SWIMLANE

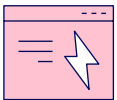# Cloud–Native Architecture

The technology behind Swimlane Turbine's
unrivaled power, scalability and performance
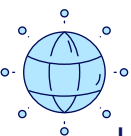
→ **Turbine's Cloud-Native Benefits**

99.9% availability and zero downtime (ZDT) updates

ROI Maximization

Unparalleled scalability & flexibility

Swimlane Turbine is a cloud–native low-code security automation platform that combines human and machine intelligence to serve as the system of record for security. Turbine transcends traditional security orchestration automation and response (SOAR) platforms by leveraging its Active Sensing Fabric to gather and action on hard–to–reach telemetry at cloud–scale. Autonomous Integrations leverage a secure API gateway to instantly connect with any API and trigger native playbook actions in order to automate any security or business process.

The platform's cloud–native architecture is built on AWS infrastructure. It provides customers with a solution that is faster to deploy and easier to manage than legacy on–prem SOAR tools. Turbine's cloud–native architecture is complete with multi–tenant, multi–brand and multi–region support. It allows for greater resilience and scalability while also reducing costs. Customers who chose to deploy Turbine in the cloud experience a more flexible and automated environment. They can easily adapt to changing demands and avoid the manual effort required in traditional architectures.

Turbine's Cloud–Native Computing Capabilities

Multi–tenancy delivers optimized account structure and level capabilities in order to gain greater control, and a superior user experience. Turbine's multi–tenant support offers the flexibility to configure distinct tenants for your development and production environments.

Multi–region support ensures that Turbine cloud can be deployed globally in order to provide redundancy for maximum availability and to adhering to regional data sovereignty requirements, like GDPR. Turbine cloud is hosted in North America, Europe, and Asia regions.

