WHITE PAPER

Sovereignty-by-Design

A Strategic Framework for Data Control and Resilience

ENTRUST

SECURING A WORLD IN MOTION

Table of Contents

The Global Data Sovereignty Crisis: Beyond Physical Residency

Data sovereignty has undergone a fundamental shift from physical residency to jurisdictional control. In an era of extraterritorial reach, the geographic location of a server is no longer the primary determinant of legal risk. Sovereignty is now defined by the interplay of legal jurisdiction, operational custody, and the technical ownership of encryption keys. Traditional cloud security models, built primarily for confidentiality, have reached a point of obsolescence in the face of these systemic jurisdictional risks.

The standard "encryption at rest" model provided by cloud hyperscalers is insufficient for modern enterprise requirements. Because cloud providers typically generate, manage, or maintain technical access to encryption keys, they retain the ability to override customer intent. When a provider holds the keys, they can be compelled by foreign authorities to decrypt and disclose data – rendering contractual safeguards and local residency irrelevant against national security inquiries or lawful access requests.

Considerations for Encryption Keys Being Used in the Cloud

Ownership – aka Responsibility

- Specifically denotes to whom the keys belong
- In the common cloud security responsibility matrix, information and data is always the responsibility of the cloud consumer
- Keys that are intrinsically linked to the data they protect usually have the same characteristic

Control – aka Management

- Specifically denotes who can carry out the various key management lifecycle tasks
- Having control means being able to carry out key lifecycle tasks and often automating them but also includes precluding others from this capability

Possession or Holding

- Specifically denotes who owns the infrastructure or geographic location where the keys physically reside

To mitigate this, CISOs must transition from policy-based assurances to structural architectural requirements. Achieving true sovereignty requires the deliberate separation of the trust layer from the data plane. By ensuring that no single third-party provider possesses the technical means to access cleartext data or usable keys, organizations can finally decouple their data security posture from the legal jurisdiction of their infrastructure providers.

Strategic Insight: Sovereignty is no longer a compliance checkbox; it is an architectural requirement. If you do not own the keys, you do not own the data. Organizations must transition from relying on provider-managed security to implementing technical measures that eliminate a provider's ability to access cleartext data.

The Four Converging Pressures on Enterprise Data

Jurisdictional Overreach

Governments are aggressively expanding surveillance authorities that apply extraterritorially. Under the **U.S. CLOUD Act**, the **EU e-Evidence Regulation (2023)**, and the **UK Investigatory Powers Act**, authorities can compel disclosure of data regardless of where it is physically stored. This creates a landscape where **Schrems II** and **GDPR** compliance cannot be met through standard contractual clauses (SCCs) alone. Furthermore, residency laws in **Canada** and the APAC region increasingly view provider-held keys as a violation of sovereign control.

AI Exposure: The Structural Risk

Cloud infrastructure has evolved into AI infrastructure, optimized for massive-scale data processing. Hyperscalers are training large language models (LLMs) on the same environments hosting enterprise workloads. Because these systems are designed for ingestion, contractual promises of "no training" are technically unenforceable if the provider holds the keys. This creates a structural risk where sensitive intellectual property can be ingested into a provider's AI model without explicit, verifiable technical blocks.

Key Control Gaps

A critical vulnerability exists when cloud providers manage the root of trust. While provider-managed encryption offers an "illusion of security," it ensures the provider retains the technical means to decrypt data for internal processes or to satisfy laws like **FISA 702**. The gap between provider-managed keys and customer-owned hardware security modules (HSMs) represents the difference between a privacy policy and a sovereign guarantee.

Operational Fragility

Centralized storage architectures create single points of failure. High-profile regional outages, such as the **Azure AD 2023** failure or recurring **AWS US-EAST-1** disruptions, prove that reliance on a single provider's infrastructure is a business continuity risk. Traditional encryption protects confidentiality but fails to address **integrity** and **availability** – leaving data vulnerable to deletion or corruption during ransomware attacks.

The Illusion of Security: Why Traditional Cloud Encryption Fails

The distinction between standard encryption and true sovereignty is the difference between permission-based access and ownership-based control.

