Continuous Monitoring Infrastructure for FedRAMP 20x

Evidence Architecture for Persistent Validation, KSI Alignment, and Machine-Readable Authorization

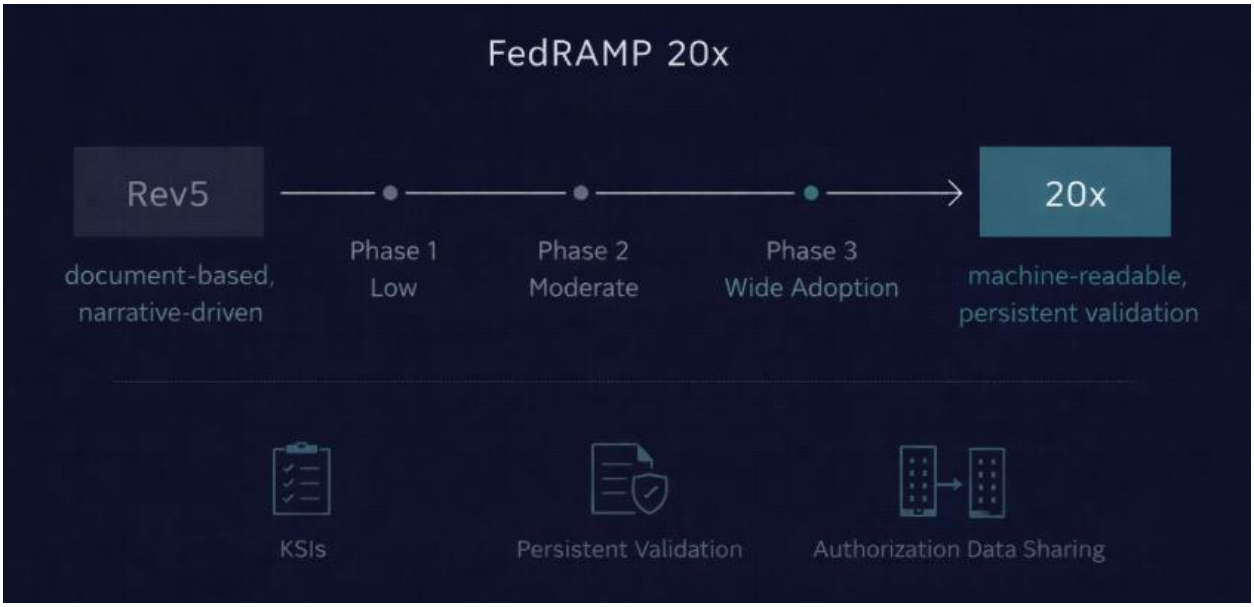
Executive Summary

FedRAMP 20x replaces document-based authorization with persistent, automated validation. Key Security Indicators must be validated at least every three days for machine-based resources, authorization packages must be machine-readable, and assessors evaluate the validation process itself — not a compiled artifact package. The era of narrative-driven compliance and point-in-time assessment is ending.

Most organizations are not architecturally prepared for this shift. Their compliance processes were built to produce documents on a cycle — not to generate machine-readable, cryptographically verifiable evidence persistently from the systems being monitored. This paper describes an evidence architecture designed for the 20x model: deterministic policy execution at the endpoint, signed and verifiable at the point of collection, aligned to KSIs, and delivered as machine-readable authorization data to assessors and agencies continuously.

What 20x Changes

FedRAMP is no longer a documentation exercise. The 20x initiative replaces narrative-heavy System Security Plans and point-in-time assessments with machine-readable authorization data and persistent automated validation. The shift is structural, not incremental.



Key Security Indicators replace control-by-control narratives. KSIs are measurable, automatable security capabilities aligned to NIST 800-53. Each must have clear pass/fail criteria,

traceability, and documented validation processes — both machine-based and non-machine-based.

Validation must be persistent, not periodic. Machine-based resources must be validated at least every three days. Failures during persistent validation are treated as vulnerabilities. This is not a reporting cadence — it is a continuous engineering obligation.

Assessment changes fundamentally. Assessors no longer review compiled artifact packages. They evaluate the validation process itself — the underlying code, pipelines, configurations, and automation tools. The question shifts from "did you document this control?" to "does your validation actually produce the security outcome you claim?"

Authorization data must be machine-readable and shared. Providers must maintain authorization data in machine-readable formats through FedRAMP-compatible trust centers. By September 2026, all Rev5 providers must transition to machine-readable packages or face deprioritization.

The timeline is real. Phase 1 Low is complete. Phase 2 Moderate is active with pilot participants now. Phase 3 targets wide-scale adoption in late 2026. Rev5 submissions will eventually end. Organizations that wait to retool will be retooling under pressure.

What Persistent Validation Actually Requires

This is not continuous monitoring with a new name. Traditional ConMon meant monthly vulnerability scans, quarterly deliverables, and annual assessments. Persistent validation means your systems prove their security posture every three days through automated processes — and failures are treated as vulnerabilities the moment they occur.

