Aurascape®

CUSTOMER CASE STUDY

THE POLICE CREDIT UNION

How The Police Credit Union Met Compliance Requirements While Enabling Responsible AI Adoption

Objectives

Safely accelerate GenAI use; protect NPI/PII; stay audit-ready by proactively aligning with emerging NCUA guidance and the NIST AI RMF.

Solution

Deploy Aurascape in two phases—first visibility, then protection—to monitor and govern AI usage with prevention-focused policies.

Projected Results

✓	27%	83%
AI Audit Ready	productivity gains	risk reduction

Customer Context

The Police Credit Union sought to stay audit-ready and compliant while improving productivity—enabling employees to use AI for summarizing procedures, drafting member communications, assisting with underwriting, and more, all without exposing member PII/NPI.

Challenges

Regulatory Expectations
GLBA/FFIEC guidelines and NCUA audits require demonstrable controls and evidence.

Shadow AI
Unvetted tools or personal accounts introduce data leakage and compliance risks.

Data Leakage
Unmonitored prompts and responses could expose sensitive data including NPI/PII, account details, or procedures.

Limited Visibility
Traditional security tools miss many brand-new AI tools and embedded AI, and lack conversation context, limiting policy precision.

Company Profile	
Headquarters	San Bruno, CA
Assets Under Management	$ 1.05B
Members	39,000
Employees	150

Objectives

- Provide audit-ready reporting and interaction logs mapped to GLBA/FFIEC/NCUA expectations.
- Surface and prevent risky interactions; uncover and remediate Shadow AI.
- Enforce policies that prevent NPI/PII exposure without blocking legitimate work.
- Gain full, contextual visibility into AI apps, users, and shared data.

Ensuring Compliance with AI Use

The Police Credit Union (TPCU) extended GLBA mandates, FFIEC procedures, Reg P safeguards, and the NCUA security program to cover AI usage—ensuring a complete AI inventory, risk scoring, and protecting member information in prompts and responses, with continuous monitoring and rapid response to risky use.

✓ **By mapping AI controls to the NIST AI RMF (Govern/Map/Measure/Manage) and NCUA AI guidance, The Police Credit Union security program demonstrates alignment with how regulators articulate AI risk.**

TPCU Regulatory Compliance Assurance with Aurascape

Extend the security program to AI (NCUA AI Compliance Plan)
Align with the NCUA's AI Compliance Plan outlining the strategies and measures in place to oversee responsible AI implementation, provide a strong AI governance framework, and ensure transparency and accountability.

Continuous monitoring & controls (NCUA Compliance Plan/Part 748; NIST Measure/Manage)
Always-on AI app inventory, user/app visibility, and new-feature discovery with auditor-ready logs and metrics. Conversation-aware guardrails protect member information across prompts and responses.

Service-provider & embedded-AI oversight (NCUA AI Compliance Plan/ Part 748; NIST Supply-Chain Risk)
Enforce enterprise accounts, block unsanctioned apps, and govern functions within AI apps.

Privacy-by-default for PII/NPI (NCUA AI Compliance Plan/Part 748; NIST Map/Measure)
Prevent SSNs, account numbers, and other identifiers from leaking via inputs and outputs—without slowing work.

Executive accountability & board reporting (NIST Govern)
Role-based reporting and natural-language investigation give leaders line-of-sight into AI use, risk, and outcomes.

How The Police Credit Union Embraced AI, Safely

TPCU projects a **27% boost in productivity** by allowing employees to safely leverage AI for:

Loan Origination & Underwriting

Staff can securely leverage AI to accelerate document review and decision support throughout the origination and underwriting process. Aurascape keeps SSNs, member info, DL images, and account/routing info from leaking out of the LOS/CRM via unapproved AI usage.

Member Support & Contact Center

Frontline employees use approved AI tools to quickly draft accurate responses to member inquiries such as balance, payoff, and dispute questions, while also summarizing account history and documenting interactions efficiently. Aurascape automatically prevents sensitive data such as SSNs, PANs, and account numbers from being exposed to unapproved AI systems, ensuring regulatory compliance.

Marketing & Member Outreach

Marketing and sales teams use approved AI tools to draft campaigns and member communications quickly and consistently, staying within defined guardrails. Aurascape ensures no sensitive or member information is exposed to public AI models during this process.

