MANAGED SOLUTIONS

Product Sheet

CYBER DEFENSE powered by CyFlare

Cyber Defense CMMC

Cyberattacks are on the rise, making organizations in every industry reconsider what it means to stay secure. And if you're a prime contractor, subcontractor or supplier supporting the Defense Industrial Base, keeping your mission-critical data secure is not an option—it's a requirement.

Our Cyber Defense CMMC (Cybersecurity Maturity Model Certification) solution, powered by CyFlare, assists you on your journey towards attaining your CMMC compliance certification. It enables your organization to meet evolving requirements while strengthening your overall security posture. We'll work closely with you to help simplify this complex process, safeguarding sensitive information and ensuring consistency in cybersecurity and compliance practices.

Key Benefits

Enhanced network security

Our Cyber Defense XDR and EDR solutions are built for organizations working toward CMMC compliance. They're delivered through a FedRAMP-authorized GovCloud environment, providing 24/7 threat detection, automated response and compliant data handling—all backed by US-based operations and a framework aligned to CMMC Level 2 requirements.

Reduced liability

Partnering with an audited SOC means you can transfer your critical security responsibilities to a team of experts. This minimizes your exposure to penalties and lost business due to non-compliance while providing you with peace of mind.

Optimized performance

Receiving a CMMC certification is typically a long and complicated process, even after a SOC is established. Cyber Defense CMMC provides a simpler, faster certification—including staffing, tooling, response playbooks and compliance reporting.

Dedicated support and monitoring

Specialized experts provide complete care to support your everyday needs. You will have a dedicated Crown Castle Client Service Manager focused on providing you with ongoing account support, including billing, account changes and renewals, quarterly business reviews and more. At the same time, we also provide specialized consultation, monitoring and communication expertise from your dedicated CyFlare Customer Success Manager and Systems Engineer.

Greater performance visibility

You'll have access to our Cyber Defense One portal, which provides high visibility into data across clouds, networks, endpoints and applications. This is a single portal for frictionless SOCaaS enablement including live chat, analytics, reporting and more.

Lower capital and operational cost

With our team of experts, you'll receive 24/7/365 monitoring and guidance where and when you need it, minimizing your operational costs.

**Crown Castle's SOC is managed and powered by CyFlare.*

Key Features

- GovCloud Infrastructure allows you to operate with confidence on a platform that's authorized to handle sensitive federal workloads. Your data will remain protected within a secure, government-vetted environment.
- Controls that map to CMMC expectations, including one year of old storage retention, role-based access controls, traceable logging, centralized investigations and response actions—enabling out-of-the-box alignment with dozens of CMMC controls.
- FedRAMP-authorized platforms that allow you to inherit a portion of required controls, streamlining your certification process and minimizing risk during assessments.
- Receive real-time dashboards and audit trails aligned to CMMC requirements, plus monthly or quarterly executive summary reports tailored for government compliance review.
- A team of US-based experts ensure complete alignment with national security and compliance mandates.
- Our SOC* is scheduled to achieve CMMC Level 2 certification through a certified third-party assessment organization (C3PAO) in Q3 2025.

Technical Specifications

Cyber Defense CMMC supports dozens of CMMC Level 2 controls. Reach out to your Cyber Defense expert for the complete Cybersecurity Maturity Model Certification Control Mapping Guide.

