White paper

The Practitioner's Guide: Mapping Container Inspection to DoW RMF Controls

anchore

Contents

The Challenge

The state of computing environments is constantly changing. Within a relatively short period of time, we have gone from bare metal servers, to virtualization, to Kubernetes and containerized applications, and now to serverless computing options in the cloud. This means that cybersecurity practices are always evolving, which is especially true in United States Government sanctioned computing environments. Whether on-premises or cloud-based, every environment brings unique challenges along with various levels of complexity and different risk landscapes. This guide focuses on containers: what they are, what they do and how to protect them. It will cover applicable controls that can be inspected, assessed, and continuously monitored.

What Is a Container?

Containers are portable, deployable packages of software that bundle an application's code with all required dependencies needed for execution, including: libraries, system tools, settings, and even the underlying operating system.

What Problems Do Containers Solve?

- **Consistency**: A containerized application runs consistently across different environments. Whether on a developer's local machine, a cloud-based Kubernetes cluster, or an on-premises server, containers allow an application to be deployed as a self-contained package, eliminating "it works on my machine" issues by bundling all necessary dependencies.
- **Efficiency (Time):** Startup time for an application is greatly reduced compared to traditional virtual machines. Because containers share the host's operating system kernel rather than booting a full guest OS, they can instantiate in seconds, significantly reducing deployment cycles and resource overhead.
- **Resilience:** Because containers are ephemeral and disposable, they provide high system resilience. If a container fails or behaves unpredictably, it can be instantly terminated and replaced with a clean, known-good instance from the original image without affecting the broader system.
- **Security:** Containers benefit from process isolation, using kernel namespaces to ensure that an application remains "caged" and unable to see or interfere with other processes on the host. Furthermore, because containers are built from immutable images, the attack surface is reduced; any unauthorized file changes are wiped away upon the next restart.
- **Scaling:** When paired with an orchestrator like Kubernetes, containerized applications scale effortlessly by spinning up identical replicas to meet demand. The orchestrator automatically balances incoming traffic across these replicas, ensuring consistent performance during traffic spikes.

Automating Container Security and Compliance

As container adoption accelerates across the DoW, securing the software supply chain becomes increasingly complex. Each container image is built with a unique web of application dependencies, possibly harboring hidden vulnerabilities, embedded secrets, or unauthorized software. In high-velocity CI/CD pipelines where thousands of images are built daily, manual inspection is impossible and can lead to information overload and critical security gaps.

Anchore Enterprise alleviates this administrative burden for ISSMs, ISSOs, and Security Engineers by automating deep image inspection and policy enforcement, using policy-as-code. Anchore Enterprise provides the granular insights necessary to verify software origins, versioning, and integrity—even in air-gapped environments.

By contributing to zero-trust architecture and utilizing Policy-as-Code, Anchore Enterprise ensures every container meets cybersecurity standards prior to deployment. With pre-built, production-ready policy packs mapped to NIST 800-53 controls, organizations can bake compliance directly into the development lifecycle, ensuring a hardened risk posture from development through deployment.

The Policy Control Map

Anchore Enterprise addresses numerous NIST 800-53 controls as indicated through the security control matrix below in two different ways via our Anchore Enterprise product deployment (Platform) and our policy-as-code engine (Policy). The table below breaks down the NIST 800-53 Control identifier, the name of the control, how Anchore Enterprise supports the control, and whether it's a platform or policy capability.

1. Anchore Enterprise product capability: PLATFORM
2. Anchore Enterprise policy-as-code capability: POLICY

Control Identifier	Control (or Control Enhancement) Name	Anchore Enterprise Role	Anchore Enterprise Capability
AC-2(1)	Account Management | Automated System Account Management	Accounts can be managed in one of three ways: Single-Sign-On, Lightweight Directory Access Protocol (LDAP), or native accounts.	PLATFORM
AC-2(7)	Account Management | Privileged User Accounts	Using built-in role-based access controls, privileged users have the least amount of rights to do their job.	PLATFORM