The validation process is the product, not the report. FedRAMP 20x assessors evaluate the machinery of validation itself — the code, the pipelines, the automation. A passing KSI is not a document that says the control is met. It is a running process that demonstrates the control is met, continuously, with evidence.

Pass/fail criteria must be deterministic and traceable. Every KSI requires documented goals with clear pass/fail criteria and traceability to the security outcome. Ambiguity is no longer

acceptable. The system either meets the required state or it does not — and the validation must prove which.

This is an architectural requirement, not a process change. Organizations cannot meet persistent validation by accelerating their current manual workflows. Compiling artifacts every three days instead of every month does not satisfy the standard. The evidence must be generated by automated, machine-based processes that are themselves auditable and assessable.

Validation coverage must be comprehensive. Assessors evaluate whether the validation processes cover all consolidated information resources listed in the provider's documentation. Gaps in coverage are gaps in authorization. Sampling is not sufficient when the expectation is persistent, automated proof.

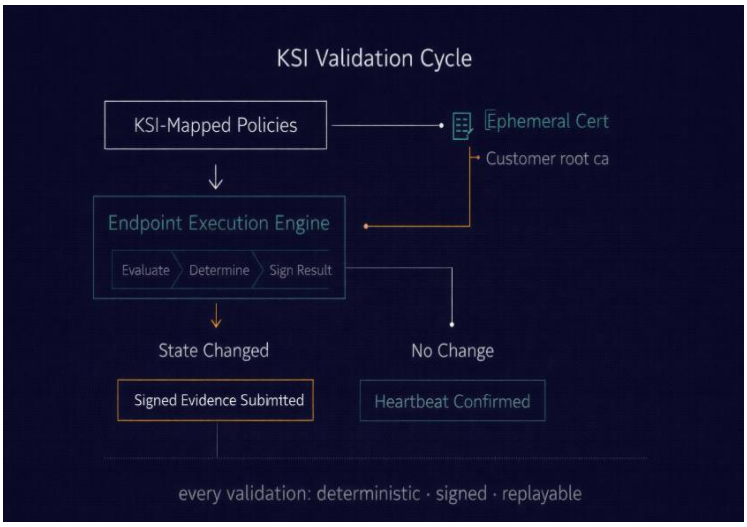
Failure to maintain persistent validation has consequences. If significant changes are not properly tracked and validated, FedRAMP may require a full Initial Assessment rather than the expected Persistent Assessment. The cost of falling behind is not a finding — it is a reset.

Deterministic Evidence for KSI Validation

The architecture was built for this model. A lightweight policy execution engine on each managed endpoint evaluates security policies deterministically — producing structured, machine-readable results with clear pass/fail outcomes mapped to specific KSIs. This is not a retrofit. It is what persistent validation looks like as engineering.

Every KSI validation is automated and repeatable. Policies are defined centrally, version-controlled, and distributed to endpoints automatically. Each evaluation executes the same logic against the same criteria every cycle. The result is reproducible — any assessor can understand exactly what was checked, what the expected state was, and what the endpoint returned.

Evidence is signed and verifiable at the point of collection. Every result is cryptographically signed with an ephemeral, identity-bound certificate before it leaves the endpoint. The signing credential chains to a customer-controlled root of trust. No unsigned, unverified data enters the evidence pipeline.



Evidence is tamper-proof and replayable. Every certificate issuance is logged in an append-only transparency ledger. Any modification is cryptographically detectable. Because evaluations are deterministic and tied to a specific policy version, any result can be re-executed to confirm the same outcome. This is the level of auditability that 20x assessors are now expected to evaluate.

Validation runs on state change, not on a timer. The engine fingerprints the evidence set after each evaluation. If state hasn't changed, a heartbeat confirms ongoing compliance. When state changes, the full result is submitted immediately. This exceeds the 72-hour persistent validation requirement — evidence reflects actual transitions, not scheduled snapshots.
No new credentials. No new attack surface. The engine authenticates through the endpoint's existing cloud IAM identity. Nothing is introduced that the organization doesn't already manage and trust.

Assessment and Authorization Data Sharing

Evidence must reach assessors as machine-readable data, not compiled documents. FedRAMP 20x requires authorization data to be shared through trust centers in machine-readable formats. The architecture delivers evidence in this form natively — structured, control-mapped, and continuously updated without manual export or reformatting.

