

# Take Control of Your CMMC Readiness

Apply the **right solutions** and obtain your certification.



Cigent Technology Inc.  
2211 Widman Way Suite 150  
Fort Myers, Florida 33901  
844-256-1825  
[www.cigent.com](http://www.cigent.com)

Cybersecurity Maturity Model Certification (CMMC) enhances protection of sensitive information through five cyber hygiene levels. To prepare for CMMC compliance, you need a formalized approach to cybersecurity to demonstrate cyber hygiene. With five levels and 17 domains, you may find yourself struggling to meet the new demands assessed by CMMC Third-Party Assessment Organizations (C3PAOs). This paper outlines the solutions you need to succeed.

## Contents

About Our One-Stop Shop	Page 2
SSU Physical Security Training	Page 3
PC Matic Whitelist Management	Page 4
Avanan Email and File Share Security	Page 5
Cigent D <sup>3</sup> E	Page 6
Cigent Secure SSD	Page 7
Cigent Managed Blueshift XDR	Page 8



## About Our One-Stop Shop

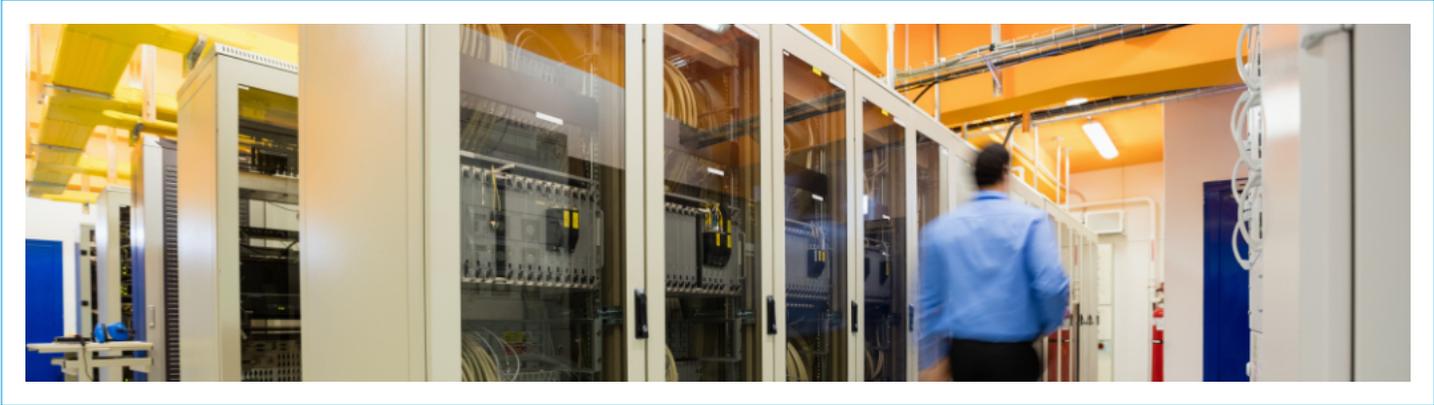


### What is CMMC?

The Cybersecurity Maturity Model Certification (CMMC) enhances protection of sensitive information through five cyber hygiene levels. Each level builds on the previous one and has their own domain requirements. The Department of Defense (DoD) specifies the required level needed for specific contracts to handle Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

### How can you achieve your certification?

To help you obtain your certification, Cigent has partnered with leading solutions providers to offer affordable, cloud managed, one-stop shop solutions that target exact requirements for your desired level. It can be difficult building your own technology stack; you need to ensure that the CMMC solutions are compatible, and that integration occurs without obstructing the other tools. That's why Cigent's one-stop shop intends to help you reach the higher CMMC levels without the burden of searching for, deploying, and managing one-off solutions. This comprehensive CMMC compliance service is backed by years of industry expertise and is based on government/military-grade technology that defends CUI against any threat vector. You need affordable solutions that guarantee achievement of your compliance goals; you've come to the right place.



## SSU Physical Security Training



### Enhance your **risk awareness**.

Physical security means protecting your physical assets that may reside in server rooms, private areas, or even in your home. If your security measures are not up to par, there's no way to target threats and see where they're coming from. For example, having one universal password for all your company systems means there are no logs to go through, which aid in tracking threats. SSU specializes in finding the right solutions for your information systems while maintaining CMMC requirements.

