# MOLI Security Overview

**private cloud · zero shared tenants · quantum-safe**

**Perdix Software treats your confidential manufacturing data with care and control.**

## SECURITY IS ARCHITECTURE, NOT AN AFTERTHOUGHT

Your proprietary manufacturing data represent years of investment — and real responsibility. You should be able to verify your deployment, control access, and expect the same standard of care from a vendor that you demand internally. From physical controls to post-quantum cryptography, MOLI's security posture is active, layered, and proven.

**1:1**
DEDICATED SERVER PER CUSTOMER

**NIST PQC**
POST-QUANTUM READY ENCRYPTION

## PROTECTION AT EVERY LAYER

### General Protection

A mutual NDA is signed with every customer before work begins. All Perdix employees sign **NDAs and Invention Assignment Agreements** upon hire and are subject to background checks. Employees are trained to treat **all** data as confidential; access to customer systems and data is granted strictly on a **need-to-know basis.** All access is terminated immediately on offboarding.

### Physical Security

MOLI cloud infrastructure runs on **Amazon Web Services** — SOC 2 Type II, ISO 27001, and FedRAMP-authorized data centers with biometric access controls, monitoring, and redundant power. Perdix offices use **logged keyfob entry**, a formal building sign-in procedure, a secure lockbox for printed material and removable media, and a fully isolated guest/device Wi-Fi network with no path to corporate infrastructure.

### Identity & Access Management

MOLI supports **Multi-Factor Authentication** via TOTP app, security key, SMS, email, or voice call. Single Sign-On via OIDC is supported as both consumer and provider. On the floor, kiosk-optimized single-factor (employee ID, barcode, keyfob) minimizes friction while maintaining accountability. **Role-based access control** and Explicit Mode limit access to what is appropriate to that user at that location.

### Dedicated Infrastructure

Every customer has their own private server — **never a shared multi-tenant environment.** Each deployment uses **unique service keys** for every external integration so a compromise in one deployment cannot reach another. Perdix staff have no routine access to customer infrastructure; access is granted to specific individuals for specific reasons at specific times only.

### Network Access Controls

Network access to each MOLI server is restricted by **customer-specific firewall rules** at the infrastructure level. HTTPS is enforced on all endpoints; all traffic uses **TLS 1.3** with forward-secret cipher suites. HTTP Strict Transport Security (HSTS) and secure cookie attributes are enforced platform-wide. Inbound port exposure is minimized to only what is operationally required.

### Software Development Security

All service keys and secrets are stored **separately from source code**. Source code is maintained in a controlled-access repository supporting multi-factor authentication. Every change undergoes **formalized peer review** and test suites are run before deployment. Developers have no routine access to customer data — access is granted only to diagnose specific issues in specific environments.

### Software Bill of Materials

All third-party code is thoroughly evaluated before inclusion — license, history, and supply chain risk assessed by the designated Codemaster role. All code is **pinned to specific versions,** and served via **private package infrastructure** — eliminating the most common software supply chain attack vectors. A live **SBOM Dashboard** is available within each deployment for independent customer verification.

### Audit & Compliance Logging

Every user action, configuration change, and system event is logged with **who, what, when, and from where** — persistently, in detail. Logs are available for export in standard, non-proprietary formats and surfaced in the MOLI dashboard for immediate review. MOLI's audit architecture is aligned with **NIST 800-171, DoD CMMC, FDA 21 CFR Part 11, and ISO 9001/13485** requirements for electronic records, signatures, and traceability.

### Quantum-Safe Cryptography

MOLI server infrastructure protects your production data against "harvest now, decrypt later" attacks that may occur as quantum computer hardware matures. Using NIST post-quantum algorithms, TLS connections to your MOLI deployment can negotiate **ML-KEM key exchange (FIPS 203)** in hybrid mode alongside classical algorithms. See the *Quantum-Safe* section on page 2 for details.

### MOLI Private Cloud

**MOLI Private Cloud** is our term for customer-specific Layer-3 firewall rules deployed at the AWS infrastructure level that restrict all inbound traffic to your MOLI server to your approved IP address ranges — and nowhere else. When MOLI Private Cloud is active, your deployment is invisible to the public internet outside your facility, VPN, or other approved connections. There is no login page to discover, no endpoint to probe, and no attack surface exposed to scanning. It is one of the most effective single security controls available for a cloud-hosted system — and it is applied by default to every MOLI deployment. **Your MOLI server answers only to you.**

## ADDITIONAL SECURITY FEATURES

Additional customer-configurable security features include...

