CAPSTONE PROJECT

Geo-Boundary Evidence Pack

What is it?

The Geo-Boundary Evidence Pack Generator is an AI-powered compliance automation platform that provides verifiable, auditor-ready proof that sensitive data traffic remains within defined geographic and sovereign boundaries.

- **Automated Geo-Compliance**: Transforms network telemetry (VPC logs, NetFlow) into data residency evidence
- **AI-Driven Narrative Engine**: Uses LLMs to synthesize routing data and BGP paths into plain-English
- **Verifiable Evidence Packs**: Generates cryptographically signed reports and "Evidence Packs"
- **Multi-Environment Sovereignty**: Architected for neutrality across multi-cloud, hybrid, and air-gapped environments, with localized AI processing to ensure absolute data isolation.
- **Proactive Risk Management**: Employs predictive models to alert on "near-miss" routing changes before they result in a jurisdictional compliance violation

Compliance Officer “Claire”

Name: Claire Beaumont
Title: Senior Director of Global Data Privacy
Company: Tier 1 Multinational Financial Services firm (e.g., "GlobalBank Corp")
Experience: 15+ years in Legal/Compliance, with the last 5 years focused on Digital Data Sovereignty.

Interests

Stays ahead of emerging laws like the EU Data Act and US Cloud Act.

International Policy: Follows geopolitical shifts that impact data residency and sovereign borders.

Goals

Ensure all regional data residency audits are passed with 100% verifiable evidence.

Reduce the "Compliance Tax", time and cost spent by engineering teams to satisfy compliance

Pain Points/Frustrations

She doesn't speak "BGP" but she is responsible for the outcome of that protocol

2-week turnaround time for "Proof” that French customer data stayed in France.

Motivations

Avoiding the fines from GDPR violations.

Being seen as a "Business Enabler" who uses technology to speed up growth rather than a "Roadblock.”

Challenges

Extracting "Sovereign Proof"

She needs to be able to explain how the AI verified the data path if a regulator asks.

Needs & Expectations

Verifiable Evidence

Human-Readable Insights

Proactive Alerting: Expects to be told at least the moment it happens, not during an audit.

Technology & Social Media

Daily user of GRC platforms (OneTrust, ServiceNow), Slack/Teams for cross-functional comms, and Tableau/PowerBI for reporting. High activity on LinkedIn for networking, sharing policy updates

Content-Type Preferences

Executive Summaries, Data-Visualizations, Whitepapers

Content that maps a feature (e.g. Geo-Fencing) directly to a regulation (GDPR Article 44).

Brands & Influences

Gartner, for strategy, Deloitte/EY (for audit standards), IAPP (International Association of Privacy Professionals). Industry thought leaders on LinkedIn who discuss the intersection of "Law and Code."

Empathy Map

Says

- I need to prove to the regulators that our German customer data never touched a US server.
- Can we get a report that a non-technical auditor can actually understand?
- Why does it take two weeks to get a simple traceroute log from the networking team?
- Is this AI-generated summary 100% accurate? I can’t afford a hallucination in a legal filing.

Thinks.

- “If the networking team messes up a BGP route, I’m the one who has to explain the $50M fine to the CEO.”
- “I wish I understood the technical side better, so I didn't feel so dependent on the engineers.”
- “There has to be a way to automate this; we are wasting hundreds of high-value man-hours on manual reporting.”
- “Is our 'Sovereign Cloud' actually sovereign, or is that just marketing fluff?”

Does.

- Reviews complex 50-page network audit logs looking for "out-of-boundary" hops.
- Attends weekly "Risk & Compliance" steering committees with the Board.
- Coordinates between the Legal department and the Network Operations Center (NOC).
- Signs off on annual compliance certifications for regional data residency laws.
- Uses LinkedIn to track the latest enforcement actions by the Irish DPC or Saudi SDAIA

Feels.

- Anxious during audit season, fearing a "hidden" compliance leak that wasn't caught in time.
- Frustrated by the slow, manual processes and the "technical wall" between her and the network data.
- Responsible for the company’s reputation and the privacy of millions of customers.
- Empowered when she has a clear, data-backed dashboard that shows 100% compliance in real-time.

Use Cases

Compliance Officer

Name: Claire Beaumont
Title: Senior Director of Global Data Privacy
Company: Tier 1 Multinational Financial Services firm (e.g., "GlobalBank Corp")
Experience: 15+ years in Legal/Compliance, with the last 5 years focused on Digital Data Sovereignty.

One-Click Auditor Reports
Instantly create simple PDF summaries for regulators to prove that sensitive customer data never left the defined region during the month.