### CMMC Levels 1–3

You can achieve CMMC levels 1–3 alongside five core domain requirements with SSU's Physical Security Training. The domains this compliance solution addresses are:

- Access Control (AC)
- Awareness and Training (AT)
- Media Protection (MP)
- Physical Protection (PE)
- Personnel Security (PE)

SSU teaches you how to mitigate risks through awareness training in security concepts such as the following:

#### Situational response

Perceiving your security posture and its threat environment to comprehend risks | This training helps you observe and analyze for system status changes in the future so you can tackle them accordingly.

#### Threat analysis

Comprehension of your organization's information weaknesses are tested against realistic cyberattacks. | This training betters your ability to combat risks. They also demonstrate how to develop programs to execute for finding and managing threats. SSU's services meet CMMC controls for levels 1–3.



[strategicsolutionsunlimited.com](http://strategicsolutionsunlimited.com)



## PC Matic Whitelist Management

Similar to how your firewall uses a deny-all, allow-by-exception approach to only allow approved traffic into your network, whitelisting is the act of employing a deny-all, allow-by-exception security posture at the endpoint. A deny-all approach is the only way to proactively prevent threats; all other detect-and-respond approaches (e.g., EDR, MDR, TDR, XDR, etc.) require the threat to occur before they can counter it. Thanks to its global and patented digital-code-signing-certificate lists, PC Matic's whitelisting removes deployment and maintenance headaches that are common with other whitelisting technologies.

### Prevent threats with a deny-all approach.

#### CMMC Levels 1–3

You can achieve CMMC levels 1–3 alongside six core domain requirements with PC Matic's Whitelist Management. The domains this compliance solution addresses are:

- Access Control (AC)
- Audit and Accountability (AU)
- Configuration Management (CM)
- Media Protection (MP)
- Risk Assessment (RM)
- System and Information Integrity (SI)



PC Matic provides the layers needed to meet CMMC levels 1–3 and differs from typical whitelist management in the following ways:

#### Initial enumeration

Unlike typical whitelisting requiring a network administrator to enumerate all the software in your environment and then populate an initial whitelist, PC Matic has a pre-populated global whitelist compiled from intelligence collected from millions of endpoints under management. This means that deployment only requires bespoke software that is unique to your environment to be addressed if you have any homegrown applications in use.

#### Patches and updates

Whenever any endpoint under management sees an unknown application, that application is automatically reviewed by PC Matic's Malware Research Team and then is added to the global whitelist if it's a safe program. This means that instead of an administrator having to update your local list for all software patches

prior to them being able to be executed in your environment, this process has been automated, greatly reducing administrative overhead.

#### Homegrown software

PC Matic's patented digital code signing certificate whitelisting means that for firms who have a lot of homegrown software, the network administrators can add their developers' signatures to the whitelist, allowing their code to run without the administrator having to allow every file. Similarly, if all the code from a developer needs to be immediately stopped, this can be done by moving that certificate to a black list. This allows for full digital code signing certificate policy enforcement in line with NIST recommendations.

#### Whitelist management options

Management options are typically available locally by hash or directory. PC Matic extends these options with global and local options by hash, directory, or code signing certificate.



## Avanan Email/File Share Security



### Collaborate **safely** through email and file share.

The #1 breach threat for users is phishing emails that aim to steal sensitive information. Malware incidence also occurs often where viruses hide in emails and act upon opening. Avanan tackles cyber-attacks through proactive email security that captures, scans, and remediates targeted issues before attacks get to your inbox. If the email is not malicious, it gets delivered.

### CMMC Level 3

You can achieve CMMC Level 3 requirements for email protections and sandboxing that encompass the System and Information Integrity (SI) domain with Avanan's email and file security.



[avanan.com](https://www.avanan.com)

To ensure you're not exposed from any angle, these security measures extend to internal, inbound, and outbound emails, as well as collaboration on file share apps. For file sharing, every time a file is clicked on, it's rescanned and then rewritten if malicious. Avanan's email/file share security covers CMMC level 3 email protections and sandboxing with the following:

### Complete Malware

Guarantees anti-phishing and advanced malware protection for Office 365 email, OneDrive and Sharepoint, G Suite Gmail and GDrive, Slack, Teams, Box, Dropbox, Citrix ShareFile or other collaboration apps.

