

Security, operations and vendor risk

This sheet answers the questions a vendor and third-party risk assessment asks first. All statements refer to the MxENV3 product as delivered.

SUPPLIER

Company	Business Technology Consulting OÜ, Sepapaja tn 6, 15551 Tallinn, Estonia
VAT ID	EE102237496
Registry	Estonian Commercial Register (Äriregister)
Contact	info@mxenv3.com
Product	MxENV3 — environment and operations tool for Murex MX.3, delivered as one Go binary.

DEPLOYMENT MODEL AND DATA FLOW

- Fully on-premises or in your own cloud: no SaaS component, no licence server, no phone-home, no outbound connection to us.
- No agents on the Murex hosts. Execution runs through your Ansible and SSH with the accounts you define.
- No customer, trade or market data leaves your infrastructure. MxENV3 processes configuration, not trading data.
- Optional metrics (OpenTelemetry) go to your own collector, not to us; the export is fail-open and can stay switched off.
- An optional central inventory server (TLS, token authentication) runs inside your network.

CREDENTIALS AND SECRETS

MxENV3 stores no secrets. Passwords are referenced by name and resolved from your vault at apply time — the repository, the inventory and the rendered files never contain them in plaintext by design.

Supported secret providers: CyberArk (AIM CLI), Ansible Vault, Infisical, KeePass, environment variables. Values are resolved at apply time, passed to tools on stdin, and never written into the inventory, the repository or the command line.

CHANGE SAFETY AND EVIDENCE

- Any command that changes a production environment refuses to run without explicit confirmation. Read-only commands and dry-runs are always safe — also at 3 a.m.
- Configuration lives in Git: who changed what, when and why. On demand, MxENV3 compares the rendered configuration against the files actually deployed on the hosts and reports differences and missing files. That lets you prove to an auditor that the environment matches the repository, instead of asserting it.
- Moving configuration objects between environments leaves an audit line; production and read-only environments are locked.
- Every command follows an exit-code contract (0 OK / 1 WARNING / 2 ERROR / 3 UNKNOWN) and can run as a dry-run.

DELIVERY, MAINTENANCE AND CONTINUITY

- Each delivered binary is built for your institution, with licence term and version compiled in. You always know what you run and until when. Nothing calls out of your network.

- MxENV3 has no runtime dependency on us: no licence server, no phone-home, no cloud component. Your inventory is plain YAML in your Git, your rendered configuration is plain files on your hosts — both remain readable and usable without the binary. Source-code escrow with a European agent and a fallback licence can be arranged on request; we provide the documents for your third-party risk assessment.
- Fixes and new features are delivered as a new binary and installed like any other file.
- Coverage, response targets and the escalation path are agreed in the contract, up to named on-call cover for the EOD window.

SUB-PROCESSORS

For the product	None. MxENV3 runs exclusively on your infrastructure.
For this website	Vercel (hosting, EU DPA and Standard Contractual Clauses), OpenPanel (cookieless analytics, EU-hosted), our own mail server for form submissions.

OUT OF SCOPE

MxENV3 does not patch, install or upgrade MX.3 itself, does not touch trade or market data, and replaces neither the vendor-supplied installation and administration tools nor your scheduler, your monitoring or your CI/CD. It manages what surrounds them: environment configuration, service orchestration, batch execution and the operational routine across 30 to 50 environments. On a Murex version we have not yet validated, applying the configuration with --strict stops instead of guessing.