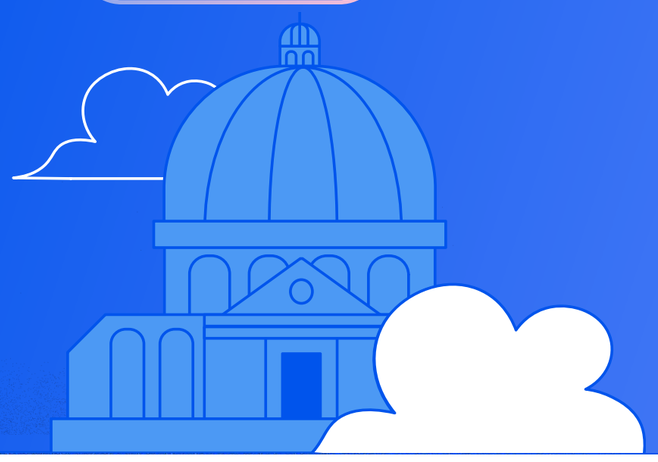
WIZ for Gov

Datasheet

Wiz for CMMC 2.0 Certification



The Cybersecurity Maturity Model Certification (CMMC) is a framework developed by the United States Department of Defense (DoD) to enhance the cybersecurity posture of contractors and subcontractors within the defense industrial base (DIB) and reduce the risk of cyber threats and attacks on sensitive government information. The primary goal of CMMC is to ensure that adequate cybersecurity practices are in place to safeguard Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) that are handled by defense contractors. Following years of development and engagement with Congress and industry stakeholders, CMMC is being phased in. White House action is expected that will require all contractors to meet CMMC requirements in order to do business with the Department.

CMMC consists of a set of cybersecurity standards and practices applicable to three maturity levels. The maturity levels are tiered, each building on the previous one's requirements. Level 1 is the foundational level, which requires you to practice the minimum cybersecurity measures. Level 2 is advanced and mandates intermediate cyber hygiene by implementing 13 domains and 110 security controls from NIST 800-171. Level 3 is expert, which involves stringent security policies based on NIST SP 800-171 & 172 standards.

Wiz strives to make it easier for organizations to secure their cloud environments and meet compliance requirements. Wiz for Gov, our upcoming FedRAMP Moderate authorized environment, enables government customers and mission partners to operate in the cloud with confidence by offering a comprehensive cloud security solution that provides complete visibility, proactive risk reduction, and automated compliance assessment in the cloud. Wiz for Gov can help organizations meet some of the controls required for CMMC certification.

The table below details how Wiz for Gov maps to CMMC 2.0 Level 2 requirements:

Domain	Identifier	Capability	Supports/ Meets	Additional notes
Access Control	3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Supports	Wiz CIEM provides visibility into who can access which resources in your cloud environment and what actions they can perform on them. Wiz analyzes your IAM policies, to help you prevent over-privileging and lateral movement. Wiz flags identities that have excessive permissions, high privileges, admin access, or access to sensitive data.
Access Control	3.1.3	Control the flow of CUI in accordance with approved authorizations.	Supports	Wiz supports full network analysis for both containers and cloud platforms and calculates the effective exposure for every cloud object. Wiz provides visibility into network paths on the Wiz Security Graph, showing resources that are exposed to the internet or can be accessed from external VPCs or accounts.
Access Control	3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Supports	Wiz CIEM provides visibility into who can access which resources in your cloud environment and what actions they can perform on them. Wiz analyzes your IAM policies, to help you prevent over-privileging and lateral movement. Wiz flags down identities that have excessive permissions, high privileges, and admin access.

Domain	Identifier	Capability	Supports/ Meets	Additional notes
Access Control	3.1.22	Control CUI posted or processed on publicly accessible systems.	Supports*	Wiz DSPM analyzes your cloud infrastructure and data assets to determine whether they contain sensitive data or secrets and correlates these data findings with other risk factors, such as external exposure and identity risks, to help you identify any possible data leaks or unauthorized access.
Audit and Accountability	3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.	Supports	Wiz connects directly with your cloud logs to provide additional context and detections related to the events occurring in your environment. This provides extraordinary visibility by connecting the actions performed to the resources on which they were performed and to the principals that performed them.
Configuration Management	3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	Meets	Wiz scans every resource in your cloud environment without agents. The Wiz Inventory page lists all technologies that Wiz has discovered across cloud platform services, coding languages, operating systems, applications, etc. Wiz CSPM provides you with out-of-the-box configuration rules that assess your cloud resources' configuration against security best practices. Wiz also provides built-in host configuration rules that assess your OS and applications against the official Center for Internet Security (CIS) organization checks, DoD Secure Technology Implementation Guides (STIGS) and industry standards.
Configuration Management	3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.	Meets	Wiz CSPM provides you with out-of-the-box configuration rules that assess your cloud resources' configuration against security best practices. Wiz also provides built-in host configuration rules that assess your OS and applications against the official Center for Internet Security (CIS) organization checks, DoD Secure Technology Implementation Guides (STIGS) and industry standards.
Configuration Management	3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	Supports	Wiz scans every technology in your cloud environment without agents, including software, and presents them all in the Inventory page. Your team can then mark the different discovered technologies as approved, unwanted, and unreviewed to monitor usage.

