

Secure the last hop for CUI.

From cloud enclave to the machine.

One controlled path for CUI, from a FedRAMP Moderate Equivalent Microsoft GCC High enclave to the machines on your floor, and back.

THE CONTROLLED PATH

Cloud ↔ Machine

CUI VAULT + ACCESS GATE

- 01 CUI Vault**
Managed Microsoft GCC High environment
- 02 Encrypted tunnel**
FIPS 140-3 validated site-to-site connection
- 03 Access Gate**
Identity-based access and segmentation
- 04 Authorized assets**
Printers / CNC / CMM / lab equipment

NO AGENTS. NO REWIRING. NO USB.

Control the whole CUI journey. Not just the cloud.

One boundary. One chain of custody. One audit story.

01 ISOLATE CUI IN GCC HIGH

Users and data stay inside a managed GCC High environment, CMMC Level 2 ready.

02 CONTROL AUTHORIZED ASSETS

Identity-based access and segmentation in front of printers, CNCs, CMMs and legacy OT.

03 SEND CUI DIRECT TO MACHINES

Drawings, toolpaths and jobs go direct. No local downloads, email or USB.

04 BRING DATA BACK SECURELY

Inspection results, as-built records and logs return the same controlled path.

05 UNIFIED SSP + EVIDENCE

Enclave and shop floor in one SSP, with mapped evidence and session logs.

06 NO RIP-AND-REPLACE

Machines keep their addresses, firmware and vendor support.

WHY IT MATTERS

Secure CUI from the cloud to the machine.

Access Gate extends enclave control to authorized printers, CNC machines, CMMs and lab equipment, so CUI never travels through an uncontrolled workstation, inbox or thumb drive.

THE TROUT + CUI VAULT MODEL

CUI Vault secures the enclave and the compliance workflow. Access Gate governs the plant floor and the last hop.

SAME MISSIONS. STRONGER TOGETHER.

BUILT FOR

Manufacturing + Engineering

Machine shops

Labs

R&D

Defense suppliers

Book a discovery call today

trout.software

hello@trout.software