Feature	Standard Cloud Encryption	True Sovereignty
Key Ownership	Provider generates and manages keys.	Customer generates and holds keys in an HSM
Access Control	Provider can override customer intent for legal requests.	Only the customer can authorize decryption.
Jurisdictional Risk	Subject to provider's legal jurisdiction (e.g., CLOUD Act).	Technical measures prevent any single provider from seeing cleartext.
AI Protection	Cleartext is available for AI model training if keys are held.	Data is fragmented and unreadable to AI systems.
Operational Resilience	Single-provider failure leads to data unavailability.	Self-healing multi-cloud distribution ensures continuity.
Compliance Alignment	Insufficient for EDPB Use Case 5/Schrems II.	Fully aligned with technical safeguard requirements.

The Sovereignty-by-Design Architecture: Entrust File Encryption

The Entrust File Encryption solution establishes a new standard by separating the **identity/trust layer** from the **data-plane operations**. This unified architecture ensures that cryptographic trust authorizes every data-plane action, while the data itself remains fragmented and unreadable to the infrastructure host. Crucially, the **"agentless"** nature of this architecture ensures these protections are implemented with **no performance penalty** and no complex endpoint management.

The platform provides six core capabilities:

- **Post-quantum ready HSMs:** Providing a hardware-enforced root of trust
- **Multi-Cloud Key Management and Compliance Manager:** Tools to understand exactly where, when, and how keys are rotated and used
- **Agentless File Encryption:** High-performance protection without the overhead of software agents
- **Fragmentation:** Sharding data to eliminate single-provider access to meaningful information
- **Multi-Cloud Distribution:** Storing data fragments across diverse, customer-owned accounts
- **Self-Healing Data Clusters:** Automatically reconstructing tampered or lost data for resilience

Technical Pillar I: Cryptographic Trust via Entrust HSMs

True sovereignty is anchored in hardware security modules (HSMs), which provide a tamper-resistant boundary for the root of trust. Entrust nShield HSMs enable the enforcement of **Hold-Your-Own-Key (HYOK)** models, which offer a higher level of sovereignty than standard Bring-Your-Own-Key (BYOK) by ensuring keys never leave the customer's controlled environment.

1. **Generate:** Securely creates cryptographic keys within a certified, hardened boundary
2. **Store:** Houses keys inside certified hardware, preventing extraction even under provider pressure
3. **Perform:** Executes all cryptographic operations inside the module, away from the host OS
4. **Protect:** Safeguards keys from unauthorized access, legal subpoenas, or operational errors
5. **Support Compliance:** Helps ensure adherence to FIPS 140-2/3, PCI, and eIDAS standards

Technical Pillar II: Data Fragmentation

Data fragmentation moves beyond traditional encryption by ensuring that no single cloud provider ever possesses a complete or meaningful dataset.

- **Ingest:** Data is brought into the platform where content, filenames, and metadata are immediately encrypted using agentless file-level encryption, ensuring **no performance degradation.**
- **Fragment:** Files are sharded into data fragments. All file structure and metadata are stripped and decoy data is mixed in to obscure the original information.
- **Distribute:** These meaningless fragments are containerized and distributed across multiple **customer-chosen and customer-owned** storage locations (e.g., AWS, Azure, on-premises).
- **Reassemble:** Upon a valid read request, fragments are reassembled transparently for the user. Because the process is agentless, the user experience remains seamless.

Solving the AI Infrastructure Risk

Because cloud infrastructure is now inextricably linked with AI training systems, organizations require technical controls rather than contractual promises. In environments optimized for massive-scale data processing, fragmented data is the only verifiable defense. Entrust ensures that the "data" available to a cloud provider is merely a collection of meaningless shards and decoy data.

Protection Checklist:

- **Cleartext Data:** Fragments are unreadable and incomplete; impossible to ingest into LLMs.
- **File Metadata:** Stripped during fragmentation to prevent data indexing.
- **Data Structure:** Destroyed through fragmentation, preventing structural pattern recognition by AI.
- **Encryption Keys:** Anchored in Entrust HSMs, remaining entirely outside the provider's infrastructure.

