# CHECKLIST:

# How to Prepare for the FedRAMP Vulnerability Scanning Requirements for Containers

## Introduction

The Federal Risk and Authorization Management Program (FedRAMP) empowers federal agencies to move applications and data to the cloud for the benefit of their agency partners and constituents. Industry estimates place the cost of projects to achieve FedRAMP certification between $75,000 and $3.5 million.[1] FedRAMP covers at least 325 security controls as defined by NIST for a "Moderate" impact system and 421 controls for a "High" impact system.

Software vendors and system integrators have increasingly turned to containers as a way to speed delivery for the cloud applications they offer. The recently released FedRAMP Vulnerability Scanning Requirements for Containers details new requirements that are specific to containerized applications. This document supplements existing FedRAMP controls, including the FedRAMP Continuous Monitoring Strategy Guide and FedRAMP Vulnerability Scanning Requirements. The following best practices offer federal agencies and the vendors that serve them an expedited path to FedRAMP for containerized applications.

[1] https://www.coalfire.com/the-coalfire-blog/september-2016/cost-of-fedramp-assessment-from-a-3pao-perspective

# Checklist

Here are some tips for helping your teams prepare new containerized applications for FedRAMP authorization and adapt your already-authorized applications to the new FedRAMP Vulnerability Scanning Requirements for Containers:

## GENERAL TIPS

□ **Identify a core group inside your organization with FedRAMP expertise.** Developers may not have compliance expertise. Cybersecurity experts may not have software development expertise. While these experts don't have to sit in the same group, look for ways, they can share their expertise across development teams on projects that require achieving Authority to Operate (ATO).

□ **Embrace and follow the Agency Authorization Playbook by FedRAMP** which includes best practices for agencies and cloud service providers (CSPs) and step-by-step guidance to follow through the pre-authorization, during authorization, authorization, and post-authorization phases that lead to an ATO.

□ **Engage with the FedRAMP PMO regularly** to monitor their latest thinking about container vulnerability scanning as they receive feedback from the field. The FedRAMP PMO also communicates with "in process" projects regularly and whenever circumstances require so take advantage of those times. The more proactive your organization is in engaging with the PMO, especially if there is an authorization roadblock, the more successful they are in moving from "In Process" to "FedRAMP Authorized."

## CONTAINER TIPS

□ **Follow all of the relevant documentation and guidance** for the FedRAMP Low, Moderate, and High-Security Control Baselines, the FedRAMP Continuous Monitoring Strategy Guide, the FedRAMP Vulnerability Scanning Requirements guide, as well as the new FedRAMP Vulnerability Scanning for Containers.

□ **Be proactive if you have to create a transition plan** for your currently authorized FedRAMP system to meet the FedRAMP Vulnerability Scanning Requirements for Containers because your organization has one month to create the plan and six months to transition your system to full compliance.

□ **Cultivate container and container security expertise across your development teams.** Look for free and fee-based online training to skill up your teams with container skills. There are a growing number of online training options from commercial training providers and vendors.

□ **Automate and integrate container security across your dev, test, staging, and production environments.** It takes longer and costs more to address compliance and security issues in a production environment, which could slow FedRAMP authorization.

□ **Select container security tools that have flexible APIs and are easy to integrate** in order to enable your DevSecOps teams to harden containers that meet relevant FedRAMP requirements composed from the National Checklist Program and defined by the National Institute of Standards and Technology (NIST) SP 800-190 and NIST 800-53.

□ **Make sure you are watching your registry for new tags**, conducting scans on everything in your registry. New registry tags that you didn't expect can be signs of a malicious attack.

□ **Make sure your project teams are scanning containers every 30 days** and that you enact container registry monitoring to monitor per unique image to ensure that containers corresponding to an image that has not been scanned within the 30-day vulnerability scanning window are not actively deployed on production.

□ **Incorporate container security tools into your DevOps pipeline** that can detect and provide recommendations automatically on remediating FedRAMP compliance issues as it relates to container security.

□ **Assign a unique asset identifier to every image class** which corresponds to one or more production-deployed containers. You must document these image-based asset identifiers in the FedRAMP Integrated Inventory Workbook Template. CSPs must implement automated mechanisms to track containers in production. Your 3PAO must validate the mechanism. Consult the FedRAMP Vulnerability Scanning Requirements for Containers for more information about working with asset identifiers as a CSP.

□ **Utilize only hardened containers as a CSP** and where applicable the hardening must be in accordance with relevant benchmarks listed in the National Checklist Program and defined by the National Institute of Standards and Technology (NIST) SP 800-70. Benchmarks are used as a baseline and may be altered. Consult the FedRAMP Vulnerability Scanning Requirements for Containers for more information about working with your 3PAO to validate your hardened containers.

## Expedite FedRAMP with Anchore

Anchore provides a continuous security and compliance platform for containers that can be used to implement best practices identified here and expedite the process for FedRAMP authorization for your containerized applications. Anchore also provides a specific Federal edition for air-gapped environments that meets security requirements ranging from DoD IL-2 to DoD IL-6. It's currently in use as a container

Headquartered in California with offices in Virginia and the UK, Anchore customers include large enterprises and government agencies that require secure and compliant cloud-native applications. To learn more about Anchore's solutions, visit www.Anchore.com.

anchore.com    info@anchore.com

anchore