*Supported by Wiz, on the Wiz for Gov feature/product roadmap

Domain	Identifier	Capability	Supports/ Meets	Additional notes
Configuration Management	3.4.9	Control and monitor user-installed software.	Meets	Wiz scans every technology in your cloud environment without agents, including software, and presents them all in the Inventory page. Your team can then mark the different discovered technologies as approved, unwanted, and unreviewed to monitor usage and set up remediation processes for unwanted software.
Incident response	3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	Supports*	Wiz can connect directly with your cloud logs to provide additional context and detections related to the events occurring in your environment. Wiz has built in threat detection rules that Wiz evaluates to detect threats, anomalies, unexpected events, unauthorized access, or risky change of configurations in near real-time on the cloud control plane and workloads in your environment. Wiz also provides an optional cloud-native detection and response eBPF-based executable designed to offer real-time visibility into your cloud and Kubernetes workloads and extend our Cloud Detection and Response offering. Wiz correlates threats across real-time signals and cloud activity in a unified view to uncover attacker movement in your cloud. You can quickly understand the impact of each detection by correlating it on the Wiz Security Graph with associated network, identity, or exposed secrets risks
Risk Assessment	3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Meets	Wiz performs agentless vulnerability scanning of every resource in your cloud environment and surfaces vulnerability findings on the Wiz Security Graph. Wiz then helps you remediate any vulnerability detected in your environment.
Security Assessment	3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	Supports	Wiz assesses your compliance against a set of built-in frameworks, including NIST SP 800-53 Revision 5 and NIST SP 171 Revision 2, and allows you to generate granular reports detailing your compliance posture across your cloud environment.

*Supported by Wiz, on the Wiz for Gov feature/product roadmap

Domain	Identifier	Capability	Supports/ Meets	Additional notes
Security Assessment	3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Supports	Wiz does continuous risk assessment of your cloud environment across vulnerabilities, identities, network exposures, misconfigurations, secrets, and malware. Risks are prioritized and modeled on the Wiz Security Graph so you can proactively remove critical risk.
System and Communications Protection	3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Supports	Wiz can expose cloud resources with improper segmentation and exposed systems through our cloud-native network analysis. Wiz calculates the effective exposure for every cloud object by analyzing the combination of network rules in network management services such as load balancers, firewalls, network interfaces, gateways, VPCs, subnets, etc. and detects resources that can be accessed from external VPCs or accounts, modeling cross-account network paths.
System and Communications Protection	3.13.16	Protect the confidentiality of CUI at rest.	Supports	Wiz's built-in configuration rules detect unencrypted resources in your cloud environment and allows you to quickly remediate them with guidance.
System and Information Integrity	3.14.1	Identify, report, and correct system flaws in a timely manner.	Supports	Wiz's agentless scanning detects vulnerabilities and end-of-life technologies and OS and provides you with patching information for quick remediation.
System and Information Integrity	3.14.3	Monitor system security alerts and advisories and take action in response.	Supports	Wiz's Threat Center shows the most important emerging threats you need to pay attention to and indicates whether Wiz detected them in your environment. The eEmerging threats are collected by the Wiz Threat Research team from various sources, including CISA, CERT-EU, and internal research.
System and Information Integrity	3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	Supports*	Wiz scans VMs, container images, serverless functions, and buckets for potentially malicious software (malware) using agentless scanning. In addition, the Wiz Runtime Sensor complements the malware scan by performing real-time analysis for files that are executed on the workload.

*Supported by Wiz, on the Wiz for Gov feature/product roadmap

Wiz transforms cloud security for customers – including 40% of the Fortune 100 – by enabling a new operating model. Our CNAPP empowers security and development teams to build fast and securely by providing visibility into their cloud environments. With Wiz, organizations can prioritize risk and stay agile. Visit https://www.wiz.io/ for more information.

WIZ for Gov