BEYOND IDENTITY

Delivering 99.99% Uptime

Reliability, Availability and Scalability are core architectural tenets

Authentication is the first user experience for all applications and services. Beyond Identity's cloud architecture, built from the beginning with the core tenets of Reliability, Availability, and Scalability (RAS), has a 99.99% uptime Service Level Objective (SLO). Beyond Identity's Zero Trust Authentication service is a 100% cloud-native, multi-tenant, SaaS service built on Amazon Web Services (AWS), which is known for its resiliency and reliability.

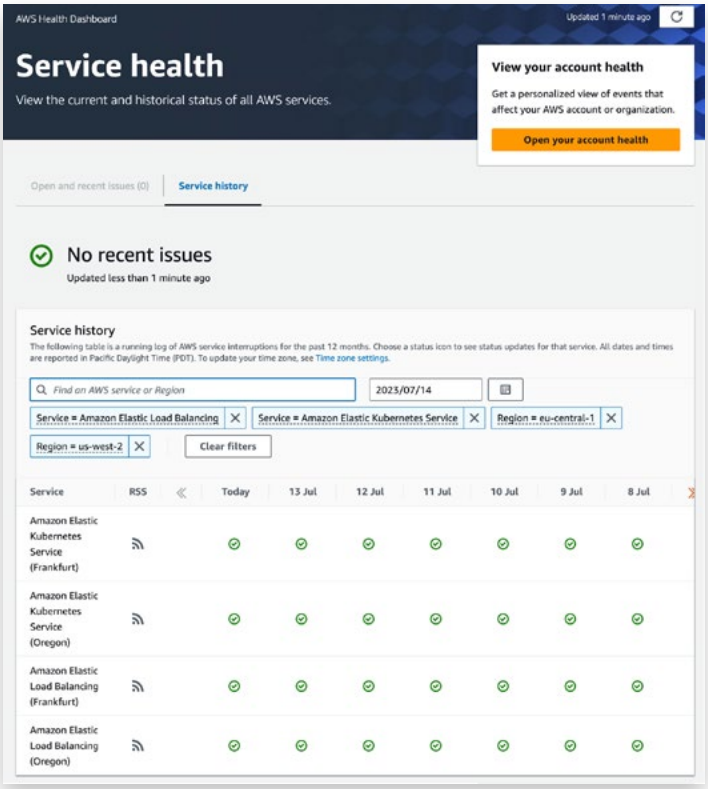

Figure 1: AWS Service health

Beyond Identity is based on Amazon's architecture best practices and is AWS Foundational Technical Review certified, The platform is built on a globally distributed, multi-tiered, and auto-scaling architecture that provides worldwide reach, delivers scale—both vertically and horizontally, and minimizes network latencies.

Key functional areas are independent of each other and separated to their plane of operation.

Administration, Authentication and Logging/Analytics services are deployed in each geographic region with deployments in both primary AWS Regions of us-east-2 and eu-central-1 with secondary services in us-west-2 and eu-west-1. Isolated Amazon Availability Zones within each Amazon Region provide in-region redundancy.

Critical system components are backed up across multiple zones. Availability Zones automatically fail-over between zones without any interruption. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable, according to Amazon standards.

The use of dispersed geographies serves redundancy, availability and data privacy goals.

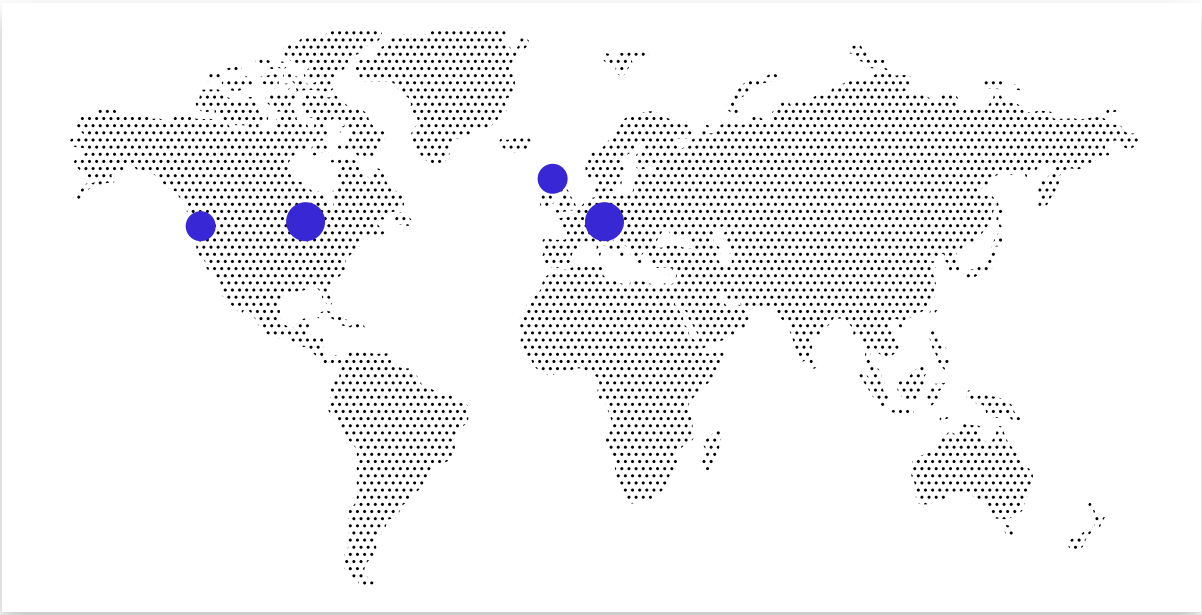

Figure 2: Beyond Identity AWS Regions

Processing power is automatically scaled, added or removed, from each key service without code changes. This allows rapid scaling to meet varying user demand.

