Spectro Cloud
GOVERNMENT



ATO acceleration for federal agencies: a more repeatable path to secure deployment

Building security and compliance into how infrastructure is deployed.

Business challenges

Authorization to Operate (ATO) is a vital part of keeping federal information systems secure. But when systems are built and authorized separately, getting there becomes onerous for you and your assessors. The key to a faster, more predictable process, and a more secure agency overall, is a predictable, consistent approach to how infrastructure is designed in the first place.

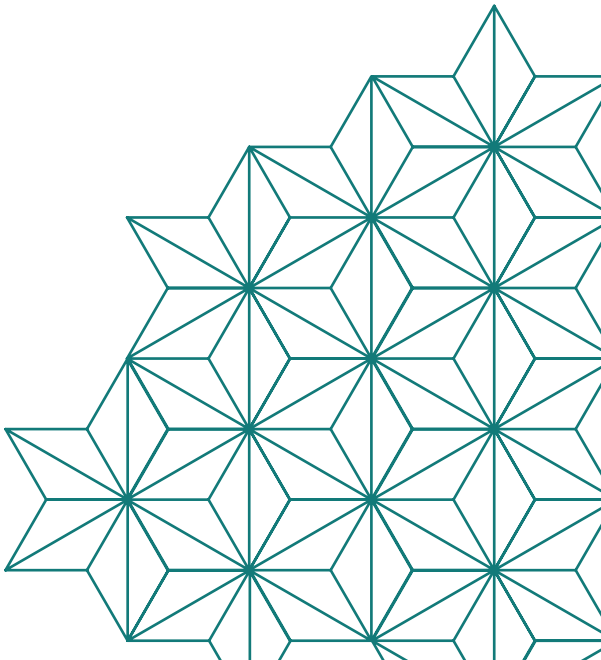
You're under constant pressure to modernize your applications and infrastructure. But new workloads and new environments often mean new ATO work: new configurations for your team to document, new controls to validate, and new evidence to assemble, before anything can go live.

For many agencies, infrastructure has grown siloed – built project by project, by different teams, at different points in time. Because each system, cloud environment, and edge deployment was built independently, authorization packages are difficult to reuse, and evidence has to be reassembled by hand for each one. Configuration drift can then slowly erode a system's security posture after authorization, sometimes without anyone noticing until the next assessment.

A shared, repeatable pattern for building compliant infrastructure won't retroactively fix every system you already have in production, but it changes what happens with every system that comes after. When infrastructure is standardized from the start, teams can reuse approved configuration patterns, documented implementation details, and supporting evidence rather than recreating them from scratch. System-specific controls, risks, and authorization decisions still require assessment, but there's less net-new infrastructure for your team to document and less unfamiliar material for your assessor to review.

Key benefits

- **Less to rebuild each time:** Configurations and evidence you've already produced can be reused as supporting material for future authorizations.
- **More consistent security posture:** Infrastructure that's deployed and maintained the same way stays closer to its originally authorized state over time.
- **Audit evidence, at the ready:** Logs, scans, and configuration history are available without a scramble.
- **Faster updates, less rework:** Security patches and configuration changes roll out the same way across every environment, instead of system by system.



© 2026 Spectro Cloud. All rights reserved.

Solution overview: what Palette VerteX actually does

Palette VerteX is Spectro Cloud's Kubernetes management platform, purpose-built for regulated and public sector environments. It models every software component that goes into an IT environment – from the operating systems up through the application layer – as a single, versioned blueprint. Once a stack is approved as part of an ATO, Palette VerteX treats that declared configuration as the desired state and continuously monitors deployed clusters for divergence.

Consistent security posture: Controls are enforced consistently as infrastructure is deployed, backed by FIPS 140-3 validated cryptography and STIG-compliant OS options.

Drift management: Declarative configuration and immutable infrastructure keep systems matched to their approved blueprint over time, so what's deployed doesn't quietly diverge from what was authorized.

Evidence for assessment: Palette VerteX maintains configuration history, audit logs, and security scan reports as infrastructure is deployed and updated. Your security team can use these directly for continuous monitoring and provide them to assessors as evidence during reauthorization. (Some evidence required by specific frameworks may still depend on integrating with your agency's existing logging or GRC tooling.)

Deployment flexibility: Palette VerteX can be deployed self-hosted, air-gapped, or in AWS GovCloud environments – fitting into the infrastructure you already run, rather than requiring a wholesale replacement.

Consistent updates: Security patches and configuration updates roll out through the same controlled process across every environment, instead of being handled system by system. Because the resulting infrastructure state is fully documented, your team has current evidence on hand to assess whether a given change affects your system's security or privacy impact – which is what actually determines whether reauthorization is required.

What this can look like in practice

Illustrative scenarios, not documented case studies.

Extending an existing system

Consider an agency running a public-facing benefits or case-management system that wants to add a new cloud-based analytics or AI capability. Because the new capability can be built on the same infrastructure blueprint, security controls, and audit history already validated for the existing environment, much of that material may be reusable as supporting evidence. The agency and its authorizing official still have to determine whether the new capability changes the system's authorization boundary, data processing, or privacy risk. A workload-specific assessment is still required, but the amount of net-new infrastructure documentation the assessor needs to review can be reduced.

Unifying multi-bureau operations

Consider a science or research agency operating on-premises systems and cloud environments across multiple program offices. A consistent deployment pattern means each office can stand up compliant infrastructure independently, without reinventing its own approach to hardening, logging, and access control — while giving the agency's security team the oversight they need across every office.

A more repeatable path to your next ATO

Authorization doesn't have to mean rebuilding the same infrastructure and compliance work for every new system, edge cluster, or cloud environment. When security, governance, and compliance are built into how your infrastructure is deployed from the start, your team has less to build and your assessors have less unfamiliar material to review — for every ATO that follows the first one.

Talk to our team about Palette VerteX for your agency

Spectro Cloud

© 2026 Spectro Cloud. All rights reserved. Spectro Cloud, Palette, and the respective logos are trademarks or registered trademarks of Spectro Cloud in the US and other countries. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Spectro Cloud and any other company. File: ATO acceleration_20261014