

nimbleNOVA

Customer Case Studies

BFSI · Healthcare · Manufacturing · IT / ITES

Stopping a Fraud Attempt Mid-Session

AM + Risk + IGA working as one — private-sector bank, 4,000+ employees across branch and corporate functions

MODULES: ACCESS MANAGEMENT · IGA · RISK (WARCHIEF)

THE CHALLENGE

- MFA fired the same way for every login, regardless of risk context
- No automatic link between a suspicious login and an SoD-sensitive role
- Security relied on end-of-day log reviews to catch anomalies

HOW NIMBLENOVA RESPONDED

- 1 Attacker logs in with valid, reset credentials from an unrecognized location
- 2 Warchief flags the new location, new network, and recent password reset
- 3 Risk score triggers step-up MFA instead of a plain allow
- 4 MFA fails — account suspended and an SoD-linked review auto-created

RESULTS: BEFORE → AFTER NIMBLENOVA

TIME TO DETECT ANOMALOUS LOGIN

Before: End-of-day review

After: Real time, at login

MFA APPLIED BY RISK CONTEXT

Before: No — same for every login

After: Yes — step-up on flagged sessions

LOGIN-TO-SOD-ROLE LINK

Before: Manual correlation, if at all

After: Automatic, same event

ACCOUNT COMPROMISE OUTCOME

Before: Would go undetected

After: Session blocked before any transaction

Closing the Gap Left by Departed Consultants

IGA + Risk for a hospital network — multi-facility network with a large base of rotating consultant doctors

MODULES: IGA · ACCESS MANAGEMENT · RISK (WARCHIEF)

THE CHALLENGE

- No automated trigger to deprovision consultant access after engagements ended
- Dormant accounts with live patient-data access were a standing DPO concern
- Consultant accounts carried the same risk posture as full-time clinicians

HOW NIMBLENOVA RESPONDED

- 1 HR system marks a consultant's engagement as complete
- 2 nimbleNOVA automatically revokes HIS, lab, and SSO access
- 3 Warchief applies stricter dormancy thresholds as a safety net
- 4 Flagged accounts surface in the next IGA certification campaign

RESULTS: BEFORE → AFTER NIMBLENOVA

CONSULTANT DEPROVISIONING

Before: Manual, ticket-dependent
After: Automated at engagement end

DORMANT ACCOUNT DISCOVERY

Before: Found only during audits
After: Flagged continuously

RISK TREATMENT FOR CONSULTANTS

Before: Same as full-time staff
After: Tailored, stricter thresholds

DPO AUDIT READINESS

Before: Reactive
After: Continuous evidence trail

Catching Privilege Creep Before It Reaches the Plant Floor

IGA + Risk — multi-plant manufacturer running SCADA-adjacent IT systems alongside standard corporate apps

MODULES: IGA · RISK (WARCHIEF) · ACCESS MANAGEMENT

THE CHALLENGE

- Mover events added access but rarely removed what was no longer needed
- No ongoing signal for excess access between certification cycles
- Plant-system entitlements got the same review cadence as everything else

HOW NIMBLENOVA RESPONDED

- 1 A supervisor moves from a plant role to a corporate project team
- 2 The Mover Access Change Report shows old and new access side by side
- 3 Warchief flags the account as holding more access than its peer group
- 4 Flagged entitlement is revoked without waiting for the next audit cycle

RESULTS: BEFORE → AFTER NIMBLENOVA

DETECTION OF EXCESS ACCESS

Before: Annual audit only

After: Continuous, between cycles

OLD VS. NEW ACCESS VISIBILITY

Before: Manual comparison

After: Single Mover Access Report

STALE PLANT-SYSTEM ACCESS

Before: Up to a year

After: Days, via out-of-cycle flag

EMPLOYEE APP ACCESS EXPERIENCE

Before: Mixed old and new access

After: Clean, current access via Launchpad

When 'Approve All' Isn't Really a Review

Catching rubberstamping in the act — mid-size IT services firm managing infrastructure access for 25+ application owners

MODULES: IGA · RISK (WARCHIEF) · ACCESS MANAGEMENT

THE CHALLENGE

- No systematic way to tell a genuine review from a rubber-stamped one
- Legacy applications accessed via password vaulting were easy to overlook
- The firm's ISO 27001 auditor began questioning review quality

