BLUEWHALE STACK

SOLUTION BRIEF

Security & Compliance — solution brief

Federated identity, role-based access and a full audit trail across every connected cloud — with data residency and air-gapped options for the most regulated estates.

One identity fabric. One audit trail.

September 2026 · Version 1.0 · www.bluewhalestack.com

Federated identity, role-based access and a full audit trail across every connected cloud — with data residency and air-gapped options for the most regulated estates.

Security & Compliance puts one identity fabric, one role model and one audit trail over every connected estate, and keeps control evidence current instead of assembling it before each inspection. CISOs and compliance teams federate the IdP they already run, enforce least-privilege roles across clouds, pin data to an in-country region, and produce the report an auditor asks for from a system of record.

10	5 ISO	72 h
Identity providers federated — Entra, Okta, Auth0, AWS Identity Center, AD and more	27001 · 27017 · 27018 · 27701 · 22301, independently audited	Breach notification commitment; sub-processor changes on 30-day notice

The challenge

Access and audit are fragmented across clouds and tools, and regulators increasingly demand provable residency and a single, trustworthy record of who did what.

How it shows up

- Each cloud has its own IAM, so joiner and leaver hygiene depends on people remembering.
- Audit evidence is screenshots gathered in the two weeks before the inspection.
- Residency is asserted in a policy document and cannot be shown per resource.

How it works

1 **Step 1**

Federate your IdP over SAML 2.0 or OIDC; SCIM maps directory groups to platform roles.

2 **Step 2**

Role-based access is enforced consistently across every connected cloud and on-prem estate.

3 **Step 3**

Every action is written to an append-only audit trail.

4 **Step 4**

Residency pins workloads and records to an in-country region — Mumbai for DPDP, Frankfurt for GDPR.

5 **Step 5**

Cloud Audit & Evidence monitors controls continuously and produces the report per regime on demand.

What is included

- 10 identity providers over SAML 2.0 / OIDC, with SCIM auto-provisioning
- Role-based access across all clouds
- Full audit trail of platform activity; WORM-backed in the Government Edition
- Data residency by region, and air-gapped deployment for the strictest estates

Modules involved

Identity & Access One identity fabric — federate your IdP and auto-provision access everywhere.	**Cloud Audit & Evidence** 11 compliance frameworks, scored from live scans.
Whale ITSM The ITSM that ships with your cloud — incidents, changes, releases, requests and problems, pre-wired to your scanner, Terraform and CMDB.	

Editions and audience

Recommended editions: Enterprise and Government.

Who it is for: CISOs, Heads of Cloud Security and compliance officers in regulated industries.

Delivered engagement — Two leading banks, Singapore & Qatar

Two banks running public cloud, private infrastructure and on-premises systems under MAS and Qatar central-bank supervision moved from weeks of manual evidence assembly per inspection to reports generated from one policy layer — and rehearsed the exit plans they had only ever documented.

> *"The last supervisory request took three days. Before, it took three weeks of five people pulling screenshots. And the exit plan has now been run as a drill, with the evidence filed."*
>
> Chief Compliance Officer, Two leading banks, Singapore & Qatar — as reported by the customer

Questions teams ask in the evaluation

01 Which certifications does the platform itself hold?

ISO/IEC 27001:2022, 27017, 27018, 27701 and ISO 22301, independently audited; plus a CSA STAR Level 1 self-assessment, a GDPR compliance assessment and a SOC 2 Type II readiness assessment. Signed certificates are in the Trust Center.

02 Is MFA enforced?

MFA follows your IdP policy for SSO. In the Government Edition MFA is mandatory on every role and privileged access always runs through PAM with session recording.

03 How does residency work on SaaS?

You choose Singapore, Mumbai, Dubai, Frankfurt or Los Angeles and data stays there. For regimes without a SaaS region, BYOC, on-prem or air-gapped deployment keeps everything in-country.

© 2026 BlueWhale Stack. Product, edition and maturity statements are as of September 2026; certifications are described exactly as their issuing bodies allow. Customer engagements are anonymized under confidentiality. Contact: sales@bluewhalestack.com.