Collections & Delinquency Management

Employees can use approved AI tools to review delinquent accounts, analyze repayment options, and summarize member payment histories. These tools help staff identify trends, prioritize outreach, and prepare accurate communications for follow-up while ensuring sensitive financial and member data remain secure.

Compliance & Risk Reporting

Compliance staff may only use approved AI tools with proper access to summarize SARs, BSA/AML alerts, and filings. Aurascape will flag any sensitive member information, and users must review and verify the message before sending to ensure compliance.

Executive & Board Reporting

Leaders use approved AI tools to review and analyze operational and financial information, while Aurascape safeguards against the exposure of highly sensitive data privileged to the C-suite and upper management.

TPCU Risks Mitigated with Aurascape

Discover & Monitor All AI Use

Automatically discover AI applications and shadow AI within existing tools, providing contextual visibility into risks, usage, and data exposure for a real-time AI inventory.

Terminate Risky AI Usage

Access controls combined with intent-aware policies block unapproved or high-risk tools and behaviors in real time, while guiding users and generating audit-ready logs.

Enable Approved Apps with Enterprise Accounts

Ensure staff use enterprise accounts for approved AI tools and guide them away from personal accounts, enabling policy-aligned AI adoption.

Secure Use of Embedded AI in SaaS & Chatbots

Govern interactions with AI features inside apps and websites—traffic traditional security tools often miss.

By uncovering and coaching users away from unsanctioned and risky AI use, TPCU projects an **83% reduction in AI-based risk.**

Protected Member Data Detected & Governed

Real-time detection and prevention stop sensitive member data (PII/NPI) in prompts and responses from reaching LLMs or third-party vendors via employee AI use.

- Member number / account number; ABA routing & MICR line elements
- SSN; driver's license / state ID; passport
- Card PAN (debit/credit), CVV, expiration
- Loan/application IDs; income docs (W-2, paystubs); wire/ACH instructions

