PulseWatch

PulseWatch for Enterprise

Proactive reliability, local/offline AI insights, security-first operations, and global visibility in one platform.

A modern monitoring platform built for teams that cannot afford silent failures.
Unified uptime checks across HTTP, TCP, Ping, DNS, CRON, and keyword validation
Built-in AI: incident summaries, latency anomaly detection, root-cause hints, and predictive risk scoring
Enterprise-grade controls: tenant isolation, MFA, audit trails, and compliance workflows
Flexible deployment: cloud-first with optional private/global node locations

Why Enterprises Replace Legacy Monitoring

Common Pain

- Tool sprawl splits telemetry, incidents, and audit evidence across disconnected systems
- Slow detection and noisy alerts create avoidable downtime and escalation fatigue
- Security/compliance teams lack product-native controls and prove-it artifacts
- Global teams need location-aware checks without standing up multiple platforms

PulseWatch Outcome

- Single operational plane for uptime, incidents, status comms, and governance
- Faster detection with structured status transitions and actionable notifications
- In-product DSAR, breach logging, and hash-chained audit records
- Cloud or hybrid rollout with remote node locations aligned to your network model

Platform Overview

Monitor Coverage

- HTTP & APIs
- TCP & Port
- Ping
- DNS
- Keywords
- CRON heartbeat

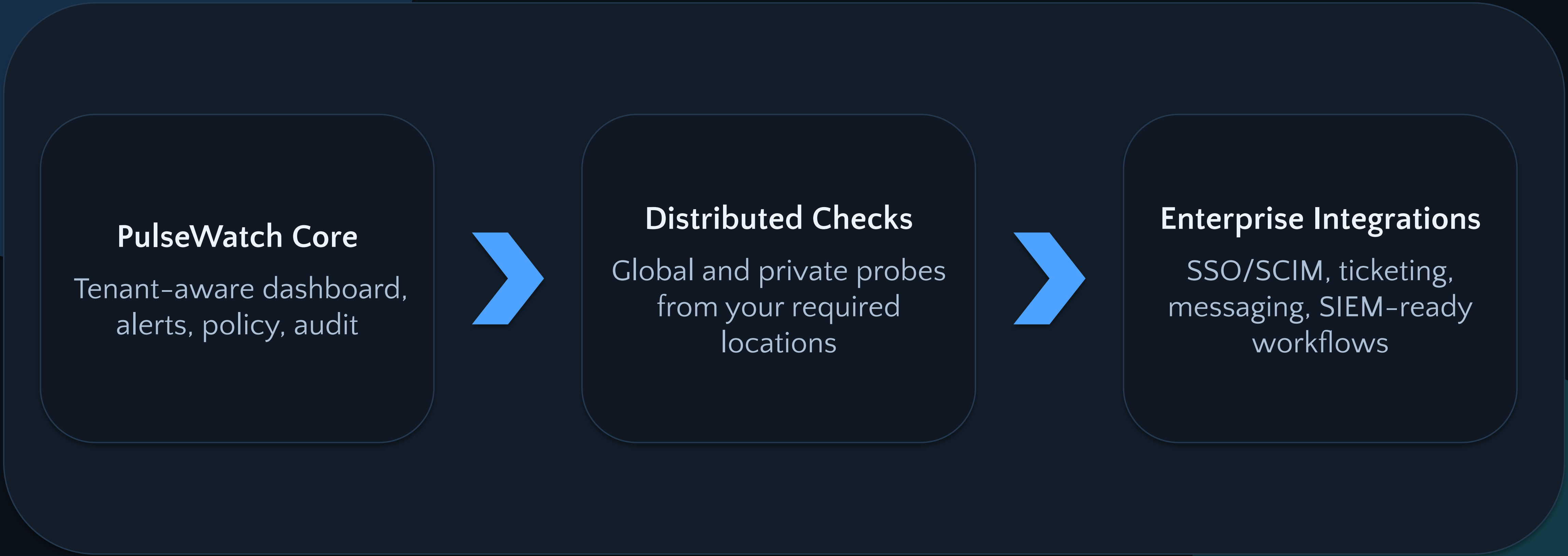
Operational Features

- Hierarchy + grouped monitors
- Maintenance windows
- AI status + incident summaries (local/offline)
- Predictive risk scoring + root-cause hints
- Plan-based governance controls

Integrations

- Email
- Slack
- Teams
- Discord
- Webhooks
- 50+ other provides

Enterprise Architecture



PulseWatch Core

Tenant-aware dashboard, alerts, policy, audit

Distributed Checks

Global and private probes from your required locations

Enterprise Integrations

SSO/SCIM, ticketing, messaging, SIEM-ready workflows

Security and Compliance by Design

Security Controls

- MFA support and privileged-role hardening
- Strict target validation and secure header policies
- Tenant isolation and role-aware access boundaries
- Hash-chained audit logs for tamper-evident traceability

Compliance Operations

- DSAR runbook workflows embedded in product operations
- Breach and incident evidence tracking
- Control matrix and evidence-pack ready documentation
- DevSecOps-friendly testing and scanning workflows

What Enterprise Buyers Get

Deployment Options

Cloud or self-hosted

Identity

SSO (SAML/OIDC) + SCIM

Scale

Unlimited monitors and locations

Support

SLA + onboarding + invoicing/PO

PulseWatch

30-Day Rollout Blueprint

First 10 days

Discovery + Design

We will define critical services and SLO targets and map identity, tenancy, and escalation flows

10-20 days

Pilot + Hardening

Now we launch priority monitors and status communication, validate our alert routes and audit controls

20-30 days

Scale + Govern

Expand to global/private nodes and teams and operationalize compliance and executive reporting

Commercial Model

Enterprise Packaging

- Custom commercial terms based on monitor volume and deployment model
- Support for invoice-based purchasing and procurement workflows
- Optional professional onboarding and architecture advisory
- Standardized success criteria for security, reliability, and adoption

Value Narrative

- Reduce MTTR with AI incident summaries and root-cause hints
- Surface degradation earlier with anomaly detection and predictive risk scoring
- Keep data control with local/offline AI (no external LLM dependency)
- Lower audit prep effort with built-in evidence and traceability
- Scale globally without adding disconnected monitoring stacks

Why PulseWatch AI Wins Enterprise Buy-In

What Enterprise Buyers Ask

1. Is AI safe for regulated environments?
2. Will model output stay explainable for engineering and compliance?
3. Can we adopt AI without sending telemetry to third-party model APIs?
4. Will AI improve MTTR quickly, without a tooling rewrite?

How PulseWatch Answers

1. Local/offline AI features are tenant-scoped and optional by policy
2. Transparent model lifecycle: bootstrap, nightly retraining, hourly scoring
3. Actionable outputs: incident summaries, root-cause hints, anomaly signals, risk forecasts and all done locally/offline
4. Faster MTTR without a tooling rewrite: PulseWatch overlays your existing stack for quicker triage and fewer blind spots

Decision Summary

PulseWatch gives enterprise teams one secure, scalable system for reliability operations.

- Modern monitoring coverage with governance-ready controls
- Flexible architecture: SaaS speed with private-node optionality
- Clear path to measurable outcomes in the first 90 days

PulseWatch

Next Step: Enterprise Technical Workshop

Align architecture, security controls, and rollout scope with your team.

Book a 60-minute workshop

Get a hands on demo of the service with one of team to answer all your questions!

Prep checklist

Critical services list

Identity/SSO constraints

Escalation channels

Compliance priorities