Instant "Wrong Border" Alerts
Get a notification the second data accidentally crosses a border, allowing you to fix it before it becomes a legal problem.

Plain-English Network Summaries
An AI that explains complex technical logs in simple language so that managers and lawyers can understand exactly how data is moving.

Proof-of-Local-Data for Sales
Win big contracts by giving potential clients a "Sovereign Certificate" that guarantees their data will stay safe and local at all times.

The Compliance Time-Machine
Easily look back at any date to show exactly where data was, making it simple to answer regulator questions in seconds.

Pain Points

Complaince Officer

Name: Claire Beaumont
Title: Senior Director of Global Data Privacy
Company: Tier 1 Multinational Financial Services firm (e.g., "GlobalBank Corp")
Experience: 15+ years in Legal/Compliance, with the last 5 years focused on Digital Data Sovereignty.

The Technical Language Barrier
Because they can't read complex network code, they must ask busy engineers to manually "translate" technical logs into simple emails for regulators.

The Massive Time Drain
Preparing for an audit takes weeks of manual work, often requiring senior staff to stop their regular jobs just to dig through old data logs.

Finding Mistakes Too Late
They currently operate on "best-effort" assumptions and only discover that data crossed a border months later during a formal audit.

Difficulty Closing Sales
They make vague promises in contracts about data staying local but lack the "hard proof“ needed to quickly convince skeptical new clients.

Auditor Skepticism
Regulators often struggle to trust raw technical data, forcing compliance teams to write long, complex explanations to prove the information is accurate.

Competitor Analysis

LEADERS

- **Cisco (ThousandEyes):** The undisputed industry standard for global visibility. They have the largest data footprint and high trust, though they are often viewed as a premium-priced "engineer-only" tool.
- **VMware (Sovereign Cloud):** Dominates the enterprise infrastructure market with a massive, loyal user base and a global ecosystem of partners specifically focused on data residency.
- **Microsoft (Azure Sovereignty):** Leverages a massive existing cloud footprint to provide built-in compliance, making it the default choice for many enterprise IT departments.

HIGH PERFORMERS

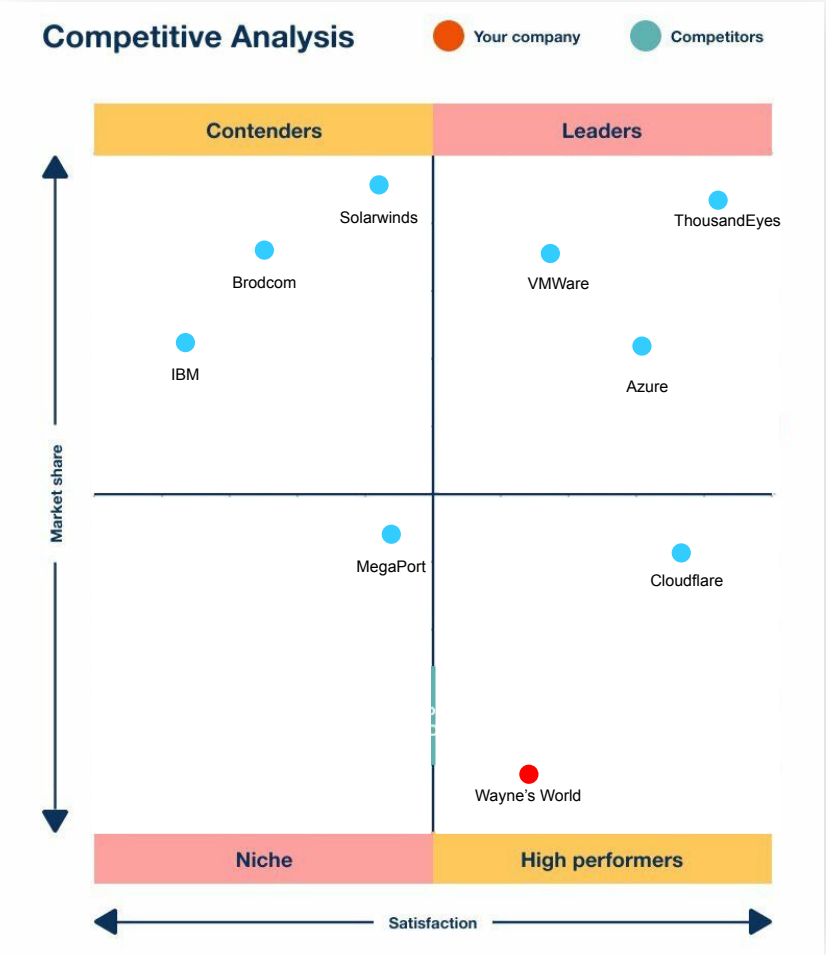
- **Wayne's World (Our Product):** The Fan Favorite. We solve the pain points that others ignore, earning high satisfaction by turning technical data into legal evidence for non-technical users.
- **Cloudflare (Geo-Suite):** Highly popular with modern IT teams for its "set-it-and-forget-it" approach to data localization and its incredibly fast edge-computing network.