Control Identifier	Control (or Control Enhancement) Name	Anchore Enterprise Role	Anchore Enterprise Capability
AC-3	Access Enforcement	Role-based access controls and multi-tenancy enforce access controls to ensure least-privilege and need to know. There are numerous roles to ensure that humans or service accounts have the privileges needed to execute their statement of work.	PLATFORM
AC-3(7)	Access Enforcement | Role-based Access Control	Role-based access controls and multi-tenancy ensure least-privilege and need to know. Roles include but are not limited to: image analyzer, admin, registry_editor, policy_editor, and read-only. For more information: https://docs.anchore.com/current/docs/configuration/user_management/rbac/	PLATFORM
AC-5	Separation of Duties	Duties can be separated by tenants and accounts via role based access controls: https://docs.anchore.com/current/docs/configuration/user_management/rbac/	PLATFORM
AC-6	Least Privilege	Based off several roles within Anchore Enterprise from read-only, to image analysis to vulnerability annotation. Least privilege is built in.	POLICY
AC-6(1)	Least Privilege | Authorize Access to Security Functions	Security functions are broken down here: https://docs.anchore.com/current/docs/configuration/user_management/rbac/	PLATFORM
AC-6(10)	Least Privilege | Prohibit Non-privileged Users from Executing Privileged Functions	Using built in role-based access controls, privileged users have the least amount of rights to do their job.	POLICY
AC-6(5)	Least Privilege | Privileged Accounts	Using built in role-based access controls, privileged users have the least amount of rights to do their job.	POLICY PLATFORM
AC-8	System Use Notification	Logon Banner can be configured to show the classification of the system and applicable color scheme.	PLATFORM
AU-2	Event Logging	Log events include but are not limited to: user authentication, rbac, role changes and api key management. https://docs.anchore.com/current/docs/configuration/logging/	PLATFORM

Control Identifier	Control (or Control Enhancement) Name	Anchore Enterprise Role	Anchore Enterprise Capability
AU-3	Content of Audit Records	Audit records contain the type of event, when it occurred, the source and outcome. https://docs.anchore.com/current/docs/configuration/logging/	PLATFORM
CA-5	Plan of Action and Milestones	Create time based allowlists based off "authorized" policy gates & triggers to pass an Anchore Enterprise scan.	POLICY
CA-5(1)	Plan of Action and Milestones | Automation Support for Accuracy and Currency	Allowlists require unique TriggerIDs to be authorized to obtain a "Go or Pass" decision.	POLICY
CA-7	Continuous Monitoring	Images in Anchore Enterprise are continuously monitored for new vulnerabilities as definitions are changed to the vulnerability database.	PLATFORM
CA-7(3)	Continuous Monitoring | Trend Analyses	Capture trends to see risk reduction of vulnerabilities & policy violations across images & SBOMs.	PLATFORM
CA-7(4)	Continuous Monitoring | Risk Monitoring	Continuously monitor for effectiveness of policy, vulnerability & changes via alerts/notifications.	PLATFORM
CA-7(6)	Continuous Monitoring | Automation Support for Monitoring	Continuously monitor all SBOMs & images within Anchore Enterprise for vulnerabilities.	PLATFORM
CM-10	Software Usage Restrictions	Software licenses are detected via Anchore Enterprise analysis. Policy-as-code can be applied to block the deployment of licenses.	POLICY
CM-10(1)	Software Usage Restrictions | Open-source Software	Enforce restrictions to organizational requirements using policy to block or allow open source software.	POLICY
CM-12	Information Location	Scan both registries and monitor via Kubernetes inventory the location of deployments. Also leverage annotations with key value pairs for downstream disconnected deployments.	PLATFORM
CM-2	Baseline Configuration	Establish baseline configurations for dockerfiles based off registry, repository or tag using policy-as-code.	POLICY

