ASTIS

Cryptographic trust layer for business data

Infrastructure access shouldn't mean data access.

ASTIS keeps business-payload plaintext out of cloud operators, AI tools, vendors, and infrastructure control planes by separating plaintext, keys, access policy, and audit evidence.

Customer-controlled keys | **Regional deployment options** | **HYOK key custody** | **Verifiable evidence**

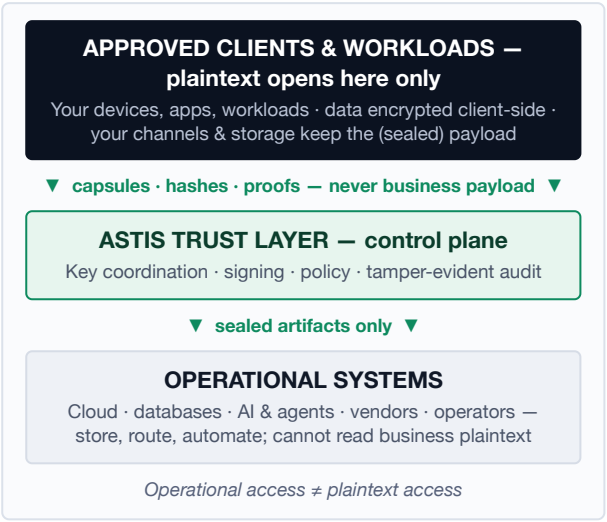
THE PROBLEM

Modern business runs on operators — cloud providers, on-prem admins, AI tools, vendors, MSPs, contractors. They need operational access. **They do not need business-payload plaintext.** Zero Trust access controls *who* can reach a system; ASTIS controls *what that system, workload, vendor, or agent can actually see*. It composes with IAM, Zero Trust Network Access (ZTNA), and KMS.

THE ASTIS BOUNDARY

ASTIS is a **control plane, not a plaintext data path**. Business payload — emails, documents, application fields, secrets — is encrypted client-side and stays under customer control, in your own channels and storage. ASTIS receives cryptographic artifacts only: key capsules, hashes, policy signals, audit events.

A breach of ASTIS, a subpoena to ASTIS, or a storage-layer breach yields **no business-payload plaintext**. Storage, encryption, access, and audit remain separate trust boundaries.



ONE TRUST LAYER — MULTIPLE INTEGRATION PATHS

APIs · SDKs · workload-bound secrets · workflow/YAML · MCP · HYOK key custody

Regain control over sensitive data across cloud, on-prem, and hybrid environments — products, workloads, vendors, AI tools, and operators work without becoming plaintext holders. **Infrastructure can operate; sensitive data stays under your control.**

COMMUNICATE
ASTIS Mail

Secure communication alongside Gmail and Microsoft 365 — no migration. Message content stays encrypted; keys and access policy are separated from mailbox storage. TTL limits long-term exposure.

Learn more → astis.io/product/mail

vs Proton/Virtru/Tuta → astis.io/compare

BUILD WITH APIs / SDKs
ASTIS API Platform

Use APIs and SDKs to add sealed-envelope encryption, hash-only sign/verify (a 32-byte digest, never the file), FPE/tokenization, key capsules, policy checks, and tamper-evident audit to your own product — regulated-data controls without building crypto yourself.

Learn more → astis.io/pricing/api

SDKs on GitHub → github.com/astis-io/astis-sdk

PROTECT WORKLOADS
Workload Secrets

Adds the runtime boundary Vault/KMS does not provide. Vault/KMS governs custody and release to authorized clients; ASTIS binds plaintext release to the attested workload — decrypted only inside that workload, in RAM, at use time. Cluster admins, etcd backups, CI logs, vendors, and cluster-read agents get ciphertext.

Learn more → astis.io/workload-secrets

vs Vault/ESO/SOPS → /compare/workload-secrets

OWN KEY CUSTODY
HYOK CVS

Keys and decryption authority stay in customer-controlled infrastructure. ASTIS coordinates cryptographic workflows without holding plaintext or key authority. HSM support; EU/EEA, US, or customer-hosted residency by agreement.

Learn more → astis.io/security

Talk to sales → astis.io/contact

AI / MCP: the same controls exposed to agents over MCP — sign, verify, tokenize, and request sealed operations without business plaintext in model context, unless runtime access is explicitly granted. **Learn more → astis.io/mcp**

BUILT FOR REGULATED DATA — NIS2 · DORA · HIPAA · GDPR · AI GOVERNANCE

NIS2 / DORA — essential entities (energy, transport, health, water, digital infrastructure, public administration), financial institutions, and ICT third-party risk programs: supplier, cloud, operator, and infrastructure plaintext exposure reduced by architecture.

NIS2 → astis.io/critical-infrastructure
DORA → astis.io/financial-services

HIPAA / Healthcare — providers, payers, and business associates handling PHI: HIPAA-aligned workflows with customer-controlled keys and audit evidence; BAA available for Enterprise/HYOK. No HIPAA certification claimed.

Healthcare → astis.io/healthcare

GDPR / AI governance — Art. 32 encryption support, TTL-bounded data minimisation, audit evidence, and regional deployment options including EU/EEA managed data plane and HYOK. Sensitive plaintext stays out of model context unless runtime access is explicitly granted.

Legal & professional → astis.io/legal-services

Don't take trust on faith. ASTIS sees zero business-payload plaintext at the edge — capsules, proofs, policy metadata, and audit events only. A compelled disclosure to ASTIS yields no business-payload plaintext. Release evidence is publicly verifiable — gpg/sha256, no ASTIS account (**github.com/astis-io/releases**); technical review pack under NDA. Live workload checks run on a real Kubernetes cluster; pod-side clients are open source.

Assurance: CASA Tier 2 complete · SOC 2 Type II in progress · ISO 27001 planned · no HIPAA/PCI/FedRAMP certification claimed — ASTIS provides the controls and evidence; the compliance verdict belongs to your assessor.

Talk to ASTIS

astis.io/contact

Try the API — portal.astis.io

Try Mail — mail.astis.io