CENTO: built for confidence

How CENTO builds enterprise-grade security for industrial systems

In today's industrial landscape, data breaches have become the most pressing cybersecurity threat. According to IBM's 2025 Cost of a Data Breach Report, the average breach costs over $4 million. For critical sectors like energy or manufacturing, the consequences can be even higher. Attackers no longer need to shut down equipment to cause harm. A single disguised file in a messaging app, opened on a technician's phone, can silently compromise an entire operation.

CENTO is built with this reality in mind. Security in the platform is not an add-on. It's part of every layer, from access control and data transmission to network architecture and recovery. The system is designed to minimize attack surfaces, prevent unauthorized access, and ensure that any incident is contained and recoverable.

At the core is role-based access control (RBAC), which ensures that every user sees and does only what's relevant to their job. Default roles like Administrator or Operator can be customized for granular access. Authentication is supported both through local credentials and integration with Active Directory, allowing centralized identity policies and faster revocation of outdated accounts.

Knowing who can access the system is only part of the picture. That's why CENTO includes activity logging, tracking logins, changes, and control actions. These logs support audits, help detect anomalies, and align with international standards like ISO/IEC 27001 and IEC 62443. Logs can be forwarded to external SIEM platforms through Syslog over TLS, ensuring secure and centralized monitoring.

To protect data in motion and at rest, CENTO uses encryption protocols like HTTPS and TLS, alongside optional hardware-level encryption. For lightweight communication between devices, the platform supports MQTT with TLS, which is especially efficient in unstable or low-bandwidth environments.

One more layer of defense is in network segmentation. CENTO operates in architectures that separate Operational Technology (OT) and IT networks, reducing the risk of external access. In highly secure deployments, the platform runs in air-gapped environments, fully isolated from the internet and external systems. Data transfer is only possible through controlled methods such as removable media or one-way gateways.

Access to CENTO's API is tightly controlled through credentials, roles, and IP whitelisting. Unauthenticated requests are rejected outright, and rate-limiting protects endpoints from abuse. Admins can manually revoke user access or respond to anomalies, especially in Active Directory–integrated environments.

If something still goes wrong — whether through misconfiguration, software issues, or a breach — CENTO supports full backup and rollback, allowing operations to be restored quickly and reliably.

Security in CENTO is not one feature. It is a system of interlocking protections that work together to defend against real-world threats. Designed for flexibility and aligned with global standards, CENTO empowers industrial organizations to operate securely, even in the most sensitive and high-risk environments.

CENTO Software HQ
113 West G St #1011,
San Diego, CA 92101
email: info@centosoftware.com
tel: +1 (858) 878 0078