Control Identifier	Control (or Control Enhancement) Name	Anchore Enterprise Role	Anchore Enterprise Capability
CM-2(2)	Baseline Configuration | Automation Support for Accuracy and Currency	Changelogs are provided for images to show the differences between images.	POLICY
CM-2(3)	Baseline Configuration | Retention of Previous Configurations	AE saves the dockerfile and sbom for all analyzed images.	PLATFORM
CM-2(6)	Baseline Configuration | Development and Test Environments	All AE images are tracked for configuration for organization of both development & test images.	PLATFORM POLICY
CM-3	Configuration Change Control	Leverage the changelog with container images to compare what changes are made between images with the same tag.	PLATFORM
CM-3(2)	Configuration Change Control | Testing, Validation, and Documentation of Changes	Images are tested against organizations security policy to ensure that only images that meet company requirements are released. Use integrity mechanisms to ensure all files or content are validated.	PLATFORM
CM-3(4)	Configuration Change Control | Security and Privacy Representatives	Role based access controls are used to ensure only authorized users can update policy and use vulnerability exchange (VEX) annotation.	PLATFORM
CM-3(5)	Configuration Change Control | Automated Security Response	Images are continuously scanned for vulnerabilities and notifications can be sent if/ when a vulnerability is sent to trigger a security response.	PLATFORM
CM-3(6)	Configuration Change Control | Cryptography Management	Ensure only authorized cryptographic modules are deployed in container images using policy-as-code.	POLICY
CM-3(7)	Configuration Change Control | Review System Changes	Trigger alerts when image tags are updated or a new vulnerability is found.	PLATFORM
CM-4	Impact Analyses	Analyze images, open source code, or even a vmdk by generating an sbom to understand impact from a CVE perspective.	PLATFORM
CM-4(2)	Impact Analyses | Verification of Controls	Validate & verify each image meets policy requirements via an AE image scan.	POLICY

Control Identifier	Control (or Control Enhancement) Name	Anchore Enterprise Role	Anchore Enterprise Capability
CM-5(5)	Access Restrictions for Change | Privilege Limitation for Production and Operation	Limit what registries or images can have certain application packages prior to deployment.	POLICY
CM-6	Configuration Settings	Use Anchore policy with rule sets, allowlists, and mappings to reflect the most restrictive settings on a case-by-case basis to implement on applicable images, source or 3rd party SBOMs. All deviations (allowlists) contain descriptions and are time based, thus providing the evidence for the exception.	POLICY
CM-6(1)	Configuration Settings | Automated Management, Application, and Verification	Anchore Enterprise's robust policy is used to automate policy scans, apply the applicable configurations, and verify the policy on a continuously monitored basis.	POLICY
CM-6(2)	Configuration Settings | Respond to Unauthorized Changes	Leverage policy-as-code to ensure only authorized changes to images are made using authoritative pipelines and role based access controls. Notifications can be sent for failed image analysis.	PLATFORM
CM-7	Least Functionality	Configure scans to identify and restrict usage to only provide mission essential capabilities, such as ports, protocols, software and/or services.	POLICY
CM-7(2)	Least Functionality | Prevent Program Execution	Denylist packages from being deployed to production, thus preventing their execution in an unauthorized manner.	POLICY
CM-7(3)	Least Functionality | Registration Compliance	Enforce compliance to ensure only authorized functions, ports, protocols and services are used in container images.	POLICY
CM-7(4)	Least Functionality | Unauthorized Software — Deny-by-exception	Implement Deny-by-exceptions policy to prohibit the use of unauthorized software using policy-as-code.	POLICY
CM-7(5)	Least Functionality | Authorized Software — Allow-by-exception	Implement allow-by-exceptions policy to prohibit the use of unauthorized software using policy-as-code.	POLICY

Control Identifier	Control (or Control Enhancement) Name	Anchore Enterprise Role	Anchore Enterprise Capability
CM-7(8)	Least Functionality | Binary or Machine Executable Code	Generate an SBOM for opensource code and allow list it in Anchore Enterprise to authorize it for use.	POLICY
CM-8	System Component Inventory	All objects within Anchore Enterprise begin with an SBOM thus creating the software component inventory.	PLATFORM
CM-8(1)	System Component Inventory | Updates During Installation and Removal	Because of the SBOM-centric deployment, the component inventory remains accurate and up-to-date even as images or SBOMs are removed from the system.	POLICY
CM-8(2)	System Component Inventory | Automated Maintenance	Because of the SBOM-centric deployment, the component inventory remains accurate and up-to-date even as images or SBOMs are removed from the system.	POLICY
CM-8(3)	System Component Inventory | Automated Unauthorized Component Detection	Use policy-as-code to detect unauthorized packages using denylisting.	
CM-8(6)	System Component Inventory | Assessed Configurations and Approved Deviations	Approved Deviations can be set via policy-as-code that can be specific to one or all of the following: Registry, repository or tag.	POLICY
CM-8(7)	System Component Inventory | Centralized Repository	All SBOMs are stored in Anchore Enterprise and can be obtained via API.	
IA-2	Identification and Authentication (organizational Users)	Accounts can be managed in one of 3 ways: Single-Sign-On, Lightweight Directory Access Protocol (LDAP), or native accounts.	PLATFORM
IA-2(10)	Identification and Authentication (organizational Users) | Single Sign-on	Accounts can be managed in one of 3 ways: Single-Sign-On, Lightweight Directory Access Protocol (LDAP), or native accounts.	PLATFORM
IA-5(7)	Authenticator Management | No Embedded Unencrypted Static Authenticators	Scan images for unencrypted static authenticators such passwords, private keys, and API keys.	POLICY