CONTENDERS

- **SolarWinds (NPM):** Found in almost every data center due to its massive history, but satisfaction is often hampered by its "Legacy" feel and the manual effort required for modern auditing.
- **Broadcom (DX NetOps):** Huge enterprise reach via its CA Technologies heritage but frequently criticized by modern compliance teams for being overly complex and "clunky" to navigate.
- **IBM (Netcool):** A giant in the telecom space with a global presence but often cited for being slow to innovate and difficult for non-technical users to generate reports from.

NICHE

- **Megaport (Virtual Edge):** Niche but highly valued by users who need fast, software-defined cloud connections with compliance "baked into the pipes."



Problem Statement

The lack of automated, verifiable, and non-technical proof of sovereign boundary compliance currently creates a trust-gap for high-value prospects, leading to a bottleneck sales pipeline for compliance focused customers and a loss in sales that could be captured through real-time 'Sovereign Ready' certification.

The Mission

“To empower global enterprises with verifiable trust by transforming complex network telemetry into automated, plain-English compliance evidence, ensuring that data sovereignty is never an obstacle to global growth."

PRFAQ

PRFAQ for Geo-Boundary Evidence Pack Generator

Press Release:

Date: May 1, 2026

Wayne's World Introduces Geo-Boundary Evidence Pack Generator: The Future of Sovereign Networking Through AI

Today, Wayne's World is thrilled to unveil the Geo-Boundary Evidence Pack Generator, an innovative AI-powered solution designed to provide verifiable, auditor-ready evidence of geographic data residency. With the evolving needs of global compliance officers and regulated industries, the Geo-Boundary Evidence Pack Generator aims to transform complex network telemetry into strategic compliance intelligence, ensuring "Zero-Trust Geo-Compliance."

"We recognized a need in the enterprise networking field to bridge the gap between technical network paths and legal proof. With the Geo-Boundary Evidence Pack Generator, we are harnessing the power of AI to address this in a way that has never been done before," says Wayne Correa, CEO and Founder of Wayne's World.

Features and Benefits:

- **Automated PDF Evidence Packs:** Instantly generate certified reports for regulators that summarize 30 days of data residency compliance in plain English.
- **Real-Time Sovereign Alerts:** Receive immediate notifications the moment a network path "flaps" outside defined national borders.
- **AI Path-to-Text Synthesis:** Leverages Large Language Models to translate complex BGP and traceroute data into human-readable narratives for non-technical auditors.
- **Cryptographic Proof of Residency:** Every report is digitally signed and timestamped, providing a tamper-proof "Sovereign Certificate" for use in audits and sales cycles.

FAQs

- **What exactly is the Geo-Boundary Evidence Pack Generator?**
  The Geo-Boundary Evidence Pack Generator is Wayne's World's latest innovation in the realm of AI, designed to automate the verification of geographic data boundaries. It is unique because it focuses on the "Provenance" of data, providing a verifiable paper trail of where data has been, rather than just how fast it moved.
- **Why did Wayne's World decide to develop an AI-based solution like the Geo-Boundary Evidence Pack Generator?**
  In our research and through feedback from Governance, Risk and Compliance (GRC) leaders like "Claire," we realized that compliance teams are currently drowning in technical logs they cannot read. AI offers a unique solution to this challenge by synthesizing millions of raw data points into a clear, executive-grade narrative that anyone can understand.
- **How does the Geo-Boundary Evidence Pack Generator differ from other products in the market?**
  While there are other solutions addressing network visibility (like Cisco ThousandEyes), what sets our product apart is its focus on the Compliance Officer and absolute sovereignty. In Phase 2, the AI "Brain" runs entirely within your managed perimeter, ensuring no sensitive telemetry ever leaves your network.
- **How do users get started with the Geo-Boundary Evidence Pack Generator?**
  Users can start with our **Phase 1 Cloud Beta** via the Wayne's World Cloud Marketplace. For enterprises requiring higher security, **Phase 2** allows you to deploy the tool as a Virtual Network Function (VNF) on **Wayne's Virtual Edge** or directly onto your own hardware in your datacenter or colocation facility.

