tiCrypt

A Platform for Regulated Workflows

NIST SP 800-171 - CMMC LEVEL 2 - ITAR - FIPS 140-3

End-to-End Encrypted Compute Environments

A single, integrated on-prem environment for storing, sharing, and processing sensitive information - without exposing data to endpoints or administrators.

How it works

- Secure enclave architecture
- Built-in access control & auditing
- Administrators cannot access user data; encryption keys remain under user control
- Data remains fully encrypted within a controlled environment - never exposed to user devices
- Users interact with data through secure sessions; endpoints act only as display terminals
- VM access through terminals and RDP
- Fine-grained permissions and continuous logging are enforced by the platform

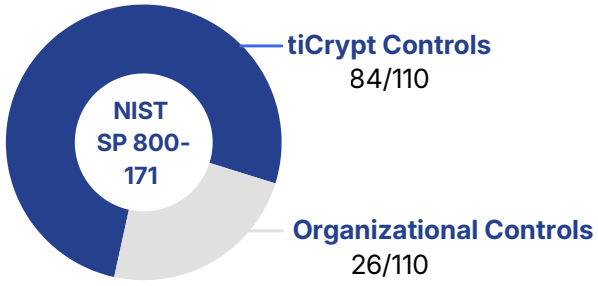
A proven solution

- Zero-trust design
- Full audit trail with tamper-resistant log
- Designed for complex regulated workflows
- On-prem deployment (bare metal), no vendor access to data
- HPC (SLURM) integration
- Zero compromises on data security
- 100% pass track record for external assessments (NIST SP 800-171/CMMC Level 2)

Deployment flexibility

- On-prem infrastructure, hardware agnostic
- Unlimited isolated (sub) enclaves for projects and subcontractors
- Scales from small teams to large multi-project environments
- Predictable cost of ownership

Enforces key NIST SP 800-171 controls



Learn more: **https://ticrypt.com**

(352)-514-0743 info@terainsights.com https://ticrypt.com