SD3 TECH

LUMIS Secure

BY SD3 TECH

REGULATED ENVIRONMENTS · CMMC · HIPAA · ITAR

Air-gapped AI for compliance-driven networks. Zero cloud. Full audit architecture.

THE AI COMPLIANCE PROBLEM:

Every cloud AI tool — ChatGPT, Copilot, Gemini — sends your data outside your network the moment you use it.
For CMMC, HIPAA, and ITAR environments, that is not an option. LUMIS Secure closes that gap.

CMMC LEVEL 2 PRACTICE DOMAINS — HOW LUMIS SECURE MAPS

CMMC · AC **Access Control**	Role-based gating controls what each user can query. Supports Level 2 AC.3.017 / AC.3.018.
CMMC · AU **Audit & Accountability**	All queries logged: user, timestamp, session. Wazuh and Splunk compatible.
CMMC · SC **Comms Protection**	Zero external API calls. No outbound data. Operates entirely within your boundary.
CMMC · IA **Identification & Auth**	Integrates with existing auth, MFA, and SSO. No separate credential surface.
CMMC · CM **Config Management**	Deployments managed via Ansible IaC — auditable, versioned, repeatable.
CMMC · MP **Media Protection**	CUI stays on your controlled hardware. Data never transits to uncontrolled media.
HIPAA · §164 **PHI Containment**	No PHI leaves the network. LUMIS never calls external APIs with patient data.
ITAR · §120 **Export Control Ready**	Technical data stays on-prem. No foreign cloud servers. No third-party LLM exposure.

IMPORTANT:

LUMIS Secure supports CMMC compliance but does not certify your organization. Full certification requires an SSP and C3PAO assessment. SD3 Tech can assist with your compliance roadmap.

Ready to close your AI compliance gap? Book a free 15-min audit.

sales@sd3tech.com · (435) 535-1362 · sd3tech.com/lumis

LUMIS Secure · Regulated Environments