Phishing Email Threats

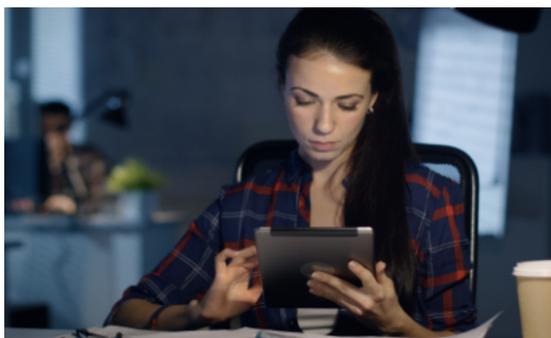
91%

Malware Incidence via Email

94%



## Cigent Dynamic Data Defense Engine



### Control access with **multifactor** authentication.

Protection of CUI is a critical requirement of CMMC Level 3. Cigent's Dynamic Data Defense Engine™ (D<sup>3</sup>E) Zero Trust file access controls utilize multifactor authentication to protect CUI from data theft and ransomware, even if a system is compromised.



### CMMC Levels 1–3

You can achieve CMMC levels 1–3 alongside six core domain requirements with Cigent D<sup>3</sup>E. The domains this compliance solution addresses are:

- Access Control (AC)
- Audit and Accountability (AU)
- Identification and Authentication (IA)
- Media Protection (MP)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

Cigent D<sup>3</sup>E's authentication capabilities also allow you or your organization to encrypt and control access to sensitive files. As a result, they are securely stored in any location and shared with only trusted users. D<sup>3</sup>E meets CMMC levels 1–3 and includes the following features:

#### Frictionless security layer

D<sup>3</sup>E provides CUI protection from any threat by putting protection as close to the data as possible.

#### Zero Trust

Multifactor authentication protects sensitive files from any threat, even if

they have access to the endpoint or have intercepted the data from a security breach or from the Cloud in transit.

#### Advanced threat sensors

Threat sensors continuously monitor your Windows system for signs of compromise and protect designated files with MFA when a threat is detected.

#### Cloud-based management

Manage all Windows 7/10 devices from a single cloud-based console with global policy settings that make centralized protection of CUI easy and effective.



Cigent Secure SSD™ features the first and only family of self-defending storage devices with cybersecurity built into the firmware itself. They include a dedicated security processor that relies on machine learning to detect and respond to ransomware, a keep-alive sensor that automatically encrypts sensitive files if security software is bypassed, and a safe room that makes data invisible to any attacker. When paired with D<sup>3</sup>E, you can remain confident that your data stays protected throughout the entire device lifecycle.

## Store files with maximum security.

### CMMC Levels 1–3

You can achieve CMMC Levels 1-3 alongside seven core domain requirements with Cigent Secure SSD. The domains this compliance solution addresses are:

- Access Control (AC)
- Identification and Authentication (IA)
- Audit and Accountability (AU)
- Maintenance (MA)
- Media Protection (MP)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

Secure SSD contains the following advantages for CMMC levels 1–3:

### Secure Drive

Use D<sup>3</sup>E to easily set up hardware-encrypted Safe Rooms on the Secure SSD. Designated files are not just inaccessible to an attacker or unauthorized party; they remain completely invisible until mounted by the user via a step-up authentication. Once mounted, if D<sup>3</sup>E or your antivirus software detects a threat, Secure Drives auto-lock until the threat clears and the authorized user re-authenticates.

### Ransomware protection

Certain Cigent Secure SSDs include a dedicated security processor that employs machine learning to automatically detect and repel ransomware attacks, even if host security software is disabled or bypassed. When an attack is detected, sensitive files stored in Safe Rooms automatically lock and disappear from the operating system layer until the threat clears. For files not stored in a Safe Room, Cigent D<sup>3</sup>E employs Zero-Trust multifactor authentication for file access, thus preventing ransomware from accessing and encrypting those files as well.

### Keep Alive Sensor

If the D<sup>3</sup>E software agent is bypassed or disabled by a bad actor, or the Secure

SSD is lost or stolen, protected files lock and Secure Drives encrypt on the fly and remain hidden, invisible, and fully inaccessible to an attacker.