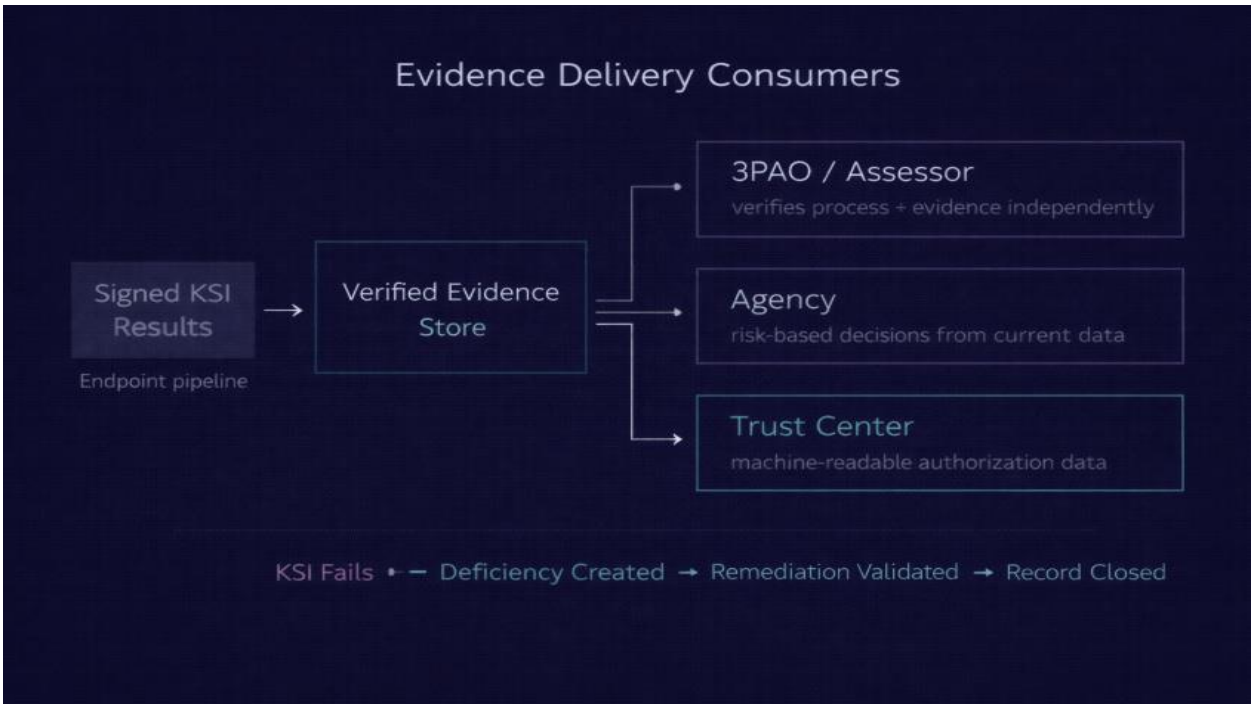
Assessment Results feed directly into the assessment process. Every KSI validation produces a structured result that maps to the underlying 800-53 control. These results are delivered as machine-readable Assessment Results that assessors consume directly. The SAR is built from living evidence, not ass
embled from static artifacts during an assessment window.

The SAP can reference the persistent validation process as its test methodology. Because every policy is mapped to a specific KSI with deterministic pass/fail criteria, the assessment plan and the evidence production are aligned by design. The assessor evaluates a running system, not a description of one.

POA&M lifecycle is automated and state-driven. When a KSI validation fails, a structured deficiency record is generated and delivered to the system of record automatically. When the endpoint demonstrates remediation through a subsequent passing evaluation, the record is closed with validated evidence. Every step is traceable and signed — from deviation through closure.

Assessors verify independently without trusting the platform. Every evidence artifact includes the cryptographic signature, certificate chain, and transparency proof. A 3PAO evaluating persistent validation can verify that evidence was produced by a legitimate workload, at the claimed time, and has not been modified. The proof is self-contained. No call back to the platform required.

Authorization data is always current. Historical versions are maintained and available. Assessors and agencies access the same evidence through the same trust center. There is one body of evidence, continuously updated, serving initial assessment, persistent assessment, and collaborative continuous monitoring simultaneously.



Executive Takeaway

FedRAMP 20x is not a future state. It is happening now. Phase 1 Low is complete. Phase 2 Moderate is active. Machine-readable authorization packages are required for all Rev5 providers by September 2026. The transition timeline is measured in months.

Persistent validation is an architectural requirement. Organizations cannot meet the 72-hour validation standard by accelerating manual processes. The evidence must be generated by automated, auditable, machine-based processes — because that is what assessors are now evaluating.

Deterministic, signed evidence is the new baseline. KSIs require clear pass/fail criteria with traceability. Evidence that is unsigned, unstructured, or manually assembled does not meet the standard 20x describes. Cryptographically verifiable evidence produced at the point of enforcement does.

The assessment model has changed. Assessors evaluate the validation process, not a document package. The architecture described in this paper produces evidence that is designed for this model — replayable, independently verifiable, and delivered as machine-readable data to assessors and agencies continuously.

Document-based compliance has an end-of-life date. FedRAMP will stop accepting new Rev5 agency authorizations and provide transition timelines for all legacy providers. Organizations that invest in persistent validation architecture now are building for the only authorization model that will exist in two years.

The destination is clear. The question is readiness. FedRAMP 20x describes what authorization should look like. The architecture described in this paper is engineering that meets that description — deterministic, verifiable, continuous, and machine-readable from endpoint to assessor.

To learn more about implementing persistent validation and machine-readable evidence production for FedRAMP 20x, contact the engineering team at **contact@scanset.io**