STAX

Control Tower vs Stax: A Comparison

Clarifying the difference between AWS Control Tower and Stax

Stax is the only truly AWS-native cloud management platform, built exclusively for AWS, that empowers customers to focus on building in the cloud, not building the cloud, so they can accelerate their business outcomes.

Stax offers solutions for establishing a Well-Architected AWS environment including guardrails, creating and managing AWS accounts and networks, infrastructure-as-code deployments, identity and access management, and monitoring cost, usage and compliance.

This is done by taking advantage of as many AWS native services as possible, and Stax provides updates as AWS releases new features and services, automatically updating customers' environments, keeping them 'evergreen'.

Stax was born out of the lessons and experience gained from nearly a decade spent delivering enterprise-grade cloud solutions to hundreds of AWS customers. It was here our founders realised they could help accelerate the delivery of cloud migrations and automate maintenance by providing a secure and compliant, feature-rich platform to help businesses operate in the AWS cloud.

In discussions with partners and customers, one common comparison raised is between Stax and AWS Control Tower. While on the surface the two may seem similar, and there is some overlap in account-related features, in reality the services are fundamentally different in their philosophy, design, and operation, and they offer different solutions for different use-cases.

Stax is not built on top of AWS Control Tower, for a variety of reasons, automation and scalability being the primary ones. This document aims to help resolve any confusion as to what Stax offers and how it compares to AWS Control Tower.

Control Tower vs. Stax: A Comparison

Factor	aws	STAX
Philosophy in one sentence	Quickly set up and configure a new AWS environment.	Buy the outcome, save time and effort, and focus on high-value activities further up the stack.
Time required to deploy foundations	To build Control Tower and have all the controls, automations, security, and guardrails in place would take weeks	Customers have access to their configured and hardened environment within five days.
Time required to configure your environment e.g. create accounts	Depending on the team size and level of experience, weeks to months at a minimum.	Days to weeks, depending on the level of configuration required by the customer.
Upfront cost	Control Tower setup by a consulting partner can cost anywhere from $15k-$150k depending on requirements. Ongoing costs depend on partner involvement. There is no extra cost for the Control Tower service itself.	Zero upfront cost for Stax foundations. Additional setup depends on requirements. Reduced partner and staff-related costs due to included security updates as part of ongoing subscription for as low as $5000 per month.
Developers/engineers required	AWS experts and infrastructure engineers. Requires an embedded squad on an ongoing basis.	Application developers (minimal AWS expertise required). Rather than an ongoing squad, this can be developers with primary responsibilities elsewhere, which can complete AWS tasks when and as needed.
Responsibility model	Recommendations and ready-made configuration, that help customers get onboard AWS following best practices. Offers no opinionated view, how customers use the platform is their responsibility.	Can take actions on customers' behalf. Offers an opinionated, battle-hardened view on the correct and safe way to use the platform, which has been tested in industry, and is continually evolving.
Aligns to CIS?	Not by default	Yes
Maintenance and updates	No automatic updates. Any features or new releases from AWS need to be developed, tested, and deployed by the customer or their partner.	Automatic updates for foundation and security features and releases from AWS, as well as new Rules and checks.

Factor	aws	STAX
Solutions offered	Manual, console-driven administration only. • AWS onboarding • Setup of landing zone with pre-configured blueprints • Guardrails • Account factory • Visibility for organizational units, accounts, and guardrails • Multi-factor authentication (MFA) and granular role-based access control (RBAC) requires the use of a separate module in AWS, which must be enabled and configured in a mostly manual process	Choose between manual console, automated APIs, and SDK interfaces for developer enablement. • Automated setup of landing zone with pre-configured foundations • Guardrails • Automated ongoing maintenance • Account creation and management • Network creation and management • Infrastructure-as-code deployment framework • Automated, centralized identity and access management, including MFA and granular RBAC • Full cost visibility, management, and optimization with real-time alerts • Pre-configured, proactive, and detective security, risk and compliance management with real-time alerts
Risk management capabilities	Enables the configuration of guardrails and detective controls, using AWS-Native services.	Pre-configured rules and guardrails ready for use via the console or API, and industry compliance frameworks are supported immediately, with no extra work required.
Cost management capabilities	None – multiple separate AWS services, must be enabled, configured, and integrated.	Pre-configured visibility, segmentation, cost allocation, and optimization features.
Networking capabilities	Single, static, isolated VPC per account, which cannot be integrated with other networks without additional work and AWS networking skills.	Cross-account, highly available, hub-and-spoke networks following AWS best practices and using AWS native services can be deployed in minutes via the console or API.

Visit **stax.io** and book a no obligation demonstration today.

STAX