A selection of our CMMC controls

Control Group	CMMC control	CMMC Level	How Cyber Defense Helps	Supported Solutions
Access Control	**AC.L2-3.1.5** – Employ the principle of least privilege, including for specific security functions and privileged accounts.	L2	The Cyber Defense One platform monitors/alerts you on privileged access use, monitors/alerts you based on the number of login attempts to detect attacks such as password spraying and monitors/alerts you on remote access risks, including detection for risky public connections such as windows remote desktop protocol (RDP) and server message block (SMB).	For detections: Cyber Defense XDR, Cyber Defense XDR M365 All tools including Cyber Defense One have role based access
	AC.L2-3.1.12 – Monitor and control remote access sessions.	L2	We enable the collection of all remote access sessions and detections for suspicious activities.	Cyber Defense XDR
	AC.L2-3.1.7 – Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	L2	We monitor privilege escalations on machines and stop active threats.	Cyber Defense EDR
Audit and Accountability	**AU.L2-3.3.1** – 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.	L2	Our search and reporting functionality gives you deeper visibility into audit logs for review. Our platform also reports on operational changes or disruptions, including the status of our logging sensor and diagnostics for log flow to alert you in the event of an audit logging process failure.	Cyber Defense XDR Cyber Defense One
	AU.L2-3.3.5 – Correlate audit record review, analysis and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious or unusual activity.	L2	Our search and reporting functionality provides deeper visibility into audit logs. Our platform correlates audit records to indications of suspicious activity and unauthorized access, then provides you with data and prioritized alerts. Our pre-built reports offer the ability to support on-demand analysis and reporting.	Cyber Defense XDR Cyber Defense One
	AU.L2-3.3.6 – Provide audit record reduction and report generation to support on-demand analysis and reporting.	L2	Our threat detection library allows for the automation of audit log analysis to help identify and act on threats and suspicious activity indicators. Our reporting provides visibility to enable organizations to audit broad and pre-machine activities.	Cyber Defense XDR Cyber Defense EDR Cyber Defense One

Crown Castle's SOC is managed and powered by CyFlare.

Control Group	CMMC control	CMMC Level	How Cyber Defense Helps	Supported Solutions
Indicdent Response	**IR.L2-3.6.1** – Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery and user response activities.	L2	We have assisted in purple-teaming for common incidents like password spraying, lateral movement, malicious code execution, privilege escalation and more. We can also test deployments to ensure you can detect and respond to incidents.	Cyber Defense One Cyber Defense Professional Services
	IR.L2-3.6.2 – Track, document and report incidents to designated officials and/or authorities both internal and external to the organization.	L2		
	IR.L2-3.6.3 – Test the organizational incident response capability.	L2		
Risk Accessmenet	**RA.L2-3.11.1** – 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.	L2	You can periodically assess risk to your operations and data with the help of our search and reporting functionality that can generate reports on security and compliance, identifying potential gaps. Our platform employs threat intelligence to guide you on your system and security architecture. It can also detect access using insecure ports via RDP, SMB and others.	Cyber Defense XDR (Complete only)
	RA.L2-3.11.2 – Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	L2	Cyber Defense CRI performs vulnerability scanning and root cause analysis on client systems. It also provides sensitive data scanning and secure configuration baselining to help inform risk.	Cyber Defense CRI
System and Information Integrity	**SI.L2-3.14.6** – Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	L2	With our automated detection and response capabilities, you can monitor your systems and inbound and outbound traffic and detect attacks and indicators of potential attacks. We can also help detect and alert unauthorized access and use of organizational systems.	Cyber Defense XDR Cyber Defense XDR M365

Why Crown Castle?

Our unique, nationwide portfolio
With approximately 90,000 route miles of fiber, we own and operate one of the largest and densest fiber networks in the country with a presence in 23 of the top 25 US markets.

Our proven track record
In our 30+ years of experience owning and operating network assets we've seen it all and we're always ready to adapt to changing network trends.

Our deep expertise
We've worked with nearly every industry so we understand your unique opportunities and challenges and can tailor solutions to meet your goals.

Our solutions

We have your networking and security needs covered. Visit our infrastructure solutions page to learn more about our suite of solutions and how they can solve your toughest challenges.

CROWN CASTLE

Crown Castle owns, operates and leases more than 40,000 cell towers and approximately 90,000 route miles of fiber supporting small cells and fiber solutions across every major US market. This nationwide portfolio of communications infrastructure connects cities and communities to essential data, technology and wireless service—bringing information, ideas and innovations to the people and businesses that need them.

For more information, please contact 1-888-689-6189 or visit **CrownCastle.com**