HOW NIMBLENOVA RESPONDED

- 1 Quarterly certification campaign launches across all application owners
- 2 Warchief detects a reviewer approving 40 items in under two minutes
- 3 The completed campaign is flagged for follow-up, not accepted at face value
- 4 IGA reopens the flagged items for a genuine, item-by-item re-review

RESULTS: BEFORE → AFTER NIMBLENOVA

RUBBERSTAMPED REVIEWS DETECTED

Before: Found by chance, spot-check

After: Flagged automatically by pattern

'COMPLETE' VS. 'GENUINE' REVIEW

Before: No distinction

After: Built into the risk layer

LEGACY APP ENTITLEMENTS REVIEWED

Before: Frequently skipped

After: Included via vaulting visibility

AUDITOR CONFIDENCE

Before: Questioned

After: Backed by detection evidence

Closing the Banking Compliance Audit Gap

Converged IGA + IRM for a growing NBFC — mid-sized Non-Banking Financial Company with ~2,400 employees and 60+ branch offices

MODULES: IGA · IRM (WARCHIEF RISK ENGINE) · COMPLIANCE REPORTING

THE CHALLENGE

- Access certification cycles took 6–8 weeks and still missed dormant accounts
- No real-time view of toxic combinations, like disbursal + approval rights
- Regulator’s annual IT examination flagged the lack of automated, evidence-backed reviews

HOW NIMBLENOVA RESPONDED

- 1 Automated joiner-mover-leaver workflows tied directly to HRMS
- 2 Warchief flagged SoD violations and high-risk combinations in near real time
- 3 Quarterly micro-certifications replaced the twice-yearly mega-review
- 4 Pre-built banking compliance report templates gave auditors a direct evidence trail

RESULTS: BEFORE → AFTER NIMBLENOVA

ACCESS CERTIFICATION CYCLE TIME

Before: 6–8 weeks

After: 9 days

SOD VIOLATIONS VISIBLE IN REAL TIME

Before: No

After: Yes, continuous

RBI AUDIT PREP EFFORT

Before: ~3 weeks, manual

After: 3 days, report-driven

ORPHANED ACCOUNTS IDENTIFIED

Before: Ad hoc, reactive

After: Detected automatically

DPDP-Ready in One Quarter

Unified SSO and consent-aware access — multi-city hospital network with 5 facilities and 3,000+ clinical and administrative staff

MODULES: ACCESS MANAGEMENT · IGA · VISHWAAS (DPDP COMPLIANCE)

GLOBAL COMPLIANCE: *Cross Identity is a global identity platform — DPDP is India's data-privacy law, and we map equivalent data-privacy requirements for every region we serve.*

THE CHALLENGE

- Staff logged into 12–15 clinical and back-office apps daily, each with separate passwords
- Consultant onboarding across facilities took 2–3 days
- No consolidated record of who accessed patient data, or under what consent basis

HOW NIMBLENOVA RESPONDED

- 1 SSO with step-up MFA unified access to patient-identifiable records
- 2 Automated provisioning for rotating consultants by facility and department
- 3 VISHWAAS mapped data access to DPDP consent and purpose-limitation rules
- 4 Audit-ready reports generated continuously for the hospital's DPO

RESULTS: BEFORE → AFTER NIMBLENOVA

CONSULTANT ONBOARDING TIME

Before: 2–3 days

After: Same day

PASSWORD-RELATED HELPDESK TICKETS

Before: ~35% of all IT tickets

After: Under 10%

DPDP COMPLIANCE REPORTING

Before: Manual, quarterly

After: Continuous, on-demand

APPLICATIONS UNDER UNIFIED SSO

Before: 0

After: 14

Taming Multi-Cloud Sprawl

CIEM and FinOps for a multi-plant manufacturer — diversified manufacturer with 8 plants across India and Southeast Asia

MODULES: CGF (CLOUD GOVERNANCE & FINOPS) · CIEM · SOT-DRIVEN LIFECYCLE

THE CHALLENGE

- Fragmented IAM policies across AWS, Azure, and GCP, with thousands of unused entitlements
- Cloud spend grew 22% year-on-year with no attribution to business units
- New hires waited days for access due to manual, disconnected provisioning