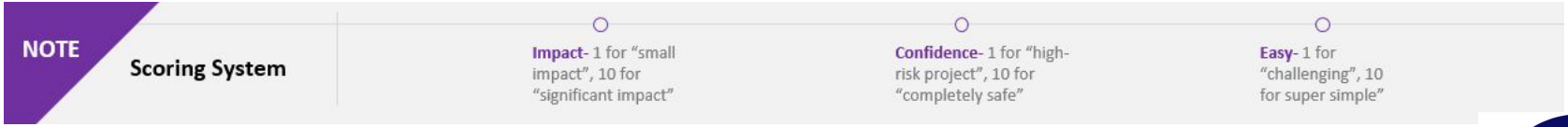
  Are there any concerns regarding data privacy and security with the Geo-Boundary Evidence Pack Generator?
  Wayne's World places the utmost importance on data privacy and security. The Generator is built with "Sovereign AI" protocols. In Phase 2, all analysis happens on localized infrastructure that you control, ensuring that the tool used to prove sovereignty is, itself, sovereign. No data is ever sent to public AI providers.

Link: https://docs.google.com/document/d/1XQXKeBxOW6kz0DVuuxNW0wCdEv7H1O_0kWXvQqQLc2c/edit?usp=sharing

RICE model

Feature	Reach	Impact	Confidence	Effort	Score
Cryptographic Evidence Signing	10	9	9	3	270
Phase 1: Cloud-Native Beta (VPC Logs)	10	7	9	4	158
"Plain-English" AI Path Synthesis	10	9	7	5	126
Phase 2: "Sovereign-Local" Appliance	8	10	8	7	91
Real-Time Geo-Violation Alerts	6	8	8	6	64
Phase 3: Fabric-Native	10	10	5	10	50

- Start with low-effort, high-impact trust features (Signing & Cloud Beta) to gain immediate market traction.
- Scale into AI-driven narratives and local hardware deployment to solve the deep privacy needs of regulated industries.
- Finish by baking the compliance engine directly into the physical network fabric of Wayne's World.



(Reach × Impact × Confidence) ÷ Effort = RICE Score

Functional requirements

Automated Telemetry Ingestion
- Cloud Phase 1 - The system MUST pull VPC Flow Logs (metadata) from Google Cloud and Azure via read-only API access.
- Sovereign Phase 2 - The system MUST ingest NetFlow (v9/v10) and IPFIX telemetry directly from on-prem or virtual routers.
- The system MUST ignore packet payload (content) and only process metadata headers to maintain user privacy.

AI-Powered Path Synthesis
- The system MUST correlate telemetry data with high-accuracy Geo-IP databases to identify the national borders crossed by each data path.
- An LLM-based engine MUST translate raw network hops (e.g., 192.168.1.1 -> 10.0.0.1) into a natural language summary (e.g., "Data traveled from Germany to France via London").
- The system MUST automatically flag any traffic that "flaps" outside a customer-defined geographic boundary.

One-Click "Evidence Pack" Generation
- The user MUST be able to generate a PDF report for any 24-hour, weekly, or monthly period with a single click.
- Reports MUST include a map visualization of data boundaries and a summary of compliance percentages.
- The system MUST allow for "Ad-Hoc" forensic reports to be generated for specific retrospective date ranges.

Cryptographic Verification
- Every generated report MUST be digitally signed using a Wayne's World private key to prevent tampering.
- Each report MUST include a unique QR code or verification link that allows an auditor to confirm the document's authenticity.

Sovereign-Local Processing (Phase 2)
- The system MUST be deployable as an isolated Virtual Network Function (VNF) on Wayne's Virtual Edge or private hardware.
- All AI inference (the LLM "Brain") MUST occur locally within the customer's managed perimeter.
- The system MUST be capable of operating in an "Air-Gapped" mode without requiring any outbound internet connection for its core functions.

User Interface
- The dashboard MUST provide a non-technical view for GRC officers (Claire) that highlights "Compliance" and "Anomalies."
- The system MUST allow for the configuration of custom "Sovereign Zones" (e.g., "Only EU-based countries are authorized").
- The dashboard MUST support "Role-Based Access Control" (RBAC) to ensure only authorized legal/compliance staff can generate reports.