Control Identifier	Control (or Control Enhancement) Name	Anchore Enterprise Role	Anchore Enterprise Capability
IA-6	Authentication Feedback	Data typed into the password field is obscured.	PLATFORM
IR-4	Incident Handling	Search across all images/SBOMs/Open source code for CVEs as part of incident handling.	PLATFORM
PM-30	Supply Chain Risk Management Strategy	Generate an SBOM prior to code being executed in your network to make a risk decision.	PLATFORM
PM-31	Continuous Monitoring Strategy	Continuously scan images for vulnerabilities.	PLATFORM
PM-4	Plan of Action and Milestones Process	Use allow lists to enforce Plan of Action & Milestones (POA&M) via code.	POLICY
PM-5	System Inventory	Continuously inventory systems via registry scans and Kubernetes inventory to maintain an up-to-date and accurate system inventory.	PLATFORM
RA-10	Threat Hunting	Search every asset within Anchore Enterpise for CVEs to discover containers, vmdks, or open source code to determine the location of zero day threats.	PLATFORM
RA-3	Risk Assessment	Identify vulnerabilities across images by leveraging data from CVE, CVSS, KEV and EPSS.	PLATFORM
RA-3(1)	Risk Assessment | Supply Chain Risk Assessment	Scan container images for malicious code, defective or vulnerable components.	PLATFORM
RA-5	Vulnerability Monitoring and Scanning	Continuously scan SBOMs, Container images, and open source code.	PLATFORM POLICY
RA-5(2)	Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned	Vulnerabilities are updated either automatically or manually (if air-gapped).	PLATFORM
RA-5(3)	Vulnerability Monitoring and Scanning | Breadth and Depth of Coverage	All data is stored as an SBOM within Anchore Enterprise and is scanned continuously for vulnerabilities.	PLATFORM

Control Identifier	Control (or Control Enhancement) Name	Anchore Enterprise Role	Anchore Enterprise Capability
RA-5(8)	Vulnerability Monitoring and Scanning | Review Historic Audit Logs	Anchore Enterprise uses both Exploit Protection Scoring System (EPSS) & Known Exploit Vulnerability (KEV) to show end users both the likelihood of exploit within 30 days & if there is a known exploit.	PLATFORM
SA-10(1)	Developer Configuration Management | Software and Firmware Integrity Verification	Use Anchore Enterprise with changelogs, policy-as-code to perform configuration management, during development, implementation, and operation of container images. Approved changes are captured via CI/CD process through merge or pull requests. Only authorized users can change policy-as-code within Anchore Enterprise. Flaws and updates are tracked via image scans.	POLICY
SA-11	Developer Testing and Evaluation	Suport ongoing testing & evaluation during the scan phase, after build, to assess for security & privacy controls by generating evidence and identifying flaws along with the respective correction.	PLATFORM
SA-15	Development Process, Standards, and Tools	Anchore Enterprise is a tool that explicitly addresses security & privacy controls for the development process by documenting and ensuring the integrity of changes to software.	PLATFORM
SA-15(7)	Development Process, Standards, and Tools | Automated Vulnerability Analysis	Anchore Enterprise performs automated vulnerability analysis on all active SBOMs/Images and sources data from CVE, EPSS, KEV and others to determine exploit potential. The results are exportable as artifacts to provide to an assessor.	PLATFORM
SA-22	Unsupported System Components	Vulnerability findings indicate whether a found vulnerability won't be fixed, thus making the component or package end of life.	PLATFORM
SA-3	System Development Life Cycle	Anchore Enterprise lives within CI/CD to shift left to provide security & compliance issues against privacy, threats & vulnerabilities to critical applications and business functions.	PLATFORM
SA-4(8)	Acquisition Process | Continuous Monitoring Plan for Controls	Continuously monitor containers, vmdks, and open source developed software by scanning with Anchore Enterprise and generating alerts on new CVEs allowing the organization to respond to known issues that are deployed downstream.	PLATFORM