HOW NIMBLENOVA RESPONDED

- 1 CIEM surfaced over-privileged roles and unused entitlements across all three clouds
- 2 FinOps cost analytics attributed cloud spend to individual plants and cost centers
- 3 HR-driven SOT connectors automated new-hire and transfer provisioning
- 4 Plant and corporate teams gained one dashboard for cloud identity risk and spend

RESULTS: BEFORE → AFTER NIMBLENOVA

UNUSED / OVER-PRIVILEGED ENTITLEMENTS

Before: Unknown, unmeasured

After: Identified and remediated

CLOUD SPEND VISIBILITY BY PLANT

Before: None

After: Full attribution by plant

NEW-HIRE PROVISIONING TIME

Before: 3–5 days

After: Under 1 day

CLOUD COST GROWTH TREND

Before: +22% YoY, untracked

After: Flattened, ongoing review

Governing AI Agents Before They Become a Blind Spot

Xenetra for an IT services firm — mid-size IT/ITES provider managing infrastructure for 30+ client accounts

MODULES: XENETRA (AI AGENT / NHI GOVERNANCE) · PAM · MSSP MULTI-TENANT PORTAL

THE CHALLENGE

- AI agents and bots were provisioned ad hoc, with no central inventory
- No policy governing what an AI agent could access, or for how long
- Privileged access across client tenants relied on shared spreadsheets of credentials

HOW NIMBLENOVA RESPONDED

- 1 Xenetra's Identity Continuity model discovers and catalogs AI agents and service accounts across client environments
- 2 Time-bound, policy-driven access replaces standing credentials, with automatic expiry and rotation
- 3 PAM enforces just-in-time privileged sessions for engineers working across client tenants, with full session recording
- 4 The MSSP multi-tenant portal lets the security desk manage all 30+ clients from one console, fully segregated

RESULTS: BEFORE → AFTER NIMBLENOVA

AI AGENTS / NHIS WITH KNOWN OWNERSHIP

Before: Untracked
After: 100% cataloged

STANDING (NON-EXPIRING) AI AGENT CREDENTIALS

Before: Common practice
After: Eliminated via policy-based expiry

PRIVILEGED SESSIONS WITH RECORDING / AUDIT TRAIL

Before: Partial, inconsistent
After: Fully enforced across all client tenants

NEW CLIENT TENANT ONBOARDING TIME (MSSP)

Before: 1–2 weeks
After: 2–3 days

Governing AI Agents Before They Become a Blind Spot

Xenetra for an IT services firm — mid-size IT/ITES provider managing infrastructure for 30+ client accounts

MODULES: XENETRA (AI AGENT / NHI GOVERNANCE) · MSSP MULTI-TENANT PORTAL

THE CHALLENGE

- AI agents and bots were provisioned ad hoc, with no central inventory
- No policy governing what an AI agent could access, or for how long
- Privileged access across client tenants relied on shared spreadsheets of credentials

HOW NIMBLENOVA RESPONDED

- 1 Xenetra's Identity Continuity model discovers and catalogs AI agents and service accounts across client environments
- 2 Time-bound, policy-driven access replaces standing credentials, with automatic expiry and rotation
- 3 Privileged access control enforces just-in-time privileged sessions for engineers working across client tenants, with full session recording
- 4 The MSSP multi-tenant portal lets the security desk manage all 30+ clients from one console, fully segregated

RESULTS: BEFORE → AFTER NIMBLENOVA

AI AGENTS / NHIS WITH KNOWN OWNERSHIP

Before: Untracked
After: 100% cataloged

STANDING (NON-EXPIRING) AI AGENT CREDENTIALS

Before: Common practice
After: Eliminated via policy-based expiry

PRIVILEGED SESSIONS WITH RECORDING / AUDIT TRAIL

Before: Partial, inconsistent
After: Fully enforced across all client tenants

NEW CLIENT TENANT ONBOARDING TIME (MSSP)

Before: 1–2 weeks
After: 2–3 days

nimbleNOVA