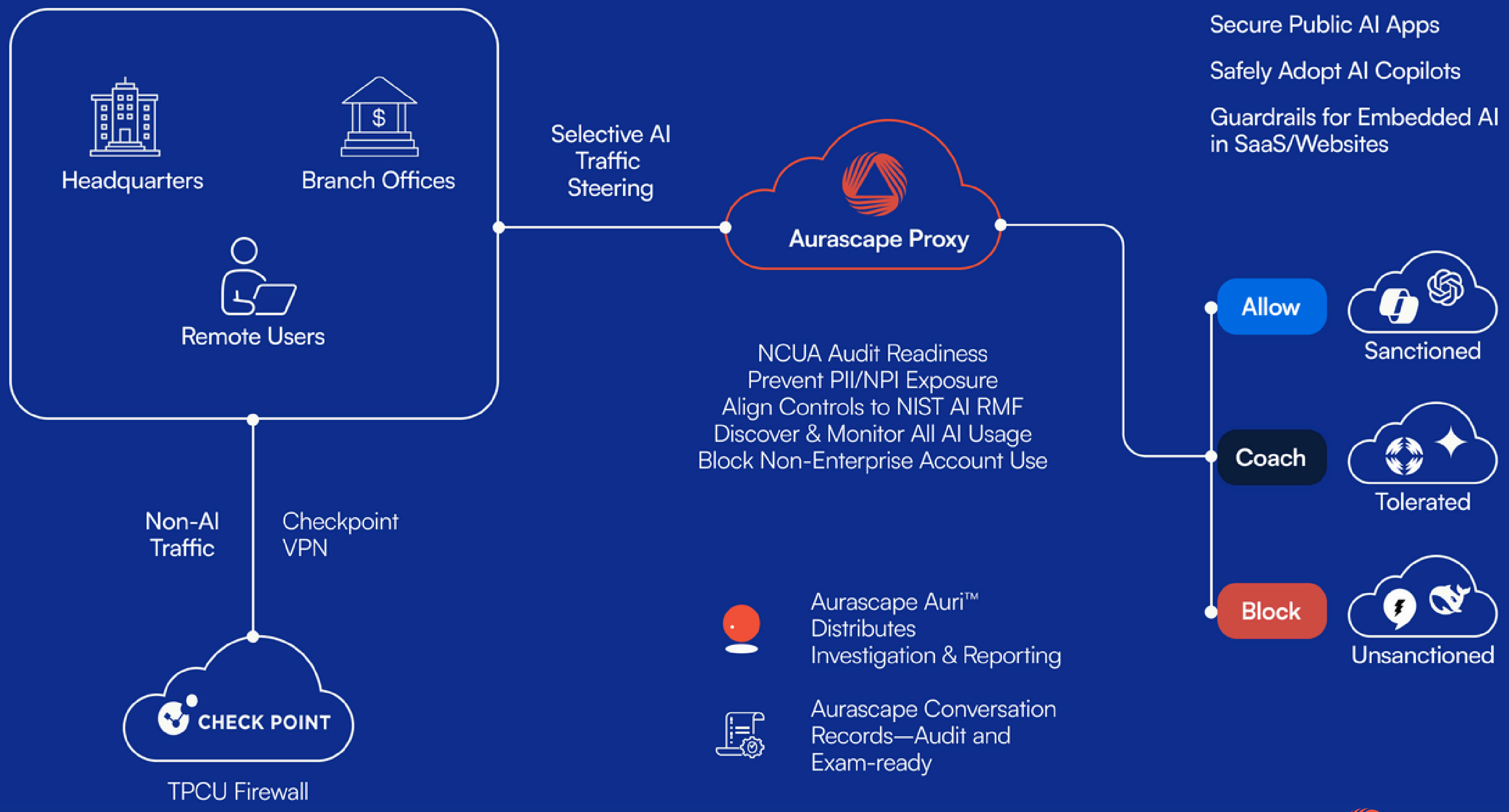
Aurascape®

Aurascape Deployment | 2-Phase Approach

Visibility | Phase 1
Build the AI app inventory with automated discovery of new AI apps and features, app risk assessments, user entitlement and data exposure visibility.

Protection | Phase 2
Coach users away from risky AI use; require enterprise accounts for approved AI apps; map data protections to credit-union classifiers to prevent sensitive data leakage.

The Police Credit Union (TPCU) Footprint



Headquarters

Branch Offices

Remote Users

Selective AI Traffic Steering

Aurascape Proxy

Secure Public AI Apps

Safely Adopt AI Copilots

Guardrails for Embedded AI in SaaS/Websites

Allow — Sanctioned

Coach — Tolerated

Block — Unsanctioned

NCUA Audit Readiness
Prevent PII/NPI Exposure
Align Controls to NIST AI RMF
Discover & Monitor All AI Usage
Block Non-Enterprise Account Use

Non-AI Traffic

Checkpoint VPN

CHECK POINT

TPCU Firewall

Aurascape Auri™ Distributes Investigation & Reporting

Aurascape Conversation Records—Audit and Exam-ready

Aurascape®

WHY AURASCAPE

Architecture & Ease
Inline, real-time prevention without PAC files or local routing changes; routes only AI traffic.

Conversation Context
Evaluates prompts and responses to catch risks on both sides.

Intent-aware Controls
Granular control over specific functions within AI apps.

Credit Union–specific Classifiers
Out-of-the-box member information data detectors for account numbers, DL, SSN, and other identifiers.

Role-based Governance
Distributed oversight for Security, Compliance, HR, and leaders via Auri™.

> “We’re prepared for the NCUA AI Compliance Plan and have implemented a clear framework to guide staff in adopting AI responsibly.
>
> **Without Aurascape, we had seriously considered blocking all GenAI usage.**
>
> That would have held us back while others moved forward.”

Victor To, CISSP
Senior Security Architect
The Police Credit Union

Aurascape®

Do A Quick Risk Assement Yourself

□ Can prove enterprise-only AI accounts are enforced.

□ Prevents NPI leakage in AI prompts and responses—with audit-ready logs.

□ Governs embedded AI in SaaS and websites (not just standalone apps).

□ Maintains a third-party AI app inventory and vendor diligence for all apps.

□ Can export audit-ready evidence of AI usage control in under 24 hours.

□ Maps controls to NIST AI RMF (Govern/Map/Measure/Manage).

Ready to get the complete view of your Risk? Start your free AI Risk Assessment now to catch AI-related risks before the auditors do.

https://aurascape.ai/risk-assessment

Aurascape, Inc.
2625 Augustine Drive, Suite 150
Santa Clara, CA 95054

Aurascape®