GOVERNMENT AND DEFENSE

A governed AI gateway that runs inside your enclave.

Janus Edge is a self-hosted gateway between your people and the AI models they use. Every request is tied to a signed-in person, checked against that person's model grants, screened for sensitive data and recorded for your SIEM. It is designed for air-gapped DoW (DoD) environments and designed to support your ATO.

FIPS EDITION

FIPS 140-3: uses the validated Go Cryptographic Module (CMVP certificate #5247) in approved mode.

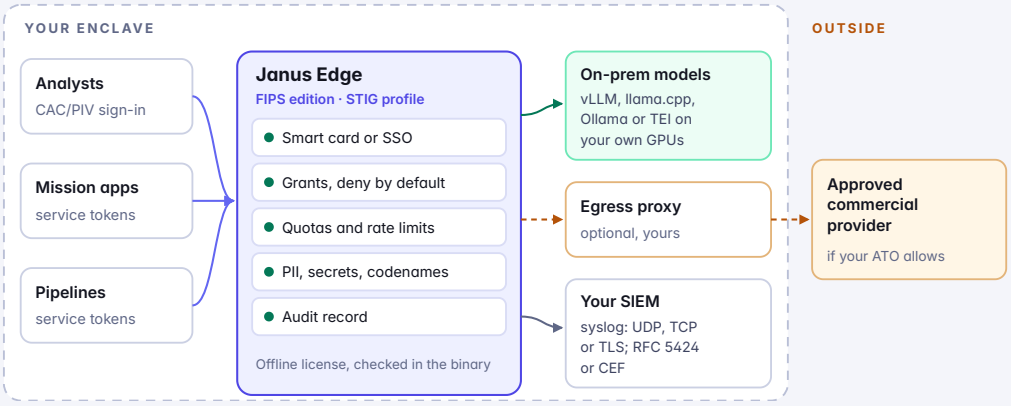
STIG PROFILE

A STIG configuration profile **built to the DISA Application Security and Development STIG**, turned on with one switch.

AIR-GAPPED

No internet access needed. Signed license files are verified inside the binary, and nothing phones home.

Where Janus sits



An example enclave deployment

Stays inside.
Requests to models on your own GPUs never leave the enclave.

No internet needed.
The license is a signed file, and the STIG profile turns off update checks and license sync.

Verified outbound.
Every outbound TLS connection checks one trust store that includes the DoD PKI root CAs.

01 · Cryptography

Which module protects the data?

Assessors ask for a module and a certificate, not a vendor's assurance.

The FIPS edition is the same source built with the Go Cryptographic Module v1.0.0 (CMVP certificate #5247) in approved mode. It refuses to start without that module in FIPS mode, and `janus --fips-status` shows the module and what it restricts.

02 · Hardened configuration

How does the baseline stay in place?

Settings drift when someone enables plain HTTP for a test or shortens audit retention.

With `JANUS_STIG_PROFILE=true`, plain HTTP, SQLite, LDAP without certificate checks, untrusted upstream TLS, any phone-home and audit retention under 913 days each stop startup with a named error.

03 · Identity

Can people sign in with their CAC?

Passwords alone don't fit an enclave where everyone carries a smart card.

CAC and PIV certificates are accepted on Janus's own TLS listener or from a trusted proxy, chained to authorities you set and revocation-checked, then matched by UPN, email or EDIPI. You can require administrators to use one.

04 · Accountability

Who used which model, from where?

Investigators need sign-in and access records with an address and an outcome.

Sign-ins, failures, lockouts, time-outs, banner acknowledgments and refused requests are recorded with source address and outcome, exported to CSV in every edition and forwarded to syslog or your SIEM.

SPECIFICATION

What you get in the FIPS edition and STIG profile

Cryptography	FIPS 140-3: uses the validated Go Cryptographic Module (CMVP certificate #5247) in approved mode (FIPS edition). The binary will not start unless that module is linked with FIPS mode on.
Delivery	Container image `ghcr.io/torvanis/janus:<version>-fips` next to the default image, plus FIPS edition binaries and offline image archives for Linux (amd64, arm64).
Restricted features	Switched off where the module does not approve the algorithm: SHA-1 authenticator codes, legacy bcrypt hashes, PDF report export, encrypted PDF attachments, the evaluation sign-in, LDAP skip-verify and untrusted upstream certificates.
STIG profile	Built to the DISA Application Security and Development STIG. `JANUS_STIG_PROFILE=true` sets the STIG defaults, works in either edition and logs a startup line listing the profile in force.
Refused at startup	Plain HTTP, SQLite, the evaluation sign-in, LDAP skip-verify, untrusted upstream TLS, update checks and license sync, and audit retention under 913 days.
Sessions, passwords	Idle sign-out in minutes for people and administrators, longest session, sessions per person, lockout, and password length, complexity, history and age. **Apply DoD STIG values** fills them in for review.
Notice and consent	The DoD Notice and Consent Banner, or your own text, acknowledged before any sign-in method.
Trust, revocation	One outbound trust store with the DoD PKI root CAs (on by default in the FIPS edition). OCSP and CRL checking, hard in the STIG profile.
Audit	Source address and outcome on sign-in and access records; 913-day retention and fail-closed administrative changes in the STIG profile.
Platform	PostgreSQL (SQLite is refused). Linux binary, container image or Helm chart; offline license verification in every edition.

What Janus does not claim

- The Go Cryptographic Module is validated under CMVP certificate #5247. Janus itself is not a validated module.
- The STIG profile is a configuration built to the DISA ASD STIG. No DISA or DoW (DoD) office has reviewed, certified or approved Janus.
- Janus comes with no authorization to operate; the ATO belongs to your system and your authorizing official.
- Janus is self-hosted software, not a cloud service. FedRAMP and DoD cloud impact levels apply to the environment you run it in.
- Audit forwarding, smart cards and hard revocation checking need infrastructure you provide.

Evidence you can show

```
$ janus --fips-status
{ "edition": "fips",
  "fips140_enabled": true,
  "module_version": "v1.0.0",
  "validated_module": true,
  "cmvp_certificate": "#5247", ... }

# startup log, STIG profile on (shortened)
msg="stig profile" enabled=true
  database=postgres offline=true
  audit_retention_days=913
  audit_fail_closed=true
```

The gateway underneath

Signing in grants nothing: each model is granted to a person, group, team or service token, with quotas on tokens, spend or requests. The Security Gateway records, redacts or blocks personal data, credentials and your codenames, and load-balanced pools spread self-hosted models across your GPU servers.

BUSINESS

FIPS edition and STIG profile, bought online.

Per seat from a 5-seat minimum, monthly or annually, by card or US bank account, with your PO number on each invoice. Offline keys come from the portal. The 30-day trial includes both features.

ENTERPRISE

Perpetual keys, purchase orders, an SLA.

An annual contract by invoice or purchase order, with an MSA and DPA. Perpetual keys run every release published by their maintenance date, with air-gap support under an SLA.

TALK TO US

Scope a deployment.

Tell us about your enclave and procurement path; we'll reply with a quote and a trial key.

janusedge.com/contact
janusedge.com/pricing

CMVP certificate #5247 (Go Cryptographic Module, FIPS 140-3) is listed at csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5247. "DoW" is the Department of War, the secondary title of the Department of Defense. Features described as of Janus 2026.11.1 (November 2026); the FIPS edition and STIG profile require a Business, Enterprise or trial license. Janus Edge is source-available under the Elastic License 2.0. Product names are trademarks of their respective owners.