Non-Functional requirements

Security & Sovereign Integrity
- The system MUST ensure that 100% of telemetry data and AI inference stay within the customer-managed perimeter (Local Hardware or Virtual Edge).
- All access to the GRC Dashboard MUST require Multi-Factor Authentication (MFA) and adhere to the principle of Least Privilege.
- All data "at rest" (on local disks) and "in transit" (between routers and the appliance) MUST be encrypted using AES-256 or higher.
- Every action taken by a user (e.g., generating a report, changing a geo-boundary) MUST be logged in a tamper-proof audit trail

Performance
- A standard monthly Evidence Pack (analyzing up to 10M flow records) MUST be generated in under 60 seconds.
- The system MUST process NetFlow/VPC metadata within 5 minutes of the actual network event to ensure timely violation alerts.
- The GRC Dashboard MUST maintain a sub-2-second response time for all standard navigation and filtering actions.

Scalability
- The system architecture MUST support horizontal scaling to handle global enterprises with thousands of routers across multiple regions.

Availability & Reliability
- The Dashboard and Evidence Generator MUST maintain 99.9% availability to ensure reports are accessible during urgent audit requests.

Usability & Accessibility
- The user interface MUST be optimized for a non-technical Compliance Officer (Claire), avoiding CLI-style outputs in the primary reporting view.
- The AI Narrative Engine MUST support report generation in English, French, and German at launch to satisfy key EU sovereign markets.

Compliance & Legal Standards
- The system's data handling processes MUST be fully compliant with GDPR (General Data Protection Regulation)
- The AI MUST provide "Source Grounding" in reports, allowing an auditor to see the raw IP/Path data that led to a specific natural-language conclusion.

Requirements for AI team

In which ways will your solution leverage AI? *Our solution uses AI to bridge the gap between complex network data and legal compliance. Specifically:*

- *Path-to-Text Synthesis (Generative AI): Translating millions of raw traceroute and BGP JSON records into human-readable narratives for non-technical auditors.*
- *Using Retrieval-Augmented Generation to compare real-time network paths against a customer's specific "Sovereign Rulebook" to identify subtle compliance leaks.*
- *Identifying patterns in BGP routing that suggest a path "flap" outside a geographic boundary is likely, allowing for proactive traffic re-routing.*

What should be the input of the model? *The model ingests Network Telemetry Metadata, not user content. Key inputs include:*

- *VPC Flow Logs & NetFlow/IPFIX Records: Source/Destination IPs, timestamps, and protocol types.*
- *BGP Path Attributes: The sequence of Autonomous Systems (AS) and cities the data passed through.*
- *Geo-IP Spatial Data: High-fidelity mapping of IP addresses to physical national borders.*
- *Customer Compliance Policies: The specific legal requirements (e.g., "Data must remain in the EU").*

Data Collection: Do you have the data needed? How will you collect it? *We leverage the customer's existing cloud logs via secure, permission-based 'Sinks.' While we don't own the physical cables, we gain global reach instantly through the cloud provider's APIs, allowing us to scale across 50+ regions without ever touching a router. We must build a Cloud-Native Ingestion Pipeline:*

- *Permission-Based "Invites": The customer grants our service Identity and Access Management (IAM) permissions (e.g., "Logging Viewer" role) to their specific cloud projects.*
- *Log Sinks & Pub/Sub: We configure a "Log Sink" within the customer's Google Cloud or Azure environment. This automatically pushes every network event into a Message Queue (like Google Pub/Sub or Azure Event Hubs).*
- *Secure Webhooks: Our AI engine "subscribes" to that message queue, streaming the network metadata into our isolated analysis environment in real-time.*

What are the key trade-offs to consider?

- *Sovereignty vs. Performance: Running a Large Language Model (LLM) locally on a customer's server (Phase 2) ensures absolute data privacy but requires more expensive hardware (GPUs) compared to a centralized cloud API.*
- *Real-Time vs. Batch: Real-time analysis of every packet is computationally expensive. Our MVP trades "Real-Time“ for "High-Frequency Batch" (every 5 mins) to keep costs down while remaining effective for audits.*

Are you training a model in-house, or using pre-trained APIs/no-code tools?

- *We use Pre-trained, Open-Source Large Language Models (like Llama-3-8B or Mistral) to provide the base "reasoning" capability. This avoids the massive cost of training a model from scratch.*
- *We fine-tune these models in-house on a proprietary dataset of Network Protocols and BGP Path behavior. This makes the model a "Domain Expert" in enterprise networking.*

Why No-Code?

- *We will use "No-Code" tools for the initial Phase 1 Prototyping (e.g., LangChain or Google Vertex AI) to validate the UI/UX before moving to the custom local engine in later phases*

Thank You!