SECURITY & COMPLIANCE

The Compliance-First SRE Agent

AI-powered IT operations with full data sovereignty and zero external exposure.

THE CHALLENGE

The Compliance Trade-Off Holding You Back

Most AI-driven SaaS tools require outbound data transfer, external credentials, and ongoing vendor connectivity — all unacceptable in regulated industries.

01

Loss of Data Sovereignty

Sensitive logs and metrics leave your perimeter and enter vendor infrastructure.

02

Increased Attack Surface

Every external endpoint added by a SaaS tool expands the breach window.

03

Third-Party Vendor Access

Credentials shared externally erode the control and auditability you need.

WHY TRADITIONAL SAAS FAILS

SaaS Tools Create Compliance Gaps

- **Outbound network access required**

  Every SaaS tool needs a route out. Your firewall rules must open, increasing exposure.

- **Logs & credentials transferred externally**

  Observability data and API keys leave your environment and enter vendor infrastructure.

- **Vendor access to production systems**

  Most tools require ongoing connectivity, a third party permanently inside your perimeter.

Compliance Risks

→ GDPR violations from data transfer

→ ISO 27001 / SOC 2 audit failure

→ BaFin / HIPAA non-compliance

→ Loss of data residency control

Compliance by Architecture

Hyground is built from the ground up to operate inside your infrastructure, never outside it.
No external SaaS dependency. No data leaves your perimeter. No vendor access required.

We Are NOT SaaS

Logs, traces, and metrics stay inside. Nothing leaves your environment. Ever.

No Vendor Connectivity

No firewall opening.
No credentials.
You remain in control of your data.

Fully Inside Your Perimeter

Runs in your own Kubernetes cluster.
No In- or Outbound

SIX PILLARS

Secure Automation from the Ground Up

01

Fully Self-Hosted

Runs in your cluster. No SaaS dependency.

02

Zero External Access

No outbound connections or firewall openings.

03

Credential Control

Secrets stay in your vault — never duplicated.

04

Flexible Integration

Connects to your existing tools as-is.

05

Bring Your Own Models

Deploy private LLMs on your own hardware.

06

Standard Tooling

Helm-deployed, IaC-compatible, fully auditable.

SECRETS & CREDENTIALS

Full Control Over Your Data and Credentials

No Outbound

No external endpoints or third-party data pipelines

100%

Credential ownership stays with your team

Never

Vendor or third-party requires system access

BRING YOUR OWN MODELS

Complete Control Over Your AI Infrastructure

Hyground gives you full sovereignty over which AI models power your operations — from permitted cloud APIs to fully air-gapped on-prem deployments.

- **External Cloud APIs**

  Use permitted LLMs (OpenAI, Anthropic, etc.) where policy allows.

- **Private Deployed LLMs**

  Run Llama, Mistral or similar open-source models in your own infra.

- **Air-Gapped Hardware**

  Fully isolated on-prem GPU deployment — zero external data flow.

AI Governance by Design

✓ No cloud provider lock-in

✓ No model training on your data

✓ Total data residency control

COMPARISON

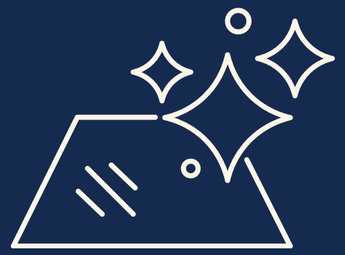
Hyground vs. Traditional SaaS

Requirement	Traditional SaaS	Hyground
Data residency	External / vendor-controlled	**Fully internal**
Credential handling	Shared or stored externally	**Customer-controlled**
Network exposure	Outbound access required	**None required**
Vendor system access	Required for operation	**Not required**
AI model governance	Limited / cloud-only	**Full control (BYOM)**

SECURITY BEYOND COMPLIANCE

A Stronger Security Posture, Built In

Hyground does not just meet compliance requirements — it actively improves your overall security posture.



Reduced Attack Surface

No external endpoints.
No third-party data pipelines.
Fewer vectors, fewer threats.

Strong Isolation

Runs fully inside your network.
Aligned with zero-trust. Nothing crosses your boundary.

Audit-Ready Architecture

Clear system edges, full action traceability and zero hidden data flows - always.

USE CASE

Real-World: Deutsche Bahn RIS

Europe’s largest railway operator needed AI-powered incident response without compromising data sovereignty and German critical infrastructure regulations.

The Setup

- Deployed in internal Kubernetes cluster
- Git, monitoring & DBs connected internally
- Secrets stay in existing vault system
- Private LLMs on on-prem GPU hardware

Result

✓ AI-powered ops - zero external data exposure

✓ Critical infrastructure maintained

✓ No SaaS dependency or vendor access

✓ Root cause analysis in under 17 minutes

Ready to Eliminate the Trade-Off?

Book a technical deep dive and see Hyground running securely inside your own environment.

Book a Demo

Hyground

hyground.ai
Dominik@hyground.ai