- **Application Firewall**: Restrict MOLI access by IP address; systemwide allow list is extended by API- and Kiosk-specific rules
- **Content Filter**: Inbound content scanning with logging / blocking of requests whose data include credit card numbers, banking numbers, social security numbers, or specific words.
- **Countersign Toolbox**: Verify identity using shared challenge words.
- **Malware Scanning**: Inbound file scanning with logging / blocking of requests whose files are infected with viruses.

## QUANTUM-SAFE CRYPTOGRAPHY — READY NOW, PROTECTED FOR WHAT'S NEXT

**ML-KEM**
FIPS 203 — Key Encapsulation

**ML-DSA**
FIPS 204 — Digital Signatures

**SLH-DSA**
FIPS 205 — Hash-Based Sigs

**Hybrid TLS**
Classical + PQC simultaneously

### Post-Quantum TLS Protects Your Manufacturing Data

Quantum computers capable of breaking conventional RSA and elliptic-curve cryptography are not yet widely deployed — but the threat is real and the timeline is advancing. The attack vector of **"harvest now, decrypt later"** means adversaries can intercept and archive encrypted traffic today, then decrypt it retroactively once sufficient quantum hardware is available. Production records, intellectual property, and personnel data collected now can become exposed in the future if the encryption protecting them is not quantum-resistant.

MOLI deploys on **Ubuntu 26.04 LTS Server**, the first Ubuntu long-term support release to ship NIST's finalized post-quantum cryptographic standards as platform defaults. Secure HTTP connections to your MOLI deployment are capable of negotiating **ML-KEM (FIPS 203) key exchange** in hybrid mode alongside classical ECDHE — so data in transit is protected against both current classical attacks and future quantum decryption simultaneously.

No action is required from your IT team; post-quantum negotiation happens automatically when both endpoints support it, and falls back gracefully when they do not.

## STANDARDS ALIGNMENT & SECURITY CULTURE

### REGULATORY ALIGNMENT

- ✓ NIST SP 800-171 / DoD CMMC — controlled unclassified information and defense cybersecurity controls
- ✓ FDA 21 CFR Part 11 — electronic records, e-signatures, and audit trails
- ✓ FDA 21 CFR Part 820 — medical device quality system regulations
- ✓ ISO 9001 / 13485 — records management, document control, and nonconformance traceability
- ✓ AS9100 / IATF 16949 — aerospace and automotive quality records
- ✓ ITAR / EAR / C-TPAT — controlled data handling and need-to-know access
- ✓ AWS SOC 2 Type II / ISO 27001 — infrastructure-level security assurance
- ✓ NIST FIPS 203 / 204 / 205 — post-quantum cryptographic standards

### SECURITY CULTURE

- ✓ Co-Founder **Steven L Smith** and Principal Engineer **Zach Kruchoski** led security engineering on the Mykonos team at **Juniper Networks** — building enterprise-grade security appliances designed to protect web infrastructure from attackers
- ✓ The engineering team participates in **hacker conferences** and probes their own systems with the same adversarial curiosity
- ✓ A formal **responsible disclosure program** invites independent security researchers to audit the platform at any time
- ✓ Security incidents and near-misses feed directly into engineering retrospectives — findings are fixed, not filed
- ✓ All Perdix staff access to customer infrastructure is **logged, time-bounded, and purpose-specific**
- ✓ Third-party code is **evaluated for supply chain risk** before inclusion

**© 2026 Perdix Software, Inc.** • **MOLI**™, **The MOLI System**™, **Multi-Operation Lean Intelligence**™, the MOLI Seal, MOLI Avatar, and MOLI trade dress are trademarks of Perdix Software, Inc. • All other marks are property of their respective owners and are used for identification purposes only. • This document is provided for informational purposes only and does not constitute a warranty or guarantee of any specific security outcome or compliance determination. No technology or product can be completely secure. Security features, posture, and certifications are subject to change without notice. • Support for Post-Quantum TLS is available in MOLI version 8.3.0 and higher. • moli-security • rev 2-perdix • 2026-11-11

Have a Security Question? **We're Ready.**

PERDIXSW.COM

**Perdix Software**
info@perdixsw.com
(585) 471-6800