Cyber Resilience: The Self-Healing Data Ecosystem

Sovereignty without resilience is incomplete. Traditional encryption protects confidentiality but leaves data vulnerable to the "missing dimensions" of security: integrity and availability. The Entrust virtual cluster continuously verifies the integrity of distributed fragments. If data fragments are lost due to a regional cloud outage or corrupted by a ransomware actor, the system automatically reconstructs the data from remaining fragments without manual intervention.

This architecture transforms multi-cloud complexity into a strategic advantage, allowing for automatic failover and protection against administrative errors or malicious destruction.

Gartner identifies data fragmentation as an infrastructure-level mechanism and a privacy-enhancing technology (PET) capable of enforcing sovereignty by ensuring that no single processor ever holds meaningful data.

Strategic Use Cases and Regulatory Alignment

Cross-Border Transfers (Schrems II/GDPR)

This architecture is a perfect implementation of **EDPB Use Case 5**, which approves split processing and technical measures that prevent processors from ever holding cleartext. By distributing data fragments across multiple jurisdictions, organizations can utilize U.S.-based cloud providers while technically mitigating CLOUD Act risks and meeting strict **Canada/APAC** residency requirements.

Ransomware & Integrity

The solution aligns with **NIS2, DHS critical infrastructure directives,** and **financial services operational resilience standards** by ensuring data integrity. By moving away from centralized storage, the "blast radius" of an attack is neutralized. Even if an attacker accesses a storage bucket, they cannot reassemble the data, and the self-healing cluster restores compromised shards automatically.

Multi-Cloud Availability

The solution enables continuous availability during hyperscaler regional outages. By replicating fragments across a mix of providers (e.g., AWS and Azure) and on-premises nodes, the architecture ensures that a failure in one provider does not result in a failure of data access, meeting the highest availability tiers.

Conclusion: Future-Proofing the Sovereign Enterprise

Entrust allows enterprises to leverage the scale of global hyperscalers without surrendering control. This "Sovereignty-by-Design" approach ensures that even under legal subpoena or cyberattack, the cloud provider has nothing meaningful to surrender and the data remains available to the rightful owner.

Executive Summary Table

Outcome	Achievement	
True Sovereignty	Data never exists in readable form with a cloud provider; HYOK enforcement.	✓
AI Protection	Structural fragmentation prevents ingestion into LLM training models.	✓
Regulatory Compliance	Aligned with GDPR, Schrems II, NIS2, and DHS resilience directives.	✓
Business Resilience	Self-healing clusters protect data integrity and availability during outages.	✓

Strategic Comparison: Future-Proofing Data Sovereignty and Resilience

Capability/Sovereignty Requirement	Traditional Cloud Encryption	BYOK/HYOK	Entrust
Root of Trust	Cloud provider-controlled	Key outside provider, but service still cloud-dependent	Customer-controlled HSM root of trust
Key Storage & Control	Provider KMS	External key management	Entrust HSMs under customer control
Key Access	Provider-accessible	Subpoena-vulnerable	HSM-enforced, non-extractable
Prevent Cloud/AI Provider Access	Provider can decrypt; files readable	Partial protection	No reconstructable data; no data, no keys
Block AI Model Ingestion	Files readable by provider	Metadata exposed	Files sharded; metadata removed
Sovereignty Enforcement	Policy/contract-based	Partial technical alignment	Technically enforced (HSM + data fragmentation
Keep Data Within Legal Jurisdiction	Stored/readable in provider cloud	Key outside, data inside	Physically distributed in customer-controlled locations
Jurisdictional Exposure	Provider jurisdiction	Reduced but still exposed	Decoupled via HSM + data fragmentation
Ransomware/Integrity Protection	Confidentiality only; encrypted files deletable	Still centralized	Integrity + self-healing, distributed
Outage Recovery/ Resilience	Single-region, provider-dependent	Latency challenges	Multi-cloud, regionally redundant, autonomous recovery
GDPR/Compliance (Use Case 5)	No split processing	Partial alignment	Full compliance via data fragmentation

For more information on file-level encryption, visit:

entrust.com/products/cryptographic-security-platform/agentless-file-encryption

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries. For more information, visit www.entrust.com.

For more information, visit **entrust.com.**

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION