



Sertainty + SecureCo: Self-Protecting Data & Stealth-Driven Network Security

Who We Are

- **Sertainty**

A leader and trailblazer in data-layer security, Sertainty embeds self-protecting metadata and fine-grained policy enforcement directly into files and data streams—ensuring persistent auditability and tamper-proof governance wherever data travels.

- **SecureCo**

A pioneer in shielding and anonymizing networks, devices, and cloud connections from identity leaks, exploitation, and breach, SecureCo neutralizes conventional TCP/IP vulnerabilities, obscures traffic patterns end-to-end, and seamlessly integrates with cloud and on-premise environments.

What We Do Together

By unifying Sertainty's self-protecting data technology with SecureCo's network cloaking, we deliver an end-to-end zero-trust platform that:

- Protects data at rest, in motion, and in use, including quantum-resistant encryption and self-enforcing file policies
- Obfuscates both file contents and network metadata, cloaking traffic paths and endpoints
- Audits every transaction with immutable audit trails and non-repudiated logs for easy compliance reporting
- Integrates out-of-the-box with AWS, Azure, Google Cloud, OneDrive, S3, Splunk, MSSPs, and more

Recent Proof-of-Concept (PoC) Highlights

- **Scope:** Hybridized and Interoperable data protection across field, industrial, commercial, and enterprise domains
- **Achievements:**
 - Demonstrated SecureCo's multi-layer cloaking of data payloads and sensor telemetry
 - Validated Sertainty's granular policy enforcement and tamper-proof audit trails
 - Verified zero-impact performance: seamless latency overhead under full obfuscation
 - Seamless integration with third-party cloud storage providers

Core Capabilities & Roles

Capability	Sertainty Role	SecureCo Role
Self-Protecting Data Utility	Embeds persistent metadata; enforces file-level policies	Software-Defined-Transport Protocol
Cloaking & Anonymization	Non-deterministic encryption. Managed sessions. Safe AI training	Masks network paths/APIs, Conceals endpoints; thwarts traffic analysis and Generational Adversarial Networks
Multi-Cloud Gateway	SDKs for OneDrive, Google Drive, S3	Software-Defined Tunnels for cloud deployments
Chain-of-Custody Logging	Immutable audit trails, non-repudiation	Resilient Data Arteries
Plug-in Extensibility	API hooks for AI/ML; private internet links	MSSP/SIEM connectors (e.g., Splunk, Dynatrace, etc.)
Zero-Trust Enforcement	Self-managing, fully contained encryption, granular access policies	Network-layer stealth/ephemeral circuit-nodes
Policy Driven Rules	Time, location, and network policy controls over data protection	Business rule enforcement policies balancing performance, access and security risk posture

Business Benefits

- **Risk Reduction:** Eliminates TCP/IP attack surfaces and metadata leaks to lower capital needs.
- **AI Resilience:** Protects against AI-driven malware and data-poisoning attacks.
- **Regulatory Compliance:** Provides tamper-proof audit logs for GDPR, HIPAA, and CMMC readiness.
- **Performance Efficiency:** Delivers multi-layer security with minimal latency.
- **Rapid Deployment:** Deploys in days via prebuilt connectors, avoiding costly hardware.
- **Convergence:** Unifies OT and IT visibility on a single platform.

Contact Us:

Amir Sternhell | CSO, Sertainty: amir.sternhell@sertainty.com

Eric Sackowitz | CTO, SecureCo: eric@secureco.io