Control Identifier	Control (or Control Enhancement) Name	Anchore Enterprise Role	Anchore Enterprise Capability
SA-4(9)	Acquisition Process | Functions, Ports, Protocols, and Services in Use	Anchore Enterprise inspects DockerFiles to validate ports, protocols & services are configured according to organizational standards.	POLICY
SA-5	System Documentation	Use Anchore Enterprise to document the Dockerfile configuration, layers, metadata along with known vulnerabilities and evidence as to why an image passed an Anchore Enterprise scan.	PLATFORM
SA-8	Security and Privacy Engineering Principles	Scan application to assess the current state of software to determine upgrades. Use secure development practices for container images to ensure consistent sanctioned builds using policy-as-code. From configuration and file validation to allowlisting packages, denying distros and even Docker instructions, this is all set via Anchore Enterprise.	PLATFORM
SA-8(1)	Security and Privacy Engineering Principles | Clear Abstractions	Set authorized ports, protocols and services via policy-as-code to ensure only authorized interfaces are exposed.	PLATFORM
SA-8(10)	Security and Privacy Engineering Principles | Hierarchical Trust	Leverage policy-as-code to ensure only authorized packages are present in Container Images, Filesystems, and 3rd party SBOMs.	POLICY
SA-8(14)	Security and Privacy Engineering Principles | Least Privilege	Ensure only the correct permissions are applied to files/binaries/packages in a container image.	POLICY
SA-8(30)	Security and Privacy Engineering Principles | Procedural Rigor	Inspect Dockerfiles from instructions, passwords, file content, configuration and packages to ensure continuous compliance.	PLATFORM
SA-8(9)	Security and Privacy Engineering Principles | Trusted Components	Validate that only authorized components are installed to include only authorized base images.	PLATFORM
SC-18	Mobile Code	Detect mobile code packages via SBOM or images.	POLICY
SC-18(1)	Mobile Code | Identify Unacceptable Code and Take Corrective Actions	Allowlist or denylist mobile code from being deployed to production environments.	POLICY

Control Identifier	Control (or Control Enhancement) Name	Anchore Enterprise Role	Anchore Enterprise Capability
SC-18(2)	Mobile Code | Acquisition, Development, and Use	Ensure only authorized commands and packages are ran within images to stop presence of mobile code.	POLICY
SC-5	Denial-of-service Protection	Detect and enforce HEALTHCHECKS are available in container images.	POLICY
SI-2	Flaw Remediation	Detect flaws or CVEs within SBOMs/Images and the applicable upgrade to remove the flaw.	POLICY PLATFORM
SI-2(2)	Flaw Remediation | Automated Flaw Remediation Status	Scan images/SBOMs for packages along with showing the fix (if available) or if a fix is not present.	POLICY PLATFORM
SI-2(3)	Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions	Measure the time taken to update and remediate flaws.	PLATFORM
SI-3	Malicious Code Protection	Scan images for malicious code.	PLATFORM
SI-5	Security Alerts, Advisories, and Directives	Alert based on vulnerabilities discovered through continuous monitoring.	PLATFORM
SR-4	Provenance	Ensure Docker files are built from a trusted source such as Chainguard.	POLICY

As shown in the table above, Anchore Enterprise implements multiple security controls to enforce Zero Trust, Continuous Monitoring, Continuous Compliance, and alerting! Policies can easily be mapped to meet categorization of systems to ensure compliance with the applicable NIST 800-53 controls that must be implemented. Policy packs are not only available for purchase from Anchore but also can be built by our end users.

About Anchore

Anchore enables organizations to speed up digital transformation and reduce risks by streamlining the development of secure and compliant cloud-native applications. Anchore's solutions integrate with existing DevOps toolchains to automate security and compliance checks throughout the software development lifecycle. Organizations can reduce costs and accelerate time to market by remediating security and compliance issues early and continuously.

To learn more about Anchore's solutions, visit **Anchore.com.**

Book a demo

anchore

sales@anchore.com

anchore.com