### Dual Mode

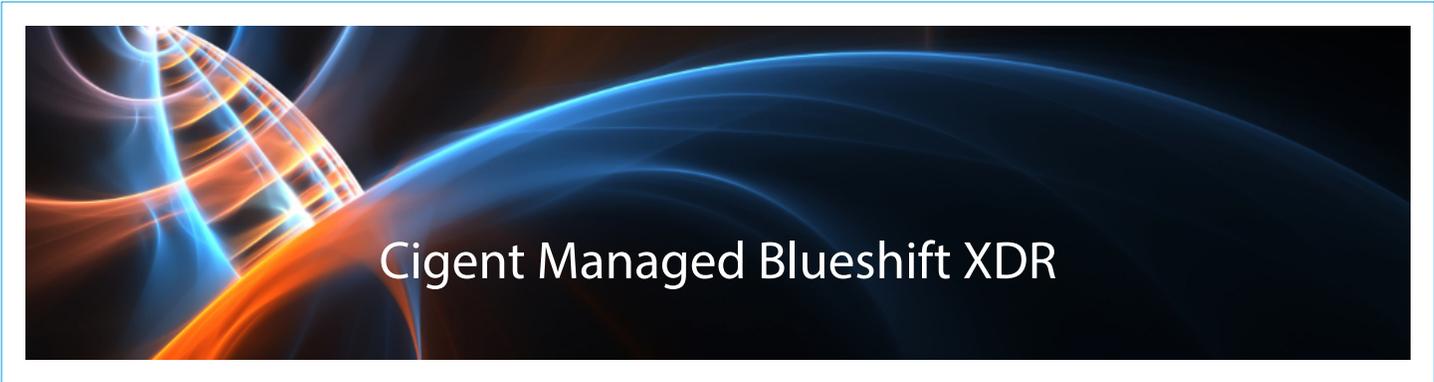
Use D<sup>3</sup>E to set up a hidden drive that remains invisible to the operating system until you flip into it using multifactor authentication. Dual Mode enables numerous use cases: segment your system into work vs personal usage, hide ultra-sensitive files from would-be attackers on the hidden drive, and install two different operating systems and share your system with another user.

### File Access Logging

Firmware archives and protects comprehensive, detailed storage data access logs from being deleted. This enables quick and effective response to endpoint data breaches or insider theft.

### True Erase

When any SSD is repurposed, retired, or destroyed, proper data sanitization must occur if sensitive CUI was previously saved on the system. Research shows that SSDs often inaccurately report successful removal of data. Cigent's built-in verification technology shows exactly what is removed and what information, if any, remains.



Imagine having some of the industry's best cyber security professionals monitoring your entire infrastructure 24/7, detecting and responding to hackers trying to steal or ransom data from any of the devices in your organization. The Cigent Blueshift XDR™ service features several layers of highly automated, advanced detection and response technology, fully managed by Cigent cybersecurity experts. Best of all, Blueshift XDR is affordable, easy to install, and immediately effective.

---

## Prevent threats with a deny-all approach.

---

### CMMC Levels 1–3

You can achieve CMMC Levels 1–3 alongside eight core domain requirements with Blueshift XDR. The domains this compliance solution address are:

- Access Control (AC)
- Audit and Accountability (AU)
- Security Assessment (CA)
- Configuration Management (CM)
- Incident Response (IR)
- Risk Management (RM)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

Cigent Blueshift XDR features the following benefits for CMMC Levels 1–3:

### Cyberthreat Sensor

Blueshift XDR is powered by a plug and protect Cyberthreat Sensor that plugs into your existing firewall or router. All data packets and log files are captured on prem and are available as needed for analysis by Cigent's Security Operations Center.

### Cyber Security Operations Center

Based in the cloud—and staffed by highly trained analysts—the Cigent CSOC does exactly what the cyber-criminals hope you don't do—keep eyes on your security operations at all times, relentlessly identifying vulnerabilities and hunting down and destroying cyber threats in customer environments.

### Cigent for Networks—Network Detection and Response

Install Cigent's C4N cyberthreat sensor in-line to securely inspect and log every data packet that moves in and out of your network. Several layers of advanced network security, including threat intelligence, external and internal deception, intrusion detection and response, advanced network analytics and behavior risk scoring, and network security monitoring are deployed to

identify and block threats. Any communications between any device on the C4N managed network and known compromised infrastructure is automatically blocked.

### Managed SIEM

Blueshift XDR supports monitored security analytics across the entire enterprise including network, cloud, containers, endpoint, server, and remote workers. All logs are uploaded to the cyber threat sensor for analysis, threat hunting, and incident response. Includes reporting and customer insight dashboards for both compliance requirements and security overview.

### Vulnerability Scanning

Blueshift XDR scans your internal network for vulnerabilities on a monthly basis. In addition, agent based vulnerability detection is logged for all assets, on prem, at home, or in the cloud. The CSOC alerts you when urgent vulnerabilities are found.

### Behavioral Network Risk Scoring

C4N profiles the network's behavior over time in order to calculate the risk/likelihood of a cybersecurity incident. Large changes in the risk score are alerted to the Cigent SOC for investigation.