Multi–brand support helps MSSP's and large distributed organizations segment and manage multiple brands or disconnected organizations within a single Turbine deployment for greater control and flexibility.
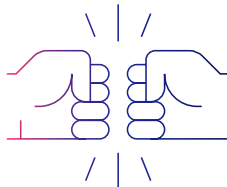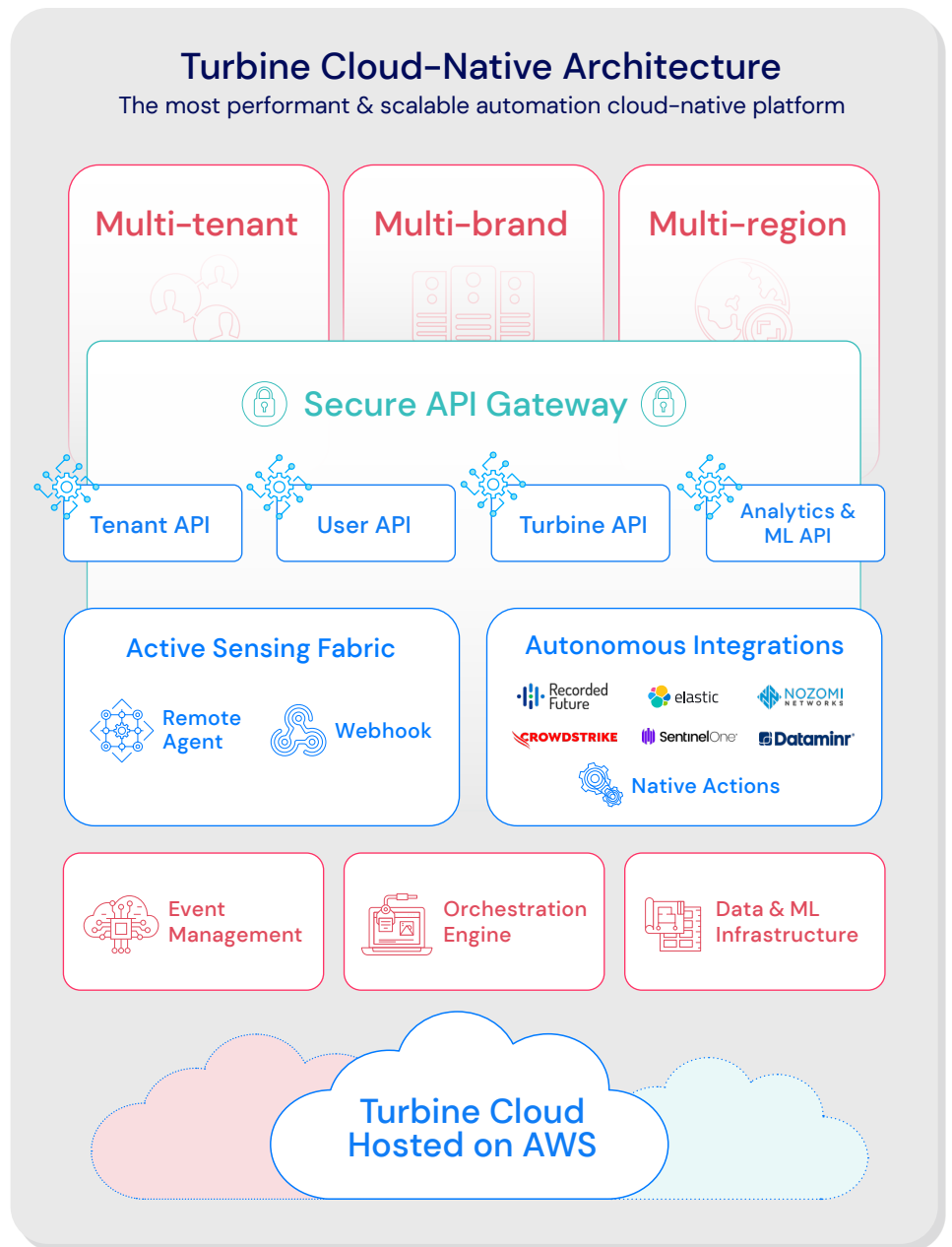
Remote agents allow customers to run any language function inside of the agent to achieve a serverless–like experience for security use cases. This feature provides a brand–new developer experience that can be run in the cloud or as an edge computing service.

Webhooks enable products, vendors or services to push real–time communication into Turbine. They are easily managed with flexible authentication options to cover a wide variety of capabilities found in third–party tools.

Connectors are vendor–specific integrations that provide a stable, portable and reliable connection to any API in a customer environment.

Native actions are automation actions that are purpose–built into Turbine's architecture in order to simplify the user experience of building automation while also optimizing performance capabilities.

The Turbine **API gateway** is the feature that enables customers to administer and integrate Turbine with any system in their environment. It ensures connectivity and delivers seamless, performant, and scalable automation outcomes.

Turbine Cloud–Native Architecture
The most performant & scalable automation cloud–native platform

Multi–tenant

Multi–brand

Multi–region

🔒 **Secure API Gateway** 🔒

Tenant API

User API

Turbine API

Analytics & ML API

Active Sensing Fabric

Remote Agent

Webhook

Autonomous Integrations

Recorded Future

elastic

NOZOMI NETWORKS

CROWDSTRIKE

SentinelOne

Dataminr

Native Actions

Event Management

Orchestration Engine

Data & ML Infrastructure

Turbine Cloud Hosted on AWS

Get Started
We're ready to help you transform your security operations with Turbine's cloud–native security automation solution. Contact a Swimlane sales representative to learn more.

Swimlane is the largest and fastest-growing pure-play security automation company. Swimlane Turbine is the world's most-capable low-code security automation and SOAR platform that unifies security operations in and beyond the SOC. The platform significantly reduces process and data fatigue, while helping security leaders overcome chronic staffing shortages and more easily quantify business value and the efficacy of security operations. Customers benefit by uniting disparate alerts, tools, processes and teams for a faster and more effective security and incident response.