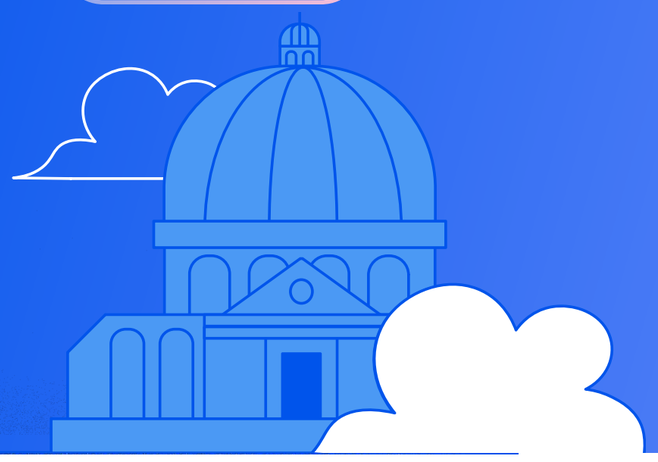
WIZ for Gov

Datasheet

Wiz for CMMC 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. CMMC has entered final ruling, and is effective December 16, 2024.

CMMC consists of a set of cybersecurity standards and practices applicable to three maturity levels. The maturity levels are tiered, with different DoD contracts requiring a specific minimum level for CUI protection. Certification is built around a flow down model, where higher level compliance covers all tiers at lower levels. Level 1 requires self attestation against the 15 security requirements listed in the FAR clause 52.204-21(b)(1). Level 2 requires the level 1 requirements plus an assessment against the 110 security requirements from the NIST SP 800-171r2. Level 2 will require either a self assessment or a third party assessment from a certified C3PAO. Level 3 requires an additional assessment against 24 selected security requirements from the NIST SP 800-172, in addition to the requirements from levels 1 and 2.

Wiz strives to make it easier for organizations to secure their cloud environments and meet compliance requirements. Wiz for Gov 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. This visibility can be enhanced through custom data classification rules, which can be used to scan for, and identify CUI data within an organization's cloud environment. Wiz for Gov can provide insight into an organizations single and multi-cloud environment to assist with self assessments, and can help organizations meet some of the NIST controls required for CMMC certification through a C3PAO.

The table below gives example details on how Wiz for Gov assists with CMMC Level 2 requirements:

Domain	Identifier	Capability	Notes on how Wiz Helps
Access Control	3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Wiz CIEM provides visibility into who can access which resources in your cloud environment and what actions they can perform on them. Wiz analyzes account usage against enabled entitlements for each identity; helping to identify over-privileging. Wiz flags identities that have excessive permissions, high privileges, admin access, and/or access to sensitive data.
Access Control	3.1.3	Control the flow of CUI in accordance with approved authorizations.	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.	Wiz CIEM provides visibility into who can access which resources in your cloud environment and what actions they can perform on them. Wiz analyzes account usage against enabled entitlements for each identity; helping to identify over-privileging. Wiz flags identities that have excessive permissions, high privileges, admin access, and/or access to sensitive data.
Access Control	3.1.22	Control CUI posted or processed on publicly accessible systems.	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.

Wiz for Government provides coverage for

Domain	Identifier	Capability	Notes on how Wiz Helps
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.	Wiz connects directly with your cloud logs to provide additional context and detection related to the events occurring in your environment. This provides expanded 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.	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.	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	3.4.4	Analyze the security impact of changes prior to implementation	Wiz helps your organization to have complete visibility over your cloud environment(s). In addition to understanding what is deployed, Wiz provides context on how different cloud resources are connected, which is useful for understanding risk to changes in configuration, as well as the blast radius for a potential compromise of a cloud component.
Configuration Management	3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities	Wiz scans various cloud components to determine which services are loaded into runtime. This helps you to limit runtime services to only those necessary. Additionally, Wiz enables visibility of ports and protocols with context to which cloud components are accessible. This information can be used to help you to determine which ports, protocols, and services should, or should not, be available within your cloud environment(s).
Configuration Management	3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services	Wiz is able to identify ports and protocols in use within your cloud environment(s). Additionally, Wiz can identify services loaded into runtime within containers, VMs, and serverless deployments. This information can be used to identify deployed components that have been deemed as nonessential for targeted removal.
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.	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.
Configuration Management	3.4.9	Control and monitor user-installed software.	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.

Domain	Identifier	Capability	Notes on how Wiz Helps
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.	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 enables cloud-native detection and response designed to offer real-time visibility into your cloud and Kubernetes workloads. 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.	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.
Risk Assessment	3.11.3	Remediate vulnerabilities in accordance with risk assessments.	The underlying graph database of Wiz enables vulnerabilities to be compared against various risks, including external network exposure, access to sensitive data, presence of over-privileged accounts, misconfigurations, and others. Through this context, Wiz identifies issues which represent the highest risk to your organization for prioritized remediation.
Security Assessment	3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	Wiz examines your cloud environment configurations against many built-in frameworks, including NIST SP 800-53 Revision 5 and NIST SP 171 Revision 2. This helps your organization to evaluate compliance against many of the technical controls within these frameworks. Granular reports against these technical controls can be generated, and potential misconfigurations are highlighted, to allow teams to have greater visibility into areas where actions may need to be taken to better align with required compliance standards.
Security Assessment	3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	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.
Security Assessment	3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	Wiz enables complete visibility into your cloud environment(s) to assist with documentation, including system security plans. Additionally, Wiz contains the ability to create custom Data Classification Rules. These rules can be tailored to help identify the location of CUI within your cloud environment. These actions can be used to assist with defining your organization's CUI boundary for CMMC compliance. This defensible boundary through the information provided by Wiz can be presented to a C3PAO or other third party; reducing the likelihood a CMMC audit will need to be redone prior to the required three year interval should your organization choose to change your C3PAO.

Domain	Identifier	Capability	Notes on how Wiz Helps
System and Communications Protection	3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	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.	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.	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.	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.	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.
System and Information Integrity	3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	In addition to the complete visibility and context provided through the Wiz Security Graph, the Wiz Runtime Sensor enables monitoring of runtime events within VMs, containers, and serverless instances. These events are examined alongside the cloud service provider logs, identity logs, and other sources to help detect unusual or unauthorized activities or conditions.
System and Information Integrity	3.14.7	Identify unauthorized use of organizational systems.	In addition to the complete visibility and context provided through the Wiz Security Graph, the Wiz Runtime Sensor enables monitoring of runtime events within VMs, containers, and serverless instances. These events are examined alongside the cloud service provider logs, identity logs, and other sources to help detect unusual or unauthorized activities or conditions. These capabilities enable your organization to implement continuous monitoring cybersecurity best practices.