

nimbleNOVA

Converged IAM. One Platform. No Gaps.

Every identity, workforce, consumer, cloud, and AI, determines what the enterprise can access, what it is exposed to, and what it can prove. Cross Identity governs all of them, from one platform, continuously.

Overview

Secure every identity in the enterprise, workforce, customers, machines, and AI agents, on one converged IAM platform. nimbleNOVA is Cross Identity's converged Identity Security and Governance platform: one policy engine, one shared identity store, and one audit trail governing every identity type, built on 26+ years of enterprise identity expertise.

A Different Category: Converged Identity Security and Governance

This is distinct from:

- Traditional IAM (standalone AM or IGA tools): addresses one discipline, leaves gaps between tools.
- Integrated suites (loosely coupled best-of-breed): separate data models, policy engines, and audit outputs remain.
- Point solutions (CIAM-only, cloud CIEM, AI governance tools): solve one problem, add integration overhead elsewhere.

Converged Identity Security and Governance means one platform, one policy engine, one audit trail, governing every identity type across every discipline.

Platform Modules

6 modules. One identity store. One platform.

All six modules share one identity store, with decisions propagating in real time across modules.

Module	What it does
Access Management (AM)	SSO, adaptive MFA, and access policy across cloud and on-prem apps.
Identity Governance & Administration (IGA)	Provisioning, access certification, and lifecycle management.
Identity Risk Management / WarChief (IRM)	Continuous risk scoring, anomaly detection, and up to 9 automated response actions.
Customer Identity (CIAM)	Consent management and data principal rights for customer-facing apps. India DPDP compliance via VISHWAAS.
Cloud Governance & FinOps (CGF)	Visibility and control over cloud entitlements and spend. Surfaces 25 to 40% in recoverable cloud waste.
AI Governance / Xenetra	Model discovery, behavior governance, prompt injection detection, and a tamper-evident AI audit trail.
Privileged Access Management (PAM)	Privileged session management, JIT access, approval workflows, and vaulting.

Deployment

Delivered as a cloud tenant. Typical deployment: 4 to 6 weeks. Compliance evidence is produced continuously, not just at audit time.

Why nimbleNOVA

- **One identity store** across all six modules, with real-time propagation, so access decisions never fall out of sync.
- **One tool for IAM plus GRC** (Governance, Risk, and Compliance), instead of stitching identity and compliance tools together.
- **Enterprise-ready connectors.**
- **IRM (WarChief) sits at the core**, not bolted on. Risk signals trigger authentication changes in AM and governance actions in IGA in real time.
- **One fabric across all identity types:** workforce, cloud, consumer, AI, and non-human.
- **A single risk dashboard** for faster threat detection and response across every identity and every module.
- **Simplified IAM ecosystem:** less fragmentation, less operational overhead, no integration dependency.

Industry Recognition

KuppingerCole, the Gartner of IAM, recognized nimbleNOVA as both Overall Leader and Strong Challenger across five domains: Identity Governance & Administration (IGA), Identity Access Governance (IAG), Access Management (AM), Cloud Infrastructure Entitlement Management (CIEM), and Identity Fabric.

KuppingerCole's lens is identity and access management alone, so the evaluation goes deeper on IAM specifically rather than covering it as one category among many.

Compliance & Certifications



Regulatory Alignment

Example regulatory frameworks the platform aligns to:

DPDPA 2023, RBI IT Governance, SEBI CSCRF, IRDAI ICS, GDPR, PCI-DSS v4.0, NIST CSF 2.0, HIPAA, and SOX.

Built For

- Identity-based breaches, privilege creep, AI attack surface, incomplete coverage
- Operational cost of running 4 to 6 identity tools, integration overhead
- Consumer identity scalability, consent management, data rights compliance
- Tool fragmentation, manual processes, certification without enforcement
- Evidence gaps for regulatory compliance audits
- Cloud cost attribution, ROI of a converged platform vs. multiple vendors

Getting Started

Start with one module, see results, and expand on your own timeline. No long contract required to begin.