



Achieving FedRAMP Compliance

How Autodesk achieved FedRAMP compliance with Witness & Archivista



Challenge

Autodesk, the Design and Make Platform Company, which develops leading creative software including AutoCAD, is a SaaS supplier to the federal government. To support the security needs of federal agencies and contractors, it has evolved its secure software development practices and achieved its Authorization to Operate (ATO) under the Federal Risk and Authorization Management Program (FedRAMP) moderate impact level.

With a continuous stream of acquisitions Autodesk operates a complex, heterogeneous tech stack blending a variety of open-source projects. To make sense of this heterogeneity, Autodesk is working to capture a variety of data throughout its software delivery lifecycle (SDLC) and bolster required compliance requirements.

Autodesk uses this data to secure its SDLC from attack vectors like dependency confusion and typo-squatting. By centralizing infrastructure as code (IaC) execution and implementing provenance collection and verification, Autodesk can mitigate these, and similar, risks effectively.



“The fact that TestifySec is so receptive to contributions made me feel that we made the right decision with Witness.”

Jesse Sanford
Software Architect at Autodesk



The fact that **Witness** and **Archivista** have reduced developer friction so significantly has really set the in-toto framework apart for us. This tooling makes the process incredibly smooth and means we can now run secure by default. We don't have to ask our software development teams to go through any hurdles to get to the point where proof is generated. Instead, we can leverage toolchains in the critical path of software being promoted to production, to generate enough trust.”

Jesse Sanford
Software Architect at Autodesk

Solution

Autodesk integrated Witness and Archivista into its CI/CD pipelines, automating the collection of critical provenance data and eliminating manual compliance tasks. This integration leveraged Witness's dynamic command line interface (CLI) observability to generate trusted telemetry, creating a seamless audit trail throughout the SDLC. Additionally, Archivista served as a centralized graph database for storing and querying in-toto attestations, enabling real-time policy validations without manual intervention. This combination streamlines governance processes and enhances security by ensuring only signed and verified software is deployed.



Achieving FedRAMP Compliance

CASE STUDY

Impact

Integrating these tools enabled all Autodesk pipelines to easily generate and store provenance and attestation data, creating a seamless trail that can be audited at any point in the SDLC. Witness provides drop-in generation of provenance for software artifacts and Archivista provides a foundation for compliance evidence gathering. Together, these tools have made meeting numerous software supply chain security control requirements possible.

FedRAMP ATO: Achieved

Opening access to new markets

Automation

of evidence collection via Witness +
Archivista

Increased Accuracy

Trusted Telemetry improves audit
findings

How Autodesk automates FedRAMP compliance and evidence collection

Like many large software producers, Autodesk's concerns about supply chain security across the wider industry (following incidents like the Solarwinds attack) had already driven considerable improvements in its security posture. For instance, Autodesk leaned heavily into the SLSA Framework and was producing SBOMs and signing its container images. However, the patterns and practices were new to the enterprise. To meet this challenge, Autodesk, along with other industry leaders, founded the Cloud Native Operational Excellence group (CNOE) – which aims to explore the problem spaces around modern software delivery, and at the forefront of that effort is software supply chain security.

In further advancement of those efforts, Autodesk is building robust tools that enable development teams to easily generate attestations to provide assurances during its SDLC processes. For instance, it has published a reference architecture and presented at KubeCon on the use of attestations to prove the trustworthiness of builds, or their artifact outputs.

Managing security across a complex stack

With a continuous stream of acquisitions, Autodesk operates a complex, heterogeneous tech stack blending a variety of open-source projects.

Its AppSec team handles managing mission-critical tooling, and maintaining security and compliance across a variety of aspects of the Autodesk SDLC. The AppSec team evaluated many security tools that have software supply chain security offerings. However, despite broad coverage, there was a lack of an open specification for evidence collection making integrating them with existing tech more difficult.

Jesse Sanford, Software Architect at Autodesk, helped design a system to perform container image signing for container-based workloads that use their CD platform, which helped with FedRAMP controls concerned with container provenance. Originally, he wanted to store these signatures and additional attestations in an OCI-compliant registry, but tying the attestations together into a useful “story” was difficult. Looking for a solution that would capture the required data and reduce developer effort to integrate tooling, he discovered Witness and then Archivista on the Cloud Native Computing Foundation (CNCF) landscape – open-source projects created and maintained by TestifySec that are part of the in-toto project.

Creating a seamless audit trail

Witness is a CLI observability tool that integrates into software development pipelines, helping organizations shift compliance left by observing developer actions. Witness provides an audit trail across the entire SDLC by implementing the in-toto specification. It provides verification of the end-to-end process with a policy engine, ensuring software is handled safely from source to deployment. Witness works hand-in-hand with Archivista – a graph and storage service for in-toto attestations that enables discovery and retrieval of attestations for software artifacts, allowing users to validate Witness policy without manually listing expected attestations. The fact that the in-toto project is also going through the graduation process at the CNCF was another plus for Autodesk, which values the impartial open-source governance provided by the foundation.



Witness was absolutely the best fit for us. A single CLI tool that uses the in-toto specification, that can be plugged in to generate attestations and then defer policy decisions to later in the process – it is incredibly powerful.

Jesse Sanford
Software Architect at Autodesk

Technical Workflow

Integrating these tools enabled all Autodesk pipelines to easily generate and store provenance and attestation data, creating a seamless trail that can be audited at any point in the SDLC. Witness provides drop-in generation of provenance for software artifacts and Archivista provides a foundation for compliance evidence gathering. Together, these tools have made meeting numerous software supply chain security control requirements possible.

Static Analysis & SBOM Creation

Witness wraps the analysis of Terraform modules, capturing critical metadata and ensuring full traceability.

SBOMs are generated for each module, documenting dependencies. Witness then captures and stores the SBOM in Archivista

Software Building and Testing

Witness generates attestations during each build and test step, ensuring provenance for all components.

Centralized Storage & Verification with Archivista

Archivista stores all attestations centrally, allowing for easy retrieval and validation through GraphQL. This enables real-time policy checks, ensuring compliance at every step in the SDLC.

Policy Enforcement & Deployment

During deployment, Witness and Archivista verify attestations, allowing only signed and compliant modules to proceed.

This creates an audit trail that ensures compliance and reduces the risk of audit findings.

Achieving FedRAMP ATO

Today, Autodesk has added Witness and Archivista into several of its CI/CD toolchains. This has helped meet FedRAMP Supply Chain Security compliance requirements that were critical to achieving their ATO. Using these tools, Autodesk can easily generate and store provenance and attestation data, creating a seamless trail that can be audited at any point in the SDLC, and allowing developers to work without being interrupted by manual compliance tasks.

Next Steps

Having reaped the benefits of cryptographic attestations with Witness and Archivista, Autodesk can more quickly provide evidence for compliance across many controls and standards. This makes it easier to enter new markets and engage with demanding consumers, including accessing the FedRAMP marketplace.

Autodesk’s AppSec and Developer Enablement teams are working together on a vision for how attestations can drive further policy decisions, including automatically failing deployments that are unsafe, or when an unexpected change is detected in their SDLC. They are also adopting Archivista to create a common data lake across of attestations for on-demand querying at scale from any point in the SDLC, as the surrounding tech stack continues to evolve.

Throughout this process, the AppSec team at Autodesk has been regularly contributing back to the in-toto framework, to continuously improve the project for all open-source users. In fact, soon after adopting Witness, they contributed a pull request, which was quickly reviewed and merged.