The architecture takes advantage of network routing to ensure enough compute power is available for all processes. Each request is routed to the node that will ensure the lowest latency. Scale is not solely about handling load, it includes request routing in the most latency-efficient manner.

Several services are used to meet these requirements. Table 1 lists the specific services and how it is used.

Service	RAS Goals
Amazon Route 53 w/ Anycast	Minimize network latency of user requests
Amazon Aurora Global Database	In region customer data residency
Amazon Elastic Load Balancers	Application availability and fault tolerance
Amazon Elastic Kubernetes Service	Kubernetes control plane availability and fault tolerance
Cloudflare	Accelerate API requests, DDOS protection and Content Caching

Table 1: Services and associated RAS Goals

Operational monitoring plays a key role in uptime delivery. The Beyond Identity platform is monitored 24x7 for reliability and performance.

The Site Reliability and Engineering (SRE) team monitors the service and has subject matter experts (SMEs) in multiple disciplines.

- Automated monitoring tools route warnings and alerts to the SRE team.
- Events and alerts are routed directly to on-call personnel and engineering teams.
- System monitoring is provided by native AWS tools and best-of-breed third party tools.

Extensive in-application monitoring and instrumentation provides self reporting health and performance metrics. Service availability is continuously published to the Status page.

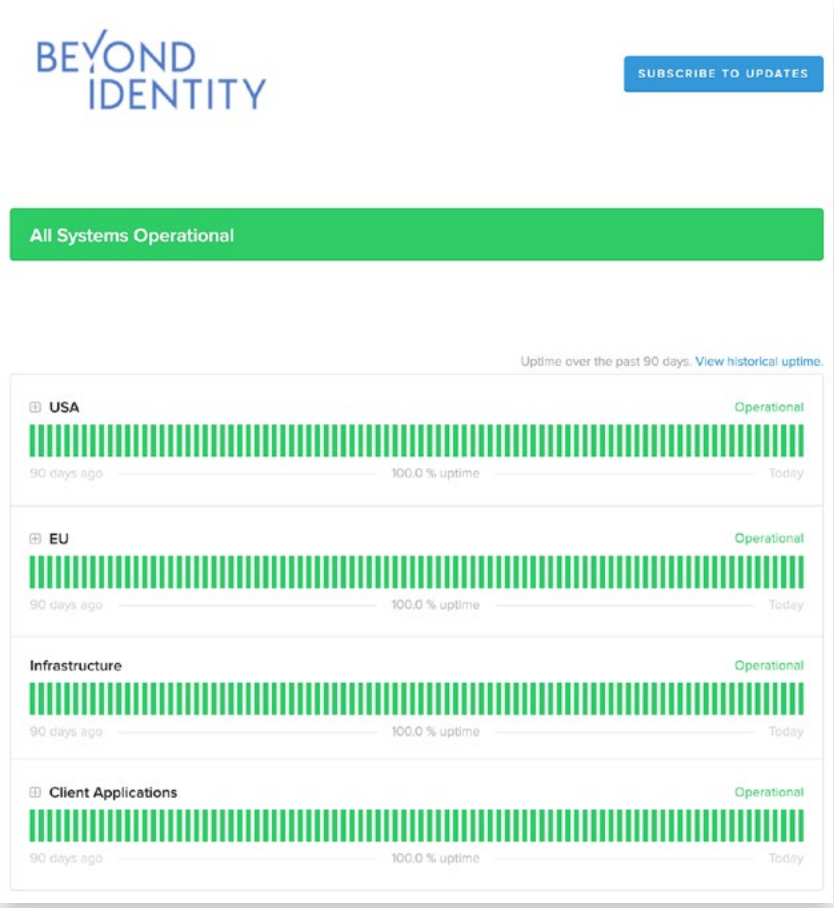

Figure 3: Beyond Identity Service health

Beyond Identity's architecture, built from the beginning with RAS as core tenets, has consistently delivered 99.99% availability.

BEYOND IDENTITY

Beyond Identity is revolutionizing digital access for organizations looking to improve protection against cyber attacks and deliver the highest levels of security for their workforces, customers and developers. Its suite of passwordless, phishing-resistant, and zero trust authentication solutions improves security and user experience. The platform delivers continuous risk-based authentication incorporating signals from the zero trust ecosystem to ensure only valid users and secure devices gain or maintain access to critical resources. Companies like Snowflake, Unqork, and Roblox rely on Beyond Identity's highly available cloud-native platform to thwart attacks and advance their zero trust strategies. To learn more about Beyond Identity's FIDO-2 certified multi-factor authentication (MFA) solutions, visit beyondidentity.com and stay connected with us on Twitter, LinkedIn, and YouTube.