device communication patterns to monitor the device.

IoT Secure®

sales@iotsecure.io | 1.404.260.7405 | www.iotsecure.io
Copyright © 2022 IoT Secure, Inc. | All Rights Reserved