

Seven tools to run your infrastructure? One console is enough.

One console for your whole infrastructure.

What it is

Proxima Console brings inventory, live topology, monitoring, on-call paging, privileged access management (PAM), AI root cause, compliance and audit into one platform — for companies that run their own infrastructure, and for the teams that run it for them.

What it replaces

Inventory

Instead of: CMDB spreadsheets

Uptime monitoring

Instead of: A separate uptime checker

On-call paging

Instead of: A separate paging service

Runbooks

Instead of: Scripts on someone's laptop

SIEM integration

Instead of: Hand-exported logs for the SOC

Audit trail

Instead of: Access logs scattered across systems

Live topology

Instead of: Hand-drawn network diagrams

Metrics & logs

Instead of: Separate metrics and log stacks

Incidents & AI root cause

Instead of: War-room guesswork

Privileged access (PAM)

Instead of: A separate PAM tool, VPNs and shared SSH keys

Compliance scoring

Instead of: Audit-season spreadsheets

Service desk + Jira

Instead of: Switching to the Jira portal for every ticket

Security and control

Hard tenant isolation

Metrics are physically separated per client — not filtered by a query the application has to remember to add.

MFA and passkeys

WebAuthn passkeys, TOTP, and Google Workspace SSO with domain restriction. Fail-closed by design.

Broker-enforced agent identity

Every agent holds its own scoped credential. An agent cannot publish as another host even if it tries.

Audit chain verified hourly

Audit entries are SHA-256 hash-chained; an independent job checks the whole chain every hour.

Environment-scoped roles

Grant a role against a single environment of a single client. Enforced across users, teams and service accounts, and fully audited.

Vault-backed secrets

Agent credentials, TLS certificates and stored secrets are issued and encrypted through HashiCorp Vault. Nothing durable sits in application config.

Changes only after approval

Remediations and destructive runbooks run only after a person with the right role approves them, and the approval is recorded.

Recorded and replayable

Access grants, terminal sessions, runbook executions and administrative changes are recorded, replayable and queryable.

How a pilot works

01

Connect one environment

Install the agent on the hosts of a single environment you pick.

02

See it mapped and monitored

Inventory, topology, uptime checks and compliance scores fill in as the agents report.

03

Review findings together

We walk through what Console found with your team and agree on next steps.

Talk to us

Book a call at console.proximaops.io or write to sales@proximaops.io.